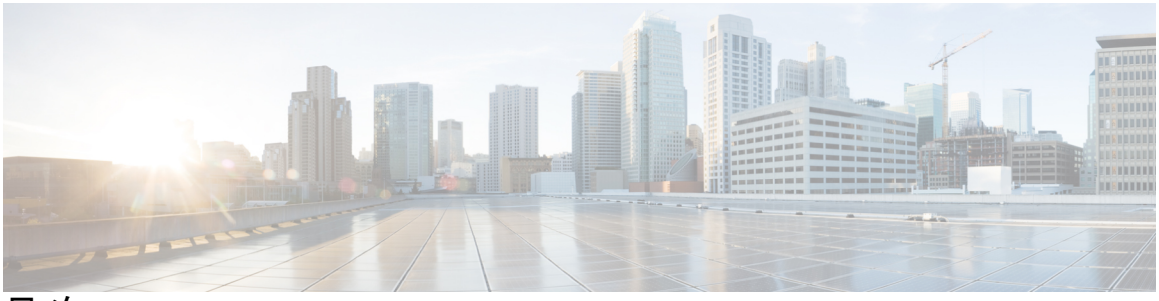
Cisco IOS XE 17.x セキュリティおよび VPN 設定ガイド

初版：2021 年 1 月 11 日

シスコシステムズ合同会社
〒107-6227 東京都港区赤坂9-7-1 ミッドタウン・タワー
http://www.cisco.com/jp
お問い合わせ先：シスコ コンタクトセンター
0120-092-255 （フリーコール、携帯・PHS含む）
電話受付時間：平日 10:00～12:00、13:00～17:00
http://www.cisco.com/jp/go/contactcenter/



目 次

【注意】シスコ製品をご使用になる前に、安全上の注意（ **www.cisco.com/jp/go/safety_warning/** ）をご確認ください。本書は、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。また、契約等の記述については、弊社販売パートナー、または、弊社担当者にご確認ください。

はじめに

ここでは、このマニュアルの対象読者、構成、および表記法について説明します。また、他のマニュアルの入手方法についても説明します。

この前書きは、次の項で構成されています。

はじめに

ここでは、このマニュアルの対象読者、構成、および表記法について説明します。また、他のマニュアルの入手方法についても説明します。

この前書きは、次の項で構成されています。

対象読者および適用範囲

このドキュメントは、Cisco Enterprise ルータの設定担当者を対象としています。このドキュメントの対象者は、主に次のとおりです。

- ネットワーキングに関する技術的な背景知識と経験を持つお客様。
- ルータベースのインターネットワーキングに関する基本的な知識に精通しているが、Cisco IOS ソフトウェアについては経験の浅いシステム管理者。
- インターネットワーキング装置のインストールと設定を担当しているシステム管理者、および Cisco IOS ソフトウェアに精通しているシステム管理者。

機能の互換性

コンフィギュレーション ガイドで説明されているデバイスで使用可能な機能などの Cisco IOS XE ソフトウェアの詳細については、それぞれのルータのドキュメントセットを参照してください。

特定の機能のサポートを確認するには、Cisco Feature Navigator ツールを使用します。これは、特定のソフトウェアリリース、フィーチャセット、またはプラットフォームをサポートする Cisco IOS XE のソフトウェアイメージを判別できるツールです。

表記法

このマニュアルでは、次の表記法を使用しています。

表記法	説明
^ または **Ctrl**	^ および **Ctrl** シンボルは、Ctrl キーを表します。たとえば、**^D** または **Ctrl**+**D** というキーの組み合わせは、**Ctrl** キーを押しながら **D** キーを押すことを意味します。キーは大文字で表記されていますが、大文字と小文字の区別はありません。
string	ストリングは、イタリックで示される引用符を付けない一組の文字です。たとえば、SNMP コミュニティ ストリングとして public を設定する場合、ストリングの前後には引用符を使用しません。引用符を使用すると、その引用符も含めてストリングとみなされます。

コマンドシンタックスの説明には、次の表記法を使用しています。

表記法	説明
ボールド	ユーザが入力するコマンドおよびキーワードを示します。
イタリック体	イタリック体の文字は、ユーザが値を指定する引数です。
[x]	省略可能な要素（キーワードまたは引数）は、角かっこで囲んで示しています。
|	縦棒で区切られている場合、複数の任意または必須のキーワードまたは引数から、1つを選択します。

表記法	説明
[x | y]	角カッコで囲まれ、縦棒で区切られたキーワードまたは引数は、任意の選択肢です。
{x | y}	波カッコで囲まれ、縦棒で区切られたキーワードまたは引数は、必須の選択肢です。

省略可能または必須の要素内に、さらに省略可能または必須の選択肢を含める場合は、角カッコや波カッコを入れ子にして示しています。たとえば、次の表を参照してください。

表記法	説明
[x {y | z}]	角カッコ内の波カッコおよび縦棒は、任意の要素内の必須の選択肢です。

例では、次の表記法を使用しています。

表記法	説明
`screen`	画面に表示される情報の例は、Courier フォントで表します。
`bold screen`	ユーザの入力が必要なテキストの例は、太字の Courier フォントで表します。
< >	山カッコで囲まれたテキストは、パスワードなど、画面に出力されないテキストを表します。
!	行の先頭にある感嘆符（!）は、コメント行を表します。また、いくつかのプロセスでも、Cisco IOS XE ソフトウェアにより感嘆符が表示されることがあります。
[ ]	角カッコは、システム プロンプトに対するデフォルトの応答です。

注意 「要注意」の意味です。機器の損傷またはデータ損失を予防するための注意事項が記述されています。

（注） 「注釈」です。役立つ情報や、このマニュアル以外の参照資料などを紹介しています。

通信、サービス、およびその他の情報

- シスコからタイムリーな関連情報を受け取るには、Cisco Profile Manager でサインアップしてください。
- 重要な技術によりビジネスに必要な影響を与えるには、Cisco Services [英語] にアクセスしてください。
- サービス リクエストを送信するには、Cisco Support [英語] にアクセスしてください。
- 安全で検証済みのエンタープライズクラスのアプリケーション、製品、ソリューション、およびサービスを探して参照するには、Cisco Marketplace にアクセスしてください。
- 一般的なネットワーク、トレーニング、認定関連の出版物を入手するには、Cisco Press にアクセスしてください。
- 特定の製品または製品ファミリの保証情報を探すには、Cisco Warranty Finder にアクセスしてください。

シスコバグ検索ツール

Cisco バグ検索ツール（BST）は、シスコ製品とソフトウェアの障害と脆弱性の包括的なリストを管理する Cisco バグ追跡システムへのゲートウェイとして機能する、Web ベースのツールです。BST は、製品とソフトウェアに関する詳細な障害情報を提供します。

マニュアルに関するフィードバック

シスコのテクニカルドキュメントに関するフィードバックを提供するには、それぞれのオンラインドキュメントの右側のペインにあるフィードバックフォームを使用してください。

トラブルシューティング

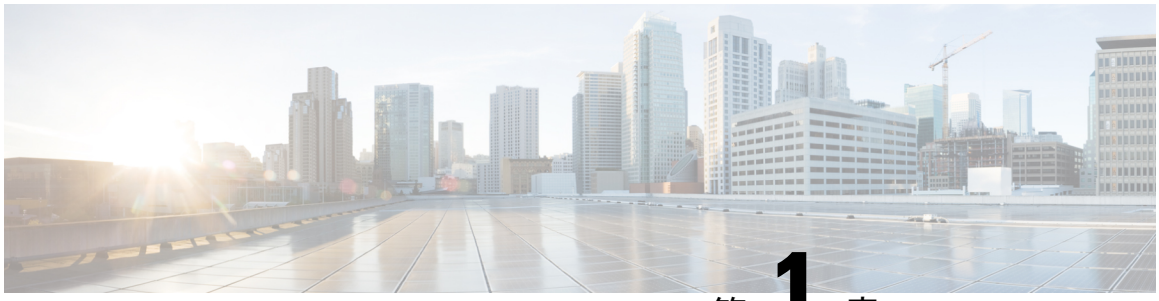
トラブルシューティングの最新の詳細情報については、
https://www.cisco.com/c/ja_jp/support/index.html にある Cisco TAC Web サイトを参照してください。

製品カテゴリに移動し、リストから製品を選択するか、製品の名前を入力します。発生している問題に関する情報を見つけるには、**トラブルシュートおよびアラート**を参照してください。

第 部

Authentication, Authorization, and Accounting（認証、許可、アカウンティング）

- AAA 用のセキュアな可逆パスワード （285 ページ）



第 1 章

認証の設定

認証は、選択したセキュリティ プロトコルに応じてログイン/パスワード ダイアログ、チャレンジ/レスポンス、メッセージング サポート、および暗号化などのユーザーの識別方法を提供します。認証は、ユーザーに対してネットワークとネットワーク サービスへのアクセスを許可する前に、ユーザーの識別を行う方法です。

認証の設定の前提条件

認証の Cisco IOS XE ソフトウェア実装は、AAA 認証方式と非認証方式に分かれています。シスコでは、可能であれば AAA セキュリティ サービスを試用して認証を実装することを推奨します。

認証の設定に関する制約事項

- 設定できる AAA 方式リストの数は 250 です。
- Web 認証は、Cisco IOS XE ソフトウェアではサポートされていません。

認証の設定に関する情報

ここでは、認証方式の名前リストを定義し、このリストをさまざまなインターフェイスに適用して、AAA 認証を設定する方法について説明します。ここでは、RADIUS 認可変更（CoA）を使用した AAA 認証の処理方法についても説明します。

認証の名前付き方式リスト

AAA 認証を設定するには、まず認証方式の名前付きリストを定義し、そのリストを各種のインターフェイスに適用します。方式リストには、実行する認証の種類と、実行するシーケンスを定義します。方式リストは特定のインターフェイスに適用され、定義済みの認証方式のいずれかが実行されます。唯一の例外は、デフォルトの方式リスト（「default」という名前）です。デフォルトの方式リストは、明示的に定義された名前付きの方式リストを持つインターフェイスを除くすべてのインターフェイスに自動的に適用されます。定義済みの方式リストは、デフォルトの方式リストに優先します。

方式リストとは、ユーザ認証のために照会される認証方式を記載したシーケンシャルリストです。方式リストを使用すると、認証に使用するセキュリティプロトコルを1つまたは複数指定できるため、最初の方式が失敗した場合に備えて認証のバックアップ システムを確保できます。Cisco IOS XE ソフトウェアは、ユーザを認証するため、リストに掲載されている最初の方式が使用されます。その方式で応答に失敗した場合、Cisco IOS XE ソフトウェアは、方式リストに掲載されている次の認証方式を選択します。このプロセスは、方式リストのいずれかの認証方式と通信に成功するか、定義されているすべての方式が試行されるまで継続されます。

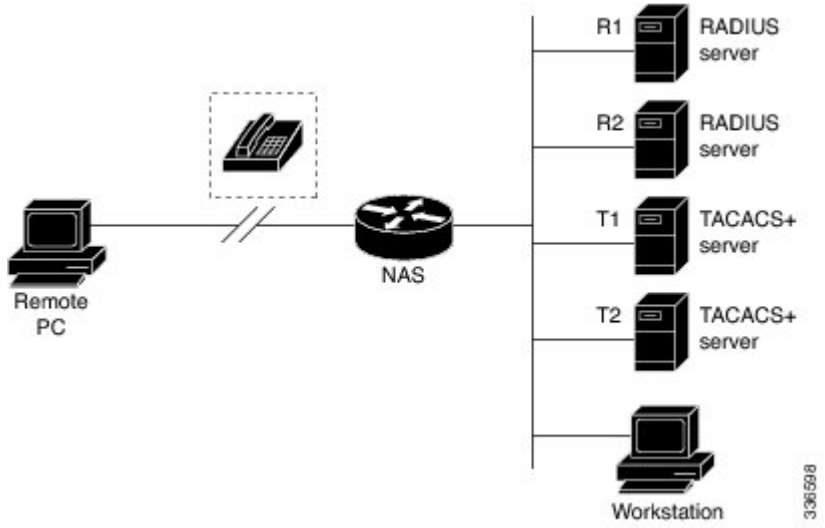
Cisco IOS XE ソフトウェアでは、前の方式からの応答がない場合にだけ、リストの次の認証方式で認証が試行される、という点が重要です。このサイクルの任意の時点で認証が失敗した場合（つまり、セキュリティ サーバまたはローカル ユーザ名データベースからユーザ アクセスの拒否応答が返される場合）、認証プロセスは停止し、その他の認証方式は試行されません。

（注） 設定できる AAA 方式リストの数は 250 です。

方式リストとサーバ グループ

サーバー グループは、方式リストに使用する既存の RADIUS または TACACS+ サーバー ホストをグループ化する方法の 1 つです。次の図に、4 台のセキュリティ サーバー（R1 と R2 は RADIUS サーバー、T1 と T2 は TACACS+ サーバー）が設置された一般的な AAA ネットワーク設定を示します。R1 と R2 で RADIUS サーバのグループを構成します。T1 と T2 で TACACS+ サーバのグループを構成します。

図 *1 :* 一般的な *AAA* ネットワーク設定



サーバー グループを使用して、設定したサーバー ホストのサブセットを指定し、特定のサービスに使用します。たとえば、サーバー グループを使用すると、R1 および R2 を 1 つのサーバー グループとして定義し、T1 および T2 を別のサーバー グループとして定義できます。また、認証ログインの方式リストに R1 および T1 を指定し、PPP 認証の方式リストに R2 および T2 を指定することもできます。

サーバ グループには、1 台のサーバに対して複数のホスト エントリを含めることができます。エントリごとに固有の識別情報を設定します。固有の識別情報は、IP アドレスと UDP ポート番号の組み合わせで構成されます。これにより、RADIUS ホストとして定義されているさまざまなポートが、固有の AAA サービスを提供できるようになります。つまり、この固有識別情報を使用して、ある IP アドレスに位置する 1 台のサーバ上に複数の UDP ポートが存在する場合、それぞれの UDP ポートに対して RADIUS 要求を送信できます。1 台の RADIUS サーバー上にある異なる 2 つのホスト エントリが 1 つのサービス（認証など）に設定されている場合、設定されている 2 番めのホスト エントリは最初のホスト エントリのフェールオーバー バックアップとして動作します。この例の場合、最初のホスト エントリがアカウンティング サービスの提供に失敗すると、同じデバイスに設定されている 2 番めのホスト エントリを使用してアカウンティング サービスを提供するように、ネットワーク アクセス サーバーが試行します（試行される RADIUS ホスト エントリの順番は、設定されている順序に従います）。

サーバ グループの設定および着信番号識別サービス（DNIS）番号に基づくサーバ グループの設定の詳細については、「Configuring RADIUS」または「Configuring TACACS+」の章を参照してください。

方式リストの例

たとえば、システム管理者が、すべてのインターフェイスに同じ認証方式を使用して PPP 接続を認証する、というセキュリティ ソリューションを決定したとします。RADIUS グループでは、まず認証情報のために R1 に接続し、応答がない場合、R2 に接続します。R2 が応答しない場合、TACACS+ グループの T1 に接続し、T1 が応答しない場合、T2 に接続します。すべての指定したサーバーが応答しなかった場合、認証はアクセス サーバー自体のローカル ユーザー

名データベースで行われます。このソリューションを実装するには、システム管理者が次のコマンドを入力してデフォルトの方式リストを作成します。

```
aaa authentication ppp default group radius group tacacs+ local
```

この例では、「default」が方式リストの名前です。この方式リストにプロトコルを含める場合、名前の後に、照会される順で指定します。デフォルトのリストは、すべてのインターフェイスに自動的に適用されます。

リモートユーザーがネットワークにダイヤルインしようとすると、ネットワーク アクセス サーバーは、まず R1 に認証情報を照会します。ユーザーが R1 から認証されると、R1 からネットワーク アクセス サーバーに対して PASS 応答が発行され、ユーザーはネットワークにアクセスできるようになります。R1 から FAIL 応答が返されると、ユーザーはアクセスを拒否され、セッションは終了します。R1 が応答しない場合、ネットワーク アクセス サーバーでは ERROR として処理され、認証情報について R2 に照会されます。このパターンは、ユーザーが認証または拒否されるか、セッションが終了するまで、残りの指定した方式について続行されます。

FAIL 応答は ERROR とまったく異なる点に注意してください。FAIL とは、適用可能な認証データベースに含まれる、認証の成功に必要な基準をユーザーが満たしていないことを示します。認証は FAIL 応答で終了します。ERROR とは、認証の照会に対してサーバーが応答しなかったことを示します。そのため、認証は試行されません。ERROR が検出された場合にだけ、認証方式リストに定義されている次の認証方式が AAA によって選択されます。

たとえば、システム管理者が、1 つのインターフェイス、または一部のインターフェイスにだけ方式リストを適用するとします。この場合、システム管理者は名前付き方式リストを作成し、その名前付きリストを対象のインターフェイスに適用します。次に、システム管理者が、インターフェイス 3 にだけ適用する認証方式を実装する場合の例を示します。

```
aaa authentication ppp default group radius group tacacs+ local
aaa authentication ppp apple group radius group tacacs+ local none
 interface async 3
 ppp authentication chap apple
```

この例では、「apple」が方式リストの名前です。また、この方式リストに含まれるプロトコルは、名前の後に、実行する順で指定されています。方式リストを作成すると、該当するインターフェイスに適用されます。AAA および PPP 認証コマンド両方の方式リスト名（apple）は一致する必要があります。

次の例では、システム管理者がサーバー グループを使用し、PPP 認証の場合は R2 および T2 だけが有効であることを指定します。この場合、管理者は、メンバがそれぞれ R2（172.16.2.7）と T2（172.16.2.77）であるサーバー グループを定義する必要があります。この例では、RADIUS サーバーグループ「rad2only」は **aaa group server** コマンドを使用して次のように定義されます。

```
aaa group server radius rad2only
 server 172.16.2.7
```

TACACS+ サーバーグループ「tac2only」は、**aaa group server** コマンドを使用して次のように定義されます。

```
aaa group server tacacs+ tac2only
 server 172.16.2.77
```

次に、管理者はサーバー グループを使用して PPP 認証を適用します。この例では、PPP 認証用のデフォルト方式リストは **group rad2only** 、**group tac2only**、**local** の順序に従います。

```
aaa authentication ppp default group rad2only group tac2only local
```

RADIUS 認可変更について

標準RADIUSインターフェイスは通常、ネットワークに接続しているデバイスから要求が送信され、クエリーが送信されたサーバが応答するプル モデルで使用されます。シスコのソフトウェアは、プッシュ モデルで使用される RFC 5176 で定義された RADIUS CoA 要求をサポートしています。このモデルでは、要求は外部サーバからネットワークに接続されたデバイスへ発信され、外部の認証、許可、アカウンティング（AAA）またはポリシー サーバからの動的なセッション再設定が可能になります。

次のセッション単位の CoA 要求を使用します。

- セッション再認証
- セッションの終了
- ポート シャットダウンでのセッション終了
- ポート バウンスでのセッション終了
- セキュリティとパスワード
- アカウンティング

CoA 要求

CoA 要求は、RFC 5176 に記載されているように、プッシュ モデルで使用することによって、セッション識別、ホスト再認証、およびセッション終了を行うことができます。モデルは、次のように、1 つの要求（CoA-Request）と 2 つの考えられる応答コードで構成されます。

- CoA acknowledgment（ACK）[CoA-ACK]
- CoA non-acknowledgment（NAK）[CoA-NAK]

要求は CoA クライアント（通常は RADIUS またはポリシー サーバ）から開始されて、リスナーとして動作するデバイスに転送されます。

RFC 5176 規定

Disconnect Request メッセージは Packet of Disconnect（POD）とも呼ばれますが、セッション終了に対してデバイスでサポートされています。

次の表に、RADIUS 認可変更（CoA）機能でサポートされている IETF 属性を示します。

表 *1:* サポートされている *IETF* 属性

属性番号	属性名
24	状態
31	Calling-Station-ID
44	Acct-Session-ID
80	Message-Authenticator
101	Error-Cause

次の表に、Error-Cause 属性で取ることができる値を示します。

表 *2: Error-Cause* の値

値	説明
201	削除された残留セッション コンテキスト
202	無効な EAP パケット（無視）
401	サポートされていない属性
402	見つからない属性
403	NAS 識別情報のミスマッチ
404	無効な要求
405	サポートされていないサービス
406	サポートされていない拡張機能
407	無効な属性値
501	管理上の禁止
502	ルート不可能な要求（プロキシ）
503	セッション コンテキストが検出されない
504	セッション コンテキストが削除できない
505	その他のプロキシ処理エラー
506	リソースが使用不可能
507	要求が発信された
508	マルチセッションの選択がサポートされてない

CoA 要求応答コード

CoA要求の応答コードは、デバイスへコマンドを発行するために使用されます。サポートされているコマンドを「CoA 要求コマンド」に示します。

RFC 5176 で定義されている CoA 要求応答コードのパケットの形式は、コード、ID、長さ、オーセンティケータ、およびタイプ、長さ、値（TLV）形式の属性から構成されます。

属性フィールドは、Cisco ベンダー固有属性（VSA）を送信するために使用します。

セッションの識別

特定のセッションに対する接続解除および CoA 要求の場合、デバイスは次の 1 つまたは複数の属性に基づいてセッションを検出します。

- Acct-Session-Id（IETF 属性 #44）
- Audit-Session-Id（シスコのベンダー固有属性（VSA））
- Calling-Station-Id（ホスト MAC アドレスを含む IETF 属性 #31）

CoA メッセージに含まれるすべてのセッション ID 属性がそのセッションと一致しない限り、デバイスは「Invalid Attribute Value」エラー コード属性を含む Disconnect-NAK または CoA-NAK を返します。

（注） CoA NAK メッセージは、キーの不一致があるすべての CoA 要求に送信されるわけではありません。メッセージは、クライアントの最初の 3 つの要求にのみ送信されます。その後、そのクライアントからのすべてのパケットがドロップされます。キーの不一致が見つかると、CoA NAK メッセージで送信される応答オーセンティケータはダミーのキー値から計算されます。

CoA ACK 応答コード

許可ステートの変更に成功した場合は、肯定確認応答（ACK）が送信されます。CoA ACK 内で返される属性は CoA 要求によって異なります。

CoA NAK 応答コード

否定応答（NAK）は許可ステートの変更に失敗したことを示し、エラーの理由を示す属性を含めることができます。

CoA 要求コマンド

デバイスでサポートされているコマンドを次の表に示します。すべての CoA コマンドには、デバイスと CoA クライアント間のセッション ID が含まれている必要があります。

表 *3:* デバイスでサポートされる *CoA* 要求コマンド

コマンド	シスコの **VSA**
Bounce host port	Cisco:Avpair="subscriber:command=bounce-host-port"
Disable host port	Cisco:Avpair="subscriber:command=disable-host-port"
Reauthenticate host	Cisco:Avpair="subscriber:command=reauthenticate"
Terminate session	VSA を必要としない標準の接続解除要求です

セッション再認証

セッション認証を開始するために、認証、許可、アカウンティング（AAA）サーバは、Cisco VSA と 1 つ以上のセッション ID 属性を含む標準 CoA 要求メッセージを送信します。Cisco VSA は、Cisco:Avpair="subscriber:command=reauthenticate" の形式です。

次のシナリオでは、現在のセッション状態によって、メッセージに対するデバイスの応答が決まります。

- セッションが現在、IEEE 802.1*x* によって認証されている場合、デバイスは Extensible Authentication Protocol over LAN（EAPoL）-RequestId メッセージをサーバに送信することで応答します。
- セッションが現在 MAC 認証バイパス（MAB）によって認証されている場合、デバイスはアクセス要求をサーバに送信し、最初に成功した認証で使用したのと同じ ID 属性を渡します。
- デバイスがコマンドを受信した際にセッション認証が実行中である場合は、デバイスはプロセスを終了し、認証シーケンスを再開し、最初に試行されるように設定された方式で開始します。

セッションの終了

CoA 接続解除要求は、ホスト ポートをディセーブルにせずにセッションを終了します。CoA 接続解除要求終了によって、指定したホストのオーセンティケータ ステート マシンが再初期化されますが、ホストのネットワークへのアクセスは制限されません。セッションが見つからない場合、デバイスは「Session Context Not Found」エラー コード属性を使用して Disconnect-NAK メッセージを返します。セッションが見つかった場合、デバイスはセッションを終了します。セッションが完全に削除されると、デバイスは Disconnect-ACK メッセージを返します。

ホストのネットワークへのアクセスを制限するには、Cisco:Avpair="subscriber:command=disable-host-port" VSA を含む CoA 要求を使用します。このコマンドは、ホストがネットワーク上で問題を起こしていることを把握し、ホストのネットワーク アクセスを即座にブロックする必要がある場合に便利です。ポートのネットワーク アクセスを復元する場合は、非 RADIUS メカニズムを使用して再びイネーブルにします。

CoA 要求の disable host port

RADIUS サーバーの CoA disable port コマンドを実行すると、セッションをホストしている認証ポートが管理的にシャットダウンされます。その結果、セッションは終了します。このコマンドは、ホストがネットワーク上で問題を起こしていることを把握し、ホストのネットワークアクセスを即座にブロックする必要がある場合に便利です。ポートのネットワーク アクセスを復元する場合は、非 RADIUS メカニズムを使用して再びイネーブルにします。このコマンドは、次の VSA を含む標準の CoA-Request メッセージで伝達されます。

Cisco:Avpair="subscriber:command=disable-host-port"

このコマンドはセッション指向であるため、「セッション ID」セクションに示されている 1 つ以上のセッション ID 属性とともに使用する必要があります。セッションを検出できない場合、デバイスは「Session Context Not Found」エラー コード属性を含む CoA-NAK メッセージを返します。デバイスは、セッションを検出すると、ホスティング ポートを無効にし、CoA-ACK メッセージを返します。

デバイスが CoA-ACK をクライアントに返す前にデバイスに障害が発生した場合、クライアントから要求が再送信されると、新しいアクティブ デバイス上でそのプロセスが繰り返されます。デバイスが CoA-ACK メッセージをクライアントに返した後でデバイスに障害が発生したが、操作が完了していない場合、その操作は新しいアクティブ デバイスで再開されます。

RADIUS サーバの CoA disable port コマンドを無視するには、「bounce および disable RADIUS CoA 要求を無視するためのデバイスの設定」を参照してください。

CoA 要求の bounce port

RADIUS サーバーの CoA bounce port が RADIUS サーバーから送信されると、認証ポートでリンクのフラップが発生します。その結果、このポートに接続している 1 つまたは複数のホストから、DHCP の再ネゴシエーションが開始されます。この状況は、VLAN の変更があり、この認証ポートに関する変化を検出するメカニズムがないデバイス（プリンタなど）がエンドポイントの場合に発生する可能性があります。CoA bounce port は、次の新しい VSA を含む標準の CoA-Request メッセージで伝達されます。

Cisco:Avpair="subscriber:command=bounce-host-port"

このコマンドはセッション指向であるため、「セッション ID」に示されている 1 つ以上のセッション ID 属性とともに使用する必要があります。セッションが見つからない場合、デバイスは「Session Context Not Found」エラー コード属性を使用して CoA-NAK メッセージを返します。このセッションがある場合は、デバイスはホスト ポートを 10 秒間ディセーブルし、再びイネーブルにし（ポート バウンス）、CoA-ACK を返します。

RADIUS サーバの CoA bounce port を無視するには、「bounce および disable RADIUS CoA 要求を無視するためのデバイスの設定」を参照してください。

ドメイン ストリッピング

radius-server domain-stripping コマンドを使用して、グローバルレベルで受信したユーザー名からドメイン名を削除できます。**radius-server domain-stripping** コマンドを設定すると、

「user@example.com」を含むすべての AAA 要求のユーザー名が「user」に再フォーマットされてリモート RADIUS サーバーに送信されます。ドメイン名は要求から削除されます。

（注） ドメイン ストリッピングは TACACS 設定では行われません。

AAA ブロードキャスト アカウンティング機能を有効にすると、アカウンティング情報を複数の AAA サーバーに同時に送信できます。つまり、アカウンティング情報を 1 つまた複数の AAA サーバーに同時にブロードキャストすることが可能です。この機能を使用すると、プライベートおよびパブリック AAA サーバーにアカウント情報を送信できます。この機能では、音声アプリケーションによる課金情報も提供されます。

ドメイン ストリッピング機能を使用すると、ドメイン ストリッピングをサーバー グループ レベルで設定できます。

サーバー単位のグループ コンフィギュレーションはグローバル コンフィギュレーションを上書きします。ドメイン ストリッピングが、グローバルではイネーブルではないがサーバー グループでイネーブルになっている場合、そのサーバー グループに対してのみイネーブルになります。また、Virtual Routing and Forwarding（VRF）固有のドメイン ストリッピングがグローバルで設定されていて、別の VRF のドメイン ストリッピングがサーバー グループで設定されている場合、ドメイン ストリッピングは両方の VRF でイネーブルになります。VRF の設定は、サーバーグループ コンフィギュレーション モードから取得されます。サーバーグループ コンフィギュレーションがグローバル コンフィギュレーション モードでディセーブルになっているが、サーバー グループ コンフィギュレーション モードで使用可能である場合、サーバーグループ コンフィギュレーション モードでのすべての設定が適用可能です。

ドメイン ストリッピングおよびブロードキャスト アカウンティングを設定した後で、設定ごとに別個のアカウンティング レコードを作成できます。

AAA 認証方式を設定する方法

（注） **aaa new-model** コマンドを使用して AAA をグローバルに有効にするまで、AAA 機能は使用できません。

この章のコマンドを使用した認証の設定例については、「認証の例」を参照してください。

AAA を使用したログイン認証の設定

AAA セキュリティ サービスにより、さまざまなログイン認証方式を容易に実行できるようになります。**aaa authentication login** コマンドを使用すると、サポートされているログイン認証方式のいずれを使用するかに関係なく、AAA 認証が有効になります。 **aaa authentication login** コマンドを使用すると、ログイン時に試行する認証方式リストを 1 つまたは複数作成できま

す。これらのリストは、**login authentication** ライン コンフィギュレーション コマンドによって適用されます。

AAA を使用してログイン認証を設定するには、グローバル コンフィギュレーション モードで次のコマンドを使用します。

手順の概要

1. Router(config)# **aaa new-model**
2. Router(config)# **aaa authentication login**{**default** | *list-name*} *method1*[*method2...*]
3. Router(config)# **line** [**aux** | **console** | **tty** | **vty**] **line-number** [**ending-line-number**]
4. Router(config-line)# **login authentication**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	Router(config)# **aaa new-model**	AAA をグローバルに有効にします。
ステップ 2	Router(config)# **aaa authentication login**{**default** | *list-name*} *method1*[*method2...*]	ローカルな認証リストを作成します。
ステップ 3	Router(config)# **line** [**aux** | **console** | **tty** | **vty**] **line-number** [**ending-line-number**]	認証リストを適用する回線について、ライン コンフィギュレーション モードを開始します。
ステップ 4	Router(config-line)# **login authentication** 例： {**default** | *list-name*}	1 つの回線または複数回線に認証リストを適用します。

次のタスク

list-name は、作成するリストを指定するときに使用される名前で、文字列を使用できます。method引数は、認証アルゴリズムが試行する実際の方式を指します。追加の認証方式は、その前の方式でエラーが返された場合に限り使用されます。前の方式が失敗した場合は使用されません。すべての方式でエラーが返されても引き続き認証を行うように指定するには、コマンドラインの最後の方式として **none** を指定します。

たとえば、（この例では）TACACS+ サーバーでエラーが返されても引き続き認証を行うように指定するには、次のコマンドを入力します。

```
aaa authentication login default group tacacs+ none
```

（注） **none** キーワードを指定すると、すべてのユーザーがログイン認証に成功するため、認証のバックアップ方式としてだけ使用してください。

login authentication コマンドにリストが指定されていない場合に使用するデフォルトのリストを作成するには、**default** キーワードの後ろにデフォルト状況で使用される方式を指定します。デフォルト認証方式リストは、自動的にすべてのインターフェイスに適用されます。

たとえば、ログイン時のユーザー認証のデフォルト方式として RADIUS を指定するには、次のコマンドを入力します。

```
aaa authentication login default group radius
```

次の表に、サポートされるログイン認証方式を示します。

表 *4: AAA* 認証ログイン方式

キーワード	**Description**
enable	認証に有効化パスワードを使用します。
krb5	Kerberos 5 を認証に使用します。
krb5-telnet	ルータへの接続に Telnet を使用する場合、Kerberos 5 Telnet 認証プロトコルを使用します。このキーワードを選択する場合、方式リストの最初の方式としてこのキーワードを指定する必要があります。
line	認証にライン パスワードを使用します。
local	認証にローカルなユーザ名データベースを使用します。
local-case	認証に大文字と小文字が区別されるローカルなユーザ名を使用します。
none	認証を使用しません。
group radius	認証にすべての RADIUS サーバのリストを使用します。
group tacacs+	認証にすべての TACACS+ サーバのリストを使用します。
group *group-name*	**aaa group server radius** または **aaa group server tacacs+** コマンドで定義されているように、認証に RADIUS または TACACS+ サーバーのサブセットを使用します。

（注） **login** コマンドによって変更されるのはユーザー名および特権レベルだけであり、シェルは実行されません。したがって、autocommand は実行されません。この状況で autocommand を実行するには、Telnet セッションをルータに復帰（ループバック）させる必要があります。この方法で autocommand 機能を実装する場合は、ルータがセキュアな Telnet セッションを使用するように設定されていることを確認してください。

イネーブル パスワードによるログイン認証

認証方式としてイネーブルパスワードを指定するには、**enable** 方式キーワードを指定して **aaa authentication login**コマンドを使用します。たとえば、他の方式リストが定義されていない場合にログイン時のユーザー認証方式としてイネーブルパスワードを指定するには、次のコマンドを入力します。

```
aaa authentication login default enable
```

ログイン認証方式としてイネーブル パスワードを使用するには、イネーブル パスワードを定義しておく必要があります。イネーブル パスワードの定義の詳細については、「Configuring Passwords and Privileges」を参照してください。

Kerberos によるログイン認証

Kerberosによる認証は、他のほとんどの認証方式とは異なり、ユーザーのパスワードはリモート アクセス サーバーに送信されません。ネットワークにログインするリモート ユーザーは、ユーザー名の指定を求められます。ユーザのエントリがキー発行局（KDC）に存在する場合は、そのユーザのパスワードを含む暗号化されたチケット認可チケット（TGT）が作成され、ルータに送信されます。次に、ユーザにパスワードの入力が求められ、ルータではそのパスワードを含む TGT の復号化が試行されます。復号化に成功すると、ユーザは認証され、ルータ上にあるユーザのクレデンシャル キャッシュに TGT が保存されます。

krb5はKINITプログラムを使用しませんが、ルータに対して認証するために、ユーザがKINITプログラムを実行して TGT を取得する必要はありません。これは、Cisco IOS XE の Kerberos 実装のログイン手順に KINIT が統合されているためです。

ログイン認証方式として Kerberos を指定するには、**krb5**方式 キーワードを指定して **aaa authentication login** コマンドを使用します。たとえば、他の方式リストが定義されていない場合にログイン時のユーザー認証方式としてKerberosを指定するには、次のコマンドを入力します。

```
aaa authentication login default krb5
```

ログイン認証方式として Kerberos を使用するには、Kerberos セキュリティ サーバーとの通信をイネーブルにしておく必要があります。Kerberosサーバーとの通信を確立する方法の詳細については、「Kerberos の設定」の章を参照してください。

ライン パスワードによるログイン認証

ログイン認証方式としてラインパスワードを指定するには、**line** 方式キーワードを指定して **aaa authentication login** コマンドを使用します。たとえば、他の方式リストが定義されていない場合にログイン時のユーザー認証方式としてラインパスワードを指定するには、次のコマンドを入力します。

```
aaa authentication login default line
```

ログイン認証方式としてライン パスワードを使用するには、ライン パスワードを定義しておく必要があります。ライン パスワードの定義の詳細については、「ライン パスワード保護の設定」を参照してください。

ローカル パスワードによるログイン認証

Cisco ルータまたはアクセスサーバーが認証にローカルユーザー名データベースを使用するように指定するには、**local** 方式キーワードを指定して **aaa authentication login** コマンドを使用します。たとえば、他の方式リストが定義されていない場合にログイン時のユーザ認証方式としてローカル ユーザ名データベースを指定するには、次のコマンドを入力します。

```
aaa authentication login default local
```

ローカルユーザ名データベースにユーザを追加する方法については、「ユーザ名認証の確立」を参照してください。

group RADIUS によるログイン認証

ログイン認証方式として RADIUS を指定するには、**group radius** 方式を指定して **aaa authentication login** コマンドを使用します。たとえば、他の方式リストが定義されていない場合にログイン時のユーザー認証方式としてRADIUSを指定するには、次のコマンドを入力します。

```
aaa authentication login default group radius
```

ログイン認証方式として RADIUS を使用するには、RADIUS セキュリティ サーバーとの通信をイネーブルにしておく必要があります。RADIUSサーバーとの通信を確立する方法の詳細については、「RADIUS の設定」の章を参照してください。

アクセス要求での RADIUS 属性 8 の設定

aaa authentication login コマンドを使用して RADIUS を指定し、NAS から IP アドレスを要求するようにログインホストを設定すると、グローバル コンフィギュレーション モードで **radius-server attribute 8 include-in-access-req** コマンドを使用して、access-request パケットで属性8（Framed-IP-Address）を送信できます。このコマンドによって、ユーザー認証の前に、NAS から RADIUS サーバーに対してユーザー IP アドレスのヒントを提供できます。属性 8 の詳細については、巻末の付録「RADIUS 属性」を参照してください。

group TACACS によるログイン認証

ログイン認証方式として TACACS+ を指定するには、**group tacacs+** 方式を指定して、**aaa authentication login** コマンドを使用します。たとえば、他の方式リストが定義されていない場合にログイン時のユーザー認証方式としてTACACS+を指定するには、次のコマンドを入力します。

```
aaa authentication login default group tacacs+
```

ログイン認証方式として TACACS+ を使用するには、TACACS+ セキュリティ サーバーとの通信をイネーブルにしておく必要があります。TACACS+ サーバーとの通信を確立する方法の詳細については、「TACACS+ の設定」の章を参照してください。

group group-name によるログイン認証

ログイン認証方式として使用する RADIUS または TACACS+ サーバーのサブセットを指定するには、**group** *group-name* 方式を指定して **aaa authentication login** コマンドを使用します。グループ名とそのグループのメンバを指定して定義するには、**aaa group server** コマンドを使用します。たとえば、**aaa group server** コマンドを使用して、**group loginrad** のメンバを最初に定義します。

```
aaa group server radius loginrad
 server 172.16.2.3
 server 172.16.2 17
 server 172.16.2.32
```

このコマンドにより、172.16.2.3、172.16.2.17、172.16.2.32 の RADIUS サーバーがグループ *loginrad* のメンバとして指定されます。

他の方式リストが定義されていない場合にログイン時のユーザー認証方式として **group loginrad** を指定するには、次のコマンドを入力します。

```
aaa authentication login default group loginrad
```

ログイン認証方式としてグループ名を使用するには、RADIUS または TACACS+ セキュリティ サーバーとの通信をイネーブルにしておく必要があります。RADIUS サーバーとの通信を確立する方法の詳細については、「RADIUS の設定」の章を参照してください。TACACS+ サーバーとの通信を確立する方法の詳細については、「TACACS+ の設定」の章を参照してください。

AAA を使用した PPP 認証の設定

多くのユーザは、async または ISDN を介したダイヤルアップでネットワーク アクセス サーバにアクセスします。async または ISDN を介したダイヤルアップは、CLI を完全にバイパスします。その代わり、接続が確立するとすぐにネットワーク プロトコル（PPP や ARA など）が開始されます。

AAA セキュリティ サービスにより、PPP を実行するシリアル インターフェイスに使用できるさまざまな認証方式の実行が容易になります。**aaa authentication ppp** コマンドを使用すると、サポートされている PPP 認証方式のいずれを使用するかに関係なく、AAA 認証が有効になります。

PPP を使用してシリアル回線に AAA 認証方式を設定するには、グローバル コンフィギュレーション モードで次のコマンドを使用します。

手順の概要

1. Router(config)# **aaa new-model**
2. Router(config)# **aaa authentication ppp** {**default** | *list-name*} *method1*[*method2...*]
3. Router(config)# **interface** *interface-type interface-number*

4. Router(config-if)# **ppp authentication** {*protocol1* [*protocol2...*]} [**if-needed**] {**default** | *list-name*} [**callin**] [**one-time**][**optional**]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	Router(config)# **aaa new-model**	AAA をグローバルに有効にします。
ステップ 2	Router(config)# **aaa authentication ppp**{**default** | *list-name*} *method1*[*method2...*]	ローカルな認証リストを作成します。
ステップ 3	Router(config)# **interface** *interface-type interface-number*	認証リストを適用するインターフェイスについて、インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	Router(config-if)# **ppp authentication** {*protocol1* [*protocol2...*]} [**if-needed**] {**default** | *list-name*} [**callin**] [**one-time**][**optional**]	1 つの回線または複数回線に認証リストを適用します。このコマンドの *protocol1* と *protocol2* は、CHAP、MS-CHAP、および PAP のプロトコルを示します。PPP 認証は、まず *protocol1* に指定された最初の認証方式を使用して試行されます。認証に *protocol1* を使用できない場合は、次に設定されているプロトコルを使用して認証のネゴシエーションを行います。

次のタスク

aaa authentication ppp コマンドを使用して、PPP を介して認証を試行するときに使用する認証方式のリストを 1 つまたは複数作成します。これらのリストは、**ppp authentication** ライン コンフィギュレーション コマンドによって適用されます。

名前付きリストが **ppp authentication** コマンドに指定されていない場合に使用するデフォルトのリストを作成するには、**default** キーワードの後ろにデフォルト状況で使用される方式を指定します。

たとえば、ユーザー認証のデフォルト方式としてローカルユーザー名データベースを指定するには、次のコマンドを入力します。

```
aaa authentication ppp default local
```

list-name は、作成するリストを指定するときに使用される名前で、任意の文字列を使用できます。method 引数は、認証アルゴリズムが試行する実際の方式を指します。追加の認証方式は、その前の方式でエラーが返された場合に限り使用されます。前の方式が失敗した場合は使用されません。すべての方式でエラーが返されても引き続き認証を行うように指定するには、コマンドラインの最後の方式として **none** を指定します。

たとえば、（この例では）TACACS+ サーバーでエラーが返されても引き続き認証を行うように指定するには、次のコマンドを入力します。

```
aaa authentication ppp default group tacacs+ none
```

（注） **none** を指定するとすべてのユーザーが認証に成功してログインできるようになるため、認証のバックアップ方式として使用する必要があります。

次の表に、サポートされるログイン認証方式を示します。

表 *5 : AAA* 認証 *PPP* 方式

キーワード	Description
if-needed	ユーザが TTY 回線で認証済みの場合、認証しません。
krb5	認証に Kerberos 5 を使用します（PAP 認証にだけ使用できます）。
local	認証にローカルなユーザ名データベースを使用します。
local-case	認証に大文字と小文字が区別されるローカルなユーザ名を使用します。
none	認証を使用しません。
group radius	認証にすべての RADIUS サーバのリストを使用します。
group tacacs+	認証にすべての TACACS+ サーバのリストを使用します。
group *group-name*	**aaa group server radius** または **aaa group server tacacs+** コマンドで定義されているように、認証に RADIUS または TACACS+ サーバーのサブセットを使用します。

Kerberos による PPP 認証

PPP を実行するインターフェイスで使用する認証方式として Kerberos を指定するには、**krb5** 方式キーワードを指定して **aaa authentication ppp** コマンドを使用します。たとえば、他の方式リストが定義されていない場合にユーザー認証方式として Kerberos を指定するには、次のコマンドを入力します。

```
aaa authentication ppp default krb5
```

PPP 認証方式として Kerberos を使用するには、Kerberos セキュリティ サーバーとの通信をイネーブルにしておく必要があります。Kerberos サーバーとの通信を確立する方法の詳細については、「Kerberos の設定」の章を参照してください。

（注） Kerberos ログイン認証は、PPP PAP 認証とだけ連携します。

ローカル パスワードによる PPP 認証

Cisco ルータまたはアクセスサーバーが認証にローカルユーザー名データベースを使用するように指定するには、方式キーワード **local** を指定して **aaa authentication ppp** コマンドを使用します。たとえば、他の方式リストが定義されていない場合に、PPP を実行する回線に使用するユーザ認証方式としてローカルユーザ名データベースを指定するには、次のコマンドを入力します。

```
aaa authentication ppp default local
```

ローカルユーザ名データベースにユーザを追加する方法については、「ユーザ名認証の確立」を参照してください。

group RADIUS による PPP 認証

ログイン認証方式として RADIUS を指定するには、**group radius** 方式を指定して **aaa authentication ppp** コマンドを使用します。たとえば、他の方式リストが定義されていない場合にログイン時のユーザー認証方式として RADIUS を指定するには、次のコマンドを入力します。

```
aaa authentication ppp default group radius
```

PPP 認証方式として RADIUS を使用するには、RADIUS セキュリティ サーバーとの通信をイネーブルにしておく必要があります。RADIUS サーバーとの通信を確立する方法の詳細については、「RADIUS の設定」の章を参照してください。

アクセス要求での RADIUS 属性 44 の設定

group radius 方式で **aaa authentication ppp** コマンドを使用して、ログイン認証方式として RADIUS を指定した後、グローバル コンフィギュレーション モードで **radius-server attribute 44 include-in-access-req** コマンドを使用して、アクセス要求パケットで属性 44（Acct-Session-ID）を送信するようにデバイスを設定できます。 このコマンドによって、RADIUS デーモンはコールを開始から終了まで追跡できます。

group TACACS による PPP 認証

ログイン認証方式として TACACS+ を指定するには、**group tacacs+** 方式を指定して、**aaa authentication ppp** コマンドを使用します。たとえば、他の方式リストが定義されていない場合にログイン時のユーザー認証方式として TACACS+ を指定するには、次のコマンドを入力します。

```
aaa authentication ppp default group tacacs+
```

PPP 認証方式として TACACS+ を使用するには、TACACS+ セキュリティ サーバーとの通信をイネーブルにしておく必要があります。TACACS+ サーバーとの通信を確立する方法の詳細については、「TACACS+ の設定」の章を参照してください。

group group-name による PPP 認証

ログイン認証方式として使用する RADIUS または TACACS+ サーバーのサブセットを指定するには、**group** *group-name* 方式を指定して **aaa authentication ppp** コマンドを使用します。グループ名とそのグループのメンバを指定して定義するには、**aaa group server** コマンドを使用します。たとえば、**aaa group server** コマンドを使用して、**group ppprad** のメンバを最初に定義します。

```
aaa group server radius ppprad
 server 172.16.2.3
 server 172.16.2 17
 server 172.16.2.32
```

このコマンドにより、172.16.2.3、172.16.2.17、172.16.2.32 の RADIUS サーバーがグループ *ppprad* のメンバとして指定されます。

他の方式リストが定義されていない場合にログイン時のユーザー認証方式として **group ppprad** を指定するには、次のコマンドを入力します。

```
aaa authentication ppp default group ppprad
```

PPP 認証方式としてグループ名を使用するには、RADIUS または TACACS+ セキュリティ サーバーとの通信をイネーブルにしておく必要があります。RADIUS サーバーとの通信を確立する方法の詳細については、「RADIUS の設定」の章を参照してください。TACACS+ サーバーとの通信を確立する方法の詳細については、「TACACS+ の設定」の章を参照してください。

PPP 要求に対する AAA スケーラビリティの設定

ネットワーク アクセス サーバー（NAS）の PPP マネージャによって割り当てられた複数のバックグラウンドプロセスを設定およびモニターして、AAA 認証要求と認可要求に対応できます。AAA スケーラビリティ機能によって、PPP に対する AAA 要求を処理するために使用される複数のプロセスを設定できるようになります。つまり、同時に認証または認可できるユーザー数が増えます。

PPP に対する AAA 要求を処理するために、特定の数のバックグラウンド プロセスを割り当てるには、グローバル コンフィギュレーション モードで次のコマンドを使用します。

コマンド	目的
`Router(config)# aaa processes number`	PPP に対する AAA 認証要求および認可要求を処理するために、特定の数のバックグラウンドプロセスを割り当てます。

引数 *number* には、PPP に対する AAA 認証要求と認可要求を処理するために確保するバックグラウンド プロセス数を定義します。また、1 ～ 2147483647 の任意の値を設定できます。PPP マネージャが PPP に対する要求を処理する方法のため、この引数には、同時に認証できる新規ユーザーの数も定義します。この引数は、いつでも増減できます。

（注） 追加バックグラウンドプロセスの割り当ては、コストが高くなる可能性があります。PPP に対する AAA 要求を処理できるバックグラウンド プロセスの最小数を設定してください。

AAA を使用した ARAP 認証の設定

aaa authentication arap コマンドを使用して、AppleTalk Remote Access Protocol（ARAP）ユーザーがデバイスにログインを試行するときに使用する認証方式のリストを1つまたは複数作成できます。これらのリストは、**arap authentication** ライン コンフィギュレーション コマンドで使用されます。

グローバル コンフィギュレーション モードで次のコマンドを使用します。

手順の概要

1. Device(config)# **aaa new-model**
2. Device(config)# **aaa authentication arap**
3. Device(config)# **line** *number*
4. Device(config-line)# **autoselect arap**
5. Device(config-line)# **autoselect during-login**
6. Device(config-line)# **arap authentication** *list-name*
7. Device(config-line)# **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	Device(config)# **aaa new-model**	AAA をグローバルに有効にします。
ステップ 2	Device(config)# **aaa authentication arap** 例： ARAPユーザーに対する認証をイネーブルにします。	
ステップ 3	Device(config)# **line** *number*	（任意）ライン コンフィギュレーション モードに変更します。
ステップ 4	Device(config-line)# **autoselect arap**	（任意）ARAP の自動選択をイネーブルにします。
ステップ 5	Device(config-line)# **autoselect during-login**	（任意）ユーザー ログイン時にARAPセッションを自動的に開始します。
ステップ 6	Device(config-line)# **arap authentication** *list-name*	（任意：**default** が **aaa authentication arap** コマンドに使用されている場合は不要）回線上のARAPに対する TACACS+ 認証を有効にします。
ステップ 7	Device(config-line)# **end**	特権 EXEC モードに戻ります。

次のタスク

list-name は、作成するリストを指定するときに使用される名前で、任意の文字列を使用できます。*method* 引数は、認証アルゴリズムが試行する方式の実際のリストを指します。試行は入力されている順序で行われます。

名前付きリストが **arap authentication** コマンドに指定されていない場合に使用するデフォルトのリストを作成するには、**default** キーワードの後ろにデフォルト状況で使用される方式を指定します。

追加の認証方式は、その前の方式でエラーが返された場合に限り使用されます。前の方式が失敗した場合は使用されません。すべての方式でエラーが返されても引き続き認証を行うように指定するには、コマンドラインの最後の方式として **none** を指定します。

（注） **none** を指定するとすべてのユーザーのログインが認証されるようになるため、認証のバックアップ方式として使用する必要があります。

次の表に、サポートされるログイン認証方式を示します。

表 *6 : AAA* 認証 *ARAP* 方式

キーワード	Description
auth-guest	ユーザが EXEC モードにログイン済みの場合にだけ、ゲスト ログインを許可します。
guest	ゲスト ログインを許可します。
line	認証にライン パスワードを使用します。
local	認証にローカルなユーザ名データベースを使用します。
local-case	認証に大文字と小文字が区別されるローカルなユーザ名を使用します。
group radius	認証にすべての RADIUS サーバのリストを使用します。
group tacacs+	認証にすべての TACACS+ サーバのリストを使用します。
group *group-name*	**aaa group server radius** または **aaa group server tacacs+** コマンドで定義されているように、認証に RADIUS または TACACS+ サーバーのサブセットを使用します。

たとえば、ARAP とともに使用するデフォルトの AAA 認証方式リストを作成するには、次のコマンドを使用します。

```
aaa authentication arap default if-needed none
```

ARAP に同じ認証方式リストを作成し、リストに *MIS-access* と名前を付けるには、次のコマンドを入力します。

```
aaa authentication arap MIS-access if-needed none
```

ここでは、次の内容について説明します。

認可済みゲスト ログインを許可する ARAP 認証

ユーザーが EXEC に正常にログイン済みの場合にだけ、ゲストログインを許可するには、**auth-guest** キーワードを指定して **aaa authentication arap** コマンドを使用します。この方式はARAP認証方式リストの先頭に指定する必要がありますが、この方式が成功しなかった場合は引き続き他の方式を試行できます。たとえば、認証のデフォルト方式として、すべての認可済みゲストログイン（つまり、EXECにログイン済みのユーザーによるログイン）を許可し、その方式が失敗した場合にだけ RADIUS を使用するには、次のコマンドを入力します。

```
aaa authentication arap default auth-guest group radius
```

（注） AAA を初期化すると、デフォルトで ARAP によるゲスト ログインはディセーブルになります。ゲストログインを許可するには、 **guest** キーワードまたは **auth-guest** キーワードを指定して **aaa authentication arap** コマンドを使用する必要があります。

ゲスト ログインを許可する ARAP 認証

ゲストログインを許可するには、**guest** キーワードを指定して **aaa authentication arap** コマンドを使用します。この方式はARAP認証方式リストの先頭に指定する必要がありますが、この方式が成功しなかった場合は引き続き他の方式を試行できます。たとえば、認証のデフォルト方式としてすべてのゲスト ログインを許可し、その方式が失敗した場合にだけ RADIUS を使用するには、次のコマンドを入力します。

```
aaa authentication arap default guest group radius
```

ライン パスワードによる ARAP 認証

認証方式としてラインパスワードを指定するには、方式キーワード **line** を指定して **aaa authentication arap** コマンドを使用します。たとえば、他の方式リストが定義されていない場合に、ARAPユーザー認証方式としてラインパスワードを指定するには、次のコマンドを入力します。

```
aaa authentication arap default line
```

ARAP 認証方式としてライン パスワードを使用するには、ライン パスワードを定義しておく必要があります。ライン パスワードの定義の詳細については、この章の「ライン パスワード保護の設定」を参照してください。

ローカル パスワードによる ARAP 認証

Cisco ルータまたはアクセスサーバーが認証にローカルユーザー名データベースを使用するように指定するには、方式キーワード **local** を指定して **aaa authentication arap**コマンドを使用し

ます。たとえば、他の方式リストが定義されていない場合に、ARAP ユーザ認証方式としてローカル ユーザ名データベースを指定するには、次のコマンドを入力します。

```
aaa authentication arap default local
```

ローカルユーザ名データベースにユーザを追加する方法については、「ユーザ名認証の確立」を参照してください。

group RADIUS による ARAP 認証

NASI 認証方式として RADIUS を指定するには、**group radius** 方式を指定して **aaa authentication arap** コマンドを使用します。たとえば、他の方式リストが定義されていない場合にログイン時のユーザー認証方式として RADIUS を指定するには、次のコマンドを入力します。

```
aaa authentication arap default group radius
```

ARAP 認証方式として RADIUS を使用する前に、RADIUS セキュリティ サーバーとの通信をイネーブルにしておく必要があります。RADIUS サーバーとの通信を確立する方法の詳細については、「RADIUS の設定」の章を参照してください。

group TACACS による ARAP 認証

ARAP 認証方式として TACACS+ を指定するには、**group tacacs+** 方式を指定して、**aaa authentication arap** コマンドを使用します。たとえば、他の方式リストが定義されていない場合にログイン時のユーザー認証方式として TACACS+ を指定するには、次のコマンドを入力します。

```
aaa authentication arap default group tacacs+
```

ARAP 認証方式として TACACS+ を使用するには、TACACS+ セキュリティ サーバーとの通信をイネーブルにしておく必要があります。TACACS+ サーバーとの通信を確立する方法の詳細については、「TACACS+ の設定」の章を参照してください。

group group-name による ARAP 認証

ARAP 認証方式として使用する RADIUS または TACACS+ サーバーのサブセットを指定するには、**group** *group-name* 方式を指定して **aaa authentication arap** コマンドを使用します。グループ名とそのグループのメンバを指定して定義するには、**aaa group server** コマンドを使用します。たとえば、**aaa group server** コマンドを使用して、**group araprad** のメンバを最初に定義します。

```
aaa group server radius araprad
 server 172.16.2.3
 server 172.16.2 17
 server 172.16.2.32
```

このコマンドにより、172.16.2.3、172.16.2.17、172.16.2.32 の RADIUS サーバーがグループ *araprad* のメンバとして指定されます。

他の方式リストが定義されていない場合にログイン時のユーザー認証方式として **group araprad** を指定するには、次のコマンドを入力します。

```
aaa authentication arap default group araprad
```

ARAP 認証方式としてグループ名を使用するには、RADIUS または TACACS+ セキュリティ サーバーとの通信をイネーブルにしておく必要があります。RADIUS サーバーとの通信を確立する方法の詳細については、「RADIUS の設定」の章を参照してください。TACACS+ サーバーとの通信を確立する方法の詳細については、「TACACS+ の設定」の章を参照してください。

AAA を使用した NASI 認証の設定

aaa authentication nasi コマンドを使用して、NetWare Asynchronous Services Interface（NASI）ユーザーがデバイスにログインを試行するときに使用する認証方式のリストを 1 つまたは複数作成できます。これらのリストは、**nasi authentication line** コンフィギュレーション コマンドで使用されます。

AAA を使用して NASI 認証を設定するには、グローバル コンフィギュレーション モードで次のコマンドを使用します。

手順の概要

1. Device(config)# **aaa new-model**
2. Device(config)# **aaa authentication nasi**
3. Device(config)# **line** *number*
4. Device(config-line)# **nasi authentication** *list-name*
5. Device(config-line)# **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	Device(config)# **aaa new-model**	AAA をグローバルに有効にします。
ステップ 2	Device(config)# **aaa authentication nasi** 例：	NASI ユーザーに対する認証をイネーブルにします。
ステップ 3	Device(config)# **line** *number*	（任意：**default** が **aaa authentication nasi** コマンドに使用されている場合は不要）ライン コンフィギュレーション モードを開始します。
ステップ 4	Device(config-line)# **nasi authentication** *list-name*	（任意：**default** が **aaa authentication nasi** コマンドに使用されている場合は不要）回線上の NASI に対する TACACS+ 認証を有効にします。
ステップ 5	Device(config-line)# **end**	特権 EXEC モードに戻ります。

次のタスク

list-name は、作成するリストを指定するときに使用される名前で、任意の文字列を使用できます。*method* 引数は、認証アルゴリズムが試行する方式の実際のリストを指します。試行は入力されている順序で行われます。

aaa authentication nasi コマンドに名前付きリストが指定されていない場合に使用するデフォルトのリストを作成するには、**default** キーワードの後ろにデフォルト状況で使用される方式を指定します。

追加の認証方式は、その前の方式でエラーが返された場合に限り使用されます。前の方式が失敗した場合は使用されません。すべての方式でエラーが返されても引き続き認証を行うように指定するには、コマンドラインの最後の方式として **none** を指定します。

（注） **none** を指定するとすべてのユーザーのログインが認証されるようになるため、認証のバックアップ方式として使用する必要があります。

次の表に、サポートされる NASI 認証方式を示します。

表 *7: AAA* 認証 *NASI* 方式

キーワード	Description
enable	認証に有効化パスワードを使用します。
line	認証にライン パスワードを使用します。
local	認証にローカルなユーザ名データベースを使用します。
local-case	認証に大文字と小文字が区別されるローカルなユーザ名を使用します。
none	認証を使用しません。
group radius	認証にすべての RADIUS サーバのリストを使用します。
group tacacs+	認証にすべての TACACS+ サーバのリストを使用します。
group *group-name*	**aaa group server radius** または **aaa group server tacacs+** コマンドで定義されているように、認証に RADIUS または TACACS+ サーバーのサブセットを使用します。

イネーブル パスワードによる NASI 認証

認証方式としてイネーブルパスワードを指定するには、キーワード **enable** を指定して **aaa authentication nasi** コマンドを使用します。たとえば、他の方式リストが定義されていない場合に、NASI ユーザー認証方式としてイネーブル パスワードを指定するには、次のコマンドを使用します。

```
aaa authentication nasi default enable
```

認証方式としてイネーブル パスワードを使用するには、イネーブル パスワードを定義しておく必要があります。イネーブル パスワードの定義の詳細については、「Configuring Passwords and Privileges」を参照してください。

ライン パスワードによる NASI 認証

認証方式としてラインパスワードを指定するには、方式キーワード **line** を指定して **aaa authentication nasi** コマンドを使用します。たとえば、他の方式リストが定義されていない場合に、NASI ユーザー認証方式としてライン パスワードを指定するには、次のコマンドを入力します。

```
aaa authentication nasi default line
```

NASI 認証方式としてライン パスワードを使用するには、ライン パスワードを定義しておく必要があります。ラインパスワードの定義の詳細については、「ラインパスワード保護の設定」を参照してください。

ローカル パスワードによる NASI 認証

Cisco ルータまたはアクセスサーバーが認証情報にローカルユーザー名データベースを使用するように指定するには、方式キーワード **local** を指定して **aaa authentication nasi** コマンドを使用します。たとえば、他の方式リストが定義されていない場合に、NASI ユーザ認証方式としてローカル ユーザ名データベースを指定するには、次のコマンドを入力します。

```
aaa authentication nasi default local
```

ローカルユーザ名データベースにユーザを追加する方法については、「ユーザ名認証の確立」を参照してください。

group RADIUS による NASI 認証

NASI 認証方式として RADIUS を指定するには **group radius** 方式を指定して **aaa authentication nasi** コマンドを使用します。たとえば、他の方式リストが定義されていない場合に、NASI ユーザー認証方式として RADIUS を指定するには、次のコマンドを入力します。

```
aaa authentication nasi default group radius
```

NASI 認証方式として RADIUS を使用するには、RADIUS セキュリティ サーバーとの通信をイネーブルにしておく必要があります。RADIUS サーバーとの通信を確立する方法の詳細については、「RADIUS の設定」の章を参照してください。

group TACACS による NASI 認証

NASI 認証方式として TACACS+ を指定するには、**group tacacs+** 方式キーワードを指定して **aaa authentication nasi** コマンドを使用します。たとえば、他の方式リストが定義されていない場合に、NASI ユーザー認証方式として TACACS+ を指定するには、次のコマンドを入力します。

```
aaa authentication nasi default group tacacs+
```

認証方式として TACACS+ を使用するには、TACACS+ セキュリティ サーバーとの通信をイネーブルにしておく必要があります。TACACS+ サーバーとの通信を確立する方法の詳細については、「TACACS+ の設定」の章を参照してください。

group group-name による NASI 認証

NASI 認証方式として使用する RADIUS または TACACS+ サーバーのサブセットを指定するには、**group** *group-name* 方式を指定して **aaa authentication nasi** コマンドを使用します。グループ名とそのグループのメンバを指定して定義するには、**aaa group server** コマンドを使用します。たとえば、**aaa group server** コマンドを使用して、**group nasirad** のメンバを最初に定義します。

```
aaa group server radius nasirad
 server 172.16.2.3
 server 172.16.2 17
 server 172.16.2.32
```

このコマンドにより、172.16.2.3、172.16.2.17、172.16.2.32 の RADIUS サーバーがグループ *nasirad* のメンバとして指定されます。

他の方式リストが定義されていない場合にログイン時のユーザー認証方式として **group nasirad** を指定するには、次のコマンドを入力します。

```
aaa authentication nasi default group nasirad
```

NASI 認証方式としてグループ名を使用するには、RADIUS または TACACS+ セキュリティ サーバーとの通信をイネーブルにしておく必要があります。RADIUS サーバーとの通信を確立する方法の詳細については、「RADIUS の設定」の章を参照してください。TACACS+ サーバーとの通信を確立する方法の詳細については、「TACACS+ の設定」の章を参照してください。

ログイン入力にかける時間の指定

timeout login response コマンドを使用すると、ログイン入力（ユーザー名やパスワードなど）がタイムアウトするまでの待機時間を指定できます。デフォルトのログイン値は 30 秒です。**timeout login response** コマンドを使用して、1 ～ 300 秒のタイムアウト値を指定できます。30 秒というデフォルトのログイン タイムアウト値を変更するには、ライン コンフィギュレーション モードで次のコマンドを使用します。

コマンド	目的
`Router(config-line)# timeout login response` *seconds*	タイムアウトまでログイン情報を待機する時間を指定します。

特権レベルでのパスワード保護のイネーブル化

ユーザーが特権EXECコマンドレベルにアクセスできるかどうかを判断するときに使用する一連の認証方式を作成するには、**aaa authentication enable default** コマンドを使用します。最大4つの認証方式を指定できます。追加の認証方式は、その前の方式でエラーが返された場合に限り使用されます。前の方式が失敗した場合は使用されません。すべての方式でエラーが返されても引き続き認証を行うように指定するには、コマンドラインの最後の方式として **none** を指定します。

グローバル コンフィギュレーション モードで次のコマンドを使用します。

コマンド	目的
`Router(config)# aaa authentication enable default method1 [method2...]`	特権 EXEC レベルを要求するユーザに対して、ユーザ ID とパスワードのチェックをイネーブルにします。 （注） ルータから RADIUS サーバーに送信されたすべての **aaa authentication enable default** 要求には、ユーザー名「$enab15$」が含まれます。TACACS+ サーバに送信された要求にはログイン認証用に入力されたユーザ名が含まれます。

メソッド引数は、認証アルゴリズムが試行した方式の実際のリストを入力された順に参照します。次の表は、サポートされているイネーブル認証方式を示します。

表 *8: AAA* 認証イネーブル デフォルト方式

キーワード	Description
enable	認証に有効化パスワードを使用します。
line	認証にライン パスワードを使用します。
none	認証を使用しません。
group radius	認証にすべての RADIUS ホストのリストを使用します。 （注） RADIUS 方式は、ユーザ名別では機能しません。
group tacacs+	認証にすべての TACACS+ ホストのリストを使用します。
group *group-name*	**aaa group server radius** または **aaa group server tacacs+** コマンドで定義されているように、認証に RADIUS または TACACS+ サーバーのサブセットを使用します。

パスワード プロンプトに表示するテキストの変更

Cisco IOS XE ソフトウェアからユーザーに対してパスワードの入力を求めるときに表示されるデフォルトテキストを変更するには、**aaa authentication password-prompt** コマンドを使用します。このコマンドによって、イネーブル パスワードと、リモート セキュリティ サーバーから提供されていないログイン パスワードのパスワード プロンプトが変更されます。このコマンドの **no** 形式を使用すると、パスワードプロンプトが次のデフォルト値に戻ります。

```
Password:
```

aaa authentication password-prompt コマンドでは、リモートの TACACS+ サーバーまたは RADIUS サーバーから提供されるダイアログは変更されません。

aaa authentication password-prompt コマンドは、RADIUS をログイン方式として使用するときに機能します。RADIUS サーバに到達不能の場合でも、コマンドで定義されたパスワードプロンプトが表示されます。aaa authentication password-prompt コマンドは、TACACS+ と併用できません。TACACS+は、NASに対して、ユーザに表示するパスワードプロンプトを提供します。TACACS+ サーバが到達可能な場合、NAS はそのサーバからパスワード プロンプトを受け取り、aaa authentication password-prompt コマンドで定義したプロンプトではなく、受け取ったプロンプトを使用します。TACACS+ サーバが到達不能の場合、aaa authentication password-prompt コマンドで定義したパスワード プロンプトが使用される可能性があります。

グローバル コンフィギュレーション モードで次のコマンドを使用します。

コマンド	目的
`Router(config)# aaa authentication password-prompt text-string`	ユーザにパスワードの入力を求めるときに表示するデフォルト テキストを変更します。

ユーザー名が空のアクセス要求が RADIUS サーバーに送信されないようにする

次の設定手順では、ユーザー名が空のアクセス要求が RADIUS サーバーに送信されないようにする方法について説明します。この機能により、RADIUS サーバーとの不要なやりとりを回避でき、RADIUS ログの量を少なくすることができます。

（注） **aaa authentication suppress null-username** コマンドを開始できるのは、Cisco IOS XE Release 2.4 です。

手順の概要

1. **enable**
2. **configure terminal**
3. **aaa new-model**

4. **aaa authentication suppress null-username**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**aaa new-model** 例： `Router(config)# configure terminal`	AAA をグローバルに有効にします。
ステップ 4	**aaa authentication suppress null-username** 例： `Router(config)# aaa authentication suppress null-username`	ユーザー名が空のアクセス要求がRADIUSサーバーに送信されないようにします。

AAA 認証のメッセージ バナーの設定

AAA は、設定可能でパーソナライズされたログインおよび failed-login バナーの使用をサポートします。ユーザーが AAA を使用して認証を受けるシステムにログインする場合、および何らかの理由で認証が失敗した場合に表示されるメッセージ バナーを設定できます。

ログイン バナーの設定

ユーザーがログインするときに表示されるメッセージを設定する（デフォルトのログイン メッセージを置き換える）には、次のタスクを実行します。

始める前に

ログイン バナーを作成するには、デリミタを設定する必要があります。設定することで、続くテキスト文字列をバナーとして表示する必要があることがシステムに通知されます。次に、テキスト文字列自体を設定する必要があります。デリミタは、バナーの末尾を示すために、テキスト ストリングの末尾で繰り返されます。デリミタには、拡張 ASCII 文字セットの任意の 1 文字を使用できます。ただし、デリミタとして定義した文字は、バナー用のテキスト文字列には使用できません。

手順の概要

1. **aaa new-model** Device(config)# **aaa new-model**
2. Device(config)# **aaa authentication banner** *delimiter string delimiter*
3. Device(config)# **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**aaa new-model** Device(config)# **aaa new-model**	AAA をイネーブルにします。
ステップ 2	Device(config)# **aaa authentication banner** *delimiter string delimiter*	パーソナライズされたログイン バナーを作成します。
ステップ 3	Device(config)# **end**	特権 EXEC モードに戻ります。

次のタスク

ログイン バナーの設定後、まだ実行していない場合は、AAA を使用した認証の基本設定を完了する必要があります。さまざまな、使用可能なAAA認証の詳細については、『認証、許可、アカウンティング コンフィギュレーション ガイド』の「認証の設定」を参照してください。

Failed-Login バナーの設定

ユーザー ログインが失敗したときに表示されるメッセージを設定する（デフォルトのfailed-loginメッセージを置き換える）には、次のタスクを実行します。

始める前に

failed-loginバナーを作成するには、デリミタを設定する必要があります。設定することで、続くテキスト文字列をバナーとして表示する必要があることがシステムに通知されます。次に、テキスト文字列自体を設定する必要があります。デリミタは、failed-loginバナーの末尾を示すために、テキスト ストリングの末尾で繰り返されます。デリミタには、拡張 ASCII 文字セットの任意の1文字を使用できます。ただし、デリミタとして定義した文字は、バナーを構成するテキスト ストリングには使用できません。

手順の概要

1. Device(config)# **aaa new-model**
2. Device(config)# **aaa authentication fail-message** *delimiter string delimiter*
3. Device(config)# **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	Device(config)# **aaa new-model**	AAA をイネーブルにします。

	コマンドまたはアクション	目的
ステップ 2	Device(config)# **aaa authentication fail-message** *delimiter string delimiter*	ユーザー ログインが失敗したときに表示されるメッセージを作成します。
ステップ 3	Device(config)# **end**	特権 EXEC モードに戻ります。

次のタスク

failed-login バナーの設定後、まだ実行していない場合は、AAA を使用した認証の基本設定を完了する必要があります。さまざまな、使用可能な AAA 認証の詳細については、『認証、許可、アカウンティング コンフィギュレーション ガイド』の「認証の設定」を参照してください。

AAA パケット オブ ディスコネクトの設定

特定のセッション属性が指定された場合、パケット オブ ディスコネクト（POD）によってネットワーク アクセス サーバー（NAS）の接続が終了されます。UNIX ワークステーション上にある POD クライアントでは、AAA から取得したセッション情報を使用して、ネットワーク アクセス サーバーで実行されている POD サーバーに接続解除パケットを送信します。NAS では、1 つまたは複数の一致するキー属性を含む任意の着信ユーザー セッションを終了します。必要なフィールドがない場合、または完全一致が見つからない場合、要求は拒否されます。

POD を設定するには、グローバル コンフィギュレーション モードで次のタスクを実行します。

手順の概要

1. Router(config)# **aaa accounting network default**
2. Router(config)# **aaa accounting delay-start**
3. Router(config)# **aaa pod server server-key**string
4. Router(config)# **radius-server host** *IP address*non-standard

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	Router(config)# **aaa accounting network default** 例： `start-stop radius`	AAA アカウンティング レコードをイネーブルにします。
ステップ 2	Router(config)# **aaa accounting delay-start**	（任意）POD パケットで使用できるように、Framed-IP-Address が割り当てられるまで、開始アカウンティング レコードの生成を遅延します。
ステップ 3	Router(config)# **aaa pod server server-key**string	POD の受信イネーブルにします。

	コマンドまたはアクション	目的
ステップ 4	Router(config)# **radius-server host** *IP address*snon-standard	RADIUS のベンダー固有バージョンを使用する RADIUS ホストを宣言します。

二重認証のイネーブル化

シスコのリリースによっては、PPP セッションの認証には、PAP または CHAP のどちらか 1 つの認証方法しか使用できないことがあります。二重認証方式の場合、ネットワーク アクセス権を得るには、リモート ユーザーが（CHAP または PAP 認証後に）認証の第 2 段階に合格する必要があります。

この第 2 段階（「二重」）の認証には、ユーザーがパスワードを知っている必要がありますが、ユーザーのリモート ホストにパスワードは保存されません。そのため、第 2 段階の認証は、ホストではなくユーザーに固有です。その結果、リモート ホストから情報が盗まれた場合でも有効な、追加のセキュリティ レベルが実現します。さらに、ユーザー別にネットワーク特権をカスタマイズできるため、柔軟性も高くなります。

第 2 段階の認証には、CHAP ではサポートされないトークン カードなど、ワンタイム パスワードを使用できます。ワンタイム パスワードを使用している場合、ユーザー パスワードが盗まれても盗用者の役に立ちません。

二重認証の機能

二重認証を使用する場合、2 つの認証/認可段階があります。この 2 つの段階は、リモート ユーザーがダイヤルインした後、および PPP セッションが開始された後に発生します。

第 1 段階では、ユーザーがリモート ホスト名を使用してログインして CHAP（または PAP）がリモート ホストを認証し、次に PPP が AAA とネゴシエートしてリモート ホストを認可します。このプロセスで、リモート ホストに関連付けられたネットワーク アクセス特権は、そのユーザーに関連付けられます。

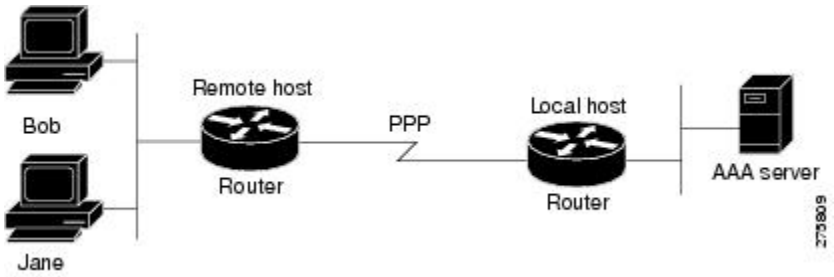
（注） ローカル ホストに対して Telnet 接続だけを許可するように、この第 1 段階ではネットワーク管理者が認可を制限することを推奨します。

第 2 段階では、リモート ユーザーが、認証を受けるネットワーク アクセス サーバーに対して Telnet を送信する必要があります。リモート ユーザーがログインする場合、AAA ログイン認証を使用してユーザーを認証する必要があります。次に、AAA を使用して再度許可を受けるために、**access-profile** コマンドを入力する必要があります。この認可が完了すると、ユーザーは二重に認証され、ユーザー別のネットワーク特権に従ってネットワークにアクセスできるようになります。

システム管理者は、セキュリティ サーバーで適切なパラメータを設定することで、各認証段階の後にリモート ユーザーが保持するネットワーク特権を決定します。二重認証を使用するには、**access-profile** コマンドを発行してアクティブ化する必要があります。

注意 複数のホストがネットワーク アクセス サーバーに対して PPP 接続を共有する場合、二重認証によって望ましくない状況が発生することがあります（次の図を参照）。まず、ユーザーBob が PPP セッションを開始し、ネットワーク アクセス サーバーで二重認証をアクティブにした場合（次の図を参照）、Bob の PPP セッションが期限切れになるまで、他のすべてのユーザーは Bob と同じネットワーク特権を持つことになります。この問題が発生するのは、PPP セッション時に Bob の認可プロファイルがネットワーク アクセス サーバーのインターフェイスに適用され、他のユーザーからの PPP トラフィックに Bob が確立した PPP セッションが使用されるためです。第 2 に、Bob が PPP セッションを開始して二重認証をアクティブにし、（Bob の PPP セッションが期限切れになる前に）別のユーザー Jane が **access-profile** コマンドを実行する場合（または、Jane がネットワーク アクセス サーバーに Telnet を送信し、**autocommand access-profile** が実行された場合）、再度許可が発生し、Jane の許可プロファイルがインターフェイスに適用され、Bob のプロファイルは置換されます。その結果、Bob の PPP トラフィックの不通や中止が発生することや、Bob が本来は持っていないレベルの特権が Bob に付与されることがあります。

図 *2:* 危険性を伴うトポロジ：複数のホストがネットワーク アクセス サーバーに対する *PPP* 接続を共有



二重認証の設定

二重認証を設定するには、次の手順を実行します。

1. **aaa-new model** グローバル コンフィギュレーション コマンドを使用して、AAA を有効にします。AAA をイネーブルにする方法の詳細については、「AAA Overview」を参照してください。
2. **aaa authentication** コマンドを使用して、ログインおよびPPP認証方式リストを使用するようにネットワークアクセスサーバーを設定します。次に、これらの方式リストを適切な回線やインターフェイスに適用します。
3. **aaa authorization** コマンドを使用して、ログイン時の AAA ネットワーク許可を設定します。ネットワーク認可の設定の詳細については、「認可の設定」の章を参照してください。
4. セキュリティ プロトコル パラメータ（たとえば、RADIUS または TACACS+）を設定します。RADIUS の詳細については、「Configuring RADIUS」の章を参照してください。TACACS+ の詳細については、「Configuring TACACS+」の章を参照してください。

5. セキュリティ サーバーで、ユーザーがローカル ホストに接続できるアクセス コントロール リストの AV ペアを使用するには、Telnet 接続を確立する必要があります。
6. （任意）autocommand として **access-profile** コマンドを設定します。autocommand を設定すると、リモートユーザーは、個人のユーザープロファイルに関連付けられた許可済み権限にアクセスするために、手動で **access-profile** コマンドを入力する必要はなくなります。

（注） **access-profile** コマンドが autocommand として設定されている場合でも、二重認証を完了するには、ユーザーがローカルホストに Telnet を送信し、ログインする必要があります。

ユーザー固有の許可ステートメントを作成する場合、次の規則に従います（これらの規則は、**access-profile** コマンドのデフォルトの動作に関連します）。

- セキュリティ サーバーでアクセス コントロール リストの AV ペアを設定する場合、有効な AV ペアを使用します。
- リモート ユーザーがインターフェイスの既存の認可（第 2 段階の認証/認可の前に存在する認可）を使用し、異なるアクセス コントロール リスト（ACL）を持つようにするには、ユーザー固有の認可定義で ACL AV ペアだけを指定します。この方法は、デフォルトの認可プロファイルを設定してリモート ホストに適用し、ACL はユーザー別に適用する場合などに有効です。
- これらのユーザー固有の許可ステートメントを後でインターフェイスに適用すると、ユーザーの許可に使用する **access-profile** コマンドの実行形式によって、既存のインターフェイス設定に追加することや、既存のインターフェイス設定を置き換えることができます。許可ステートメントを設定する前に、**access-profile** コマンドの機能について理解する必要があります。
- ISDN または Multilink PPP を使用する予定がある場合、ローカル ホストで仮想テンプレートも設定する必要があります。

二重認証に関する問題を解決するには、**debug aaa per-user** デバッグコマンドを使用します。このコマンドの詳細については、『*Cisco IOS Debug Command Reference*』を参照してください。

二重認証後のユーザー プロファイルへのアクセス

二重認証で、リモート ユーザーがローカル ホスト名を使用してローカル ホストに対する PPP リンクを確立すると、リモート ホストは CHAP（または PAP）認証されます。CHAP（または PAP）認証後、PPP は AAA とネゴシエートして、リモート ホストに関連付けられたネットワーク アクセス特権をユーザーに割り当てます（この段階の特権では、ユーザーがローカル ホストに接続するには Telnet 接続を必須にするという制限を付けることを推奨します）。

ユーザーが二重認証の第 2 段階を開始する必要があり、ローカル ホストに対して Telnet 接続を確立する場合、ユーザーは個人のユーザー名とパスワード（CHAP または PAP のユーザー名とパスワードとは異なります）を入力します。この処理の結果、個人のユーザー名/パスワードに従って AAA 認証が発生します。ただし、ローカル ホストに関連付けられた初期の権限が

有効です。ローカルホストに関連付けられた権限は、**access-profile** コマンドを使用して、ユーザープロファイルのユーザー用に定義されている権限で置き換えられるか、結合されます。

二重認証後にユーザープロファイルにアクセスするには、EXEC コンフィギュレーション モードで次のコマンドを使用します。

コマンド	目的
Router> **access-profile** [**merge** | **replace**] [**ignore-sanity-checks**]	二重認証後に、ユーザに関連付けられた権限にアクセスします。

autocommand として実行するように **access-profile** コマンドを設定した場合、リモートユーザーのログイン後に自動的に実行されます。

自動二重認証のイネーブル化

自動二重認証を実装することで、ユーザーにとって二重認証プロセスが容易になります。自動二重認証は、二重認証が持つセキュリティ上の利点をすべて備えていますが、リモート ユーザーにとってよりシンプルでユーザーフレンドリなインターフェイスです。二重認証の場合、ユーザー認証の第 2 レベルは、ユーザーがネットワーク アクセス サーバーまたはルータに Telnet に送信し、ユーザー名とパスワードを入力したときに完了します。自動二重認証の場合、ユーザーがネットワーク アクセス サーバーに Telnet を送信する必要はありません。その代わり、ユーザー名とパスワードまたは Personal Identification Number（PIN）の入力を求めるダイアログボックスが表示されます。自動二重認証機能を使用するには、対応するクライアント アプリケーションがリモート ユーザー ホストで実行されている必要があります。

（注） 自動二重認証は、既存の二重認証機能と同様に、Multilink PPP ISDN 接続専用です。自動二重認証は、X.25 や SLIP など他のプロトコルとは併用できません。

自動二重認証は、既存の二重認証機能の強化です。自動二重認証を設定するには、まず次の手順を実行して二重認証を設定する必要があります。

1. **aaa-new model** グローバル コンフィギュレーション コマンドを使用して、AAA を有効にします。
2. **aaa authentication** コマンドを使用して、ログインおよびPPP認証方式リストを使用するようにネットワークアクセスサーバーを設定します。次に、これらの方式リストを適切な回線やインターフェイスに適用します。
3. **aaa authorization** コマンドを使用して、ログイン時の AAA ネットワーク許可を設定します。ネットワーク認可の設定の詳細については、「認可の設定」の章を参照してください。
4. セキュリティ プロトコル パラメータ（たとえば、RADIUS または TACACS+）を設定します。RADIUS の詳細については、「Configuring RADIUS」の章を参照してください。TACACS+ の詳細については、「Configuring TACACS+」の章を参照してください。

5. セキュリティ サーバーで、ユーザーがローカル ホストに接続できるアクセス コントロール リストの AV ペアを使用するには、Telnet 接続を確立する必要があります。
6. autocommand として **access-profile** コマンドを設定します。autocommand を設定すると、リモートユーザーは、個人のユーザープロファイルに関連付けられた許可済み権限にアクセスするために、手動で **access-profile** コマンドを入力する必要はなくなります。autocommand の設定方法については、『*CiscoIOS Dial Technologies Command Reference* , Release 12.2.』の **autocommand** コマンドを参照してください。

（注） **access-profile** コマンドが autocommand として設定されている場合でも、二重認証を完了するには、ユーザーがローカルホストに Telnet を送信し、ログインする必要があります。

ユーザー固有の許可ステートメントを作成する場合、次の規則に従います（これらの規則は、**access-profile** コマンドのデフォルトの動作に関連します）。

- セキュリティ サーバーでアクセス コントロール リストの AV ペアを設定する場合、有効な AV ペアを使用します。
- リモート ユーザーがインターフェイスの既存の認可（第 2 段階の認証/認可の前に存在する認可）を使用し、異なるアクセス コントロール リスト（ACL）を持つようにするには、ユーザー固有の認可定義で ACL AV ペアだけを指定します。この方法は、デフォルトの認可プロファイルを設定してリモート ホストに適用し、ACL はユーザー別に適用する場合などに有効です。
- これらのユーザー固有の許可ステートメントを後でインターフェイスに適用すると、ユーザーの許可に使用する **access-profile** コマンドの実行方法によって、既存のインターフェイス設定に追加することや、既存のインターフェイス設定を置き換えることができます。許可ステートメントを設定する前に、**access-profile** コマンドの機能について理解する必要があります。
- ISDN または Multilink PPP を使用する予定がある場合、ローカル ホストで仮想テンプレートも設定する必要があります。

二重認証に関する問題を解決するには、**debug aaa per-user** デバッグコマンドを使用します。このコマンドの詳細については、『*Cisco IOS Debug Command Reference*』を参照してください。

二重認証を設定したら、自動機能を追加できます。

自動二重認証の設定

自動ダブル認証を設定するには、グローバル コンフィギュレーション モードで次のコマンドを使用します。

手順の概要

1. Router(config)# **ip trigger-authentication**
2. 次のいずれかを実行します。

- Router(config)# **interface bri** *number*
-
-
- Router(config)# **interface serial** *number* **:23**

3. Router(config-if)#**ip trigger-authentication**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	Router(config)# **ip trigger-authentication** 例： `[timeout seconds] [port number]`	二重認証の自動化をイネーブルにします。
ステップ 2	次のいずれかを実行します。 • Router(config)# **interface bri** *number* • • • Router(config)# **interface serial** *number* **:23**	ISDN BRI インターフェイスまたは ISDN PRI インターフェイスを選択し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	Router(config-if)#**ip trigger-authentication**	自動二重認証をインターフェイスに適用します。

自動二重認証のトラブルシューティング

自動二重認証の問題を解決するには、特権 EXEC モードで次のコマンドを使用します。

手順の概要

1. Router# **show ip trigger-authentication**
2. Router# **clear ip trigger-authentication**
3. Router# **debug ip trigger-authentication**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	Router# **show ip trigger-authentication**	自動二重認証が試行され、成功または失敗したリモート ホストのリストが表示されます。
ステップ 2	Router# **clear ip trigger-authentication**	自動二重認証が試行されたリモートホストのリストをクリアします（これは、**show ip trigger-authentication** コマンドで表示されるテーブルをクリアします）。
ステップ 3	Router# **debug ip trigger-authentication**	自動二重認証に関する **debug** の出力が表示されます。

RADIUS CoA 用の動的認可サービスの設定

次の手順を実行して、動的許可サービスの認証、許可、アカウンティング（AAA）サーバとしてデバイスを有効にします。このサービスは、入力方向と出力方向でポリシー マップをプッシュする認可変更（CoA）機能をサポートします。

手順の概要

1. **enable**
2. **configure terminal**
3. **aaa new-model**
4. **aaa server radius dynamic-author**
5. **client** {*ip-addr* | *hostname*} [**server-key** [**0** | **7**] *string*]
6. **domain** {**delimiter** *character* | **stripping** | [**right-to-left**]}
7. **port** *port-num*
8. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**aaa new-model** 例： `Device(config)# aaa new-model`	AAA をグローバルに有効にします。
ステップ 4	**aaa server radius dynamic-author** 例： `Device(config)# aaa server radius dynamic-author`	ローカル AAA サーバを動的認可サービス用にセットアップして、動的認可ローカル サーバ コンフィギュレーション モードに入ります。このサービスは、ポリシー マップを入力方向と出力方向にプッシュする CoA 機能をサポートするように有効にする必要があります。 • このモードでは、RADIUS アプリケーション コマンドが設定されます。
ステップ 5	**client** {*ip-addr* | *hostname*} [**server-key** [**0** | **7**] *string*] 例：	AAA サーバー クライアントの IP アドレスまたはホスト名を設定します。

	コマンドまたはアクション	目的
	`Device(config-locsvr-da-radius)# client 192.168.0.5 server-key cisco1`	• オプションの **server-key** キーワードと *string* 引数を使用して、クライアントレベルのサーバーキーを設定します。 （注） クライアント レベルでサーバー キーを設定すると、グローバル レベルで設定されたサーバーキーが上書きされます。
ステップ 6	**domain** {**delimiter** *character* | **stripping** | [**right-to-left**]} 例： `Device(config-locsvr-da-radius)# domain stripping right-to-left`	（任意）RADIUS アプリケーションについてユーザ名のドメイン オプションを設定します。 • **delimiter** キーワードで、ドメインデリミタを指定します。次のいずれかのオプションを *character* 引数に指定できます。**@**、**/**、**$**、**%**、\、**#**、または **-**。 • **stripping** キーワードは、着信のユーザー名と、**@** ドメインデリミタの左側にある名前を比較します。 • The **right-to-left** キーワードは、右から左方向に見て最初のデリミタで文字列を終了します。
ステップ 7	**port** *port-num* 例： `Device(config-locsvr-da-radius)# port 3799`	CoA 要求に UDP ポートを設定します。
ステップ 8	**end** 例： `Device(config-locsvr-da-radius)# end`	特権 EXEC モードに戻ります。

bounce および disable RADIUS CoA 要求を無視するためのデバイスの設定

複数のホストを使用して認証ポートを認証していて、このポートで 1 つのホストに対してフラップする認可変更（CoA）要求があるか、このポートで終了するホストセッションがある場合、このポート上のその他のホストにも影響があります。したがって、複数のホストを使用して認証されたポートは、フラップの場合に 1 つまたは複数のホストから DHCP の再ネゴシエーションをトリガーします。または、1 つまたは複数のホストについて、セッションをホストする認証ポートを管理的にシャットダウンします。

次の手順を使用して、bounce port コマンドまたは disable port コマンドの形式で RADIUS サーバの認可変更（CoA）要求を無視するようにデバイスを設定します。

手順の概要

1. **enable**
2. **configure terminal**
3. **aaa new-model**
4. **authentication command bounce-port ignore**
5. **authentication command disable-port ignore**
6. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**aaa new-model** 例： `Device(config)# aaa new-model`	認証、認可、アカウンティング（AAA）をグローバルに有効化します。
ステップ 4	**authentication command bounce-port ignore** 例： `Device(config)# authentication command bounce-port ignore`	（任意）RADIUS サーバの bounce port コマンドを無視するようにデバイスを設定します。無視しない場合、認証ポート上でホストがフラップをリンクし、結果として、そのポートに接続する 1 つまたは複数のホストから DHCP 再ネゴシエーションが発生します。
ステップ 5	**authentication command disable-port ignore** 例： `Device(config)# authentication command disable-port ignore`	（任意）RADIUS サーバの CoA disable port コマンドを無視するようにデバイスを設定します。無視しない場合、1 または複数のホスト セッションをホストする認証ポートが管理的にシャットダウンされます。 • ポートがシャットダウンされると、セッションも終了します。
ステップ 6	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。

サーバー グループ レベルでのドメイン ストリッピングの設定

手順の概要

1. **enable**
2. **configure terminal**
3. **aaa group server radius** *server-name*
4. **domain-stripping** [**strip-suffix** *word*] [**right-to-left**] [**prefix-delimiter** *word*] [**delimiter** *word*]
5. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**aaa group server radius** *server-name* 例： `Device(config)# aaa group server radius rad1`	RADIUS サーバを追加し、サーバ グループ RADIUS コンフィギュレーション モードを開始します。 • *server-name* 引数には、RADIUS サーバー グループ名を指定します。
ステップ 4	**domain-stripping** [**strip-suffix** *word*] [**right-to-left**] [**prefix-delimiter** *word*] [**delimiter** *word*] 例： `Device(config-sg-radius)# domain-stripping delimiter username@example.com`	サーバー グループ レベルでドメイン ストリッピングを設定します。
ステップ 5	**end** 例： `Device(config-sg-radius)# end`	サーバー グループ RADIUS コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

非 AAA 認証方式

ライン パスワード保護の設定

このタスクは、パスワードを入力し、パスワード チェック処理を確立することで、端末回線にアクセス コントロールを提供するために使用します。

（注） ライン パスワード保護を設定し、TACACS または拡張 TACACS を設定する場合、TACACS のユーザー名とパスワードの方が、ライン パスワードよりも優先されます。まだセキュリティ ポリシーを実装していない場合、AAA を使用することを推奨します。

手順の概要

1. **enable**
2. **configure terminal**
3. **line** [**aux** | **console** | **tty** | **vty**] *line-number* [*ending-line-number*]
4. **password** *password*
5. **login**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**line** [**aux** | **console** | **tty** | **vty**] *line-number* [*ending-line-number*] 例： `Router(config)# line console 0`	ライン コンフィギュレーション モードを開始します。
ステップ 4	**password** *password* 例： `Router(config-line)# secret word`	回線上の端末または他のデバイスにパスワードを割り当てます。パスワードチェッカでは大文字と小文字が区別され、スペースを使用できます。たとえば、パスワード「Secret」とパスワード「secret」は異なるパスワードです。また、「two words」は有効なパスワードです。
ステップ 5	**login** 例： `Router(config-line)# login`	ログイン時のパスワードチェックをイネーブルにします。 このコマンドの**no**形式を使用してパスワードチェックを無効にすると、ラインパスワード検証を無効にできます。

	コマンドまたはアクション	目的
		（注） **login** コマンドによって変更されるのはユーザー名および特権レベルだけであり、シェルは実行されません。したがって、autocommand は実行されません。この状況で autocommand を実行するには、Telnet セッションをルータに復帰（ループバック）させる必要があります。この方法で autocommand 機能を実装する場合は、ルータがセキュアな Telnet セッションを使用するように設定されていることを確認してください。

ユーザー名認証の確立

ユーザー名ベースの認証システムを作成できます。これは、次のような場合に役立ちます。

- TACACS をサポートしないネットワークに、TACACS のようなユーザー名と暗号化されたパスワード認証システムを提供する場合
- 特殊なケース（たとえば、アクセスリストの確認、パスワードの確認なし、ログイン時の autocommand の実行、「エスケープなし」の状況など）に備えたログインを提供する場合

ユーザ名の認証を確立するには、システム設定の必要に応じて、グローバル コンフィギュレーション モードで次のコマンドを使用します。

手順の概要

1. 次のいずれかを実行します。
   - Router(config)# **username** *name* [**nopassword** | **password** *password* | **password** *encryption-type encrypted password*]
   -
   -
   - Router(config)# **username** *name* [**access-class** *number*]
2. Router(config)# **username** *name* [**privilege** *level*]
3. Router(config)# **username** *name* [**autocommand** *command*]
4. Router(config)# **username** *name* [**noescape**] [**nohangup**]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	次のいずれかを実行します。 • Router(config)# **username** *name* [**nopassword** | **password** *password* | **password** *encryption-type encrypted password*] • • • Router(config)# **username** *name* [**access-class** *number*]	暗号化されたパスワードを使用してユーザー名認証を確立します。 または （任意）アクセス リストによるユーザー名認証を確立します。
ステップ 2	Router(config)# **username** *name* [**privilege** *level*]	（任意）ユーザーの特権レベルを設定します。
ステップ 3	Router(config)# **username** *name* [**autocommand** *command*]	（任意）自動実行されるコマンドを指定します。
ステップ 4	Router(config)# **username** *name* [**noescape**] [**nohangup**]	（任意）「エスケープなし」のログイン環境を設定します。

次のタスク

キーワード **noescape** を指定すると、ユーザーは接続先のホストでエスケープ文字を使用できなくなります。**nohangup** 機能を使用すると、autocommand の使用後に接続が解除されません。

⚠

注意 **service password-encryption** コマンドを有効にしない限り、設定のパスワードはクリアテキストで表示されます。**service password-encryption** コマンドに関する詳細情報については、『*Cisco IOS Security Command Reference*』を参照してください。

CHAP 認証または PAP 認証の有効化

インターネット サービス プロバイダー（ISP）のダイヤル ソリューションに使用されている最も一般的なトランスポート プロトコルの 1 つは、ポイントツーポイント プロトコル（PPP）です。従来、リモート ユーザーはアクセス サーバーにダイヤルインして、PPP セッションを開始していました。PPP のネゴシエート後は、リモート ユーザーは ISP ネットワークに接続され、そしてインターネットに接続されます。

ISP はアクセス サーバーへの接続を顧客に限定したいため、リモート ユーザーはアクセス サーバーに対して認証を受けてから、PPP セッションを開始する必要があります。通常、リモート ユーザーは、アクセス サーバーからのプロンプトに応じてユーザー名とパスワードを入力して、認証を受けます。これは実行可能なソリューションですが、管理が困難で、リモート ユーザーにとっても面倒です。

よりよいソリューションは、PPP に組み込まれた認証プロトコルを使用することです。この場合、リモート ユーザーはアクセス サーバーにダイヤルインし、アクセス サーバーと PPP の最

小サブセットを開始します。この操作で、ISP のネットワークに対するアクセス権はリモートユーザーに付与されません。単に、アクセス サーバーがリモート デバイスと通話できるだけです。

現在、PPP は 2 つの認証プロトコルをサポートします。パスワード認証プロトコル（PAP）およびチャレンジ ハンドシェイク認証プロトコル（CHAP）の 2 つです。いずれも RFC 1334 で規定され、同期インターフェイスと非同期インターフェイスでサポートされます。PAP または CHAP を介する認証は、サーバーからのプロンプトを受けてユーザー名とパスワードを入力する方法と同等です。CHAP の場合、接続の間にリモートユーザーのパスワードは送信されないため、より安全性が高いと考えられます。

（PAP 認証または CHAP 認証の有無に関係なく）PPP はダイヤルアウト ソリューションでもサポートされます。アクセス サーバーがダイヤルアウト機能を使用するのは、アクセス サーバーからリモート デバイスに対してコールを開始し、PPP などのトランスポート プロトコルを起動しようとするときです。

CHAP と PAP に関する詳細については、『*Cisco IOS XE Dial Technologies Configuration Guide* , Release 2』を参照してください。

（注） CHAP または PAP を使用するには、PPP カプセル化を実行する必要があります。

インターフェイスで CHAP をイネーブルにし、リモート デバイスがそのインターフェイスに接続しようとすると、アクセス サーバーからリモート デバイスに CHAP パケットが送信されます。CHAP パケットは、リモートデバイスに応答するように要求または「チャレンジ」します。チャレンジ パケットは、ローカル ルータの ID、ランダム番号、およびホスト名から構成されます。

リモート デバイスは、チャレンジ パケットを受信すると、ID、リモート デバイスのパスワード、およびランダム番号を連結し、リモートデバイスのパスワードを使用してすべてを暗号化します。リモートデバイスは、その結果を、暗号化プロセスで使用されたパスワードに関連付けられた名前とともにアクセス サーバーに返信します。

アクセス サーバーがその応答を受信すると、受信した名前を使用して、ユーザー データベースに保存されているパスワードを取得します。取得したパスワードは、暗号化プロセスで使用されたリモート デバイスと同じパスワードです。アクセス サーバーは、新しく取得したパスワードを使用して、連結された情報を暗号化します。その結果が応答パケットで送信された結果と一致する場合、認証は成功です。

CHAP 認証を使用する利点は、リモート デバイスのパスワードがクリア テキストで送信されないことです。結果として、他のデバイスによるパスワード盗用や、ISP のネットワークに対する不正アクセスの取得を回避できます。

CHAP トランザクションが発生するのは、リンクが確立したときだけです。アクセス サーバーは、以降のコール中にパスワードを要求しません（ただし、ローカルデバイスは、コール中に他のデバイスからこのような要求があった場合、応答する可能性があります）。

PAP をイネーブルにすると、アクセス サーバに接続しようとするリモート ルータは、認証要求を送信する必要があります。認証要求に指定されているユーザー名とパスワードが受け入れられた場合、Cisco IOS XE ソフトウェアから認証の確認応答が送信されます。

CHAP または PAP をイネーブルにすると、アクセス サーバーは、ダイヤルインするリモート デバイスからの認証を必須にするようになります。イネーブルにしたプロトコルをリモートデバイスがサポートしていない場合、コールはドロップされます。

CHAP または PAP を使用するには、次のタスクを実行する必要があります。

1. PPP カプセル化をイネーブルにします。
2. インターフェイスで CHAP または PAP をイネーブルにします。
3. CHAP の場合、認証が必須の各リモート システムについて、ホスト名の認証および秘密（パスワード）を設定します。

PPP カプセル化の有効化

PPP カプセル化をイネーブルにするには、インターフェイス コンフィギュレーション モードで次のコマンドを使用します。

コマンド	目的
`Router(config-if)# encapsulation ppp`	インターフェイスで PPP をイネーブルにします。

PAP または CHAP のイネーブル化

PPP カプセル化として設定されているインターフェイスで、CHAP 認証または PAP 認証をイネーブルにするには、インターフェイス コンフィギュレーション モードで次のコマンドを使用します。

コマンド	目的
`Router(config-if)# ppp authentication {protocol1 [protocol2...]} [if-needed] {default | list-name} [callin] [one-time]`	サポートされる認証プロトコルと、使用順序を定義します。このコマンドの *protocol1* と protocol2 は、CHAP、MS-CHAP、および PAP のプロトコルを示します。PPP 認証は、まず *protocol1* に指定された最初の認証方式を使用して試行されます。認証に *protocol1* を使用できない場合は、次に設定されているプロトコルを使用して認証のネゴシエーションを行います。

インターフェイスで **ppp authentication chap** を設定する場合、そのインターフェイスで PPP 接続を開始するすべての受信コールは、CHAP を使用して認証される必要があります。同様に、**ppp authentication pap** を設定する場合、PPP 接続を開始するすべての受信コールは、PAP を使用して認証される必要があります。**ppp authentication chap pap** を設定する場合、アクセスサーバーは、CHAP を使用して PPP セッションを開始するすべての受信コールを認証しようとします。リモート デバイスが CHAP をサポートしない場合、アクセス サーバーは PAP を使用して

コールを認証しようとします。リモート デバイスが CHAP も PAP もサポートしない場合、認証は失敗し、コールはドロップされます。**ppp authentication pap chap** を設定する場合、アクセスサーバーは、PAP を使用して PPP セッションを開始するすべての受信コールを認証しようとします。リモート デバイスが PAP をサポートしない場合、アクセス サーバーは CHAP を使用してコールを認証しようとします。リモートデバイスがいずれのプロトコルもサポートしない場合、認証は失敗し、コールはドロップされます。**callin** キーワードを指定して **ppp authentication** コマンドを設定すると、アクセスサーバーは、リモートデバイスがコールを開始した場合にだけ、リモートデバイスの認証を行います。

認証方式リストと **one-time** キーワードを使用できるのは、AAA を有効にした場合だけです。TACACS または拡張 TACACS を有効にしている場合は、使用できません。**ppp authentication** コマンドを使用して認証方式リストの名前を指定すると、PPP は、指定した方式リストに定義されている方式を使用して、接続を認証しようとします。AAA をイネーブルにし、名前で定義されている方式リストがない場合、PPP は、デフォルトに定義されている方式を使用して接続を認証しようとします。**one-time** キーワードを指定して **ppp authentication** コマンドを使用すると、認証中にワンタイムパスワードをサポートできます。

if-needed キーワードを使用できるのは、TACACS または拡張 TACACS を使用している場合だけです。**if-needed** キーワードを指定して **ppp authentication** コマンドを使用することは、現在のコール期間中にリモートデバイスがまだ認証されていない場合にだけ、PPP が PAP または CHAP を介してリモートデバイスを認証することを示します。リモートデバイスが、標準のログイン手順で認証を受け、EXEC プロンプトから PPP を開始した場合、**ppp authentication chap if-needed** がインターフェイスで設定されていれば、PPP は CHAP を介して認証しません。

注意 **aaa authentication ppp** コマンドを使用して設定されていない *list-name* を使用する場合、その回線での PPP は無効になります。

ローカルルータまたはアクセスサーバーが認証を必須とする各リモートシステムについて、**username** エントリを追加する方法については、「ユーザー名認証の確立 （44 ページ）」を参照してください。

着信認証と発信認証

PPP は双方向の認証をサポートしています。通常、リモート デバイスがアクセス サーバーにダイヤルインするときは、それが許可されているアクセスであることをリモートデバイスが証明するように、アクセス サーバーから要求されます。これは着信認証と呼ばれます。同時に、リモート デバイスは、身元を証明するようにアクセス サーバーに要求することもできます。これは発信認証と呼ばれます。また、アクセス サーバーは、リモート デバイスに対してコールを開始するときにも、発信認証を実行します。

発信 PAP 認証のイネーブル化

発信 PAP 認証をイネーブルにするには、インターフェイス コンフィギュレーション モードで次のコマンドを使用します。

コマンド	目的
`Router(config-if)# ppp pap sent-username username password password`	発信PAP認証をイネーブルにします。

アクセスサーバーからリモートデバイスに対してコールを開始する場合は常に、またはアウトバウンド認証のためにリモートデバイスの要求に応答する必要がある場合は、**ppp pap sent-username** コマンドで指定されたユーザー名とパスワードを使用して自身を認証します。

PAP 認証要求の拒否

ピアからの PAP 認証要求を拒否するには（つまり、すべてのコールで PAP 認証をディセーブルにするには）、インターフェイス コンフィギュレーション モードで次のコマンドを使用します。

コマンド	目的
`Router(config-if)# ppp pap refuse`	PAP 認証を要求するピアからの PAP 認証を拒否します。

refuse キーワードが使用されない場合、ルータはピアから受信した PAP 認証チャレンジを拒否しません。

共通 CHAP パスワードの作成

リモート CHAP 認証だけの場合、不明なピアからのチャレンジに対して使用する共通 CHAP シークレットパスワードを作成するように、ルータを設定できます。たとえば、ルータが、新しい（つまり不明な）ルータが追加された、ルータのロータリー（別ベンダー製のルータ、または古いバージョンの Cisco IOS ソフトウェアを実行するルータ）に発信する場合などです。**ppp chap password** コマンドを使用すると、任意のダイヤラインターフェイスまたは非同期グループインターフェイスで、複数のユーザー名およびパスワード コンフィギュレーション コマンドをこのコマンドの単一のコピーで置換できます。

ルータのコレクションに発信するルータが、共通の CHAP シークレット パスワードを設定できるようにするには、インターフェイス コンフィギュレーション モードで次のコマンドを使用します。

コマンド	目的
`Router(config-if)# ppp chap password secret`	ルータのコレクションに発信するルータが、共通のCHAPシークレット パスワードを設定できるようにします。

CHAP 認証要求の拒否

ピアからのCHAP認証要求を拒否するには（つまり、すべてのコールでCHAP認証をディセーブルにするには）、インターフェイス コンフィギュレーション モードで次のコマンドを使用します。

コマンド	目的
`Router(config-if)# ppp chap refuse [callin]`	CHAP 認証を要求するピアからの CHAP 認証を拒否します。

callin キーワードが使用されると、ルータは、ピアから受信した CHAP 認証チャレンジへの応答を拒否します。ただし、ルータが送信する CHAP チャレンジに対しては、ピアが応答することを必須とします。

（**ppp pap sent-username** コマンドを使用して）発信 PAP がイネーブルの場合、拒否パケットの認証方式として、PAP が提案されます。

ピアが認証されるまで CHAP 認証を遅延する

ピアがルータから認証を受けるまで、CHAP 認証を要求するピアに対してルータを認証しないように指定するには、インターフェイス コンフィギュレーション モードで次のコマンドを使用します。

コマンド	目的
`Router(config-if)# ppp chap wait secret`	ピアがルータから認証を受けるまで、CHAP 認証を遅延するようにルータを設定します。

このコマンド（デフォルト）により、CHAP 認証を要求するピアがルータの認証を受けてから、ルータがピアの認証を受けるように指定します。**no ppp chap wait** コマンドにより、ルータが認証チャレンジに即座に応答するように指定されます。

MS-CHAP の使用

マイクロソフト チャレンジ ハンドシェイク認証プロトコル（MS-CHAP）は、Microsoft バージョンの CHAP であり、RFC 1994 の拡張です。標準バージョンの CHAP と同様に、MS-CHAP は PPP 認証に使用されます。この場合、Microsoft Windows NT または Microsoft Windows 95 を使用する PC と、ネットワーク アクセス サーバーとして動作する Cisco デバイスまたはアクセス サーバーとの間に認証が発生します。

MS-CHAP と標準の CHAP の違いは次のとおりです。

- MS-CHAP をイネーブルにするには、LCP オプション 3 の Authentication Protocol で、CHAP Algorithm 0x80 をネゴシエートします。
- MS-CHAP 応答パケットは、Microsoft Windows NT 3.5 および 3.51、Microsoft Windows 95、および Microsoft LAN Manager 2.*x* と互換性を持つように設計されたフォーマットです。このフォーマットを使用する場合、オーセンティケータは、クリア パスワードまたは可逆的に暗号化されたパスワードを保存する必要はありません。
- MS-CHAP には、オーセンティケータが制御する認証リトライ メカニズムがあります。

- MS-CHAPには、オーセンティケータが制御するチャレンジパスワードメカニズムがあります。
- MS-CHAP には、Failure パケット メッセージ フィールドで返される「reason-for failure」コード セットが定義されています。

実装したセキュリティ プロトコルに応じて、AAA セキュリティ サービスの有無にかかわらず、MS-CHAPによるPPP認証を使用できます。AAAをイネーブルにしている場合、MS-CHAPを使用するPPP認証は、TACACS+およびRADIUSの両方と併用できます。次の表に、RADIUSが MS-CHAP をサポートできるベンダー固有 RADIUS 属性（IETF Attribute 26）を示します。

表 *9 : MS-CHAP* 用のベンダー固有 *RADIUS* 属性

ベンダーID番号	ベンダータイプ番号	ベンダー固有属性	説明
311	11	MSCHAP-Challenge	ネットワーク アクセス サーバがMS-CHAPユーザに送信するチャレンジが含まれます。これは、Access-Request パケットと Access-Challenge パケットの両方で使用できます。
211	11	MSCHAP-Response	PPP MS-CHAP ユーザがチャレンジに対する応答で提供するレスポンス値が含まれます。Access-Requestパケットでしか使用されません。この属性は、PPP CHAP ID と同じです

MS-CHAP を使用した PPP 認証の定義

MS-CHAP を使用して PPP 認証を定義するには、インターフェイス コンフィギュレーション モードで次のコマンドを使用します。

手順の概要

1. Router(config-if)#**encapsulation ppp**
2. Router(config-if)# **ppp authentication ms-chap** [**if-needed**] [*list-name* | **default**] [**callin**] [**one-time**]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	Router(config-if)#**encapsulation ppp**	PPP カプセル化をイネーブルにします。
ステップ 2	Router(config-if)# **ppp authentication ms-chap** [**if-needed**] [*list-name* | **default**] [**callin**] [**one-time**]	MS-CHAP を使用して PPP 認証を定義します。

次のタスク

あるインターフェイスで **ppp authentication ms-chap** を設定する場合、PPP 接続を開始するそのインターフェイスに着信するすべてのコールは、MS-CHAP を使用して認証する必要があります。**callin** キーワードを指定して **ppp authentication** コマンドを設定すると、アクセスサーバーは、リモートデバイスがコールを開始した場合にだけ、リモートデバイスの認証を行います。

認証方式リストと **one-time** キーワードを使用できるのは、AAA を有効にした場合だけです。TACACS または拡張 TACACS を有効にしている場合は、使用できません。**ppp authentication** コマンドを使用して認証方式リストの名前を指定すると、PPPは、指定した方式リストに定義されている方式を使用して、接続を認証しようとします。AAA をイネーブルにし、名前で定義されている方式リストがない場合、PPPは、デフォルトに定義されている方式を使用して接続を認証しようとします。**one-time** キーワードを指定して **ppp authentication** コマンドを使用すると、認証中にワンタイムパスワードをサポートできます。

if-needed キーワードを使用できるのは、TACACS または拡張 TACACS を使用している場合だけです。**if-needed** キーワードを指定して **ppp authentication** コマンドを使用することは、現在のコール期間中にリモートデバイスがまだ認証されていない場合にだけ、PPP が MS-CHAP を介してリモートデバイスを認証することを示します。リモートデバイスが、標準のログイン手順で認証を受け、EXEC プロンプトから PPP を開始した場合、**ppp authentication chap if-needed** が設定されていれば、PPP は MS-CHAP を介して認証しません。

（注） MS-CHAP を使用する PPP 認証と、ユーザー名認証を併用する場合、ローカル ユーザー名/パスワードデータベースにMS-CHAPシークレットを含める必要があります。ユーザ名認証の詳細については、「ユーザ名認証の確立」の項を参照してください。

認証の例

RADIUS 認証の例

ここでは、RADIUS を使用する 2 つの設定例を紹介します。

次に、RADIUS を使用して認証および認可を行うようにルータを設定する例を示します。

```
aaa authentication login radius-login group radius local
aaa authentication ppp radius-ppp if-needed group radius
aaa authorization exec default group radius if-authenticated
aaa authorization network default group radius
line 3
login authentication radius-login
interface serial 0
ppp authentication radius-ppp
```

この RADIUS 認証および認可設定のサンプル行は、次のように定義されます。

- aaa authentication login radius-login group radius local コマンドを実行すると、ルータは、ログイン プロンプトで認証に RADIUS を使用するように設定されます。RADIUS がエラーを返すと、ユーザーはローカル データベースを使用して認証されます。
- aaa authentication ppp radius-ppp if-needed group radius コマンドを実行すると、ユーザーがまだログインしていない場合、Cisco IOS XE ソフトウェアは CHAP または PAP による PPP 認証を使用するように設定されます。EXEC 施設がユーザーを認証すると、PPP 認証は実行されません。
- aaa authorization exec default group radius if-authenticated コマンドを実行すると、autocommand や特権レベルなど、EXEC 認可時に使用される情報について、RADIUS データベースに照会されます。ただし、ユーザーの認証が成功した場合にだけ、権限が付与されます。
- aaa authorization network default group radius コマンドを実行すると、ネットワーク認可、アドレス割り当て、および他のアクセス リストについて RADIUS に照会されます。
- **login authentication radius-login** コマンドを使用すると、ライン 3 について radius-login 方式リストが有効になります。
- **ppp authentication radius-ppp** コマンドを使用すると、シリアルインターフェイス 0 について radius-ppp 方式リストが有効になります。

次に、ユーザー名とパスワードの入力を求め、その内容を確認し、ユーザーの EXEC レベルを認可し、特権レベル 2 の認可方式として指定するように、ルータを設定する例を示します。この例では、ユーザー名プロンプトにローカルユーザー名を入力すると、そのユーザー名が認証に使用されます。

ローカルデータベースを使用してユーザーが認証されると、RADIUS 認証からのデータは保存されないため、RADIUS を使用する EXEC 認可は失敗します。また、この方式リストではローカル データベースを使用して autocommand を検索します。autocommand がない場合、ユーザーは EXEC ユーザーになります。次に、ユーザーが特権レベル 2 に設定されているコマンドを発行しようとすると、TACACS+ を使用してコマンドの認可が試行されます。

```
aaa authentication login default group radius local
aaa authorization exec default group radius local
aaa authorization command 2 default group tacacs+ if-authenticated
radius-server host 172.16.71.146 auth-port 1645 acct-port 1646
radius-server attribute 44 include-in-access-req
radius-server attribute 8 include-in-access-req
```

この RADIUS 認証および認可設定のサンプル行は、次のように定義されます。

- aaa authentication login default group radius local コマンドにより、RADIUS（RADIUS が応答しない場合はルータのローカル ユーザー データベース）がユーザー名およびパスワードを確認するように指定します。
- aaa authorization exec default group radius local コマンドにより、RADIUS を使用してユーザーが認証される場合、ユーザーの EXEC レベルの設定に RADIUS 認証情報を使用するように指定します。RADIUS 情報が使用されない場合、このコマンドにより、EXEC 認可にローカル ユーザー データベースが使用されるように指定します。

- aaa authorization command 2 default group tacacs+ if-authenticated コマンドにより、すでにユーザーの認証が成功している場合、特権レベル 2 に設定されているコマンドに TACACS+ 認可を指定します。
- radius-server host 172.16.71.146 auth-port 1645 acct-port 1646 コマンドにより、RADIUS サーバー ホストの IP アドレス、認証要求の UDP 宛先ポート、およびアカウンティング要求の UDP 宛先ポートを指定します。
- radius-server attribute 44 include-in-access-req コマンドにより、access-request パケットで RADIUS 属性 44（Acct-Session-ID）を送信します。
- radius-server attribute 8 include-in-access-req コマンドにより、access-request パケットで RADIUS 属性 8（Framed-IP-Address）を送信します。

TACACS 認証の例

次に、PPP 認証に使用するセキュリティ プロトコルとして TACACS+ を設定する例を示します。

```
aaa new-model
aaa authentication ppp test group tacacs+ local
interface serial 0
ppp authentication chap pap test
tacacs-server host 192.0.2.3
tacacs-server key goaway
```

この TACACS+ 認証設定のサンプル行は、次のように定義されます。

- **aaa new-model** コマンドは、AAA セキュリティ サービスをイネーブルにします。
- **aaa authentication** コマンドにより、PPP を実行するシリアル インターフェイスに使用する方式リスト「test」を定義します。キーワード **group tacacs+** は、TACACS+ を介して認証を実行することを示します。認証中に TACACS+ から何らかのエラーが返される場合、キーワード **local** は、ネットワーク アクセス サーバー上のローカル データベースを使用して認証が試行されることを示します。
- **interface** コマンドにより、回線を選択します。
- **ppp authentication** コマンドにより、この回線に test 方式リストを適用します。
- **tacacs-server host** コマンドにより、TACACS+ デーモンが 192.0.2.3 という IP アドレスを持っていると指定します。
- **tacacs-server key** コマンドにより、共有暗号キーを「goaway」に定義します。

次に、PPP に AAA 認証を設定する例を示します。

```
aaa authentication ppp default if-needed group tacacs+ local
```

この例のキーワード **default** は、デフォルトですべてのインターフェイスに PPP 認証が適用されることを示します。**if-needed** キーワードは、ユーザーが ASCII ログイン手順を介してすで

に認証済みの場合、PPPは不要なので、スキップできることを示します。認証が必要な場合、**group tacacs+** キーワードは、TACACS+ を介して認証が実行されることを示します。認証中にTACACS+ から何らかのエラーが返される場合、キーワード **local** は、ネットワーク アクセス サーバー上のローカル データベースを使用して認証が試行されることを示します。

次に、PAP に同じ認証アルゴリズムを作成し、「default」ではなく「MIS-access」の方式リストを呼び出す例を示します。

```
aaa authentication ppp MIS-access if-needed group tacacs+ local
interface serial 0
ppp authentication pap MIS-access
```

この例では、リストはどのインターフェイスにも適用されないため（自動的にすべてのインターフェイスに適用されるデフォルトリストとは異なります）、管理者は **interface** コマンドを使用して、この認証スキームを適用するインターフェイスを選択する必要があります。次に、管理者は **ppp authentication** コマンドを使用して、選択したインターフェイスにこの方式リストを適用する必要があります。

Kerberos 認証の例

ログイン認証方式として Kerberos を指定するには、次のコマンドを使用します。

```
aaa authentication login default krb5
```

PPP に Kerberos 認証を指定するには、次のコマンドを使用します。

```
aaa authentication ppp default krb5
```

AAA スケーラビリティの例

次に、セキュリティ プロトコルとして RADIUS による AAA を使用する一般的なセキュリティ設定例を示します。この例では、ネットワーク アクセス サーバーは、16 バックアップ プロセスを割り当てて PPP に対する AAA 要求を処理するように設定されています。

```
aaa new-model
radius-server host alcatraz
radius-server key myRaDiUSpassWoRd
radius-server configure-nas
username root password ALongPassword
aaa authentication ppp dialins group radius local
aaa authentication login admins local
aaa authorization network default group radius local
aaa accounting network default start-stop group radius
aaa processes 16
line 1 16
 autoselect ppp
 autoselect during-login
 login authentication admins
 modem dialin
interface group-async 1
 group-range 1 16
 encapsulation ppp
 ppp authentication pap dialins
```

この RADIUS AAA 設定のサンプル行は、次のように定義されます。

- **aaa new-model** コマンドは、AAA ネットワーク セキュリティ サービスをイネーブルにします。
- **radius-server host** コマンドは RADIUS サーバー ホストの名前を定義します。
- **radius-server key** コマンドは、ネットワーク アクセス サーバーと RADIUS サーバー ホストの間の共有秘密テキスト文字列を定義します。
- **radius-server configure-nas** コマンドは、デバイスが最初に起動したときに、シスコ ルータまたはアクセスサーバーがスタティックルートと IP プール定義について RADIUS サーバーに照会するように定義します。
- **username** コマンドはユーザー名とパスワードを定義します。これらの情報は、PPP パスワード認証プロトコル（PAP）の発信元身元確認に使用されます。
- **aaa authentication ppp dialins group radius local** コマンドで、まず RADIUS 認証を指定する認証方式リスト「dialins」を定義します。次に、（RADIUS サーバーが応答しない場合）PPP を使用するシリアル回線でローカル認証が使用されます。
- **aaa authentication login admins local** コマンドは、ログイン認証に別の方式リスト「admins」を定義します。
- **aaa authorization network default group radius local** コマンドは、アドレスと他のネットワーク パラメータを RADIUS ユーザーに割り当てるために使用されます。
- **aaa accounting network default start-stop group radius** コマンドは、PPP の使用状況を追跡します。
- **aaa processes** コマンドにより、PPP に対する AAA 要求を処理するために 16 個のバックグラウンドプロセスを割り当てます。
- **line** コマンドはコンフィギュレーション モードをグローバル コンフィギュレーションからライン コンフィギュレーションに切り替え、設定対象の回線を指定します。
- **autoselect ppp** コマンドは、選択した回線上で PPP セッションを自動的に開始できるようにします。
- **autoselect during-login** コマンドを使用すると、Return キーを押さずにユーザ名およびパスワードのプロンプトが表示されます。ユーザがログインすると、autoselect 機能（この場合は PPP）が開始します。
- **login authentication admins** コマンドは、ログイン認証に「admins」方式リストを適用します。
- **modem dialin** コマンドは、選択した回線に接続されているモデムを設定し、着信コールだけを受け入れるようにします。
- **interface group-async** コマンドは、非同期インターフェイス グループを選択して定義します。

- **group-range** コマンドは、インターフェイス グループ内のメンバ非同期インターフェイスを定義します。
- **encapsulation ppp** コマンドは、指定のインターフェイスに使用されるカプセル化方式として PPP を設定します。
- **ppp authentication pap dialins** コマンドは「dialins」方式リストを指定したインターフェイスに適用します。

例：AAA 認証のログイン バナーおよび Failed-Login バナーの設定

次に、ユーザーがシステムにログインするときに表示されるログイン バナー（この場合、「Unauthorized Access Prohibited」というフレーズ）を設定する例を示します。アスタリスク（*）はデリミタとして使用されます。RADIUS はデフォルト ログイン認証方式として指定されます。

```
Device> enable
Device# configure terminal
Device(config)# aaa new-model
Device(config)# aaa authentication banner *Unauthorized Access Prohibited*
Device(config)# aaa authentication login default group radius
```

この設定によって、次のログイン バナーが表示されます。

```
Unauthorized Access Prohibited
Username:
```

次の例では、ユーザーがシステムにログインしようとして失敗すると表示される Failed-Login バナー（この場合、「Failed login. Try again」というフレーズ）を設定する方法を示します。アスタリスク（*）はデリミタとして使用されます。RADIUS はデフォルト ログイン認証方式として指定されます。

```
Device> enable
Device# configure terminal
Device(config)# aaa new-model
Device(config)# aaa authentication banner *Unauthorized Access Prohibited*
Device(config)# aaa authentication fail-message *Failed login. Try again.*
Device(config)# aaa authentication login default group radius
```

この設定によって、次のログイン バナーおよび Failed-Login バナーが表示されます。

```
Unauthorized Access Prohibited
Username:
Password:
Failed login. Try again.
```

AAA パケット オブ ディスコネクト サーバ キーの例

次に、パケット オブ ディスコネクト（POD）を設定する例を示します。その結果、特定のセッション属性が指定されると、ネットワーク アクセス サーバー（NAS）の接続が終了します。

```
aaa new-model
```

```
aaa authentication ppp default radius
aaa accounting network default start-stop radius
aaa accounting delay-start
aaa pod server server-key xyz123
radius-server host 192.0.2.3 non-standard
radius-server key rad123
```

二重認証の例

ここでは、二重認証に使用できる設定例を示します。実際のネットワークおよびセキュリティ要件によっては、この例とは大幅に異なる可能性があります。

（注） 設定例には、特定の IP アドレスと他の特定の情報が含まれます。この情報は説明のための例であり、実際の設定には異なる IP アドレス、異なるユーザー名とパスワード、異なる認可ステートメントを使用します。

二重認証による AAA のローカル ホストの設定例

次の 2 つの例では、PPP とログイン認証、およびネットワークと EXEC 認可に AAA を使用するようにローカル ホストを設定する方法を示します。例はそれぞれRADIUS の例と TACACS+ の例です。

いずれの例でも、先頭の 3 行で AAA を設定し、特定のサーバーを AAA サーバーとして設定しています。続く 2 行で PPP およびログイン認証に AAA を設定し、最後の 2 行でネットワークおよび EXEC 認可を設定します。最後の行が必要なのは、**access-profile** コマンドを autocommand として実行する場合だけです。

次に、RADIUS AAA サーバーを使用するデバイス設定の例を示します。

```
aaa new-model
radius-server host secureserver
radius-server key myradiuskey
aaa authentication ppp default group radius
aaa authentication login default group radius
aaa authorization network default group radius
aaa authorization exec default group radius
```

次に、TACACS+ サーバーを使用するデバイス設定の例を示します。

```
aaa new-model
tacacs-server host security
tacacs-server key mytacacskey
aaa authentication ppp default group tacacs+
aaa authentication login default group tacacs+
aaa authorization network default group tacacs+
aaa authorization exec default group tacacs+
```

第 1 段階の PPP 認証と認可に関する AAA サーバの設定例

次に、AAA サーバーでの設定例を示します。また、RADIUS 用の AAA 設定例の一部を示します。

TACACS+ サーバーも同様に設定できます（「TACACS による設定完了の例」を参照してください）。

この例では、二重認証の第 1 段階で CHAP によって認証される「hostx」というリモート ホストに関する認証/認可を定義します。ACL AV ペアは、リモート ホストによる Telnet 接続をローカル ホストに制限しています。ローカル ホストの IP アドレスは 10.0.0.2 です。

次に、RADIUS 用の AAA サーバーの設定例を一部示します。

```
hostx   Password = "welcome"
        User-Service-Type = Framed-User,
        Framed-Protocol = PPP,
        cisco-avpair = "lcp:interface-config=ip unnumbered fastethernet 0",
        cisco-avpair = "ip:inacl#3=permit tcp any 172.21.114.0 0.0.0.255 eq telnet",
        cisco-avpair = "ip:inacl#4=deny icmp any any",
        cisco-avpair = "ip:route#5=10.0.0.0 255.0.0.0",
        cisco-avpair = "ip:route#6=10.10.0.0 255.0.0.0",
        cisco-avpair = "ipx:inacl#3=deny any"
```

第 2 段階の Per-User 認証と認可に関する AAA サーバの設定例

ここでは、RADIUS サーバーでの AAA 設定例の一部を示します。これらの設定では、ユーザ名が「patuser」のユーザ（Pat）の認証と認可を定義します。このユーザは、二重認証の第 2 段階でユーザ認証されます。

TACACS+ サーバーも同様に設定できます（「TACACS による設定完了の例」を参照してください）。

3 つの例は、**access-profile** コマンドの 3 つの各形式で使用できる RADIUS AAA 設定の例を示します。

最初の例は、**access-profile** コマンドのデフォルトの形式（キーワードなし）で機能する AAA 設定例の一部を示します。1 つの ACL AV ペアのみが定義されます。また、この例では autocommand として **access-profile** コマンドも設定します。

```
patuser   Password = "welcome"
          User-Service-Type = Shell-User,
          cisco-avpair = "shell:autocmd=access-profile"
          User-Service-Type = Framed-User,
          Framed-Protocol = PPP,
          cisco-avpair = "ip:inacl#3=permit tcp any host 10.0.0.2 eq telnet",
          cisco-avpair = "ip:inacl#4=deny icmp any any"
```

2 番目の例は、**access-profile** コマンドの **access-profile merge** 形式で機能する AAA 設定例の一部を示します。また、この例では autocommand として **access-profile merge** コマンドも設定します。

```
patuser   Password = "welcome"
          User-Service-Type = Shell-User,
          cisco-avpair = "shell:autocmd=access-profile merge"
          User-Service-Type = Framed-User,
          Framed-Protocol = PPP,
          cisco-avpair = "ip:inacl#3=permit tcp any any"
          cisco-avpair = "ip:route=10.0.0.0 255.255.0.0",
          cisco-avpair = "ip:route=10.1.0.0 255.255.0.0",
          cisco-avpair = "ip:route=10.2.0.0 255.255.0.0"
```

3 番目の例は、**access-profile** コマンドの **access-profile replace** 形式で機能する AAA 設定例の一部を示します。また、この例では autocommand として **access-profile replace** コマンドも設定します。

```
patuser   Password = "welcome"
          User-Service-Type = Shell-User,
          cisco-avpair = "shell:autocmd=access-profile replace"
          User-Service-Type = Framed-User,
          Framed-Protocol = PPP,
          cisco-avpair = "ip:inacl#3=permit tcp any any",
          cisco-avpair = "ip:inacl#4=permit icmp any any",
          cisco-avpair = "ip:route=10.10.0.0 255.255.0.0",
          cisco-avpair = "ip:route=10.11.0.0 255.255.0.0",
          cisco-avpair = "ip:route=10.12.0.0 255.255.0.0"
```

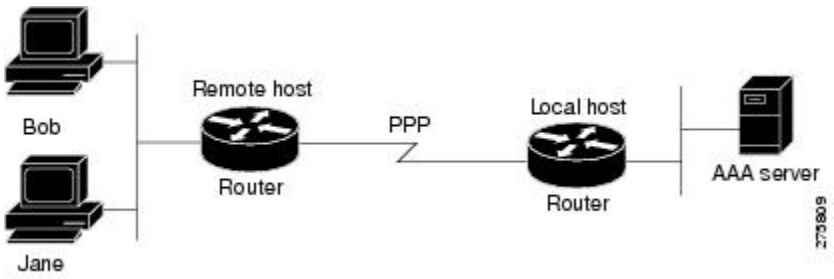
TACACS による設定完了の例

この例では、リモートホスト（二重認証の第 1 段階で使用）および特定のユーザー（二重認証の第 2 段階で使用）の両方向けの、TACACS+ 認可プロファイルの設定を示します。この TACACS+ の例には、前の RADIUS の例とほぼ同じ設定情報が使用されます。

この設定例は、リモート ホスト「hostx」および 3 ユーザ（ユーザ名が「pat_default」、「pat_merge」、および「pat_replace」）の TACACS+ サーバ上にある認証/認可プロファイルを示します。これら 3 つのユーザー名の設定は、**access-profile** コマンドの 3 種類のフォームに対応する異なる設定を示しています。また、3 つのユーザー設定は、**access-profile** コマンドの各形式について autocommand の設定方法も示しています。

次の図に、トポロジを示します。図の後に、TACACS+ 設定ファイルの例を示します。

図 *3:* 二重認証のトポロジ例



この設定例は、リモート ホスト「hostx」および 3 ユーザ（ユーザ名が「pat_default」、「pat_merge」、および「pat_replace」）の TACACS+ サーバ上にある認証/認可プロファイルを示します。

```
key = "mytacacskey"
default authorization = permit
#-----------------------------Remote Host (BRI)-------------------------
#
# This allows the remote host to be authenticated by the local host
# during fist-stage authentication, and provides the remote host
# authorization profile.
#
#-----------------------------------------------------------------------
user = hostx
```

```
{
    login = cleartext “welcome”
    chap = cleartext “welcome”
    service = ppp protocol = lcp {
                interface-config=”ip unnumbered fastethernet 0"
    }
    service = ppp protocol = ip {
            # It is important to have the hash sign and some string after
            # it. This indicates to the NAS that you have a per-user
            # config.
            inacl#3=”permit tcp any 172.21.114.0 0.0.0.255 eq telnet”
            inacl#4=”deny icmp any any”
            route#5=”10.0.0.0 255.0.0.0"
            route#6=”10.10.0.0 255.0.0.0"
    }
    service = ppp protocol = ipx {
            # see previous comment about the hash sign and string, in protocol = ip
            inacl#3=”deny any”
    }
}
#------------------- “access-profile” default user “only acls” ------------------
#
# Without arguments, access-profile removes any access-lists it can find
# in the old configuration (both per-user and per-interface), and makes sure
# that the new profile contains ONLY access-list definitions.
#
#-------------------------------------------------------------------------------
user = pat_default
{
        login = cleartext “welcome”
        chap = cleartext “welcome”
        service = exec
        {
                # This is the autocommand that executes when pat_default logs in.
                autocmd = “access-profile”
        }
        service = ppp protocol = ip {
                # Put whatever access-lists, static routes, whatever
                # here.
                # If you leave this blank, the user will have NO IP
                # access-lists (not even the ones installed prior to
                # this)!
                inacl#3=”permit tcp any host 10.0.0.2 eq telnet”
                inacl#4=”deny icmp any any”
        }
        service = ppp protocol = ipx {
                # Put whatever access-lists, static routes, whatever
                # here.
                # If you leave this blank, the user will have NO IPX
                # access-lists (not even the ones installed prior to
                # this)!
        }
}
#--------------------- “access-profile merge” user --------------------------
#
# With the 'merge' option, first all old access-lists are removed (as before),
# but then (almost) all AV pairs are uploaded and installed. This will allow
# for uploading any custom static routes, sap-filters, and so on, that the user
# may need in his or her profile. This needs to be used with care, as it leaves
# open the possibility of conflicting configurations.
#
#-------------------------------------------------------------------------------
user = pat_merge
{
```

```
        login = cleartext “welcome”
        chap = cleartext “welcome”
        service = exec
        {
                # This is the autocommand that executes when pat_merge logs in.
                autocmd = “access-profile merge”
        }
        service = ppp protocol = ip
        {
                # Put whatever access-lists, static routes, whatever
                # here.
                # If you leave this blank, the user will have NO IP
                # access-lists (not even the ones installed prior to
                # this)!
                inacl#3=”permit tcp any any”
                route#2=”10.0.0.0 255.255.0.0"
                route#3=”10.1.0.0 255.255.0.0"
                route#4=”10.2.0.0 255.255.0.0"
        }
        service = ppp protocol = ipx
        {
                # Put whatever access-lists, static routes, whatever
                # here.
                # If you leave this blank, the user will have NO IPX
                # access-lists (not even the ones installed prior to
                # this)!
        }
}
#--------------------- “access-profile replace” user ----------------------------
#
# With the 'replace' option, ALL old configuration is removed and ALL new
# configuration is installed.
#
# One caveat: access-profile checks the new configuration for address-pool and
# address AV pairs. As addresses cannot be renegotiated at this point, the
# command will fail (and complain) when it encounters such an AV pair.
# Such AV pairs are considered to be “invalid” for this context.
#-------------------------------------------------------------------------------
user = pat_replace
{
        login = cleartex
t
“
welcome
”
        chap = cleartext “welcome”
        service = exec
        {
                # This is the autocommand that executes when pat_replace logs in.
                autocmd = “access-profile replace”
        }
        service = ppp protocol = ip
        {
                # Put whatever access-lists, static routes, whatever
                # here.
                # If you leave this blank, the user will have NO IP
                # access-lists (not even the ones installed prior to
                # this)!
                inacl#3=”permit tcp any any”
                inacl#4=”permit icmp any any”
                route#2=”10.10.0.0 255.255.0.0"
                route#3=”10.11.0.0 255.255.0.0"
                route#4=”10.12.0.0 255.255.0.0"
        }
```

```
        service = ppp protocol = ipx
        {
                # put whatever access-lists, static routes, whatever
                # here.
                # If you leave this blank, the user will have NO IPX
                # access-lists (not even the ones installed prior to
                # this)!
        }
}
```

自動二重認証の例

次に、自動二重認証が設定された設定ファイル全体の例を示します。自動二重認証に適用されるコンフィギュレーション コマンドは、2つのアスタリスク（**）を使用した記述よりも優先されます。

```
Current configuration:
!
version 11.3
no service password-encryption
!
hostname myrouter
!
!
! **The following AAA commands are used to configure double authentication:
!
! **The following command enables AAA:
aaa new-model
! **The following command enables user authentication via the RADIUS AAA server:
!
aaa authentication login default none
aaa authentication ppp default group radius
! **The following command causes the remote user's authorization profile to be
! downloaded from the AAA server to the router when required:
!
aaa authorization network default group radius
!
enable password mypassword
!
ip host blue 172.21.127.226
ip host green 172.21.127.218
ip host red 172.21.127.114
ip domain-name example.com
ip name-server 172.16.2.75
!
!
interface FastEthernet0/0/0
 ip address 172.21.127.186 255.255.255.248
 no ip route-cache
 no ip mroute-cache
 no keepalive
 ntp disable
 no cdp enable
!
interface Virtual-Template1
 ip unnumbered loopback0
 no ip route-cache
 no ip mroute-cache
!
! **The following command specifies that device authentication occurs via PPP CHAP:
 ppp authentication chap
```

```
!
router eigrp 109
 network 172.21.0.0
 no auto-summary
!
ip default-gateway 172.21.127.185
no ip classless
ip route 172.21.127.114 255.255.255.255 172.21.127.113
! **Virtual profiles are required for double authentication to work:
virtual-profile virtual-template 1
dialer-list 1 protocol ip permit
no cdp run
! **The following command defines where the TACACS+ AAA server is:
tacacs-server host 172.16.57.35 port 1049
tacacs-server timeout 90
! **The following command defines the key to use with TACACS+ traffic (required):
tacacs-server key mytacacskey
snmp-server community public RO
!
line con 0
 exec-timeout 0 0
 login authentication console
line aux 0
 transport input all
line vty 0 4
 exec-timeout 0 0
 password lab
!
end
```

この RADIUS AAA 設定のサンプル行は、次のように定義されます。

- **aaa new-model** コマンドは、AAA ネットワーク セキュリティ サービスをイネーブルにします。
- **aaa authentication login admins local** コマンドは、ログイン認証に別の方式リスト「admins」を定義します。
- **aaa authentication ppp dialins group radius local** コマンドで、まず RADIUS 認証を指定する認証方式リスト「dialins」を定義します。次に、（RADIUS サーバーが応答しない場合）PPP を使用するシリアル回線でローカル認証が使用されます。
- **aaa authorization network default group radius local** コマンドは、アドレスと他のネットワーク パラメータを RADIUS ユーザーに割り当てるために使用されます。
- **aaa accounting network default start-stop group radius** コマンドは、PPP の使用状況を追跡します。
- **username** コマンドはユーザー名とパスワードを定義します。これらの情報は、PPP パスワード認証プロトコル（PAP）の発信元身元確認に使用されます。
- **radius-server host** コマンドは RADIUS サーバー ホストの名前を定義します。
- **radius-server key** コマンドは、ネットワーク アクセス サーバーと RADIUS サーバー ホストの間の共有秘密テキスト文字列を定義します。
- **interface group-async** コマンドは、非同期インターフェイス グループを選択して定義します。

- **group-range** コマンドは、インターフェイス グループ内のメンバ非同期インターフェイスを定義します。
- **encapsulation ppp** コマンドは、指定のインターフェイスに使用されるカプセル化方式として PPP を設定します。
- **ppp authentication ms-chap dialins** コマンドは PPP 認証方式として MS-CHAP を選択し、特定のインターフェイスに「dialins」方式リストを適用します。
- **line** コマンドはコンフィギュレーション モードをグローバル コンフィギュレーションからライン コンフィギュレーションに切り替え、設定対象の回線を指定します。
- **autoselect ppp** コマンドは、選択した回線上で PPP セッションを自動的に開始できるようにします。
- **autoselect during-login** コマンドを使用すると、Return キーを押さずにユーザ名およびパスワードのプロンプトが表示されます。ユーザがログインすると、autoselect機能（この場合は PPP）が開始します。
- **login authentication admins** コマンドは、ログイン認証に「admins」方式リストを適用します。
- **modem dialin** コマンドは、選択した回線に接続されているモデムを設定し、着信コールだけを受け入れるようにします。

その他の参考資料

ここでは、認証の設定機能に関する関連資料について説明します。

関連資料

関連項目	マニュアル タイトル
許可	『*Cisco IOS XE Security Configuration Guide: Securing User Services*, Release 2』の「Configuring Authorization」
アカウンティング	『*Cisco IOS XE Security Configuration Guide: Securing User Service* , Release 2』の「Configuring Accounting」
セキュリティ コマンド	『*Cisco IOS Security Command Reference*』

標準

標準	タイトル
この機能でサポートされる新規の標準または変更された標準はありません。また、既存の標準のサポートは変更されていません。	--

MIB

MIB	MIB のリンク
この機能によってサポートされる新しい MIB または変更された MIB はありません。またこの機能による既存 MIB のサポートに変更はありません。	選択したプラットフォーム、Cisco IOS XE ソフトウェア リリース、およびフィーチャ セットの MIB の場所を検索しダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

RFC

RFC	タイトル
RFC 1334	PPP 認証プロトコル
RFC 2433	「Microsoft PPP CHAP Extensions」
RFC 2903	「*Generic AAA Architecture*」
RFC 2904	「*AAA Authorization Framework*」
RFC 2906	「*AAA Authorization Requirements*」
RFC 2989	「*Criteria for Evaluating AAA Protocols for Network Access*」

シスコのテクニカル サポート

説明	リンク
シスコのサポート Web サイトでは、シスコの製品やテクノロジーに関するトラブルシューティングにお役立ていただけるように、マニュアルやツールをはじめとする豊富なオンライン リソースを提供しています。 お使いの製品のセキュリティ情報や技術情報を入手するために、Cisco Notification Service（Field Notice からアクセス）、Cisco Technical Services Newsletter、Really Simple Syndication（RSS）フィードなどの各種サービスに加入できます。 シスコのサポート Web サイトのツールにアクセスする際は、Cisco.com のユーザ ID およびパスワードが必要です。	http://www.cisco.com/en/US/support/index.html

認証の設定に関する機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

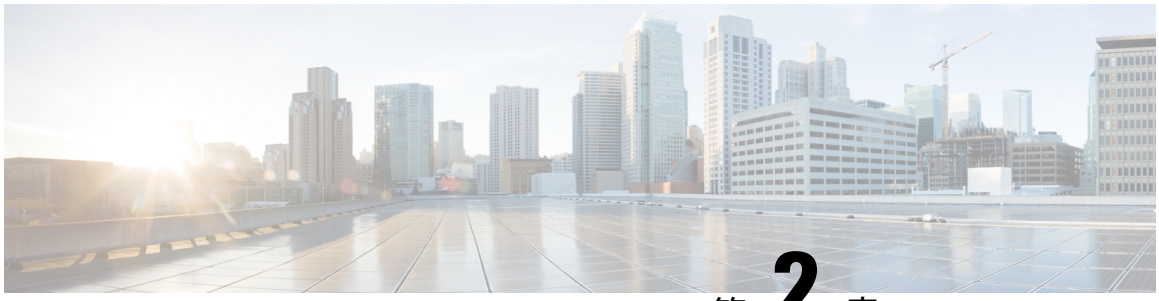
プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *10 :* 認証の設定に関する機能情報

機能名	リリース	機能情報
AAA 方式リストの拡張	Cisco IOS XE Release 2.1	この機能を使用すると、認証、許可、アカウンティングのフォールバック方式を有効にすることができます。フォールバック方式では、RADIUS または TACACS+ サーバまたは、場合によってはローカル データベースのグループ化の試行が行われます。 Cisco IOS XE Release 2.1 では、Cisco ASR 1000 シリーズ Aggregation Services Router にこの機能が実装されました。 次のコマンドが導入または変更されました。**aaa authentication ppp**。
AAA のユーザ別スケーラビリティ	Cisco IOS XE Release 2.3	AAA のユーザー別スケーラビリティ機能では、**ip vrf** および **ip unnumbered** コマンド向けに 2 つの RADIUS VSA がサポートされています。優れた拡張性を達成するために完全な VA インターフェイスの代わりに指定されている場合は、サブバーチャル アクセス インターフェイスを作成します。 Cisco IOS XE Release 2.3 では、Cisco ASR 1000 シリーズ Aggregation Services Router にこの機能が実装されました。

機能名	リリース	機能情報
チャレンジ ハンドシェイク認証プロトコル（CHAP）	Cisco IOS XE Release 2.1	現在、PPP は 2 つの認証プロトコルをサポートします。パスワード認証プロトコル（PAP）およびチャレンジ ハンドシェイク認証プロトコル（CHAP）の 2 つです。いずれも RFC 1334 で規定され、同期インターフェイスと非同期インターフェイスでサポートされます。PAP または CHAP を介する認証は、サーバーからのプロンプトを受けてユーザー名とパスワードを入力する方法と同等です。CHAP の場合、接続の間にリモート ユーザーのパスワードは送信されないため、より安全性が高いと考えられます。 この機能は、Cisco IOS XE Release 2.1 で Cisco ASR 1000 シリーズ アグリゲーション サービス ルータに導入されました。 次のコマンドが導入または変更されました。**ppp authentication**、 **ppp chap password**、 **ppp chap refuse**。
サーバ グループ レベルでのドメイン ストリッピング	Cisco IOS XE Release 3.4S	ドメイン ストリッピング機能を使用すると、ドメイン ストリッピングをサーバー グループ レベルで設定できます。サーバー単位のグループ コンフィギュレーションはグローバル コンフィギュレーションを上書きします。 この機能に関する詳細については、次の各項を参照してください。 • ドメイン ストリッピング • サーバー グループ レベルでのドメイン ストリッピングの設定 次のコマンドが導入されました：**domain-stripping**
二重認証	Cisco IOS XE Release 2.1	この機能は、Cisco IOS XE Release 2.1 で Cisco ASR 1000 シリーズ アグリゲーション サービス ルータに導入されました。 次のコマンドが導入または変更されました。**aaa authentication**、 **aaa authorization**、 **access-profile**。
AAA 認証のメッセージ バナー	Cisco IOS XE Release 2.1	Cisco IOS XE Release 2.1 では、Cisco ASR 1000 シリーズ Aggregation Services Router にこの機能が実装されました。 次のコマンドが導入されました。**aaa authentication banner**。

機能名	リリース	機能情報
MS-CHAP バージョン 1	Cisco IOS XE Release 2.1	マイクロソフト チャレンジ ハンドシェイク認証プロトコル（MS-CHAP）は、Microsoft バージョンの CHAP であり、RFC 1994 の拡張です。標準バージョンの CHAP と同様に、MS-CHAP は PPP 認証に使用されます。この場合、Microsoft Windows NT または Microsoft Windows 95 を使用する PC と、ネットワーク アクセス サーバとして動作する Cisco ルータまたはアクセス サーバとの間に認証が発生します。 Cisco IOS XE Release 2.1 では、Cisco ASR 1000 シリーズ Aggregation Services Router にこの機能が実装されました。 次のコマンドが導入または変更されました。**ppp authentication**。
Password Authentication Protocol（PAP）	Cisco IOS XE Release 2.1	現在、PPP は 2 つの認証プロトコルをサポートします。パスワード認証プロトコル（PAP）およびチャレンジハンドシェイク認証プロトコル（CHAP）の 2 つです。いずれも RFC 1334 で規定され、同期インターフェイスと非同期インターフェイスでサポートされます。PAP または CHAP を介する認証は、サーバーからのプロンプトを受けてユーザー名とパスワードを入力する方法と同等です。CHAP の場合、接続の間にリモート ユーザーのパスワードは送信されないため、より安全性が高いと考えられます。 この機能は、Cisco IOS XE Release 2.1 で Cisco ASR 1000 シリーズ アグリゲーション サービス ルータに導入されました。 次のコマンドが導入または変更されました。**ppp authentication**、**ppp pap sent-username**、 **ppp pap refuse**。
RADIUS：ユーザ名が空のアクセス要求を送信しないようにする CLI	Cisco IOS XE Release 2.4	この認証機能によって、ユーザ名が空のアクセス要求が RADIUS サーバに送信されないようにします。この機能により、RADIUS サーバとの不要なやりとりを回避でき、RADIUS ログの量を少なくすることができます。 Cisco IOS XE Release 2.4 では、Cisco ASR 1000 シリーズ Aggregation Services Router にこの機能が実装されました。 次のコマンドが導入されました。**aaa authentication suppress null-username**。



第 2 章

RADIUS 許可の変更

RADIUS認可変更（CoA）機能は、認証、許可、アカウンティング（AAA）セッションの属性を、セッション認証後に変更するためのメカニズムを提供します。AAAでユーザ、またはユーザ グループのポリシーに変更がある場合、管理者はCisco Secure Access Control Server（ACS）などのAAAサーバからRADIUS CoAパケットを送信して認証を再初期化し、新しいポリシーを適用することができます。

RADIUS 認可変更に関する情報

RADIUS 認可変更について

標準RADIUSインターフェイスは通常、ネットワークに接続しているデバイスから要求が送信され、クエリーが送信されたサーバが応答するプル モデルで使用されます。シスコのソフトウェアは、プッシュ モデルで使用されるRFC 5176で定義されたRADIUS CoA要求をサポートしています。このモデルでは、要求は外部サーバからネットワークに接続されたデバイスへ発信され、外部の認証、許可、アカウンティング（AAA）またはポリシー サーバからの動的なセッション再設定が可能になります。

次のセッション単位のCoA要求を使用します。

- セッション再認証
- セッションの終了
- ポート シャットダウンでのセッション終了
- ポート バウンスでのセッション終了
- セキュリティとパスワード

- アカウンティング

CoA 要求

CoA 要求は、RFC 5176 に記載されているように、プッシュ モデルで使用することによって、セッション識別、ホスト再認証、およびセッション終了を行うことができます。モデルは、次のように、1 つの要求（CoA-Request）と 2 つの考えられる応答コードで構成されます。

- CoA acknowledgment（ACK）[CoA-ACK]
- CoA non-acknowledgment（NAK）[CoA-NAK]

要求は CoA クライアント（通常は RADIUS またはポリシー サーバ）から開始されて、リスナーとして動作するデバイスに転送されます。

RFC 5176 規定

Disconnect Request メッセージは Packet of Disconnect（POD）とも呼ばれますが、セッション終了に対してデバイスでサポートされています。

次の表に、RADIUS 認可変更（CoA）機能でサポートされている IETF 属性を示します。

表 *11 :* サポートされている *IETF* 属性

属性番号	属性名
24	状態
31	Calling-Station-ID
44	Acct-Session-ID
80	Message-Authenticator
101	Error-Cause

次の表に、Error-Cause 属性で取ることができる値を示します。

表 *12 : Error-Cause* の値

値	説明
201	削除された残留セッション コンテキスト
202	無効な EAP パケット（無視）
401	サポートされていない属性
402	見つからない属性
403	NAS 識別情報のミスマッチ

値	説明
404	無効な要求
405	サポートされていないサービス
406	サポートされていない拡張機能
407	無効な属性値
501	管理上の禁止
502	ルート不可能な要求（プロキシ）
503	セッション コンテキストが検出されない
504	セッション コンテキストが削除できない
505	その他のプロキシ処理エラー
506	リソースが使用不可能
507	要求が発信された
508	マルチ セッションの選択がサポートされてない

CoA 要求応答コード

CoA 要求の応答コードは、デバイスへコマンドを発行するために使用されます。サポートされているコマンドを「CoA 要求コマンド」に示します。

RFC 5176 で定義されている CoA 要求応答コードのパケットの形式は、コード、ID、長さ、オーセンティケータ、およびタイプ、長さ、値（TLV）形式の属性から構成されます。

属性フィールドは、Cisco ベンダー固有属性（VSA）を送信するために使用します。

セッションの識別

特定のセッションに対する接続解除および CoA 要求の場合、デバイスは次の 1 つまたは複数の属性に基づいてセッションを検出します。

- Acct-Session-Id（IETF 属性 #44）
- Audit-Session-Id（シスコのベンダー固有属性（VSA））
- Calling-Station-Id（ホスト MAC アドレスを含む IETF 属性 #31）

CoA メッセージに含まれるすべてのセッション ID 属性がそのセッションと一致しない限り、デバイスは「Invalid Attribute Value」エラー コード属性を含む Disconnect-NAK または CoA-NAK を返します。

（注） CoA NAK メッセージは、キーの不一致があるすべての CoA 要求に送信されるわけではありません。メッセージは、クライアントの最初の 3 つの要求にのみ送信されます。その後、そのクライアントからのすべてのパケットがドロップされます。キーの不一致が見つかると、CoA NAK メッセージで送信される応答オーセンティケータはダミーのキー値から計算されます。

CoA ACK 応答コード

許可ステートの変更に成功した場合は、肯定確認応答（ACK）が送信されます。CoA ACK 内で返される属性は CoA 要求によって異なります。

CoA NAK 応答コード

否定応答（NAK）は許可ステートの変更に失敗したことを示し、エラーの理由を示す属性を含めることができます。

CoA 要求コマンド

デバイスでサポートされているコマンドを次の表に示します。すべての CoA コマンドには、デバイスと CoA クライアント間のセッション ID が含まれている必要があります。

表 *13*：デバイスでサポートされる *CoA* 要求コマンド

コマンド	シスコの VSA
Bounce host port	Cisco:Avpair="subscriber:command=bounce-host-port"
Disable host port	Cisco:Avpair="subscriber:command=disable-host-port"
Reauthenticate host	Cisco:Avpair="subscriber:command=reauthenticate"
Terminate session	VSA を必要としない標準の接続解除要求です

セッション再認証

セッション認証を開始するために、認証、許可、アカウンティング（AAA）サーバは、Cisco VSA と 1 つ以上のセッション ID 属性を含む標準 CoA 要求メッセージを送信します。Cisco VSA は、Cisco:Avpair=“subscriber:command=reauthenticate” の形式です。

次のシナリオでは、現在のセッション状態によって、メッセージに対するデバイスの応答が決まります。

- セッションが現在、IEEE 802.1*x* によって認証されている場合、デバイスは Extensible Authentication Protocol over LAN（EAPoL）-RequestId メッセージをサーバに送信することで応答します。
- セッションが現在 MAC 認証バイパス（MAB）によって認証されている場合、デバイスはアクセス要求をサーバに送信し、最初に成功した認証で使用したのと同じ ID 属性を渡します。

- デバイスがコマンドを受信した際にセッション認証が実行中である場合は、デバイスはプロセスを終了し、認証シーケンスを再開し、最初に試行されるように設定された方式で開始します。

セッションの終了

CoA 接続解除要求は、ホスト ポートをディセーブルにせずにセッションを終了します。CoA 接続解除要求終了によって、指定したホストのオーセンティケータ ステート マシンが再初期化されますが、ホストのネットワークへのアクセスは制限されません。セッションが見つからない場合、デバイスは「Session Context Not Found」エラー コード属性を使用して Disconnect-NAK メッセージを返します。セッションが見つかった場合、デバイスはセッションを終了します。セッションが完全に削除されると、デバイスは Disconnect-ACK メッセージを返します。

ホストのネットワークへのアクセスを制限するには、Cisco:Avpair="subscriber:command=disable-host-port" VSA を含む CoA 要求を使用します。このコマンドは、ホストがネットワーク上で問題を起こしていることを把握し、ホストのネットワーク アクセスを即座にブロックする必要がある場合に便利です。ポートのネットワーク アクセスを復元する場合は、非 RADIUS メカニズムを使用して再びイネーブルにします。

CoA 要求の disable host port

RADIUS サーバーの CoA disable port コマンドを実行すると、セッションをホストしている認証ポートが管理的にシャットダウンされます。その結果、セッションは終了します。このコマンドは、ホストがネットワーク上で問題を起こしていることを把握し、ホストのネットワーク アクセスを即座にブロックする必要がある場合に便利です。ポートのネットワーク アクセスを復元する場合は、非 RADIUS メカニズムを使用して再びイネーブルにします。このコマンドは、次の VSA を含む標準の CoA-Request メッセージで伝達されます。

Cisco:Avpair="subscriber:command=disable-host-port"

このコマンドはセッション指向であるため、「セッション ID」セクションに示されている 1 つ以上のセッション ID 属性とともに使用する必要があります。セッションを検出できない場合、デバイスは「Session Context Not Found」エラー コード属性を含む CoA-NAK メッセージを返します。デバイスは、セッションを検出すると、ホスティング ポートを無効にし、CoA-ACK メッセージを返します。

デバイスが CoA-ACK をクライアントに返す前にデバイスに障害が発生した場合、クライアントから要求が再送信されると、新しいアクティブ デバイス上でそのプロセスが繰り返されます。デバイスが CoA-ACK メッセージをクライアントに返した後でデバイスに障害が発生したが、操作が完了していない場合、その操作は新しいアクティブ デバイスで再開されます。

RADIUS サーバの CoA disable port コマンドを無視するには、「bounce および disable RADIUS CoA 要求を無視するためのデバイスの設定」を参照してください。

CoA 要求の bounce port

RADIUS サーバーの CoA bounce port が RADIUS サーバーから送信されると、認証ポートでリンクのフラップが発生します。その結果、このポートに接続している 1 つまたは複数のホストから、DHCP の再ネゴシエーションが開始されます。この状況は、VLAN の変更があり、この認証ポートに関する変化を検出するメカニズムがないデバイス（プリンタなど）がエンドポイ

ントの場合に発生する可能性があります。CoA bounce port は、次の新しい VSA を含む標準の CoA-Request メッセージで伝達されます。

Cisco:Avpair="subscriber:command=bounce-host-port"

このコマンドはセッション指向であるため、「セッション ID」に示されている 1 つ以上のセッション ID 属性とともに使用する必要があります。セッションが見つからない場合、デバイスは「Session Context Not Found」エラー コード属性を使用して CoA-NAK メッセージを返します。このセッションがある場合は、デバイスはホスト ポートを 10 秒間ディセーブルし、再びイネーブルにし（ポート バウンス）、CoA-ACK を返します。

RADIUS サーバの CoA bounce port を無視するには、「bounce および disable RADIUS CoA 要求を無視するためのデバイスの設定」を参照してください。

RADIUS 認可変更の設定方法

RADIUS 認可変更の設定

手順の概要

1. **enable**
2. **configure terminal**
3. **aaa new-model**
4. **aaa server radius dynamic-author**
5. **client** {*ip-address* | *name* [**vrf** *vrf-name*]} **server-key** [**0** | **7**] *string*
6. **port** *port-number*
7. **auth-type** {**any** | **all** | **session-key**}
8. **ignore session-key**
9. **ignore server-key**
10. **exit**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**aaa new-model** 例：	認証、認可、アカウンティング（AAA）をグローバルに有効化します。

	コマンドまたはアクション	目的
	`Device(config)# aaa new-model`	
ステップ 4	**aaa server radius dynamic-author** 例： `Device(config)# aaa server radius dynamic-author`	ダイナミック認可ローカル サーバー コンフィギュレーション モードを開始し、デバイスが認可変更（CoA）を受け入れ、要求を取り外す RADIUS クライアントを指定します。デバイスを AAA サーバーとして設定し、外部ポリシー サーバーとの連携を可能にする。
ステップ 5	**client** {*ip-address* | *name* [**vrf** *vrf-name*]} **server-key** [**0** | **7**] *string* 例： `Device(config-locsvr-da-radius)# client 10.0.0.1`	RADIUS キーをデバイスと RADIUS クライアントとの間で共有されるように設定します。
ステップ 6	**port** *port-number* 例： `Device(config-locsvr-da-radius)# port 3799`	設定された RADIUS クライアントから RADIUS 要求をデバイスが受信するポートを指定します。 （注） パケットオブディスコネクトのデフォルト ポートは 1700 です。ACS 5.1 と相互運用するためには、ポート 3799 が必要です。
ステップ 7	**auth-type** {**any** | **all** | **session-key**} 例： `Device(config-locsvr-da-radius)# auth-type all`	デバイスが RADIUS クライアントに使用する認可のタイプを指定します。クライアントは、認可用に設定された属性と一致していなければなりません。
ステップ 8	**ignore session-key** 例： `Device(config-locsvr-da-radius)# ignore session-key`	（オプション）セッション キーを無視するようにデバイスを設定します。
ステップ 9	**ignore server-key** 例： `Device(config-locsvr-da-radius)# ignore server-key`	（オプション）サーバー キーを無視するようにデバイスを設定します。
ステップ 10	**exit** 例： `Device(config-locsvr-da-radius)# exit`	グローバル コンフィギュレーション モードに戻ります。

bounce および disable RADIUS CoA 要求を無視するためのデバイスの設定

複数のホストを使用して認証ポートを認証していて、このポートで 1 つのホストに対してフラップする認可変更（CoA）要求があるか、このポートで終了するホストセッションがある場合、このポート上のその他のホストにも影響があります。したがって、複数のホストを使用して認証されたポートは、フラップの場合に 1 つまたは複数のホストから DHCP の再ネゴシエーションをトリガーします。または、1 つまたは複数のホストについて、セッションをホストする認証ポートを管理的にシャットダウンします。

次の手順を使用して、bounce port コマンドまたは disable port コマンドの形式で RADIUS サーバの認可変更（CoA）要求を無視するようにデバイスを設定します。

手順の概要

1. **enable**
2. **configure terminal**
3. **aaa new-model**
4. **authentication command bounce-port ignore**
5. **authentication command disable-port ignore**
6. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**aaa new-model** 例： `Device(config)# aaa new-model`	認証、認可、アカウンティング（AAA）をグローバルに有効化します。
ステップ 4	**authentication command bounce-port ignore** 例： `Device(config)# authentication command bounce-port ignore`	（任意）RADIUS サーバの bounce port コマンドを無視するようにデバイスを設定します。無視しない場合、認証ポート上でホストがフラップをリンクし、結果として、そのポートに接続する 1 つまたは複数のホストから DHCP 再ネゴシエーションが発生します。

	コマンドまたはアクション	目的
ステップ 5	**authentication command disable-port ignore** 例： `Device(config)# authentication command disable-port ignore`	（任意）RADIUS サーバの CoA disable port コマンドを無視するようにデバイスを設定します。無視しない場合、1 または複数のホスト セッションをホストする認証ポートが管理的にシャットダウンされます。 • ポートがシャットダウンされると、セッションも終了します。
ステップ 6	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。

RADIUS CoA 用の動的認可サービスの設定

次の手順を実行して、動的許可サービスの認証、許可、アカウンティング（AAA）サーバとしてデバイスを有効にします。このサービスは、入力方向と出力方向でポリシー マップをプッシュする認可変更（CoA）機能をサポートします。

手順の概要

1. **enable**
2. **configure terminal**
3. **aaa new-model**
4. **aaa server radius dynamic-author**
5. **client** {*ip-addr* | *hostname*} [**server-key** [**0** | **7**] *string*]
6. **domain** {**delimiter** *character* | **stripping** | [**right-to-left**]}
7. **port** *port-num*
8. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 3	**aaa new-model** 例： `Device(config)# aaa new-model`	AAA をグローバルに有効にします。
ステップ 4	**aaa server radius dynamic-author** 例： `Device(config)# aaa server radius dynamic-author`	ローカル AAA サーバを動的認可サービス用にセットアップして、動的認可ローカル サーバ コンフィギュレーション モードに入ります。このサービスは、ポリシー マップを入力方向と出力方向にプッシュする CoA 機能をサポートするように有効にする必要があります。 • このモードでは、RADIUS アプリケーション コマンドが設定されます。
ステップ 5	**client** {*ip-addr* | *hostname*} [**server-key** [**0** | **7**] *string*] 例： `Device(config-locsvr-da-radius)# client 192.168.0.5 server-key cisco1`	AAA サーバー クライアントの IP アドレスまたはホスト名を設定します。 • オプションの **server-key** キーワードと *string* 引数を使用して、クライアントレベルのサーバー キーを設定します。 （注） クライアント レベルでサーバー キーを設定すると、グローバル レベルで設定されたサーバー キーが上書きされます。
ステップ 6	**domain** {**delimiter** *character* | **stripping** | [**right-to-left**]} 例： `Device(config-locsvr-da-radius)# domain stripping right-to-left`	（任意）RADIUS アプリケーションについてユーザ名のドメイン オプションを設定します。 • **delimiter** キーワードで、ドメインデリミタを指定します。次のいずれかのオプションを *character* 引数に指定できます。**@**、**/**、**$**、**%**、****、**#**、または **-**。 • **stripping** キーワードは、着信のユーザー名と、**@** ドメインデリミタの左側にある名前を比較します。 • The **right-to-left** キーワードは、右から左方向に見て最初のデリミタで文字列を終了します。
ステップ 7	**port** *port-num* 例： `Device(config-locsvr-da-radius)# port 3799`	CoA 要求に UDP ポートを設定します。

	コマンドまたはアクション	目的
ステップ 8	**end** 例： `Device(config-locsvr-da-radius)# end`	特権 EXEC モードに戻ります。

RADIUS 認可変更のモニタリングとトラブルシューティング

RADIUS認可変更機能のモニタリングおよび問題を解決するために、次のコマンドを使用できます。

表 *14 : RADIUS* 認可変更のモニタリングとトラブルシューティング

コマンド	目的
debug aaa coa	CoA 処理のデバッグ情報を表示します。
debug aaa pod	パケットオブディスコネクト（POD）パケットに関連するデバッグ メッセージを表示します。
debug radius	RADIUS 関連の情報を表示します。
show aaa attributes protocol radius	認証、許可、アカウンティング（AAA）属性番号と対応するAAA属性名のマッピングを表示します。

RADIUS 認可変更の設定例

例：RADIUS 認可変更の設定

```
Device> enable
Device# configure terminal
Device(config)# aaa new-model
Device(config)# aaa server radius dynamic-author
Device(config-locsvr-da-radius)# client 10.0.0.1
Device(config-locsvr-da-radius)# server-key cisco123
Device(config-locsvr-da-radius)# port 3799
Device(config-locsvr-da-radius)# auth-type all
Device(config-locsvr-da-radius)# ignore session-key
Device(config-locsvr-da-radius)# ignore server-key
Device(config-locsvr-da-radius)# end
```

例：bounce および disable RADIUS 要求を無視するためのデバイスの設定

```
Device> enable
Device# configure terminal
Device(config)# aaa new-model
Device(config)# authentication command bounce-port ignore
Device(config)# authentication command disable-port ignore
Device(config)# end
```

例：RADIUS CoA 用の動的認可サービスの設定

次に、認証、許可、アカウンティング（AAA）サーバとしてのデバイスが、入力方向と出力方向でポリシー マップをプッシュする認可変更（CoA）機能をサポートするように設定する例を示します。

```
Device> enable
Device# configure terminal
Device(config)# aaa new-model
Device(config)# aaa server radius dynamic-author
Device(config-locsvr-da-radius)# client 192.168.0.5 server-key cisco1
Device(config-locsvr-da-radius)# domain delimiter @
Device(config-locsvr-da-radius)# port 3799
Device(config-locsvr-da-radius)# end
```

RADIUS 認可変更に関する追加情報

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『Cisco IOS Master Command List, All Releases』

関連項目	マニュアル タイトル
セキュリティ コマンド	• 『Security Command Reference: Commands A to C』 • 『Security Command Reference: Commands D to L』 • 『Security Command Reference: Commands M to R』 • 『Security Command Reference: Commands S to Z』
AAA の設定	『*Authentication, Authorization, and Accounting Configuration Guide*』

標準および RFC

標準/RFC	タイトル
RFC 2903	「*Generic AAA Architecture*」
RFC 5176	「*Dynamic Authorization Extensions to Remote Authentication Dial In User Service (RADIUS)*」

シスコのテクニカル サポート

説明	リンク
右の URL にアクセスして、シスコのテクニカル サポートを最大限に活用してください。これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

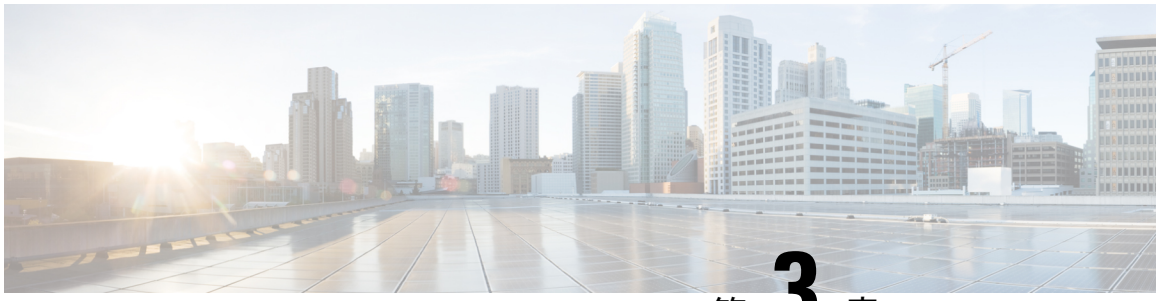
RADIUS 認可変更の機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *15 : RADIUS* 認可変更の機能情報

機能名	リリース	機能情報
RADIUS 許可の変更		RADIUS 認可変更（CoA）機能は、AAA セッションの属性をセッション認証後に変更するためのメカニズムを提供します。AAA でユーザ、またはユーザ グループのポリシーに変更がある場合、管理者は Cisco Secure Access Control Server（ACS）などの AAA サーバから RADIUS CoA パケットを送信して認証を再初期化し、新しいポリシーを適用することができます。 次のコマンドが導入または変更されました。**aaa server radius dynamic-author**、**authentication command bounce-port ignore**、**authentication command disable-port ignore**



第 3 章

AAA 認証のメッセージ バナー

AAA 認証のメッセージ バナー機能は、ユーザ認証のためにパーソナライズされたログイン バナーおよび failed-login バナーを設定するために使用されます。ユーザが認証、許可、アカウンティング（AAA）を使用して認証を受けるシステムにログインする場合に認証が失敗すると、メッセージ バナーが表示されます。

AAA 認証のメッセージ バナーに関する情報

AAA 認証のログイン バナーおよび Failed-Login バナー

ログイン バナーおよび failed-login バナーは、認証、許可、およびアカウンティング（AAA）認証用のバナーとして表示する必要があるテキスト文字列そのものをシステムに通知するデリミタを使用します。デリミタは、ログイン バナーまたは failed-login バナーの末尾を示すために、テキスト文字列の末尾で繰り返されます。デリミタには、拡張 ASCII 文字セットの任意の 1 文字を使用できます。ただし、デリミタとして定義した文字は、バナー用のテキスト文字列には使用できません。

ログイン バナーまたは failed-login バナーには、最大 2996 文字を表示できます。

AAA 認証のメッセージ バナーの設定方法

AAA 認証のログイン バナーの設定

次の作業を行って、ユーザがログインするときに表示されるバナーを設定します（デフォルトのログイン メッセージを置き換えます）。ログインバナーを無効にするには、**no aaa authentication banner** コマンドを使用します。

手順の概要

1. **enable**
2. **configure terminal**
3. **aaa new-model**
4. **aaa authentication banner** *delimiter-string delimiter*
5. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**aaa new-model** 例： `Device(config)# aaa new-model`	AAA をグローバルに有効にします。
ステップ 4	**aaa authentication banner** *delimiter-string delimiter* 例： `Device(config)# aaa authentication banner *Unauthorized Access Prohibited*`	パーソナライズされたログイン バナーを作成します。
ステップ 5	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。

AAA 認証の Failed-Login バナーの設定

次の作業を行って、ユーザ ログインが失敗したときに表示される faild-login バナーを設定します（デフォルトのメッセージを failed-login に置き換えます）。failed-login バナーをディセーブルにするには、**no aaa authentication fail-message** コマンドを使用します。

手順の概要

1. **enable**
2. **configure terminal**
3. **aaa new-model**
4. **aaa authentication banner** *delimiter-string delimiter*
5. **aaa authentication fail-message** *delimiter-string delimiter*
6. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**aaa new-model** 例： `Device(config)# aaa new-model`	AAA をグローバルに開始します。
ステップ 4	**aaa authentication banner** *delimiter-string delimiter* 例： `Device(config)# aaa authentication banner *Unauthorized Access Prohibited*`	パーソナライズされたログイン バナーを作成します。
ステップ 5	**aaa authentication fail-message** *delimiter-string delimiter* 例： `Device(config)# aaa authentication fail-message *Failed login. Try again*`	ユーザー ログインが失敗したときに表示されるメッセージを作成します。

	コマンドまたはアクション	目的
ステップ 6	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。

AAA 認証のメッセージ バナーの設定例

例：AAA 認証のログイン バナーおよび Failed-Login バナーの設定

次に、ユーザーがシステムにログインするときに表示されるログイン バナー（この場合、「Unauthorized Access Prohibited」というフレーズ）を設定する例を示します。アスタリスク（*）はデリミタとして使用されます。RADIUS はデフォルト ログイン認証方式として指定されます。

```
Device> enable
Device# configure terminal
Device(config)# aaa new-model
Device(config)# aaa authentication banner *Unauthorized Access Prohibited*
Device(config)# aaa authentication login default group radius
```

この設定によって、次のログイン バナーが表示されます。

```
Unauthorized Access Prohibited
Username:
```

次の例では、ユーザーがシステムにログインしようとして失敗すると表示される Failed-Login バナー（この場合、「Failed login. Try again」というフレーズ）を設定する方法を示します。アスタリスク（*）はデリミタとして使用されます。RADIUS はデフォルト ログイン認証方式として指定されます。

```
Device> enable
Device# configure terminal
Device(config)# aaa new-model
Device(config)# aaa authentication banner *Unauthorized Access Prohibited*
Device(config)# aaa authentication fail-message *Failed login. Try again.*
Device(config)# aaa authentication login default group radius
```

この設定によって、次のログイン バナーおよび Failed-Login バナーが表示されます。

```
Unauthorized Access Prohibited
Username:
Password:
Failed login. Try again.
```

AAA 認証のメッセージ バナーに関する追加情報

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『Cisco IOS Master Command List, All Releases』
セキュリティ コマンド	• 『Security Command Reference: Commands A to C』 • 『Security Command Reference: Commands D to L』 • 『Security Command Reference: Commands M to R』 • 『Security Command Reference: Commands S to Z』
AAA の設定	『*Authentication, Authorization, and Accounting Configuration Guide*』

シスコのテクニカル サポート

説明	リンク
右の URL にアクセスして、シスコのテクニカル サポートを最大限に活用してください。これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

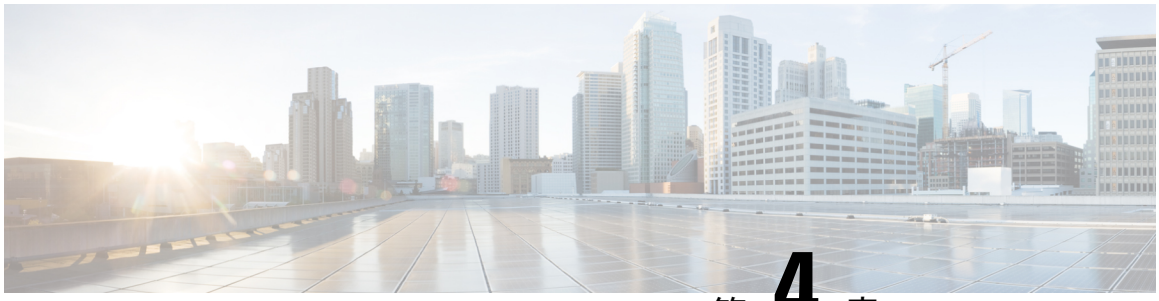
AAA 認証のメッセージ バナーの機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *16 : AAA* 認証のメッセージ バナーの機能情報

機能名	リリース	機能情報
AAA 認証のメッセージバナー		AAA 認証のメッセージバナー機能により、ユーザ認証のためにパーソナライズされたログイン バナーおよび failed-login バナーを設定できます。ユーザが認証、許可、アカウンティング（AAA）を使用して認証を受けるシステムにログインする場合に認証が失敗すると、メッセージ バナーが表示されます。 次のコマンドが導入または変更されました。**aaa authentication banner**、 **aaa authentication fail-message**、、および **aaa new-model**。



第 4 章

サーバ グループ レベルでの AAA ドメイン ストリッピング

サーバ グループ レベルでの AAA ドメイン ストリッピング機能を使用すると、ドメイン ストリッピングをサーバ グループ レベルで設定できます。

サーバ グループ レベルでの AAA ドメイン ストリッピングに関する情報

radius-server domain-stripping コマンドを使用して、グローバルレベルで受信したユーザー名からドメイン名を削除できます。 **radius-server domain-stripping** コマンドを設定すると、「user@example.com」を含むすべての AAA 要求のユーザー名が「user」に再フォーマットされてリモート RADIUS サーバーに送信されます。ドメイン名は要求から削除されます。

（注） ドメイン ストリッピングは TACACS 設定では行われません。

AAA ブロードキャスト アカウンティング機能を有効にすると、アカウンティング情報を複数の AAA サーバーに同時に送信できます。つまり、アカウンティング情報を 1 つまた複数の AAA サーバーに同時にブロードキャストすることが可能です。この機能を使用すると、プライベートおよびパブリック AAA サーバーにアカウント情報を送信できます。この機能では、音声アプリケーションによる課金情報も提供されます。

サーバーグループ RADIUS コンフィギュレーション モードで **domain-stripping** コマンドを使用すると、ドメインストリッピングをサーバーグループレベルで設定できます。サーバー単位のグループ コンフィギュレーションはグローバル コンフィギュレーションを上書きします。

ドメイン ストリッピングが、グローバルではイネーブルではないがサーバー グループでイネーブルになっている場合、そのサーバー グループに対してのみイネーブルになります。また、Virtual Routing and Forwarding（VRF）固有のドメイン ストリッピングがグローバルで設定されていて、別の VRF のドメイン ストリッピングがサーバー グループで設定されている場合、ドメイン ストリッピングは両方の VRF でイネーブルになります。VRF の設定は、サーバーグループ コンフィギュレーション モードから取得されます。サーバーグループ コンフィギュレーションがグローバル コンフィギュレーション モードでディセーブルになっているが、サーバーグループ コンフィギュレーション モードで使用可能である場合、サーバーグループ コンフィギュレーション モードでのすべての設定が適用可能です。

ドメイン ストリッピングおよびブロードキャスト アカウンティングを設定した後で、設定ごとに別個のアカウンティング レコードを作成できます。

サーバ レベル グループでの AAA ドメイン ストリッピングの設定方法

サーバー グループ レベルでのドメイン ストリッピングの設定

手順の概要

1. **enable**
2. **configure terminal**
3. **aaa new-model**
4. **aaa group server radius** *server-name*
5. **domain-stripping** [**strip-suffix** *word*] [**right-to-left**] [**prefix-delimiter** *word*] [**delimiter** *word*]
6. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**aaa new-model** 例： `Device(config)# aaa new-model`	AAA をイネーブルにします。

	コマンドまたはアクション	目的
ステップ 4	**aaa group server radius** *server-name* 例： `Device(config)# aaa group server radius rad1`	RADIUS サーバを追加し、サーバ グループ RADIUS コンフィギュレーション モードを開始します。 • *server-name* 引数には、RADIUS サーバー グループ名を指定します。
ステップ 5	**domain-stripping** [**strip-suffix** *word*] [**right-to-left**] [**prefix-delimiter** *word*] [**delimiter** *word*] 例： `Device(config-sg-radius)# domain-stripping delimiter username@example.com`	サーバー グループ レベルでドメイン ストリッピングを設定します。
ステップ 6	**end** 例： `Device(config-sg-radius)# end`	サーバー グループ RADIUS コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

サーバ グループ レベルでの AAA ドメイン ストリッピングの設定例

例：サーバ グループ レベルでの AAA ドメイン ストリッピング

次に、サーバ グループ レベルでのドメイン ストリッピング設定の例を示します。

```
Device> enable
Device# configure terminal
Device(config)# aaa new-model
Device(config)# aaa group server radius rad1
Device(config-sg-radius)# domain-stripping right-to-left delimiter @$/
Device(config-sg-radius)# end
```

その他の参考資料

ここでは、認証の設定機能に関する関連資料について説明します。

関連資料

関連項目	マニュアル タイトル
許可	『*Cisco IOS XE Security Configuration Guide: Securing User Services*, Release 2』の「Configuring Authorization」

関連項目	マニュアル タイトル
アカウンティング	『*Cisco IOS XE Security Configuration Guide: Securing User Service* , Release 2』の「Configuring Accounting」
セキュリティ コマンド	『*Cisco IOS Security Command Reference*』

標準

標準	タイトル
この機能でサポートされる新規の標準または変更された標準はありません。また、既存の標準のサポートは変更されていません。	--

MIB

MIB	MIB のリンク
この機能によってサポートされる新しい MIB または変更された MIB はありません。またこの機能による既存 MIB のサポートに変更はありません。	選択したプラットフォーム、Cisco IOS XE ソフトウェア リリース、およびフィーチャ セットの MIB の場所を検索しダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

RFC

RFC	タイトル
RFC 1334	PPP 認証プロトコル
RFC 2433	「Microsoft PPP CHAP Extensions」
RFC 2903	「*Generic AAA Architecture*」
RFC 2904	「*AAA Authorization Framework*」
RFC 2906	「*AAA Authorization Requirements*」
RFC 2989	「*Criteria for Evaluating AAA Protocols for Network Access*」

シスコのテクニカル サポート

説明	リンク
シスコのサポート Web サイトでは、シスコの製品やテクノロジーに関するトラブルシューティングにお役立ていただけるように、マニュアルやツールをはじめとする豊富なオンライン リソースを提供しています。 お使いの製品のセキュリティ情報や技術情報を入手するために、Cisco Notification Service（Field Notice からアクセス）、Cisco Technical Services Newsletter、Really Simple Syndication（RSS）フィードなどの各種サービスに加入できます。 シスコのサポート Web サイトのツールにアクセスする際は、Cisco.com のユーザ ID およびパスワードが必要です。	http://www.cisco.com/en/US/support/index.html

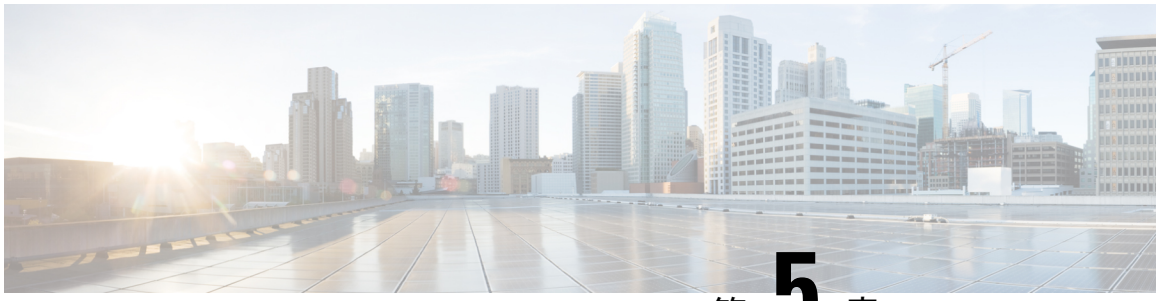
サーバ グループ レベルでの AAA ドメイン ストリッピングの機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *17*：サーバ グループ レベルでの *AAA* ドメイン ストリッピングの機能情報

機能名	リリース	機能情報
サーバ グループ レベルでの AAA ドメイン ストリッピング	Cisco IOS XE Release 3.4S	サーバ グループ レベルでの AAA ドメイン ストリッピング機能を使用すると、ドメイン ストリッピングをサーバ グループ レベルで設定できます。 次のコマンドが導入されました：**domain-stripping**



第 5 章

AAA Double Authentication Secured by Absolute Timeout

AAA Double Authentication Secured by Absolute Timeout 機能により、ユーザ単位のセッション タイムアウトを使用して保護することで、二重の認証メカニズムが確保されます。この機能は、サービスプロバイダーにより認可されたネットワークへの接続を最適化し、不要なセッションが接続されないようにすることで、ネットワークへのアクセス全体のセキュリティを高めます。

AAA Double Authentication Secured by Absolute Timeout の前提条件

- Cisco RADIUS サーバまたは TACACS+ サーバにアクセスできる必要があります。また、RADIUS または TACACS+ の設定方法を十分に理解していることが必要です。
- 認証、許可、アカウンティング（AAA）の設定方法および AAA 自動二重認証の有効化方法を十分理解していることが必要です。

AAA Double Authentication Secured by Absolute Timeout の制約事項

- AAA Double Authentication Secured by Absolute Timeout 機能は、PPP 接続専用です。自動二重認証は、X.25 やシリアル ライン インターネット プロトコル（SLIP）などの他のプロトコルとともに使用することはできません。
- TACACS+ サーバが使用されている場合、パフォーマンスにわずかに影響することがあります。ただし、RADIUS サーバが使用されている場合は、パフォーマンスへの影響はありません。

AAA Double Authentication Secured by AbsoluteTimeout に関する情報

AAA 二重認証

ホストのユーザ名とパスワードを使用して最初の認証を渡すために、AAA 二重認証メカニズムを使用します。2 回目の認証は、チャレンジ ハンドシェイク認証プロトコル（CHAP）またはパスワード認証プロトコル（PAP）認証の後で行われますが、このときはログインユーザ名とそのパスワードが使用されます。最初の認証では、PPP セッション タイムアウトがローカルまたはリモートで設定されていれば、PPP セッション タイムアウトがバーチャル アクセス インターフェイスに適用されます。

AAA Double Authentication Secured by Absolute Timeout 機能により、ユーザ単位のセッション タイムアウトを使用して保護することで、二重の認証メカニズムが確保されます。ユーザ単位のセッション タイムアウトは、一般的な絶対タイムアウト値よりも優先されるほか、カスタマイズすることが可能です。このメカニズムの動作原理は、二重認証のユーザ単位のアクセス コントロール リスト（ACL）と同じです。

AAA Double Authentication Secured by Absolute Timeout の適用方法

AAA Double Authentication Secured by Absolute Timeout の適用

絶対タイムアウトを適用するために、リンク コントロール プロトコル（LCP）のユーザ単位の属性としてログイン ユーザ プロファイルでセッション タイムアウトを設定する必要があります。AAA 二重認証を有効にするには、**access-profile** コマンドを使用します。このコマンド

は、PPPセッション中にインターフェイスにユーザ単位の認可属性を適用するために使用されます。**access-profile** コマンドを使用する前に、LCP のユーザー単位の属性（セッションタイムアウトなど）を再度認可してから、ネットワーク制御プロトコル（NCP）を再度認可して、ACL やルートなどの他の必要な条件を適用します。「AAA Double Authentication Secured by Absolute Timeout の例」を参照してください。

（注） TACACS+ユーザ プロファイルのタイムアウト設定は、RADIUS ユーザ プロファイルの設定とは異なります。RADIUS プロファイルでは、autocommand の **access-profile** とともに 1 つのセッションタイムアウトだけが設定されています。このタイムアウトは EXEC セッションおよび PPP セッションにそれぞれ適用されます。TACACS+ では、タイムアウトはサービス タイプ「exec」および「ppp」（LCP）下で設定し、EXEC セッションと PPP セッションに適用する必要があります。タイムアウトをサービス タイプ「ppp」下でのみ設定すると、そのタイムアウト値は EXEC 認可で使用できず、EXEC セッションに適用されません。

AAA Double Authentication Secured by Absolute Timeout の設定例

例：RADIUS ユーザ プロファイル

次の出力例は、RADIUS ユーザ プロファイルが適用されていることと、AAA 二重認証が絶対タイムアウトによって保護されていることを示しています。

```
aaapbx2 Password = "password1",
 Service-Type = Framed,
 Framed-Protocol = PPP,
 Session-Timeout = 180,
 Idle-Timeout = 180000,
 cisco-avpair = "ip:inacl#1=permit tcp any any eq telnet"
 cisco-avpair = "ip:inacl#2=permit icmp any any"
broker_default Password = "password1",
 Service-Type = Administrative,
 cisco-avpair = "shell:autocmd=access-profile",
 Session-Timeout = 360,
 cisco-avpair = "ip:inacl#1=permit tcp any any"
 cisco-avpair = "ip:inacl#2=permit icmp any any"
broker_merge Password = "password1",
 Service-Type = Administrative,
 cisco-avpair = "shell:autocmd=access-profile merge",
 Session-Timeout = 360,
 cisco-avpair = "ip:inacl#1=permit tcp any any"
 cisco-avpair = "ip:inacl#2=permit icmp any any"
 cisco-avpair = "ip:route#3=10.4.0.0 255.0.0.0"
 cisco-avpair = "ip:route#4=10.5.0.0 255.0.0.0"
 cisco-avpair = "ip:route#5=10.6.0.0 255.0.0.0"
broker_replace Password = "password1",
 Service-Type = Administrative,
 cisco-avpair = "shell:autocmd=access-profile replace",
 Session-Timeout = 360,
```

```
 cisco-avpair = "ip:inacl#1=permit tcp any any"
 cisco-avpair = "ip:inacl#2=permit icmp any any"
 cisco-avpair = "ip:route#3=10.4.0.0 255.0.0.0"
 cisco-avpair = "ip:route#4=10.5.0.0 255.0.0.0"
 cisco-avpair = "ip:route#5=10.6.0.0 255.0.0.0"
```

例：TACACS ユーザ プロファイル

次の出力例は、TACACS+ ユーザ プロファイルが適用されていることと、AAA 二重認証が絶対タイムアウトによって保護されていることを示しています。

リモート ホスト認証

次に、最初の段階の認証でリモート ホストがローカル ホストによって認証され、リモート ホストの認可プロファイルが提供される例を示します。

```
user = aaapbx2
 chap = cleartext Cisco
 pap = cleartext cisco
 login = cleartext cisco
 service = ppp protocol = lcp
  idletime = 3000
  timeout = 3
 service = ppp protocol = ip
  inacl#1="permit tcp any any eq telnet"
 service = ppp protocol = ipx
```

引数のない access-profile コマンドの使用

引数を何も付けずに **access-profile** コマンドを実行すると、古い設定（ユーザー単位およびインターフェイス単位）で見つかったアクセスリストがすべて削除され、アクセスリストの定義のみが新しいプロファイルに存在する状態になります。

```
user = broker_default
 login = cleartext Cisco
 chap = cleartext "cisco"
 service = exec
  autocmd = "access-profile"
! This is the autocommand that executes when broker_default logs in.
  timeout = 6
 service = ppp protocol = lcp
  timeout = 6
 service = ppp protocol = ip
! Put access lists, static routes, and other requirements that are
! needed here. Read the software specifications for details. If you leave
! this blank, the user will have no access lists (not even the ones that were
! installed prior to the creation of this user profile)!
  inacl#1="permit tcp any any"
  inacl#2="permit icmp host 10.0.0.0 any"
 service = ppp protocol = ipx
! Put access lists, static routes, and other requirements that are
! needed here. Read the software specifications for details. If you leave
! this blank, the user will have no access lists (not even the ones that were
! installed prior to the creation of this user profile)!
```

merge キーワードを指定した access-profile コマンドの使用

access-profile コマンドの **merge** キーワードを使用して、すべての古いアクセスリストを削除すると、属性と値（AV）のペアのアップロードおよびインストールが許可されます。**merge** キーワードを使用すると、カスタムのスタティックルート、Service Advertisement Protocol（SAP）フィルタ、プロファイルに必要になることがある他の要件をアップロードできます。**merge** キーワードは競合する設定のあらゆる要素を未処理のままにするため、注意して設定してください。

```
user = broker_merge
 login = cleartext Cisco
 chap = cleartext "cisco"
 service = exec
  autocmd = "access-profile merge"
! This is the autocommand that executes when broker_merge logs in.
  timeout = 6
 service = ppp protocol = lcp
 timeout = 6
 service = ppp protocol = ip
! Put access lists, static routes, and other requirements that are
! needed here. Read the software specifications for details. If you leave
! this blank, the user will have no access lists (not even the ones that were
! installed prior to the creation of this user profile)!
  route#1="10.4.0.0 255.0.0.0"
  route#2="10.5.0.0 255.0.0.0"
  route#3="10.6.0.0 255.0.0.0"
  inacl#5="permit tcp any any"
  inacl#6="permit icmp host 10.60.0.0 any"
 service = ppp protocol = ipx
! Put access lists, static routes, and other requirements that are
! needed here. Read the software specifications for details. If you leave
! this blank, the user will have no access lists (not even the ones that were
! installed prior to the creation of this user profile)!
```

replace キーワードを指定した access-profile コマンドの使用

access-profile コマンドに **replace** キーワードを指定して実行すると、古い設定がすべて削除され、新しい設定がインストールされます。

（注） **access-profile** コマンドを設定すると、アドレスプールとアドレスと AV のペアについて新しい設定がチェックされます。この時点でアドレスは再ネゴシエートできないため、このコマンドはそのようなアドレスと AV のペアを検出すると正常に動作しません。

```
user = broker_replace
 login = cleartext Cisco
 chap = cleartext "cisco"
 service = exec
  autocmd = "access-profile replace"
! This is the autocommand that executes when broker_replace logs in.
  timeout = 6
 service = ppp protocol = lcp
  timeout = 6
 service = ppp protocol = ip
! Put access lists, static routes, and other requirements that are
! needed here. Read the software specifications for details. If you leave
```

```
! this blank, the user will have no access lists (not even the ones that were
! installed prior to the creation of this user profile)!
  route#1="10.7.0.0 255.0.0.0"
  route#2="10.8.0.0 255.0.0.0"
  route#3="10.9.0.0 255.0.0.0"
  inacl#4="permit tcp any any"
 service = ppp protocol = ipx
! Put access lists, static routes, and other requirements that are
! needed here. Read the software specifications for details. If you leave
! this blank, the user will have no access lists (not even the ones that were
! installed prior to the creation of this user profile)!
```

（注） TACACS+ユーザプロファイルのタイムアウト設定は、RADIUSユーザプロファイルの設定とは異なります。RADIUSプロファイルでは、autocommandの**access-profile**とともに1つのセッションタイムアウトだけが設定されています。このタイムアウトはEXECセッションおよびPPPセッションに適用されます。TACACS+ユーザプロファイルでは、タイムアウトはサービスタイプ「exec」および「ppp」（LCP）下で設定し、EXECセッションとPPPセッションにそれぞれ適用する必要があります。タイムアウトをサービスタイプ「ppp」下でのみ設定すると、そのタイムアウト値はEXEC認可で使用できず、EXECセッションに適用されません。

その他の参考資料

関連資料

関連項目	マニュアルタイトル
Cisco IOSコマンド	『Master Command List, All Releases』
セキュリティコマンド	• 『Security Command Reference: Commands A to C』 • 『Security Command Reference: Commands D to L』 • 『Security Command Reference: Commands M to R』 • 『Security Command Reference: Commands S to Z』

シスコのテクニカル サポート

説明	リンク
右の URL にアクセスして、シスコのテクニカル サポートを最大限に活用してください。これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

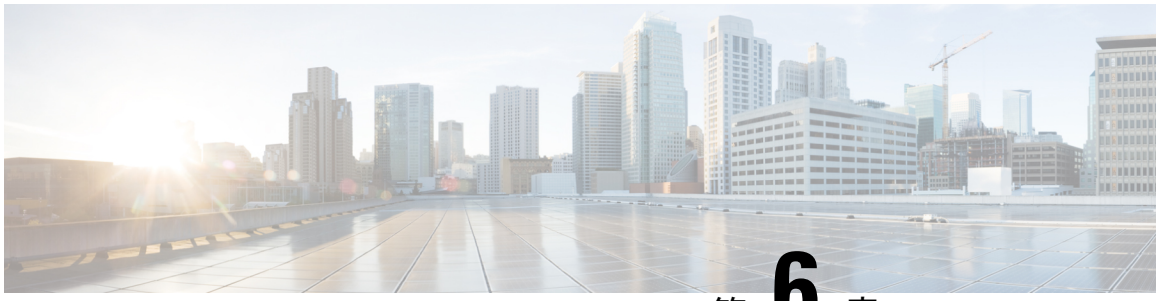
AAA Double Authentication Secured by AbsoluteTimeout の機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *18 : AAA Double Authentication Secured by AbsoluteTimeout* の機能情報

機能名	リリース	機能情報
AAA Double Authentication Secured by Absolute Timeout		AAA Double Authentication Secured by Absolute Timeout 機能により、ユーザ単位のセッション タイムアウトを使用して保護することで、二重の認証メカニズムが確保されます。この機能では、サービス プロバイダーによるネットワークへの接続を認可された接続のみに最適化し、不要なセッションが接続されないようにすることで、ネットワークへのアクセス全体のセキュリティを高めます。



第 6 章

AAA RADIUS レコードのスロットリング

Throttling of AAA (RADIUS) Records 機能は、RADIUS サーバに送信されるアクセス（認証および認可）およびアカウンティング レコードのスロットリングをサポートします。この機能により、ユーザーはルータからRADIUSサーバーに対して生成されるレコードの突然のバーストへの対応に十分な帯域幅がない場合などに、適切なスロットリングレートを設定して、ネットワークの輻輳や不安定さを防ぐことができます。

AAA RADIUS レコードのスロットリングに関する情報

AAA RADIUS レコードのスロットリング機能の利点

RADIUSクライアントとして機能するネットワーク アクセス サーバ（NAS）は、アカウンティングまたはアクセス要求のバーストを生成し、重大なネットワーク輻輳を生じさせたり、RADIUS サーバに RADIUS トラフィックのバーストによる過負荷を生じさせる場合があります。複数の NAS で RADIUS サーバとのやり取りがあると、この問題が悪化する可能性があります。

次の条件は、RADIUS トラフィックの突然のバーストをトリガーします。

- すべての加入者セッションを順にダウン状態にし、各加入者へのアカウンティング要求を生成するインターフェイス フラップ。
- 前項で説明されているシナリオなど、スイッチオーバーで停止しなかったすべてのセッションに開始レコードを生成するハイアベイラビリティ（HA）プログラム。

帯域幅が不十分であったり、RADIUS サーバの応答が遅い場合に、多数の要求が生成されると、ネットワークが不安定になる場合があります。ユーザ データグラム プロトコル（UDP）トランスポート層およびRADIUSプロトコルには、フロー制御メカニズムがありません。この

機能で提供されるスロットリング メカニズムは、これらの問題へのソリューションを提供します。

スロットリング アクセス要求とアカウンティング レコード

Throttling of AAA (RADIUS) Records 機能には、NAS レベルでパケットを制御するメカニズム（フロー制御）が導入されています。これにより、RADIUS サーバのパフォーマンスが向上しました。

特定の用途があるため、アクセス要求とアカウンティング レコードは別々に処理する必要があります。アクセス要求パケットは時間依存ですが、アカウンティング レコード パケットは時間依存ではありません。

- アクセス要求への応答が適切なタイミングでクライアントに返されない場合、プロトコルまたはユーザはタイムアウトし、デバイスの伝送レートが影響を受けます。
- アカウンティング レコード パケットは、リアルタイム クリティカルではありません。

同じサーバでしきい値を設定する場合、時間依存のアクセス要求パケットを扱うしきい値を優先し、アカウンティング レコード パケットにはより低次のしきい値を配置することが重要です。

インターネット サービス プロバイダー（ISP）がアクセス要求とアカウンティング レコードに個別の RADIUS サーバを使用していて、アカウンティング レコードのスロットリングのみが必要な場合もあります。

変更点

- Throttling of AAA (RADIUS) Records は、デフォルトではディセーブルです。
- スロットリング機能は、グローバルにまたはサーバ グループ レベルで設定できます。

AAA RADIUS レコードのスロットリングの設定方法

ここでは、グローバルおよびサーバ グループの両方の RADIUS サーバに送信されるアクセス（認証および認可）およびアカウンティング レコードのスロットリングを設定する方法について説明します。

server-group コンフィギュレーションは、特定のサーバ グループのスロットリングのイネーブル化またはディセーブル化、およびそのサーバ グループのしきい値の指定に使用されます。

（注） server-group コンフィギュレーションは、設定された任意のグローバル コンフィギュレーションを上書きします。

アカウンティングおよびアクセス要求パケットのグローバルなスロットリング

アカウンティングおよびアクセス要求パケットのグローバルなスロットリングを設定するには、次のタスクを実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **radius-server throttle { accounting** *threshold*] [**access** *threshold* [**access-timeout** *number-of-timeouts*]]}
4. **exit**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**radius-server throttle { accounting** *threshold*] [**access** *threshold* [**access-timeout** *number-of-timeouts*]]} 例： `Router(config)# radius-server throttle accounting 100 access 200 access-timeout 2`	アカウンティングおよびアクセス要求パケットにグローバルなスロットリングを設定します。 この例では次のようになります。 • アカウンティングのしきい値（範囲は 0 ～ 65536）を 100 に、アクセスのしきい値を 200 に設定します。 （注） デフォルトのしきい値は 0 です（スロットリングはディセーブル）。 • トランザクションごとのタイムアウト回数の値（範囲は 1 ～ 10）を 2 に設定します。
ステップ 4	**exit** 例： `Router(config)# exit`	グローバル コンフィギュレーション モードを終了します。

サーバグループごとのアカウンティングおよびアクセス要求パケットのスロットリング

次の server-group コンフィギュレーションは、指定されたサーバ グループのイネーブル化またはディセーブル化、およびそのサーバ グループへのしきい値の指定に使用できます。

server-group アカウンティングおよびアクセス要求パケットのスロットリングを設定するには、次のタスクを実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **aaa group server radius** *server-group-name*
4. **throttle** {[**accounting** *threshold*] [**access** *threshold* [**access-timeout** *number-of-timeouts*]]}
5. **exit**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**aaa group server radius** *server-group-name* 例： `Device(config)# aaa group server radius myservergroup`	server-group コンフィギュレーション モードを開始します。
ステップ 4	**throttle** {[**accounting** *threshold*] [**access** *threshold* [**access-timeout** *number-of-timeouts*]]} 例： `Device(config-sg-radius)# throttle accounting 100 access 200 access-timeout 2`	アカウンティングおよびアクセス要求パケットに指定された server-group のスロットリング値を設定します。 この例では次のようになります。 • アカウンティングのしきい値（範囲は 0 ～ 65536）を 100 に、アクセスのしきい値を 200 に設定します。 （注） デフォルトのしきい値は 0 です（スロットリングはディセーブル）。

	コマンドまたはアクション	目的
		• トランザクションごとのタイムアウト回数の値（範囲は 1 ～ 10）を 2 に設定します。
ステップ 5	**exit** 例： `Device(config-sg-radius)# exit`	server-group コンフィギュレーション モードを終了します。

AAA RADIUS レコードのスロットリングの設定例

アカウンティングおよびアクセス要求パケットのグローバルなスロットリングの例

次に、サーバに送信するアカウンティング要求の回数を100に制限する方法の例を示します。

```
enable
configure terminal
radius-server throttle accounting 100
```

次に、サーバに送信するアクセス要求パケットの回数を200に制限し、トランザクションごとに許可されるタイムアウトの回数を 2 に設定する方法の例を示します。

```
enable
configure terminal
radius-server throttle access 200
radius-server throttle access 200 access-timeout 2
```

次に、アカウンティングおよびアクセス要求パケットの両方のスロットリングを設定する例を示します。

```
enable
configure terminal
radius-server throttle accounting 100 access 200
```

サーバグループごとのアカウンティングおよびアクセス要求パケットのスロットリングの例

次に、server-group-A に送信するアカウンティング要求の回数を 100 に制限する方法の例を示します。

```
enable
configure terminal
aaa group server radius server-group-A
throttle accounting 100
```

次に、server-group-A に送信するアクセス要求パケットの回数を 200 に制限し、トランザクションごとに許可されるタイムアウトの回数を 2 に設定する方法の例を示します。

```
enable
configure terminal
aaa group server radius server-group-A
throttle access 200 access-timeout 2
```

次に、server-group-A のアカウンティングおよびアクセス要求パケットの両方のスロットリングを設定する例を示します。

```
enable
configure terminal
aaa group server radius server-group-A
throttle accounting 100 access 200
```

その他の参考資料

ここでは、Throttling of AAA (RADIUS) Records 機能に関する参考資料について説明します。

関連資料

関連項目	マニュアル タイトル
セキュリティ機能	『*Cisco IOS XE Security Configuration Guide: Securing User Services*, Release 2』
セキュリティ コマンド	『*Cisco IOS Security Command Reference*』

標準

標準	タイトル
この機能でサポートされる新規の標準または変更された標準はありません。また、既存の標準のサポートは変更されていません。	--

MIB

MIB	MIB のリンク
この機能によってサポートされる新しい MIB または変更された MIB はありません。またこの機能による既存 MIB のサポートに変更はありません。	選択したプラットフォーム、Cisco IOS XE ソフトウェア リリース、およびフィーチャ セットの MIB の場所を検索しダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

RFC

RFC	タイトル
この機能によりサポートされた新規 RFC または改訂 RFC はありません。またこの機能による既存 RFC のサポートに変更はありません。	--

シスコのテクニカル サポート

説明	リンク
シスコのサポート Web サイトでは、シスコの製品やテクノロジーに関するトラブルシューティングにお役立ていただけるように、マニュアルやツールをはじめとする豊富なオンライン リソースを提供しています。 お使いの製品のセキュリティ情報や技術情報を入手するために、Cisco Notification Service（Field Notice からアクセス）、Cisco Technical Services Newsletter、Really Simple Syndication（RSS）フィードなどの各種サービスに加入できます。 シスコのサポート Web サイトのツールにアクセスする際は、Cisco.com のユーザ ID およびパスワードが必要です。	http://www.cisco.com/en/US/support/index.html

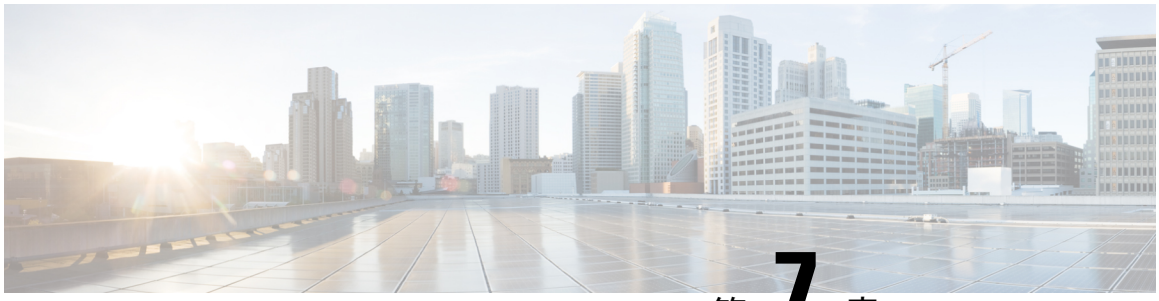
AAA RADIUS レコードのスロットリングの機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *19 : AAA*（*RADIUS*）レコードのスロットリングの機能情報

機能名	リリース	機能情報
AAA（RADIUS）レコードのスロットリング	Cisco IOS XE Release 2.1	Throttling of AAA (RADIUS) Records 機能は、RADIUS サーバに送信されるアクセス（認証および認可）およびアカウンティング レコードのスロットリングをサポートします。この機能により、ユーザは Cisco IOS XE ルータから RADIUS サーバに対して生成されるレコードの突然のバーストへの対応に十分な帯域幅がない場合などに、適切なスロットリング レートを設定して、ネットワークの輻輳や不安定さを防ぐことができます。 この機能は、Cisco IOS XE Release 2.1 で、Cisco ASR 1000 シリーズアグリゲーションサービスルータに導入されました。 この機能により、次のコマンドが導入または変更されました。**radius-server throttle, throttle**



第 7 章

RADIUS パケット オブ ディスコネクト

RADIUS パケット オブ ディスコネクト機能は、接続された音声コールを終了させるために使用します。

RADIUS パケット オブ ディスコネクトの前提条件

『*Cisco IOS XE Security Configuration Guide: Securing User Services* , Release 2』で説明されているように、AAA を設定します。

RADIUS パケット オブ ディスコネクトの制約事項

以下により、適切に一致する識別情報の通知が行われる必要があります。

- 課金サーバとゲートウェイの設定
- ゲートウェイのオリジナル アカウンティング開始要求
- サーバの POD 要求

RADIUS パケット オブ ディスコネクトに関する情報

パケット オブ ディスコネクト（PoD）は RADIUS access_request パケットであり、RADIUS access_accept パケットによりセッションが承認された後、認証するエージェント サーバがユーザを接続解除するときに使用されるようになっています。

POD が必要な場合

POD が必要な場合としては、少なくとも次の 2 つの状況が考えられます。

- 不正使用の検出。これは、コールを承認後でなければ実行できません。価格構造が複雑でコールを受け入れる前に最大セッション期間を推定できない。ある種のディスカウントが適用されるか、複数のユーザが同じサブスクリプションを同時に使用している場合が、これに当てはまります。
- 認可されていないサーバからユーザが切断されるのを防ぐには、POD パケットを発行する認可エージェントが パケット オブ ディスコネクト要求に 3 つのパラメータを含める必要があります。接続解除されるコールに対して、すべてのパラメータは、ゲートウェイの期待値と一致している必要があります。パラメータが一致しないと、ゲートウェイはパケットオブディスコネクトのパケットを破棄し、エージェントに NACK（否定応答）メッセージを送信します。

POD パラメータ

POD には次のパラメータがあります。

- このコールに対してゲートウェイから受信されたものと同じ内容の h323-conf-id ベンダー固有属性（VSA）
- 対象の区間に対してゲートウェイから受信されたものと同じ内容の h323-call-origin VSA。
- POD 要求の *authentication* フィールドで伝送される 16 バイトの MD5 ハッシュ値。
- Cisco IOS XE ソフトウェアは、RFC 3576 の『*Dynamic Authorization Extensions to RADIUS*』（POD を介してサポートされるディスコネクト メッセージ（DM）および認可変更（CoA）の両方を公式にサポートするために RADIUS 標準を拡張）に基づいて POD コード 50 を音声 POD 要求のコード値として割り当てます。

RFC 3576 では、以下の POD コードを指定します。

-
  - 40：切断要求
  - 41：切断 ACK
  - 42：切断 NAK
  - 43：CoA 要求
  - 44：CoA-ACK
  - 45：CoA-NAK

RADIUS パケット オブ ディスコネクトの設定方法

RADIUS POD の設定

次のタスクを使用して、RADIUS POD を設定します。

手順の概要

1. **enable**
2. **configure terminal**
3. Router (config)# **aaa pod server** [**port** *port-number*] [**auth-type** {**any**| **all**| **session-key**}] **server-key** [*encryption-type*] *string*
4. Router# **end**
5. Router# **show running-configuration**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	Router (config)# **aaa pod server** [**port** *port-number*] [**auth-type** {**any**| **all**| **session-key**}] **server-key** [*encryption-type*] *string* 例： `Router(config)# aaa pod server server-key xyz123`	次のような特定のセッション属性が提供されると、インバウンド ユーザ セッションを切断できます。 • **port** *port-number*：（任意）POD 要求に使用されるネットワーク アクセス サーバーのユーザー データグラム プロトコル（UDP）ポート。デフォルト値は 1700 です。 • **auth-type**：（任意）セッションの切断に必要な認証の種類。 • **any**：POD パケット内で送信されたすべての属性と一致するセッションが切断されます。POD パケットには、4 つのキー属性（user-name、framed-IP-address、session-ID、session-key）の 1 つまたは複数が含まれることがあります。

	コマンドまたはアクション	目的
		• **all**：4つの主要属性のすべてに一致するセッションだけが切断されます。 **All** がデフォルトです。 • **session-key**：一致する session-key 属性を持つセッションが切断されます。他のすべての属性は無視されます。 • **server-key--** 共有秘密テキスト文字列を設定します。 • *encryption-type*：（任意）直後のテキストが暗号化されるかどうか、および暗号化される場合は使用される暗号化タイプを定義する 1 桁の数字。定義されている暗号化タイプは、0（直後のテキストは暗号化されない）および 7（テキストはシスコが定義した暗号化アルゴリズムを使用して暗号化される）です。 • *string*：ネットワーク アクセス サーバーとクライアント ワークステーションの間で共有される共有秘密テキスト文字列。この事前共有キーは、両方のシステムで同じである必要があります。
ステップ 4	Router# **end**	グローバル コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

ステップ 5	Router# **show running-configuration**
	例：
	`Router# show running-configuration`
	例：
	`!`
	例：
	`aaa authentication login h323 group radius`
	例：
	`aaa authorization exec h323 group radius`
	例：
	`aaa accounting update newinfo`
	例：
		ゲートウェイが特権 EXEC モードで正しく設定されていることを確認します。

	コマンドまたはアクション	目的

	`aaa accounting connection h323 start-stop group radius`
	例：
	`aaa pod server server-key cisco`
	例：
	`aaa session-id common`
	例：
	`!`	

トラブルシューティングのヒント

AAA Dead-Server Detection を設定したら、**show running-config** コマンドを使用して、その設定を確認してください。この確認が特に重要になるのは、**no** 形式の **radius-server dead-criteria** コマンドを使用している場合です。**show running-config** コマンドの出力は、**radius-server dead-criteria** コマンドを使用して設定した「Dead Criteria Details」フィールドと同じ値を示している必要があります。

RADIUS POD の設定の確認

RADIUS POD 設定を確認するには、次の例に示すように **show running configuration** 特権 EXEC コマンドを使用します。

```
Router# show running-configuration
!
aaa authentication login h323 group radius
aaa authorization exec h323 group radius
aaa accounting update newinfo
aaa accounting connection h323 start-stop group radius
aaa pod server server-key cisco
aaa session-id common
.
.
.
```

その他の参考資料

次の項で、RADIUS パケット オブ ディスコネクト機能に関する参考資料を紹介します。

関連資料

関連項目	マニュアル タイトル
AAA	『*Cisco IOS XE Security Configuration Guide, Securing User Services*, Release 2』の「Authentication, Authorization, and Accounting (AAA)」
セキュリティ コマンド	『*Cisco IOS Security Command Reference*』
CLI 設定	『*Cisco IOS XE Configuration Fundamentals Configuration Guide*, Release 2』

標準

標準	タイトル
この機能でサポートされる新規の標準または変更された標準はありません。また、既存の標準のサポートは変更されていません。	--

MIB

MIB	MIB のリンク
この機能によってサポートされる新しい MIB または変更された MIB はありません。またこの機能による既存 MIB のサポートに変更はありません。	選択したプラットフォーム、Cisco IOS XE ソフトウェア リリース、およびフィーチャ セットの MIB の場所を検索しダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

RFC

RFC	タイトル
RFC 2865	『*Remote Authentication Dial-in User Service*』
RFC 3576	『*Dynamic Authorization Extensions to RADIUS*』

シスコのテクニカル サポート

説明	リンク
シスコのサポート Web サイトでは、シスコの製品やテクノロジーに関するトラブルシューティングにお役立ていただけるように、マニュアルやツールをはじめとする豊富なオンライン リソースを提供しています。 お使いの製品のセキュリティ情報や技術情報を入手するために、Cisco Notification Service（Field Notice からアクセス）、Cisco Technical Services Newsletter、Really Simple Syndication（RSS）フィードなどの各種サービスに加入できます。 シスコのサポート Web サイトのツールにアクセスする際は、Cisco.com のユーザ ID およびパスワードが必要です。	http://www.cisco.com/en/US/support/index.html

RADIUS パケット オブ ディスコネクトの機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *20 : RADIUS* パケット オブ ディスコネクトの機能情報

機能名	リリース	機能情報
RADIUS パケット オブ ディスコネクト	Cisco IOS XE Release 2.1	RADIUS パケット オブ ディスコネクト機能は、接続された音声コールを終了させるために使用します。 この機能は、Cisco IOS XE Release 2.1 で Cisco ASR 1000 シリーズ アグリゲーション サービス ルータに導入されました。 次のコマンドが導入または変更されました。**aaa pod server, debug aaa pod**

用語集

AAA：認証、許可、およびアカウンティングセキュリティ サービスのフレームワークであり、ユーザーの身元確認（認証）、リモート アクセス コントロール（許可）、課金、監査、およびレポートに使用するセキュリティ サーバー情報の収集と送信（アカウンティング）の方式を定めています。

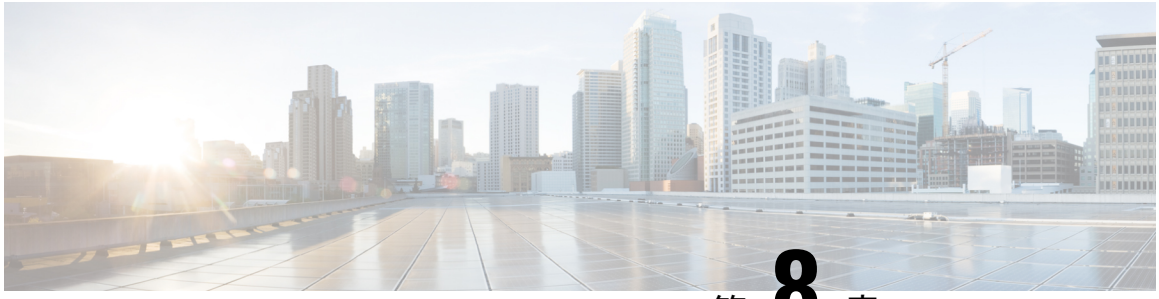
L2TP ：レイヤ 2 トンネル プロトコル。レイヤ 2 トンネル プロトコルを使用すると、ISP などのアクセス サービスが仮想トンネルを作成し、顧客のリモート サイトやリモート ユーザを企業のホーム ネットワークにリンクさせることができます。具体的には、ISP アクセス ポイント（POP）にあるネットワーク アクセス サーバ（NAS）がリモート ユーザと PPP メッセージを交換し、L2F または L2TP の要求や応答を使用して顧客のトンネル サーバと通信し、トンネルのセットアップを行います。

PE：Provider Edge（プロバイダーエッジ）。サービス プロバイダー ネットワークのエッジ上のネットワーキング デバイス。

RADIUS ：リモート認証ダイヤルイン ユーザー サービス。RADIUS は、不正なアクセスからネットワークのセキュリティを保護する分散クライアント/サーバ システムです。シスコの実装では RADIUS クライアントは Cisco ルータ上で稼働します。認証要求は、すべてのユーザ認証情報とネットワーク サービス アクセス情報が格納されている中央の RADIUS サーバに送信されます。

VPN：Virtual Private Network（仮想プライベートネットワーク）。リモートでダイヤルイン ネットワークをホーム ネットワークに存在させ、あたかも直接接続されているかのように見せるシステム。VPN は、L2TP および L2F を使用し、LAC ではなく、LNS でレイヤ 2 およびより高次のネットワーク接続を終了させます。

VRF：Virtual Route Forwarding（仮想ルーティングおよびフォワーディング）。最初は、ルータにグローバルのデフォルト ルーティング/フォワーディング テーブルは 1 つしかありません。VRF は、複数の分離されたルーティング/フォワーディング テーブルとして表示でき、ユーザのルートには別のユーザのルートとの相互関係はありません。



第 8 章

AAA 認可および AAA 認証のキャッシュ

AAA 認可キャッシュ機能および AAA 認証のキャッシュ機能を使用すると、設定した一連のユーザ プロファイルまたはサービス プロファイルの認可応答と認証応答をキャッシュに格納することができます。このため、認可応答および認証応答から返されるユーザ プロファイルとサービス プロファイルを複数のソースから照会できるようになり、オフロード サーバだけに依存する必要がなくなるので、パフォーマンスとネットワークの信頼性レベルが向上します。また、この機能のフェールオーバー メカニズムにより、ネットワークの RADIUS サーバまたは TACACS+ サーバが認可応答や認証応答を返せなくなっても、ネットワークのユーザや管理者は引き続きネットワークにアクセスできます。

認可プロファイルおよび認証プロファイルのキャッシュ機能の実装の前提条件

認可プロファイルおよび認証プロファイルのキャッシュ機能の実装には、次の前提条件が適用されます。

- プロファイル キャッシュ機能の実装方法を理解している必要があります。つまり、ネットワークのパフォーマンスを向上させたり、ネットワークの認証（RADIUS）サーバや認可（TACACS+）サーバが使用できなくなった場合にフェールオーバーを実行したりするためにプロファイルがどのようにキャッシュされるかを理解している必要があります。
- RADIUS サーバ グループと TACACS+ サーバ グループがすでに設定されている必要があります。

認可プロファイルおよび認証プロファイルのキャッシュ機能の実装について

認可プロファイルおよび認証プロファイルのキャッシュ機能によるネットワーク パフォーマンスの最適化

RADIUS クライアントおよび TACACS+ クライアントは Cisco ルータ上で稼働し、ユーザ認証およびネットワーク サービス アクセスに関するすべての情報を保持する中央の RADIUS サーバまたは TACACS+ サーバへ認証要求を送信します。ルータはオフロードの RADIUS サーバまたは TACACS+ サーバと通信してコールを認証した後、ポリシーまたはサービスをそのコールに適用する必要があります。認証、許可、アカウンティング（AAA）アカウンティングと異なり、AAA 認証および AAA 認可はブロッキング手順です。つまり、コールの認証中および認可中は、コールセットアップは進行しません。したがって、そのような認証要求または認可要求が、ルータから RADIUS オフロード サーバまたは TACACS+ サーバに渡されて処理される時間と、そのサーバからルータに渡されて処理される時間は、コールセットアップの処理に必要な時間に直に影響します。転送中の通信の問題、オフロードサーバの利用率、その他のさまざまな要因が、コール セットアップのパフォーマンスを大幅に低下させるのは、AAA 認証および AAA 認可の手順に原因があります。この問題がさらに顕著になるのは、複数の AAA 認証および AAA 認可が 1 つのコールまたはセッションに必要になるときです。

この問題の解決策は、そのような認証要求の影響を最小限にすることです。そのために、ルータで特定のユーザの認証応答および認可応答をキャッシュに格納して、要求をオフロードサーバに何度も送信する必要をなくします。このプロファイルキャッシュ機能により、コールセットアップ時間が大幅に短縮されます。また、プロファイルキャッシュ機能によってネットワークの信頼性レベルが上がります。これは、認証応答および認可応答から返されるユーザ プロファイルやサービスプロファイルを複数のソースから照会できるようになり、オフロードサーバだけに依存する必要がなくなるためです。

このようにパフォーマンスを最適化するためには、ユーザがルータから認証されるときに AAA キャッシュ プロファイルが最初に照会されるように認証方式リストを設定する必要があります。詳細については、「認可プロファイルおよび認証プロファイルのキャッシュ機能の方式リスト」を参照してください。

フェールオーバーメカニズムとしての認可プロファイルおよび認証プロファイルのキャッシュ機能

何らかの理由で、RADIUS サーバまたは TACACS+ サーバが認証応答および認可応答を返せない場合、ネットワークのユーザおよび管理者はネットワークから締め出されることがあります。プロファイルのキャッシング機能により、認証フェーズを完了しなくてもユーザ名の承認が可能になります。たとえば、ユーザ名が user100@example.com でパスワードが secretpassword1 のユーザは、正規表現「.*@example.com」を使用してプロファイル キャッシュに格納されま

す。ユーザ名が user101@example.com で、パスワードが secretpassword2 である別のユーザもまた、同じ正規表現を使用して格納できます。「.*@example.com」プロファイルのユーザの数が何千にもなる可能性があるため、個人のパスワードを使用して各ユーザの認証を行うのは現実的ではありません。このため、認証はディセーブル化され、各ユーザは単にキャッシュに格納されている共通のアクセス応答の認証プロファイルにアクセスします。

Challenge Handshake Authentication Protocol（CHAP）、Microsoft チャレンジ ハンドシェイク認証プロトコル（MS-CHAP）、または拡張認証プロトコル（EAP）などの、クライアントと AAA オフロード サーバの間で暗号化されたパスワードを使用する高度なセキュリティ メカニズムを使用する場合に、同じ理論が当てはまります。認証プロファイルを処理するために、これらの一意で、安全なユーザ名とパスワードのプロファイルを許可するには、認証をバイパスします。

このフェールオーバー機能を利用するためには、ユーザがルータから認証されるときにキャッシュ サーバ グループが最後に照会されるように認証および認可の方式リストを設定する必要があります。詳細については、「認可プロファイルおよび認証プロファイルのキャッシュ機能の方式リスト」を参照してください。

認可プロファイルおよび認証プロファイルのキャッシュ機能の方式リスト

方式リストとは、ユーザ認証のために照会される認証方式を記載したシーケンシャル リストです。サポートされているのは、ローカル（ローカルのデータベースを使用）、なし（なにも実行しない）、RADIUS サーバーグループ、または TACACS+ サーバーグループなどの方式です。通常は、複数の方式を方式リストに設定できます。ソフトウェアは、ユーザーを認証するため、リストに記載されている最初の方式が使用されます。その方式で応答に失敗した場合、ソフトウェアは、方式リストに記載されている次の認証方式を選択します。この処理は、リストのいずれかの認証方式で正常に通信できるか、方式リストで定義されているすべての方式を試行するまで続行されます。

ネットワークのパフォーマンスを最適化したり、プロファイル キャッシング機能を使用してフェールオーバー機能を有効にするには、方式リストの認証および認可の方式の順序を変更します。ネットワーク パフォーマンスを最適化するためには、キャッシュ サーバ グループが方式リストで最初に検出されるようにします。フェールオーバー機能を有効にするためには、キャッシュ サーバ グループが方式リストで最後に検出されるようにします。

認可プロファイルおよび認証プロファイルのキャッシュ機能に関するガイドライン

特定のアクセス ポイント（POP）の特定のルータで、認証および認可を要求できるユーザ名とプロファイルの数は相当な数になることがあるため、ユーザ名とプロファイルをすべてキャッシュするのは現実的ではありません。このため、ユーザ名およびプロファイルのうち、一般的に使用されるものや、一般的な認証応答や認可応答を共有するものだけをキャッシングに使用するように設定する必要があります。ドメインベースのサービスプロファイルに加え、America Online（AOL）のコールに使用される aolip や aolnet などの一般的に使用されるユーザ名や、公

衆電話交換網（PSTN）のコールを、ネットワークに接続されたストレージ デバイスに接続するのに使用される事前認証の着信番号識別サービス（DNIS）番号はいずれも、認証および認可のキャッシュ機能の効果が現れるユーザ名とプロファイルの例です。

認可プロファイルおよび認証プロファイルのキャッシュ機能を実装するための一般的な設定手順

認可プロファイルおよび認証プロファイルのキャッシュ機能を実装するには、次の手順を行います。

1. キャッシュ プロファイル グループを作成し、各グループのキャッシュに格納する情報についてのルールを定義します。

ユーザ名に正確に一致するエントリ、正規表現に一致するエントリ、またはすべての認証要求および認可要求をキャッシュに格納することを指定します。

1. 新しく定義したキャッシュ グループを参照するようにサーバ グループを更新します。
2. キャッシュに格納された情報を使用してネットワークのパフォーマンスを最適化したり、フェールオーバー メカニズムを有効にしたりするように認証または認可の方式リストを更新します。

認可プロファイルおよび認証プロファイルのキャッシュ機能の実装方法

キャッシュ プロファイル グループの作成とキャッシュ処理ルールの定義

次の作業を行って、キャッシュ プロファイル グループを作成し、そのグループのキャッシュに格納する情報についてのルールを定義して、キャッシュ プロファイルのエントリの確認と管理を行います。

手順の概要

1. **enable**
2. **configure terminal**
3. **aaa new-model**
4. **aaa cache profile** *group-name*
5. **profile** *name* [**no-auth**]
6. 手順 4 のプロファイル グループに追加する各ユーザ名に対して手順 5 を繰り返します。
7. **regexp** *matchexpression* {**any**| **only**}[**no-auth**]

8. 手順4で定義されたキャッシュ プロファイル グループに追加する各正規表現に対して手順 7 を繰り返します。
9. **all** [**no-auth**]
10. **end**
11. **show aaa cache group** *name*
12. **clear aaa cache group** *name* {**profile** *name*| **all**}
13. **debug aaa cache group**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**aaa new-model** 例： `Router(config)# aaa new-model`	AAAアクセス コントロール モデルをイネーブルにします。
ステップ 4	**aaa cache profile** *group-name* 例： `Router(config)# aaa cache profile networkusers@companyname`	認証および認可のキャッシュ プロファイル サーバ グループを定義し、プロファイル マップ コンフィギュレーション モードを開始します。
ステップ 5	**profile** *name* [**no-auth**] 例： `Router(config-profile-map# profile networkuser1 no-auth`	ユーザ名の一致に基づいて個々の認証および認可プロファイルのキャッシュを作成します。 • *name* 引数は、認証または認可のサービス要求によって照会されるユーザ名と正確に一致する必要があります。 • **no-auth** キーワードを使用して、このユーザーの認証をバイパスします。
ステップ 6	手順 4 のプロファイル グループに追加する各ユーザ名に対して手順 5 を繰り返します。	--
ステップ 7	**regexp** *matchexpression* {**any**| **only**}[**no-auth**] 例：	（任意）正規表現に基づいて、一致するエントリをキャッシュ プロファイル グループに作成します。

	コマンドまたはアクション	目的
	`Router(config-profile-map)# regexp .*@example.com any no-auth`	• **any** キーワードを使用すると、正規表現に一致する一意のユーザー名がすべて保存されます。 • **only** キーワードを使用すると、正規表現に一致するすべてのユーザー名に対して1つのプロファイルエントリのみがキャッシュされます。 • **no-auth** キーワードを使用して、このユーザーまたは一連のユーザーの認証をバイパスします。 • 正規表現のプロファイル グループ内のエントリの数が何千にもなる可能性があるため、そして各要求の検証を正規表現に対して行うと時間がかかる場合があるため、キャッシュプロファイル グループで正規表現を使用することは推奨されません。
ステップ 8	手順 4 で定義されたキャッシュ プロファイル グループに追加する各正規表現に対して手順 7 を繰り返します。	--
ステップ 9	**all** [**no-auth**] **例**： `Router(config-profile-map)# all no-auth`	（任意）認証要求および認可要求をすべてキャッシュに格納することを指定します。 • **all** コマンドは、特定のサービス認可要求に対して使用しますが、認証要求を処理するときは使用しないでください。
ステップ 10	**end** **例**： `Router(config-profile-map)# end`	特権 EXEC モードに戻ります。
ステップ 11	**show aaa cache group** *name* **例**： `Router# show aaa cache group networkusers@companyname`	（任意）指定したグループのすべてのキャッシュ エントリを表示します。
ステップ 12	**clear aaa cache group** *name* {**profile** *name*| **all**} **例**： `Router# clear aaa cache group networkusers@companyname profile networkuser1`	（任意）キャッシュの1つまたはすべてのエントリをクリアします。

	コマンドまたはアクション	目的
ステップ 13	**debug aaa cache group** 例： `Router# debug aaa cache group`	（任意）キャッシュに格納されているエントリのデバッグ情報を表示します。

キャッシュ プロファイル グループ情報を使用する RADIUS および TACACS サーバ グループの定義

このタスクを実行して、RADIUS および TACACS+ サーバ グループが各キャッシュ プロファイル グループに保存されている情報をどのように使用するかを定義します。

始める前に

RADIUS サーバ グループと TACACS+ サーバ グループが作成されている必要があります。

手順の概要

1. **enable**
2. **configure terminal**
3. **aaa new-model**
4. **aaa group server radius** *group-name* or**aaa group server tacacs+** *group-name*
5. **cache authorization profile** *name*
6. **cache authentication profile** *name*
7. **cache expiry** *hours* {**enforce failover**}
8. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**aaa new-model** 例： `Router(config)# aaa new-model`	AAA アクセス コントロール モデルをイネーブルにします。

	コマンドまたはアクション	目的
ステップ 4	**aaa group server radius** *group-name* or**aaa group server tacacs+** *group-name* 例： `Router(config)# aaa group server radius networkusers@companyname`	RADIUS サーバ グループ コンフィギュレーション モードを開始します。 • TACACS+ サーバー グループ コンフィギュレーション モードを開始するには、**aaa group server tacacs+** *group-name* コマンドを使用します。
ステップ 5	**cache authorization profile** *name* 例： `Router(config-sg-radius)# cache authorization profile networkusers@companyname`	この RADIUS または TACACS+ サーバ グループのプロファイルのネットワーク ユーザで認可のキャッシュ処理ルールをアクティブにします。 • このコマンドの *name* 引数は、AAA キャッシュ プロファイル グループ名です。
ステップ 6	**cache authentication profile** *name* 例： `Router(config-sq-radius)# cache authentication profile networkusers@companyname`	この RADIUS または TACACS+ サーバ グループのプロファイルのネットワーク ユーザで認証のキャッシュ処理ルールをアクティブにします。
ステップ 7	**cache expiry** *hours* {**enforce failover**} 例： `Router(config-sq-radius)# cache expiry 240 failover`	（オプション）キャッシュ プロファイルのエントリが期限切れになる（古くなる）までの時間を設定します。 • **enforce** キーワードは、期限切れになったキャッシュプロファイルのエントリを再使用しないことを指定するときに使用します。 • **failover** キーワードは、他のすべての方式でユーザーを認証および認可できなかった場合にキャッシュプロファイルの期限切れのエントリを使用することを指定するときに使用します。
ステップ 8	**end** 例： `Router(config-sg-radius)# end`	特権 EXEC モードに戻ります。

キャッシュ情報の使用方法を指定するための認可および認証の方式リストの更新

次の作業を行って、認可および認証のキャッシュ情報を使用するように認可および認証の方式リストを更新します。

始める前に

方式リストをすでに定義している必要があります。

手順の概要

1. **enable**
2. **configure terminal**
3. **aaa new-model**
4. **aaa authorization** {**network** | **exec** | **commands** *level* | **reverse-access**| **configuration**} {**default** | *list-name*} [*method1* [*method2...*]]
5. **aaa authentication ppp** {**default** | *list-name*} *method1* [*method2...*]
6. **aaa authentication login** {**default** | *list-name*} *method1* [*method2...*]
7. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**aaa new-model** 例： `Router(config)# aaa new-model`	AAA アクセス コントロール モデルをイネーブルにします。
ステップ 4	**aaa authorization** {**network**	**exec**	**commands** *level*	**reverse-access**| **configuration**} {**default**	*list-name*} [*method1* [*method2...*]] 例： `Router(config)# aaa authorization network default cache networkusers@companyname group networkusers@companyname`	AAA認可を有効にし、指定した機能にユーザがアクセスしたときに使用される認可方式を定義する方式リストを作成します。
ステップ 5	**aaa authentication ppp** {**default**	*list-name*} *method1* [*method2...*] 例： `Router(config)# aaa authentication ppp default cache networkusers@companyname group networkusers@companyname`	PPP が実行されているシリアルインターフェイスで使用する 1 つまたは複数の認証方式を指定します。

	コマンドまたはアクション	目的
ステップ 6	**aaa authentication login** {**default** | *list-name*} *method1* [*method2...*] 例： `Router(config)# aaa authentication login default cache adminusers group adminusers`	ログイン時の認証を設定します。
ステップ 7	**end** 例： `Router(config)# end`	特権 EXEC モードに戻ります。

認可プロファイルおよび認証プロファイルのキャッシュ機能を実装するための設定例

ネットワークを最適化するための認可プロファイルおよび認証プロファイルのキャッシュ機能の実装例

次の設定例について説明します。

- ネットワーク上のすべての管理者名を含むキャッシュ プロファイル グループ adminusers を定義し、すべてのログイン セッションと exec セッションに使用するデフォルトのリストとして設定します。
- RADIUS サーバ グループの新しいキャッシュ処理ルールをアクティブにします。
- 新しいキャッシュ プロファイル グループを認証および認可の方式リストに追加し、このキャッシュ プロファイル グループが最初に照会されるように方式の順序を変更します。

```
configure terminal

 aaa new-model

 ! Define aaa cache profile groups and the rules for what information is saved to cache.

 aaa cache profile admin_users

 profile adminuser1

 profile adminuser2

 profile adminuser3
```

```
 profile adminuser4

 profile adminuser5

 exit

 ! Define server groups that use the cache information in each profile group.

 aaa group server radius admins@companyname.com

 cache authorization profile admin_users

 cache authentication profile admin_users

 ! Update authentication and authorization method lists to specify how profile groups
and server groups are used.

 aaa authentication login default cache admins@companyname.com group admins@companyname.com

 aaa authorization exec default cache admins@companyname.com group admins@companyname.com

 end
```

フェールオーバーメカニズムとしての認可プロファイルおよび認証プロファイルのキャッシュ機能の実装例

次の設定例について説明します。

- RADIUS サーバまたは TACACS+ サーバが万一使用できなくなった場合でも、管理者が引き続きネットワークにアクセスできるように、ネットワーク上のすべての管理者を含むキャッシュ プロファイル グループ admin_users を作成します。
- RADIUS サーバまたは TACACS+ サーバが万一使用できなくなった場合でも、ABC という会社のユーザがネットワークの使用を認可されるように、ネットワーク上のこれらのユーザをすべて含むキャッシュ プロファイル グループ abc_users を作成します。
- RADIUS サーバの各プロファイル グループの新しいキャッシュ処理ルールをアクティブにします。
- 新しいキャッシュ プロファイル グループを認証および認可の方式リストに追加し、このキャッシュ プロファイル グループが最後に照会されるように方式の順序を変更します。

```
configure terminal

 aaa new-model

 ! Define aaa cache profile groups and the rules for what information is saved to cache.
```

```
aaa cache profile admin_users

profile admin1

profile admin2

profile admin3

exit

aaa cache profile abcusers

profile .*@example.com only no-auth

exit

! Define server groups that use the cache information in each cache profile group.

aaa group server tacacs+ admins@companyname.com

server 10.1.1.1

server 10.20.1.1

cache authentication profile admin_users

cache authorization profile admin_users

exit

aaa group server radius abcusers@example.com

server 172.16.1.1

server 172.20.1.1

cache authentication profile abcusers

cache authorization profile abcusers

exit

! Update authentication and authorization method lists to specify how cache is used.

aaa authentication login default cache admins@companyname.com group admins@companyname.com

aaa authorization exec default cache admins@companyname.com group admins@companyname.com
```

```
aaa authentication ppp default group abcusers@example.com cache abcusers@example.com
aaa authorization network default group abcusers@example.com cache abcusers@example.com
end
```

RADIUS 認可変更に関する追加情報

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『Cisco IOS Master Command List, All Releases』
セキュリティ コマンド	• 『Security Command Reference: Commands A to C』 • 『Security Command Reference: Commands D to L』 • 『Security Command Reference: Commands M to R』 • 『Security Command Reference: Commands S to Z』
AAA の設定	『*Authentication, Authorization, and Accounting Configuration Guide*』

標準および RFC

標準/RFC	タイトル
RFC 2903	「*Generic AAA Architecture*」
RFC 5176	「*Dynamic Authorization Extensions to Remote Authentication Dial In User Service (RADIUS)*」

シスコのテクニカル サポート

説明	リンク
右の URL にアクセスして、シスコのテクニカル サポートを最大限に活用してください。これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

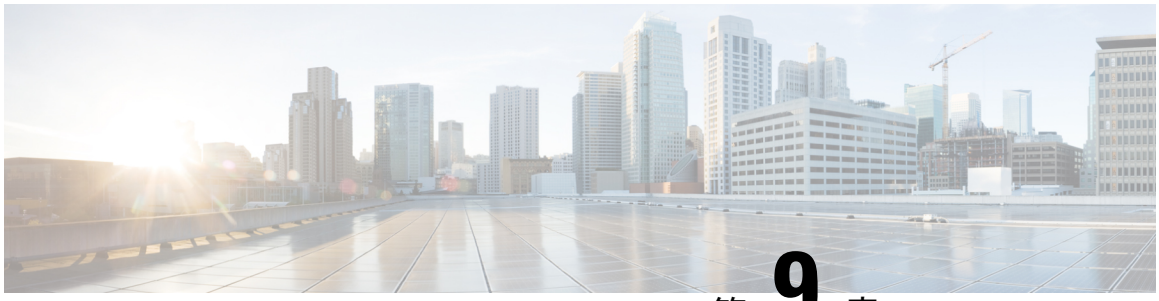
認可プロファイルおよび認証プロファイルのキャッシュ機能の実装の機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *21* : 認証プロファイルおよび認可プロファイルのキャッシュ機能の実装の機能情報

機能名	リリース	機能情報
AAA 認可および AAA 認証のキャッシュ	Cisco IOS XE Release 2.3	この機能により、ネットワークのパフォーマンスが最適化されるほか、RADIUS サーバまたは TACACS+ サーバが何らかの理由で使用できなくなった場合のフェールオーバー メカニズムが確立されます。 Cisco IOS XE Release 2.3 では、Cisco ASR 1000 シリーズ Aggregation Services Router にこの機能が実装されました。 次のコマンドが導入または変更されました。**aaa authentication login**、**aaa authentication ppp**、**aaa authorization**、**aaa cache profile**、**all (profile map configuration)**、**cache authentication profile (server group configuration)**、**cache authorization profile (server group configuration)**、**cache expiry (server group configuration)**、**clear aaa cache group**、**debug aaa cache group**、**profile (profile map configuration)**、**regexp (profile map configuration)**、**show aaa cache group**。



第 9 章

認可の設定

AAA 認可を使用すると、ユーザーが利用できるサービスを制限できます。AAA 認可をイネーブルにすると、ネットワーク アクセス サーバーはユーザーのプロファイルから取得した情報を使用して、ユーザーの設定を設定します。このプロファイルは、ローカル ユーザー データベースまたはセキュリティ サーバーにあります。認可が完了すると、ユーザー プロファイルの情報で許可されているサービスであれば、ユーザーは要求したサービスに対するアクセス権を付与されます。

AAA 認可の前提条件

名前付き方式リストを使用して認証を設定する前に、まず、次のタスクを実行する必要があります。

- ネットワーク アクセス サーバで AAA をイネーブルにします。
- AAA 認証を設定します。一般的に、認可は認証後に実行し、認証が適切に動作することに依存します。AAA 認証の設定方法については、「認証の設定」モジュールを参照してください。
- RADIUS または TACACS+ 認可を発行している場合、RADIUS または TACACS+ セキュリティ サーバーの特性を定義します。シスコのネットワーク アクセス サーバーを設定して RADIUS セキュリティ サーバーと通信する方法の詳細については、「RADIUS の設定」の章を参照してください。シスコのネットワーク アクセス サーバーを設定して TACACS+ セキュリティ サーバーと通信する方法の詳細については、「TACACS+ の設定」モジュールを参照してください。

- ローカル認可を発行している場合、**username** コマンドを使用して、特定のユーザーに関連付けられている権限を定義します。**username** コマンドの詳細については、『*Cisco IOS Security Command Reference*』を参照してください。

認可の設定の概要

認可の名前付き方式リスト

許可方式リストによって、許可の実行方法とこれらの方式の実行順序が定義されます。方式リストは、順に照会する認可方式（RADIUS または TACACS+ など）を記述した指定リストです。方式リストを使用すると、許可に使用するセキュリティプロトコルを1つ以上指定できるため、最初の方式が失敗した場合のバックアップシステムを確保できます。Cisco IOS XE ソフトウェアでは、特定のネットワーク サービスについてユーザーを許可するために最初の方式が使用されます。その方式が応答しない場合、リストの次の方式が選択されます。このプロセスは、リストのいずれかの認可方式と通信に成功するか、定義されているすべての方式が試行されるまで継続されます。

（注） Cisco IOS XE ソフトウェアでは、前の方式からの応答がない場合にのみ、リストの次の許可方式が試行されます。このサイクルの任意の時点で許可が失敗した場合（つまり、セキュリティサーバーまたはローカル ユーザー名データベースからユーザー サービスの拒否応答が返される場合）、許可プロセスは停止し、その他の許可方式は試行されません。

方式リストは、要求した認可タイプに固有です。

- Commands：ユーザが実行する EXEC モード コマンドに適用されます。コマンドの認可は、特定の特権レベルに関連付けられた、グローバル コンフィギュレーション コマンドなどのすべての EXEC モード コマンドについて、認可を試行します。
- EXEC：ユーザ EXEC ターミナル セッションに関連付けられた属性に適用されます。
- Network：ネットワーク接続に適用されます。これには、PPP、SLIP、または ARAP 接続が含まれます。
- Reverse Access：リバース Telnet セッションに適用されます。

方式の指定リストを作成すると、指定した許可タイプに対して特定の許可方式リストが定義されます。

定義されると、方式リストを特定の回線またはインターフェイスに適用してから、定義済み方式のいずれかを実行する必要があります。唯一の例外は、デフォルトの方式リスト（「default」という名前）です。名前付き方式リストを指定せずに、特定の許可タイプ用の **aaa authorization** コマンドが発行されると、名前付き方式リストが明示的に定義されている場合を除いて、すべてのインターフェイスまたは回線にデフォルトの方式リストが自動的に適用されます。（定義

済みの方式リストは、デフォルトの方式リストに優先します）。デフォルトの方式リストが定義されていない場合、デフォルトでローカル認可が実行されます。

AAA 認可方式

AAA は 5 種類の認可方式をサポートしています。

- TACACS+：ネットワーク アクセス サーバは、TACACS+ セキュリティ デーモンと認可情報を交換します。TACACS+ 認可は、属性値ペアを関連付けることでユーザに特定の権限を定義します。属性ペアは適切なユーザとともにTACACS+セキュリティ サーバのデータベースに保存されます。
- If-Authenticated：ユーザが認証に成功した場合、ユーザは要求した機能にアクセスできます。
- None：ネットワーク アクセス サーバは、認可情報を要求しません。認可は、この回線/インターフェイスで実行されません。
- Local：ルータまたはアクセスサーバーは、**username** コマンドの定義に従って、ローカルデータベースに問い合わせて、たとえばユーザーに固有の権限を許可します。ローカルデータベースを介して制御できるのは、一部の機能だけです。
- RADIUS：ネットワーク アクセス サーバは RADIUS セキュリティ サーバからの認可情報を要求します。RADIUS認可では、属性を関連付けることでユーザーに固有の権限を定義します。属性は適切なユーザーとともにRADIUSサーバー上のデータベースに保存されます。

（注） CSCuc32663 では、パスワードおよび認可ログは、TACACS+、LDAP、または RADIUS セキュリティ サーバーへ送信される前にマスクされます。マスクされていない情報を TACACS+、LDAP または RADIUS セキュリティサーバーに送信するには、**aaa authorization commands visible-keys** コマンドを使用します。

認可方式

ネットワークアクセスサーバーから TACACS+ セキュリティサーバーを介して認可情報を要求するには、**group tacacs+** *method* キーワードを指定して **aaa authorization** コマンドを使用します。TACACS+ セキュリティ サーバーを使用して認可を設定する詳細な方法については、「TACACS+ の設定」の章を参照してください。TACACS+ サーバーが、PPP や ARA などのネットワーク サービスの使用を認可できるようにする例については、「TACACS 認可の例」を参照してください。

ユーザーが認証済みであれば、要求した機能へのアクセスを許可するには、**if-authenticated** *method* キーワードを指定して **aaa authorization** コマンドを使用します。この方式を選択する場合、すべての要求した機能は、認証済みユーザーに自動的に許可されます。

特定のインターフェイスまたは回線から認可を実行したくない場合があります。指定した回線またはインターフェイスで許可動作を停止するには、**none** *method* キーワードを使用します。この方式を選択すると、すべてのアクションについて認可はディセーブルになります。

ローカル許可を選択するには（つまり、ルータまたはアクセスサーバーがローカルユーザーデータベースに問い合わせて、ユーザーが使用可能な機能を決定する場合）、**local** *method* キーワードを指定して **aaa authorization** コマンドを使用します。ローカル許可に関連する機能は、**username** グローバル コンフィギュレーション コマンドを使用して定義します。許可されている機能のリストについては、「認証の設定」の章を参照してください。

ネットワークアクセスサーバーからRADIUSセキュリティサーバーを介して許可を要求するには、**radius** *method* キーワードを使用します。RADIUS セキュリティ サーバーを使用して認可を設定する詳細な方法については、「RADIUS の設定」の章を参照してください。

ネットワークアクセスサーバーからRADIUSセキュリティサーバーを介して許可を要求するには、**group radius** *method* キーワードを指定して **aaa authorization** コマンドを使用します。RADIUSセキュリティ サーバーを使用して認可を設定する詳細な方法については、「RADIUSの設定」の章を参照してください。RADIUSサーバーがサービスを認可できるようにする例については、「RADIUS 認可の例」を参照してください。

（注） SLIP の認可方式リストは、関連インターフェイスで PPP に設定されているすべての方式に従います。特定のインターフェイスに定義および適用されるリストがない場合（またはPPP設定が指定されていない場合）、認可のデフォルト設定が適用されます。

方式リストとサーバ グループ

サーバー グループは、方式リストに使用する既存の RADIUS または TACACS+ サーバー ホストをグループ化する方法の 1 つです。次の図に、4 台のセキュリティ サーバ（R1 と R2 は RADIUS サーバ、T1 と T2 は TACACS+ サーバ）が設置された一般的な AAA ネットワーク設定を示します。R1 と R2 で RADIUS サーバのグループを構成します。T1 と T2 で TACACS+ サーバのグループを構成します。

サーバー グループを使用して、設定したサーバー ホストのサブセットを指定し、特定のサービスに使用します。たとえば、サーバーグループを使用すると、R1およびR2を別のサーバーグループとして定義し、T1およびT2を別のサーバー グループとして定義できます。つまり、R1 と T1 を方式リストに指定できるか、または R2 と T2 を方式リストに指定できます。そのため、RADIUS および TACACS+ のリソースを割り当てる場合の柔軟性が高くなります。

サーバグループには、1台のサーバに対して複数のホストエントリを含めることができます。エントリごとに固有の識別情報を設定します。固有の識別情報は、IP アドレスと UDP ポート番号の組み合わせで構成されます。これにより、RADIUSホストとして定義されているさまざまなポートが、固有の AAA サービスを提供できるようになります。つまり、この固有識別情報を使用して、ある IP アドレスに位置する 1 台のサーバ上に複数の UDP ポートが存在する場合、それぞれの UDP ポートに対して RADIUS 要求を送信できます。1 台の RADIUS サーバー上にある異なる2つのホストエントリが1つのサービス（認可など）に設定されている場合、設定されている 2 番めのホスト エントリは最初のホスト エントリのフェールオーバー バック

アップとして動作します。この例の場合、最初のホスト エントリがアカウンティング サービスの提供に失敗すると、同じデバイスに設定されている2番めのホストエントリを使用してアカウンティングサービスを提供するように、ネットワーク アクセス サーバーが試行します（試行される RADIUS ホスト エントリの順番は、設定されている順序に従います）。

サーバー グループの設定および DNIS 番号に基づくサーバー グループの設定の詳細については、「RADIUS の設定」または「TACACS+ の設定」の章を参照してください。

AAA 認可タイプ

Cisco IOS XE ソフトウェアは、5 種類の認可をサポートしています。

- Commands：ユーザが実行する EXEC モード コマンドに適用されます。コマンドの認可は、特定の特権レベルに関連付けられた、グローバル コンフィギュレーション コマンドなどのすべての EXEC モード コマンドについて、認可を試行します。
- EXEC：ユーザ EXEC ターミナル セッションに関連付けられた属性に適用されます。
- Network：ネットワーク接続に適用されます。これには、PPP、SLIP、または ARAP 接続が含まれます。
- Reverse Access：リバース Telnet セッションに適用されます。
- Configuration：AAA サーバからのコンフィギュレーションのダウンロードに適用されます。
- IP Mobile：IP モバイル サービスの認可に適用されます。

承認タイプ

名前付き認可方式リストは、指定される認可の種類によって変わります。

ユーザー別に固有のセキュリティ ポリシーを適用する認可をイネーブルにする方式リストを作成するには、auth-proxy キーワードを使用します。認証プロキシ機能の詳細については、このガイドの「Traffic Filtering and Firewalls」の部の「Configuring Authentication Proxy」を参照してください。

すべてのネットワーク関連サービス要求（SLIP、PPP、PPP NCP、ARAP など）について認可を有効にする方式リストを作成するには、**network** キーワードを使用します。

ユーザーがEXECシェルを実行できるかどうかを認可で決定できるように方式リストを作成するには、**exec** キーワードを使用します。

特定の特権レベルに関連付けられた個々のEXECコマンドについて認可を有効にする方式リストを作成するには、**commands**キーワードを使用します。これにより、指定されたコマンド レベル（0 ～ 15）に関連付けられているすべてのコマンドを認可できます。

リバースTelnet機能について認可を有効にする方式リストを作成するには、**reverse-access**キーワードを使用します。

Cisco IOS XE ソフトウェアでサポートされている認可のタイプの詳細については、「AAA 認可タイプ」を参照してください。

認可の属性値ペア

RADIUS および TACACS+ の認可はいずれも、セキュリティ サーバーのデータベースに保存されている属性を処理することで、ユーザーに固有の権限を定義します。RADIUS と TACACS+ のいずれも、属性はセキュリティ サーバーに定義され、ユーザーに関連付けられ、ユーザーの接続に適用されるネットワーク アクセス サーバーに送信されます。

サポートされる RADIUS 属性のリストについては、「RADIUS 属性の概要および RADIUS IETF 属性」の章を参照してください。サポートされる TACACS+ の AV ペアのリストについては、「TACACS+ の設定」の章を参照してください。

認可の設定方法

この章のコマンドを使用した認可の設定例については、「認可の設定例」を参照してください。

名前付き方式リストによる AAA 認可の設定

名前付き方式リストを使用して AAA 認可を設定するには、グローバル コンフィギュレーション モードで次のコマンドを使用します。

手順の概要

1. Router(config)# **aaa authorization** {**auth-proxy** | **network** | **exec** | **commands** *level* | **reverse-access** | **configuration** | **ipmobile**} {**default** | *list-name*} [*method1* [*method2...*]]
2. 次のいずれかを実行します。
   - Router(config)# **line** [**aux** | **console** | **tty** | **vty**] *line-number* [*ending-line-number*]
   -
   -
   - Router(config)# **interface** *interface-type interface-number*
3. 次のいずれかを実行します。
   - Router(config-line)# **authorization**{**arap** | **commands** *level* | **exec** | **reverse-access**} {**default** | *list-name*}
   -
   -
   - Router(config-line)# **ppp authorization**{**default** | *list-name*}

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	Router(config)# **aaa authorization** {**auth-proxy** | **network** | **exec** | **commands** *level* | **reverse-access** | **configuration** | **ipmobile**} {**default** | *list-name*} [*method1* [*method2...*]]	特定の認可タイプの認可方式リストを作成し、認可をイネーブルにします。
ステップ 2	次のいずれかを実行します。 • Router(config)# **line** [**aux** | **console** | **tty** | **vty**] *line-number* [*ending-line-number*] • • • Router(config)# **interface** *interface-type interface-number*	認可方式リストを適用する回線について、ライン コンフィギュレーション モードを開始します。 または、認可方式リストを適用するインターフェイスについて、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	次のいずれかを実行します。 • Router(config-line)# **authorization**{**arap** | **commands** *level* | **exec** | **reverse-access**} {**default** | *list-name*} • • • Router(config-line)# **ppp authorization**{**default** | *list-name*}	1 つの回線または複数回線に認可リストを適用します。 または、1つのインターフェイスまたは複数インターフェイスに認可リストを適用します。

グローバル コンフィギュレーション コマンドの認可のディセーブル化

commands キーワードを指定して **aaa authorization** コマンドを使用すると、その特権レベルに関連付けられているすべての EXEC モードコマンド（グローバル コンフィギュレーション コマンドを含む）に対して許可が試行されます。一部の EXEC レベル コマンドと同じコンフィギュレーション コマンドもあるため、認可プロセスが混乱する可能性があります。**no aaa authorization config-commands** を使用すると、ネットワーク アクセス サーバーがコンフィギュレーション コマンド認可の試行を停止します。

すべてのグローバル コンフィギュレーション コマンドについてAAA認可をディセーブルにするには、グローバル コンフィギュレーション モードで次のコマンドを使用します。

コマンド	目的
`Device(config)# no aaa authorization config-commands`	すべてのグローバル コンフィギュレーション コマンドについて認可をディセーブルにします。

コンソール上で AAA 認可をディセーブルにするには、グローバル コンフィギュレーション モードで次のコマンドを使用します。

（注） デフォルトでコンソールの AAA 認可はディセーブルです。コンソールで AAA 許可が有効になっている場合は、AAA の設定段階で **no aaa authorization console** コマンドを設定して無効にします。ユーザー認証用のコンソールでは AAA をディセーブルにする必要があります。

コマンド	目的
`Device(config)# no aaa authorization console`	コンソールでの認証を無効にします。

リバース Telnet の認可の設定

Telnet は、リモート ターミナル接続に使用される標準ターミナル エミュレーション プロトコルです。通常、ネットワーク アクセス サーバーに（主にダイヤルアップ接続経由で）ログインし、Telnet を使用してそのネットワーク アクセス サーバーから他のネットワーク デバイスにアクセスします。ただし、場合によっては、リバース Telnet セッションを確立する必要があります。リバース Telnet セッションでは、反対方向の Telnet 接続（つまり、ネットワーク内部から、ネットワーク周辺にあるネットワーク アクセス サーバーに対する接続）が確立されます。その接続によって、ネットワーク アクセス サーバーに接続しているモデムや他のデバイスへのアクセスを取得します。リバース Telnet は、ユーザーがネットワーク アクセス サーバーに接続されているモデム ポートに Telnet を送信できるようにすることで、ユーザーにダイヤルアウト機能を提供します。

リバース Telnet を介してアクセスできるポートのアクセス権を制御することが重要です。適切に制御しないと、たとえば、不正ユーザーがモデムに自由にアクセスし、着信コールをトラップして迂回させたり、不正な宛先にコールを送信したりする可能性があります。

リバース Telnet 時の認証は、Telnet 用の標準の AAA ログイン手順を介して実行されます。通常、Telnet またはリバース Telnet セッションを確立するには、ユーザーはユーザー名とパスワードを指定する必要があります。リバース Telnet 認可は、認証に加えて認可を必須にすることで、追加（任意）レベルのセキュリティを提供します。リバース Telnet 認可をイネーブルにすることで、標準の Telnet ログイン手順を介してユーザー認証を完了した後に、RADIUS または TACACS+ を使用して、そのユーザーが非同期ポートにリバース Telnet アクセスを実行できるかどうかを認可できます。

リバース Telnet 認可には次の利点があります。

- リバース Telnet アクティビティを実行しているユーザーに、リバース Telnet を使用して特定の非同期ポートにアクセスする権限を付与することで、追加レベルの保護を実現しています。
- リバース Telnet 認可を管理できる（アクセス リスト以外の）代替方式があります。

ネットワーク アクセス サーバーが TACACS+ または RADIUS サーバーからの認可情報を要求するように設定してから、ユーザーによるリバース Telnet セッションの確立を許可するには、グローバル コンフィギュレーション モードで次のコマンドを使用します。

コマンド	目的
`Router(config)# aaa authorization reverse-access method1 [method2 ...]`	ネットワーク アクセス サーバーが認可情報を要求するように設定してから、ユーザーによるリバースTelnetセッションの確立を許可します。

この機能によって、ネットワーク アクセス サーバーは、セキュリティ サーバー（RADIUS または TACACS+）からリバース Telnet 認可情報を要求できます。セキュリティ サーバー上のユーザーに固有のリバース Telnet 特権を設定する必要があります。

認可設定の例

TACACS 認可の例

次に、TACACS+ サーバーを使用して、PPP や ARA などのネットワーク サービスの使用を認可する例を示します。TACACS+ サーバーが使用不能の場合、または認可プロセス中にエラーが発生した場合、フォールバック方式（none）はすべての認可要求を許可することです。

```
aaa authorization network default group tacacs+ none
```

次に、TACACS+ を使用してネットワークの認可を許可する例を示します。

```
aaa authorization network default group tacacs+
```

次に、同じ認可を提供し、「*mci*」と「*att*」というアドレス プールも作成する例を示します。

```
aaa authorization network default group tacacs+
ip address-pool local
ip local-pool mci 172.16.0.1 172.16.0.255
ip local-pool att 172.17.0.1 172.17.0.255
```

これらのアドレス プールは、TACACS デーモンによって選択できます。デーモンの設定例を次に示します。

```
user = mci_customer1 {
    login = cleartext "some password"
    service = ppp protocol = ip {
        addr-pool=mci
    }
}
user = att_customer1 {
    login = cleartext "some other password"
    service = ppp protocol = ip {
        addr-pool=att
     }
```

RADIUS 認可の例

次に、RADIUS を使用して認可を行うようにルータを設定する方法の例を示します。

```
aaa new-model
aaa authorization exec default group radius if-authenticated
aaa authorization network default group radius
radius-server host ip
radius-server key
```

この RADIUS 認可設定のサンプル行は、次のように定義されます。

- **aaa authorization exec default group radius if-authenticated** コマンドで、ネットワークアクセスサーバーが RADIUS サーバーに接続して、ユーザーのログイン時にユーザーが EXEC シェルを起動する権限があるかどうかを決定するように設定します。ネットワークアクセスサーバーが RADIUS サーバーに接続するときにエラーが発生した場合、フォールバック方式は、ユーザーが適切に認証されていると CLI の起動を許可します。

返される RADIUS 情報を使用して、その接続に適用される autocommand または接続アクセスリストを指定できます。

- **aaa authorization network default group radius** コマンドにより、RADIUS を介するネットワーク許可を設定します。この操作は、アドレス割り当ての管理、アクセスリストのアプリケーション、および他の多様なユーザー別の数量に使用できます。

（注） この例ではフォールバック方式を指定していないため、何らかの理由で認可に失敗すると、RADIUS サーバーからの応答はありません。

リバース Telnet 認可の例

次に、ネットワーク アクセス サーバーが TACACS+ セキュリティ サーバーから認可情報を要求してから、ユーザーによるリバース Telnet セッションの確立を許可する例を示します。

```
aaa new-model
aaa authentication login default group tacacs+
aaa authorization reverse-access default group tacacs+
!
tacacs-server host 172.31.255.0
tacacs-server timeout 90
tacacs-server key goaway
```

この TACACS+ リバース Telnet 認可設定のサンプル行は、次のように定義されます。

- **aaa new-model** コマンドは AAA を有効にします。
- **aaa authentication login default group tacacs+** コマンドで、ログイン時のユーザー認証のデフォルト方式として TACACS+ を指定します。
- リバース Telnet セッションを確立しようとしているときに、**aaa authorization reverse-access default group tacacs+** コマンドで、ユーザー認可の方式として TACACS+ を指定します。
- **tacacs-server host** コマンドで、TACACS+ サーバーを指定します。

- **tacacs-server timeout** コマンドで、ネットワークアクセスサーバーが TACACS+ サーバーの応答を待機する期間を設定します。
- **tacacs-server key** コマンドで、ネットワークアクセスサーバーと TACACS+ デーモン間のすべての TACACS+ 通信に使用される暗号キーを定義します。

次に、ネットワーク アクセス サーバー「maple」上のポート tty2、およびネットワーク アクセス サーバー「oak」上のポート tty5 に対するリバース Telnet アクセス権をユーザー pat に付与する汎用の TACACS+ サーバーを設定する例を示します。

```
user = pat
  login = cleartext lab
  service = raccess {
    port#1 = maple/tty2
    port#2 = oak/tty5
```

（注） この例では、「maple」と「oak」には、DNS 名またはエイリアスではなく、ネットワーク アクセス サーバーのホスト名が設定されています。

次に、TACACS+ サーバー（CiscoSecure）を設定して、ユーザー pat にリバース Telnet アクセス権を付与する例を示します。

```
user = pat
profile_id = 90
profile_cycle = 1
member = Tacacs_Users
service=shell {
default cmd=permit
}
service=raccess {
allow "c2511e0" "tty1" ".*"
refuse ".*" ".*" ".*"
password = clear "goaway"
```

（注） CiscoSecure は、バージョン 2.1(*x*)～ バージョン 2.2(1) のコマンドライン インターフェイスを使用して、リバース Telnet だけをサポートしています。

空の「service=raccess {}」句は、リバース Telnet のネットワーク アクセス サーバー ポートに対して無条件のアクセス権をユーザーに許可しています。「service=raccess」句が存在しない場合、ユーザーはリバース Telnet のすべてのポートに対してアクセスを拒否されます。

TACACS+の設定の詳細については、「TACACS+の設定」の章を参照してください。CiscoSecure の設定の詳細については、『*CiscoSecure Access Control Server User Guide*』の version 2.1(2) 以降を参照してください。

次に、ネットワーク アクセス サーバーが RADIUS セキュリティ サーバーから認可を要求してから、ユーザーによるリバース Telnet セッションの確立を許可する例を示します。

```
aaa new-model
```

```
aaa authentication login default group radius
aaa authorization reverse-access default group radius
!
radius-server host 172.31.255.0
radius-server key go away
auth-port 1645 acct-port 1646
```

この RADIUS リバース Telnet 認可設定のサンプル行は、次のように定義されます。

- **aaa new-model** コマンドは AAA を有効にします。
- **aaa authentication login default group radius** コマンドで、ログイン時のユーザー認証のデフォルト方式として RADIUS を指定します。
- リバース Telnet セッションを確立しようとしているときに、**aaa authorization reverse-access default group radius** コマンドで、ユーザー認可の方式として RADIUS を指定します。
- **radius-server host** コマンドで、RADIUS サーバーを指定します。
- **radius-server key** コマンドで、ネットワークアクセスサーバーと RADIUS デーモン間のすべての RADIUS 通信に使用される暗号キーを定義します。

次に、ネットワーク アクセス サーバー「maple」上のポート tty2 で、ユーザー「pat」にリバース Telnet アクセス権を付与する RADIUS サーバーに要求を送信する例を示します。

```
Username = "pat"
Password = "goaway"
User-Service-Type = Shell-User
cisco-avpair = "raccess:port#1=maple/tty2"
```

構文「raccess:port=any/any」で、リバース Telnet のネットワーク アクセス サーバー ポートに対して無条件のアクセス権をユーザーに許可します。「raccess:port={*nasname* }/{*tty number* }」句がユーザー プロファイルにない場合、ユーザーはすべてのポートでリバース Telnet へのアクセスを拒否されます。

RADIUS の設定の詳細については、「RADIUS の設定」の章を参照してください。

その他の参考資料

関連資料

関連項目	マニュアル タイトル
セキュリティ コマンド	『Cisco IOS Security Command Reference』
IPSec	IPsec 仮想トンネル インターフェイス機能のドキュメント

MIB

MIB	MIB のリンク
なし	選択したプラットフォーム、Cisco ソフトウェア リリース、およびフィーチャ セットの MIB を検索してダウンロードする場合は、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

シスコのテクニカル サポート

説明	リンク
右の URL にアクセスして、シスコのテクニカル サポートを最大限に活用してください。これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

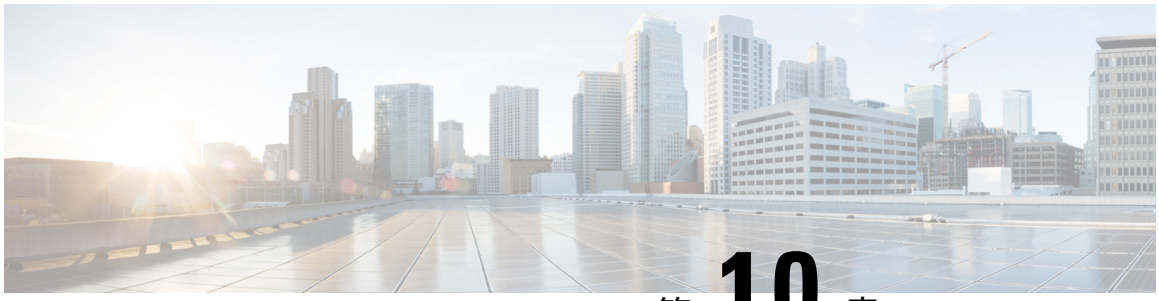
認可の設定に関する機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *22 :* 認可の設定に関する機能情報

機能名	リリース	機能情報
AAA 認可およびアカウンティングの名前付き方式リスト	Cisco IOS XE Release 2.1	許可方式リストによって、許可の実行方法とこれらの方式の実行順序が定義されます。方式リストは、順に照会する認可方式（RADIUS または TACACS+ など）を記述した指定リストです。 Cisco IOS XE Release 2.1 では、Cisco ASR 1000 シリーズ Aggregation Services Router にこの機能が実装されました。



第 10 章

アカウンティングの設定

AAA アカウンティング機能を使用すると、ユーザーがアクセスするサービス、およびユーザーが消費するネットワーク リソース量を追跡できます。AAA アカウンティングをイネーブルにすると、ネットワーク アクセス サーバーから TACACS+ または RADIUS セキュリティ サーバー（実装しているセキュリティ手法によって異なります）に対して、アカウンティング レコードの形式でユーザー アクティビティがレポートされます。各アカウンティング レコードにはアカウンティングの Attribute-Value（AV）ペアが含まれ、レコードはセキュリティ サーバに格納されます。このデータを分析して、ネットワーク管理、クライアント課金、および監査に利用できます。

アカウンティングを設定するための前提条件

次のタスクを実行してから、名前付き方式リストを使用してアカウンティングを設定します。

- ネットワーク アクセス サーバで AAA をイネーブルにします。
- RADIUS または TACACS+ 認可が発行されている場合、RADIUS または TACACS+ セキュリティ サーバの特性を定義します。シスコのネットワーク アクセス サーバを設定して RADIUS セキュリティ サーバと通信する方法の詳細については、「Configuring RADIUS」の章を参照してください。シスコのネットワーク アクセス サーバを設定して TACACS+ セキュリティ サーバと通信する方法の詳細については、「Configuring TACACS+」の章を参照してください。

アカウンティングの設定の制約事項

AAA アカウンティング機能には次の制限があります。

- アカウンティング情報は、最大 4 台の AAA サーバに同時送信できます。
- Service Selection Gateway（SSG）制限：SSG システムの場合、**aaa accounting network broadcast** コマンドを実行すると、**start-stop** アカウンティングレコードのみがブロードキャストされます。**ssg accounting interval** コマンドを使用して中間アカウンティングレコードを設定する場合、中間アカウンティングレコードは、設定したデフォルトRADIUSサーバーにのみ送信されます。

アカウンティングの設定に関する情報

アカウンティングの名前付き方式リスト

認証および認可方式リストと同様に、アカウンティングの方式リストには、アカウンティングの実行方法とその方式を実行するシーケンスが定義されています。

アカウンティングの方式指定リストには、特定のセキュリティプロトコルを指定し、アカウンティングサービスの特定の行またはインターフェイスに使用できます。唯一の例外はデフォルトの方式リスト（偶然に「default」と名前が付けられている）です。デフォルトの方式リストは、明示的に定義された名前付きの方式リストを持つインターフェイスを除くすべてのインターフェイスに自動的に適用されます。定義済みの方式リストは、デフォルトの方式リストに優先します。

方式リストは、順に照会するアカウンティング方式（RADIUS、TACACS+ など）を記述する指定リストです。方式リストでは、アカウンティングに1つまたは複数のセキュリティプロトコルを指定できます。そのため、最初の方式が失敗した場合にアカウンティングのバックアップ システムを確保できます。Cisco IOS XE ソフトウェアでは、方式リストのうち、アカウンティングをサポートする最初の方式が使用されます。その方式が応答しない場合、方式リストの次のアカウンティング方式が選択されます。このプロセスは、リストのいずれかのアカウンティング方式と通信に成功するか、定義されているすべての方式が試行されるまで継続されます。

（注） Cisco IOS XE ソフトウェアでは、前の方式からの応答がない場合にのみ、リストの次のアカウンティング方式でアカウンティングが試行されます。このサイクルの任意の時点でアカウンティングが失敗した場合（つまり、セキュリティ サーバーからユーザー アクセスの拒否応答が返される場合）、アカウンティング プロセスは停止し、その他のアカウンティング方式は試行されません。

アカウンティング方式リストは、要求されるアカウンティングの種類によって変わります。AAA は、次の 6 種類のアカウンティングをサポートしています。

- Network：パケットやバイト カウントなど、すべての PPP、SLIP、または ARAP セッションに関する情報を提供します。
- EXEC：ネットワーク アクセス サーバのユーザ EXEC ターミナル セッションに関する情報を提供します。
- Command：ユーザが発行する EXEC モード コマンドに関する情報を提供します。コマンド アカウンティングは、特定の特権レベルに関連付けられた、グローバル コンフィギュレーション コマンドなどのすべての EXEC モード コマンドについて、アカウンティング レコードを生成します。
- Connection：Telnet、ローカルエリア トランスポート（LAT）、TN3270、パケット アセンブラ/ディスアセンブラ（PAD）、rlogin などのネットワーク アクセス サーバから行われたすべてのアウトバンド接続に関する情報を出力します。
- System：システムレベルのイベントに関する情報を提供します。
- Resource：ユーザ認証に成功したコールの「開始」および「終了」レコードを提供します。また、認証に失敗したコールの「終了」レコードを提供します。

（注） システム アカウンティングは、名前付きアカウンティング リストを使用しません。システム アカウンティングのデフォルト リストだけを定義できます。

方式指定リストが作成されると、指定したアカウンティング タイプのアカウンティング方式のリストが定義されます。

アカウンティング方式リストを特定の回線またはインターフェイスに適用してから、定義済み方式のいずれかを実行する必要があります。唯一の例外は、デフォルトの方式リスト（「default」という名前）です。特定のアカウンティングの種類の **aaa accounting** コマンドを、名前付き方式リストを指定しないで発行した場合、名前付き方式リストが明示的に定義されているものを除いて、すべてのインターフェイスまたは回線にデフォルトの方式リストが自動的に適用されます（定義済みの方式リストは、デフォルトの方式リストに優先します）。デフォルトの方式リストが定義されていない場合、アカウンティングは実行されません。

ここでは、次の内容について説明します。

方式リストとサーバ グループ

サーバー グループは、方式リストに使用する既存の RADIUS または TACACS+ サーバー ホストをグループ化する方法の 1 つです。次の図に、4 台のセキュリティ サーバ（R1 と R2 は RADIUS サーバ、T1 と T2 は TACACS+ サーバ）が設置された一般的な AAA ネットワーク設定を示します。R1 と R2 は RADIUS サーバーのグループから構成されます。T1 と T2 は TACACS+ サーバーのグループから構成されます。

Cisco IOS XE ソフトウェアでは、RADIUS および TACACS+ サーバ設定はグローバルです。サーバー グループを使用して、設定済みのサーバー ホストのサブセットを指定できます。このようなサーバー グループは、特定のサービスに使用できます。たとえば、サーバー グループを使用すると、R1 と R2 を個別のサーバー グループ（SG1 と SG2）として定義し、T1 と T2 を個別のサーバー グループ（SG3 と SG4）として定義できます。つまり、R1 と T1（SG1 と SG3）を方式リストに指定できるか、または R2 と T2（SG2 と SG4）を方式リストに指定できます。そのため、RADIUS および TACACS+ のリソースを割り当てる場合の柔軟性が高くなります。

サーバ グループには、1 台のサーバに対して複数のホストエントリを含めることができます。エントリごとに固有の識別情報を設定します。固有の識別情報は、IP アドレスと UDP ポート番号の組み合わせで構成されます。これにより、RADIUS ホストとして定義されているさまざまなポートが、固有の AAA サービスを提供できるようになります。つまり、この固有識別情報を使用して、ある IP アドレスに位置する 1 台のサーバ上に複数の UDP ポートが存在する場合、それぞれの UDP ポートに対して RADIUS 要求を送信できます。1 台の RADIUS サーバ上にある異なる 2 つのホストエントリが 1 つのサービス（アカウンティングなど）に設定されている場合、設定されている 2 番めのホスト エントリは最初のホスト エントリのフェールオーバー バックアップとして動作します。この場合、最初のホスト エントリがアカウンティング サービスを提供できなかった場合、ネットワーク アクセス サーバは同じ装置上でアカウンティング サービス用に設定されている 2 番めのホストエントリを試行します（試行される RADIUS ホスト エントリの順番は、設定されている順序に従います）。

DNIS 番号に基づくサーバ グループの設定およびサーバ グループの設定の詳細については、『*Cisco IOS XE Security Configuration Guide: Securing User Services* Release 2』の「Configuring RADIUS」または「Configuring TACACS+」を参照してください。

AAA アカウンティング方式

Cisco IOS XE はアカウンティングについて次の 2 つの方式をサポートします。

- TACACS+：ネットワーク アクセス サーバは、アカウンティング レコードの形式で TACACS+ セキュリティ サーバに対してユーザ アクティビティを報告します。各アカウンティング レコードにはアカウンティングの Attribute-Value（AV）ペアが含まれ、レコードはセキュリティ サーバに格納されます。
- RADIUS：ネットワーク アクセス サーバは、アカウンティング レコードの形式で RADIUS セキュリティ サーバに対してユーザ アクティビティを報告します。各アカウンティング レコードにはアカウンティングの Attribute-Value（AV）ペアが含まれ、レコードはセキュリティ サーバに格納されます。

（注） CSCuc32663 では、パスワードおよびアカウンティング ログは、TACACS+ または RADIUS セキュリティ サーバーへ送信される前にマスクされます。マスクされていない情報を TACACS+ または RADIUS セキュリティ サーバに送信するには、**aaa accounting commands visible-keys** コマンドを使用します。

アカウンティング レコードの種類

最小限のアカウンティングの場合、**stop-only** キーワードを使用します。このキーワードによって、要求されたユーザープロセスの終了時に、終了レコードアカウンティング通知を送信するよう、指定した方式（RADIUS または TACACS+）に指示します。詳細なアカウンティング情報が必要な場合、**start-stop** キーワードを使用して、要求されたイベントの開始時には開始アカウンティング通知、そのイベントの終了時には修理用アカウンティング通知を送信します。この回線またはインターフェイスですべてのアカウンティング アクティビティを終了するには、**none** キーワードを使用します。

アカウンティング方式

次の表に、サポートされるアカウンティング キーワードを示します。

表 *23 : AAA* アカウンティング方式

キーワード	説明
group radius	アカウンティングにすべての RADIUS サーバーのリストを使用します。
group tacacs+	アカウンティングにすべての TACACS+ サーバーのリストを使用します。
group group-name	*group-name* サーバー グループで定義したように、アカウンティングのための RADIUS サーバーまたは TACACS+ サーバーのサブセットを使用します。

method 引数は、認証アルゴリズムが試行する実際の方式を指します。追加の認証方式は、直前の方式で（失敗した場合ではなく）エラーが返された場合にのみ使用されます。他のすべての方式がエラーを返しても、認証に成功したことを指定するには、コマンドで追加の方式を指定します。たとえば、TACACS+ 認証がエラーを返す場合に認証のバックアップ方式として RADIUS を指定する acct_tac1 という方式リストを作成するには、次のコマンドを入力します。

```
aaa accounting network acct_tac1 stop-only group tacacs+ group radius
```

aaa accounting コマンドで名前付きリストが指定されて「いない」場合に使用するデフォルトのリストを作成するには、**default** キーワードの後ろにデフォルト状況で使用される方式を指定します。デフォルト認証方式リストは、自動的にすべてのインターフェイスに適用されます。

たとえば、ログイン時のユーザー認証のデフォルト方式として RADIUS を指定するには、次のコマンドを入力します。

```
aaa accounting network default stop-only group radius
```

AAA アカウンティングは、次の方式をサポートします。

- **group tacacs** ：ネットワーク アクセス サーバーからアカウンティング情報を TACACS+ セキュリティサーバーに送信するようにするには、**group tacacs+** 方式キーワードを使用します。

- **group radius** ：ネットワーク アクセス サーバーからアカウンティング情報を RADIUS セキュリティサーバーに送信するようにするには、**group radius** 方式キーワードを使用します。

（注） SLIP のアカウンティング方式リストは、関連インターフェイスで PPP に設定されているすべての方式に従います。特定のインターフェイスに定義および適用されるリストがない場合（または PPP 設定が指定されていない場合）、アカウンティングのデフォルト設定が適用されます。

- **group** *group-name* ：RADIUS または TACACS+ サーバーのサブセットを指定して、アカウンティング方式として使用するには、**group** *group-name* 方式を指定して **aaa accounting** コマンドを使用します。グループ名とそのグループのメンバを指定して定義するには、**aaa group server** コマンドを使用します。たとえば、**aaa group server** コマンドを使用して、**group loginrad** のメンバを最初に定義します。

```
aaa group server radius loginrad
 server 172.16.2.3
 server 172.16.2 17
 server 172.16.2.32
```

このコマンドにより、172.16.2.3、172.16.2.17、172.16.2.32 の RADIUS サーバーがグループ *loginrad* のメンバとして指定されます。

他の方式リストが定義されていない場合、ネットワークアカウンティングの方式として**group loginrad** を指定するには、次のコマンドを入力します。

```
aaa accounting network default start-stop group loginrad
```

アカウンティング方式としてグループ名を使用するには、事前にRADIUSまたはTACACS+セキュリティ サーバーとの通信をイネーブルにする必要があります。

AAA アカウンティング タイプ

名前付きアカウンティング方式リストは、指定したタイプのアカウンティングに固有です。

- **network**：すべてのネットワーク関連サービス要求（SLIP、PPP、PPP NCP、ARAP などのプロトコル）について認可をイネーブルにする方式リストを作成するには、**aaa accounting** コマンドで**network** キーワードを使用します。たとえば、ARAP（ネットワーク）セッションにアカウント情報を提供する方式リストを作成するには、**accounting** コマンドで **arap** キーワードを使用します。
- **exec**：ネットワーク アクセス サーバー上のユーザー EXEC ターミナルセッションに関するアカウンティングレコード（ユーザー名、日付、開始時刻、終了時刻など）を提供する方式リストを作成するには、**exec** キーワードを使用します。

- **commands**：特定の特権レベルに関連付けられた特定の EXEC コマンドに関するアカウンティング情報を提供する方式リストを作成するには、**commands** キーワードを使用します。
- **connection**：ネットワーク アクセス サーバーから開始されるすべての発信接続に関するアカウンティング情報を提供する方式リストを作成するには、**connection** キーワードを使用します。
- resource：ユーザ認証に成功したコールまたは認証に失敗したコールのアカウンティング レコードを提供する方式リストを作成します。

（注） システム アカウンティングは、名前付き方式リストをサポートしません。

ネットワーク アカウンティング

ネットワーク アカウンティングは、パケットやバイト カウントなど、すべての PPP、SLIP、または ARAP セッションに関する情報を提供します。

次に、EXEC セッションを介して着信する PPP ユーザの RADIUS ネットワーク アカウンティング レコードに含まれる情報の例を示します。

```
Wed Jun 27 04:44:45 2001
        NAS-IP-Address = “172.16.25.15”
        NAS-Port = 5
        User-Name = “username1”
        Client-Port-DNIS = “4327528”
        Caller-ID = “562”
        Acct-Status-Type = Start
        Acct-Authentic = RADIUS
        Service-Type = Exec-User
        Acct-Session-Id = “0000000D”
        Acct-Delay-Time = 0
        User-Id = “username1”
        NAS-Identifier = “172.16.25.15”

Wed Jun 27 04:45:00 2001
        NAS-IP-Address = “172.16.25.15”
        NAS-Port = 5
        User-Name = “username1”
        Client-Port-DNIS = “4327528”
        Caller-ID = “562”
        Acct-Status-Type = Start
        Acct-Authentic = RADIUS
        Service-Type = Framed
        Acct-Session-Id = “0000000E”
        Framed-IP-Address = “10.1.1.2”
        Framed-Protocol = PPP
        Acct-Delay-Time = 0
        User-Id = “username1”
        NAS-Identifier = “172.16.25.15”
Wed Jun 27 04:47:46 2001
        NAS-IP-Address = “172.16.25.15”
        NAS-Port = 5
        User-Name = “username1”
```

```
        Client-Port-DNIS = “4327528”
        Caller-ID = “562”
        Acct-Status-Type = Stop
        Acct-Authentic = RADIUS
        Service-Type = Framed
        Acct-Session-Id = “0000000E”
        Framed-IP-Address = “10.1.1.2”
        Framed-Protocol = PPP
        Acct-Input-Octets = 3075
        Acct-Output-Octets = 167
        Acct-Input-Packets = 39
        Acct-Output-Packets = 9
        Acct-Session-Time = 171
        Acct-Delay-Time = 0
        User-Id = “username1”
        NAS-Identifier = “172.16.25.15”
Wed Jun 27 04:48:45 2001
        NAS-IP-Address = “172.16.25.15”
        NAS-Port = 5
        User-Name = “username1”
        Client-Port-DNIS = “4327528”
        Caller-ID = “408”
        Acct-Status-Type = Stop
        Acct-Authentic = RADIUS
        Service-Type = Exec-User
        Acct-Session-Id = “0000000D”
        Acct-Delay-Time = 0
        User-Id = “username1”
        NAS-Identifier = “172.16.25.15”
```

次に、最初にEXECセッションを開始したPPPユーザのTACACS+ネットワーク アカウンティング レコードに含まれる情報の例を示します。

```
Wed Jun 27 04:00:35 2001 172.16.25.15    username1   tty4    562/4327528
starttask_id=28      service=shell
Wed Jun 27 04:00:46 2001 172.16.25.15    username1   tty4 562/4327528    starttask_id=30
      addr=10.1.1.1   service=ppp
Wed Jun 27 04:00:49 2001 172.16.25.15    username1   tty4    408/4327528     update
   task_id=30      addr=10.1.1.1   service=ppp     protocol=ip     addr=10.1.1.1
Wed Jun 27 04:01:31 2001 172.16.25.15    username1   tty4    562/4327528     stoptask_id=30
       addr=10.1.1.1   service=ppp     protocol=ip     addr=10.1.1.1   bytes_in=2844
     bytes_out=1682  paks_in=36      paks_out=24     elapsed_time=51
Wed Jun 27 04:01:32 2001 172.16.25.15    username1   tty4    562/4327528     stoptask_id=28
       service=shell   elapsed_time=57
```

（注） アカウンティング パケット レコードの正確なフォーマットは、セキュリティ サーバ デーモンに応じて変わります。

次に、autoselectを介して着信するPPPユーザのRADIUSネットワーク アカウンティング レコードに含まれる情報の例を示します。

```
Wed Jun 27 04:30:52 2001
        NAS-IP-Address = “172.16.25.15”
        NAS-Port = 3
        User-Name = “username1”
        Client-Port-DNIS = “4327528”
        Caller-ID = “562”
        Acct-Status-Type = Start
```

```
        Acct-Authentic = RADIUS
        Service-Type = Framed
        Acct-Session-Id = "0000000B"
        Framed-Protocol = PPP
        Acct-Delay-Time = 0
        User-Id = "username1"
        NAS-Identifier = "172.16.25.15"

Wed Jun 27 04:36:49 2001
        NAS-IP-Address = "172.16.25.15"
        NAS-Port = 3
        User-Name = "username1"
        Client-Port-DNIS = "4327528"
        Caller-ID = "562"
        Acct-Status-Type = Stop
        Acct-Authentic = RADIUS
        Service-Type = Framed
        Acct-Session-Id = "0000000B"
        Framed-Protocol = PPP
        Framed-IP-Address = "10.1.1.1"
        Acct-Input-Octets = 8630
        Acct-Output-Octets = 5722
        Acct-Input-Packets = 94
        Acct-Output-Packets = 64
        Acct-Session-Time = 357
        Acct-Delay-Time = 0
        User-Id = "username1"
        NAS-Identifier = "172.16.25.15"
```

次に、autoselect を介して着信する PPP ユーザの TACACS+ ネットワーク アカウンティング レコードに含まれる情報の例を示します。

```
Wed Jun 27 04:02:19 2001 172.16.25.15    username1   Async5  562/4327528
starttask_id=35      service=ppp
Wed Jun 27 04:02:25 2001 172.16.25.15    username1   Async5  562/4327528     update
   task_id=35      service=ppp     protocol=ip     addr=10.1.1.2
Wed Jun 27 04:05:03 2001 172.16.25.15   username1   Async5  562/4327528    stoptask_id=35
       service=ppp     protocol=ip     addr=10.1.1.2   bytes_in=3366   bytes_out=2149
     paks_in=42      paks_out=28     elapsed_time=164
```

EXEC アカウンティング

EXEC アカウンティングは、ネットワーク アクセス サーバ上にあるユーザ EXEC ターミナル セッション（ユーザ シェル）に関する情報を提供します。たとえば、ユーザ名、日付、開始時刻と終了時刻、アクセス サーバの IP アドレス、および（ダイヤルイン ユーザの場合）発信元の電話番号などです。

次に、ダイヤルイン ユーザの RADIUS EXEC アカウンティング レコードに含まれる情報の例を示します。

```
Wed Jun 27 04:26:23 2001
        NAS-IP-Address = "172.16.25.15"
        NAS-Port = 1
        User-Name = "username1"
        Client-Port-DNIS = "4327528"
        Caller-ID = "5622329483"
        Acct-Status-Type = Start
        Acct-Authentic = RADIUS
        Service-Type = Exec-User
        Acct-Session-Id = "00000006"
```

```
        Acct-Delay-Time = 0
        User-Id = "username1"
        NAS-Identifier = "172.16.25.15"
Wed Jun 27 04:27:25 2001
        NAS-IP-Address = "172.16.25.15"
        NAS-Port = 1
        User-Name = "username1"
        Client-Port-DNIS = "4327528"
        Caller-ID = "5622329483"
        Acct-Status-Type = Stop
        Acct-Authentic = RADIUS
        Service-Type = Exec-User
        Acct-Session-Id = "00000006"
        Acct-Session-Time = 62
        Acct-Delay-Time = 0
        User-Id = "username1"
        NAS-Identifier = "172.16.25.15"
```

次に、ダイヤルイン ユーザの TACACS+ EXEC アカウンティング レコードに含まれる情報の例を示します。

```
Wed Jun 27 03:46:21 2001        172.16.25.15    username1   tty3    5622329430/4327528
 start    task_id=2       service=shell
Wed Jun 27 04:08:55 2001        172.16.25.15    username1   tty3    5622329430/4327528
 stop     task_id=2       service=shell   elapsed_time=1354
```

次に、Telnet ユーザの RADIUS EXEC アカウンティング レコードに含まれる情報の例を示します。

```
Wed Jun 27 04:48:32 2001
        NAS-IP-Address = "172.16.25.15"
        NAS-Port = 26
        User-Name = "username1"
        Caller-ID = "10.68.202.158"
        Acct-Status-Type = Start
        Acct-Authentic = RADIUS
        Service-Type = Exec-User
        Acct-Session-Id = "00000010"
        Acct-Delay-Time = 0
        User-Id = "username1"
        NAS-Identifier = "172.16.25.15"

Wed Jun 27 04:48:46 2001
        NAS-IP-Address = "172.16.25.15"
        NAS-Port = 26
        User-Name = "username1"
        Caller-ID = "10.68.202.158"
        Acct-Status-Type = Stop
        Acct-Authentic = RADIUS
        Service-Type = Exec-User
        Acct-Session-Id = "00000010"
        Acct-Session-Time = 14
        Acct-Delay-Time = 0
        User-Id = "username1"
        NAS-Identifier = "172.16.25.15"
```

次に、Telnet ユーザの TACACS+ EXEC アカウンティング レコードに含まれる情報の例を示します。

```
Wed Jun 27 04:06:53 2001        172.16.25.15    username1   tty26   10.68.202.158
starttask_id=41      service=shell
```

```
Wed Jun 27 04:07:02 2001        172.16.25.15    username1   tty26   10.68.202.158
stoptask_id=41       service=shell   elapsed_time=9
```

コマンド アカウンティング

コマンド アカウンティングは、ネットワーク アクセス サーバで実行される各特権レベルの EXEC シェル コマンドに関する情報を提供します。各コマンド アカウンティング レコードには、その特権レベルで実行されるコマンド、各コマンドが実行された日時、および実行したユーザのリストが含まれます。

次に、特権レベル 1 の TACACS+ コマンド アカウンティング レコードに含まれる情報の例を示します。

```
Wed Jun 27 03:46:47 2001        172.16.25.15    username1   tty3    5622329430/4327528
 stop     task_id=3       service=shell   priv-lvl=1      cmd=show version <cr>
Wed Jun 27 03:46:58 2001        172.16.25.15    username1   tty3    5622329430/4327528
 stop     task_id=4       service=shell   priv-lvl=1      cmd=show interfaces <cr>
Wed Jun 27 03:47:03 2001        172.16.25.15    username1   tty3    5622329430/4327528
 stop     task_id=5       service=shell   priv-lvl=1      cmd=show ip route <cr>
```

次に、特権レベル 15 の TACACS+ コマンド アカウンティング レコードに含まれる情報の例を示します。

```
Wed Jun 27 03:47:17 2001        172.16.25.15    username1   tty3    5622329430/4327528
 stop     task_id=6       service=shell   priv-lvl=15     cmd=configure terminal <cr>
Wed Jun 27 03:47:21 2001        172.16.25.15    username1   tty3    5622329430/4327528
 stop     task_id=7       service=shell   priv-lvl=15     cmd=interface
GigabitEthernet0/0/0 <cr>
Wed Jun 27 03:47:29 2001        172.16.25.15    username1   tty3    56223294304327528
stop     task_id=8       service=shell   priv-lvl=15     cmd=ip address 10.1.1.1
255.255.255.0 <cr>
```

（注） シスコの RADIUS 実装は、コマンド アカウンティングをサポートしていません。

接続アカウンティング

接続アカウンティングは、Telnet、LAT、TN3270、PAD、rlogin などのネットワーク アクセス サーバから行われるすべての発信接続に関する情報を提供します。

次に、発信 Telnet 接続の RADIUS 接続アカウンティング レコードに含まれる情報の例を示します。

```
Wed Jun 27 04:28:00 2001
        NAS-IP-Address = "172.16.25.15"
        NAS-Port = 2
        User-Name = "username1"
        Client-Port-DNIS = "4327528"
        Caller-ID = "5622329477"
        Acct-Status-Type = Start
        Acct-Authentic = RADIUS
        Service-Type = Login
        Acct-Session-Id = "00000008"
        Login-Service = Telnet
```

```
        Login-IP-Host = "10.68.202.158"
        Acct-Delay-Time = 0
        User-Id = "username1"
        NAS-Identifier = "172.16.25.15"

Wed Jun 27 04:28:39 2001
        NAS-IP-Address = "172.16.25.15"
        NAS-Port = 2
        User-Name = "username1"
        Client-Port-DNIS = "4327528"
        Caller-ID = "5622329477"
        Acct-Status-Type = Stop
        Acct-Authentic = RADIUS
        Service-Type = Login
        Acct-Session-Id = "00000008"
        Login-Service = Telnet
        Login-IP-Host = "10.68.202.158"
        Acct-Input-Octets = 10774
        Acct-Output-Octets = 112
        Acct-Input-Packets = 91
        Acct-Output-Packets = 99
        Acct-Session-Time = 39
        Acct-Delay-Time = 0
        User-Id = "username1"
        NAS-Identifier = "172.16.25.15"
```

次に、発信 Telnet 接続の TACACS+ 接続アカウンティング レコードに含まれる情報の例を示します。

```
Wed Jun 27 03:47:43 2001        172.16.25.15    username1   tty3    5622329430/4327528
 start    task_id=10      service=connection      protocol=telnet addr=10.68.202.158
cmd=telnet username1-sun
Wed Jun 27 03:48:38 2001        172.16.25.15    username1   tty3    5622329430/4327528
 stop     task_id=10      service=connection      protocol=telnet addr=10.68.202.158
cmd=telnet username1-sun     bytes_in=4467   bytes_out=96    paks_in=61      paks_out=72
 elapsed_time=55
```

次に、発信 rlogin 接続の RADIUS 接続アカウンティング レコードに含まれる情報の例を示します。

```
Wed Jun 27 04:29:48 2001
        NAS-IP-Address = "172.16.25.15"
        NAS-Port = 2
        User-Name = "username1"
        Client-Port-DNIS = "4327528"
        Caller-ID = "5622329477"
        Acct-Status-Type = Start
        Acct-Authentic = RADIUS
        Service-Type = Login
        Acct-Session-Id = "0000000A"
        Login-Service = Rlogin
        Login-IP-Host = "10.68.202.158"
        Acct-Delay-Time = 0
        User-Id = "username1"
        NAS-Identifier = "172.16.25.15"

Wed Jun 27 04:30:09 2001
        NAS-IP-Address = "172.16.25.15"
        NAS-Port = 2
        User-Name = "username1"
        Client-Port-DNIS = "4327528"
        Caller-ID = "5622329477"
```

```
Acct-Status-Type = Stop
Acct-Authentic = RADIUS
Service-Type = Login
Acct-Session-Id = "0000000A"
Login-Service = Rlogin
Login-IP-Host = "10.68.202.158"
Acct-Input-Octets = 18686
Acct-Output-Octets = 86
Acct-Input-Packets = 90
Acct-Output-Packets = 68
Acct-Session-Time = 22
Acct-Delay-Time = 0
User-Id = "username1"
NAS-Identifier = "172.16.25.15"
```

次に、発信 rlogin 接続の TACACS+ 接続アカウンティング レコードに含まれる情報の例を示します。

```
Wed Jun 27 03:48:46 2001        172.16.25.15    username1   tty3    5622329430/4327528
 start    task_id=12      service=connection      protocol=rlogin addr=10.68.202.158
cmd=rlogin username1-sun /user username1
Wed Jun 27 03:51:37 2001        172.16.25.15    username1   tty3    5622329430/4327528
 stop     task_id=12      service=connection      protocol=rlogin addr=10.68.202.158
cmd=rlogin username1-sun /user username1 bytes_in=659926 bytes_out=138   paks_in=2378
  paks_
out=1251        elapsed_time=171
```

次に、発信 LAT 接続の TACACS+ 接続アカウンティング レコードに含まれる情報の例を示します。

```
Wed Jun 27 03:53:06 2001        172.16.25.15    username1   tty3    5622329430/4327528
 start    task_id=18      service=connection      protocol=lat    addr=VAX        cmd=lat
 VAX
Wed Jun 27 03:54:15 2001        172.16.25.15    username1   tty3    5622329430/4327528
 stop     task_id=18      service=connection      protocol=lat    addr=VAX        cmd=lat
 VAX  bytes_in=0      bytes_out=0     paks_in=0      paks_out=0      elapsed_time=6
```

システム アカウンティング

システム アカウンティングは、すべてのシステムレベル イベント（たとえば、システムのリブート時やアカウンティングのオン/オフ時）に関する情報を提供します。

次のアカウンティング レコードは、AAA アカウンティングがオフになったことを示す一般的な TACACS+ システム アカウンティング レコード サーバを示します。

```
Wed Jun 27 03:55:32 2001       172.16.25.15    unknown unknown unknown start   task_id=25
   service=system  event=sys_acct  reason=reconfigure
```

（注） アカウンティング パケット レコードの正確なフォーマットは、TACACS+デーモンに応じて変わります。

次のアカウンティング レコードは、AAAアカウンティングがオンになったことを示すTACACS+ システム アカウンティング レコードを示します。

```
Wed Jun 27 03:55:22 2001       172.16.25.15    unknown unknown unknown stop    task_id=23
   service=system  event=sys_acct  reason=reconfigure
```

システム リソースを測定する追加のタスクについては、他の Cisco IOS XE ソフトウェア コンフィギュレーション ガイドを参照してください。たとえば、IP アカウンティング タスクについては、『*CiscoIOS XE Application Services Configuration Guide,* Release 2』の「Configuring IP Services」を参照してください。

リソース アカウンティング

シスコが採用している AAA アカウンティングでは、ユーザー認証を通過したコールに対する「開始」レコードと「終了」レコードがサポートされます。ユーザー認証の一部として認証に失敗したコールの「終了」レコードを生成する追加機能もサポートされます。このようなレコードは、ネットワークを管理およびモニタするアカウンティング レコードを採用する場合に必要です。

ここでは、次の内容について説明します。

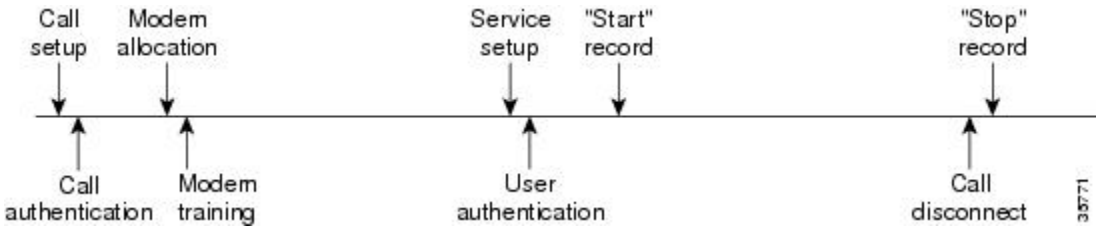
AAA リソース失敗終了アカウンティング

AAA リソース失敗終了アカウンティングの前には、コール設定シーケンスのユーザー認証段階に到達できなかったコールについて、アカウンティング レコードを提供する方式がありませんでした。このようなレコードは、ネットワークおよびその卸売りの顧客を管理およびモニターするアカウンティング レコードを採用する場合に必要です。

この機能によって、ユーザー認証に到達しなかったコールの「終了」アカウンティング レコードが生成されます。「終了」レコードは、コール設定の時点から生成されます。ユーザー認証に成功したすべてのコールは、従来と同様に動作します。つまり、追加のアカウンティング レコードは確認されません。

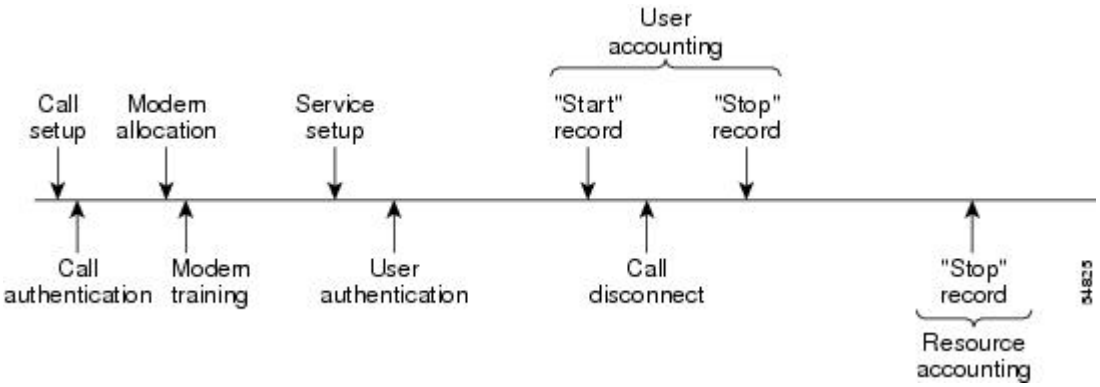
次の図に、通常のコール フローで、AAA リソース失敗終了アカウンティングを有効にしていないコール シーケンスを示します。

図 *4:* 通常のフローで *AAA* リソース失敗終了アカウンティングをイネーブルにしていないモデム ダイヤルイン コール設定シーケンス



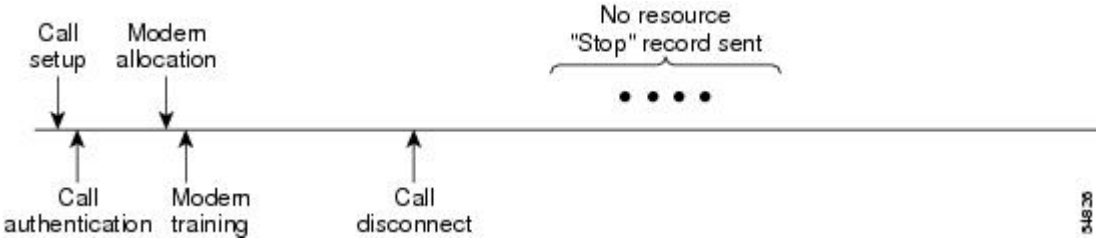
次の図に、通常のコール フローで、AAA リソース失敗終了アカウンティングをイネーブルにしたコール シーケンスを示します。

図 *5:* 通常のフローで *AAA* リソース失敗終了アカウンティングをイネーブルにしたモデム ダイヤルイン コール設定シーケンス



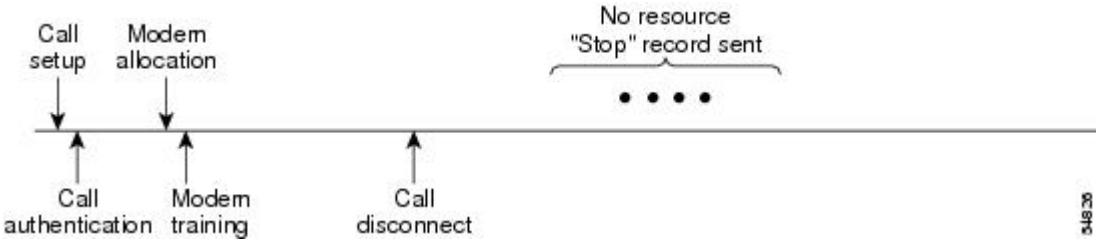
次の図に、ユーザ認証前にコールの接続解除が発生し、AAA リソース失敗終了アカウンティングをイネーブルにしたコール設定シーケンスを示します。

図 *6:* ユーザ認証前にコールの接続解除が発生し、*AAA* リソース失敗終了アカウンティングをイネーブルにしたモデム ダイヤルイン コール設定シーケンス



次の図に、ユーザ認証前にコールの接続解除が発生し、AAA リソース失敗終了アカウンティングをイネーブルにしていないコール設定シーケンスを示します。

図 *7:* ユーザ認証前にコールの接続解除が発生し、*AAA* リソース失敗終了アカウンティングをイネーブルにしていない モデム ダイヤルイン コール設定シーケンス



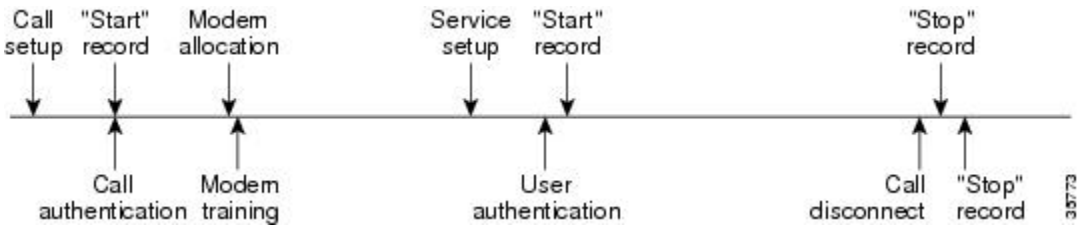
開始 - 終了レコードの AAA リソース アカウンティング

開始 - 終了レコードの AAA リソース アカウンティングは、各コール設定時に「開始」レコードを送信し、コールの接続解除時に対応する「終了」レコードを送信する機能をサポートしています。この機能は、アカウンティング レコードなどを報告するデータの発信元の 1 つから、卸売りの顧客を管理およびモニターするために使用できます。

この機能を使用すると、コール設定およびコールの接続解除の「開始 - 終了」アカウンティング レコードは、デバイスに対するリソース接続の進行状況を追跡します。個別のユーザー認証「開始 - 終了」アカウンティング レコードが、ユーザー管理の進行状況を追跡します。これら 2 セットのアカウンティング レコードは、そのコールで固有のセッション ID を使用して相互リンクされます。

次の図は、AAA リソース開始 - 終了アカウンティングを有効にしたコール設定シーケンスを示します。

図 *8:* リソース開始 - 終了アカウンティングをイネーブルにしたモデム ダイヤルイン コール設定シーケンス



AAA アカウンティングの強化

AAA ブロードキャスト アカウンティング

AAA ブロードキャスト アカウンティングを有効にすると、アカウンティング情報を複数の AAA サーバに同時に送信できます。つまり、アカウンティング情報を 1 つまた複数の AAA サーバに同時にブロードキャストすることが可能です。この機能を使用すると、サービス プロバイダーは自社使用のプライベート AAA サーバやエンドユーザの AAA サーバにアカウンティング情報を送信できるようになります。この機能では、音声アプリケーションによる課金情報も提供されます。

ブロードキャストは、RADIUS または TACACS+ サーバのグループに使用できます。また、各サーバ グループは、他のグループとは関係なく、フェールオーバーの場合のバックアップ サーバを定義できます。

したがって、サービス プロバイダーとそのエンド ユーザは、アカウンティング サーバに異なるプロトコル（RADIUS または TACACS+）を使用できます。また、サービス プロバイダーとそのエンド ユーザは、それぞれ単独でバックアップ サーバを指定することもできます。音声アプリケーションについては、独自のフェールオーバー シーケンスを持つ個別のグループを介して、冗長的なアカウンティング情報を単独で管理できます。

AAA セッション MIB

ユーザが AAA セッション MIB 機能を使用すると、簡易ネットワーク管理プロトコル（SNMP）を使用して自身の認証済みクライアント接続をモニタおよび終了できます。そのクライアントのデータが提示されるため、RADIUS または TACACS+ サーバから報告される AAA アカウンティング情報に直接関連付けることができます。AAA セッション MIB は、次の情報を提供します。

- 各 AAA 機能の統計情報（show radius statistics コマンドと併用する場合）

- AAA 機能を提供するサーバのステータス
- 外部 AAA サーバの ID
- （アイドル時間などの）リアルタイム情報（アクティブ コールを終了するかどうかを評価する SNMP ネットワークが使用する追加基準を提供します）

次の表に、認証済みクライアントと AAA セッション MIB 機能との接続をモニタおよび終了するために使用できる SNMP ユーザエンド データ オブジェクトを示します。

表 *24 : SNMP* エンドユーザ データ オブジェクト

フィールド	**Descriptions**
SessionId	AAA アカウンティング プロトコルに使用されるセッション ID（RADIUS 属性 44（Acct-Session-ID）から報告される値と同じ）
UserId	ユーザ ログイン ID または（ログインが使用できない場合）長さがゼロの文字列
IpAddr	セッションの IP アドレスまたは（IP アドレスが適用されない場合、または使用できない場合）0.0.0.0
IdleTime	セッションがアイドルになってからの経過時間
Disconnect	そのクライアントとの接続を解除するために使用されるセッション終了オブジェクト
CallId	コール トラッカー レコードが保存した、このアカウンティング セッションに対応するエントリ インデックス

次の表に、システム別に SNMP を使用する AAA セッション MIB 機能から提供される AAA の概要情報を示します。

表 *25 : SNMP AAA* セッションの概要

Field	**Descriptions**
ActiveTableEntries	現在アクティブなセッションの数
ActiveTableHighWaterMark	システムが最後に再インストールされてからの接続セッションの最大数
TotalSessions	システムが最後に再インストールされてからのセッションの合計数
DisconnectedSessions	システムが最後に再インストールされてから接続解除されたセッションの合計数

アカウンティング属性と値のペア

ネットワーク アクセス サーバは、TACACS+ 属性と値（AV）のペアまたは RADIUS 属性（実装しているセキュリティ方式によって異なります）に定義されたアカウンティング機能を監視します。

AAA アカウンティングの設定方法

名前付き方式リストによる AAA アカウンティングの設定

名前付き方式リストを使用して AAA アカウンティングを設定するには、グローバル コンフィギュレーション モードで次のコマンドを使用します。

手順の概要

1. **aaa accounting** {**system** | **network** | **exec** | **connection** | **commands** *level*} {**default** | *list-name*} {**start-stop** | **stop-only** | **none**} [*method1* [*method2...*]]
2. **line** [**aux** | **console** | **tty** | **vty**] *line-number* [*ending-line-number*]
3. **accounting** {**arap** | **commands** *level* | **connection** | **exec**} {**default** | *list-name*}

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**aaa accounting** {**system** | **network** | **exec** | **connection** | **commands** *level*} {**default** | *list-name*} {**start-stop** | **stop-only** | **none**} [*method1* [*method2...*]]	アカウンティング方式リストを作成し、アカウンティングを有効にします。引数 *list-name* は、作成したリストに名前を付けるときに使用される文字列です。
ステップ 2	**line** [**aux** | **console** | **tty** | **vty**] *line-number* [*ending-line-number*] 例： `Router(config)# interface interface-type interface-number`	アカウンティング方式リストを適用する回線のライン コンフィギュレーション モードを開始するか、アカウンティング方式リストを適用するインターフェイスのインターフェイス コンフィギュレーション モードを開始します。
ステップ 3	**accounting** {**arap** | **commands** *level* | **connection** | **exec**} {**default** | *list-name*} 例： `Router(config-if)# ppp accounting {default | list-name}`	1 つの回線または回線セットにアカウンティング方式リストを適用するか、1 つのインターフェイスまたはインターフェイスセットにアカウンティング方式リストを適用します。

次のタスク

（注） システム アカウンティングは、名前付き方式リストを使用しません。システム アカウンティングの場合、デフォルトの方式リストだけを定義します。

ヌル ユーザ名セッション時のアカウンティング レコード生成の抑制

AAA アカウンティングをアクティブにすると、Cisco IOS XE ソフトウェアは、システム上にあるすべてのユーザにアカウンティング レコードを発行します。このとき、プロトコル変換のためにユーザ名文字列がヌルのユーザも含まれます。この例では、**aaa authentication login** *method-list* **none** コマンドが適用される回線で着信するユーザがそれに該当します。関連付けられているユーザ名がないセッションについて、アカウンティング レコードが生成されないようにするには、グローバル コンフィギュレーション モードで次のコマンドを使用します。

コマンドまたはアクション	目的
`Router(config)# aaa accounting suppress null-username`	ユーザ名文字列がヌルのユーザについて、アカウンティング レコードが生成されないようにします。

中間アカウンティング レコードの生成

アカウンティング サーバに定期的な中間アカウンティング レコードを送信できるようにするには、グローバル コンフィギュレーション モードで次のコマンドを使用します。

コマンドまたはアクション	目的
`Router(config)# aaa accounting update [newinfo] [periodic] number`	アカウンティング サーバに送信される定期的中間アカウンティング レコードをイネーブルにします。

aaa accounting update コマンド をアクティブにすると、Cisco IOS XE ソフトウェアによってシステム上のすべてのユーザーの中間アカウンティングレコードが発行されます。**newinfo** キーワードを使用した場合は、レポートする新しいアカウンティング情報が発生するたびに、中間アカウンティング レコードがアカウンティング サーバーに送信されます。たとえば、インターネット プロトコル コントロール プロトコル（IPCP）がリモート ピアとの IP アドレスのネゴシエーションを完了したときにこれが発生します。中間アカウンティング レコードには、リモート ピアに使用されるネゴシエート済み IP アドレスが含まれます。

aaa accounting update コマンドを **periodic** キーワードとともに使用すると、中間アカウンティングレコードは引数の数字で定義されたとおり定期的に送信されます。中間アカウンティング レコードには、中間アカウンティング レコードが送信される時間までに、そのユーザについて記録されたすべてのアカウンティング情報が含まれます。

⚠

注意 多数のユーザがネットワークにログインしている場合には、**aaa accounting update periodic** コマンドを使用すると、重度の輻輳が発生する可能性があります。

定期的アカウンティング レコードを有効化する代替手段の設定

次の代替手段を使用して、アカウンティング サーバーに送信される定期的中間アカウンティング レコードをイネーブルにできます。

手順の概要

1. **enable**
2. **configure terminal**
3. **aaa accounting network default**
4. **action-type** {**none** | **start-stop** [**periodic** {**disable** | **interval** *minutes*}] | **stop-only**}
5. **exit**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**aaa accounting network default** 例： `Router(config)# aaa accounting network default`	すべてのネットワーク関連のサービス要求のデフォルトのアカウンティングを設定し、アカウンティング方式リストのコンフィギュレーション モードを開始します。

ステップ 4	**action-type** {**none** | **start-stop** [**periodic** {**disable** | **interval** *minutes*}] | **stop-only**}
	例：
	`Router(cfg-acct-mlist)# action-type start-stop`
	例：
	`periodic interval 5`
		アカウンティング レコードに対して実行されるアクションのタイプを指定します。
		• （任意）periodic キーワードは、定期的なアカウンティング アクションを示します。
		• interval キーワードは、定期的なアカウンティング間隔を指定します。
		• value 引数は、アカウンティング更新レコードの間隔を指定します（分単位）。

	コマンドまたはアクション	目的
		• disable キーワードは、定期的なアカウンティングをディセーブルにします。
ステップ 5	**exit** 例： `Router(cfg-acct-mlist)# exit`	グローバル コンフィギュレーション モードに戻ります。

中間サービス アカウンティング レコードの生成

このタスクを実行して、サブスクライバに対する定期的な間隔での中間サービスアカウンティング レコードの生成をイネーブルにします。

始める前に

ユーザー サービス プロファイルの RADIUS 属性 85 は設定済みの中間の間隔値よりも常に優先されます。RADIUS 属性 85 は、ユーザー サービス プロファイル内にある必要があります。詳細については、RADIUS 属性の概要および RADIUS IETF 属性の機能のドキュメントを参照してください。

（注） RADIUS 属性 85 がユーザー サービス プロファイル内にない場合、中間アカウンティング レコードの生成で設定された中間の間隔値がサービスの中間アカウンティング レコードに使用されます。

手順の概要

1. **enable**
2. **configure terminal**
3. **subscriber service accounting interim-interval** *minutes*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 3	**subscriber service accounting interim-interval** *minutes* 例： `Router(config)# subscriber service accounting interim-interval 10`	サブスクライバに対する定期的な間隔での中間サービス アカウンティング レコードの生成をイネーブルにします。*minutes* 引数は、アカウンティング更新レコードを送信する定期的な間隔を 1 ～ 71582 分で示します。

失敗したログインまたはセッションに対するアカウンティングレコードの生成

AAA アカウンティングをアクティブにすると、Cisco IOS XE ソフトウェアは、ログイン認証に失敗したシステム ユーザー、またはログイン認証には成功しても何らかの理由で PPP ネゴシエーションに失敗したユーザーのアカウンティング レコードを生成しません。

ログイン時またはセッション ネゴシエーション中の認証に失敗したユーザーについて、アカウンティング終了レコードを生成するように指定するには、グローバル コンフィギュレーション モードで次のコマンドを使用します。

コマンドまたはアクション	目的
aaa accounting send stop-record authentication failure	ログイン時またはセッション ネゴシエーション中の認証に失敗したユーザについて、「終了」レコードを生成します。

EXEC-Stop レコードよりも前のアカウンティング NETWORK-Stop レコードの指定

EXEC 終了セッションを開始する PPP ユーザーの場合、EXEC-stop レコードの前に、NETWORK レコードを生成するように指定できます。特定のサービスについて顧客に課金する場合など、状況によっては、ネットワークの開始レコードと終了レコードを一緒に保持する方が望ましいことがあります。その際、基本的に、EXEC の開始メッセージと終了メッセージのフレームワーク内に「ネスト」にします。たとえば、PPP を使用するユーザー ダイヤルインによって、EXEC-start、NETWORK-start、EXEC-stop、NETWORK-stop というレコードを作成できます。ネットワーク アカウンティング レコードをネストにすることで、NETWORK-stop レコードは NETWORK-start メッセージ（EXEC-start、NETWORK-start、NETWORK-stop、EXEC-stop）に従います。

ユーザー セッションのアカウンティング レコードをネストするには、グローバル コンフィギュレーション モードで次のコマンドを使用します。

コマンドまたはアクション	目的
aaa accounting nested	ネットワーク アカウンティング レコードをネストします。

スイッチオーバー上のシステム アカウンティング レコードの抑制

スイッチオーバー中のシステム アカウンティングオンおよびアカウンティングオフ メッセージを抑制するには、グローバル コンフィギュレーション モードで次のコマンドを使用します。

コマンドまたはアクション	目的
aaa accounting redundancy suppress system-records	スイッチオーバー中のシステム アカウンティング レコードを抑制します。

AAA リソース失敗終了アカウンティングの設定

リソース失敗終了アカウンティングをイネーブルにするには、グローバル コンフィギュレーション モードで次のコマンドを使用します。

コマンドまたはアクション	目的
aaa accounting resource *method-list* **stop-failure group** *server-group*	ユーザー認証に到達しないコールについて、「終了」レコードを生成します。 （注） AAA リソース失敗終了アカウンティング機能を設定する前に、アカウンティングを設定するための前提条件 （149 ページ） のセクションに記載されている作業を実行し、ネットワーク アクセス サーバー上でSNMP を有効にしてください。Cisco ASR 1000 シリーズ アグリゲーション サービス ルータ上で SNMP をイネーブルにする方法の詳細については、『Cisco IOS XE Network Management Configuration Guide』の「Configuring SNMP Support」の章を参照してください。

開始 - 終了レコードの AAA リソース アカウンティングの設定

開始 - 終了レコードのフル リソース アカウンティングをイネーブルにするには、グローバル コンフィギュレーション モードで次のコマンドを使用します。

コマンドまたはアクション	目的
aaa accounting resource *method-list* **start-stop group** *server-group*	各コール設定時に「開始」レコードを送信し、コールの接続解除時に対応する「終了」レコードを送信する機能をサポートします。 （注） この機能を設定する前に、アカウンティングを設定するための前提条件 （149 ページ）に記載されている作業を実行し、ネットワーク アクセス サーバ上で SNMP をイネーブルにしてください。Cisco ASR 1000 シリーズ アグリゲーション サービス ルータ上で SNMP をイネーブルにする方法の詳細については、『Cisco IOS XE Network Management Configuration Guide, Release 2』の「Configuring SNMP Support」の章を参照してください。

AAA ブロードキャスト アカウンティングの設定

AAA ブロードキャスト アカウンティングを設定するには、グローバル コンフィギュレーション モードで **aaa accounting** コマンドを使用します。このコマンドは、**broadcast** キーワードを使用できるように変更されました。

コマンドまたはアクション	目的
aaa accounting {**system** | **network** | **exec** | **connection** | **commands** *level*} {**default** | *list-name*} {**start-stop** | **stop-only** | **none**} [**broadcast**] *method1* [*method2...*]	複数の AAA サーバに対するアカウンティング レコードの送信をイネーブルにします。各グループの最初のサーバに対し、アカウンティング レコードを同時に送信します。最初のサーバが使用できない場合はフェールオーバーが発生し、そのグループ内に定義されているバックアップ サーバが使用されます。

DNIS による AAA ブロードキャスト アカウンティングの設定

AAA ブロードキャスト アカウンティングを設定するには、グローバル コンフィギュレーション モードで **aaa dnis map accounting network** コマンドを使用します。このコマンドは、**broadcast** キーワードおよび複数のサーバーグループを使用できるように変更されました。

コマンドまたはアクション	目的
aaa dnis map *dnis-number* **accounting network** [**start-stop** | **stop-only** | **none**] [**broadcast**] *method1* [*method2...*]	DNIS によるアカウンティングの設定を許可します。このコマンドは、グローバルの **aaa accounting** コマンドよりも優先されます。 複数の AAA サーバに対するアカウンティング レコードの送信をイネーブルにします。各グループの最初のサーバに対し、アカウンティング レコードを同時に送信します。最初のサーバが使用できない場合はフェールオーバーが発生し、そのグループ内に定義されているバックアップ サーバが使用されます。

AAA セッション MIB の設定

次のタスクは、次の AAA セッション MIB 機能の設定よりも前に実行する必要があります。

- SNMP を設定します。SNMP については、『Cisco IOS XE Network Management Configuration Guide』の「Configuring SNMP Support」の章を参照してください。
- AAA を設定します。
- RADIUS または TACACS+ サーバの特性を定義します。

（注） SNMP を多用すると、全体のシステム パフォーマンスに影響が出る可能性があります。そのため、この機能を使用するときに、通常のネットワーク管理パフォーマンスを考慮する必要があります。

AAA セッション MIB を設定するには、グローバル コンフィギュレーション モードで次のコマンドを使用します。

コマンドまたはアクション	目的
aaa session-mib disconnect	SNMP を使用して、認証済みクライアント接続をモニタおよび終了します。 コールを終了するには、disconnect キーワードを使用します。

AAA サーバが到達不能な場合のルータとのセッションの確立

AAA サーバが到達不能の場合に、ルータとの間にコンソール セッションを確立するには、グローバル コンフィギュレーション モードで次のコマンドを使用します。

コマンドまたはアクション	目的
no aaa accounting system guarantee-first	**aaa accounting system guarantee-first** コマンドは、システムアカウントを最初のレコードとして保証します。これは、デフォルトの条件です。 状況によっては、システムの再ロードが完了するまで（3分よりも長くかかる可能性があります）、ユーザーがコンソールまたはTelnet接続でセッションを開始できない可能性があります。この問題を解決するには、**no aaa accounting system guarantee-first** コマンドを使用します。

アカウンティングのモニタリング

RADIUS または TACACS+ アカウンティングの場合、特定の **show** コマンドは存在しません。ログインしているユーザーに関する情報を表示するアカウンティング レコードを取得するには、特権 EXEC モードで次のコマンドを使用します。

コマンドまたはアクション	目的
show accounting	ネットワークでアクティブなアカウント可能なイベントの表示を許可し、アカウンティング サーバでデータが損失した場合に情報を収集できます。

アカウンティングのトラブルシューティング

アカウンティング情報の問題を解決するには、特権 EXEC モードで次のコマンドを使用します。

コマンドまたはアクション	目的
debug aaa accounting	説明の義務があるイベントが発生したときに、その情報を表示します。

AAA アカウンティングの設定例

方式指定リストの設定の例

次に、RADIUS サーバーから AAA サービスを提供するために Cisco AS5200（AAA および RADIUSセキュリティ サーバーとの通信で有効）を設定する例を示します。RADIUS サーバーが応答に失敗すると、認証情報と認可情報についてローカルデータベースへの照会が行われ、アカウンティング サービスは TACACS+ サーバーによって処理されます。

```
aaa new-model
aaa authentication login admins local
aaa authentication ppp dialins group radius local
aaa authorization network network1 group radius local
aaa accounting network network2 start-stop group radius group tacacs+
username root password ALongPassword
tacacs-server host 172.31.255.0
tacacs-server key goaway
radius-server host 172.16.2.7
radius-server key myRaDiUSpassWoRd
interface group-async 1
 group-range 1 16
 encapsulation ppp
 ppp authentication chap dialins
 ppp authorization network1
 ppp accounting network2
line 1 16
 autoselect ppp
 autoselect during-login
 login authentication admins
 modem dialin
```

この RADIUS AAA 設定のサンプル行は、次のように定義されます。

- **aaa new-model** コマンドは、AAA ネットワーク セキュリティ サービスをイネーブルにします。
- **aaa authentication login admins local** コマンドは、ログイン認証に方式リスト「admins」を定義します。
- **aaa authentication ppp dialins group radius local** コマンドで、認証方式リスト「dialins」を定義します。このリストは、最初にRADIUS認証を指定して、次に（RADIUSサーバーが応答しない場合）PPP を使用してシリアル回線上でローカル認証が使用されます。
- **aaa authorization network network1 group radius local** コマンドで、「network1」というネットワーク許可方式リストを定義します。これにより、PPP を使用してシリアル回線上でRADIUS許可を使用するよう指定されます。RADIUS サーバーが応答に失敗すると、ローカル ネットワークの認可が実行されます。
- **aaa accounting network network2 start-stop group radius group tacacs+** コマンドで、「network2」というネットワーク アカウンティング方式リストを定義します。これにより、PPPを使用してシリアル回線上でRADIUSアカウンティングサービス（この場合、特定のイベントに対する開始レコードと終了レコード）を使用するよう指定されます。RADIUS サーバが応答に失敗すると、アカウンティングサービスは TACACS+ サーバによって処理されます。
- **username** コマンドはユーザ名とパスワードを定義します。これらの情報は、PPPパスワード認証プロトコル（PAP）の発信元身元確認に使用されます。
- **tacacs-server host** コマンドは TACACS+ サーバー ホストの名前を定義します。
- **tacacs-server key** コマンドは、ネットワーク アクセス サーバーと TACACS+ サーバー ホストの間の共有秘密テキスト文字列を定義します。
- **radius-server host** コマンドは RADIUS サーバー ホストの名前を定義します。

- **radius-server key** コマンドは、ネットワーク アクセス サーバーと RADIUS サーバー ホストの間の共有秘密テキスト文字列を定義します。
- **interface group-async** コマンドは、非同期インターフェイス グループを選択して定義します。
- **group-range** コマンドは、インターフェイス グループ内のメンバ非同期インターフェイスを定義します。
- **encapsulation ppp** コマンドは、指定のインターフェイスに使用されるカプセル化方式として PPP を設定します。
- **ppp authentication chap dialins** コマンドは、PPP 認証方式としてチャレンジハンドシェイク認証プロトコル（CHAP）を選択し、指定したインターフェイスに「dialins」方式リストを適用します。
- **ppp authorization network1** コマンドによって、blue1 ネットワーク許可方式リストが、指定したインターフェイスに適用されます。
- **ppp accounting network2** コマンドによって、red1 ネットワーク アカウンティング方式リストが、指定したインターフェイスに適用されます。
- **line** コマンドはコンフィギュレーション モードをグローバル コンフィギュレーションからライン コンフィギュレーションに切り替え、設定対象の回線を指定します。
- **autoselect ppp** コマンドは、選択した回線上で PPP セッションを自動的に開始できるように Cisco IOS XE ソフトウェアを設定します。
- **autoselect during-login** コマンドを使用すると、Return キーを押さずにユーザ名およびパスワードのプロンプトが表示されます。ユーザがログインすると、autoselect 機能（この場合は PPP）が開始します。
- **login authentication admins** コマンドは、ログイン認証に admins 方式リストを適用します。
- **modem dialin** コマンドは、選択した回線に接続されているモデムを設定し、着信コールだけを受け入れるようにします。

show accounting コマンドを使用すると、前述の設定に関する出力が次のように生成されます。

```
Active Accounted actions on tty1, User username2 Priv 1
 Task ID 5, Network Accounting record, 00:00:52 Elapsed
 task_id=5 service=ppp protocol=ip address=10.0.0.98
```

次の表に、前述の出力に含まれるフィールドについて説明します。

表 *26 : show accounting* のフィールドの説明

フィールド	説明
Active Accounted actions on	ユーザがログインに使用する端末回線またはインターフェイス名
User	ユーザの ID。

フィールド	説明
Priv	ユーザの特権レベル。
Task ID	各アカウンティング セッションの固有識別情報
Accounting Record	アカウンティング セッション タイプ
Elapsed	このセッション タイプの期間（hh:mm:ss）
attribute=value	このアカウンティング セッションに関連付けられている AV ペア

AAA リソース アカウンティングの設定の例

次に、リソース失敗終了アカウンティング、および 開始 - 終了レコード機能のリソース アカウンティングを設定する例を示します。

```
!Enable AAA on your network access server.
aaa new-model
!Enable authentication at login and list the AOL string name to use for login
authentication.
aaa authentication login AOL group radius local
!Enable authentication for ppp and list the default method to use for PPP authentication.
aaa authentication ppp default group radius local
!Enable authorization for all exec sessions and list the AOL string name to use for
authorization.
aaa authorization exec AOL group radius if-authenticated
!Enable authorization for all network-related service requests and list the default
method to use for all network-related authorizations.
aaa authorization network default group radius if-authenticated
!Enable accounting for all exec sessions and list the default method to use for all
start-stop accounting services.
aaa accounting exec default start-stop group radius
!Enable accounting for all network-related service requests and list the default method
 to use for all start-stop accounting services.
aaa accounting network default start-stop group radius
!Enable failure stop accounting.
aaa accounting resource default stop-failure group radius
!Enable resource accounting for start-stop records.
aaa accounting resource default start-stop group radius
```

AAA ブロードキャスト アカウンティングの設定の例

次に、グローバル **aaa accounting** コマンドを使用して、ブロードキャスト アカウンティングを有効にする例を示します。

```
aaa group server radius isp
 server 10.0.0.1
 server 10.0.0.2
aaa group server tacacs+ isp_customer
 server 172.0.0.1
aaa accounting network default start-stop broadcast group isp group isp_customer
radius-server host 10.0.0.1
radius-server host 10.0.0.2
```

```
radius-server key key1
tacacs-server host 172.0.0.1 key key2
```

broadcast キーワードによって、ネットワーク接続に関する「開始」および「終了」アカウンティング レコードが、グループ isp ではサーバー 10.0.0.1 に、グループ isp_customer ではサーバー 172.0.0.1 に同時送信されます。サーバ 10.0.0.1 が使用できなくなると、サーバ 10.0.0.2 へのフェールオーバーが行われます。サーバ 172.0.0.1 が使用できなくなっても、グループ isp_customer にはバックアップ サーバが設定されていないため、フェールオーバーは行われません。

DNIS による AAA ブロードキャスト アカウンティングの設定の例

次に、グローバル **aaa dnis map accounting network** コマンドを使用して、DNIS によるブロードキャスト アカウンティングを有効にする例を示します。

```
aaa group server radius isp
 server 10.0.0.1
 server 10.0.0.2
aaa group server tacacs+ isp_customer
 server 172.0.0.1
aaa dnis map enable
aaa dnis map 7777 accounting network start-stop broadcast group isp group isp_customer
radius-server host 10.0.0.1
radius-server host 10.0.0.2
radius-server key key_1
tacacs-server host 172.0.0.1 key key_2
```

broadcast キーワードによって、DNIS 番号 7777 のネットワーク接続コールに関する「開始」および「終了」アカウンティング レコードが、グループ isp ではサーバー 10.0.0.1 に、グループ isp_customer ではサーバー 172.0.0.1 に同時送信されます。サーバ 10.0.0.1 が使用できなくなると、サーバ 10.0.0.2 へのフェールオーバーが行われます。サーバ 172.0.0.1 が使用できなくなっても、グループ isp_customer にはバックアップ サーバが設定されていないため、フェールオーバーは行われません。

AAA セッション MIB の例

次に、AAA セッション MIB 機能を設定して、PPP ユーザの認証済みクライアント接続を解除する例を示します。

```
aaa new-model
aaa authentication ppp default group radius
aaa authorization network default group radius
aaa accounting network default start-stop group radius
aaa session-mib disconnect
```

その他の参考資料

ここでは、アカウンティングの設定機能に関する関連資料について説明します。

関連資料

関連項目	マニュアル タイトル
SNMP の設定	『*Cisco IOS XE Network Management Configuration Guide*』
SNMP コマンド	『*Cisco IOS Network Management Command Reference*』
セキュリティ コマンド	『*Cisco IOS Security Command Reference*』
RADIUS の設定	RADIUS の設定
TACACS+ の設定	TACACS+ の設定
IP サービスの設定	『*Cisco IOS XE Application Services Configuration Guide*』

標準

標準	タイトル
この機能でサポートされる新規の標準または変更された標準はありません。また、既存の標準のサポートは変更されていません。	--

MIB

MIB	MIB のリンク
• CISCO-AAA-SESSION-MIB	選択したプラットフォーム、Cisco IOS XE ソフトウェア リリース、および機能セットの MIB を検索してダウンロードする場合は、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

RFC

RFC	タイトル
この機能によりサポートされた新規 RFC または改訂 RFC はありません。またこの機能による既存 RFC のサポートに変更はありません。	--

シスコのテクニカル サポート

説明	リンク
シスコのサポート Web サイトでは、シスコの製品やテクノロジーに関するトラブルシューティングにお役立ていただけるように、マニュアルやツールをはじめとする豊富なオンライン リソースを提供しています。 お使いの製品のセキュリティ情報や技術情報を入手するために、Cisco Notification Service（Field Notice からアクセス）、Cisco Technical Services Newsletter、Really Simple Syndication（RSS）フィードなどの各種サービスに加入できます。 シスコのサポート Web サイトのツールにアクセスする際は、Cisco.com のユーザ ID およびパスワードが必要です。	http://www.cisco.com/en/US/support/index.html

アカウンティングの設定に関する機能情報

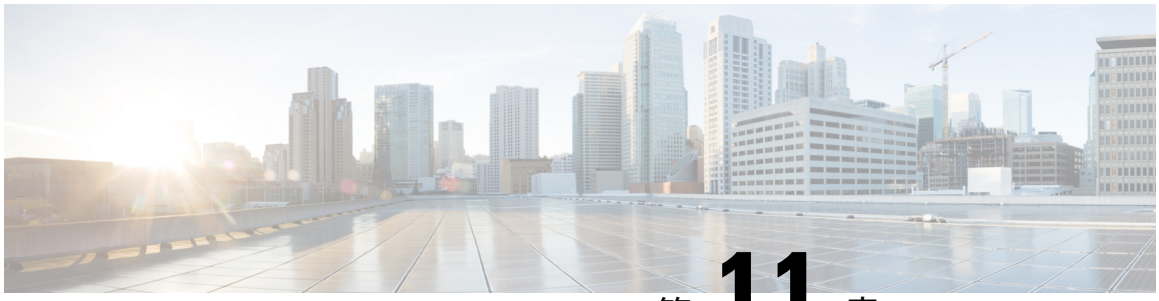
次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *27 :* アカウンティングの設定に関する機能情報

機能名	リリース	機能情報
AAA ブロードキャスト アカウンティング	Cisco IOS XE Release 2.1	AAA ブロードキャスト アカウンティングを有効にすると、アカウンティング情報を複数の AAA サーバに同時に送信できます。つまり、アカウンティング情報を 1 つまた複数の AAA サーバに同時にブロードキャストすることが可能です。 Cisco IOS XE Release 2.1 では、Cisco ASR 1000 シリーズ Aggregation Services Router にこの機能が実装されました。 次のコマンドが導入または変更されました。**aaa accounting**。

機能名	リリース	機能情報
AAAセッションMIB	Cisco IOS XE Release 2.1	ユーザがAAAセッションMIB機能を使用すると、簡易ネットワーク管理プロトコル（SNMP）を使用して自身の認証済みクライアント接続をモニタおよび終了できます。 Cisco IOS XE Release 2.1 では、Cisco ASR 1000 シリーズ Aggregation Services Router にこの機能が実装されました。 次のコマンドが導入または変更されました。**aaa session-mib disconnect**。
接続アカウンティング	Cisco IOS XE Release 2.1	接続アカウンティングは、Telnet、ローカルエリア トランスポート（LAT）、TN3270、Packet Assembler/disassembler（PAD）、rlogin など、ネットワーク アクセス サーバからの発信接続すべてに関する情報を提供します。 Cisco IOS XE Release 2.1 では、Cisco ASR 1000 シリーズ Aggregation Services Router にこの機能が実装されました。
AAA中間アカウンティング	Cisco IOS XE Release 2.4	AAA 中間アカウンティングにより、レポートする必要がある新しいアカウンティング情報が発生するたびに、または定期的に、アカウンティング サーバに中間アカウンティング レコードを送信できます。 Cisco IOS XE Release 2.4 では、Cisco ASR 1000 シリーズ Aggregation Services Router にこの機能が実装されました。 次のコマンドが導入または変更されました。**aaa accounting update** および **subscriber service accounting interim-interval**。



第 11 章

AAA-SERVER-MIB Set Operation

AAA-SERVER-MIB Set Operation 機能により、CISCO-AAA-SERVER-MIB を使用して認証、許可、アカウンティング（AAA）サーバを設定する機能を拡張できます。この機能を使用すると、次のことができます。

- 新しい AAA サーバを作成または追加する。
- CISCO-AAA-SERVER-MIB で「KEY」を修正する。
- AAA サーバの設定を削除する。

AAA-SERVER-MIB Set Operation の前提条件

AAA がルータで有効になっている必要があります。つまり、**aaa new-model** コマンドが設定されている必要があります。この設定が行われていない場合、SET 操作は失敗します。

AAA-SERVER-MIB Set Operation の制約事項

現時点では、CISCO SNMP SET 操作は RADIUS プロトコルに対してのみサポートされています。このため、追加、修正、削除できるのはグローバル コンフィギュレーション モードの RADIUS サーバだけです。

AAA-SERVER-MIB Set Operation に関する情報

CISCO-AAA-SERVER-MIB

CISCO-AAA-SERVER-MIB により、サーバ自体と AAA サーバの動作、および外部サーバとの AAA 通信の両方の状態が統計情報に反映されます。CISCO-AAA-SERVER-MIB からは次の情報が得られます。

- 各 AAA 動作の統計情報
- AAA 機能を使用できるようになっているサーバのステータス
- 外部 AAA サーバの ID

CISCO-AAA-SERVER-MIB Set Operation

Cisco IOS XE Release 2.1 では、CISCO-AAA-SERVER-MIB は GET と SET 両方の操作をサポートしています。SET 操作を使用すると、次の作業を行うことができます。

- 新しい AAA サーバを作成または追加する。
- CISCO-AAA-SERVER-MIB でキーを修正する。この「秘密キー」は、ネットワーク アクセス サーバ（NAS）および AAA サーバに存在する AAA サーバへの接続をセキュリティ保護するために使用されます。
- AAA サーバの設定を削除する。

Configure AAA-SERVER-MIB Set Operation の設定方法

この機能を使用するに当たって、特別な設定は必要ありません。簡易ネットワーク管理プロトコル（SNMP）フレームワークを使用して MIB を管理できます。SNMP の設定については、「追加情報」を参照してください。

RADIUS サーバの設定およびサーバの統計情報の確認

RADIUS サーバの設定やサーバの統計情報は、次の手順を実行することで確認できます。

手順の概要

1. **enable**
2. **show running-config | include radius-server host**
3. **show aaa servers**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**show running-config | include radius-server host** 例： `Router# show running-config | include radius-server host`	グローバル コンフィギュレーション モードで設定されているRADIUSサーバーをすべて表示します。
ステップ 3	**show aaa servers** 例： `Router# show aaa servers`	認証、許可、およびアカウンティング（AAA）サーバとの間で送受信された要求の数に関するデータを表示します。

AAA-SERVER-MIB Set Operation の設定例

RADIUS サーバの設定およびサーバの統計情報の例

次の出力例は、SET操作の前と後のRADIUSサーバの設定およびサーバの統計情報を示しています。

SET 操作の前

```
Router# show running-config | include radius-server host
! The following line is for server 1.
radius-server host 172.19.192.238 auth-port 2095 acct-port 2096 key cisco2
! The following line is for server 2.
radius-server host 172.19.192.238 auth-port 1645 acct-port 1646
```

サーバーの統計情報

```
Router# show aaa servers
RADIUS: id 2, priority 1, host 172.19.192.238, auth-port 2095, acct-port 2096
State: current UP, duration 25s, previous duration 0s
     Dead: total time 0s, count 7
Authen: request 8, timeouts 8
     Response: unexpected 0, server error 0, incorrect 0, time 0ms
     Transaction: success 0, failure 2
Author: request 0, timeouts 0
     Response: unexpected 0, server error 0, incorrect 0, time 0ms
     Transaction: success 0, failure 0
Account: request 0, timeouts 0
     Response: unexpected 0, server error 0, incorrect 0, time 0ms
```

```
     Transaction: success 0, failure 0
Elapsed time since counters last cleared: 5m
RADIUS: id 3, priority 2, host 172.19.192.238, auth-port 1645, acct-port 1646
State: current UP, duration 5s, previous duration 0s
     Dead: total time 0s, count 2
Authen: request 8, timeouts 8
     Response: unexpected 0, server error 0, incorrect 0, time 0ms
     Transaction: success 0, failure 4
Author: request 0, timeouts 0
     Response: unexpected 0, server error 0, incorrect 0, time 0ms
     Transaction: success 0, failure 0
Account: request 0, timeouts 0
     Response: unexpected 0, server error 0, incorrect 0, time 0ms
     Transaction: success 0, failure 0
Elapsed time since counters last cleared: 3m
```

RADIUS サーバの設定と統計情報をチェックする SNMP GET 操作

```
aaa-server5:/users/smetri> getmany 10.0.1.42 casConfigTable
casAddress.2.2 = 172.19.192.238
casAddress.2.3 = 172.19.192.238
casAuthenPort.2.2 = 2095
casAuthenPort.2.3 = 1645
casAcctPort.2.2 = 2096
casAcctPort.2.3 = 1646
casKey.2.2 =
casKey.2.3 =
! The following line shows priority for server 1.
casPriority.2.2 = 1
! The following line shows priority for server 2.
casPriority.2.3 = 2
casConfigRowStatus.2.2 = active(1)
casConfigRowStatus.2.3 = active(1)
aaa-server5:/users/smetri>
```

SNMP SET 操作

RADIUS サーバのキーが変更されています。また、インデックス「1」が使用されています。このインデックスは、エントリの追加、削除、修正に使用されるワイルドカードとして機能します。

```
Change the key for server 1:=>
aaa-server5:/users/smetri>  setany -v2c 10.0.1.42 public casAddress.2.1 -a 172.19.192.238
 casAuthenPort.2.1 -i 2095 casAcctPort.2.1 -i 2096 casKey.2.1 -o king
casAddress.2.1 = 172.19.192.238
casAuthenPort.2.1 = 2095
casAcctPort.2.1 = 2096
casKey.2.1 = king
aaa-server5:/users/smetri>
```

SET 操作の後

上記のSNMP SET操作後、ルータの設定が変更されます。SET操作後の出力を次に示します。

```
Router# show running-config | include radius-server host
radius-server host 172.19.192.238 auth-port 1645 acct-port 1646
! The following line shows a change in the key value to “king.”
radius-server host 172.19.192.238 auth-port 2095 acct-port 2096 key king
```

```
Router# show aaa servers
RADIUS: id 3, priority 1, host 172.19.192.238, auth-port 1645, acct-port 1646
State: current UP, duration 189s, previous duration 0s
     Dead: total time 0s, count 2
Authen: request 8, timeouts 8
     Response: unexpected 0, server error 0, incorrect 0, time 0ms
     Transaction: success 0, failure 4
Author: request 0, timeouts 0
     Response: unexpected 0, server error 0, incorrect 0, time 0ms
     Transaction: success 0, failure 0
Account: request 0, timeouts 0
     Response: unexpected 0, server error 0, incorrect 0, time 0ms
     Transaction: success 0, failure 0
Elapsed time since counters last cleared: 6m

! The following line shows a new server with new statistics.
RADIUS: id 4, priority 2, host 172.19.192.238, auth-port 2095, acct-port 2096
State: current UP, duration 209s, previous duration 0s
     Dead: total time 0s, count 7
Authen: request 0, timeouts 0
     Response: unexpected 0, server error 0, incorrect 0, time 0ms
     Transaction: success 0, failure 0
Author: request 0, timeouts 0
     Response: unexpected 0, server error 0, incorrect 0, time 0ms
     Transaction: success 0, failure 0
Account: request 0, timeouts 0
     Response: unexpected 0, server error 0, incorrect 0, time 0ms
```

その他の参考資料

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『Cisco IOS Master Command List, All Releases』
認証コマンド	『*Cisco IOS Security Command Reference*』
IEEE 802.1x-Flexible Authentication	『*Securing User Services Configuration Library*』

MIB

MIB	MIB のリンク
• CISCO-AUTH-FRAMEWORK-MIB • CISCO-MAC-AUTH-BYPASS-MIB • CISCO-PAE-MIB • IEEE8021-PAE-MIB	選択したプラットフォーム、Cisco IOS ソフトウェア リリース、およびフィーチャセットの MIB を検索してダウンロードする場合は、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

RFC

RFC	タイトル
RFC 3580	『*IEEE 802.1x Remote Authentication Dial In User Service (RADIUS)*』

シスコのテクニカル サポート

説明	リンク
右の URL にアクセスして、シスコのテクニカル サポートを最大限に活用してください。これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

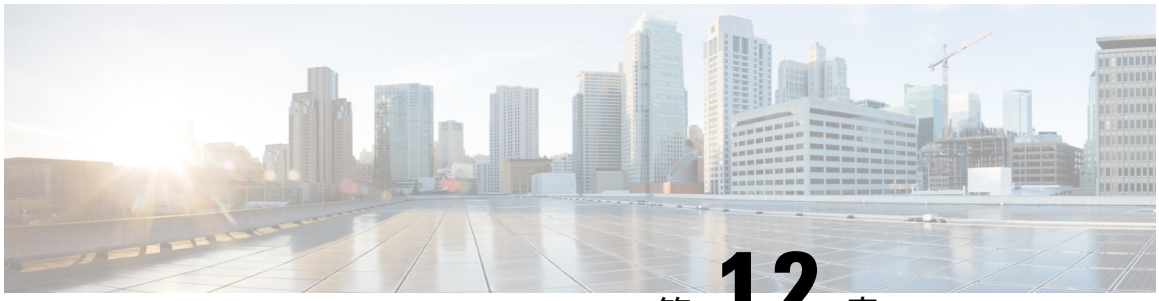
AAA-SERVER-MIB Set Operation の機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *28 : AAA-SERVER-MIB Set Operation* の機能情報

機能名	リリース	機能情報
AAA-SERVER-MIB Set Operation	Cisco IOS XE リリース 2.1	この機能は、Cisco ASR 1000 シリーズのアグリゲーション サービス ルータで導入されました。



第 12 章

Per VRF AAA

Per VRF AAA 機能により、ISP は、認証、許可、アカウンティング（AAA）サービスをバーチャル プライベート ネットワーク（VPN）ルーティング/転送（VRF）インスタンスに基づいて区分して、カスタマーに独自の AAA サービスの一部を制御させることができます。

サーバ グループのサーバ リストは、グローバル コンフィギュレーションでのホストへの参照に加えて、プライベート サーバの定義を含めるために拡張されています。このため、カスタマー サーバとグローバル サービス プロバイダーのサーバに同時にアクセスできます。

Cisco IOS XE Release 2.4 以降のリリースでは、ローカルまたはリモートで保存したカスタマー テンプレートを使用し、カスタマー テンプレートに保存された情報に基づいて、AAA サービスを実行できます。この機能は、Dynamic Per VRF AAA 機能と呼ばれています。

Per VRF AAA の前提条件

Per VRF AAA 機能を設定する前に、AAA をイネーブルにする必要があります。詳細については、6 ページの「Per VRF AAA の設定方法」を参照してください。

Per VRF AAA の制約事項

- この機能は、RADIUS サーバについてのみサポートされています。

- すべての機能について、ネットワーク アクセス サーバ（NAS）と AAA サーバとの間で一貫性が必要なため、サーバ グループごとの設定ではなく、Per VRF を設定したら、動作パラメータを定義する必要があります。
- ローカルまたはリモートでカスタマーテンプレートを設定する機能は、Cisco IOS XE Release 2.4 以降のリリースでのみ使用できます。

Per VRF AAA に関する情報

Per VRF AAA 機能を使用する場合、AAA サービスを VRF インスタンスに基づいたものにできます。この機能により、プロバイダー エッジ（PE）または仮想ホーム ゲートウェイ（VHG）で、カスタマーのバーチャルプライベート ネットワーク（VPN）に関連付けられたカスタマーの RADIUS サーバと RADIUS プロキシを経由せずに直接通信できます。RADIUS プロキシを使用する必要がないため、ISP は、VPN による提供サービスをより効率的に拡張でき、カスタマーにさらに柔軟性を提供できます。

Per VRF AAA の機能

カスタマーごとに AAA をサポートするには、一部の AAA 機能をで VRF を認識させる必要があります。つまり、ISP は、AAA サーバグループ、方式リスト、システム アカウンティング、およびプロトコル固有のパラメータなどの動作パラメータを定義し、これらのパラメータを特定の VRF インスタンスにバインドできる必要があります。動作パラメータの定義とバインディングには、次の 1 つ以上の方式が使用できます。

- バーチャル プライベート ダイヤルアップ ネットワーク（VPDN）：特定のカスタマーに設定されたに仮想テンプレートまたはダイヤラ インターフェイス。
- ローカルで定義されたカスタマーテンプレート：カスタマーの定義による Per VPN。カスタマー テンプレートは、ローカルで VHG に保存されます。この方式は、ドメイン名または着信番号識別サービス（DNIS）に基づいて、リモート ユーザを特定の VPN に関連付け、カスタマーの AAA サーバに対する仮想アクセス インターフェイスおよびすべての動作パラメータに VPN 固有の設定を提供する場合に使用できます。
- リモートで定義されたカスタマー テンプレート：RADIUS プロファイルでサービス プロバイダーの AAA サーバに保存された、カスタマーの定義による Per VPN。この方式は、ドメイン名または DNIS に基づいて、リモート ユーザを特定の VPN に関連付け、カスタマーの AAA サーバに対する仮想アクセス インターフェイスおよびすべての動作パラメータに VPN 固有の設定を提供する場合に使用できます。

（注） ローカルまたはリモートで定義されたカスタマー テンプレートを設定する機能は、Cisco IOS XE Release 2.4 以降のリリースでのみ使用できます。

AAA アカウンティング レコード

シスコが採用している AAA アカウンティングでは、ユーザー認証を通過したコールに対する「開始」レコードと「終了」レコードがサポートされます。開始レコードと終了レコードは、ユーザがアカウンティング レコードを使用してネットワークを管理およびモニタするために必要です。

新しいベンダー固有属性

インターネット技術特別調査委員会（IETF）ドラフト標準には、ネットワーク アクセス サーバと RADIUS サーバの間でベンダー固有属性（VSA）属性 26 を使用してベンダー固有の情報を伝達する方法が規定されています。属性 26 は VSA をカプセル化します。このため、ベンダーは一般的な用途に適さない独自の拡張属性をサポートできます。

シスコの RADIUS 実装は、この仕様で推奨される形式を使用して、1 つのベンダー固有オプションをサポートしています。シスコのベンダー ID は 9 であり、サポート対象のオプションはベンダータイプ 1（名前は「cisco-avpair」）です。値は、次の形式のストリングです。

```
protocol : attribute sep value *
```

「protocol」は、特定の認可タイプに使用するシスコの「protocol」属性の値です。「attribute」および「value」は、シスコの TACACS+ 仕様で定義されている適切な属性値（AV）ペアです。「sep」は、必須の属性の場合は「=」、任意指定の属性の場合は「*」です。これにより、TACACS+ 認可で使用できるすべての機能を RADIUS にも使用できるようになります。

次の表に、現在 Per VRF AAA でサポートされている VSA の概要を示します。

表 *29 : Per VRF AAA* でサポートされる *VSA*

VSA 名	**値の種類**	**説明**
（注） 別の拡張子が明示的に記述されている場合を除き、各 VSA には VSA 名の前に拡張子「template:」が必要です。		
account-delay	string	この VSA は「on」にする必要があります。この VSA の機能は、カスタマーテンプレートの **aaa accounting delay-start** コマンドと同じです。

VSA 名	値の種類	説明
account-send-stop	string	この VSA は「on」にする必要があります。この VSA の機能は、**failure** キーワードを指定した **aaa accounting send stop-record authentication** コマンドと同じです。
account-send-success-remote	string	この VSA は「on」にする必要があります。この VSA の機能は、**success** キーワードを指定した **aaa accounting send stop-record authentication** コマンドと同じです。
attr-44	string	この VSA は「access-req」にする必要があります。この VSA の機能は、**radius-server attribute 44 include-in-access-req** コマンドと同じです。
ip-addr	string	この VSA は、IP アドレスを指定します。その後に、ルータが独自の IP アドレスを示すために使用するマスク、およびクライアントとのネゴシエーションのマスクが続きます。例：ip-addr=192.168.202.169 255.255.255.255。
ip-unnumbered	string	この VSA は、ルータ上のインターフェイスの名前を指定します。この VSA の機能は、「Loopback 0」などのインターフェイス名を指定する **ip unnumbered** コマンドと同じです。
ip-vrf	string	この VSA は、エンドユーザのパケットに使用する VRF を指定します。この VRF 名は、**ip vrf forwarding** コマンドを使用してルータに使用する名前に一致させる必要があります。
peer-ip-pool	string	この VSA は、ピアに割り当てられるアドレスの IP アドレス プールの名前を指定します。このプールは、**ip local pool** コマンドを使用して設定するか、RADIUS 経由で自動的にダウンロード可能にする必要があります。

VSA 名	値の種類	説明
ppp-acct-list	string	このVSAは、PPPセッションに使用するアカウンティング方式リストを定義します。 VSA 構文は次のとおりです。「ppp-acct-list=[start-stop | stop-only | none] group X [group Y] [broadcast]」これは、**aaa accounting network mylist** コマンド機能と等しくなります。 ユーザは、start-stop、stop-only、または none オプションを少なくとも 1 つ指定する必要があります。start-stop または stop-only を指定した場合、ユーザは少なくとも 1 つ、ただし 4 つ以内のグループ引数を指定する必要があります。各グループ名は、整数で構成する必要があります。グループ内のサーバは、VSA「rad-serv」を経由して、access-accept で識別されている必要があります。各グループが指定されると、ユーザはブロードキャスト オプションを指定できます。
ppp-authen-list	string	このVSAは、PPPセッションで使用する認証方式リスト、および複数の方式が指定されている場合は、方式を使用する順序を定義します。 VSA 構文は次のとおりです。「ppp-authen-list=[groupX | local | local-case | none | if-needed]」これは、**aaa authentication ppp mylist** コマンド機能と等しくなります。 ユーザは少なくとも 1 つ、ただし 4 つ以内の認証方式を指定する必要があります。サーバ グループが指定されている場合、グループ名は整数である必要があります。グループ内のサーバは、VSA「rad-serv」を経由して、access-accept で識別されている必要があります。
ppp-authen-type	string	このVSAを使用すると、エンドユーザは、pap、chap、eap、ms-chap、ms-chap-v2、any のいずれかの認証タイプ、または使用可能なタイプをスペースで区切って、少なくとも 1 つの認証タイプを指定できます。 エンド ユーザは、この VSA で指定された方式のみを使用して、ログインが許可されます。 PPP は属性で提示された順序で、これらの認証方式を試行します。

VSA 名	値の種類	説明
ppp-author-list	string	このVSAは、PPPセッションに使用する認可方式リストを定義します。使用する方式と順序を示します。 VSA構文は次のとおりです。「ppp-author-list=[groupX] [local] [if-authenticated] [none]」これは、**aaa authorization network mylist** コマンド機能に等しくなります。 ユーザは少なくとも1つ、ただし4つ以内の認可方式を指定する必要があります。サーバグループが指定されている場合、グループ名は整数である必要があります。グループ内のサーバは、VSA「rad-serv」を経由して、access-accept で識別されている必要があります。
（注） RADIUS VSA（rad-serv、rad-serv-filter、rad-serv-source-if、およびrad-serv-vrf）は、VSA名の前にプレフィックス「aaa:」が必要です。		
rad-serv	string	このVSAは、サーバのグループとともに、IPアドレス、キー、タイムアウト、およびサーバの再送信回数を示します。 VSA構文は次のとおりです。「rad-serv=a.b.c.d [key SomeKey] [auth-port X] [acct-port Y] [retransmit V] [timeout W]」IPアドレス以外、すべてのパラメータはオプションで、任意の順序で発行できます。オプションのパラメータが指定されていない場合、デフォルト値が使用されます。 キーには、スペースを含めることはできません。「retransmit V」の「V」は、1～100の値で、「timeout W」の「W」は1～1000の値です。

VSA 名	値の種類	説明
rad-serv-filter	string	VSA 構文は次のとおりです。「rad-serv-filter=authorization | accounting-request | reply-accept | reject-filtername」filtername は **radius-server attribute list filtername** コマンドを使用して定義する必要があります。 （注） この VSA は、Cisco IOS XE Release 2.3 以降のリリースでサポートされています。
rad-serv-source-if	string	この VSA は、RADIUS パケットの送信に使用するインターフェイスの名前を指定します。指定されたインターフェイスは、ルータ上に設定されたインターフェイスと一致する必要があります。
rad-serv-vrf	string	この VSA は、RADIUS パケットの送信に使用する VRF の名前を指定します。VRF 名は、**ip vrf forwarding** コマンドを使用して指定された名前と一致する必要があります。

VRF 認識 Framed-Route

Cisco IOS XE Release 2.3 以降では、Cisco ASR 1000 シリーズ アグリゲーション サービス ルータは、VRF 認識 framed-route をサポートしています。この機能のサポートを有効にするために必要な設定はありません。framed-route は自動的に検出されます。framed-route がインターフェイスに関連付けられた VRF の一部である場合、ルートは適宜適用されます。

Per VRF AAA の設定方法

Per VRF AAA の設定

AAA の設定

AAA をイネーブルにするには、次の手順を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **aaa new-model**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**aaa new-model** 例： `Router(config)# aaa new-model`	AAA をグローバルに有効にします。

サーバ グループの設定

サーバ グループを設定するには、次の手順を実行する必要があります。

手順の概要

1. **enable**
2. **configure terminal**
3. **aaa new-model**
4. **aaa group server radius** *groupname*
5. **server-private** *ip-address* [**auth-port** *port-number* | **acct-port** *port-number*] [**non-standard**] [**timeout** *seconds*] [**retransmit** *retries*] [**key** *string*]
6. **exit**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 3	**aaa new-model** 例： `Router(config)# aaa new-model`	AAA をグローバルに有効にします。
ステップ 4	**aaa group server radius** *groupname* 例： `Router(config)# aaa group server radius v2.44.com`	複数の RADIUS サーバホストを別々のリストと別々の方式にグループ分けします。server-group コンフィギュレーション モードを開始します。
ステップ 5	**server-private** *ip-address* [**auth-port** *port-number* | **acct-port** *port-number*] [**non-standard**] [**timeout** *seconds*] [**retransmit** *retries*] [**key** *string*] 例： `Router(config-sg-radius)# server-private 10.10.130.2 auth-port 1600 key ww`	グループ サーバに対するプライベート RADIUS サーバの IP アドレスを設定します。 （注） プライベート サーバ パラメータが指定されていない場合、グローバル コンフィギュレーションが使用されます。グローバル コンフィギュレーションが指定されていない場合、デフォルト値が使用されます。
ステップ 6	**exit** 例： `Router(config-sg-radius)# exit`	server-group コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードに戻ります。

Per VRF AAA の認証、許可、アカウンティングの設定

Per VRF AAA の認証、許可、アカウンティングを設定するには、次の手順を実行する必要があります。

手順の概要

1. **enable**
2. **configure terminal**
3. **aaa new-model**
4. **aaa authentication ppp** {**default** | *list-name*} *method1* [*method2...*]
5. **aaa authorization** {**network** | **exec** | **commands** *level* | **reverse-access** | **configuration**} {**default** | *list-name*} *method1* [*method2...*]
6. **aaa accounting system default** [**vrf** *vrf-name*] {**start-stop** | **stop-only** | **none**} [**broadcast**] **group** *groupname*
7. **aaa accounting delay-start** [**vrf** *vrf-name*]
8. **aaa accounting send stop-record authentication** {**failure** | **success remote-server**} [**vrf** *vrf-name*]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**aaa new-model** 例： `Router(config)# aaa new-model`	AAA をグローバルに有効にします。
ステップ 4	**aaa authentication ppp** {**default** | *list-name*} *method1* [*method2...*] 例： `Router(config)# aaa authentication ppp method_list_v2.44.com group v2.44.com`	PPP を実行しているシリアルインターフェイス上で使用する 1 つ以上の AAA 認証方式を指定します。
ステップ 5	**aaa authorization** {**network** | **exec** | **commands** *level* | **reverse-access** | **configuration**} {**default** | *list-name*} *method1* [*method2...*] 例： `Router(config)# aaa authorization network method_list_v2.44.com group v2.44.com`	ネットワークへのユーザアクセスを制限するパラメータを設定します。
ステップ 6	**aaa accounting system default** [**vrf** *vrf-name*] {**start-stop** | **stop-only** | **none**} [**broadcast**] **group** *groupname* 例： `Router(config)# aaa accounting system default vrf v2.44.com start-stop group v2.44.com`	課金、またはRADIUSを使用する際のセキュリティのために、要求されたサービスのAAAアカウンティングをイネーブルにします。
ステップ 7	**aaa accounting delay-start** [**vrf** *vrf-name*] 例： `Router(config)# aaa acounting delay-start vrf v2.44.com`	ユーザの IP アドレスが確立されるまで、アカウンティング開始レコードの生成を表示します。
ステップ 8	**aaa accounting send stop-record authentication** {**failure** | **success remote-server**} [**vrf** *vrf-name*]	アカウンティング終了レコードを生成します。

	コマンドまたはアクション	目的
	例： `Router(config)# aaa accounting send stop-record authentication failure vrf v2.44.com`	**failure** キーワードを使用すると、認証中に拒否されたコールに対する「終了」レコードが送信されます。 **success** キーワードを使用すると、次のいずれかの基準を満たすコールに対して、「終了」レコードが送信されます。 • コールが終了したときに、リモート AAA サーバによって認証されるコール。 • リモート AAA サーバによって認証されず、開始レコードが送信されたコール。 • 正常に確立され、「stop-only」**aaa accounting** 設定で終了したコール。 （注） **success** および **remote-server** キーワードは、Cisco IOS XE Release 2.4 以降のリリースで使用できます。

Per VRF AAA の RADIUS 固有のコマンドの設定

Per VRF AAA の RADIUS 固有のコマンドを設定するには、次の手順を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **ip radius source-interface** *subinterface-name* [**vrf** *vrf-name*]
4. **radius-server attribute 44 include-in-access-req** [**vrf** *vrf-name*]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 3	**ip radius source-interface** *subinterface-name* [**vrf** *vrf-name*] 例： `Router(config)# ip radius source-interface loopback55`	すべての発信 RADIUS パケットに対して、RADIUS に指定されたインターフェイスの IP アドレスを強制的に使用させ、Per VRF に基づいて仕様をイネーブルにします。
ステップ 4	**radius-server attribute 44 include-in-access-req** [**vrf** *vrf-name*] 例： `Router(config)# radius-server attribute 44 include-in-access-req vrf v2.44.com`	ユーザ認証前に、アクセス要求パケットで、RADIUS 属性 44 を送信し、Per VRF に基づいて仕様を有効にします。

Per VRF AAA のインターフェイス固有のコマンドの設定

Per VRF AAA のインターフェイス固有のコマンドを設定するには、次の手順を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **interface** *type number* [*name-tag*]
4. **ip vrf forwarding** *vrf-name*
5. **ppp authentication** {*protocol1* [*protocol2...*]} *listname*
6. **ppp authorization** *list-name*
7. **ppp accounting default**
8. **exit**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface** *type number* [*name-tag*] 例：	インターフェイス タイプを設定し、インターフェイス コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
	`Router(config)# interface loopback11`	
ステップ 4	**ip vrf forwarding** *vrf-name* 例： `Router(config-if)# ip vrf forwarding v2.44.com`	インターフェイスと VRF を関連付けます。
ステップ 5	**ppp authentication** {*protocol1* [*protocol2...*]} *listname* 例： `Router(config-if)# ppp authentication chap callin V2_44_com`	チャレンジハンドシェイク認証プロトコル（CHAP）およびパスワード認証プロトコル（PAP）のいずれかまたは両方をイネーブルにし、CHAP および PAP 認証がインターフェイスで選択される順序を指定します。
ステップ 6	**ppp authorization** *list-name* 例： `Router(config-if)# ppp authorization V2_44_com`	選択したインターフェイスで、AAA認可をイネーブルにします。
ステップ 7	**ppp accounting default** 例： `Router(config-if)# ppp accounting default`	選択したインターフェイスで、AAAアカウンティング サービスをイネーブルにします。
ステップ 8	**exit** 例： `Router(config)# exit`	インターフェイス コンフィギュレーション モードを終了します。

ローカル カスタマー テンプレートを使用した Per VRF AAA の設定

AAA の設定

「Per VRF AAA の設定」で説明する作業を実行します。

サーバ グループの設定

「サーバ グループの設定」で説明する作業を実行します。

Per VRF AAA の認証、許可、アカウンティングの設定

「Per VRF AAA の認証、許可、アカウンティングの設定」で説明する作業を実行します。

ローカル カスタマー テンプレートを使用した Per VRF AAA の認可の設定

ローカル テンプレートを使用した Per VRF AAA の認可を設定するには、次の手順を実行する必要があります。

手順の概要

1. **enable**
2. **configure terminal**
3. **aaa authorization template**
4. **aaa authorization network default local**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**aaa authorization template** 例： `Router(config)# aaa authorization template`	ローカルまたはリモート テンプレートの使用をイネーブルにします。
ステップ 4	**aaa authorization network default local** 例： `Router(config)# aaa authorization network default local`	ローカルを認可のデフォルト方式として指定します。

ローカル カスタマー テンプレートの設定

ローカル カスタマー テンプレートを設定するには、次の手順を実行する必要があります。

手順の概要

1. **enable**
2. **configure terminal**
3. **vpdn search-order domain**
4. **template** *name* [**default** | **exit** | **multilink** | **no** | **peer** | **ppp**]
5. **peer default ip address pool** *pool-name*

6. **ppp authentication** {*protocol1* [*protocol2...*]} [**if-needed**] [*list-name* | **default**] [**callin**] [**one-time**]
7. **ppp authorization** [**default** | *list-name*]
8. **aaa accounting** {**auth-proxy** | **system** | **network** | **exec** | **connection** | **commands** *level*} {**default** | *list-name*} [**vrf** *vrf-name*] {**start-stop** | **stop-only** | **none**} [**broadcast**] **group** *groupname*
9. **exit**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**vpdn search-order domain** 例： `Router (config)# vpdn search-order domain`	ドメインに基づいてプロファイルを検索します。
ステップ 4	**template** *name* [**default** | **exit** | **multilink** | **no** | **peer** | **ppp**] 例： `Router (config)# template v2.44.com`	カスタマー プロファイル テンプレートを作成し、受信先のカスタマーに関連する一意の名前を割り当てます。 テンプレート コンフィギュレーション モードを開始します。 （注） ステップ 5、6、および 7 はオプションです。カスタマーアプリケーション要件に適した **multilink**、**peer**、および **ppp** キーワードを入力します。
ステップ 5	**peer default ip address pool** *pool-name* 例： `Router(config-template)# peer default ip address pool v2_44_com_pool`	（任意）このテンプレートの添付先のカスタマープロファイルが、指定した名前のローカル IP アドレスプールを使用するように指定します。
ステップ 6	**ppp authentication** {*protocol1* [*protocol2...*]} [**if-needed**] [*list-name* | **default**] [**callin**] [**one-time**] 例： `Router(config-template)# ppp authentication chap`	（任意）PPP リンク認証方式を設定します。

	コマンドまたはアクション	目的
ステップ 7	**ppp authorization** [**default** | *list-name*] 例： `Router(config-template)# ppp authorization v2_44_com`	（任意）PPP リンク認可方式を設定します。
ステップ 8	**aaa accounting** {**auth-proxy** | **system** | **network** | **exec** | **connection** | **commands** *level*} {**default** | *list-name*} [**vrf** *vrf-name*] {**start-stop** | **stop-only** | **none**} [**broadcast**] **group** *groupname* 例： `Router(config-template)# aaa accounting v2_44_com`	（任意）指定したカスタマープロファイルで、AAA 動作パラメータをイネーブルにします。
ステップ 9	**exit** 例： `Router(config-template)# exit`	テンプレート コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードに戻ります。

リモート カスタマー テンプレートを使用した Per VRF AAA の設定

AAA の設定

「Per VRF AAA の設定」で説明する作業を実行します。

サーバ グループの設定

「サーバ グループの設定」で説明する作業を実行します。

リモート カスタマー プロファイルを使用した Per VRF AAA の認証の設定

リモート カスタマー プロファイルを使用した Per VRF AAA の認証を設定するには、次の手順を実行する必要があります。

手順の概要

1. **enable**
2. **configure terminal**
3. **aaa authentication ppp** {**default** | *list-name*} *method1* [*method2...*]
4. **aaa authorization** {**network** | **exec** | **commands** *level* | **reverse-access** | **configuration**} {**default** | *list-name*} [[*method1* [*method2...*]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**aaa authentication ppp** {**default** | *list-name*} *method1* [*method2...*] 例： `Router(config)# ppp authentication ppp default group radius`	PPP を実行するシリアル インターフェイス上で使用する 1 つ以上の認証、許可、アカウンティング（AAA）認証方式を指定します。
ステップ 4	**aaa authorization** {**network** | **exec** | **commands** *level* | **reverse-access** | **configuration**} {**default** | *list-name*} [[*method1* [*method2...*] 例： `Router(config)# aaa authorization network default group sp`	ネットワークへのユーザアクセスを制限するパラメータを設定します。

リモート カスタマー プロファイルを使用した Per VRF AAA の認可の設定

リモート カスタマー プロファイルを使用した Per VRF AAA の認可を設定するには、次の手順を実行する必要があります。

手順の概要

1. **enable**
2. **configure terminal**
3. **aaa authorization template**
4. **aaa authorization** {**network** \| **exec** \| **commands** *level* \| **reverse-access** \| **configuration**} {**default** \| *list-name*} [[*method1* [*method2...*]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例：	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。

	コマンドまたはアクション	目的
	`Router> enable`	
ステップ 2	**configure terminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**aaa authorization template** 例： `Router(config)# aaa authorization template`	ローカルまたはリモート テンプレートの使用をイネーブルにします。
ステップ 4	**aaa authorization** {**network** | **exec** | **commands** *level* | **reverse-access** | **configuration**} {**default** | *list-name*} [[*method1* [*method2...*] 例： `Router(config)# aaa authorization network default sp`	認可のデフォルト方式として指定されたサーバ グループを指定します。

SP RADIUS サーバ上の RADIUS プロファイルの設定

サービスプロバイダー（SP）RADIUSサーバ上でRADIUSプロファイルを設定します。RADIUSプロファイルを更新する方法の例については、「リモート RADIUS カスタマー テンプレートを使用した Per VRF AAA の例」を参照してください。

VRF ルーティングの設定確認

VRF のルーティング設定を確認するには、次の手順を実行する必要があります。

手順の概要

1. **enable**
2. **configure terminal**
3. show ip route vrf *vrf-name*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。

	コマンドまたはアクション	目的
ステップ 2	**configure terminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	show ip route vrf *vrf-name* 例： `Router(config)# show ip route vrf northvrf`	VRF に関連付けられた IP ルーティング テーブルを表示します。

Per VRF AAA 設定のトラブルシューティング

Per VRF AAA 機能の問題を解決するには、EXEC モードで次のコマンドを少なくとも 1 つ使用します。

コマンド	目的
`Router# debug aaa accounting`	説明の義務があるイベントが発生したときに、その情報を表示します。
`Router# debug aaa authentication`	AAA 認証に関する情報を表示します。
`Router# debug aaa authorization`	AAA 認可に関する情報を表示します。
`Router# debug ppp negotiation`	PPP を実装するインターネットワークでのトラフィックおよび交換に関する情報を表示します。
`Router# debug radius`	RADIUS 関連の情報を表示します。
`Router# debug vpdn event`	VPN の通常のトンネルの確立、またはシャットダウンの一部であるレイヤ 2 プロトコル（L2TP）のエラーおよびイベントを表示します。
`Router# debug vpdn error`	VPN のデバッグ トレースを表示します。

Per VRF AAA の設定例

Per VRF の設定の例

Per VRF AAA の例

次に、関連付けられたプライベート サーバで AAA サーバ グループを使用して Per VRF AAA 機能を設定する方法の例を示します。

```
aaa new-model
aaa authentication ppp method_list_v1.55.com group v1.55.com
aaa authorization network method_list_v1.55.com group v1.55.com
aaa accounting network method_list_v1.55.com start-stop group v1.55.com
aaa accounting system default vrf v1.55.com start-stop group v1.55.com
aaa accounting delay-start vrf v1.55.com
aaa accounting send stop-record authentication failure vrf v1.55.com
aaa group server radius v1.55.com
    server-private 10.10.132.4 auth-port 1645 acct-port 1646 key ww
    ip vrf forwarding v1.55.com
ip radius source-interface loopback55
radius-server attribute 44 include-in-access-req vrf v1.55.com
```

ローカルで定義されたカスタマー テンプレートを使用した Per VRF AAA の例

次に、関連付けられたプライベート サーバのある AAA サーバ グループで、ローカルで定義されたカスタマー テンプレートを使用して Per VRF AAA 機能を設定する方法の例を示します。

```
aaa new-model
aaa authentication ppp method_list_v1.55.com group v1.55.com
aaa authorization network method_list_v1.55.com group v1.55.com
aaa authorization network default local
aaa authorization template
aaa accounting network method_list_v1.55.com start-stop group v1.55.com
aaa accounting system default vrf v1.55.com start-stop group v1.55.com
aaa group server radius V1_55_com
  server-private 10.10.132.4 auth-port 1645 acct-port 1646 key ww
  ip vrf forwarding V1.55.com
template V1.55.com
  peer default ip address pool V1_55_com_pool
  ppp authentication chap callin V1_55_com
  ppp authorization V1_55_com
  ppp accounting V1_55_com
  aaa accounting delay-start
  aaa accounting send stop-record authentication failure
  radius-server attribute 44 include-in-access-req
  ip vrf forwarding v1.55.com
  ip radius source-interface Loopback55
```

リモート RADIUS カスタマー テンプレートを使用した Per VRF AAA の例

次に、関連付けられたプライベート サーバのある AAA サーバ グループで、SP RADIUS サーバ上にリモートで定義したカスタマー テンプレートを使用して Per VRF AAA 機能を設定する方法の例を示します。

```
aaa new-model
aaa authentication ppp default group radius
aaa authorization template
aaa authorization network default group sp
aaa group server radius sp
   server 10.3.3.3
radius-server host 10.3.3.3 auth-port 1645 acct-port 1646 key sp_key
```

次の RADIUS サーバ プロファイルは、SP RADIUS サーバ上で設定されます。

```
cisco-avpair = "aaa:rad-serv#1=10.10.132.4 key ww"
cisco-avpair = "aaa:rad-serv-vrf#1=V1.55.com"
cisco-avpair = "aaa:rad-serv-source-if#1=Loopback 55"
cisco-avpair = "template:ppp-authen-list=group 1"
cisco-avpair = "template:ppp-author-list=group 1"
cisco-avpair = "template:ppp-acct-list= start-stop group 1"
cisco-avpair = "template:account-delay=on"
cisco-avpair = "template:account-send-stop=on"
cisco-avpair = "template:rad-attr44=access-req"
cisco-avpair = "template:peer-ip-pool=V1.55-pool"
cisco-avpair = "template:ip-vrf=V1.55.com"
cisco-avpair = "template:ip-unnumbered=Loopback 55"
framed-protocol = ppp
service-type = framed
```

カスタマー テンプレートの例

RADIUS Attribute Screening およびブロードキャスト アカウンティングを使用してローカルで設定されたカスタマー テンプレートの例

次に、RADIUS Attribute Screening およびブロードキャスト アカウンティングを含む追加機能を設定する、単一のカスタマー向けにローカルで設定されたテンプレートを作成する方法の例を示します。

```
aaa authentication ppp default local group radius
aaa authentication ppp V1_55_com group V1_55_com
aaa authorization template
aaa authorization network default local group radius
aaa authorization network V1_55_com group V1_55_com
aaa accounting network V1_55_com start-stop broadcast group V1_55_com group SP_AAA_server
aaa group server radius SP_AAA_server
 server 10.10.100.7 auth-port 1645 acct-port 1646
aaa group server radius V1_55_com
 server-private 10.10.132.4 auth-port 1645 acct-port 1646
 authorization accept min-author
 accounting accept usage-only
 ip vrf forwarding V1.55.com
ip vrf V1.55.com
 rd 1:55
 route-target export 1:55
```

```
 route-target import 1:55
template V1.55.com
 peer default ip address pool V1.55-pool
 ppp authentication chap callin V1_55_com
 ppp authorization V1_55_com
 ppp accounting V1_55_com
 aaa accounting delay-start
 aaa accounting send stop-record authentication failure
 radius-server attribute 44 include-in-access-req
vpdn-group V1.55
 accept-dialin
  protocol l2tp
  virtual-template 13
 terminate-from hostname lac-lb-V1.55
 source-ip 10.10.104.12
 lcp renegotiation always
 l2tp tunnel password 7 060506324F41
interface Virtual-Template13
 ip vrf forwarding V1.55.com
 ip unnumbered Loopback55
 ppp authentication chap callin
 ppp multilink
ip local pool V1.55-pool 10.1.55.10 10.1.55.19 group V1.55-group
ip radius source-interface Loopback0
ip radius source-interface Loopback55 vrf V1.55.com
radius-server attribute list min-author
 attribute 6-7,22,27-28,242
radius-server attribute list usage-only
 attribute 1,40,42-43,46
radius-server host 10.10.100.7 auth-port 1645 acct-port 1646 key ww
radius-server host 10.10.132.4 auth-port 1645 acct-port 1646 key ww
```

RADIUS Attribute Screening およびブロードキャスト アカウンティングを使用してリモートで設定されたカスタマー テンプレートの例

次に、RADIUS Attribute Screening およびブロードキャスト アカウンティングを含む追加機能を設定する、単一のカスタマー向けにリモートで設定されたテンプレートを作成する方法の例を示します。

```
aaa authentication ppp default local group radius
aaa authorization template
aaa authorization network default local group radius
ip vrf V1.55.com
 rd 1:55
 route-target export 1:55
 route-target import 1:55
vpdn-group V1.55
 accept-dialin
  protocol l2tp
  virtual-template 13
 terminate-from hostname lac-lb-V1.55
 source-ip 10.10.104.12
 lcp renegotiation always
 l2tp tunnel password 7 060506324F41
interface Virtual-Template13
 no ip address
 ppp authentication chap callin
 ppp multilink
ip local pool V1.55-pool 10.1.55.10 10.1.55.19 group V1.55-group
radius-server attribute list min-author
 attribute 6-7,22,27-28,242
```

```
radius-server attribute list usage-only
 attribute 1,40,42-43,46
```

カスタマーテンプレートは、v1.55.com の RADIUS サーバプロファイルとして保存されます。

```
cisco-avpair = "aaa:rad-serv#1=10.10.132.4 key ww"
cisco-avpair = "aaa:rad-serv-vrf#1=V1.55.com"
cisco-avpair = "aaa:rad-serv-source-if#1=Loopback 55"
cisco-avpair = "aaa:rad-serv#2=10.10.100.7 key ww"
cisco-avpair = "aaa:rad-serv-source-if#2=Loopback 0"
cisco-avpair = "template:ppp-authen-list=group 1"
cisco-avpair = "template:ppp-author-list=group 1"
cisco-avpair = "template:ppp-acct-list= start-stop group 1 group 2 broadcast"
cisco-avpair = "template:account-delay=on"
cisco-avpair = "template:account-send-stop=on"
cisco-avpair = "template:rad-attr44=access-req"
cisco-avpair = "aaa:rad-serv-filter#1=authorization accept min-author"
cisco-avpair = "aaa:rad-serv-filter#1=accounting accept usage-only"
cisco-avpair = "template:peer-ip-pool=V1.55-pool"
cisco-avpair = "template:ip-vrf=V1.55.com"
cisco-avpair = "template:ip-unnumbered=Loopback 55"
framed-protocol = ppp
service-type = framed
```

AAA アカウンティング終了レコードの例

次に、**start-stop** または **stop-only** キーワードを指定して **aaa accounting** コマンドを発行したときに、「終了」レコードの生成を制御する **aaa accounting send stop-record authentication** コマンドを設定する方法を示す、AAA アカウンティング終了レコードの例を示します。

（注） **success** および **remote-server** キーワードは、Cisco IOS XE Release 2.4 以降のリリースで使用できます。

AAA アカウンティング終了レコードと拒否されたコールの例

次に、**aaa accounting send stop-record authentication** コマンドを **success** キーワードを指定して発行した場合に、認証中に拒否されたコールに関する「終了」レコードが送信されている例を示します。

```
Router# show running-config | include aaa
.
.
.
aaa new-model
aaa authentication ppp default group radius
aaa authorization network default local
aaa accounting send stop-record authentication success remote-server
aaa accounting network default start-stop group radius
Router#
*Jul  7 03:39:40.199: AAA/BIND(00000026): Bind i/f Virtual-Template2
*Jul  7 03:39:40.199: ppp21 AAA/AUTHOR/LCP: Authorization succeeds trivially
*Jul  7 03:39:42.199: RADIUS/ENCODE(00000026):Orig. component type = PPoE
*Jul  7 03:39:42.199: RADIUS:  AAA Unsupported     [156] 7
*Jul  7 03:39:42.199: RADIUS:   30 2F 30 2F
```

```
30                                  [0/0/0]
*Jul  7 03:39:42.199: RADIUS(00000026): Config NAS IP: 10.0.0.0
*Jul  7 03:39:42.199: RADIUS/ENCODE(00000026): acct_session_id: 55
*Jul  7 03:39:42.199: RADIUS(00000026): sending
*Jul  7 03:39:42.199: RADIUS/ENCODE: Best Local IP-Address 10.0.1.123 for
Radius-Server 172.19.192.238
*Jul  7 03:39:42.199: RADIUS(00000026): Send Access-Request to
172.19.192.238:2195 id 1645/14, len 94
*Jul  7 03:39:42.199: RADIUS:  authenticator A6 D1 6B A4 76 9D 52 CF - 33 5D
16 BE AC 7E 5F A6
*Jul  7 03:39:42.199: RADIUS:  Framed-Protocol     [7]   6
PPP                         [1]
*Jul  7 03:39:42.199: RADIUS:  User-Name           [1]   16  "user@example.com"
*Jul  7 03:39:42.199: RADIUS:  CHAP-Password       [3]   19  *
*Jul  7 03:39:42.199: RADIUS:  NAS-Port-Type       [61]  6
Virtual                     [5]
*Jul  7 03:39:42.199: RADIUS:  NAS-Port            [5]   6
0
*Jul  7 03:39:42.199: RADIUS:  NAS-Port-Id         [87]  9   "0/0/0/0"
*Jul  7 03:39:42.199: RADIUS:  Service-Type        [6]   6
Framed                      [2]
*Jul  7 03:39:42.199: RADIUS:  NAS-IP-Address      [4]   6
10.0.1.123
*Jul  7 03:39:42.271: RADIUS: Received from id 1645/14 172.19.192.238:2195,
Access-Accept, len 194
*Jul  7 03:39:42.271: RADIUS:  authenticator 30 AD FF 8E 59 0C E4 6C - BA 11
23 63 81 DE 6F D7
*Jul  7 03:39:42.271: RADIUS:  Framed-Protocol     [7]   6
PPP                         [1]
*Jul  7 03:39:42.275: RADIUS:  Service-Type        [6]   6
Framed                      [2]
*Jul  7 03:39:42.275: RADIUS:  Vendor, Cisco       [26]  26
*Jul  7 03:39:42.275: RADIUS:   Cisco AVpair       [1]   20  "vpdn:tunnel-
id=lac"
*Jul  7 03:39:42.275: RADIUS:  Vendor, Cisco       [26]  29
*Jul  7 03:39:42.275: RADIUS:   Cisco AVpair       [1]   23  "vpdn:tunnel-
type=l2tp"
*Jul  7 03:39:42.275: RADIUS:  Vendor, Cisco       [26]  30
*Jul  7 03:39:42.275: RADIUS:   Cisco AVpair       [1]   24  "vpdn:gw-
password=cisco"
*Jul  7 03:39:42.275: RADIUS:  Vendor, Cisco       [26]  31
*Jul  7 03:39:42.275: RADIUS:   Cisco AVpair       [1]   25  "vpdn:nas-
password=cisco"
*Jul  7 03:39:42.275: RADIUS:  Vendor, Cisco       [26]  34
*Jul  7 03:39:42.275: RADIUS:   Cisco AVpair       [1]   28  "vpdn:ip-
addresses=10.0.0.2"
*Jul  7 03:39:42.275: RADIUS:  Service-Type        [6]   6
Framed                      [2]
*Jul  7 03:39:42.275: RADIUS:  Framed-Protocol     [7]   6
PPP                         [1]
*Jul  7 03:39:42.275: RADIUS(00000026): Received from id 1645/14
*Jul  7 03:39:42.275: ppp21 PPP/AAA: Check Attr: Framed-Protocol
*Jul  7 03:39:42.275: ppp21 PPP/AAA: Check Attr: service-type
*Jul  7 03:39:42.275: ppp21 PPP/AAA: Check Attr: tunnel-id
*Jul  7 03:39:42.275: ppp21 PPP/AAA: Check Attr: tunnel-type
*Jul  7 03:39:42.275: ppp21 PPP/AAA: Check Attr: gw-password
*Jul  7 03:39:42.275: ppp21 PPP/AAA: Check Attr: nas-password
*Jul  7 03:39:42.275: ppp21 PPP/AAA: Check Attr: ip-addresses
*Jul  7 03:39:42.275: ppp21 PPP/AAA: Check Attr: service-type
*Jul  7 03:39:42.275: ppp21 PPP/AAA: Check Attr: Framed-Protocol
*Jul  7 03:39:42.279: AAA/BIND(00000027): Bind i/f
*Jul  7 03:39:42.279:  Tnl 21407 L2TP: O SCCRQ
*Jul  7 03:39:42.279:  Tnl 21407 L2TP: O SCCRQ, flg TLS, ver 2, len 134, tnl
0, ns 0, nr 0
```

```
         C8 02 00 86 00 00 00 00 00 00 00 80 08 00 00
         00 00 00 01 80 08 00 00 00 02 01 00 00 08 00 00
         00 06 11 30 80 09 00 00 00 07 6C 61 63 00 19 00
         00 00 08 43 69 73 63 6F 20 53 79 73 74 65 6D 73
         2C 20 49 6E 63 2E 80 ...
*Jul  7 03:39:49.279:  Tnl 21407 L2TP: O StopCCN
*Jul  7 03:39:49.279:  Tnl 21407 L2TP: O StopCCN, flg TLS, ver 2, len 66, tnl
0, ns 1, nr 0
         C8 02 00 42 00 00 00 00 00 01 00 00 80 08 00 00
         00 00 00 04 80 1E 00 00 00 01 00 02 00 06 54 6F
         6F 20 6D 61 6E 79 20 72 65 74 72 61 6E 73 6D 69
         74 73 00 08 00 09 00 69 00 01 80 08 00 00 00 09
         53 9F
*Jul  7 03:39:49.279: RADIUS/ENCODE(00000026):Orig. component type = PPoE
*Jul  7 03:39:49.279: RADIUS(00000026): Config NAS IP: 10.0.0.0
*Jul  7 03:39:49.279: RADIUS(00000026): sending
*Jul  7 03:39:49.279: RADIUS/ENCODE: Best Local IP-Address 10.0.1.123 for
Radius-Server 172.19.192.238
*Jul  7 03:39:49.279: RADIUS(00000026): Send Accounting-Request to
172.19.192.238:2196 id 1646/32, len 179
*Jul  7 03:39:49.279: RADIUS:  authenticator 0A 85 2F F0 65 6F 25 E1 - 97 54
CC BF EA F7 62 89
*Jul  7 03:39:49.279: RADIUS:  Acct-Session-Id     [44]  10  "00000037"
*Jul  7 03:39:49.279: RADIUS:  Framed-Protocol     [7]   6
PPP                       [1]
*Jul  7 03:39:49.279: RADIUS:  Tunnel-Medium-Type  [65]  6
00:IPv4                   [1]
*Jul  7 03:39:49.279: RADIUS:  Tunnel-Client-Endpoi[66]  10  "10.0.0.1"
*Jul  7 03:39:49.279: RADIUS:  Tunnel-Server-Endpoi[67]  10  "10.0.0.2"
*Jul  7 03:39:49.283: RADIUS:  Tunnel-Type         [64]  6
00:L2TP                   [3]
*Jul  7 03:39:49.283: RADIUS:  Acct-Tunnel-Connecti[68]  3   "0"
*Jul  7 03:39:49.283: RADIUS:  Tunnel-Client-Auth-I[90]  5   "lac"
*Jul  7 03:39:49.283: RADIUS:  User-Name           [1]   16  "user@example.com"
*Jul  7 03:39:49.283: RADIUS:  Acct-Authentic      [45]  6
RADIUS                    [1]
*Jul  7 03:39:49.283: RADIUS:  Acct-Session-Time   [46]  6
0
*Jul  7 03:39:49.283: RADIUS:  Acct-Input-Octets   [42]  6
0
*Jul  7 03:39:49.283: RADIUS:  Acct-Output-Octets  [43]  6
0
*Jul  7 03:39:49.283: RADIUS:  Acct-Input-Packets  [47]  6
0
*Jul  7 03:39:49.283: RADIUS:  Acct-Output-Packets [48]  6
0
*Jul  7 03:39:49.283: RADIUS:  Acct-Terminate-Cause[49]  6   nas-
error                  [9]
*Jul  7 03:39:49.283: RADIUS:  Acct-Status-Type    [40]  6
Stop                      [2]
*Jul  7 03:39:49.283: RADIUS:  NAS-Port-Type       [61]  6
Virtual                   [5]
*Jul  7 03:39:49.283: RADIUS:  NAS-Port            [5]   6
0
*Jul  7 03:39:49.283: RADIUS:  NAS-Port-Id         [87]  9   "0/0/0/0"
*Jul  7 03:39:49.283: RADIUS:  Service-Type        [6]   6
Framed                    [2]
*Jul  7 03:39:49.283: RADIUS:  NAS-IP-Address      [4]   6
10.0.1.123
*Jul  7 03:39:49.283: RADIUS:  Acct-Delay-Time     [41]  6
0
*Jul  7 03:39:49.335: RADIUS: Received from id 1646/32 172.19.192.238:2196,
Accounting-response, len 20
```

```
*Jul  7 03:39:49.335: RADIUS:  authenticator C8 C4 61 AF 4D 9F 78 07 - 94 2B
44 44 17 56 EC 03
```

AAA アカウンティング終了レコードと成功したコールの例

次に、**aaa accounting send stop-record authentication** コマンドを **failure** キーワードを指定して発行した場合に、成功したコールに関する「開始」および「終了」レコードが送信されている例を示します。

```
Router# show running-config | include aaa

.
.
.
aaa new-model
aaa authentication ppp default group radius
aaa authorization network default local
aaa accounting send stop-record authentication failure
aaa accounting network default start-stop group radius
.
.
.
*Jul  7 03:28:31.543: AAA/BIND(00000018): Bind i/f Virtual-Template2
*Jul  7 03:28:31.547: ppp14 AAA/AUTHOR/LCP: Authorization succeeds trivially
*Jul  7 03:28:33.555: AAA/AUTHOR (0x18): Pick method list 'default'
*Jul  7 03:28:33.555: AAA/BIND(00000019): Bind i/f
*Jul  7 03:28:33.555:  Tnl 5192 L2TP: O SCCRQ
*Jul  7 03:28:33.555:  Tnl 5192 L2TP: O SCCRQ, flg TLS, ver 2, len 141, tnl 0,
ns 0, nr 0
         C8 02 00 8D 00 00 00 00 00 00 00 00 80 08 00 00
         00 00 00 01 80 08 00 00 00 02 01 00 00 08 00 00
         00 06 11 30 80 10 00 00 00 07 4C 41 43 2D 74 75
         6E 6E 65 6C 00 19 00 00 00 08 43 69 73 63 6F 20
         53 79 73 74 65 6D 73 ...
*Jul  7 03:28:33.563:  Tnl 5192 L2TP: Parse  AVP 0, len 8, flag 0x8000 (M)
*Jul  7 03:28:33.563:  Tnl 5192 L2TP: Parse SCCRP
*Jul  7 03:28:33.563:  Tnl 5192 L2TP: Parse  AVP 2, len 8, flag 0x8000 (M)
*Jul  7 03:28:33.563:  Tnl 5192 L2TP: Protocol Ver 256
*Jul  7 03:28:33.563:  Tnl 5192 L2TP: Parse  AVP 3, len 10, flag 0x8000 (M)
*Jul  7 03:28:33.563:  Tnl 5192 L2TP: Framing Cap 0x0
*Jul  7 03:28:33.563:  Tnl 5192 L2TP: Parse  AVP 4, len 10, flag 0x8000 (M)
*Jul  7 03:28:33.567:  Tnl 5192 L2TP: Bearer Cap 0x0
*Jul  7 03:28:33.567:  Tnl 5192 L2TP: Parse  AVP 6, len 8, flag 0x0
*Jul  7 03:28:33.567:  Tnl 5192 L2TP: Firmware Ver 0x1120
*Jul  7 03:28:33.567:  Tnl 5192 L2TP: Parse  AVP 7, len 16, flag 0x8000 (M)
*Jul  7 03:28:33.567:  Tnl 5192 L2TP: Hostname LNS-tunnel
*Jul  7 03:28:33.567:  Tnl 5192 L2TP: Parse  AVP 8, len 25, flag 0x0
*Jul  7 03:28:33.567:  Tnl 5192 L2TP: Vendor Name Cisco Systems, Inc.
*Jul  7 03:28:33.567:  Tnl 5192 L2TP: Parse  AVP 9, len 8, flag 0x8000 (M)
*Jul  7 03:28:33.567:  Tnl 5192 L2TP: Assigned Tunnel ID 6897
*Jul  7 03:28:33.567:  Tnl 5192 L2TP: Parse  AVP 10, len 8, flag 0x8000 (M)
*Jul  7 03:28:33.567:  Tnl 5192 L2TP: Rx Window Size 20050
*Jul  7 03:28:33.567:  Tnl 5192 L2TP: Parse  AVP 11, len 22, flag 0x8000 (M)
*Jul  7 03:28:33.567:  Tnl 5192 L2TP: Chlng
         81 13 03 F6 A8 E4 1D DD 25 18 25 6E 67 8C 7C 39
*Jul  7 03:28:33.567:  Tnl 5192 L2TP: Parse  AVP 13, len 22, flag 0x8000 (M)
*Jul  7 03:28:33.567:  Tnl 5192 L2TP: Chlng Resp
         4D 52 91 DC 1A 43 B3 31 B4 F5 B8 E1 88 22 4F 41
*Jul  7 03:28:33.571:  Tnl 5192 L2TP: No missing AVPs in SCCRP
*Jul  7 03:28:33.571:  Tnl 5192 L2TP: I SCCRP, flg TLS, ver 2, len 157, tnl
5192, ns 0, nr 1
contiguous pak, size 157
```

```
         C8 02 00 9D 14 48 00 00 00 00 00 01 80 08 00 00
         00 00 00 02 80 08 00 00 00 02 01 00 80 0A 00 00
         00 03 00 00 00 00 80 0A 00 00 00 04 00 00 00 00
         00 08 00 00 00 06 11 20 80 10 00 00 00 07 4C 4E
         53 2D 74 75 6E 6E 65 6C ...
*Jul  7 03:28:33.571:  Tnl 5192 L2TP: I SCCRP from LNS-tunnel
*Jul  7 03:28:33.571:  Tnl 5192 L2TP: O SCCCN  to LNS-tunnel tnlid 6897
*Jul  7 03:28:33.571:  Tnl 5192 L2TP: O SCCCN, flg TLS, ver 2, len 42, tnl
6897, ns 1, nr 1
         C8 02 00 2A 1A F1 00 00 00 01 00 01 80 08 00 00
         00 00 00 03 80 16 00 00 00 0D 32 24 17 BC 6A 19
         B1 79 F3 F9 A9 D4 67 7D 9A DB
*Jul  7 03:28:33.571: uid:14 Tnl/Sn 5192/11 L2TP: O ICRQ to LNS-tunnel 6897/0
*Jul  7 03:28:33.571: uid:14 Tnl/Sn 5192/11 L2TP: O ICRQ, flg TLS, ver 2, len
63, tnl 6897, lsid 11, rsid 0, ns 2, nr 1
         C8 02 00 3F 1A F1 00 00 00 02 00 01 80 08 00 00
         00 00 00 0A 80 0A 00 00 00 0F C8 14 B4 03 80 08
         00 00 00 0E 00 0B 80 0A 00 00 00 12 00 00 00 00
         00 0F 00 09 00 64 0F 10 09 02 02 00 1B 00 00
*Jul  7 03:28:33.575: uid:14 Tnl/Sn 5192/11 L2TP: Parse  AVP 0, len 8, flag
0x8000 (M)
*Jul  7 03:28:33.575: uid:14 Tnl/Sn 5192/11 L2TP: Parse ICRP
*Jul  7 03:28:33.575: uid:14 Tnl/Sn 5192/11 L2TP: Parse  AVP 14, len 8, flag
0x8000 (M)
*Jul  7 03:28:33.575: uid:14 Tnl/Sn 5192/11 L2TP: Assigned Call ID 5
*Jul  7 03:28:33.575: uid:14 Tnl/Sn 5192/11 L2TP: No missing AVPs in ICRP
*Jul  7 03:28:33.575: uid:14 Tnl/Sn 5192/11 L2TP: I ICRP, flg TLS, ver 2, len
28, tnl 5192, lsid 11, rsid 0, ns 1, nr 3
contiguous pak, size 28
         C8 02 00 1C 14 48 00 0B 00 01 00 03 80 08 00 00
         00 00 00 0B 80 08 00 00 00 0E 00 05
*Jul  7 03:28:33.579: uid:14 Tnl/Sn 5192/11 L2TP: O ICCN to LNS-tunnel 6897/5
*Jul  7 03:28:33.579: uid:14 Tnl/Sn 5192/11 L2TP: O ICCN, flg TLS, ver 2, len
167, tnl 6897, lsid 11, rsid 5, ns 3, nr 2
         C8 02 00 A7 1A F1 00 05 00 03 00 02 80 08 00 00
         00 00 00 0C 80 0A 00 00 00 18 06 1A 80 00 00 0A
         00 00 00 26 06 1A 80 00 80 0A 00 00 00 13 00 00
         00 01 00 15 00 00 00 1B 01 04 05 D4 03 05 C2 23
         05 05 06 0A 0B E2 7A ...
*Jul  7 03:28:33.579: RADIUS/ENCODE(00000018):Orig. component type = PPoE
*Jul  7 03:28:33.579: RADIUS(00000018): Config NAS IP: 10.0.0.0
*Jul  7 03:28:33.579: RADIUS(00000018): sending
*Jul  7 03:28:33.579: RADIUS/ENCODE: Best Local IP-Address 10.0.1.123 for
Radius-Server 172.19.192.238
*Jul  7 03:28:33.579: RADIUS(00000018): Send Accounting-Request to
172.19.192.238:2196 id 1646/23, len 176
*Jul  7 03:28:33.579: RADIUS:  authenticator 3C 81 D6 C5 2B 6D 21 8E - 19 FF
43 B5 41 86 A8 A5
*Jul  7 03:28:33.579: RADIUS:  Acct-Session-Id     [44]  10  "00000023"
*Jul  7 03:28:33.579: RADIUS:  Framed-Protocol     [7]   6
PPP                        [1]
*Jul  7 03:28:33.579: RADIUS:  Tunnel-Medium-Type  [65]  6
00:IPv4                    [1]
*Jul  7 03:28:33.583: RADIUS:  Tunnel-Client-Endpoi[66]  10  "10.0.0.1"
*Jul  7 03:28:33.583: RADIUS:  Tunnel-Server-Endpoi[67]  10  "10.0.0.2"
*Jul  7 03:28:33.583: RADIUS:  Tunnel-Assignment-Id[82]  5   "lac"
*Jul  7 03:28:33.583: RADIUS:  Tunnel-Type         [64]  6
00:L2TP                    [3]
*Jul  7 03:28:33.583: RADIUS:  Acct-Tunnel-Connecti[68]  12  "3356800003"
*Jul  7 03:28:33.583: RADIUS:  Tunnel-Client-Auth-I[90]  12  "LAC-tunnel"
*Jul  7 03:28:33.583: RADIUS:  Tunnel-Server-Auth-I[91]  12  "LNS-tunnel"
*Jul  7 03:28:33.583: RADIUS:  User-Name           [1]   16  "user@example.com"
*Jul  7 03:28:33.583: RADIUS:  Acct-Authentic      [45]  6
Local                      [2]
```

```
*Jul  7 03:28:33.583: RADIUS:  Acct-Status-Type    [40]  6
Start                     [1]
*Jul  7 03:28:33.583: RADIUS:  NAS-Port-Type       [61]  6
Virtual                   [5]
*Jul  7 03:28:33.583: RADIUS:  NAS-Port            [5]   6
0
*Jul  7 03:28:33.583: RADIUS:  NAS-Port-Id         [87]  9   "0/0/0/0"
*Jul  7 03:28:33.583: RADIUS:  Service-Type        [6]   6
Framed                    [2]
*Jul  7 03:28:33.583: RADIUS:  NAS-IP-Address      [4]   6
10.0.1.123
*Jul  7 03:28:33.583: RADIUS:  Acct-Delay-Time     [41]  6
0
*Jul  7 03:28:33.683: RADIUS: Received from id 1646/23 172.19.192.238:2196,
Accounting-response, len 20
*Jul  7 03:28:33.683: RADIUS:  authenticator 1C E9 53 42 A2 8A 58 9A - C3 CC
1D 79 9F A4 6F 3A
```

その他の参考資料

ここでは、Per VRF AAA に関する関連資料について説明します。

関連資料

関連項目	マニュアル タイトル
サーバ グループの設定	『*Cisco IOS XE Security Configuration Guide: Securing User Services*, Release 2』の「Configuring RADIUS」の章
RADIUS 属性スクリーニング	『*Cisco IOS XE Security Configuration Guide: Securing User Services*, Release 2』の「RADIUS Attribute Value Screening」の章
ブロードキャストアカウンティングの設定	『*Cisco IOS XE Security Configuration Guide: Securing User Services*, Release 2』の「Configuring Accounting」の章
Cisco IOS セキュリティ コマンド	『*Cisco IOS Security Command Reference*』
Cisco IOS Switching Services コマンド	『*Cisco IOS IP Switching Command Reference*』
マルチプロトコルラベルスイッチングの設定	『*Cisco IOS XE Multiprotocol Label Switching Configuration Guide*, Release 2』
仮想テンプレートの設定	『*Cisco IOS XE Dial Technologies Configuration Guide*, Release 2』の「Virtual Templates and Profiles」

標準

標準	タイトル
この機能でサポートされる新規の標準または変更された標準はありません。また、既存の標準のサポートは変更されていません。	--

MIB

MIB	MIB のリンク
この機能によってサポートされる新しい MIB または変更された MIB はありません。またこの機能による既存 MIB のサポートに変更はありません。	選択したプラットフォーム、Cisco IOS XE ソフトウェア リリース、およびフィーチャ セットの MIB の場所を検索しダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

RFC

RFC	タイトル
この機能でサポートが追加または変更された RFC はありません。	--

シスコのテクニカル サポート

説明	リンク
シスコのサポート Web サイトでは、シスコの製品やテクノロジーに関するトラブルシューティングにお役立ていただけるように、マニュアルやツールをはじめとする豊富なオンライン リソースを提供しています。 お使いの製品のセキュリティ情報や技術情報を入手するために、Cisco Notification Service（Field Notice からアクセス）、Cisco Technical Services Newsletter、Really Simple Syndication（RSS）フィードなどの各種サービスに加入できます。 シスコのサポート Web サイトのツールにアクセスする際は、Cisco.com のユーザ ID およびパスワードが必要です。	http://www.cisco.com/en/US/support/index.html

Per VRF AAA の機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *30 : Per VRF AAA* の機能情報

機能名	リリース	機能情報
Per VRF AAA	Cisco IOS XE Release 2.1	Per VRF AAA 機能により、バーチャル プライベート ネットワーク（VPN）ルーティング/転送（VRF）インスタンスに基づいた、認証、許可、アカウンティング（AAA）が行えます。 Cisco IOS XE Release 2.1 では、Cisco ASR 1000 シリーズ Aggregation Services Router にこの機能が実装されました。 次のコマンドが導入または変更されました。**aaa accounting, aaa accounting delay-start, ip radius source-interface, server-private (RADIUS)**、**ip vrf forwarding (server-group)**、**radius-server domain-stripping**、 **aaa authorization template**。
RADIUS Per-VRF サーバ グループ	Cisco IOS XE Release 2.1	RADIUS Per-VRF サーバ グループ機能を使用して、インターネット サービス プロバイダー（ISP）は、Virtual Route Forwarding（VRF）に基づいて RADIUS サーバ グループを分割できます。つまり、VRF に属する RADIUS サーバ グループを定義することができます。この機能は、「aaa:rad-serv-vrf」の VSA によってサポートされています。 Cisco IOS XE Release 2.1 では、Cisco ASR 1000 シリーズ Aggregation Services Router にこの機能が実装されました。 次のコマンドが導入または変更されました。**ip vrf forwarding**。
Attribute Filtering Per-Domain and VRF Aware Framed-Routes	Cisco IOS XE Release 2.3	Attribute Filtering Per-Domain and VRF Aware Framed-Routes 機能により、ドメイン単位の属性フィルタリングおよび VRF 認識 Framed-Route が可能です。これにより「aaa:rad-serv-filter」の VSA のサポートが追加されます。 Cisco IOS XE Release 2.3 では、Cisco ASR 1000 シリーズ Aggregation Services Router にこの機能が実装されました。

機能名	リリース	機能情報
AAA CLI レコード停止機能拡張	Cisco IOS XE Release 2.4	AAA CLI レコード停止機能拡張機能により、AAA サーバから Access Accept を受信する場合にのみアカウンティング終了レコードが送信されます。 Cisco IOS XE Release 2.4 では、Cisco ASR 1000 シリーズ Aggregation Services Router にこの機能が実装されました。 次のコマンドが導入または変更されました。**aaa accounting send stop-record authentication**。
Dynamic Per VRF AAA	Cisco IOS XE Release 2.4	Dynamic Per VRF AAA 機能により、ローカルまたはリモートで保存したカスタマーテンプレートを使用し、カスタマーテンプレートに保存された情報に基づいて、AAA サービスを実行できます。 Cisco IOS XE Release 2.4 では、Cisco ASR 1000 シリーズ Aggregation Services Router にこの機能が実装されました。

用語集

AAA：認証、許可、アカウンティング。セキュリティ サービスのフレームワークであり、ユーザの身元確認（認証）、リモート アクセス コントロール（許可）、課金、監査、およびレポートに使用するセキュリティ サーバ情報の収集と送信（アカウンティング）の方式を定めています。

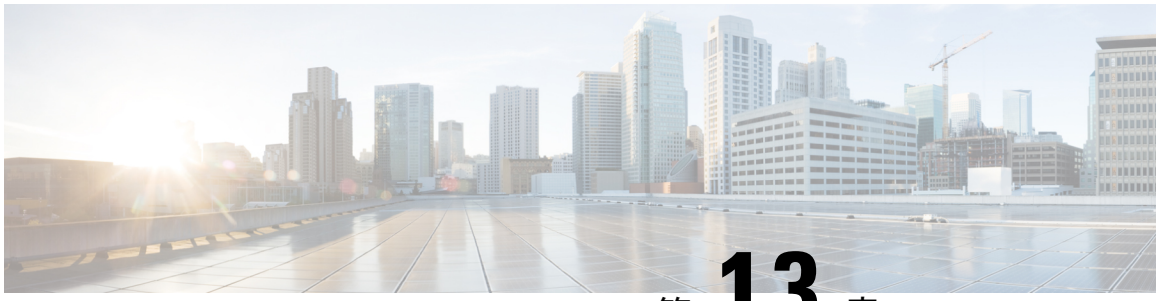
L2TP：Layer 2 Tunnel Protocol。レイヤ 2 トンネル プロトコルを使用すると、ISP などのアクセス サービスが仮想トンネルを作成し、顧客のリモート サイトやリモート ユーザを企業のホーム ネットワークにリンクさせることができます。具体的には、ISP アクセス ポイント（POP）にあるネットワーク アクセス サーバ（NAS）がリモート ユーザと PPP メッセージを交換し、L2F または L2TP の要求や応答を使用して顧客のトンネル サーバと通信し、トンネルのセットアップを行います。

PE：プロバイダー エッジ。サービス プロバイダー ネットワークのエッジ上のネットワーキング デバイス。

RADIUS ：リモート認証ダイヤルイン ユーザー サービス。RADIUS は、不正なアクセスからネットワークのセキュリティを保護する分散クライアント/サーバ システムです。シスコの実装では RADIUS クライアントは Cisco ルータ上で稼働します。認証要求は、すべてのユーザ認証情報とネットワーク サービス アクセス情報が格納されている中央の RADIUS サーバに送信されます。

VPN：Virtual Private Network（仮想プライベートネットワーク）。リモートでダイヤルイン ネットワークをホーム ネットワークに存在させ、あたかも直接接続されているかのように見せるシステム。VPN は、L2TP および L2F を使用し、LAC ではなく、LNS でレイヤ 2 およびより高次のネットワーク接続を終了させます。

VRF：Virtual Route Forwarding（仮想ルーティングおよびフォワーディング）。最初は、ルータにグローバルのデフォルト ルーティング/フォワーディング テーブルは 1 つしかありません。VRF は、複数の分離されたルーティング/フォワーディング テーブルとして表示でき、ユーザのルートには別のユーザのルートとの相互関係はありません。



第 13 章

AAA の IPv6 サポート

IPv6 用の認証、許可、アカウンティング（AAA）サポートは RFC 3162 に準拠しています。このモジュールでは、IPv6 用の AAA オプションの設定方法を示します。

AAA の IPv6 サポートに関する情報

AAA over IPv6

ベンダー固有属性（VSA）を使用して、IPv6 を介して認証、許可、アカウンティング（AAA）をサポートします。Cisco VSA は、inacl、outacl、prefix、および route です。

AAA プロトコルを使用して、プレフィックス プールおよびプール名を設定できます。お客様は、シスコ デバイスと通信するために IPv6 RADIUS サーバまたは TACACS+ サーバを導入できます。

IPv6 RADIUS 属性の AAA サポート

RFC 3162 で説明されているように、IPv6 では次の RADIUS 属性がサポートされます。

- Framed-Interface-Id
- Framed-IPv6-Pool
- Framed-IPv6-Prefix
- Framed-IPv6-Route
- Login-IPv6-Host

IPv6 では、次の RADIUS 属性がサポートされます。

- Delegated-IPv6-Prefix（RFC 4818）
- Delegated-IPv6-Prefix-Pool
- DNS-Server-IPv6-Address
- IPv6 ACL
- IPv6_DNS_Servers
- IPv6 Pool
- IPv6 Prefix#
- IPv6 Route

上記の属性は、RADIUS サーバで設定して、アクセス サーバにダウンロードして、ここでアクセス接続に適用できます。

IPv6 の AAA 属性を使用するための前提条件

IPv6 の AAA 属性は RFC 3162 に準拠しており、RFC 3162 をサポートできる RADIUS サーバを必要とします。

IPv6 環境での仮想アクセス用の RADIUS ユーザ単位属性

仮想アクセスでは次の IPv6 RADIUS 属性がサポートされ、属性と値（AV）のペアとして使用できます。

- Delegated-IPv6-Prefix
- Delegated-IPv6-Prefix-Pool
- DNS-Server-IPv6-Address
- Framed-Interface-Id
- Framed-IPv6-Pool
- Framed-IPv6-Prefix
- Framed-IPv6-Route
- IPv6 ACL
- IPv6_DNS_Servers
- IPv6 Pool
- IPv6 Prefix#
- IPv6 Route
- Login-IPv6-Host

Delegated-IPv6-Prefix

Delegated-IPv6-Prefix 属性は、ネットワークで使用されるユーザに委任される IPv6 プレフィックスを示します。この属性は、RADIUS サーバと委託デバイスの間の DHCP プレフィックス委任中に使用されます。DHCP バージョン 6（DHCPv6）サーバをホストするネットワーク アクセス サーバ（NAS）は、委託デバイスとして動作できます。

次に、Delegated-IPv6-Prefix 属性を使用する例を示します。

```
ipv6:delegated-prefix=2001:DB8::/64
```

（注） この属性では Cisco VSA 形式はサポートされません。この属性を Cisco VSA 形式でユーザ プロファイルに追加しようとすると、RADIUS サーバの応答に失敗します。この属性に使用するのは IETF 属性形式のみです。

Delegated-IPv6-Prefix-Pool

Delegated-IPv6-Prefix-Pool 属性は、プレフィックスが選択され、デバイスに委任されるプレフィックス プールの名前を示します。

プレフィックス委任は IPv6 プレフィックスを委任するための DHCPv6 オプションです。プレフィックス委任には、プレフィックスを選択し、それを要求側のデバイスに一時的に割り当てる委託デバイスが関与します。委任デバイスは、プレフィックスを選択するために多くの戦略を使用します。1 つの方法では、デバイス上でローカルに定義されている名前のプレフィックス プールからプレフィックスを選択します。

Delegated-IPv6-Prefix-Pool 属性は、割り当てられたプレフィックス プールの名前を示します。RADIUS サーバは、この属性を使用して、DHCPv6 サーバをホスティングして、委託デバイスとして動作する NAS にプレフィックス プールの名前を知らせます。

ネットワークで、DHCPv6 プレフィックス委任と ICMPv6 ステートレス アドレス自動設定を共に使用してもかまいません。この場合、Delegated-IPv6-Prefix-Pool 属性と Framed-IPv6-Pool 属性の両方を同じパケット内に含めることができます。曖昧さを回避するために、Delegated-IPv6-Prefix-Pool を DHCPv6 委任で使用されるプレフィックス プールの認可およびアカウンティングに制限して、Framed-IPv6-Pool 属性を SLAAC で使用されるプレフィックス プールの認可およびアカウンティングに使用する必要があります。

次に、アドレス プレフィックスが pool1 という名前のプールから選択される例を示します。プレフィックス プール pool1は、Delegated-IPv6-Prefix-Pool 属性を使用して、RADIUS サーバから委託デバイスにダウンロードされます。次にデバイスは、このプレフィックス プールからアドレス プレフィックス 2001:DB8::/64 を選択します。

```
Cisco:Cisco-AVpair = "ipv6:delegated-ipv6-pool = pool1"
!
ipv6 dhcp pool pool1
address prefix 2001:DB8::/64
!
```

DNS-Server-IPv6-Address

DNS-Server-IPv6-Address 属性は、ドメイン ネーム システム（DNS）サーバの IPv6 アドレスを示します。DHCPv6 サーバは、DNS サーバの IPv6 アドレスを持つホストを設定できます。DNS サーバの IPv6 アドレスを、ICMPv6 デバイスからルータ アドバタイズメント メッセージを使用してホストに伝送することもできます。

NAS は、ホストからの DHCPv6 要求を処理する DHCPv6 サーバをホストすることがあります。また NAS は、ルータ アドバタイズメント メッセージを提供するデバイスとして機能することもあります。したがって、この属性は DNS サーバの IPv6 アドレスを NAS に提供するために使用されます。

NAS がホストに複数の再帰 DNS サーバを通知する必要がある場合、この属性を NAS からホストに送信される Access-Accept パケットに複数回含めることができます。

次に、DNS-Server-IPv6-Address 属性を使用して DNS サーバの IPv6 アドレスを定義する例を示します。

```
Cisco:Cisco-AVpair = "ipv6:ipv6-dns-servers-addr=2001:DB8::"
```

Framed-Interface-Id

Framed-Interface-Id 属性は、ユーザ用に設定する IPv6 インターフェイス ID を示します。

この属性は、Interface-Identifier オプションの IPv6 制御プロトコル（IPv6CP）ネゴシエーション中に使用されます。ネゴシエーションに成功すると、NAS はこの属性を使用して、推奨される IPv6 インターフェイス識別子を Access-Request パケットを使用して RADIUS サーバに知らせます。この属性は、Access-Accept パケットで使用されることもあります。

Framed-IPv6-Pool

Framed-IPv6-Pool 属性は、ユーザに IPv6 プレフィックスを割り当てるために使用するプールの名前を示します。このプールは、デバイスでローカルに定義するか、プールをダウンロードできる RADIUS サーバで定義する必要があります。

Framed-IPv6-Prefix

Framed-IPv6-Prefix 属性は、ユーザ用に設定する IPv6 プレフィックス（および対応するルート）を示します。そのため、この属性は Cisco VSA と同じ機能を実行し、仮想アクセスのみに使用されます。NAS はこの属性を使用して、推奨される IPv6 プレフィックスを Access-Request パケットを使用して RADIUS サーバに知らせます。この属性は Access-Accept で使用されることもあり、これらのパケットで複数回出現することがあります。NAS では、プレフィックスの対応ルートが作成されます。

この属性は、Neighbor Discovery Protocol のルータ アドバタイズメント メッセージでアドバタイズするプレフィックスを指定するために、ユーザによって使用されます。

この属性は DHCPv6 プレフィックス委任にも使用でき、RADIUS サーバのユーザ用には別のプロファイルを作成する必要があります。この別のプロファイルに関連付けられたユーザ名には、サフィックス「-dhcpv6」が付いています。

Framed-IPv6-Prefix 属性の処理は、この別のプロファイルとユーザの通常のプロファイルでは異なります。NAS がルータ アドバタイズメント メッセージを使用してプレフィックスを送信する必要がある場合、プレフィックスは、ユーザの通常のプロファイルの Framed-IPv6-Prefix 属性に配置されます。NAS がリモート ユーザのネットワークにプレフィックスを委任する必要がある場合、プレフィックスはユーザの別のプロファイルの Framed-IPv6-Prefix 属性に配置されます。

（注） この属性では、RADIUS IETF 属性形式と Cisco VSA 形式がサポートされます。

Framed-IPv6-Route

Framed-IPv6-Route 属性は、NAS のユーザ用に設定されるルーティング情報を示します。この属性は Cisco VSAと同じ機能を実行します。属性の値は文字列であり、**ipv6 route** コマンドを使用して指定します。

IPv6 ACL

IPv6 ACL 属性は、完全な IPv6 アクセス リストを指定するために使用されます。アクセス リストの一意の名前が自動的に生成されます。アクセス リストは、各ユーザがログアウトしたときに削除されます。インターフェイス上の以前のアクセス リストが再適用されます。

inacl 属性と outacl 属性を使用すると、デバイスに特定の既存のアクセス リストを設定できます。次に、番号 1 で識別されるアクセス リストを定義する例を示します。

```
cisco-avpair = "ipv6:inacl#1=permit 2001:DB8:cc00:1::/48",
cisco-avpair = "ipv6:outacl#1=deny 2001:DB8::/10",
```

IPv6_DNS_Servers

IPv6_DNS_Servers 属性は、最大 2 つの DNS サーバ アドレスを DHCPv6 サーバに送信するために使用されます。DNS サーバ アドレスは、インターフェイス DHCPv6 サブブロックに保存され、DHCPv6 プールの他の設定よりも優先されます。この属性は、AAA の開始および終了通知に対して返される属性にも含まれます。

IPv6 Pool

IPv6 Pool 属性は、RADIUS 認証の IPv6 プロトコルをサポートするために IPv4 アドレス プール属性を拡張します。この属性は、プレフィックスの選択元の NAS 上のローカル プールの名前を指定します。そして PPP を設定するときとプロトコルを IPv6 と指定するときに使用されます。アドレス プールはローカル プーリングで使用でき、NAS 上に事前に設定されたローカル プールの名前を指定します。

IPv6 Prefix#

IPv6 Prefix# 属性は、Neighbor Discovery Protocol のルータ アドバタイズメント メッセージでアドバタイズするプレフィックスを示します。この属性が使用されている場合は、対応するルー

ト（ユーザ単位のスタティックルートとしてマークされています）が、特定のプレフィックスのルーティング情報ベース（RIB）テーブルにインストールされます。

次に、アドバタイズするプレフィックスを指定する例を示します。

```
cisco-avpair = "ipv6:prefix#1=2001:DB8::/64",
cisco-avpair = "ipv6:prefix#2=2001:DB8::/64",
```

IPv6 Route

IPv6 Route 属性は、ユーザ用のスタティックルートを指定するために使用されます。スタティックルートが適切なのは、シスコのソフトウェアが宛先へのルートを動的に作成できない場合です。スタティックルートの作成の詳細については、**ipv6 route** コマンドを参照してください。

次に、スタティック ルートの定義で IPv6 route 属性を使用する例を示します。

```
cisco-avpair = "ipv6:route#1=2001:DB8:cc00:1::/48",
cisco-avpair = "ipv6:route#2=2001:DB8:cc00:2::/48",
```

Login-IPv6-Host

Login-IPv6-Host 属性は、Login-Service 属性が含まれている場合のユーザの接続先のホストの IPv6 アドレスを示します。NAS は、あるホストの使用を推奨する RADIUS サーバとの通信のために、Access-Request パケット内の Login-IPv6-Host 属性を使用します。

IPv6 用の AAA サポートの設定方法

DHCPv6 AAA オプションの設定

次のタスクを実行して、AAA サーバからプレフィックスを取得するオプションを設定します。

手順の概要

1. **enable**
2. **configure terminal**
3. **ipv6 dhcp pool** *pool-name*
4. **prefix-delegation aaa** [**method-list** *method-list*] [*lifetime*]
5. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。

	コマンドまたはアクション	目的
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ipv6 dhcp pool** *pool-name* 例： `Device(config)# ipv6 dhcp pool pool1`	DHCPv6 設定情報プールを設定し、IPv6 DHCP プール コンフィギュレーション モードを開始します。
ステップ 4	**prefix-delegation aaa** [**method-list** *method-list*] [*lifetime*] 例： `Device(config-dhcpv6)# prefix-delegation aaa method-list list1`	プレフィックスを AAA サーバから取得することを指定します。
ステップ 5	**end** 例： `Device(config-dhcpv6)# end`	IPv6 DHCP プール コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

AAA の IPv6 サポートの設定例

例：DHCPv6 AAA オプションの設定

次に、AAA サーバからプレフィックスを取得する DHCPv6 オプションを設定する例を示します。

```
Device> enable
Device# configure terminal
Device(config)# ipv6 dhcp pool pool1
Device(config-dhcpv6)# prefix-delegation aaa method-list list1
Device(config-dhcpv6)# end
```

例：RADIUS の設定

次の RADIUS 設定例は、スタティック ルートを確立するための AV ペアの定義を示します。

```
campus1 Auth-Type = Local, Password = "mypassword"
                User-Service-Type = Framed-User,
                Framed-Protocol = PPP,
                cisco-avpair = "ipv6:inacl#1=permit 2001:DB8:1::/64 any",
                cisco-avpair = "ipv6:route=2001:DB8:2::/64",
                cisco-avpair = "ipv6:route=2001:DB8:3::/64",
                cisco-avpair = "ipv6:prefix=2001:DB8:2::/64 0 0 onlink autoconfig",
                cisco-avpair = "ipv6:prefix=2001:DB8:3::/64 0 0 onlink autoconfig",
                cisco-avpair = "ip:route=10.0.0.0 255.0.0.0",
```

その他の参考資料

関連資料

関連項目	マニュアル タイトル
time-range コマンドを使用した時間範囲の指定	『*Cisco IOS XE Network Management Configuration Guide*』の「*Performing Basic System Management*」章
ネットワーク管理コマンドの説明	『*Cisco IOS Network Management Command Reference*』

標準

標準	タイトル
この機能でサポートされる新規の標準または変更された標準はありません。また、既存の標準のサポートは変更されていません。	--

MIB

MIB	MIB のリンク
この機能によってサポートされる新しい MIB または変更された MIB はありません。またこの機能による既存 MIB のサポートに変更はありません。	選択したプラットフォーム、Cisco IOS XE ソフトウェア リリース、およびフィーチャ セットの MIB の場所を検索しダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

RFC

RFC	タイトル
この機能によりサポートされた新規 RFC または改訂 RFC はありません。またこの機能による既存 RFC のサポートに変更はありません。	--

シスコのテクニカル サポート

説明	リンク
右の URL にアクセスして、シスコのテクニカル サポートを最大限に活用してください。これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

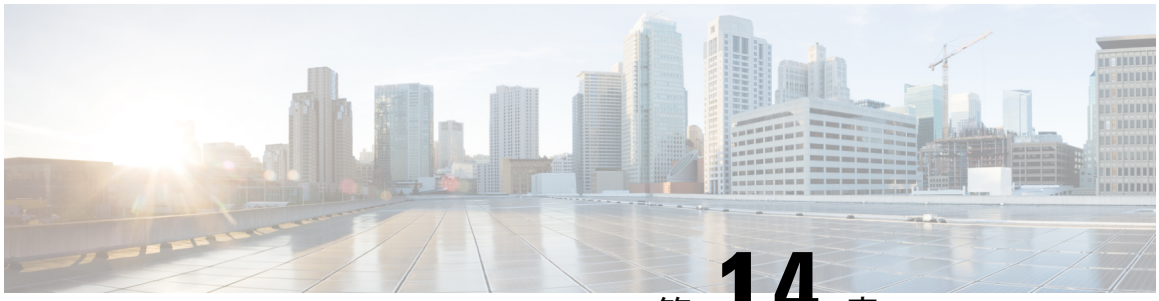
RADIUS over IPv6 の機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *31 : RADIUS over IPv6* の機能情報

機能名	リリース	機能情報
RADIUS over IPv6	15.1(1)SY	RFC 3162 に定義されている RADIUS 属性。



第 14 章

TACACS+ over IPv6

IPv6 サーバは、TACACS+ と共に使用するよう設定できます。

TACACS+ over IPv6 に関する情報

Terminal Access Controller Access Control System（TACACS+）セキュリティ プロトコルはユーザの検証を集中的に行います。TACACS+ サービスは、通常 UNIX または Windows NT ワークステーション上で稼働する TACACS+ デーモンのデータベースで管理されます。デバイスに設定した TACACS+ 機能を有効にするには、その前に、TACACS+ サーバにアクセスして TACACS+ サーバを設定する必要があります。

TACACS+ では、認証、許可、アカウンティングの各ファシリティを個別に提供します。TACACS+を使用すると、単一のアクセス コントロール サーバー（TACACS+ デーモン）で、各サービス（認証、許可、アカウンティング）を個別に提供できます。各サービスは固有のデータベースにアソシエートされており、デーモンの機能に応じて、そのサーバーまたはネットワーク上で使用可能な他のサービスを利用できます。

AAA over IPv6

ベンダー固有属性（VSA）を使用して、IPv6 を介して認証、許可、アカウンティング（AAA）をサポートします。Cisco VSA は、inacl、outacl、prefix、および route です。

AAA プロトコルを使用して、プレフィックス プールおよびプール名を設定できます。お客様は、シスコ デバイスと通信するために IPv6 RADIUS サーバまたは TACACS+ サーバを導入できます。

IPv6 トランスポートを介した TACACS+

IPv6 サーバは、TACACS+ を使用するよう設定できます。IPv4 または IPv6 アドレスの代わりに名前を使用して、TACACS+ を使用するよう IPv6 と IPv4 の両方のサーバを設定できます。

TACACS+ over IPv6 の設定方法

IPv6 を介した TACACS+ サーバの設定

手順の概要

1. **enable**
2. **configure terminal**
3. **tacacs server** *name*
4. **address ipv6** *ipv6-address*
5. **key** [**0** | **7**] *key-string*
6. **port** [*number*
7. **send-nat-address**
8. **single-connection**
9. **timeout** *seconds*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**tacacs server** *name* 例： `Device(config)# tacacs server server1`	IPv6 に対して TACACS+ サーバを設定して、TACACS+ サーバ コンフィギュレーション モードを開始します。
ステップ 4	**address ipv6** *ipv6-address* 例： `Device(config-server-tacacs)# address ipv6 2001:DB8:3333:4::5`	TACACS+ サーバの IPv6 アドレスを設定します。

	コマンドまたはアクション	目的
ステップ 5	**key** [**0** | **7**] *key-string* 例： `Device(config-server-tacacs)# key 0 key1`	TACACS+ サーバでサーバ単位の暗号キーを設定します。
ステップ 6	**port** [*number* 例： `Device(config-server-tacacs)# port 12`	TACACS+ 接続に使用する TCP ポートを指定します。
ステップ 7	**send-nat-address** 例： `Device(config-server-tacacs)# send-nat-address`	クライアントの NAT 後のアドレスを TACACS+ サーバに送信します。
ステップ 8	**single-connection** 例： `Device(config-server-tacacs)# single-connection`	単一の TCP 接続を使用してすべての TACACS パケットを同じサーバに送信できるようにします。
ステップ 9	**timeout** *seconds* 例： `Device(config-server-tacacs)# timeout 10`	指定された TACACS サーバからの応答を待機する時間を設定します。

TACACS+ パケットでの送信元アドレスの指定

手順の概要

1. **enable**
2. **configure terminal**
3. **ipv6 tacacs source-interface** *type number*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例：	グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
	`Router# configure terminal`	
ステップ 3	**ipv6 tacacs source-interface** *type number* 例： `Router(config)# ipv6 tacacs source-interface GigabitEthernet 0/0/0`	TACACS+ パケットで送信元アドレスに使用するインターフェイスを指定します。

TACACS+ サーバ グループ オプションの設定

手順の概要

1. **enable**
2. **configure terminal**
3. **aaa group server tacacs+** *group-name*
4. **server name** *server-name*
5. **server-private** {*ip-address* | *name* | *ipv6-address*} [**nat**] [**single-connection**] [**port** *port-number*] [**timeout** *seconds*] [**key** [**0** | **7**] *string*]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**aaa group server tacacs+** *group-name* 例： `Device(config)# aaa group server tacacs+ group1`	各種の TACACS+ サーバ ホストを別個のリストと別個の方式にグループ化します。
ステップ 4	**server name** *server-name* 例： `Device(config-sg-tacacs+)# server name server1`	IPv6 TACACS+ サーバを指定します。

	コマンドまたはアクション	目的
ステップ 5	**server-private** {*ip-address* | *name* | *ipv6-address*} [**nat**] [**single-connection**] [**port** *port-number*] [**timeout** *seconds*] [**key** [**0** | **7**] *string*] 例： `Device(config-sg-tacacs+)# server-private 2001:DB8:3333:4::5 port 19 key key1`	グループ サーバに対するプライベート TACACS+ サーバの IPv6 アドレスを設定します。

TACACS+ over IPv6 の設定例

例：IPv6 を介した TACACS+ サーバの設定

```
Device# show tacacs

          Tacacs+ Server:          server1
          Server Address:          FE80::200:F8FF:FE21:67CF
            Socket opens:          0
           Socket closes:          0
           Socket aborts:          0
           Socket errors:          0
        Socket Timeouts:           0
  Failed Connect Attempts:         0
       Total Packets Sent:         0
       Total Packets Recv:         0
```

その他の参考資料

ここでは、MSCHAP バージョン 2 の機能に関する関連資料について説明します。

関連資料

関連項目	マニュアル タイトル
PPP インターフェイスの設定	『*Cisco IOS Dial Technologies Configuration Guide* , Release 12.4T』の「PPP Configuration」
シスコのネットワーキング装置の設定および管理に必要なタスクとコマンドの説明	『*Cisco IOS Dial Technologies Command Reference*』
IOS セキュリティ コマンドの一覧	『*Cisco IOS Security Command Reference*』

関連項目	マニュアル タイトル
AAA を使用した PPP 認証の設定	『*Cisco IOS Security Configuration Guide: Securing User Services* , Release 12.4T』の「Configuring Authentication」モジュールの「Configuring PPP Authentication Using AAA」
RADIUS 認証の設定	『*Cisco IOS Security Configuration Guide: Securing User Services*, Release 12.4T』の「Configuring RADIUS」モジュール

標準

標準	タイトル
この機能がサポートする新しい規格または変更された規格はありません。	--

MIB

MIB	MIB のリンク
この機能によってサポートされる新しい MIB または変更された MIB はありません。	選択したプラットフォーム、Cisco IOS リリース、およびフィーチャ セットに関する MIB を探してダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

RFC

RFC	タイトル
RFC 1661	ポイントツーポイント プロトコル（*PPP*）
RFC 2548	『*Microsoft Vendor-specific RADIUS Attributes*』
RFC 2759	「*Microsoft PPP CHAP Extensions, Version 2*」

シスコのテクニカル サポート

説明	リンク
シスコのサポート Web サイトでは、シスコの製品やテクノロジーに関するトラブルシューティングにお役立ていただけるように、マニュアルやツールをはじめとする豊富なオンライン リソースを提供しています。 お使いの製品のセキュリティ情報や技術情報を入手するために、Cisco Notification Service（Field Notice からアクセス）、Cisco Technical Services Newsletter、Really Simple Syndication（RSS）フィードなどの各種サービスに加入できます。 シスコのサポート Web サイトのツールにアクセスする際は、Cisco.com のユーザ ID およびパスワードが必要です。	http://www.cisco.com/en/US/support/index.html

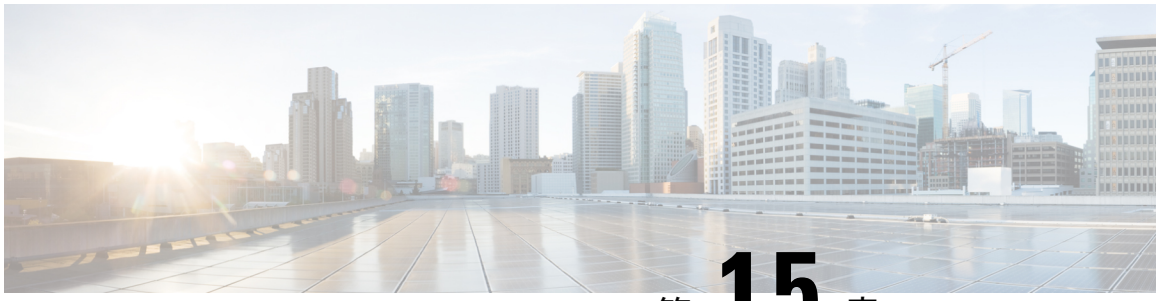
TACACS+ over IPv6 の機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *32 : TACACS+ over IPv6* の機能情報

機能名	リリース	機能情報
TACACS+ over IPv6	Cisco IOS XE Release 3.2S	TACACS+ over IPv6 がサポートされます。 次のコマンドが導入または変更されました。**aaa group server tacacs+**、**address ipv6 (TACACS+)**、**ipv6 tacacs source-interface**、**key (TACACS+)**、**port (TACACS+)**、**send-nat-address**、**server name (IPv6 TACACS+)**、**server-private (TACACS+)**、**single-connection**、**tacacs server**、**timeout (TACACS+)**。



第 15 章

AAA Dead-Server Detection

AAA Dead-Server Detection 機能を使用すると、RADIUS サーバーをデッド状態と指定するための条件を設定できます。条件が明示的に設定されていない場合は、条件は未処理のトランザクションの数に基づいて動的に計算されます。この機能を使用すると、デッドタイムが短くなり、パケット処理が高速になります。

AAA Dead-Server Detection の前提条件

- RADIUS サーバーにアクセスできる必要があります。
- RADIUS サーバーの設定方法を十分理解していることが必要です。
- 認証、許可、アカウンティング（AAA）の設定方法を十分理解していることが必要です。
- あるサーバーをデッド状態と指定するためには、まず **radius-server deadtime** コマンドを設定する必要があります。このコマンドを設定していない場合は、サーバをデッド状態と指定するための条件に適合していても、サーバは「アップ」状態になります。

AAA Dead-Server Detection の制約事項

- サーバがデッド状態と指定されるまでにルータで発生する必要がある連続タイムアウト回数には、最初の転送は含まれません。つまり、再転送の回数のみがカウントされます。

AAA Dead-Server Detection について

RADIUS サーバーをデッド状態と指定するための条件

AAA Dead-Server Detection 機能を使用すると、RADIUS サーバをデッド状態と指定するための条件を決定できます。つまり、ルータがRADIUSサーバから有効なパケットを最後に受け取ってからRADIUSサーバがデッド状態と指定されるまでに経過する必要がある最低時間を秒単位で設定することができます。ルータの起動後にパケットを受信せずにタイムアウトになった場合は、この時間の条件は満たされたものとして処理されます。

さらに、RADIUSサーバーがデッド状態と指定されるまでにルータで発生する必要がある連続タイムアウト回数を設定することもできます。サーバーが認証とアカウンティングの両方を実行する場合、両方の種類のパケットがこの回数に含まれます。正しく作成されていないパケットは、タイムアウトになっているものとしてカウントされます。カウントされるのは再転送だけで、最初の転送はカウントされません。（タイムアウトになるたびに再転送が1回行われることになります）。

（注） 時間の条件と試行回数の条件の両方を満たしていないと、サーバーはデッド状態と指定されません。

RADIUS Dead-Server Detection を設定すると、応答を停止している RADIUS サーバーが即時検出されます。また、サーバが「動きが鈍い」（応答が遅い）状態になっているときに誤ってデッド状態と指定されなくなるほか、デッド状態からライブ状態になってすぐにまたデッド状態になる現象を回避できます。この未応答RADIUSサーバの即時検出、動きが鈍いサーバの誤検出の回避、デッド状態とライブ状態を繰り返す現象の回避が有効になると、デッドタイムが短くなり、パケット処理が高速になります。

AAA Dead-Server Detection の設定方法

AAA Dead-Server Detection の設定

AAA Dead-Server Detection を設定する手順は、次のとおりです。

手順の概要

1. **enable**
2. **configure terminal**
3. **aaa new-model**
4. **radius-server deadtime** *minutes*
5. **radius-server dead-criteria** [**time** *seconds*] [**tries** *number-of-tries*]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**aaa new-model** 例： `Router (config)# aaa new-model`	AAA アクセス コントロール モデルをイネーブルにします。
ステップ 4	**radius-server deadtime** *minutes* 例： `Router (config)# radius-server deadtime 5`	いくつかのサーバーが使用不能になったときの RADIUS サーバーの応答時間を短くし、使用不能になったサーバーがすぐにスキップされるようにします。
ステップ 5	**radius-server dead-criteria** [**time** *seconds*] [**tries** *number-of-tries*] 例： `Router (config)# radius-server dead-criteria time 5 tries 4`	RADIUS サーバをデッド状態と指定するための条件のいずれかまたは両方を、指定した定数で適用します。

トラブルシューティングのヒント

AAA Dead-Server Detection を設定したら、**show running-config** コマンドを使用して、その設定を確認してください。この確認が特に重要になるのは、**no** 形式の **radius-server dead-criteria** コマンドを使用している場合です。**show running-config** コマンドの出力は、**radius-server dead-criteria** コマンドを使用して設定した「Dead Criteria Details」フィールドと同じ値を示している必要があります。

AAA Dead-Server Detection の確認

AAA Dead-Server Detection の設定を確認する手順は、次のとおりです。**show** および **debug** コマンドは、任意の順番で使用できます。

手順の概要

1. **enable**
2. **debug aaa dead-criteria transactions**

3. **show aaa dead-criteria**
4. **show aaa servers** [**private** | **public**]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**debug aaa dead-criteria transactions** 例： `Router# debug aaa dead-criteria transactions`	デッド条件の AAA トランザクションの値を表示します。
ステップ 3	**show aaa dead-criteria** 例： `Router# show aaa dead-criteria`	AAA サーバのデッド条件に関する情報を表示します。
ステップ 4	**show aaa servers** [**private**	**public**] 例： `Router# show aaa server private`	パブリックおよびプライベートのすべての認証、許可、アカウンティング（AAA）RADIUS サーバーとの間で送受信されたパケットのステータスと数を表示します。 • **private** キーワードを付けると、パブリック AAA サーバーのみについて表示されます。 • **public** キーワードを付けると、パブリック AAA サーバーのみについて表示されます。

AAA Dead-Server Detection の設定例

AAA Dead-Server Detection の設定の例

次の例では、5 秒後および 4 回の試行後にルータがデッド状態と見なされます。

```
Router (config)# aaa new-model
Router (config)# radius-server deadtime 5
Router (config)# radius-server dead-criteria time 5 tries 4
```

debug aaa dead-criteria transactions コマンドの例

次の出力例は、特定のサーバグループのデッド条件のトランザクションに関する情報を示しています。

```
Router# debug aaa dead-criteria transactions
AAA Transaction debugs debugging is on
*Nov 14 23:44:17.403: AAA/SG/TRANSAC: Computed Retransmit Tries: 22, Current Max Tries:
 22
*Nov 14 23:44:17.403: AAA/SG/TRANSAC: Computed Dead Detect Interval: 25s, Current Max
Interval: 25s
*Nov 14 23:44:17.403: AAA/SG/TRANSAC: Estimated Outstanding Transactions: 6, Current Max
 Transactions: 6
```

show aaa dead-criteria コマンドの例

次の出力例は、IP アドレス 172.19.192.80 の RADIUS サーバーに対してデッド サーバー検出に関する情報が要求されたことを示しています。

```
Router# show aaa dead-criteria radius 172.19.192.80 radius
RADIUS Server Dead Criteria:
============================
Server Details:
    Address : 172.19.192.80
    Auth Port : 1645
    Acct Port : 1646
Server Group : radius
Dead Criteria Details:
    Configured Retransmits : 62
    Configured Timeout : 27
    Estimated Outstanding Transactions: 5
    Dead Detect Time : 25s
    Computed Retransmit Tries: 22
    Statistics Gathered Since Last Successful Transaction
=====================================================
Max Computed Outstanding Transactions: 5
Max Computed Dead Detect Time: 25s
Max Computed Retransmits : 22
```

その他の参考資料

ここでは、AAA Dead-Server Detection 機能の関連資料について説明します。

関連資料

関連項目	マニュアル タイトル
RADIUS の設定	「RADIUS の設定」機能モジュール。

関連項目	マニュアル タイトル
AAA の設定	認証の設定
	認可の設定
	アカウンティングの設定
セキュリティ コマンド	『*Cisco IOS Security Command Reference*』

標準

標準	タイトル
この機能でサポートされる新規の標準または変更された標準はありません。また、既存の標準のサポートは変更されていません。	--

MIB

MIB	MIB のリンク
この機能によってサポートされる新しい MIB または変更された MIB はありません。またこの機能による既存MIBのサポートに変更はありません。	選択したプラットフォーム、Cisco IOS リリース、およびフィーチャ セットに関する MIB を探してダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

RFC

RFC	タイトル
RFC 2865	『*Remote Authentication Dial In User Service (RADIUS)*』

シスコのテクニカル サポート

説明	リンク
シスコのサポート Web サイトでは、シスコの製品やテクノロジーに関するトラブルシューティングにお役立ていただけるように、マニュアルやツールをはじめとする豊富なオンライン リソースを提供しています。 お使いの製品のセキュリティ情報や技術情報を入手するために、Cisco Notification Service（Field Notice からアクセス）、Cisco Technical Services Newsletter、Really Simple Syndication（RSS）フィードなどの各種サービスに加入できます。 シスコのサポート Web サイトのツールにアクセスする際は、Cisco.com のユーザ ID およびパスワードが必要です。	http://www.cisco.com/en/US/support/index.html

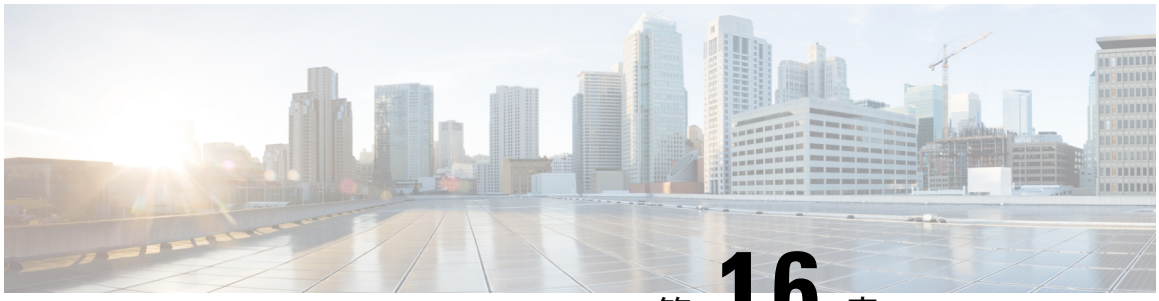
AAA Dead-Server Detection の機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *33 : AAA Dead-Server Detection* の機能情報

機能名	リリース	機能情報
AAA Dead-Server Detection	Cisco IOS XE Release 3.9S	RADIUS サーバをデッド状態と指定するための条件を設定できます。 次のコマンドが導入または変更されました。**debug aaa dead-criteria transactions**、**radius-server dead-criteria**、**show aaa dead-criteria**、**show aaa servers**。



第 16 章

Login Password Retry Lockout

Login Password Retry Lockout 機能により、システム管理者はユーザによるログイン試行が設定した回数失敗すると、ローカルの認証、許可、アカウンティング（AAA）ユーザ アカウントをロックアウトできます。

Login Password Retry Lockout の前提条件

- AAA コンポーネントを含む Cisco IOS イメージを実行する必要があります。

Login Password Retry Lockout の制約事項

- パスワードを推測している攻撃者とパスワードを誤って複数回入力している認証されたユーザとの区別はされないため、認証されたユーザもロックアウトされます。
- サービス拒絶（DoS）攻撃もあり得ます。つまり、認証されたユーザのユーザ名が攻撃者に知られた場合、認証されたユーザがロックアウトされる可能性もあります。

Login Password Retry Lockout に関する情報

ローカル AAA ユーザ アカウントのロックアウト

Login Password Retry Lockout 機能により、システム管理者は、AAA ユーザ アカウントに一致するユーザ名を使用したユーザによるログインが指定した回数失敗すると、ローカルAAAユーザ アカウントをロックアウトできます。ロックアウトされたユーザは、ユーザ アカウントが管理者によってロック解除されるまで、再度正常にログインすることはできなくなります。

ユーザがシステムによってロックされるか、システム管理者によってロック解除されると、システムメッセージが生成されます。次に示すのは、このようなシステムメッセージの例です。

```
%AAA-5-USER_LOCKED: User user1 locked out on authentication failure.
```

システム管理者はロックアウトできません。

（注） システム管理者は特殊なユーザで、最大の特権レベル（ルート権限 - レベル 15）を使用して設定されています。これより低い特権レベルを使用して設定されたユーザーは、**enable** コマンドを使用して特権レベルを変更できます。ルート権限（レベル 15）に変更可能なユーザは、システム管理者として機能できます。

この機能は、ASCII、チャレンジ ハンドシェイク認証プロトコル（CHAP）およびパスワード認証プロトコル（PAP）など、任意のログイン認証方式に適用できます。

（注） ロックされたステータスによる認証エラー後、ユーザにメッセージは表示されません（つまり、通常の認証エラーとユーザのロックされたステータスによる認証エラーは区別されません）。

Login Password Retry Lockout の設定方法

Login Password Retry Lockout の設定

Login Password Retry Lockout 機能を設定するには、次の手順を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **username** *name* [**privilege** *level*] **password** *encryption-type password*

4. **aaa new-model**
5. **aaa local authentication attempts max-fail** *number-of-unsuccessful-attempts*
6. **aaa authentication login default** *method*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**username** *name* [**privilege** *level*] **password** *encryption-type password* 例： `Device(config)# username user1 privilege 15 password 0 cisco`	ユーザ名をベースとした認証システムを構築します。
ステップ 4	**aaa new-model** 例： `Device(config)# aaa new-model`	AAA アクセス コントロール モデルをイネーブルにします。
ステップ 5	**aaa local authentication attempts max-fail** *number-of-unsuccessful-attempts* 例： `Device(config)# aaa local authentication attempts max-fail 3`	ユーザがロックアウトされるまでの試行の失敗回数の上限を指定します。
ステップ 6	**aaa authentication login default** *method* 例： `Device(config)# aaa authentication login default local`	ログイン時の認証、許可、アカウンティング（AAA）認証方式を設定します。たとえば、**aaa authentication login default** *local* はローカル AAA ユーザーデータベースを指定します。

ログインがロックアウトされたユーザのロック解除

ログインがロックアウトされたユーザをロック解除するには、次の手順を実行します。

（注） この作業を実行できるのは、ルート権限（レベル 15）を持つユーザだけです。

手順の概要

1. **enable**
2. **clear aaa local user lockout** {**username** *username* | **all**}

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**clear aaa local user lockout** {**username** *username*	**all**} 例： `Device# clear aaa local user lockout username user1`	ロックアウトされたユーザをロック解除します。

ユーザの失敗したログイン試行のクリア

この作業は、ユーザ設定が変更され、すでに記録されている、失敗したユーザのログイン試行をクリアする必要がある場合に役立ちます。

すでに記録されている、失敗したユーザのログイン試行をクリアするには、次の手順を実行します。

手順の概要

1. **enable**
2. **clear aaa local user fail-attempts** {**username** *username* | **all**}

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**clear aaa local user fail-attempts** {**username** *username*	**all**}	失敗したユーザの試行をクリアします。

	コマンドまたはアクション	目的
	例： `Device# clear aaa local user fail-attempts username user1`	• このコマンドは、ユーザ設定が変更され、すでに記録されている失敗した試行をクリアする必要がある場合に役立ちます。

Login Password Retry Lockout のステータスのモニタおよびメンテナンス

Login Password Retry Lockout 設定ステータスのモニタとメンテナンスを行うには、次の手順を実行します。

手順の概要

1. **enable**
2. **show aaa local user lockout**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**show aaa local user lockout** 例： `Device# show aaa local user lockout`	現在の Login Password Retry Lockout 設定でロックアウトされているユーザのリストを表示します。

例

次の出力は、user1 がロックアウトされていることを示しています。

```
Device# show aaa local user lockout
          Local-user          Lock time
          user1               04:28:49 UTC Sat Jun 19 2004
```

Login Password Retry Lockout の設定例

Login Password Retry Lockout 設定の表示の例

次の **show running-config** コマンド出力は、Login Password Retry Lockout 設定で、ユーザーの試行の失敗回数の上限が 2 に設定されていることを示します。

```
Device # show running-config
Building configuration...
Current configuration : 1214 bytes
!
version 12.3
no service pad
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname LAC-2
!
boot-start-marker
boot-end-marker
!
!
username sysadmin
username sysad privilege 15 password 0 cisco
username user1 password 0 cisco
aaa new-model
aaa local authentication attempts max-fail 2
!
!
aaa authentication login default local
aaa dnis map enable
aaa session-id common
```

その他の参考資料

ここでは、Login Password Retry Lockout に関する関連資料について説明します。

関連資料

関連項目	マニュアル タイトル
Cisco IOS セキュリティ コマンド	『*Cisco IOS Security Command Reference*』

標準

標準	タイトル
なし	--

MIB

MIB	MIB のリンク
なし	選択したプラットフォーム、Cisco IOS リリース、およびフィーチャ セットに関する MIB を探してダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

RFC

RFC	タイトル
なし	--

シスコのテクニカル サポート

説明	リンク
シスコのサポート Web サイトでは、シスコの製品やテクノロジーに関するトラブルシューティングにお役立ていただけるように、マニュアルやツールをはじめとする豊富なオンライン リソースを提供しています。 お使いの製品のセキュリティ情報や技術情報を入手するために、Cisco Notification Service（Field Notice からアクセス）、Cisco Technical Services Newsletter、Really Simple Syndication（RSS）フィードなどの各種サービスに加入できます。 シスコのサポート Web サイトのツールにアクセスする際は、Cisco.com のユーザ ID およびパスワードが必要です。	http://www.cisco.com/en/US/support/index.html

Login Password Retry Lockout の機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

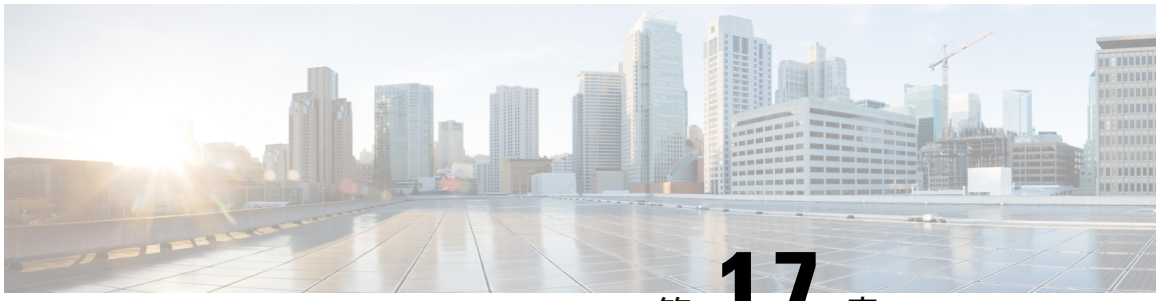
プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *34 : Login Password Retry Lockout* の機能情報

機能名	リリース	機能情報
Login Password Retry Lockout	Cisco IOS XE Release 3.9S	Login Password Retry Lockout 機能により、システム管理者はユーザによるログイン試行が設定した回数失敗すると、ローカル AAA ユーザ アカウントをロックアウトできます。 次のコマンドが導入または変更されました。**aaa local authentication attempts max-fail**、**clear aaa local user fail-attempts**、**clear aaa local user lockout**。

用語集

- **local AAA method**：ルータ上にローカル ユーザー データベースを設定し、そのデータベースから、AAA にユーザーの認証または認可を提供させる方式。
- **local AAA user**：ローカル AAA 方式を使用して認証されたユーザー。



第 17 章

MSCHAP バージョン 2

Cisco IOS リリース 12.2(2)XB5 で導入された MSCHAP バージョン 2 機能を使用すると、Cisco ルータは、Microsoft Windows オペレーティング システムを使用するコンピュータとネットワーク アクセス サーバ（NAS）間の PPP 接続にマイクロソフト チャレンジ ハンドシェイク認証プロトコル バージョン 2（MSCHAP V2）の認証を使用できます。

Cisco IOS リリース 12.4(6)T では、MSCHAP V2 が新機能をサポートするようになりました。これを MSCHAPv2 のパスワード エージングの AAA でのサポートと呼びます。Cisco IOS リリース 12.4(6)T よりも前のバージョンでは、パスワード認証プロトコル（PAP）ベースのクライアントが認証、許可、アカウンティング（AAA）サブシステムにユーザ名とパスワードの値を送信すると、AAA が RADIUS サーバへの認証要求を生成していました。パスワードが失効している場合は、RADIUS サーバにより認証失敗のメッセージが返信されますが、認証が失敗した理由は AAA サブシステムには渡されていませんでした。そのため、認証が失敗したためにユーザはアクセスを拒否されますが、アクセスが拒否された理由は通知されませんでした。

Cisco IOS リリース 12.4(6)T で使用可能になったパスワード エージング機能は、パスワードが失効したことをクリプトベースのクライアントに通知し、ユーザがパスワードを変更するための一般的な方法を提供します。パスワードエージング機能では、クリプトベースのクライアントのみをサポートします。

MSCHAP バージョン 2 の前提条件

- **interface** コマンドを使用してインターフェイス タイプを設定し、インターフェイス コンフィギュレーション モードを開始します。

- **encapsulation** コマンドを使用して、PPP をカプセル化するためのインターフェイスを設定します。
- クライアントのオペレーティング システムが MSCHAP V2 のすべての機能をサポートしていることを確認してください。
- Cisco IOS リリース 12.4(6)T のパスワード エージング機能は、クリプトベースのクライアントの RADIUS 認証のみをサポートします。
- RADIUS サーバーが送信する認証失敗属性を MSCHAP バージョン 2 機能が正しく解釈していることを確認するには、**ppp max-bad-auth** コマンドを設定し、認証のリトライ回数を 2 回以上に設定する必要があります。

また、 **radius server vsa send authentication** コマンドを設定し、RADIUS クライアントがベンダー固有属性を RADIUS サーバーに送信できるようにする必要があります。パスワード変更機能は、RADIUS 認証のみでサポートされています。

- Microsoft Windows 2000、Microsoft Windows XP、および Microsoft Windows NT のオペレーティング システムには、パスワード変更機能の動作を妨げる既知の注意事項があります。次の URL で Microsoft のパッチをダウンロードする必要があります。

http://support.microsoft.com/default.aspx?scid=kb;en-us;Q326770

これらのタスクの実行の詳細については、『*Cisco IOS Dial Technologies Configuration Guide* , Release 12.4T』の「PPP Configuration」を参照してください。RADIUS サーバで認証を設定する必要があります。RADIUS サーバでの RADIUS 認証の設定の詳細については、ベンダー固有のマニュアルを参照してください。

MSCHAP バージョン 2 の制約事項

- MSCHAP V2 の認証は、MSCHAP V1 の認証と互換性がありません。
- パスワード変更オプションは RADIUS 認証のみでサポートされており、ローカル認証では使用できません。

MSCHAP バージョン 2 の概要

MSCHAP V2 の認証は、Microsoft Windows 2000 オペレーティング システムが使用するデフォルトの認証方式です。この認証方式をサポートする Cisco ルータを使用すると、Microsoft Windows 2000 オペレーティング システムのユーザは、クライアントで認証方式を設定せずにリモートの PPP セッションを確立できます。

MSCHAP V2 の認証では、MSCHAP V1 または標準の CHAP 認証では使用できない追加機能が導入されました。それは、パスワードの変更機能です。パスワード変更機能を使用すると、パスワードが失効したことを RADIUS サーバがレポートした場合に、クライアントがアカウントのパスワードを変更できます。

（注） MSCHAP V2 の認証は更新バージョンの MSCHAP です。これは、MSCHAP バージョン 1（V1）と似ていますが、互換性はありません。MSCHAP V2 では、ピアとパスワード変更機能の間の相互認証が導入されました。

MSCHAP バージョン 2 の設定方法

MSCHAP V2 の認証の設定

ローカル認証または RADIUS 認証で MSCHAP V2 認証を受け入れるように NAS を設定し、RADIUS 認証の認証失敗属性およびベンダー固有の RADIUS 属性を適切に解釈できるようにするには、グローバル コンフィギュレーション モードで次のコマンドを使用します。

手順の概要

1. **enable**
2. **configure terminal**
3. **radius-server vsa send authentication**
4. **interface** *type number*
5. **ppp max-bad-auth** *number*
6. **ppp authentication ms-chap-v2**
7. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**radius-server vsa send authentication** 例： `Device(config)# radius-server vsa send authentication`	ベンダー固有属性を認識して使用するように NAS を設定します。

	コマンドまたはアクション	目的
ステップ 4	**interface** *type number* 例： `Device(config)# interface Gigabitethernet 1/0/1`	インターフェイス タイプを設定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 5	**ppp max-bad-auth** *number* 例： `Device(config-if)# ppp max-bad-auth 2`	認証が失敗した直後、または指定された認証のリトライ回数の範囲内である場合にはリセットするように、ポイントツーポイント インターフェイスを設定します。 • *number* 引数のデフォルト値は 0 秒（即座に実行）です。 • 範囲は 0 ～ 255 です。 （注） NAS が認証失敗属性を解釈できるように、*number* 引数の値には最低でも 2 を設定する必要があります。
ステップ 6	**ppp authentication ms-chap-v2** 例： `Device(config-if)# ppp authentication ms-chap-v2`	NAS で MSCHAP V2 認証をイネーブルにします。

ステップ 7	**end**
	例：
	`Device(config-if)#`
	`end`
		特権 EXEC モードに戻ります。

MSCHAP V2 設定の確認

MSCHAP バージョン 2 機能が正しく設定されているかどうかを確認するには、次の手順を実行します。

手順の概要

1. **show running-config interface** *type number*
2. **debug ppp negotiation**
3. **debug ppp authentication**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**show running-config interface** *type number* 例： `Device# show running-config interface Asynch65`	MSCHAP V2 の設定が、指定されたインターフェイスの認証方式であることを確認します。
ステップ 2	**debug ppp negotiation** 例： `Device# debug ppp negotiation`	MSCHAP V2 のネゴシエーションが成功していることを確認します。
ステップ 3	**debug ppp authentication** 例： `Device# debug ppp authentication`	MSCHAP V2 認証が成功していることを確認します。

クリプトベースのクライアントのパスワード エージングの設定

AAA セキュリティ サービスにより、さまざまなログイン認証方式を容易に実行できるようになります。**aaa authentication login** コマンドを使用すると、サポートされているログイン認証方式のいずれを使用するかに関係なく、AAA 認証が有効になります。 **aaa authentication login** コマンドを使用すると、ログイン時に試行する認証方式リストを 1 つまたは複数作成できます。これらのリストは、**login authentication** ライン コンフィギュレーション コマンドによって適用されます。

RADIUS サーバが新しいパスワードを要求すると、AAA はクリプト クライアントにクエリーを実行し、今度はユーザに新しいパスワードを入力するように求めます。

クリプトベースのクライアントにログイン認証とパスワード エージングを設定するには、グローバル コンフィギュレーション モードで次のコマンドを使用します。

（注） AAA のパスワード失効インフラストラクチャは、パスワードが失効したことを Easy VPN に通知し、ユーザがパスワードを変更するための一般的な方法を提供します。RADIUS サーバのドメイン削除機能と AAA のパスワード失効のサポートをうまく組み合わせて使用してください。

手順の概要

1. **enable**
2. **configure terminal**
3. **aaa new-model**
4. **aaa authentication login** {**default** | *list-name*} **passwd-expiry** *method1* [*method2...*]
5. **crypto map** *map-name* **client authentication list** *list-name*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**aaa new-model** 例： `Device(config)# aaa new-model`	AAA をグローバルに有効にします。
ステップ 4	**aaa authentication login** {**default** | *list-name*} **passwd-expiry** *method1* [*method2...*] 例： `Device(config)# aaa authentication login userauthen passwd-expiry group radius`	ローカルの認証リストでクリプトベースのクライアントのパスワード エージングをイネーブルにします。
ステップ 5	**crypto map** *map-name* **client authentication list** *list-name* 例： 例： `Device(config)# crypto map clientmap client authentication list userauthen`	既存のクリプトマップで、ユーザ認証（認証方式のリスト）を設定します。

設定例

ローカル認証の設定の例

次の例では、非同期インターフェイスに PPP を設定し、ローカルで MSCHAP V2 認証をイネーブルにします。

```
interface Async65
  ip address 10.0.0.2 255.0.0.0
  encapsulation ppp
  async mode dedicated
```

```
  no peer default ip address
  ppp max-bad-auth 3
  ppp authentication ms-chap-v2
  username client password secret
```

RADIUS 認証の設定の例

次の例では、非同期インターフェイスに PPP を設定し、RADIUS を使用して MSCHAP V2 認証をイネーブルにします。

```
interface Async65
  ip address 10.0.0.2 255.0.0.0
  encapsulation ppp
  async mode dedicated
  no peer default ip address
  ppp max-bad-auth 3
  ppp authentication ms-chap-v2
  exit
aaa authentication ppp default group radius
 radius-server host 10.0.0.2 255.0.0.0
 radius-server key secret
 radius-server vsa send authentication
```

クリプト認証を使用したパスワード エージングの設定の例

次の例では、クリプトベースのクライアントを持つ AAA を使用して、パスワード エージングを設定します。

```
aaa authentication login userauthen passwd-expiry group radius
!
aaa session-id common
!
crypto isakmp policy 3
 encr 3des
 authentication pre-share
 group 2
!
crypto isakmp client configuration group 3000client
 key cisco123
 dns 10.1.1.10
 wins 10.1.1.20
 domain cisco.com
 pool ippool
 acl 153
!
crypto ipsec transform-set myset esp-3des esp-sha-hmac
!
crypto dynamic-map dynmap 10
 set transform-set myset
!
crypto map clientmap client authentication list userauthen
!
radius-server host 10.140.15.203 auth-port 1645 acct-port 1646
radius-server domain-stripping prefix-delimiter $
radius-server key cisco123
radius-server vsa send authentication
radius-server vsa send authentication 3gpp2
```

```
!
end
```

その他の参考資料

ここでは、MSCHAP バージョン 2 の機能に関する関連資料について説明します。

関連資料

関連項目	マニュアル タイトル
PPP インターフェイスの設定	『*Cisco IOS Dial Technologies Configuration Guide* , Release 12.4T』の「PPP Configuration」
シスコのネットワーキング装置の設定および管理に必要なタスクとコマンドの説明	『*Cisco IOS Dial Technologies Command Reference*』
IOS セキュリティ コマンドの一覧	『*Cisco IOS Security Command Reference*』
AAA を使用した PPP 認証の設定	『*Cisco IOS Security Configuration Guide: Securing User Services* , Release 12.4T』の「Configuring Authentication」モジュールの「Configuring PPP Authentication Using AAA」
RADIUS 認証の設定	『*Cisco IOS Security Configuration Guide: Securing User Services*, Release 12.4T』の「Configuring RADIUS」モジュール

標準

標準	タイトル
この機能がサポートする新しい規格または変更された規格はありません。	--

MIB

MIB	MIB のリンク
この機能によってサポートされる新しい MIB または変更された MIB はありません。	選択したプラットフォーム、Cisco IOS リリース、およびフィーチャ セットに関する MIB を探してダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

RFC

RFC	タイトル
RFC 1661	ポイントツーポイント プロトコル（*PPP*）
RFC 2548	『*Microsoft Vendor-specific RADIUS Attributes*』
RFC 2759	「*Microsoft PPP CHAP Extensions, Version 2*」

シスコのテクニカル サポート

説明	リンク
シスコのサポート Web サイトでは、シスコの製品やテクノロジーに関するトラブルシューティングにお役立ていただけるように、マニュアルやツールをはじめとする豊富なオンライン リソースを提供しています。 お使いの製品のセキュリティ情報や技術情報を入手するために、Cisco Notification Service（Field Notice からアクセス）、Cisco Technical Services Newsletter、Really Simple Syndication（RSS）フィードなどの各種サービスに加入できます。 シスコのサポート Web サイトのツールにアクセスする際は、Cisco.com のユーザ ID およびパスワードが必要です。	http://www.cisco.com/en/US/support/index.html

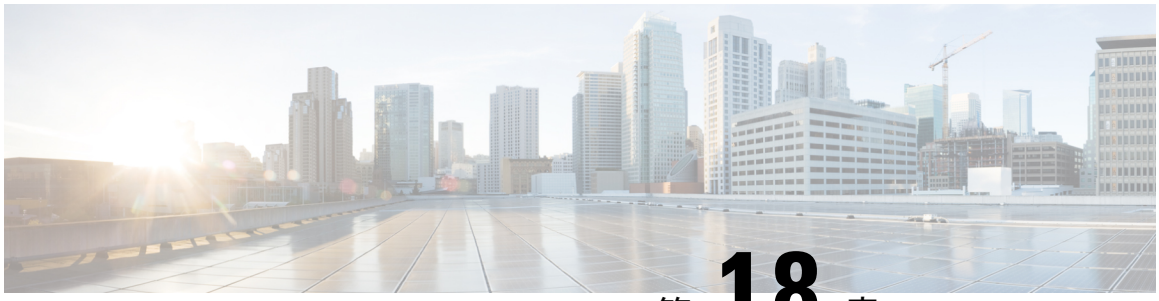
MSCHAP バージョン 2 の機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *35 : MSCHAP* バージョン *2* の機能情報

機能名	リリース	機能情報
MSCHAP バージョン 2	Cisco IOS XE Release 3.9S	MSCHAP バージョン 2 機能を使用すると、Cisco ルータは、Microsoft Windows オペレーティング システムを使用するコンピュータとネットワーク アクセス サーバ（NAS）間の PPP 接続にマイクロソフト チャレンジ ハンドシェイク認証プロトコル バージョン 2（MSCHAP V2）の認証を使用できます。 次のコマンドが導入または変更されました。**aaa authentication login** および **ppp authentication ms-chap-v2.**



第 18 章

AAA ブロードキャスト アカウンティング - 必須応答サポート

AAA ブロードキャスト アカウンティング - 必須応答サポート機能は、ゲートウェイ GPRS サポート ノード（GGSN）を介して各サーバ グループでのブロードキャスト アカウンティングをサポートするメカニズムを実現します。GGSN は、General Packet Radio Service（GPRS）のワイヤレス データ ネットワークと、インターネットやプライベート ネットワークなどその他のネットワーク間のゲートウェイとして動作します。

AAA ブロードキャスト アカウンティング - 必須応答サポートの前提条件

GGSN を設定するための準備作業の詳細については、『Cisco GGSN Release 8.0 Configuration Guide』を参照してください。

AAA ブロードキャスト アカウンティング - 必須応答サポートの制約事項

アカウンティング情報は、最大 10 台の AAA サーバに同時に送信することができます。

AAA ブロードキャスト アカウンティング - 必須応答サポートに関する情報

AAA ブロードキャスト アカウンティング - 必須応答サポート機能により、最大 10 個のサーバ グループ（方式）を方式リストで設定することができます。次の項では、GGSN をサポートするために使用される AAA アカウンティングの種類について説明します。

AAA ブロードキャスト アカウンティング

AAA ブロードキャスト アカウンティングを有効にすると、アカウンティング情報を複数の認証、許可、アカウンティング（AAA）サーバに同時に送信できます。つまり、アカウンティング情報を 1 つまた複数の AAA サーバに同時にブロードキャストすることが可能です。この機能を使用すると、サービス プロバイダーは自社使用のプライベート AAA サーバやエンドユーザの AAA サーバにアカウンティング情報を送信できるようになります。この機能では、音声アプリケーションによる課金情報も提供されます。

RADIUS サーバまたは TACACS+ サーバのサーバ グループ間でブロードキャストを実行できるほか、他のグループと関係なく、サーバ グループごとにフェールオーバー用のバックアップ サーバを定義できます。フェールオーバーは、複数のサーバがサーバ グループで定義されているときに発生する可能性のある処理で、サーバ グループの 1 番目のサーバに情報が送信されたとき、このサーバが使用できなくなっていれば、サーバ グループの次のサーバに情報が送信されるプロセスを指しています。このプロセスは、情報がサーバ グループ内の 1 つのサーバに正常に送信されるまで、またはサーバ グループ内の使用可能なサーバのリストがなくなるまで続きます。

ブロードキャストアカウンティングと待機アカウンティングの同時使用

Cisco GGSN リリース 8.0 以降では、ブロードキャスト アカウンティングと待機アカウンティングが一緒に動作するように設定できます。待機アカウンティング機能はアクセスポイント ネーム（APN）レベルで設定されるのに対し、ブロードキャスト アカウンティングは AAA 方式レベルで指定されます。

ブロードキャスト アカウンティングでは、開始、停止、中間の各アカウンティング レコードが方式リストで設定されているすべてのサーバ グループに送信されます。サーバ グループ内では、アカウンティング レコードは最初のアクティブなサーバに送信されます。アクティブ サーバに到達できない場合、アカウンティング レコードはグループの次のサーバに送信されます。

さらに、方式リストの 1 つまたは複数のサーバ グループを「必須」と設定することができます。これは、そのサーバ グループのサーバがアカウンティング開始メッセージに応答する必要があるということです。APN レベルの待機アカウンティングを有効にすると、パケット デー

タ プロトコル（PDP）コンテキストが確立される前に、すべての必須サーバ グループからのアカウンティング応答が受信されるようになります。

ブロードキャストアカウンティングと待機アカウンティングを同時に使用することの利点は、次のとおりです。

- アカウンティング レコードが複数のサーバに送信されます。エントリが作成されると、ユーザはさまざまなサービスの使用を開始できます。
- 冗長性を確保するため、複数の AAA サーバにレコードが送信されます。
- PDP コンテキストの確立は、すべての必須サーバが有効なアカウンティング開始レコードを受信したときにのみ確立され、情報の損失が防止されます。
- ブロードキャスト レコードは、方式リストの最大 10 個のサーバ グループに送信できます。

ブロードキャストアカウンティングと待機アカウンティングを同時に設定する場合は、次の点に注意してください。

- 方式リストの設定では、**mandatory** キーワードはブロードキャストアカウンティングが設定されている場合にだけ使用できます。
- 待機アカウンティングが必要ない場合、すべてのサーバ グループへのブロードキャストアカウンティングは、必須グループを定義しないで使用できます。
- ブロードキャストアカウンティングの設定時に必須サーバ グループを指定しない場合は、待機アカウンティングの機能は Cisco GGSN リリース 7.0 以前と同じになります。
- 待機アカウンティングは PPP PDP コンテキストには適用されません。
- PDP は、すべての必須サーバからアカウンティング応答が受信された場合にだけ作成されます。
- 定期的なタイマーは、アカウンティング応答（PDP 作成）が受信されたときに開始されます。

（注） 複数のサーバ グループを必須サーバ グループとして方式リストで定義できます。

GGSN での AAA ブロードキャスト アカウンティングのサポート方法

GGSN でのブロードキャスト アカウンティングと待機アカウンティングの設定

この項の作業では、GGSN でブロードキャスト アカウンティングと待機アカウンティングを設定する方法を説明します。

手順の概要

1. **enable**
2. **configure terminal**
3. **aaa new-model**
4. **aaa accounting network** {*method-list-name* | **default**}
5. **action-type** {**start-stop** | **stop-only**| **none**}
6. **broadcast**
7. **group** *server-group* [**mandatory**]
8. **exit**
9. **gprs access-point-list** *list-name*
10. **access-point** *access-point-index*
11. **aaa-group accounting** *method-list name*
12. **gtp-response-message wait-accounting**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**aaa new-model** 例： `Router# aaa new-model`	アクセス コントロールの新しいコマンドおよび機能を有効にします（以前のコマンドを無効にします）。

	コマンドまたはアクション	目的
ステップ 4	**aaa accounting network** {*method-list-name* | **default**} 例： `Router(config)# aaa accounting network net1`	RADIUS使用時の課金またはセキュリティ用に、要求されたサービスの認証、許可、アカウンティング（AAA）アカウンティングを有効にし、アカウンティング方式リスト モードを開始します。 • *method-list-name* 引数は、最大 31 文字の名前付きアカウンティング リストです。最大数を超える文字は、いずれも却下されます。 • **default** キーワードでは、デフォルトのアカウンティングリストを指定します。
ステップ 5	**action-type** {**start-stop** | **stop-only**| **none**} 例： `Router(cfg-acct-mlist)#action-type start-stop`	ある種のアクションをアカウンティング レコードで実行します。値は次のとおりです。 • **start-stop**：プロセスの開始時に "start" accounting 通知を送信し、プロセスの終了時に "stop" accounting 通知を送信します。 • **stop-only**：要求されたユーザープロセスの終了時に、"stop" アカウンティング通知を送信します。 • **none**：この回線またはインターフェイスでアカウンティングサービスをディセーブルにします。
ステップ 6	**broadcast** 例： `Router(cfg-acct-mlist)#broadcast`	（任意）複数の AAA サーバへのアカウンティング レコードの送信をイネーブルにします。各グループの最初のサーバに対し、アカウンティング レコードを同時に送信します。最初のサーバが使用できない場合はフェールオーバーが発生し、そのグループ内に定義されているバックアップ サーバが使用されます。
ステップ 7	**group** *server-group* [**mandatory**] 例： `Router(cfg-acct-mlist)#group server1`	サーバ グループを指定します。必要に応じて、**mandatory** キーワードを指定して、サーバーグループを必須と定義します。サーバ グループが必須である場合、そのサーバ グループのサーバがアカウンティング開始メッセージに応答する必要があります。 （注） 最大 10 個のサーバ グループを 1 つの方式リストで定義できます。

	コマンドまたはアクション	目的
ステップ 8	**exit**	アカウンティング方式リストのコンフィギュレーション モードを終了します。
ステップ 9	**gprs access-point-list** *list-name* 例： `Router(config)# gprs access-point-list public1`	GGSN でパブリック データ ネットワーク（PDN）のアクセス ポイントを定義するためのアクセス ポイント リストを設定し、グローバル コンフィギュレーション モードを開始します。
ステップ 10	**access-point** *access-point-index* 例： `Router(config-ap-list)# access-point 11`	アクセス ポイント番号を指定し、アクセス ポイント コンフィギュレーション モードを開始します。
ステップ 11	**aaa-group accounting** *method-list name* 例： `Router(config-access-point)#aaa-group accounting net1`	アカウンティング サーバ グループを指定します。
ステップ 12	**gtp-response-message wait-accounting** 例： `Router(config-access-point)# gtp-response-message wait-accounting`	サービング GPRS サポート ノード（SGSN）に Create PDP Context Response を送信する前に、RADIUS アカウンティング応答を待機するように APN を設定します。

AAA ブロードキャスト アカウンティング - 必須応答サポートの設定例

AAA ブロードキャスト アカウンティング - 必須応答サポートの例

次の例では、SGSN に Create PDP Context Response を送信する前に、RADIUS サーバからの RADIUS アカウンティング応答を待機するように GGSN がグローバルに設定されます。GGSN は、access-point 1 を除くすべてのアクセス ポイントで受信された PDP コンテキスト要求の応答を待機します。RADIUS 応答メッセージの待機は、**no gtp response-message wait-accounting** コマンドを使用して access-point 1 で無効化されています。

```
! Enables AAA globally
!
aaa new-model
!
! Defines AAA server group
!
aaa group server radius abc
 server 10.2.3.4 auth-port 1645 acct-port 1646
```

```
 server 10.6.7.8 auth-port 1645 acct-port 1646
!
! Configures AAA authentication and authorization
!
aaa authentication ppp abc group abc
aaa authorization network abc group abc
aaa accounting network abc
 action-type start-stop
 broadcast
 group SG1 mandatory
 group SG2
 group SG3 mandatory
!
gprs access-point-list gprs
 access-point 1
  access-mode non-transparent
  access-point-name www.pdn1.com
  aaa-group authentication abc
!
! Disables waiting for RADIUS response
! message at APN 1
!
  no gtp response-message wait-accounting
  exit
access-point 2
 access-mode non-transparent
 access-point-name www.pdn2.com
 aaa-group authentication abc
!
! Enables waiting for RADIUS response
! messages across all APNs (except APN 1)
!
gprs gtp response-message wait-accounting
!
! Configures global RADIUS server hosts
! and specifies destination ports for
! authentication and accounting requests
!
radius-server host 10.2.3.4 auth-port 1645 acct-port 1646 non-standard
radius-server host 10.6.7.8 auth-port 1645 acct-port 1646 non-standard
radius-server key ggsntel
```

その他の参考資料

ここでは、AAA ブロードキャスト アカウンティング - 必須応答サポート機能に関する参考資料を紹介します。

関連資料

関連項目	マニュアル タイトル
GGSN の設定の準備作業	『*Cisco GGSN Release 8.0 Configuration Guide*』
AAA コマンド	『*Cisco IOS Security Command Reference Guide*』
AAA 機能	『*Cisco IOS Security Configuration Guide: Securing User Services*』

標準

標準	タイトル
この機能でサポートされる新規の標準または変更された標準はありません。また、既存の標準のサポートは変更されていません。	--

MIB

MIB	MIB のリンク
この機能によってサポートされる新しい MIB または変更された MIB はありません。またこの機能による既存MIBのサポートに変更はありません。	選択したプラットフォーム、Cisco IOS リリース、およびフィーチャ セットに関する MIB を探してダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

RFC

RFC	タイトル
この機能によりサポートされた新規 RFC または改訂 RFC はありません。またこの機能による既存 RFC のサポートに変更はありません。	--

シスコのテクニカル サポート

説明	リンク
シスコのサポート Web サイトでは、シスコの製品やテクノロジーに関するトラブルシューティングにお役立ていただけるように、マニュアルやツールをはじめとする豊富なオンライン リソースを提供しています。 お使いの製品のセキュリティ情報や技術情報を入手するために、Cisco Notification Service（Field Notice からアクセス）、Cisco Technical Services Newsletter、Really Simple Syndication（RSS）フィードなどの各種サービスに加入できます。 シスコのサポート Web サイトのツールにアクセスする際は、Cisco.com のユーザ ID およびパスワードが必要です。	http://www.cisco.com/en/US/support/index.html

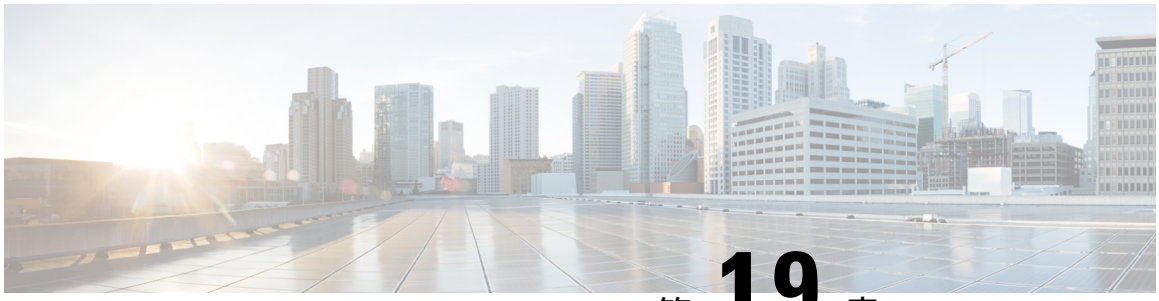
AAA ブロードキャスト アカウンティング - 必須応答サポートの機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *36 : AAA* ブロードキャスト アカウンティング - 必須応答サポートの機能情報

機能名	リリース	機能情報
AAA ブロードキャスト アカウンティング - 必須応答サポート	Cisco IOS XE Release 3.9S	AAA ブロードキャスト アカウンティング - 必須応答サポート機能は、ゲートウェイ GPRS サポート ノード（GGSN）を介して各サーバ グループでのブロードキャスト アカウンティングをサポートするメカニズムを実現します。GGSN は、General Packet Radio Service（GPRS）のワイヤレス データ ネットワークと、インターネットやプライベート ネットワークなどその他のネットワーク間のゲートウェイとして動作します。 次のコマンドが導入または変更されました。**aaa accounting network**、**aaa-group accounting**、**access-point**、**action-type**、**broadcast**、**gprs access-point-list**、**group**、**gtp-response-message wait-accounting**



第 19 章

コモン クライテリアに準拠したパスワードの強度と管理

コモン クライテリアに準拠したパスワードの強度と管理機能は、ユーザ パスワードを指定するルールの保存、検索、提供のためのパスワード ポリシーおよびセキュリティ メカニズムを指定するために使用されます。

ローカルユーザについては、ユーザのプロファイルとパスワード情報が重要なパラメータとともにシスコデバイスに保存され、このプロファイルを使用して、ユーザのローカル認証が行われます。このユーザになり得るのは、管理者（ターミナルアクセス）またはネットワークユーザ（たとえば、ネットワーク アクセスのために認証された PPP ユーザ）です。

リモート ユーザについては、ユーザ プロファイル情報がリモート サーバに保存されている場合、管理アクセスとネットワーク アクセスの双方にサードパーティの認証、許可、およびアカウンティング（AAA）サーバを使って AAA サービスが提供される可能性があります。

コモンクライテリアに準拠したパスワードの強度と管理の制約事項

- vty を使用して同時にシステムにログインできるユーザは 4 人までです。

コモンクライテリアに準拠したパスワードの強度と管理に関する情報

パスワード構成ポリシー

パスワード構成ポリシーでは、パスワードを作成するために、英字の大文字小文字、数字、特殊文字（「!」、「@」、「#」、「$」、「%」、「^」、「&」、「*」、「(」、「)」など）を自由に組み合わせて使用できます。

パスワード長ポリシー

パスワードの最小長と最大長は、管理者により柔軟に設定することが可能です。推奨されるパスワードの最小長は 8 文字です。管理者は、パスワードの最小長（1）も最大長（64）も指定できます。

パスワード ライフタイム ポリシー

セキュリティ管理者は、パスワードのライフタイムを最大限にするための設定可能オプションを提供できます。ライフタイムパラメータが設定されていない場合、設定済みのパスワードは無限に有効です。最大ライフタイムは、設定可能な値を年、月、日、時間、分、および秒単位で入力することにより設定できます。ライフタイム設定は設定の一部であるためリロード後も有効ですが、パスワード作成時刻はシステムがリブートするたびに新しい時刻に更新されます。たとえば、パスワードに1ヵ月のライフタイムが設定されており、29日目にシステムがリブートした場合、そのパスワードはシステム リブート後 1 ヵ月間有効になります。

月数を使用してライフタイムを設定すると、ポリシーは、指定された月の日数に関係なくライフタイムを 30 日に設定します。

パスワード有効期限ポリシー

ユーザがログインを試みたときにこのユーザのパスワードクレデンシャルが期限切れになっていた場合、次の処理が行われます。

1. ユーザは、期限切れのパスワードの入力に成功した後、新しいパスワードを設定するよう求められます。
2. ユーザが新しいパスワードを入力すると、パスワード セキュリティ ポリシーに照らしてそのパスワードが検証されます。
3. 新しいパスワードがパスワードセキュリティポリシーに適合していれば、AAAデータベースが更新され、ユーザーは新しいパスワードで認証されます。

4. 新しいパスワードがパスワード セキュリティ ポリシーに適合していない場合、ユーザは再度パスワードの入力を求められます。再試行数は、AAA では制限されていません。認証失敗の場合のパスワード プロンプトの再試行数は、それぞれのターミナル アクセス インタラクティブ モジュールによって制御されます。たとえば Telnet では、3 回失敗するとセッションが終了します。

パスワードのライフタイムを設定されていないユーザがすでにログインしているときに、セキュリティ管理者がそのユーザのライフタイムを設定すると、ライフタイムがデータベースに設定されます。同じユーザが次回に認証されるときに、システムがパスワードの期限を確認します。パスワード期限がチェックされるのは認証フェーズの間のみです。

すでに認証済みかつシステムにログイン中のユーザのパスワードが期限切れになっても、何のアクションも起こりません。同じユーザが次に認証されるときに初めて、ユーザにパスワード変更が求められます。

パスワード変更ポリシー

新しいパスワードは、前のパスワードから 4 文字以上変更されている必要があります。パスワード変更のきっかけとなるシナリオとしては、次のようなものが考えられます。

- セキュリティ管理者がパスワードの変更を求める場合。
- ユーザがプロファイル使用による認証を試みたが、そのプロファイルのパスワードが期限切れになっている場合。

セキュリティ管理者がパスワード セキュリティ ポリシーを変更し、既存のプロファイルがそのパスワード セキュリティ ポリシー ルールに適合しなくなっても、ユーザがすでにシステムにログインしている場合には、何のアクションも起こりません。ユーザは、パスワードセキュリティ制限に適合しないプロファイルを使用して認証を試みたときに初めて、パスワードを変更するよう求められます。

ユーザがパスワードを変更すると、セキュリティ管理者によって古いプロファイルに設定されているライフタイム パラメータが、新しいパスワードのライフタイム パラメータとして引き継がれます。

dot1x などの非インタラクティブ クライアントでは、パスワードの期限が切れると、適切なエラー メッセージがクライアントに送られます。クライアントは、セキュリティ管理者に連絡してパスワードを更新する必要があります。

ユーザ再認証ポリシー

ユーザがパスワードを変更すると、ユーザの再認証が行われます。

期限満了時にパスワードを変更すると、新しいパスワードに対してユーザ認証が行われます。このような場合、実際には、以前のクレデンシャルに基づいて認証が行われ、データベースで新しいパスワードが更新されます。

（注） ユーザがパスワードを変更できるのは、ログイン中かつ古いパスワードの期限が切れた後のみです。ただし、セキュリティ管理者はこのユーザのパスワードをいつでも変更できます。

フレームド（非インタラクティブ）セッションのサポート

dot1x などのクライアントがローカルデータベースを使用して認証を行うときには、コモン クライテリアに準拠したパスワードの強度と管理機能が適用されます。ただし、パスワードの期限が切れると、クライアントによるパスワード変更はできなくなります。そのようなクライアントには適切なエラー メッセージが送られます。そのユーザは、セキュリティ管理者にパスワードの変更を要求する必要があります。

コモンクライテリアに準拠したパスワードの強度と管理の設定方法

パスワード セキュリティ ポリシーの設定

パスワード セキュリティ ポリシーを作成し、そのポリシーを特定のユーザー プロファイルに適用するには、次の作業を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **aaa new-model**
4. **aaa common-criteria policy** *policy-name*
5. **char-changes** *number*
6. **max-length** *number*
7. **min-length** *number*
8. **numeric-count** *number*
9. **special-case** *number*
10. **exit**
11. **username** *username* **common-criteria-policy** *policy-name* **password** *password*
12. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例：	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。

	コマンドまたはアクション	目的
	`Device> enable`	
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**aaa new-model** 例： `Device(config)# aaa new-model`	AAA をグローバルに有効にします。
ステップ 4	**aaa common-criteria policy** *policy-name* 例： `Device(config)# aaa common-criteria policy policy1`	AAAセキュリティ パスワード ポリシーを作成し、コモン クライテリア設定ポリシー モードを開始します。
ステップ 5	**char-changes** *number* 例： `Device(config-cc-policy)# char-changes 4`	（任意）古いパスワードから新規のパスワードへの変更文字数を指定します。
ステップ 6	**max-length** *number* 例： `Device(config-cc-policy)# max-length 25`	（任意）パスワードの最大長を指定します。
ステップ 7	**min-length** *number* 例： `Device(config-cc-policy)# min-length 8`	（任意）パスワードの最小長を指定します。
ステップ 8	**numeric-count** *number* 例： `Device(config-cc-policy)# numeric-count 4`	（任意）パスワード内の数字の数を指定します。
ステップ 9	**special-case** *number* 例： `Device(config-cc-policy)# special-case 3`	（任意）パスワード内の特殊文字の数を指定します。

	コマンドまたはアクション	目的
ステップ 10	**exit** 例： `Device(config-cc-policy)# exit`	（任意）コモン クライテリア設定ポリシー モードを終了し、グローバル コンフィギュレーション モードに戻ります。
ステップ 11	**username** *username* **common-criteria-policy** *policy-name* **password** *password* 例： `Device(config)# username user1 common-criteria-policy policy1 password password1`	（任意）ユーザ プロファイルに特定のポリシーとパスワードを適用します。
ステップ 12	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。

コモン クライテリア ポリシーの確認

すべてのコモン クライテリア セキュリティ ポリシーを確認するには、次の作業を実行します。

手順の概要

1. **enable**
2. **show aaa common-criteria policy name** *policy-name*
3. **show aaa common-criteria policy all**

手順の詳細

ステップ 1 **enable**

特権 EXEC モードをイネーブルにします。

例：

```
Device> enable
```

ステップ 2 **show aaa common-criteria policy name** *policy-name*

特定のポリシーのパスワード セキュリティ ポリシー情報を表示します。

例：

```
Device# show aaa common-criteria policy name policy1

Policy name: policy1
Minimum length: 1
Maximum length: 64
```

```
Upper Count: 20
Lower Count: 20
Numeric Count: 5
Special Count: 2
Number of character changes 4
Valid forever. User tied to this policy will not expire.
```

ステップ 3 show aaa common-criteria policy all

設定されたすべてのポリシーのパスワード セキュリティ ポリシー情報を表示します。

例：

```
Device# show aaa common-criteria policy all
==========================================================================
Policy name: policy1
Minimum length: 1
Maximum length: 64
Upper Count: 20
Lower Count: 20
Numeric Count: 5
Special Count: 2
Number of character changes 4
Valid forever. User tied to this policy will not expire.
==========================================================================
Policy name: policy2
Minimum length: 1
Maximum length: 34
Upper Count: 10
Lower Count: 5
Numeric Count: 4
Special Count: 2
Number of character changes 2
Valid forever. User tied to this policy will not expire.
==========================================================================
```

トラブルシューティングのヒント

debug aaa common-criteria コマンドを使用して、AAA コモンクライテリアをトラブルシューティングします。

コモンクライテリアに準拠したパスワードの強度と管理の機能の設定例

例：コモン クライテリアに準拠したパスワードの強度と管理

次の例は、コモン クライテリア セキュリティ ポリシーを作成し、特定のポリシーをユーザ プロファイルに適用する方法を示しています。

```
Device> enable
Device# configure terminal
```

```
Device(config)# aaa new-model
Device(config)# aaa common-criteria policy policy1
Device(config-cc-policy)# char-changes 4
Device(config-cc-policy)# max-length 20
Device(config-cc-policy)# min-length 6
Device(config-cc-policy)# numeric-count 2
Device(config-cc-policy)# special-case 2
Device(config-cc-policy)# exit
Device(config)# username user1 common-criteria-policy policy1 password password1
Device(config)# end
```

その他の参考資料

次の項で、RADIUS パケット オブ ディスコネクト機能に関する参考資料を紹介します。

関連資料

関連項目	マニュアル タイトル
AAA	『*Cisco IOS XE Security Configuration Guide, Securing User Services*, Release 2』の「Authentication, Authorization, and Accounting (AAA)」
セキュリティ コマンド	『*Cisco IOS Security Command Reference*』
CLI 設定	『*Cisco IOS XE Configuration Fundamentals Configuration Guide*, Release 2』

標準

標準	タイトル
この機能でサポートされる新規の標準または変更された標準はありません。また、既存の標準のサポートは変更されていません。	--

MIB

MIB	MIB のリンク
この機能によってサポートされる新しい MIB または変更された MIB はありません。またこの機能による既存 MIB のサポートに変更はありません。	選択したプラットフォーム、Cisco IOS XE ソフトウェア リリース、およびフィーチャ セットの MIB の場所を検索しダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

RFC

RFC	タイトル
RFC 2865	『*Remote Authentication Dial-in User Service*』
RFC 3576	『*Dynamic Authorization Extensions to RADIUS*』

シスコのテクニカル サポート

説明	リンク
シスコのサポート Web サイトでは、シスコの製品やテクノロジーに関するトラブルシューティングにお役立ていただけるように、マニュアルやツールをはじめとする豊富なオンライン リソースを提供しています。 お使いの製品のセキュリティ情報や技術情報を入手するために、Cisco Notification Service（Field Notice からアクセス）、Cisco Technical Services Newsletter、Really Simple Syndication（RSS）フィードなどの各種サービスに加入できます。 シスコのサポート Web サイトのツールにアクセスする際は、Cisco.com のユーザ ID およびパスワードが必要です。	http://www.cisco.com/en/US/support/index.html

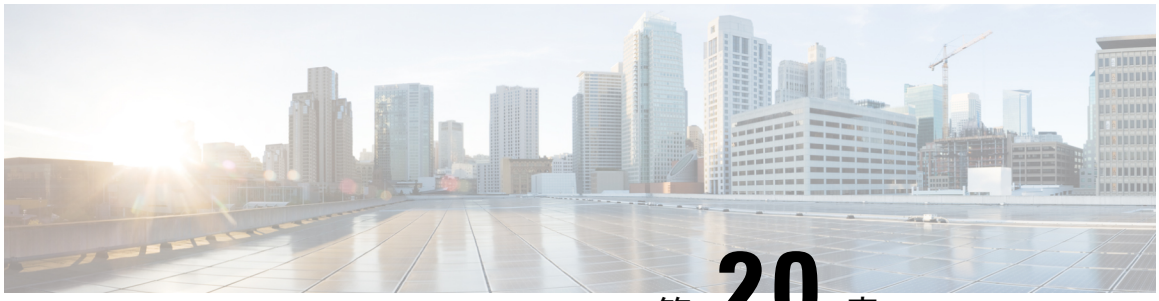
コモンクライテリアに準拠したパスワードの強度と管理の機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *37 :* コモン クライテリアに準拠したパスワードの強度と管理の機能情報

機能名	リリース	機能情報
コモン クライテリアに準拠したパスワードの強度と管理		コモン クライテリアに準拠したパスワードの強度と管理機能は、ユーザーパスワードを指定するルールの保存、検索、提供のためのパスワード ポリシーおよびセキュリティ メカニズムを指定するために使用されます。 次のコマンドが導入または変更されました。**aaa common-criteria policy**、**debug aaa common-criteria**、および **show aaa common-criteria policy**。



第 20 章

AAA 用のセキュアな可逆パスワード

AAA 用のセキュアな可逆パスワードの機能は、タイプ 6 の AES（Advanced Encryption Scheme）パスワードによる認証、許可、およびアカウンティング（AAA）設定のセキュアな可逆暗号化を可能にします。

AAA 用のセキュアな可逆パスワードの前提条件

タイプ 6 パスワード暗号化では、次のコマンドを有効にする必要があります。

- **password encryption aes**
- **key config-key password-encrypt** [*password*]
- **aaa new-model**

AAA 用のセキュアな可逆パスワードに関する情報

セキュアな可逆パスワード

Cisco IOS 設定のパスワードには、セキュアなストレージが必要です。これにより、必要なときにいつでも認証方式がユーザーログイン情報にアクセスできるように、可逆暗号化のキーを保存できます。

可逆暗号化は、可逆的な対称暗号化アルゴリズムを使用してパスワードを暗号化するプロセスです。ユーザーが入力したパスワードが有効かどうかを確認するために、パスワードが復号され、ユーザーが入力したパスワードと比較されます。この暗号化を実行するには、対称暗号化アルゴリズムにキーが必要です。

タイプ 6 の高度暗号化方式（AES）で暗号化されたパスワードは、認証、許可、およびアカウンティング（AAA）機能の可逆パスワードを保護するために役立ちます。このタイプ 6 の暗号キーは、プライベート NVRAM に保存され、保護されます。

AAA ネットワーク設定では、Lightweight Directory Access Protocol（LDAP）、RADIUS、またはTACACS+ サーバーホストが使用されます。RADIUS、TACACS+、またはLDAP ホストサーバーを設定するには、それぞれ **radius server host** コマンド、**tacacs-server host** コマンド、および **ldap server** コマンドを使用します。

タイプ 6 暗号化の設定

次のコマンドが、認証、許可、およびアカウンティング（AAA）機能を設定するためのセキュアな可逆パスワードを有効にする type **6** キーワードで更新されました。セキュリティコマンドの詳細については、『*Cisco IOS Security Command Reference*』を参照してください。AAA 設定の詳細については、『*Authentication, Authorization, and Accounting Configuration Guide*』を参照してください。

- **aaa configuration**
  - **aaa configuration** {**config-username username** *username* [**password** [**0** | **7**] *password*] | {**pool** | **route**} **username** *username* [**password** [**0** | **6** | **7**] *password*}
- **bind authenticate root-dn (config-ldap-server)**
  - **bind authenticate root-dn** *username* **password** {**0** *string* | **6** *string* | **7** *string*} *string*
- **client (config-locsvr-da-radius)**
  - **client** *ip-address* **server-key** [**0** | **6** | **7**] *word*
- **key (config-radius-server)**
  - **key** {**0** *string* | **6** *string* | **7** *string*} *string*
- **key (config-server-tacacs)**
  - **key** {**0** *string* | **6** *string* | **7** *string*} *string*
- **pac key (config-radius-server)**
  - **pac key** {**0** *string* | **6** *string* | **7** *string*} *string*
- **password (config-filter)**
  - **password** [**0** | **6** | **7**] *password*
- **server-private (RADIUS)**
  - **server-private** *ip-address* [**auth-port** *port-number* | **acct-port** *port-number*] [**non-standard**] [**timeout** *seconds*] [**retransmit** *retries*] [**key** [**0** | **6** | **7**] *string*]
- **server-private (TACACS+)**

- **server-private** {*ip-address* | *name* | *ipv6-address*} [**nat**] [**single-connection**] [**port** *port-number*] [**timeout** *seconds*] [**key** [**0** | **6** | **7**] *string*]

- **tacacs-server host**
  - **tacacs-server host** {*host-name* | *host-ip-address*} [**key** {**0** *string* | **6** *string* | **7** *string*} *string*] [[**nat**] [**port** [*integer*]] [**single-connection**] [**timeout** [*integer*]]]

- **tacacas-server key**
  - **tacacs-server key** {**0** *string* | **6** *string* | **7** *string*} *string*

AAA 用のセキュアな可逆パスワードに関する追加情報

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『Cisco IOS Master Command List, All Releases』
セキュリティ コマンド	• 『Cisco IOS Security Command Reference: Commands A to C』[英語] • 『Cisco IOS Security Command Reference: Commands D to L』[英語] • 『Cisco IOS Security Command Reference: Commands M to R』[英語] • 『Cisco IOS Security Command Reference: Commands S to Z』[英語]
AAA の設定	『*Authentication, Authorization, and Accounting Configuration Guide*』

シスコのテクニカル サポート

説明	リンク
シスコのサポート Web サイトでは、シスコの製品やテクノロジーに関するトラブルシューティングにお役立ていただけるように、マニュアルやツールをはじめとする豊富なオンライン リソースを提供しています。 お使いの製品のセキュリティ情報や技術情報を入手するために、Cisco Notification Service（Field Notice からアクセス）、Cisco Technical Services Newsletter、Really Simple Syndication（RSS）フィードなどの各種サービスに加入できます。 シスコのサポート Web サイトのツールにアクセスする際は、Cisco.com のユーザ ID およびパスワードが必要です。	http://www.cisco.com/support

AAA 用のセキュアな可逆パスワードに関する機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

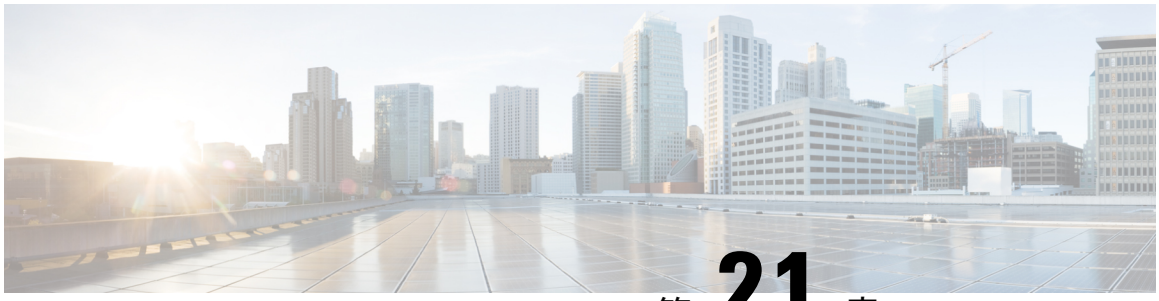
プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *38 : AAA* 用のセキュアな可逆パスワードに関する機能情報

機能名	リリース	機能情報
AAA 用のセキュアな可逆パスワード	15.4(1)T	AAA 用のセキュアな可逆パスワードの機能は、タイプ 6 の AES（Advanced Encryption Scheme）パスワードによる認証、許可、およびアカウンティング（AAA）設定のセキュアな可逆暗号化を可能にします。 次のコマンドが導入または変更されました。**aaa configuration**、**bind authenticate root-dn (config-ldap-server)**、**client (config-locsvr-da-radius)**、**key (config-radius-server)**、**key (config-server-tacacs)**、**pac key (config-radius-server)**、**password (config-filter)**、**server-private (RADIUS)**、**server-private (TACACS+)**、**tacacs-server host**、および **tacacas-server key**。

第 II 部

セキュア シェル



第 21 章

リバース SSH 拡張

セキュア シェル（SSH）のバージョン 1 と 2 に対してサポートされているリバース SSH 拡張機能は、SSH を有効にしなければならない端末または補助回線ごとに別々の回線を設定する必要がないようにリバース SSH を設定する代替手段を提供します。この機能は、ロータリー グループの制限も排除します。

リバース SSH 拡張の前提条件

- SSH を有効にする必要があります。
- SSH クライアントとサーバーで同じバージョンの SSH が動作している必要があります。

リバース SSH 拡張の制約事項

- リバース SSH の代替手段をコンソール アクセス用に設定する場合、**-l** キーワード、*userid* **:**{*number*} {*ip-address*} デリミタ、および引数が必須です。

リバース SSH 拡張に関する情報

リバース Telnet

リバース Telnet を使用すると、特定のポート範囲に Telnet を実行したり、端末または補助回線に接続することができます。リバース Telnet は、他のシスコ デバイスのコンソールへの端末回線を複数内蔵したシスコ デバイスとの接続によく使用されていました。Telnet を使用すると、特定の回線上のターミナル サーバに Telnet することによって、どの場所からでも簡単にデバイス コンソールに到達できます。この Telnet アプローチは、デバイスへのすべてのネットワーク接続が切断されている場合でも、そのデバイスの設定に使用できます。また、リバース Telnet は、シスコ デバイスに接続されたモデムをダイヤルアウトに使用することもできます（通常は、ロータリー デバイスと一緒に使用します）。

リバース SSH

リバース Telnet は SSH を使用して実現できます。リバース Telnet と違って、SSH はセキュアな接続を提供します。リバース SSH 拡張機能は、SSH の設定を容易にします。この機能を使用すれば、SSH を有効にする端末または補助回線ごとに別々の回線を設定する必要がなくなります。以前のリバース SSH 設定方法では、アクセスできるポートの数が 100 に制限されていました。リバース SSH 拡張機能では、ポートの数に制限がありません。リバース SSH 設定の代替手段については、リバース SSH 拡張の設定方法 （292 ページ）を参照してください。

リバース SSH 拡張の設定方法

コンソール アクセス用のリバース SSH の設定

SSH サーバ上でリバース SSH コンソール アクセスを設定するには、次の手順を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **line** *line-number ending-line-number*
4. **no exec**
5. **login authentication** *listname*
6. **transport input ssh**
7. **exit**
8. **exit**
9. **ssh -l** *userid* **:** {*number*} {*ip-address*}

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**line** *line-number ending-line-number* 例： `Device# line 1 3`	設定用の回線を特定して、ライン コンフィギュレーション モードに入ります。
ステップ 4	**no exec** 例： `Device(config-line)# no exec`	回線上の EXEC 処理を無効にします。
ステップ 5	**login authentication** *listname* 例： `Device(config-line)# login authentication default`	回線のログイン認証メカニズムを定義します。 （注） 認証方式はユーザ名とパスワードを使用する必要があります。
ステップ 6	**transport input ssh** 例： `Device(config-line)# transport input ssh`	デバイスの特定の回線への接続に使用されるプロトコルを定義します。 • リバース SSH 拡張機能の場合は、**ssh** キーワードを使用する必要があります。
ステップ 7	**exit** 例： `Device(config-line)# exit`	ライン コンフィギュレーション モードを終了します。
ステップ 8	**exit** 例： `Device(config)# exit`	グローバル コンフィギュレーション モードを終了します。

	コマンドまたはアクション	目的
ステップ 9	**ssh -l** *userid* **:** {*number*} {*ip-address*} 例： `Device# ssh -l lab:1 router.example.com`	SSH サーバを実行しているリモート ネットワーキング デバイスにログインするときに使用されるユーザ ID を指定します。 • *userid*：ユーザー ID。 • **:**：ポート番号と端末 IP アドレスが userid 引数に続くことを示します。 • *number*：端末番号または補助回線番号。 • *ip-address*：ターミナル サーバーの IP アドレス。 （注） リバース SSH の代替手段をモデム アクセス用に設定する場合は、*userid* 引数、**:rotary**{*number*}{*ip-address*} デリミタ、および引数が必須です。

モデム アクセス用のリバース SSH の設定

リバース SSH をモデム アクセス用に設定するには、後述の「手順の概要」で示す手順を実行します。

この設定では、リバース SSH がダイヤルアウト回線に使用されるモデム上で設定されます。ダイヤルアウト モデムのいずれかに到達するには、下のステップ 10 に示すように、任意の SSH クライアントを使用して SSH セッションを開始し、ロータリー デバイスから次に使用可能なモデムに到達します。

手順の概要

1. **enable**
2. **configure terminal**
3. **line** *line-number ending-line-number*
4. **no exec**
5. **login authentication** *listname*
6. **rotary** *group*
7. **transport input ssh**
8. **exit**
9. **exit**
10. **ssh -l** *userid* **:rotary** {*number*} {*ip-address*}

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**line** *line-number ending-line-number* 例： `Device# line 1 200`	設定用の回線を特定して、ライン コンフィギュレーション モードに入ります。
ステップ 4	**no exec** 例： `Device(config-line)# no exec`	回線上の EXEC 処理を無効にします。
ステップ 5	**login authentication** *listname* 例： `Device(config-line)# login authentication default`	回線のログイン認証メカニズムを定義します。 （注） 認証方式はユーザ名とパスワードを使用する必要があります。
ステップ 6	**rotary** *group* 例： `Device(config-line)# rotary 1`	1 つ以上の仮想端末回線または 1 つの補助ポート回線からなる回線グループを定義します。
ステップ 7	**transport input ssh** 例： `Device(config-line)# transport input ssh`	デバイスの特定の回線への接続に使用されるプロトコルを定義します。 • リバース SSH 拡張機能の場合は、**ssh** キーワードを使用する必要があります。
ステップ 8	**exit** 例： `Device(config-line)# exit`	ライン コンフィギュレーション モードを終了します。
ステップ 9	**exit** 例：	グローバル コンフィギュレーション モードを終了します。

	コマンドまたはアクション	目的
	`Device(config)# exit`	
ステップ 10	**ssh -l** *userid* **:rotary** {*number*} {*ip-address*} 例： `Device# ssh -l lab:rotary1 router.example.com`	SSH サーバを実行しているリモート ネットワーキングデバイスにログインするときに使用されるユーザ ID を指定します。 • *userid*：ユーザー ID。 • **:**：ポート番号と端末 IP アドレスが *userid* 引数に続くことを示します。 • *number*：端末番号または補助回線番号。 • *ip-address*：ターミナル サーバーの IP アドレス。 （注） リバース SSH の代替手段をモデム アクセス用に設定する場合は、*userid* 引数、**:rotary**{*number*}{*ip-address*} デリミタ、および引数が必須です。

クライアント上でのリバース SSH のトラブルシューティング

クライアント（リモート デバイス）上でリバース SSH 設定の問題を解決するには、次の手順を実行します。

手順の概要

1. **enable**
2. **debug ip ssh client**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**debug ip ssh client** 例： `Device# debug ip ssh client`	SSH クライアントに関するデバッギング メッセージを表示します。

サーバ上でのリバース SSH のトラブルシューティング

ターミナル サーバ上でリバース SSH 設定の問題を解決するには、次の手順を実行します。各ステップは、互いに独立しているため、任意の順序で設定できます。

手順の概要

1. **enable**
2. **debug ip ssh**
3. **show ssh**
4. **show line**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**debug ip ssh** 例： `Device# debug ip ssh`	SSH サーバに関するデバッギング メッセージを表示します。
ステップ 3	**show ssh** 例： `Device# show ssh`	SSH サーバ接続のステータスを表示します。
ステップ 4	**show line** 例： `Device# show line`	端末回線のパラメータを表示します。

リバース SSH 拡張の設定例

リバース SSH コンソール アクセスの例

次の設定例は、リバース SSH が端末回線 1 ～ 3 のコンソール アクセス用に設定されていることを示しています。

ターミナル サーバーの設定

```
line 1 3
   no exec
   login authentication default
   transport input ssh
```

クライアント設定

SSHクライアント上で設定された次のコマンドは、それぞれ、回線1、2、および3とのリバース SSH セッションを形成します。

```
ssh -l lab:1 router.example.com
ssh -l lab:2 router.example.com
ssh -l lab:3 router.example.com
```

リバース SSH モデム アクセスの例

次の設定例では、ダイヤルアウト回線の 1 ～ 200 がモデム アクセス用のロータリー グループ 1 にグループ分けされています。

```
line 1 200
   no exec
   login authentication default
   rotary 1
   transport input ssh
   exit
```

次のコマンドは、リバース SSH がロータリー グループの最初の空き回線に接続されることを表示します。

```
ssh -l lab:rotary1 router.example.com
```

その他の参考資料

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『Cisco IOS Master Commands List, All Releases』
セキュア シェルの設定	『セキュア シェル コンフィギュレーション ガイド』
セキュリティ コマンド	『Cisco IOS セキュリティ コマンド リファレンス』

シスコのテクニカル サポート

説明	リンク
右の URL にアクセスして、シスコのテクニカル サポートを最大限に活用してください。これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『Cisco IOS Master Commands List, All Releases』
セキュア シェルの設定	『セキュア シェル コンフィギュレーション ガイド』
セキュリティ コマンド	『Cisco IOS セキュリティ コマンド リファレンス』

標準

標準	タイトル
この機能がサポートする新しい規格または変更された規格はありません。	--

MIB

MIB	MIB のリンク
なし	選択したプラットフォーム、Cisco ソフトウェア リリース、およびフィーチャ セットの MIB を検索してダウンロードする場合は、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

RFC

RFC	タイトル
なし	--

シスコのテクニカル サポート

説明	リンク
右の URL にアクセスして、シスコのテクニカル サポートを最大限に活用してください。これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

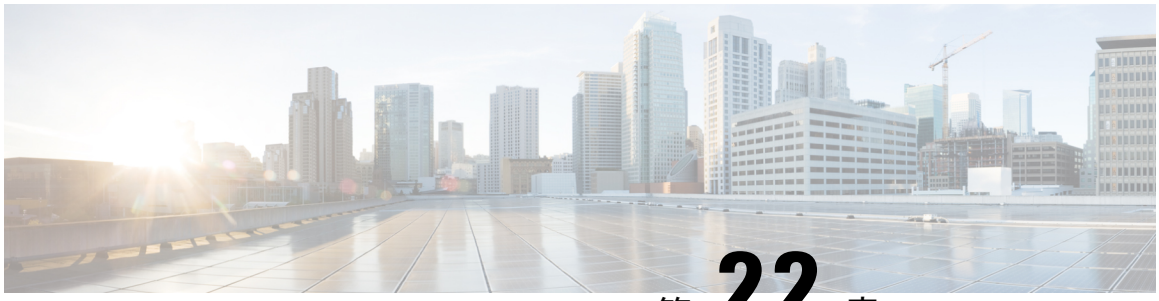
リバース SSH 拡張の機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *39* : リバース *SSH* 拡張の機能情報

機能名	リリース	機能情報
リバース SSH 拡張		セキュア シェル（SSH）のバージョン 1 と 2 に対してサポートされているリバース SSH 拡張機能は、SSH を有効にしなければならない端末または補助回線ごとに別々の回線を設定する必要がないようにリバース SSH を設定する代替手段を提供します。この機能は、ロータリー グループの制限も排除します。 次のコマンドが導入されました：**ssh**



第 22 章

セキュア コピー

セキュア コピー（SCP）機能は、ルータ設定またはルータ イメージ ファイルをコピーするセキュアで認証された方法を提供します。SCP は、セキュア シェル（SSH）、アプリケーション、および Berkeley r ツールのセキュアな代替手段を提供するプロトコルに依存します。

セキュア コピーの前提条件

- SCP を有効にする前に、ルータ上で SSH、認証、および認可を正しく設定する必要があります。
- SCP は SSH を使用してセキュアな転送を実行するため、ルータには RSA キーのペアが必要です。

セキュアコピーのパフォーマンス向上に関する制限事項

- ウィンドウ サイズの増加は、主に SCP 操作に対してのみ使用する必要があります。
- プラットフォームのタイプによっては、ウィンドウ サイズが最大の場合に CPU 使用率が高くなることがあります。
- 万一に備えて、デフォルト サイズの 4 倍まで増やすことができます。

Secure Copy に関する情報

SCP の機能

SCP は一連の Berkeley の r-tools に基づいて設計されているため、その動作内容は、SCP が SSH のセキュリティに対応している点を除けば、Remote Copy Protocol（RCP）と類似しています。加えて、SCP は、ユーザーが正しい権限レベルを持っていることをルータ上で判断できるように、認証、許可、アカウンティング（AAA）許可を設定する必要があります。

SCP を使用すると、適切な許可を得たユーザーは、**copy** コマンドを使用して、Cisco IOS XE ファイル システム（IFS）内に存在する任意のファイルをルータとやり取りすることができます。許可された管理者はワークステーションからこの操作を実行することもできます。

SCP の設定方法

SCP の設定

Cisco ルータを有効にして、SCP サーバー側機能用に設定するには、次の手順を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **aaa new-model**
4. **aaa authentication login** {**default** | *list-name*} *method1*[*method2...*]
5. **aaa authorization** {**network** | **exec** | **commands** *level* | **reverse-access** | **configuration**} {**default** | *list-name*} [*method1* [*method2...*]]
6. **username** *name* [**privilege** *level]*{ **password** *encryption-type encrypted-password*}
7. **ip scp server enable**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 3	**aaa new-model** 例： `Router (config)# aaa new-model`	ログイン時の AAA 認証を設定します。
ステップ 4	**aaa authentication login** {**default** | *list-name*} *method1*[*method2...*] 例： `Router (config)# aaa authentication login default group tacacs+`	AAA アクセス コントロール システムをイネーブルにします。
ステップ 5	**aaa authorization** {**network** | **exec** | **commands** *level* | **reverse-access** | **configuration**} {**default** | *list-name*} [*method1* [*method2...*]] 例： `Router (config)# aaa authorization exec default group tacacs+`	ネットワークへのユーザ アクセスを制限するパラメータを設定します。 （注） **The exec** キーワードは、認可を実行してユーザーがEXECシェルの実行を許可されているかどうかを判断します。したがって、SCPを設定するときにこのキーワードを使用する必要があります。
ステップ 6	**username** *name* [**privilege** *level]*{ **password** *encryption-type encrypted-password*} 例： `Router (config)# username superuser privilege 2 password 0 superpassword`	ユーザー名をベースとした認証システムを構築します。 （注） TACACS+やRADIUSなどのネットワークベースの認証メカニズムが設定されている場合は、この手順を省略できます。
ステップ 7	**ip scp server enable** 例： `Router (config)# ip scp server enable`	SCP サーバー側機能を有効にします。

SCP の確認

SCP サーバー側機能を確認するには、次の手順を実行します。

手順の概要

1. **enable**
2. **show running-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**show running-config** 例： `Router# show running-config`	SCP サーバー側機能を確認します。

SCP のトラブルシューティング

手順の概要

1. **enable**
2. **debug ip scp**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**debug ip scp** 例： `Router# debug ip scp`	SCP 認証問題を解決します。

セキュア コピーの設定例

ローカル認証を使用した SCP サーバー側の設定例

次の例は、SCP のサーバー側機能の設定方法を示しています。この例では、ローカルに定義されたユーザ名とパスワードを使用します。

```
! AAA authentication and authorization must be configured properly for SCP to work.
aaa new-model
aaa authentication login default local
```

```
aaa authorization exec default local
username tiger privilege 15 password 0 lab
! SSH must be configured and functioning properly.
ip ssh time-out 120
ip ssh authentication-retries 3
ip scp server enable
```

ネットワークベース認証を使用した SCP サーバー側の設定例

次の例は、ネットワークベースの認証メカニズムを使用した SCP のサーバ側機能の設定方法を示しています。

```
! AAA authentication and authorization must be configured properly for SCP to work.
aaa new-model
aaa authentication login default group tacacs+
aaa authorization exec default group tacacs+
! SSH must be configured and functioning properly.
ip ssh time-out 120
ip ssh authentication-retries 3
ip scp server enable
```

その他の参考資料

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『Cisco IOS Master Commands List, All Releases』
セキュリティ コマンド：コマンド構文の詳細、コマンド モード、コマンド履歴、デフォルト設定、使用上のガイドライン、および例	『*Cisco IOS Security Command Reference*』
セキュア シェル	セキュア シェルおよびセキュア シェル バージョン 2 サポート設定の機能モジュール。
認証と認可の設定	認証設定、認可設定、およびアカウンティング設定の機能モジュール。

標準

標準	タイトル
なし	--

MIB

MIB	MIB のリンク
なし	選択したプラットフォーム、Cisco ソフトウェア リリース、およびフィーチャ セットの MIB を検索してダウンロードする場合は、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

RFC

RFC	タイトル
この機能によりサポートされた新規 RFC または改訂 RFC はありません。またこの機能による既存 RFC のサポートに変更はありません。	--

シスコのテクニカル サポート

説明	リンク
右の URL にアクセスして、シスコのテクニカル サポートを最大限に活用してください。これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

セキュア コピーの機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *40 :* セキュア コピーの機能情報

機能名	リリース	機能の設定情報
セキュア コピー	Cisco IOS XE Release 2.1	セキュア コピー（SCP）機能は、ルータ設定またはルータ イメージ ファイルをコピーするセキュアで認証された方法を提供します。SCPは、セキュア シェル（SSH）、アプリケーション、およびBerkeley rツールのセキュアな代替手段を提供するプロトコルに依存します。 この機能は、Cisco IOS XE Release2.1 で、Cisco ASR 1000 シリーズアグリゲーション サービス ルータに導入されました。 次のコマンドが導入または変更されました：**debug ip scp**、**ip scp server enable**。

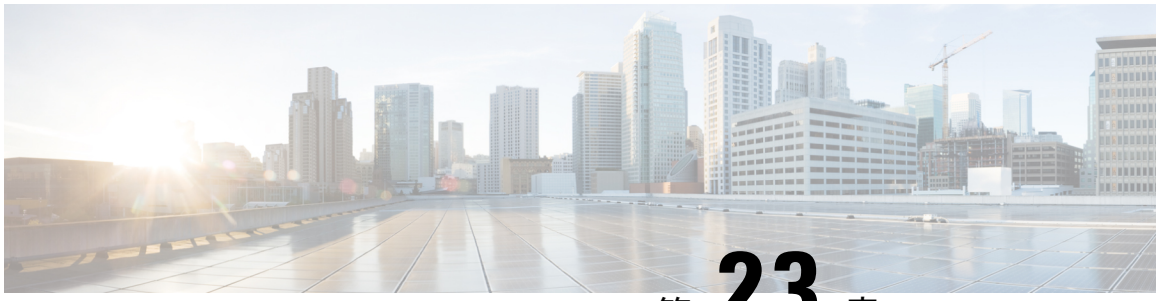
用語集

AAA：認証、許可、およびアカウンティングセキュリティ サービスのフレームワークであり、ユーザーの身元確認（認証）、リモート アクセス コントロール（許可）、課金、監査、およびレポートに使用するセキュリティ サーバー情報の収集と送信（アカウンティング）の方式を定めています。

rcp ：リモート コピーセキュリティをリモート シェル（Berkeley r ツール スイート）に依存している rcp は、ルータ イメージやスタートアップ コンフィギュレーションなどのファイルをルータとやり取りします。

SCP ：セキュア コピーセキュリティを SSH に依存している SCP サポートは、Cisco IOS XE ファイル システム内のあらゆるもののセキュアで認証されたコピーを可能にします。SCP は rcp から派生したものです。

SSH ：セキュア シェルBerkeley r ツールのセキュアな代替手段を提供するアプリケーションとプロトコル。プロトコルは標準の暗号メカニズムを使用してセッションの安全を確保します。アプリケーションは Berkeley の rexec および rsh ツールと同様に使用できます。SSH バージョン 1 は Cisco IOS XE ソフトウェアに実装されています。



第 23 章

セキュア シェル バージョン 2 サポート

セキュア シェル バージョン 2 サポート機能で、セキュア シェル（SSH）バージョン 2 を設定できます（SSH バージョン 1 サポートは、以前のシスコ ソフトウェア リリースに実装されていました）。SSH は、信頼性の高いトランスポート層の上部で実行され、強力な認証機能と暗号化機能を提供します。SSH では、信頼できる転送として定義されているのは TCP のみです。SSH で、ネットワーク上の他のコンピュータに安全にアクセスしたり、コマンドを安全に実行できます。SSH とともに提供されるセキュア コピー プロトコル（SCP）機能で、ファイルを安全に転送できます。

セキュア シェル バージョン 2 サポートの前提条件

- SSH を設定する前に、ご使用のデバイスに必要なイメージがロードされていることを確認します。SSH サーバーには、ご使用のリリースに応じた k9（Triple Data Encryption Standard [3DES]）ソフトウェア イメージが必要です。
- SSH バージョン 2 をサポートする SSH リモート デバイスを使用する必要があります。また、シスコ デバイスに接続する必要があります。
- SCP は、認証、認可、およびアカウンティング（AAA）によって正しく機能します。そのため、SSH サーバーで Secure Copy Protocol が有効になるようにデバイスで AAA を設定する必要があります。

（注） SSH バージョン 2 サーバーと SSH バージョン 2 クライアントは、ご使用のリリースに応じてシスコ ソフトウェアでサポートされます（SSH クライアントは SSH バージョン 1 プロトコルと SSH バージョン 2 プロトコルの両方を実行します。SSH クライアントは、ご使用のリリースに応じて k8 および k9 イメージの両方でサポートされます）。

ソフトウェア イメージのダウンロードに関する情報については、『*Cisco IOS Configuration Fundamentals* コンフィギュレーション ガイド』を参照してください。

セキュア シェル バージョン 2 サポートの制約事項

- Cisco IOS XE リリース 17.10 以降、セキュアシェルバージョン 1.99 はサポートされていません。
- セキュア シェル（SSH）サーバーと SSH クライアントは、Triple Data Encryption Standard（3DES）ソフトウェア イメージでサポートされます。
- サポートされるアプリケーションは、実行シェル、remote コマンドの実行、Secure Copy Protocol（SCP）のみです。
- Rivest、Shamir、および Adleman（RSA）キー生成は SSH サーバー側の要件です。SSH クライアントとして動作するデバイスは、RSA キーを生成する必要がありません。
- Cisco IOS XE リリース 17.10 以降、RSA キーペアの最小サイズは 2048 ビットである必要があります。

  Cisco IOS XE リリース 17.11 以降では、弱い RSA キーを引き続き使用する場合、**crypto engine compliance shield disable** コマンドを使用してデバイスで CSDL コンプライアンスを無効にし、再起動してください。
- 次の機能はサポートされていません。
  - ポート フォワーディング。
  - Compression

セキュア シェル バージョン 2 サポートに関する情報

SSH バージョン 2

セキュア シェル バージョン 2 サポート機能で、SSH バージョン 2 を設定できます。

SSH バージョン 2 サーバの設定は、SSH バージョン 1 の設定と同様です。**ip ssh version** コマンドは、設定する SSH バージョンを定義します。このコマンドを設定しない場合、デフォルト

で SSH は互換モードで実行されます。バージョン 1 とバージョン 2 両方の接続が利用できます。

（注） SSHバージョン1は、標準として定義されていないプロトコルです。未定義のプロトコル（バージョン 1）にデバイスがフォールバックしないようにするには、 **ip ssh version** コマンドを使用してバージョン 2 を指定する必要があります。

ip ssh rsa keypair-name コマンドを使用すると、設定した Rivest、Shamir、および Adleman（RSA）キーを使用して SSH 接続を実行できます。すでに、SSH は生成済みの最初の RSA キーにリンクされています（つまり、最初の RSA キー ペアが生成された時点で SSH はイネーブルになっています）。この動作は存在していますが、**ip ssh rsa keypair-name** コマンドを使用してこの動作を行わないようにすることができます。 **ip ssh rsa keypair-name** コマンドをキー ペアの名前を指定して設定すると、SSH は、キー ペアが存在する場合に有効になるか、キー ペアを後で作成する場合は後から有効になります。このコマンドを使用して SSH をイネーブルにする場合、Cisco ソフトウェアの SSH バージョン 1 では必要な、ホスト名とドメイン名を設定を設定する必要はありません。

（注） ログイン バナーは SSH バージョン 2 でサポートされますが、セキュア シェル バージョン 1 ではサポートされません。

セキュア シェル バージョン 2 の機能拡張

SSH バージョン 2 の機能拡張には、Virtual Routing and Forwarding（VRF）-Aware SSH、SSH デバッグ機能拡張、および Diffie-Hellman（DH）グループ交換のサポートなどの追加機能がいくつか含まれています。

（注） VRF-Aware SSH 機能は、ご使用のリリースに応じてサポートされます。

Cisco SSH 実装では従来、768 ビット絶対値が使用されていましたが、DH グループ 14（2048 ビット）およびグループ 16（4096 ビット）暗号化アプリケーションに対応するため、より大きなキーサイズの必要性が高まり、優先DH グループを確立するクライアントとサーバー間のメッセージ交換が必要になっています。**ip ssh dh min size** コマンドは、SSH サーバー上のモジュラス サイズを設定します。これに加え、**ssh** コマンドが拡張され、SSH クライアント側のクライアントの VRF インスタンス名を IP アドレスとともに使用して、正しいルーティング テーブルを検索し、接続を確立する機能に、VRF 認識が追加されました。

SSH debug コマンドが修正され、デバッグが拡張されました。**debug ip ssh** コマンドは、デバッグ プロセスを簡素化するために拡張されました。デバッグ プロセスを簡素化する前、このコマンドでは、明確に必要かどうかに関係なく SSH に関連するすべてのデバッグ メッセージが

印刷されました。この動作は依然として存在しますが、 **debug ip ssh** コマンドをキーワードを指定して設定した場合、メッセージはキーワードで指定した情報に制限されます。

セキュア シェル バージョン 2 の RSA キーに関する機能拡張

Cisco SSH バージョン 2 は、キーボード インタラクティブ認証方式およびパスワード ベースの認証方式をサポートしています。RSA キーの SSH バージョン 2 拡張機能は、クライアントとサーバ向けの RSA ベースの公開キー認証もサポートしています。

ユーザ認証：RSA ベースのユーザ認証では、各ユーザに関連付けられている秘密キー/公開キーのペアを認証に使用します。ユーザは秘密キー/公開キーのペアをクライアントで生成し、公開キーを Cisco SSH サーバで設定して、認証を完了します。

クレデンシャルの確立を試行する SSH ユーザは、秘密キーを使用して暗号化された署名を提示します。署名とユーザの公開キーは、認証のために SSH サーバに送信されます。SSH サーバでは、ユーザから提示された公開キーに対してハッシュを計算します。ハッシュは、サーバに一致するエントリがあるかどうかを判断するために使用されます。一致が見つかった場合、RSA ベースのメッセージ検証が公開キーを使用して実行されます。その結果、暗号化されたシグニチャに基づいて、ユーザのアクセスは認証されるか拒否されます。

サーバ認証：SSH セッションの確立中に、Cisco SSH クライアントは、キー交換フェーズ中に使用できるサーバ ホスト キーを使用して、SSH サーバを認証します。SSH サーバ キーは、SSH サーバの識別に使用されます。これらのキーは SSH がイネーブルになるときに作成され、クライアント側で設定する必要があります。

サーバ認証の場合、Cisco SSH クライアントが各サーバにホスト キーを割り当てる必要があります。クライアントがサーバとの間で SSH セッションを確立しようとすると、クライアントはキー交換メッセージの一部として、サーバの署名を受信します。厳密なホスト キーのチェック フラグがクライアント側でイネーブルの場合、そのサーバに対応するホスト キー エントリがあるかどうかがクライアントで確認されます。一致が見つかると、クライアントはサーバ ホスト キーを使用して署名の検証を試行します。サーバの認証に成功すると、セッションの確立処理は続行します。失敗すると、処理は終了し、「Server Authentication Failed」というメッセージが表示されます。

（注） 公開キーをサーバで格納する際、メモリを使用します。したがって、SSH サーバで設定できる公開キーの数は、1 ユーザに最大 2 つの公開キーを作成した場合 10 ユーザ分に限られます。

（注） シスコ サーバは RSA ベースのユーザ認証をサポートしていますが、シスコ クライアントは認証方式として公開キーを提案できません。RSA ベースの認証に対するオープンな SSH クライアントからの要求を Cisco サーバが受信した場合、サーバは認証要求を受け入れます。

（注） サーバ認証の場合、サーバの RSA 公開キーを手動で設定し、Cisco SSH クライアント側で **ip ssh stricthostkeycheck** コマンドを設定します。

SNMP トラップ生成

ご使用のリリースに応じて、簡易ネットワーク管理プロトコル（SNMP）トラップは、トラップが有効で SNMP デバッグがオンになっている場合、SSH セッションが終了した際に自動的に生成されます。SNMP トラップの有効化に関する情報については、『SNMP Configuration Guide』の「Configuring SNMP Support」モジュールを参照してください。

（注） **snmp-server host** コマンドを設定する場合、IP アドレスは、SSH（telnet）クライアントがあり、SSH サーバへの IP 接続が可能な PC のアドレスにする必要があります。

また、**debug snmp packet** コマンドを使用して SNMP デバッグを有効にし、トラップを表示する必要があります。トラップ情報には、送信バイト数や SSH セッションで使用されたプロトコルなどの情報が含まれます。

SSH キーボード インタラクティブ認証

SSH キーボード インタラクティブ認証機能は、SSH での汎用メッセージ認証とも呼ばれ、異なる種類の認証メカニズムを実装するために使用できる方式です。基本的に、現在サポートされている、ユーザの入力のみが必要な認証方式はすべて、この機能で実行することができます。この機能は自動的にイネーブルになります。

次の方式がサポートされています。

- パスワード
- サーバが送信するチャレンジに応答する番号またはストリングを印刷する SecurID およびハードウェア トークン
- プラグイン可能な認証モジュール（PAM）
- S/KEY（およびその他の使い捨てキー）

自動的にイネーブルにされた SSH キーボードインタラクティブ認証機能のさまざまなシナリオの例については、例：SSH キーボード インタラクティブ認証 （330 ページ） を参照してください。

セキュア シェル バージョン 2 サポートの設定方法

ホスト名およびドメイン名を使用した SSH バージョン 2 のデバイス設定

手順の概要

1. **enable**
2. **configure terminal**
3. **hostname** *name*
4. **ip domain-name** *name*
5. **crypto key generate rsa**
6. **ip ssh** [**time-out** *seconds* | **authentication-retries** *integer*]
7. **ip ssh version** [**1** | **2**]
8. **exit**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**hostname** *name* 例： `Device(config)# hostname cisco7200`	デバイスのホスト名を設定します。
ステップ 4	**ip domain-name** *name* 例： `cisco7200(config)# ip domain-name example.com`	デバイスのドメイン名を設定します。
ステップ 5	**crypto key generate rsa** 例： `cisco7200(config)# crypto key generate rsa`	ローカルおよびリモート認証用に SSH サーバをイネーブルにします。

	コマンドまたはアクション	目的
ステップ 6	**ip ssh** [**time-out** *seconds* | **authentication-retries** *integer*] 例： `cisco7200(config)# ip ssh time-out 120`	（任意）デバイス上で SSH 制御変数を設定します。
ステップ 7	**ip ssh version** [**1** | **2**] 例： `cisco7200(config)# ip ssh version 1`	（任意）デバイスで実行する SSH のバージョンを指定します。
ステップ 8	**exit** 例： `cisco7200(config)# exit`	グローバル コンフィギュレーション モードを終了し、特権 EXEC モードを開始します。 • デフォルト ホストに戻るには、**no hostname** コマンドを使用します。

RSA キー ペアを使用した SSH バージョン 2 のデバイス設定

ステップ 1 **enable**

例：

```
Device> enable
```

特権 EXEC モードを有効にします。

- パスワードを入力します（要求された場合）。

ステップ 2 **configure terminal**

例：

```
Device# configure terminal
```

グローバル コンフィギュレーション モードを開始します。

ステップ 3 **ip ssh rsa keypair-name** *keypair-name*

例：

```
Device(config)# ip ssh rsa keypair-name sshkeys
```

SSH に使用する RSA キー ペアを指定します。

（注） シスコ デバイスには複数の RSA キー ペアを設定できます。

ステップ 4 **crypto key generate rsa usage-keys label** *key-label* **modulus** *modulus-size*

例：

```
Device(config)# crypto key generate rsa usage-keys label sshkeys modulus 768
```

デバイスでローカルおよびリモート認証を行う SSH サーバを有効にします。

- SSH バージョン 2 では、絶対サイズは 768 ビット以上である必要があります。

（注） RSA キー ペアを削除するには、**crypto key zeroize rsa** コマンドを使用します。RSA キー ペアを削除すると、SSH サーバは自動的に無効になります。

ステップ 5 **ip ssh** [**time-out** *seconds* | **authentication-retries** *integer*]

例：

```
Device(config)# ip ssh time-out 12
```

デバイス上で SSH 制御変数を設定します。

ステップ 6 **ip ssh version 2**

例：

```
Device(config)# ip ssh version 2
```

デバイスで実行する SSH のバージョンを指定します。

ステップ 7 **exit**

例：

```
Device(config)# exit
```

グローバル コンフィギュレーション モードを終了し、特権 EXEC モードを開始します。

RSA ベースのユーザ認証を実行するための Cisco SSH サーバの設定

ステップ 1 **enable**

例：

```
Device> enable
```

特権 EXEC モードを有効にします。

- パスワードを入力します（要求された場合）。

ステップ 2 **configure terminal**

例：

```
Device# configure terminal
```

グローバル コンフィギュレーション モードを開始します。

ステップ 3 **hostname** *name*

例：

```
Device(config)# hostname host1
```

ホスト名を指定します。

ステップ 4 **ip domain-name** *name*

例：

```
host1(config)# ip domain-name name1
```

Cisco ソフトウェアで使用するデフォルトのドメイン名を定義し、不完全なホスト名のドメインを補完します。

ステップ 5 **crypto key generate rsa**

例：

```
host1(config)# crypto key generate rsa
```

RSA キー ペアを生成します。

ステップ 6 **ip ssh pubkey-chain**

例：

```
host1(config)# ip ssh pubkey-chain
```

SSH サーバ上のユーザおよびサーバ認証用に SSH-RSA キーを設定し、公開キー コンフィギュレーション モードを開始します。

- サーバに保存されている RSA 公開キーが、クライアントに保存されている公開キーと秘密キーのペアを使用して検証されると、ユーザ認証は成功です。

ステップ 7 **username** *username*

例：

```
host1(conf-ssh-pubkey)# username user1
```

SSH ユーザ名を設定し、公開キー ユーザ コンフィギュレーション モードを開始します。

ステップ 8 **key-string**

例：

```
host1(conf-ssh-pubkey-user)# key-string
```

リモート ピアの RSA 公開キーを指定し、公開キー データ コンフィギュレーション モードを開始します。

（注） オープン SSH クライアントから（言い換えると .ssh/id_rsa.pub ファイルから）公開キー値を取得できます。

ステップ 9 **key-hash** *key-type key-name*

例：

```
host1(conf-ssh-pubkey-data)# key-hash ssh-rsa key1
```

（任意）SSH キー タイプとバージョンを指定します。

- 秘密キー/公開キー ペアの設定では、キー タイプを ssh-rsa にする必要があります。
- **key-string** コマンドが設定されている場合に限りこの手順は任意です。
- **key-string** コマンドと **key-hash** コマンドのいずれかを設定する必要があります。

（注） 公開キー ストリングのハッシュを計算するには、ハッシュ処理ソフトウェアを使用します。また、別のシスコ デバイスからハッシュ値をコピーすることもできます。初めて公開キー データを入力する場合、**key-string** コマンドを使用して公開キー データを入力することを推奨します。

ステップ 10 **end**

例：

```
host1(conf-ssh-pubkey-data)# end
```

公開キー データ コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

- デフォルト ホストに戻るには、 **no hostname** コマンドを使用します。

RSA ベースのサーバ認証を実行するための Cisco IOS SSH サーバの設定

ステップ 1 **enable**

例：

```
Device> enable
```

特権 EXEC モードを有効にします。

- パスワードを入力します（要求された場合）。

ステップ 2 **configure terminal**

例：

```
Device# configure terminal
```

グローバル コンフィギュレーション モードを開始します。

ステップ 3 **hostname** *name*

例：

```
Device(config)# hostname host1
```

ホスト名を指定します。

ステップ 4 **ip domain-name** *name*

例：

```
host1(config)# ip domain-name name1
```

Cisco ソフトウェアで使用するデフォルトのドメイン名を定義し、不完全なホスト名のドメインを補完します。

ステップ 5 **crypto key generate rsa**

例：

```
host1(config)# crypto key generate rsa
```

RSA キー ペアを生成します。

ステップ 6 **ip ssh pubkey-chain**

例：

```
host1(config)# ip ssh pubkey-chain
```

SSH サーバ上のユーザおよびサーバ認証用に SSH-RSA キーを設定し、公開キー コンフィギュレーション モードを開始します。

ステップ 7 **server** *server-name*

例：

```
host1(conf-ssh-pubkey)# server server1
```

デバイスでの公開キー認証について SSH サーバを有効にし、公開キー サーバ コンフィギュレーション モードを開始します。

ステップ 8 **key-string**

例：

```
host1(conf-ssh-pubkey-server)# key-string
```

リモート ピアの RSA 公開キーを指定し、公開キー データ コンフィギュレーション モードを開始します。

（注） オープン SSH クライアントから（言い換えると .ssh/id_rsa.pub ファイルから）公開キー値を取得できます。

ステップ 9 **exit**

例：

```
host1(conf-ssh-pubkey-data)# exit
```

公開キー データ コンフィギュレーション モードを終了し、公開キー サーバ コンフィギュレーション モードを開始します。

ステップ 10 **key-hash** *key-type key-name*

例：

```
host1(conf-ssh-pubkey-server)# key-hash ssh-rsa key1
```

（任意）SSH キー タイプとバージョンを指定します。

- 秘密キー/公開キー ペアの設定では、キー タイプを ssh-rsa にする必要があります。
- **key-string** コマンドが設定されている場合に限りこの手順は任意です。
- **key-string** コマンドと **key-hash** コマンドのいずれかを設定する必要があります。

（注） 公開キー ストリングのハッシュを計算するには、ハッシュ処理ソフトウェアを使用します。また、別のシスコ デバイスからハッシュ値をコピーすることもできます。初めて公開キー データを入力する場合、**key-string** コマンドを使用して公開キー データを入力することを推奨します。

ステップ 11 **end**

例：

```
host1(conf-ssh-pubkey-server)# end
```

公開キー サーバ コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

ステップ 12 **configure terminal**

例：

```
host1# configure terminal
```

グローバル コンフィギュレーション モードを開始します。

ステップ 13 **ip ssh stricthostkeycheck**

例：

```
host1(config)# ip ssh stricthostkeycheck
```

サーバ認証が実行されることを確認します。

- 障害が発生すると、接続は終了します。
- デフォルト ホストに戻るには、 **no hostname** コマンドを使用します。

リモート デバイスとの暗号化セッションの開始

（注） 接続するデバイスは、シスコ ソフトウェアでサポートされる暗号化アルゴリズムを備えたセキュア シェル（SSH）サーバをサポートしている必要があります。また、デバイスを有効にする必要はありません。SSH はディセーブル モードで実行できます。

ssh [**-v** {**1** | **2**} | **-c** {**aes128-ctr** | **aes192-ctr** | **aes256-ctr** | **aes128-cbc** | **3des** | **aes192-cbc** | **aes256-cbc**} | **-l** *user-id* | **-l** *user-id***:***vrf-name number ip-address ip-address* | **-l** *user-id***:***rotary number ip-address* | **-m** {**hmac-md5-128** | **hmac-md5-96** | **hmac-sha1-160** | **hmac-sha1-96**} | **-o numberofpasswordprompts** *n* | **-p** *port-num*] {*ip-addr* | *hostname*} [**command** | **-vrf**]

例：

```
Device# ssh -v 2 -c aes256-ctr -m hmac-sha1-96 -l user2 10.76.82.24
```

リモート ネットワーク デバイスとの暗号化されたセッションを開始します。

トラブルシューティングのヒント

ip ssh version コマンドは、SSH の設定のトラブルシューティングに使用できます。バージョンを変更することによって、問題がある SSH バージョンを特定できます。

SSH サーバでの Secure Copy Protocol のイネーブル化

（注） 次のタスクでは、SCP のサーバ側機能を設定します。このタスクは、デバイスでリモートのワークステーションからファイルを安全にコピーできる一般的な設定を示しています。

ステップ 1 **enable**

例：

```
Device> enable
```

特権 EXEC モードを有効にします。

- パスワードを入力します（要求された場合）。

ステップ 2 **configure terminal**

例：

```
Device# configure terminal
```

グローバル コンフィギュレーション モードを開始します。

ステップ 3 **aaa new-model**

例：

```
Device(config)# aaa new-model
```

AAA アクセス コントロール モデルをイネーブルにします。

ステップ 4 **aaa authentication login default local**

例：

```
Device(config)# aaa authentication login default local
```

認証時にローカルのユーザ名データベースを使用するように、ログイン時の AAA 認証を設定します。

ステップ 5 **aaa authorization exec defaultlocal**

例：

```
Device(config)# aaa authorization exec default local
```

ユーザ アクセスを制限するパラメータをネットワークに設定します。許可を実行し、ユーザ ID で EXEC シェルの実行を許可するかどうかを定義します。その後、システムで許可にローカル データベースを使用する必要があることを指定します。

ステップ 6 **username***name* **privilege** *privilege-level* **password** *password*

例：

```
Device(config)# username samplename privilege 15 password password1
```

ユーザ名ベースの認証システムを確立し、ユーザ名、権限レベル、および非暗号化パスワードを指定します。

（注） *privilege-level* 引数の最小値は 15 です。権限レベルが 15 未満の場合、接続が切断されます。

ステップ 7 **ip ssh time-out***seconds*

例：

```
Device(config)# ip ssh time-out 120
```

デバイスが SSH クライアントの応答を待つ時間間隔を、秒単位で設定します。

ステップ 8 **ip ssh authentication-retries** 整数

例：

```
Device(config)# ip ssh authentication-retries 3
```

インターフェイスのリセット後、認証を試行する回数を設定します。

ステップ 9 **ip scpserverenable**

例：

```
Device(config)# ip scp server enable
```

デバイスで、リモート ワークステーションから安全にファイルをコピーできるようにします。

ステップ 10 **exit**

例：

```
Device(config)# exit
```

グローバル コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

ステップ 11 **debug ip scp**

例：

```
Device# debug ip scp
```

（任意）SCP 認証の問題に関する診断情報を提供します。

セキュア シェル接続のステータスの確認

ステップ 1 **enable**

例：

```
Device> enable
```

特権 EXEC モードを有効にします。

- パスワードを入力します（要求された場合）。

ステップ 2 **show ssh**

例：

```
Device# show ssh
```

SSH サーバ接続のステータスを表示します。

ステップ 3 **exit**

例：

```
Device# exit
```

特権 EXEC モードを終了し、ユーザ EXEC モードに戻ります。

例

次の **show ssh** コマンドの出力例には、バージョン 1 およびバージョン 2 接続の複数の SSH バージョン 1 およびバージョン 2 接続のステータスが表示されています。

```
------------------------------------------------------------------------
Device# show ssh

Connection      Version Encryption      State                   Username
 0              1.5     3DES            Session started         lab
Connection Version Mode Encryption  Hmac                State
Username
1          2.0     IN   aes128-cbc  hmac-md5     Session started       lab
1          2.0     OUT  aes128-cbc  hmac-md5     Session started       lab
------------------------------------------------------------------------
```

次の **show ssh** コマンドの出力例には、バージョン 2 接続（バージョン 1 接続なし）の複数の SSH バージョン 2 およびバージョン 1 接続のステータスが表示されています。

```
------------------------------------------------------------------------
Device# show ssh

Connection Version Mode Encryption  Hmac                State
Username
1          2.0     IN   aes128-cbc  hmac-md5     Session started       lab
1          2.0     OUT  aes128-cbc  hmac-md5     Session started       lab
%No SSHv1 server connections running.
------------------------------------------------------------------------
```

次の **show ssh** コマンドの出力例には、バージョン 2 接続（バージョン 1 接続なし）の複数の SSH バージョン 1 およびバージョン 2 接続のステータスが表示されています。

```
------------------------------------------------------------------------
Device# show ssh

Connection      Version Encryption      State                   Username
 0              1.5     3DES            Session started         lab
%No SSHv2 server connections running.
------------------------------------------------------------------------
```

セキュア シェル ステータスの確認

ステップ 1　enable

例：

```
Device> enable
```

特権 EXEC モードを有効にします。

- パスワードを入力します（要求された場合）。

ステップ 2　show ip ssh

例：

```
Device# show ip ssh
```

SSH のバージョンおよび設定データを表示します。

ステップ 3　exit

例：

```
Device# exit
```

特権 EXEC モードを終了し、ユーザ EXEC モードに戻ります。

例

次の **show ip ssh** コマンドの出力例には、有効な SSH のバージョン、認証タイムアウト値、およびバージョン 1 およびバージョン 2 接続の認証の再試行回数が表示されています。

```
------------------------------------------------------------------------
Device# show ip ssh

SSH Enabled - version 1.99
Authentication timeout: 120 secs; Authentication retries: 3
------------------------------------------------------------------------
```

次の **show ip ssh** コマンドの出力例には、有効な SSH のバージョン、認証タイムアウト値、およびバージョン 2 接続（バージョン 1 接続なし）の認証の再試行回数が表示されています。

```
------------------------------------------------------------------------
Device# show ip ssh

SSH Enabled - version 2.0
Authentication timeout: 120 secs; Authentication retries: 3
------------------------------------------------------------------------
```

次の **show ip ssh** コマンドの出力例には、有効な SSH のバージョン、認証タイムアウト値、およびバージョン 1 接続（バージョン 2 接続なし）の認証の再試行回数が表示されています。

```
------------------------------------------------------------------------
Device# show ip ssh

3d06h: %SYS-5-CONFIG_I: Configured from console by console
SSH Enabled - version 1.5
Authentication timeout: 120 secs; Authentication retries: 3
------------------------------------------------------------------------
```

セキュア シェル バージョン 2 のモニタリングと維持

ステップ 1 **enable**

例：

```
Device> enable
```

特権 EXEC モードを有効にします。

- パスワードを入力します（要求された場合）。

ステップ 2 **debug ip ssh**

例：

```
Device# debug ip ssh
```

SSH のデバッグを有効にします。

ステップ 3 **debug snmp packet**

例：

```
Device# debug snmp packet
```

デバイスによって送受信されたすべての SNMP パケットのデバッグを有効にします。

例

次の **debug ip ssh** コマンドの出力例は、接続が SSH バージョン 2 接続であることを示します。

```
Device# debug ip ssh

00:33:55: SSH1: starting SSH control process
00:33:55: SSH1: sent protocol version id SSH-1.99-Cisco-1.25
00:33:55: SSH1: protocol version id is - SSH-2.0-OpenSSH_2.5.2p2
00:33:55: SSH2 1: send: len 280 (includes padlen 4)
00:33:55: SSH2 1: SSH2_MSG_KEXINIT sent
00:33:55: SSH2 1: ssh_receive: 536 bytes received
00:33:55: SSH2 1: input: packet len 632
```

```
00:33:55: SSH2 1: partial packet 8, need 624, maclen 0
00:33:55: SSH2 1: ssh_receive: 96 bytes received
00:33:55: SSH2 1: partial packet 8, need 624, maclen 0
00:33:55: SSH2 1: input: padlen 11
00:33:55: SSH2 1: received packet type 20
00:33:55: SSH2 1: SSH2_MSG_KEXINIT received
00:33:55: SSH2: kex: client->server aes128-cbc hmac-md5 none
00:33:55: SSH2: kex: server->client aes128-cbc hmac-md5 none
00:33:55: SSH2 1: expecting SSH2_MSG_KEXDH_INIT
00:33:55: SSH2 1: ssh_receive: 144 bytes received
00:33:55: SSH2 1: input: packet len 144
00:33:55: SSH2 1: partial packet 8, need 136, maclen 0
00:33:55: SSH2 1: input: padlen 5
00:33:55: SSH2 1: received packet type 30
00:33:55: SSH2 1: SSH2_MSG_KEXDH_INIT received
00:33:55: SSH2 1: signature length 111
00:33:55: SSH2 1: send: len 384 (includes padlen 7)
00:33:55: SSH2: kex_derive_keys complete
00:33:55: SSH2 1: send: len 16 (includes padlen 10)
00:33:55: SSH2 1: newkeys: mode 1
00:33:55: SSH2 1: SSH2_MSG_NEWKEYS sent
00:33:55: SSH2 1: waiting for SSH2_MSG_NEWKEYS
00:33:55: SSH2 1: ssh_receive: 16 bytes received
00:33:55: SSH2 1: input: packet len 16
00:33:55: SSH2 1: partial packet 8, need 8, maclen 0
00:33:55: SSH2 1: input: padlen 10
00:33:55: SSH2 1: newkeys: mode 0
00:33:55: SSH2 1: received packet type 2100:33:55: SSH2 1: SSH2_MSG_NEWKEYS received
00:33:56: SSH2 1: ssh_receive: 48 bytes received
00:33:56: SSH2 1: input: packet len 32
00:33:56: SSH2 1: partial packet 16, need 16, maclen 16
00:33:56: SSH2 1: MAC #3 ok
00:33:56: SSH2 1: input: padlen 10
00:33:56: SSH2 1: received packet type 5
00:33:56: SSH2 1: send: len 32 (includes padlen 10)
00:33:56: SSH2 1: done calc MAC out #3
00:33:56: SSH2 1: ssh_receive: 64 bytes received
00:33:56: SSH2 1: input: packet len 48
00:33:56: SSH2 1: partial packet 16, need 32, maclen 16
00:33:56: SSH2 1: MAC #4 ok
00:33:56: SSH2 1: input: padlen 9
00:33:56: SSH2 1: received packet type 50
00:33:56: SSH2 1: send: len 32 (includes padlen 13)
00:33:56: SSH2 1: done calc MAC out #4
00:34:04: SSH2 1: ssh_receive: 160 bytes received
00:34:04: SSH2 1: input: packet len 64
00:34:04: SSH2 1: partial packet 16, need 48, maclen 16
00:34:04: SSH2 1: MAC #5 ok
00:34:04: SSH2 1: input: padlen 13
00:34:04: SSH2 1: received packet type 50
00:34:04: SSH2 1: send: len 16 (includes padlen 10)
00:34:04: SSH2 1: done calc MAC out #5
00:34:04: SSH2 1: authentication successful for lab
00:34:04: SSH2 1: input: packet len 64
00:34:04: SSH2 1: partial packet 16, need 48, maclen 16
00:34:04: SSH2 1: MAC #6 ok
00:34:04: SSH2 1: input: padlen 6
00:34:04: SSH2 1: received packet type 2
00:34:04: SSH2 1: ssh_receive: 64 bytes received
00:34:04: SSH2 1: input: packet len 48
00:34:04: SSH2 1: partial packet 16, need 32, maclen 16
00:34:04: SSH2 1: MAC #7 ok
00:34:04: SSH2 1: input: padlen 19
00:34:04: SSH2 1: received packet type 90
```

```
00:34:04: SSH2 1: channel open request
00:34:04: SSH2 1: send: len 32 (includes padlen 10)
00:34:04: SSH2 1: done calc MAC out #6
00:34:04: SSH2 1: ssh_receive: 192 bytes received
00:34:04: SSH2 1: input: packet len 64
00:34:04: SSH2 1: partial packet 16, need 48, maclen 16
00:34:04: SSH2 1: MAC #8 ok
00:34:04: SSH2 1: input: padlen 13
00:34:04: SSH2 1: received packet type 98
00:34:04: SSH2 1: pty-req request
00:34:04: SSH2 1: setting TTY - requested: height 24, width 80; set: height 24,
width 80
00:34:04: SSH2 1: input: packet len 96
00:34:04: SSH2 1: partial packet 16, need 80, maclen 16
00:34:04: SSH2 1: MAC #9 ok
00:34:04: SSH2 1: input: padlen 11
00:34:04: SSH2 1: received packet type 98
00:34:04: SSH2 1: x11-req request
00:34:04: SSH2 1: ssh_receive: 48 bytes received
00:34:04: SSH2 1: input: packet len 32
00:34:04: SSH2 1: partial packet 16, need 16, maclen 16
00:34:04: SSH2 1: MAC #10 ok
00:34:04: SSH2 1: input: padlen 12
00:34:04: SSH2 1: received packet type 98
00:34:04: SSH2 1: shell request
00:34:04: SSH2 1: shell message received
00:34:04: SSH2 1: starting shell for vty
00:34:04: SSH2 1: send: len 48 (includes padlen 18)
00:34:04: SSH2 1: done calc MAC out #7
00:34:07: SSH2 1: ssh_receive: 48 bytes received
00:34:07: SSH2 1: input: packet len 32
00:34:07: SSH2 1: partial packet 16, need 16, maclen 16
00:34:07: SSH2 1: MAC #11 ok
00:34:07: SSH2 1: input: padlen 17
00:34:07: SSH2 1: received packet type 94
00:34:07: SSH2 1: send: len 32 (includes padlen 17)
00:34:07: SSH2 1: done calc MAC out #8
00:34:07: SSH2 1: ssh_receive: 48 bytes received
00:34:07: SSH2 1: input: packet len 32
00:34:07: SSH2 1: partial packet 16, need 16, maclen 16
00:34:07: SSH2 1: MAC #12 ok
00:34:07: SSH2 1: input: padlen 17
00:34:07: SSH2 1: received packet type 94
00:34:07: SSH2 1: send: len 32 (includes padlen 17)
00:34:07: SSH2 1: done calc MAC out #9
00:34:07: SSH2 1: ssh_receive: 48 bytes received
00:34:07: SSH2 1: input: packet len 32
00:34:07: SSH2 1: partial packet 16, need 16, maclen 16
00:34:07: SSH2 1: MAC #13 ok
00:34:07: SSH2 1: input: padlen 17
00:34:07: SSH2 1: received packet type 94
00:34:07: SSH2 1: send: len 32 (includes padlen 17)
00:34:07: SSH2 1: done calc MAC out #10
00:34:08: SSH2 1: ssh_receive: 48 bytes received
00:34:08: SSH2 1: input: packet len 32
00:34:08: SSH2 1: partial packet 16, need 16, maclen 16
00:34:08: SSH2 1: MAC #14 ok
00:34:08: SSH2 1: input: padlen 17
00:34:08: SSH2 1: received packet type 94
00:34:08: SSH2 1: send: len 32 (includes padlen 17)
00:34:08: SSH2 1: done calc MAC out #11
00:34:08: SSH2 1: ssh_receive: 48 bytes received
00:34:08: SSH2 1: input: packet len 32
00:34:08: SSH2 1: partial packet 16, need 16, maclen 16
```

```
00:34:08: SSH2 1: MAC #15 ok
00:34:08: SSH2 1: input: padlen 17
00:34:08: SSH2 1: received packet type 94
00:34:08: SSH2 1: send: len 32 (includes padlen 16)
00:34:08: SSH2 1: done calc MAC out #12
00:34:08: SSH2 1: send: len 48 (includes padlen 18)
00:34:08: SSH2 1: done calc MAC out #13
00:34:08: SSH2 1: send: len 16 (includes padlen 6)
00:34:08: SSH2 1: done calc MAC out #14
00:34:08: SSH2 1: send: len 16 (includes padlen 6)
00:34:08: SSH2 1: done calc MAC out #15
00:34:08: SSH1: Session terminated normally
```

セキュア シェル バージョン 2 サポートの設定例

例：セキュア シェル バージョン 1 の設定

```
Device# configure terminal
Device(config)# ip ssh version 1ip ssh version 2
```

例：セキュア シェル バージョン 2 の設定

```
Device# configure terminal
Device(config)# ip ssh version 2
```

例：セキュア シェル バージョン 1 および 2 の設定

```
Device# configure terminal
Device(config)# no ip ssh version
```

例：リモート デバイスでの暗号化セッションの開始

```
Device# ssh -v 2 -c aes256-cbc -m hmac-sha1-160 -l shaship 10.76.82.24
```

例：サーバ側 SCP の設定

次の例では、SCP のサーバ側機能の設定方法を示します。この例では、デバイスでの AAA 認証および許可も設定しています。この例では、ローカルに定義されたユーザ名とパスワードを使用します。

```
Device# configure terminal
Device(config)# aaa new-model
Device(config)# aaa authentication login default local
```

```
Device(config)# aaa authorization exec default local
Device(config)# username samplename privilege 15 password password1
Device(config)# ip ssh time-out 120
Device(config)# ip ssh authentication-retries 3
Device(config)# ip scp server enable
```

例：SNMP トラップの設定

次の例では、設定済みの SNMP トラップを示します。トラップ通知は、SSH セッションが終了すると自動的に生成されます。この例の a、b、c、d は SSH クライアントの IP アドレスです。SNMP トラップデバッグ出力の例については、「例：SNMP のデバッグ （332 ページ）」を参照してください。

```
snmp-server
snmp-server host a.b.c.d public tty
```

例：SSH キーボード インタラクティブ認証

例：クライアント側のデバッグの有効化

次の例では、クライアント側のデバッグがオンになっており、プロンプトの最大数が 6（SSH キーボード インタラクティブ認証方式のために 3 つ、パスワード認証方式のために 3 つ）になっています。

```
Password:
Password:
Password:
Password:
Password:
Password: cisco123
Last login: Tue Dec 6 13:15:21 2005 from 10.76.248.213
user1@courier:~> exit
logout
[Connection to 10.76.248.200 closed by foreign host]
Device1# debug ip ssh client

SSH Client debugging is on

Device1# ssh -l lab 10.1.1.3

Password:
*Nov 17 12:50:53.199: SSH0: sent protocol version id SSH-1.99-Cisco-1.25
*Nov 17 12:50:53.199: SSH CLIENT0: protocol version id is - SSH-1.99-Cisco-1.25
*Nov 17 12:50:53.199: SSH CLIENT0: sent protocol version id SSH-1.99-Cisco-1.25
*Nov 17 12:50:53.199: SSH CLIENT0: protocol version exchange successful
*Nov 17 12:50:53.203: SSH0: protocol version id is - SSH-1.99-Cisco-1.25
*Nov 17 12:50:53.335: SSH CLIENT0: key exchange successful and encryption on
*Nov 17 12:50:53.335: SSH2 CLIENT 0: using method keyboard-interactive
Password:
Password:
Password:
*Nov 17 12:51:01.887: SSH2 CLIENT 0: using method password authentication
Password:
Password: lab
```

```
Device2>

*Nov 17 12:51:11.407: SSH2 CLIENT 0: SSH2_MSG_USERAUTH_SUCCESS message received
*Nov 17 12:51:11.407: SSH CLIENT0: user authenticated
*Nov 17 12:51:11.407: SSH2 CLIENT 0: pty-req request sent
*Nov 17 12:51:11.411: SSH2 CLIENT 0: shell request sent
*Nov 17 12:51:11.411: SSH CLIENT0: session open
```

例：ブランク パスワードの変更による ChPass の有効化

次の例では、ChPass 機能が有効になっており、SSH キーボード インタラクティブ認証方式を使用してブランク パスワードが変更されています。TACACS+ アクセス コントロール サーバ（ACS）は、バックエンド AAA サーバとして使用されています。

```
Device1# ssh -l cisco 10.1.1.3

Password:
Old Password: cisco
New Password: cisco123
Re-enter New password: cisco123

Device2> exit

[Connection to 10.1.1.3 closed by foreign host]
```

例：ChPass の有効化および初回ログインでのパスワード変更

次の例では、ChPass 機能が有効になっており、TACACS+ ACS はバックエンド サーバとして使用されています。パスワードは、SSH キーボード インタラクティブ 認証方式を使用して最初のログインで変更されています。

```
Device1# ssh -l cisco 10.1.1.3

Password: cisco
Your password has expired.
Enter a new one now.
New Password: cisco123
Re-enter New password: cisco123

Device2> exit

[Connection to 10.1.1.3 closed by foreign host]

Device1# ssh -l cisco 10.1.1.3

Password:cisco1
Your password has expired.
Enter a new one now.
New Password: cisco
Re-enter New password: cisco12
The New and Re-entered passwords have to be the same.
Try again.
New Password: cisco
Re-enter New password: cisco

Device2>
```

例：ChPass の有効化および 3 回ログインした後のパスワードの失効

次の例では、ChPass 機能が有効になっており、TACACS+ ACS はバックエンド AAA サーバとして使用されています。パスワードは、SSH キーボード インタラクティブ認証方式を使用して 3 回ログインした後に期限切れになります。

```
Device# ssh -l cisco. 10.1.1.3

Password: cisco

Device2> exit

[Connection to 10.1.1.3 closed by foreign host]

Device1# ssh -l cisco 10.1.1.3

Password: cisco

Device2> exit

Device1# ssh -l cisco 10.1.1.3

Password: cisco

Device2> exit

[Connection to 10.1.1.3 closed by foreign host]

Device1# ssh -l cisco 10.1.1.3

Password: cisco
Your password has expired.
Enter a new one now.
New Password: cisco123
Re-enter New password: cisco123

Device2>
```

例：SNMP のデバッグ

次に、**debug snmp packet** コマンドの出力例を示します。出力には、SSH セッションの SNMP トラップ情報が含まれます。

```
Device1# debug snmp packet

SNMP packet debugging is on
Device1# ssh -l lab 10.0.0.2
Password:

Device2# exit

[Connection to 10.0.0.2 closed by foreign host]
Device1#
*Jul 18 10:18:42.619: SNMP: Queuing packet to 10.0.0.2
*Jul 18 10:18:42.619: SNMP: V1 Trap, ent cisco, addr 10.0.0.1, gentrap 6, spectrap 1
local.9.3.1.1.2.1 = 6
tcpConnEntry.1.10.0.0.1.22.10.0.0.2.55246 = 4
ltcpConnEntry.5.10.0.0.1.22.10.0.0.2.55246 = 1015
```

```
ltcpConnEntry.1.10.0.0.1.22.10.0.0.2.55246 = 1056
ltcpConnEntry.2.10.0.0.1.22.10.0.0.2.55246 = 1392
local.9.2.1.18.2 = lab
*Jul 18 10:18:42.879: SNMP: Packet sent via UDP to 10.0.0.2

Device1#
```

例：SSH のデバッグの強化

次に、**debug ip ssh detail** コマンドの出力例を示します。出力には、SSH プロトコルとチャネル要求に関するデバッグ情報が含まれます。

```
Device# debug ip ssh detail

00:04:22: SSH0: starting SSH control process
00:04:22: SSH0: sent protocol version id SSH-1.99-Cisco-1.25
00:04:22: SSH0: protocol version id is - SSH-1.99-Cisco-1.25
00:04:22: SSH2 0: SSH2_MSG_KEXINIT sent
00:04:22: SSH2 0: SSH2_MSG_KEXINIT received
00:04:22: SSH2:kex: client->server enc:aes128-cbc mac:hmac-sha1
00:04:22: SSH2:kex: server->client enc:aes128-cbc mac:hmac-sha1
00:04:22: SSH2 0: expecting SSH2_MSG_KEXDH_INIT
00:04:22: SSH2 0: SSH2_MSG_KEXDH_INIT received
00:04:22: SSH2: kex_derive_keys complete
00:04:22: SSH2 0: SSH2_MSG_NEWKEYS sent
00:04:22: SSH2 0: waiting for SSH2_MSG_NEWKEYS
00:04:22: SSH2 0: SSH2_MSG_NEWKEYS received
00:04:24: SSH2 0: authentication successful for lab
00:04:24: SSH2 0: channel open request
00:04:24: SSH2 0: pty-req request
00:04:24: SSH2 0: setting TTY - requested: height 24, width 80; set: height 24, width
80
00:04:24: SSH2 0: shell request
00:04:24: SSH2 0: shell message received
00:04:24: SSH2 0: starting shell for vty
00:04:38: SSH0: Session terminated normally
```

次に、**debug ip ssh packet** コマンドの出力例を示します。出力には、SSH パケットに関するデバッグ情報が含まれます。

```
Device# debug ip ssh packet

00:05:43: SSH2 0: send:packet of  length 280 (length also includes padlen of 4)
00:05:43: SSH2 0: ssh_receive: 64 bytes received
00:05:43: SSH2 0: input: total packet length of 280 bytes
00:05:43: SSH2 0: partial packet length(block size)8 bytes,needed 272 bytes, maclen 0
00:05:43: SSH2 0: ssh_receive: 64 bytes received
00:05:43: SSH2 0: partial packet length(block size)8 bytes,needed 272 bytes, maclen 0
00:05:43: SSH2 0: ssh_receive: 64 bytes received
00:05:43: SSH2 0: partial packet length(block size)8 bytes,needed 272 bytes, maclen 0
00:05:43: SSH2 0: ssh_receive: 64 bytes received
00:05:43: SSH2 0: partial packet length(block size)8 bytes,needed 272 bytes, maclen 0
00:05:43: SSH2 0: ssh_receive: 24 bytes received
00:05:43: SSH2 0: partial packet length(block size)8 bytes,needed 272 bytes, maclen 0
00:05:43: SSH2 0: input: padlength 4 bytes
00:05:43: SSH2 0: ssh_receive: 64 bytes received
00:05:43: SSH2 0: input: total packet length of 144 bytes
00:05:43: SSH2 0: partial packet length(block size)8 bytes,needed 136 bytes, maclen 0
00:05:43: SSH2 0: ssh_receive: 64 bytes received
```

```
00:05:43: SSH2 0: partial packet length(block size)8 bytes,needed 136 bytes, maclen 0
00:05:43: SSH2 0: ssh_receive: 16 bytes received
00:05:43: SSH2 0: partial packet length(block size)8 bytes,needed 136 bytes, maclen 0
00:05:43: SSH2 0: input: padlength 6 bytes
00:05:43: SSH2 0: signature length 143
00:05:43: SSH2 0: send:packet of  length 448 (length also includes padlen of 7)
00:05:43: SSH2 0: send:packet of  length 16 (length also includes padlen of 10)
00:05:43: SSH2 0: newkeys: mode 1
00:05:43: SSH2 0: ssh_receive: 16 bytes received
00:05:43: SSH2 0: input: total packet length of 16 bytes
00:05:43: SSH2 0: partial packet length(block size)8 bytes,needed 8 bytes, maclen 0
00:05:43: SSH2 0: input: padlength 10 bytes
00:05:43: SSH2 0: newkeys: mode 0
00:05:43: SSH2 0: ssh_receive: 52 bytes received
00:05:43: SSH2 0: input: total packet length of 32 bytes
00:05:43: SSH2 0: partial packet length(block size)16 bytes,needed 16 bytes, maclen 20
00:05:43: SSH2 0: MAC compared for #3 :ok
```

セキュア シェル バージョン 2 サポートの追加情報

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『Cisco IOS Master Command List, All Releases』
AAA ホスト名およびホスト ドメインの設定タスク セキュア シェルの設定タスク	『*Security Configuration Guide*：*Securing User Services*』
ソフトウェア イメージのダウンロード 設定の基礎	『*Cisco IOS Configuration Fundamentals Configuration Guide*』
IPsec の設定作業	『*Security Configuration Guide*：*Secure Connectivity*』
SNMP トラップの設定タスク	『*SNMP Configuration Guide*』

標準

標準	タイトル
IETF Secure Shell Version 2 Draft 規格	Internet Engineering Task Force の Web サイト

シスコのテクニカル サポート

説明	リンク
右の URL にアクセスして、シスコのテクニカル サポートを最大限に活用してください。これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

セキュア シェル バージョン 2 サポートの機能情報

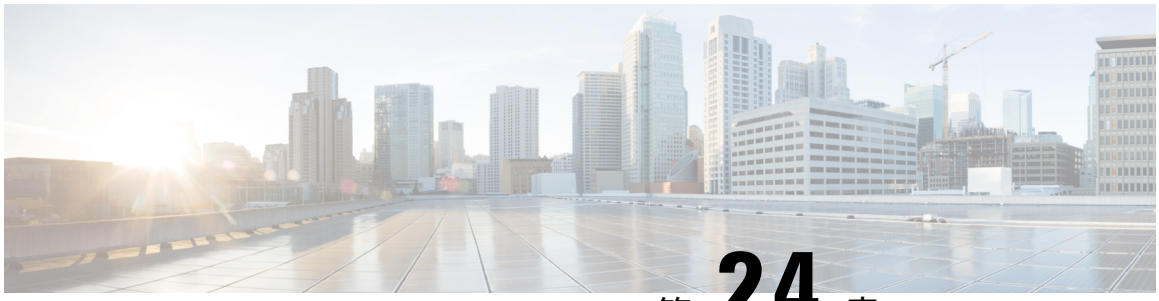
次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *41* : セキュア シェル バージョン *2* サポートの機能情報

機能名	リリース	機能情報
セキュア シェル バージョン 2 サポート		セキュア シェル バージョン 2 サポート機能を使用して、セキュア シェル（SSH）バージョン 2 を設定できます（SSH バージョン 1 のサポートは、以前の Cisco IOS ソフトウェア リリースで実装されていました）。SSH は、信頼性の高いトランスポート層の上部で実行され、強力な認証機能と暗号化機能を提供します。SSH バージョン 2 は、AES カウンタベース暗号化モードもサポートします。 次のコマンドが導入または変更されました：**debug ip ssh**、**ip ssh min dh size**、**ip ssh rsa keypair-name**、**ip ssh version**、**ssh**。
セキュア シェル バージョン 2 クライアントおよびサーバー サポート		Cisco IOS イメージが、SSH セッション終了時に SNMP トラップを自動的に生成するよう更新されました。

機能名	リリース	機能情報
SSH キーボードインタラクティブ認証		SSH キーボード インタラクティブ認証機能は、SSH での汎用メッセージ認証とも呼ばれ、異なる種類の認証メカニズムを実装するために使用できる方式です。基本的に、現在サポートされている、ユーザの入力のみが必要な認証方式はすべて、この機能で実行することができます。
セキュア シェル バージョン 2 の機能拡張		セキュア シェル バージョン 2 の機能拡張には、VRF aware SSH、SSH デバッグ機能拡張、および DH グループ 14 および 16 交換のサポートなどの、追加機能がいくつか含まれています。 次のコマンドが導入または変更されました：**debug ip ssh**、**ip ssh dh min size**。
セキュア シェル バージョン 2 の RSA キーに関する機能拡張		RSA キーのセキュア シェル バージョン 2 機能拡張には、SSH 向け RSA キー ベースのユーザー認証や、SSH サーバー ホスト キーの保存や検証のサポートなどの、追加機能がいくつか含まれています。 次のコマンドが導入または変更されました：**ip ssh pubkey-chain**、**ip ssh stricthostkeycheck**。



第 24 章

セキュア シェル：ユーザー認証方式の設定

セキュア シェル：ユーザー認証方式の設定機能によって、セキュア シェル（SSH）サーバーで使用可能なユーザー認証方式を設定できます。

セキュア シェルの制約事項：ユーザー認証方式の設定

セキュア シェル（SSH）サーバーと SSH クライアントは、データ暗号化ソフトウェア（DES）（56 ビット）および 3DES（168 ビット）イメージでのみサポートされます。

セキュア シェルに関する情報：ユーザー認証方式の設定

セキュア シェル ユーザー認証の概要

セキュア シェル（SSH）を使用することによって、SSH クライアントはシスコデバイス（Cisco IOS SSH サーバー）に対してセキュアで暗号化された接続を確立できます。SSH クライアントは SSH プロトコルを使用して、デバイス認証と暗号化を実行します。

SSH サーバーは、3 種類のユーザー認証方式をサポートし、これらの認証方式を事前に定義された次の順序で SSH クライアントに送信します。

- 公開キー認証方式

- キーボード インタラクティブ認証方式
- パスワード認証方式

デフォルトでは、すべてのユーザー認証方式が有効になっています。無効な方式が SSH ユーザー認証プロトコルでネゴシエートされないように特定のユーザー認証を無効にするには、**no ip ssh server authenticate user** {**publickey** | **keyboard** | **pasword**} コマンドを使用します。この機能によって、SSHサーバーは、事前に定義された順序とは異なる順序で希望のユーザー認証方式を指定できます。**ip ssh server authenticate user** {**publickey** | **keyboard** | **pasword**} コマンドを使用すると、無効になっているユーザー認証方式を有効にできます。

RFC 4252（セキュア シェル（SSH）認証プロトコル）のとおり、公開キー認証方式は必須です。この機能によって、SSH サーバーで RFC の動作をオーバーライドして、公開キー認証を含む任意の SSH ユーザー認証方式を無効にすることができます。

たとえば、SSHサーバーでパスワード認証方式を希望する場合、SSHサーバーで公開キー認証方式とキーボードインタラクティブ認証方式を無効にすることができます。

セキュアシェルの設定方法：ユーザー認証方式の設定方法

SSH サーバーのユーザー認証の設定

このタスクを実行して、セキュア シェル（SSH）サーバーでのユーザー認証方式を設定します。

手順の概要

1. **enable**
2. **configure terminal**
3. **no ip ssh server authenticate user** {**publickey** | **keyboard** | **pasword**}
4. **ip ssh server authenticate user** {**publickey** | **keyboard** | **pasword**}
5. **default ip ssh server authenticate user**
6. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。

	コマンドまたはアクション	目的
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。

ステップ 3	**no ip ssh server authenticate user** {**publickey** | **keyboard** | **pasword**}
	例：
	`Device(config)# no ip ssh server authenticate user publickey`
	`%SSH:Publickey disabled.Overriding RFC`
		セキュア シェル（SSH）サーバーでユーザー認証方式を無効にします。
		（注） **no ip ssh server authenticate user publickey** コマンドを使用して公開キー認証を無効にすると、警告メッセージが表示されます。このコマンドは、公開キー認証が必須であることが明記されている RFC 4252（セキュア シェル（SSH）認証プロトコル）の動作をオーバーライドします。

ステップ 4	**ip ssh server authenticate user** {**publickey** | **keyboard** | **pasword**} 例： `Device(config)# ip ssh server authenticate user publickey`	SSH サーバーで無効になっているユーザー認証方法を有効にします。
ステップ 5	**default ip ssh server authenticate user** 例： `Device(config)# default ip ssh server authenticate user`	すべてのユーザー認証方式が事前に定義された順序で有効になっているデフォルトの動作に戻ります。
ステップ 6	**end** 例： `Device(config)# end`	グローバル コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

トラブルシューティングのヒント

- **no ip ssh server authenticate user publickey** コマンドを使用して公開キーベースの認証方式を無効にすると、公開キー認証が必須の RFC 4252（セキュア シェル（SSH）認証プロトコル）の動作がオーバーライドされ、次の警告メッセージが表示されます。

  `%SSH:Publickey disabled.Overriding RFC`

- 3 つすべての認証方式が無効になっている場合、次の警告メッセージが表示されます。

  `%SSH:No auth method configured.Incoming connection will be dropped`

- 3 つすべての認証方式が SSH サーバーで無効になっているときに SSH クライアントから SSH セッション要求を受信した場合、接続要求は SSH サーバーでドロップされ、次の形式でシステム ログ メッセージが表示されます。

```
%SSH-3-NO_USERAUTH: No auth method configured for SSH Server. Incoming connection
from <ip address> (tty = <ttynum>) dropped
```

SSH サーバーのユーザー認証の確認

手順の概要

1. **enable**
2. **show ip ssh**

手順の詳細

ステップ 1 enable

特権 EXEC モードを有効にします。

- パスワードを入力します（要求された場合）。

例：

```
Device> enable
```

ステップ 2 show ip ssh

セキュア シェル（SSH）のバージョンおよび設定データを表示します。

例：

次の **show ip ssh** コマンドの出力例では、3 つすべてのユーザー認証方式が SSH サーバーで有効になっていることを確認します。

```
Device# show ip ssh

Authentication methods:publickey,keyboard-interactive,password
```

次の **show ip ssh** コマンドの出力例では、3 つすべてのユーザー認証方式が SSH サーバーで無効になっていることを確認します。

```
Device# show ip ssh

Authentication methods:NONE
```

セキュア シェルの設定例：ユーザー認証方式の設定

例：ユーザー認証方式の無効化

次の例では、公開キーベースの認証方式およびキーボードベースの認証方式を無効にし、パスワードベースの認証方式を使用して SSH クライアントが SSH サーバーに接続できるようにする方法を示します。

```
Device> enable
Device# configure terminal
Device(config)# no ip ssh server authenticate user publickey
%SSH:Publickey disabled.Overriding RFC
Device(config)# no ip ssh server authenticate user keyboard
Device(config)# exit
```

例：ユーザー認証方式の有効化

次の例では、公開キーベースの認証方式およびキーボードベースの認証方式を有効にする方法を示します。

```
Device> enable
Device# configure terminal
Device(config)# ip ssh server authenticate user publickey
Device(config)# ip ssh server authenticate user keyboard
Device(config)# exit
```

例：デフォルトのユーザー認証方式の設定

次の例では、3 つすべてのユーザー認証方式が事前に定義された順序で有効になっているデフォルトの動作に戻す方法を示します。

```
Device> enable
Device# configure terminal
Device(config)# default ip ssh server authenticate user
Device(config)# exit
```

セキュア シェルの追加情報：ユーザー認証方式の設定

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『Cisco IOS Master Command List, All Releases』
セキュリティ コマンド	• 『Cisco IOS Security Command Reference: Commands A to C』 • 『Cisco IOS Security Command Reference: Commands D to L』 • 『Cisco IOS Security Command Reference: Commands M to R』 • 『Cisco IOS Security Command Reference: Commands S to Z』
SSH の設定	『セキュア シェル コンフィギュレーション ガイド』

標準および RFC

標準/RFC	タイトル
RFC 4252	『セキュア シェル（*SSH*）認証プロトコル』
RFC 4253	『セキュア シェル（*SSH*）トランスポート層プロトコル』

シスコのテクニカル サポート

説明	リンク
シスコのサポート Web サイトでは、シスコの製品やテクノロジーに関するトラブルシューティングにお役立ていただけるように、マニュアルやツールをはじめとする豊富なオンライン リソースを提供しています。 お使いの製品のセキュリティ情報や技術情報を入手するために、Cisco Notification Service（Field Notice からアクセス）、Cisco Technical Services Newsletter、Really Simple Syndication（RSS）フィードなどの各種サービスに加入できます。 シスコのサポート Web サイトのツールにアクセスする際は、Cisco.com のユーザ ID およびパスワードが必要です。	http://www.cisco.com/support

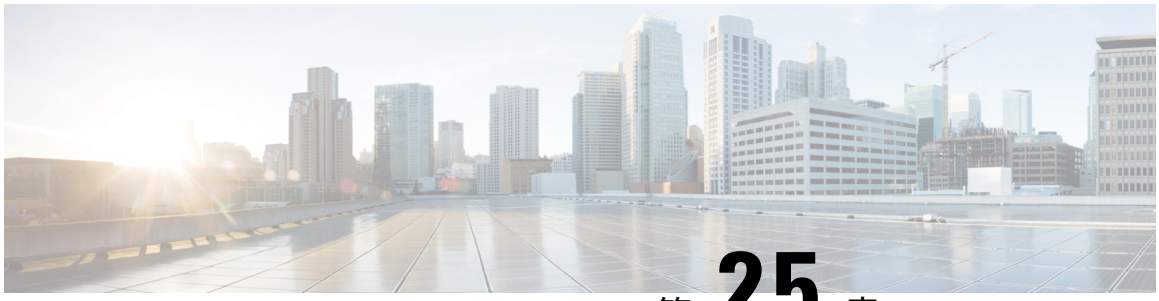
セキュア シェルの機能情報：ユーザー認証方式の設定

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *42*：セキュア シェルの機能情報：ユーザー認証方式の設定

機能名	リリース	機能情報
セキュア シェル：ユーザー認証方式の設定	Cisco IOS XE Release 3.10S	セキュア シェル：ユーザー認証方式の設定機能によって、セキュア シェル（SSH）サーバーで使用可能なユーザー認証方式を設定できます。 次のコマンドが導入されました：**ip ssh server authenticate user**。 この機能は、Cisco IOS XE Release3.10 で、Cisco ASR 1000 シリーズアグリゲーション サービス ルータに導入されました。



第 25 章

SSH 認証の X.509v3 証明書

SSH 認証の X.509v3 証明書機能は、サーバー内で X.509v3 デジタル証明書を使用し、セキュアシェル（SSH）サーバー側でユーザー認証を使用します。

このモジュールでは、デジタル証明書用のサーバおよびユーザ証明書プロファイルを設定する方法について説明します。

SSH 認証の X.509v3 証明書の前提条件

- SSH 認証の X.509v3 証明書機能では、**ip ssh server authenticate user** コマンドの代わりに **ip ssh server algorithm authentication** コマンドが導入されます。**ip ssh server authenticate user** コマンドを使用すると、次の警告メッセージが表示されます。

```
Warning: SSH command accepted but this CLI will be deprecated soon. Please move to
new CLI "ip ssh server algorithm authentication". Please configure "default ip ssh
server authenticate user" to make CLI ineffective.
```

  - **default ip ssh server authenticate user** コマンドを使用して、**ip ssh server authenticate user** コマンドを無効にします。その後、IOS セキュア シェル（SSH）サーバーは **ip ssh server algorithm authentication** コマンドを使用して起動します。

SSH 認証の X.509v3 証明書の制約事項

- SSH 認証の X.509v3 証明書機能の実装は、IOS セキュア シェル（SSH）サーバー側にのみ適用できます。

- IOS SSH サーバーは、IOS SSH サーバー側のサーバーおよびユーザー認証について、x509v3-ssh-rsa アルゴリズム ベースの証明書のみをサポートします。

SSH 認証用の X.509v3 証明書に関する情報

デジタル証明書

認証の有効性は、公開署名キーとその署名者のアイデンティティとの関連の強さに依存します。X.509v3 形式（RFC5280）のデジタル証明書は、アイデンティティの管理を実行するために使用されます。信頼できるルート証明機関とその中間証明機関による署名の連鎖によって、指定の公開署名キーと指定のデジタル アイデンティティがバインドされます。

公開キーインフラストラクチャ（PKI）のトラストポイントは、デジタル証明書の管理に役立ちます。証明書とトラストポイントを関連付けることによって、証明書を追跡できます。トラストポイントには、認証局（CA）、さまざまなアイデンティティ パラメータ、およびデジタル証明書に関する情報が含まれています。複数のトラストポイントを作成して、異なる証明書に関連付けることができます。

X.509v3 を使用したサーバーおよびユーザー認証

サーバー認証の場合、IOS セキュア シェル（SSH）が確認のためにそれ自体の証明書を SSH クライアントに送信します。このサーバ証明書は、サーバ証明書プロファイル（ssh-server-cert-profile-server コンフィギュレーション モード）で設定されたトラストポイントに関連付けられます。

ユーザ認証の場合、SSH クライアントが確認のためにユーザの証明書を IOS SSH サーバに送信します。SSH サーバは、サーバ証明書プロファイル（ssh-server-cert-profile-user コンフィギュレーション モード）で設定された公開キーインフラストラクチャ（PKI）トラストポイントを使用して、受信したユーザ証明書を確認します。

デフォルトでは、証明書ベースの認証が、IOS SSH サーバ端末でサーバおよびユーザに対して有効になっています。

SSH 認証用の X.509v3 証明書の設定方法

サーバー認証にデジタル証明書を使用するための IOS SSH サーバーの設定

手順の概要

1. **enable**

2. **configure terminal**
3. **ip ssh server algorithm hostkey** {**x509v3-ssh-rsa** [**ssh-rsa**] | **ssh-rsa** [**x509v3-ssh-rsa**]}
4. **ip ssh server certificate profile**
5. **server**
6. **trustpoint sign** *PKI-trustpoint-name*
7. **ocsp-response include**
8. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ip ssh server algorithm hostkey** {**x509v3-ssh-rsa** [**ssh-rsa**]	**ssh-rsa** [**x509v3-ssh-rsa**]} 例： `Device(config)# ip ssh server algorithm hostkey x509v3-ssh-rsa`	ホスト キー アルゴリズムの順序を定義します。セキュア シェル（SSH）クライアントとネゴシエートされるのは、設定済みのアルゴリズムのみです。 （注） IOS SSH サーバーには、1 つ以上の設定済みホスト キー アルゴリズムが必要です。 • ssh-rsa：公開キーベース認証 • x509v3-ssh-rsa：証明書ベース認証
ステップ 4	**ip ssh server certificate profile** 例： `Device(config)# ip ssh server certificate profile`	サーバー証明書プロファイルおよびユーザー証明書プロファイルを設定し、SSH 証明書プロファイル コンフィギュレーション モードを開始します。
ステップ 5	**server** 例： `Device(ssh-server-cert-profile)# server`	サーバー証明書プロファイルを設定し、SSH サーバー証明書プロファイルのユーザー コンフィギュレーション モードを開始します。
ステップ 6	**trustpoint sign** *PKI-trustpoint-name* 例：	公開キー インフラストラクチャ（PKI）トラストポイントをサーバ証明書プロファイルにアタッチします。SSH サーバは、この PKI トラストポイントに関連付けられた証明書をサーバ認証に使用します。

	コマンドまたはアクション	目的
	`Device(ssh-server-cert-profile-server)# trustpoint sign trust1`	
ステップ 7	**ocsp-response include** 例： `Device(ssh-server-cert-profile-server)# ocsp-response include`	（任意）Online Certificate Status Protocol（OCSP）の応答または OCSP ステープリングをサーバ証明書と一緒に送信します。 （注） デフォルトではこのコマンドの「no」形式が設定されており、OCSP 応答はサーバー証明書と一緒には送信されません。
ステップ 8	**end** 例： `Device(ssh-server-cert-profile-server)# end`	SSH サーバー証明書プロファイルのサーバー コンフィギュレーション モードを終了し、特権 EXEC モードを開始します。

ユーザ認証用のユーザのデジタル証明書を確認するためのIOSSSHサーバの設定

手順の概要

1. **enable**
2. **configure terminal**
3. **ip ssh server algorithm authentication** {**publickey** | **keyboard** | **password**}
4. **ip ssh server algorithm publickey** {**x509v3-ssh-rsa** [**ssh-rsa**] | **ssh-rsa** [**x509v3-ssh-rsa**]}
5. **ip ssh server certificate profile**
6. **user**
7. **trustpoint verify** *PKI-trustpoint-name*
8. **ocsp-response required**
9. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 3	**ip ssh server algorithm authentication** {**publickey** | **keyboard** | **password**} 例： `Device(config)# ip ssh server algorithm authentication publickey`	ユーザ認証アルゴリズムの順序を定義します。セキュア シェル（SSH）クライアントとネゴシエートされるのは、設定済みのアルゴリズムのみです。 （注） IOS SSH サーバには、1 つ以上の設定済みユーザ認証アルゴリズムが必要です。 （注） ユーザー認証に証明書方式を使用するには、**publickey** キーワードを設定する必要があります。 （注） **ip ssh server algorithm authentication** コマンドは **ip ssh server authenticate user** コマンドの代わりに使用します。
ステップ 4	**ip ssh server algorithm publickey** {**x509v3-ssh-rsa** [**ssh-rsa**] | **ssh-rsa** [**x509v3-ssh-rsa**]} 例： `Device(config)# ip ssh server algorithm publickey x509v3-ssh-rsa`	公開キー アルゴリズムの順序を定義します。SSH クライアントによってユーザ認証に許可されるのは、設定済みのアルゴリズムのみです。 （注） IOS SSH クライアントには、1 つ以上の設定済み公開キー アルゴリズムが必要です。 • ssh-rsa：公開キーベース認証 • x509v3-ssh-rsa：証明書ベース認証
ステップ 5	**ip ssh server certificate profile** 例： `Device(config)# ip ssh server certificate profile`	サーバ証明書プロファイルおよびユーザ証明書プロファイルを設定し、SSH 証明書プロファイル コンフィギュレーション モードを開始します。
ステップ 6	**user** 例： `Device(ssh-server-cert-profile)# user`	ユーザ証明書プロファイルを設定し、SSH サーバ証明書プロファイルのユーザ コンフィギュレーション モードを開始します。
ステップ 7	**trustpoint verify** *PKI-trustpoint-name* 例： `Device(ssh-server-cert-profile-user)# trustpoint verify trust2`	受信したユーザ証明書の確認に使用される公開キー インフラストラクチャ（PKI）トラストポイントを設定します。 （注） 同じコマンドを複数回実行することで、複数のトラストポイントを設定します。最大 10 のトラストポイントを設定できます。

	コマンドまたはアクション	目的
ステップ 8	**ocsp-response required** 例： `Device(ssh-server-cert-profile-user)# ocsp-response required`	（任意）受信したユーザ証明書による Online Certificate Status Protocol（OCSP）の応答の有無を要求します。 （注） デフォルトではこのコマンドの「no」形式が設定されており、ユーザー証明書は OCSP 応答なしで受け入れられます。
ステップ 9	**end** 例： `Device(ssh-server-cert-profile-user)# end`	SSH サーバー証明書プロファイルのユーザー コンフィギュレーション モードを終了し、特権 EXEC モードを開始します。

デジタル証明書を使用したサーバーおよびユーザー認証の設定の確認

手順の概要

1. **enable**
2. **show ip ssh**

手順の詳細

ステップ 1 enable

特権 EXEC モードを有効にします。

- パスワードを入力します（要求された場合）。

例：

```
Device> enable
```

ステップ 2 show ip ssh

現在設定されている認証方式を表示します。証明書ベース認証の使用を確認するには、x509v3-ssh-rsa アルゴリズムが設定済みのホスト キー アルゴリズムであることを確認します。

例：

```
Device# show ip ssh

SSH Enabled - version 1.99
Authentication methods:publickey,keyboard-interactive,password
Authentication Publickey Algorithms:x509v3-ssh-rsa,ssh-rsa
Hostkey Algorithms:x509v3-ssh-rsa,ssh-rsa
Authentication timeout: 120 secs; Authentication retries: 3
```

```
Minimum expected Diffie Hellman key size : 1024 bits
```

SSH 認証用の X.509v3 証明書の設定例

例：サーバー認証にデジタル証明書を使用するためのIOSSSHサーバーの設定

```
Device> enable
Device# configure terminal
Device(config)# ip ssh server algorithm hostkey x509v3-ssh-rsa
Device(config)# ip ssh server certificate profile
Device(ssh-server-cert-profile)# server
Device(ssh-server-cert-profile-server)# trustpoint sign trust1
Device(ssh-server-cert-profile-server)# exit
```

例：ユーザ認証用のユーザのデジタル証明書を確認するためのIOSSSHサーバの設定

```
Device> enable
Device# configure terminal
Device(config)# ip ssh server algorithm authentication publickey
Device(config)# ip ssh server algorithm publickey x509v3-ssh-rsa
Device(config)# ip ssh server certificate profile
Device(ssh-server-cert-profile)# user
Device(ssh-server-cert-profile-user)# trustpoint verify trust2
Device(ssh-server-cert-profile-user)# end
```

SSH 認証用の X.509v3 証明書に関するその他の参考資料

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『Cisco IOS Master Command List, All Releases』

関連項目	マニュアル タイトル
セキュリティ コマンド	• 『Cisco IOS Security Command Reference: Commands A to C』[英語] • 『Cisco IOS Security Command Reference: Commands D to L』[英語] • 『Cisco IOS Security Command Reference: Commands M to R』 [英語] • 『Cisco IOS Security Command Reference: Commands S to Z』[英語]
SSH 認証	『セキュア シェル コンフィギュレーション ガイド』の「セキュア シェル：ユーザー認証方式の設定」の章
公開キー インフラストラクチャ（PKI）のトラストポイント	『*Public Key Infrastructure Configuration Guide*』の「Configuring and Managing a Cisco IOS Certificate Server for PKI Deployment」の章

シスコのテクニカル サポート

説明	リンク
シスコのサポート Web サイトでは、シスコの製品やテクノロジーに関するトラブルシューティングにお役立ていただけるように、マニュアルやツールをはじめとする豊富なオンライン リソースを提供しています。 お使いの製品のセキュリティ情報や技術情報を入手するために、Cisco Notification Service（Field Notice からアクセス）、Cisco Technical Services Newsletter、Really Simple Syndication（RSS）フィードなどの各種サービスに加入できます。 シスコのサポート Web サイトのツールにアクセスする際は、Cisco.com のユーザ ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

SSH 認証用の X.509v3 証明書の機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *43 : SSH* 認証の *X.509v3* 証明書の機能情報

機能名	リリース	機能情報
SSH 認証の X.509v3 証明書		SSH 認証の X.509v3 証明書機能は、サーバー内で X.509v3 デジタル証明書を使用し、セキュア シェル（SSH）サーバー側でユーザー認証を使用します。 次のコマンドが導入または変更されました。**ip ssh server algorithm hostkey**、**ip ssh server algorithm authentication**、**ip ssh server certificate profile**

第 26 章

コモン クライテリア認定用の SSH アルゴリズム

コモンクライテリア認定用の SSH アルゴリズム機能によって、コモンクライテリア認定を取得したアルゴリズムのリストおよび順序が提供されます。このモジュールでは、認定されたアルゴリズムのリストに基づいて SSH 接続を制限できるように、セキュア シェル（SSH）サーバーおよびクライアントの暗号化、メッセージ認証コード（MAC）、およびホスト キー アルゴリズムの設定方法について説明します。

コモンクライテリア認証のための SSH アルゴリズムの制限

- Cisco IOS XE リリース 17.10 以降、次のキー交換および MAC アルゴリズムがデフォルトのリストから削除されました。

  キー交換アルゴリズム：

  - diffie-hellman-group14-sha1

  MAC アルゴリズム：

  - hmac-sha1
  - hmac-sha2-256
  - hmac-sha2-512

（注） **ip ssh server algorithm kex** コマンドを使用するとキー交換アルゴリズムを設定でき、**ip ssh server algorithm mac** コマンドを使用すると MAC アルゴリズムを設定できます。

コモンクライテリア認定用のSSHアルゴリズムに関する情報

コモン クライテリア認定用の SSH アルゴリズム

セキュア シェル（SSH）設定によって、Cisco IOS SSH サーバーおよびクライアントは、許可リストから設定されたアルゴリズムのネゴシエーションのみを許可することができます。リモートパーティが許可リストに含まれていないアルゴリズムのみを使用してネゴシエートしようとすると、要求は拒否され、セッションは確立されません。

Cisco IOS SSH サーバー アルゴリズム

Cisco IOS セキュアシェル（SSH）サーバーは、次の順序で暗号化アルゴリズム（Advanced Encryption Standard カウンタモード [AES-CTR]、AES 暗号ブロック連鎖 [AES-CBC]、Triple Data Encryption Standard [3DES]、Galois/Counter Mode [GCM]）、メッセージ認証コード（MAC）アルゴリズム、ホストキーアルゴリズム、キー交換（KEX）DH グループアルゴリズム、および公開キーアルゴリズムをサポートします。

表 *44 :* サポートされるデフォルトおよびデフォルト以外の *IOS SSH* サーバーアルゴリズム

サポートされるアルゴリズム	デフォルト	非デフォルト
暗号化	**1.** chacha20-poly1305@openssh.com **2.** aes128-gcm@openssh.com **3.** aes256-gcm@openssh.com **4.** aes128-gcm **5.** aes256-gcm **6.** aes128-ctr **7.** aes192-ctr **8.** aes256-ctr	• aes128-cbc • aes192-cbc • aes256-cbc • 3des-cbc

サポートされるアルゴリズム	デフォルト	非デフォルト
HMAC	1. hmac-sha2-256-etm@openssh.com 2. hmac-sha2-512-etm@openssh.com	• hmac-sha1 • hmac-sha2-256 • hmac-sha2-512
ホストキー	1. rsa-sha2-512 2. rsa-sha2-256 3. ssh-rsa	• x509v3-ssh-rsa
KEX DH グループ	1. curve25519-sha256 2. curve25519-sha256@libssh.org 3. ecdh-sha2-nistp256 4. ecdh-sha2-nistp384 5. ecdh-sha2-nistp521 6. diffie-hellman-group14-sha256 7. diffie-hellman-group16-sha512	• diffie-hellman-group14-sha1
公開キー	1. ssh-rsa 2. ecdsa-sha2-nistp256 3. ecdsa-sha2-nistp384 4. ecdsa-sha2-nistp521 5. ssh-ed25519 6. x509v3-ecdsa-sha2-nistp256 7. x509v3-ecdsa-sha2-nistp384 8. x509v3-ecdsa-sha2-nistp521 9. rsa-sha2-256 10. rsa-sha2-512 11. x509v3-rsa2048-sha256	• x509v3-ssh-rsa

Cisco IOS SSH クライアント アルゴリズム

Cisco IOS セキュアシェル（SSH）クライアントは、次の順序で暗号化アルゴリズム（Advanced Encryption Standard カウンタモード [AES-CTR]、AES 暗号ブロック連鎖 [AES-CBC]、Triple Data

Encryption Standard [3DES]、Galois/Counter Mode (GCM)）、MAC アルゴリズム、および KEX DH グループアルゴリズムをサポートします。

表 *45 :* サポートされるデフォルトおよびデフォルト以外の *IOS SSH* サーバーアルゴリズム

サポートされるアルゴリズム	デフォルト	非デフォルト
暗号化	**1.** chacha20-poly1305@openssh.com **2.** aes128-gcm@openssh.com **3.** aes256-gcm@openssh.com **4.** aes128-gcm **5.** aes256-gcm **6.** aes128-ctr **7.** aes192-ctr **8.** aes256-ctr	• aes128-cbc • aes192-cbc • aes256-cbc • 3des-cbc
HMAC	**1.** hmac-sha2-256-etm@openssh.com **2.** hmac-sha2-512-etm@openssh.com	• hmac-sha1 • hmac-sha2-256 • hmac-sha2-512
KEX DH グループ	**1.** curve25519-sha256 **2.** curve25519-sha256@libssh.org **3.** ecdh-sha2-nistp256 **4.** ecdh-sha2-nistp384 **5.** ecdh-sha2-nistp521 **6.** diffie-hellman-group14-sha256 **7.** diffie-hellman-group16-sha512	• diffie-hellman-group14-sha1

コモンクライテリア認定用のSSHアルゴリズムの設定方法

Cisco IOS SSHサーバーおよびクライアントの暗号キーアルゴリズムの設定

手順の概要

1. **enable**
2. **configure terminal**
3. **ip ssh** {**server** | **client**} **algorithm encryption** {**aes128-ctr** | **aes192-ctr** | **aes256-ctr** | **aes128-cbc** | **3des-cbc** | **aes192-cbc** | **aes256-cbc**}
4. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。

ステップ 3	**ip ssh** {**server**	**client**} **algorithm encryption** {**aes128-ctr**	**aes192-ctr**	**aes256-ctr**	**aes128-cbc**	**3des-cbc**	**aes192-cbc**	**aes256-cbc**}
								例：
								`Device(config)# ip ssh server algorithm encryption aes128-ctr aes192-ctr aes256-ctr aes128-cbc 3des-cbc aes192-cbc aes256-cbc`
								`Device(config)# ip ssh client algorithm encryption aes128-ctr aes192-ctr aes256-ctr aes128-cbc 3des-cbc aes192-cbc aes256-cbc`
									SSHサーバーおよびクライアントでの暗号化アルゴリズムの順序を定義します。この順序は、アルゴリズムのネゴシエーション時に指定されます。
									（注） Cisco IOS SSH サーバーおよびクライアントには、1つ以上の設定済み暗号化アルゴリズムが必要です。
									（注） 以前設定したアルゴリズムのリストから1つのアルゴリズムを無効にするには、このコマンドの **no** 形式を使用します。複数のアルゴリズムを無効にするには、このコマンドの **no** 形式を異なるアルゴリズム名で複数回使用します。

	コマンドまたはアクション	目的
		（注） デフォルト設定では、次に示すようにこのコマンドのデフォルト形式を使用します。 `Device(config)# ip ssh server algorithm encryption aes128-ctr aes192-ctr aes256-ctr aes128-cbc 3des-cbc aes192-cbc aes256-cbc`
ステップ 4	**end** 例： `Device(config)# end`	グローバル コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

トラブルシューティングのヒント

設定で最後の暗号化アルゴリズムを無効にしようとすると、次のメッセージが表示されてコマンドが拒否されます。

```
% SSH command rejected: All encryption algorithms cannot be disabled
```

Cisco IOS SSH サーバーおよびクライアントの MAC アルゴリズムの設定

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ip ssh** {**server** | **client**} **algorithm mac** {**hmac-sha2** | **hmac-sha2-96**} 例： `Device(config)# ip ssh server algorithm mac hmac-sha2 hmac-sha2-96`	SSH サーバーおよびクライアントでの MAC（メッセージ認証コード）アルゴリズムの順序を定義します。この順序は、アルゴリズムのネゴシエーション時に指定されます。

	コマンドまたはアクション	目的
	`Device(config)# ip ssh client algorithm mac hmac-sha2 hmac-sha2-96`	（注） Cisco IOS SSH サーバーおよびクライアントには、1 つ以上の設定済みハッシュ メッセージ認証コード（HMAC）アルゴリズムが必要です。 （注） 以前設定したアルゴリズムのリストから 1 つのアルゴリズムを無効にするには、このコマンドの **no** 形式を使用します。複数のアルゴリズムを無効にするには、このコマンドの **no** 形式を異なるアルゴリズム名で複数回使用します。 （注） デフォルト設定では、次に示すようにこのコマンドのデフォルト形式を使用します。 `Device(config)# ip ssh server algorithm mac hmac-sha2 hmac-sha2-96`
ステップ 4	**end** 例： `Device(config)# end`	グローバル コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

トラブルシューティングのヒント

設定で最後の MAC アルゴリズムを無効にしようとすると、次のメッセージが表示されてコマンドが拒否されます。

```
% SSH command rejected: All mac algorithms cannot be disabled
```

Cisco IOS SSH サーバーのホスト キー アルゴリズムの設定

手順の概要

1. **enable**
2. **configure terminal**
3. **ip ssh server algorithm hostkey** {**x509v3-ssh-rsa** | **ssh-rsa**}
4. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ip ssh server algorithm hostkey** {**x509v3-ssh-rsa** | **ssh-rsa**} 例： `Device(config)# ip ssh server algorithm hostkey x509v3-ssh-rsa ssh-rsa`	ホストキーアルゴリズムの順序を定義します。Cisco IOS セキュア シェル（SSH）クライアントとネゴシエートされるのは、設定済みのアルゴリズムのみです。 （注） Cisco IOS SSH サーバーには、1 つ以上の設定済みホスト キー アルゴリズムが必要です。 • x509v3-ssh-rsa：X.509v3 証明書ベース認証 • ssh-rsa：公開キーベース認証 （注） 以前設定したアルゴリズムのリストから 1 つのアルゴリズムを無効にするには、このコマンドの **no** 形式を使用します。複数のアルゴリズムを無効にするには、このコマンドの **no** 形式を異なるアルゴリズム名で複数回使用します。 （注） デフォルト設定では、次に示すようにこのコマンドのデフォルト形式を使用します。 `Device(config)# ip ssh server algorithm hostkey x509v3-ssh-rsa ssh-rsa`
ステップ 4	**end** 例： `Device(config)# end`	グローバル コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

トラブルシューティングのヒント

設定で最後のホスト キー アルゴリズムを無効にしようとすると、次のメッセージが表示されてコマンドが拒否されます。

```
% SSH command rejected: All hostkey algorithms cannot be disabled
```

コモン クライテリア認定用の SSH アルゴリズムの確認

手順の概要

1. **enable**
2. **show ip ssh**

手順の詳細

ステップ 1 enable

特権 EXEC モードを有効にします。

- パスワードを入力します（要求された場合）。

例：

```
Device> enable
```

ステップ 2 show ip ssh

設定済みのセキュア シェル（SSH）暗号化、ホスト キー、およびメッセージ認証コード（MAC）アルゴリズムを表示します。

例：

次の **show ip ssh** コマンドの出力例は、デフォルトの順序で設定された暗号化アルゴリズムを示しています。

```
Device# show ip ssh
Encryption Algorithms: aes128-ctr, aes192-ctr, aes256-ctr, aes128-cbc, 3des-cbc, aes192-cbc, aes256-cbc
```

次の **show ip ssh** コマンドの出力例は、デフォルトの順序で設定された MAC アルゴリズムを示しています。

```
Device# show ip ssh
MAC Algorithms: hmac-sha1 hmac-sha1-96
```

次の **show ip ssh** コマンドの出力例は、デフォルトの順序で設定されたホスト キー アルゴリズムを示しています。

```
Device# show ip ssh

Hostkey Algorithms: x509v3-ssh-rsa, ssh-rsa
```

コモンクライテリア認定用の SSH アルゴリズムの設定例

例：Cisco IOS SSH サーバーの暗号キー アルゴリズムの設定

```
Device> enable
Device# configure terminal
Device(config)# ip ssh server algorithm encryption aes128-ctr aes192-ctr aes256-ctr
aes128-cbc 3des-cbc aes192-cbc aes256-cbc
Device(config)# end
```

例：Cisco IOS SSH クライアントの暗号キー アルゴリズムの設定

```
Device> enable
Device# configure terminal
Device(config)# ip ssh client algorithm encryption aes128-ctr aes192-ctr aes256-ctr
aes128-cbc 3des-cbc aes192-cbc aes256-cbc
Device(config)# end
```

例：Cisco IOS SSH サーバーの MAC アルゴリズムの設定

```
Device> enable
Device# configure terminal
Device(config)# ip ssh server algorithm mac hmac-sha1 hmac-sha1-96
Device(config)# end
```

例：Cisco IOS SSH サーバー用のキー交換 DH グループの設定

```
Device> enable
Device# configure terminal
Device(config)# ip ssh server algorithm kex diffie-hellman-group-exchange-sha1
Device(config)# end
```

```
Device> enable
Device# configure terminal
Device(config)# ip ssh server algorithm kex diffie-hellman-group14-sha1
Device(config)# end
```

例：Cisco IOS SSH サーバーのホスト キー アルゴリズムの設定

```
Device> enable
Device# configure terminal
Device(config)# ip ssh server algorithm hostkey x509v3-ssh-rsa ssh-rsa
Device(config)# end
```

コモンクライテリア認定用のSSHアルゴリズムの追加情報

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『Cisco IOS Master Command List, All Releases』
セキュリティ コマンド	• 『Cisco IOS Security Command Reference: Commands A to C』[英語] • 『Cisco IOS Security Command Reference: Commands D to L』[英語] • 『Cisco IOS Security Command Reference: Commands M to R』[英語] • 『Cisco IOS Security Command Reference: Commands S to Z』[英語]
SSH 認証	『セキュア シェル コンフィギュレーション ガイド』の「セキュア シェル：ユーザー認証方式の設定」の章
サーバーおよびユーザー認証での X.509v3 デジタル証明書	『セキュア シェル コンフィギュレーション ガイド』の「SSH 認証の X.509v3 証明書」の章

シスコのテクニカル サポート

説明	リンク
シスコのサポート Web サイトでは、シスコの製品やテクノロジーに関するトラブルシューティングにお役立ていただけるように、マニュアルやツールをはじめとする豊富なオンライン リソースを提供しています。 お使いの製品のセキュリティ情報や技術情報を入手するために、Cisco Notification Service（Field Notice からアクセス）、Cisco Technical Services Newsletter、Really Simple Syndication（RSS）フィードなどの各種サービスに加入できます。 シスコのサポート Web サイトのツールにアクセスする際は、Cisco.com のユーザ ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

コモンクライテリア認定用の SSH アルゴリズムの機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *46* : コモン クライテリア認定用の *SSH* アルゴリズムの機能情報

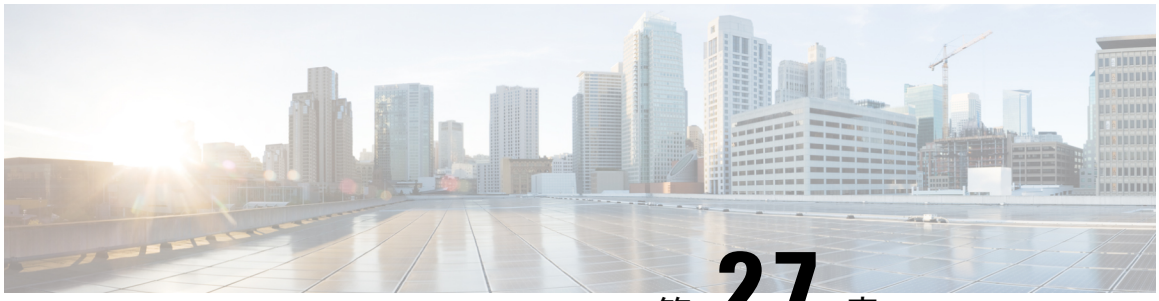
機能名	リリース	機能情報
コモン クライテリア認定用の SSH アルゴリズム	Cisco IOS XE Everest 16.5.1a	コモンクライテリア認定用の SSH アルゴリズム機能によって、コモンクライテリア認定を取得したアルゴリズムのリストおよび順序が提供されます。このモジュールでは、認定されたアルゴリズムのリストに基づいて SSH 接続を制限できるように、セキュアシェル（SSH）サーバーおよびクライアントの暗号化、メッセージ認証コード（MAC）、およびホストキー アルゴリズムの設定方法について説明します。 この機能により、次のコマンドが導入されました：**ip ssh** {**server** | **client**} **algorithm encryption**、**ip ssh** {**server** | **client**} **algorithm mac**。
コモン クライテリア認定用の SSH アルゴリズム	Cisco IOS XE Cupertino 17.8.1	次のアルゴリズムに対する Cisco IOS SSH サーバーおよびクライアントのサポートが導入されました。 • chacha20-poly1305@openssh.com • ssh-ed25519 • curve25519-sha256@libssh.org
コモン クライテリア認定用の SSH アルゴリズム	Cisco IOS XE Cupertino 17.9.1	次のアルゴリズムに対する Cisco IOS SSH サーバーおよびクライアントのサポートが導入されました。 • aes128-gcm@openssh.com • aes256-gcm@openssh.com

弱い暗号の廃止	Cisco IOS XE リリース 17.10	次の変更が導入されました。
		• セキュアシェルバージョン 1.99 は、サポートされません。
		• 次の弱いキー交換および MAC アルゴリズムは、アルゴリズムのデフォルトリストから削除されます。
		  • diffie-hellman-group14-sha1
		  • hmac-sha1
		  • hmac-sha2-256
		  • hmac-sha2-512

機能名	リリース	機能情報
コモン クライテリア認定用の SSH アルゴリズム	Cisco IOS XE リリース 17.11.1a	次のアルゴリズムに対する Cisco IOS SSH サーバーおよびクライアントのサポートが導入されました。 • curve25519-sha256 • diffie-hellman-group14-sha256 • diffie-hellman-group16-sha512 • x509v3-rsa2048-sha256

第 III 部

アクセス コントロール リスト



第 27 章

IP アクセス リストの概要

アクセス コントロール リスト（ACL）は、パケット フィルタリングを実行して、ネットワークを介して移動するパケットと移動先を制御します。パケット フィルタリングによって、ネットワーク トラフィックを制限し、ユーザーおよびデバイスのネットワークに対するアクセスを制限し、トラフィックがネットワークから外部に送信されるのを防ぐことで、セキュリティを実現します。IP アクセス リストによって、スプーフィングやサービス妨害攻撃の可能性を軽減し、ファイアウォールを介した動的で一時的なユーザー アクセスが可能になります。

また、IP アクセス リストは、セキュリティ以外の用途にも使用できます。たとえば、帯域幅制御、ルーティング アップデートのコンテンツの制限、ルートの再配布、ダイヤルオンデマンド（DDR）呼び出しのトリガー、デバッグ出力の制限、Quality of Service（QoS）機能のトラフィックの識別と分類などです。このモジュールでは、IP アクセス リストの概要について説明します。

IP アクセス リストに関する情報

IP アクセス リストの利点

アクセス コントロール リスト（ACL）は、ネットワークを通過するパケットのフローを制御するためにパケット フィルタリングを実行します。パケット フィルタリングによってユーザーおよびデバイスのネットワークに対するアクセスを制限し、セキュリティの手段として利用できます。アクセス リストによってトラフィック数を減らすことで、ネットワーク リソースを節約できます。アクセス リストを使用した場合の利点は次のとおりです。

- 着信 rsh および rcp 要求を認証する：アクセス リストは、デバイスへのアクセスを制御するように構成された認証データベース内のローカル ユーザー、リモート ホスト、およびリモート ユーザーの識別を簡素化できます。Cisco ソフトウェアは認証データベースを使用して、リモート シェル（rsh）およびリモート コピー（rcp）プロトコルの着信要求を受け取ることができます。

- 不要なトラフィックまたはユーザーをブロックする：アクセスリストを使用すると、インターフェイス上の着信パケットまたは発信パケットをフィルタできるため、送信元アドレス、宛先アドレス、またはユーザー認証に基づいてネットワークへのアクセスを制御できます。また、アクセスリストを使用して、デバイスインターフェイスで転送またはブロックするトラフィックの種類を決定することもできます。たとえば、電子メールトラフィックはネットワークでルーティングすることを許可し、すべてのTelnetトラフィックはネットワークに入ることをブロックするようにアクセス リストを使用できます。
- vtyへのアクセスを制御する：インバウンドvty（Telnet）でのアクセス リストは、デバイスへの回線にアクセスできるユーザーを制御できます。アウトバウンドvtyでのアクセス リストは、デバイスからの回線が到達可能な宛先を制御できます。
- QoS機能のトラフィックを特定または分類する：アクセス リストは、Weighted Random Early Detection（WRED）および専用アクセス レート（CAR）のIPプレシデンスを設定することで、輻輳回避を提供します。また、クラスベース均等化キューイング（CBWFQ）、プライオリティ キューイング、カスタム キューイングのために輻輳管理を提供します。
- debugコマンド出力を制限する：アクセス リストは、IPアドレスやプロトコルに基づいてdebug出力を制限できます。
- 帯域幅制御を提供する：低速リンクでのアクセス リストはネットワークでの過剰なトラフィックを防止できます。
- NAT制御を提供する：アクセス リストによって、ネットワーク アドレス変換（NAT）が変換するアドレスを制御できます。
- DoS攻撃の可能性を低減する：アクセスリストは、サービス妨害（DoS）攻撃の可能性を低減させます。ホストからのトラフィック、ネットワーク、またはネットワークにアクセスするユーザーを制御するようにIP発信元アドレスを指定します。TCPインターセプト機能を設定することで、接続に関する要求でサーバーにフラッディングが発生しないようにすることができます。
- ルーティング アップデートの内容を制限する：アクセス リストによって、ネットワーク内で送信、受信、または再配布されるルーティング アップデートを制御できます。
- ダイヤルオンデマンド コールをトリガーする：アクセス リストによって、ダイヤルおよび切断条件を適用できます。

アクセスリストを使用する必要がある境界ルータおよびファイアウォール ルータ

アクセスリストを設定する理由は多数あります。たとえば、アクセスリストを使用して、ルーティング アップデートのコンテンツを制限したり、トラフィック フローを制御したりできます。アクセスリストを設定する最も重要な理由の1つは、ネットワークに対するアクセスを制御することで、ネットワークに基本レベルのセキュリティを提供することです。ルータでアクセスリストを設定しない場合、ルータを通過するすべてのパケットは、ネットワークのすべての部分で許可される可能性があります。

アクセスリストで、ネットワークの一部に対してアクセスを許可するホストと、同じ領域に対してアクセスを禁止するホストを設定できます。以下の図では、適切なアクセスリストをルータのインターフェイスに適用することで、ホスト A は Human Resources ネットワークに対するアクセスが許可され、ホスト B は Human Resources ネットワークに対するアクセスが禁止されます。

ファイアウォール ルータにはアクセス リストを使用する必要があります。多くの場合、ファイアウォールルータは内部ネットワークと外部ネットワーク（インターネット）の間に配置されます。また、ネットワークの2つの部分の間に配置されたルータにアクセスリストを使用して、内部ネットワークの特定の部分に発着信するトラフィックを制御できます。

アクセスリストのセキュリティ上の利点を実現するために、場合によっては、少なくとも境界ルータでアクセスリストを設定する必要があります。境界ルータとは、ネットワークのエッジにあるルータです。このようなアクセスリストは、外部ネットワークから、または内部ネットワークのあまり制御されていない領域から、内部ネットワークの機密性が高い領域に対する基本的なバッファとして機能します。このような境界ルータでは、ルータインターフェイスに設定されている各ネットワーク プロトコルに合わせてアクセス リストを設定する必要があります。着信トラフィック、発信トラフィック、またはその両方がインターフェイスでフィルタされるように、アクセス リストを設定できます。

アクセス リストは個々のプロトコル ベースで定義されます。つまり、各プロトコルのトラフィック フローを制御する場合、インターフェイスでイネーブルにするプロトコルごとにアクセス リストを定義する必要があります。

アクセス リストの定義

アクセス コントロール リスト（ACL）は、ネットワークを通過するパケットの動きを制御するためにパケット フィルタリングを実行します。パケット フィルタリングは、ネットワークへのトラフィックのアクセスを限定し、ユーザーおよびデバイスのネットワークに対するアクセスを制限し、トラフィックがネットワークから流出するのを防ぐことで、セキュリティを提供します。IP アクセス リストによって、スプーフィングやサービス妨害攻撃の可能性を軽減し、ファイアウォールを介した動的で一時的なユーザー アクセスが可能になります。

また、IP アクセス リストは、セキュリティ以外の用途にも使用できます。たとえば、帯域幅制御、ルーティング アップデートのコンテンツの制限、ルートの再配布、ダイヤルオンデマンド（DDR）呼び出しのトリガー、デバッグ出力の制限、Quality of Service（QoS）機能のトラフィックの識別と分類などです。

アクセス リストは、少なくとも 1 つの **permit** ステートメント、および任意の 1 つまたは複数の **deny** ステートメントで構成される順次リストです。IP アクセス リストの場合、これらのステートメントは IP アドレス、上位層の IP プロトコルなどの IP パケットのフィールドに適用できます。

アクセスリストは名前または番号で識別および参照されます。アクセスリストはパケットフィルタとして動作し、各アクセスリストに定義されている条件に基づいてパケットがフィルタされます。

アクセスリストを構成した後でアクセスリストを有効にするには、アクセスリストをインターフェイスに適用するか（**ip access-group** コマンドを使用）、vty に適用するか（**access-class** コ

マンドを使用）、またはアクセス リストを許容するあらゆるコマンドでアクセス リストを参照する必要があります。複数のコマンドから同じアクセス リストを参照できます。

次の構成では、branchoffices という名前の IP アクセス リストがファスト イーサネット インターフェイス 0/1/0 上で構成され、着信パケットに適用されます。発信元アドレスとマスクのペアで指定されているネットワーク以外は、ファスト イーサネット インターフェイス 0/1/0 にアクセスできません。ネットワーク 172.16.7.0 上の送信元から発信されるパケットの宛先に、制限はありません。ネットワーク 172.16.2.0 上の送信元から発信されるパケットの宛先は、172.31.5.4 にする必要があります。

```
ip access-list extended branchoffices
 10 permit 172.16.7.0 0.0.0.3 any
 20 permit 172.16.2.0 0.0.0.255 host 172.31.5.4
!
interface fastethernet 0/1/0
 ip access-group branchoffices in
```

アクセス リストのルール

アクセス リストには、次のルールが適用されます。

- 1 つのインターフェイス、1 つのプロトコル、1 つの方向につき、許可されるアクセス リストは 1 つだけです。
- アクセス リストには少なくとも 1 つの **permit** ステートメントが含まれる必要があります。そうしないと、ネットワークに入るすべてのパケットが拒否されます。
- アクセス リスト条件または一致基準の構成順序は重要です。パケットを転送するかブロックするかを決定するときに、シスコソフトウェアは、それぞれの条件ステートメントに対してステートメントの作成順にパケットをテストします。一致が見つかると、条件ステートメントはそれ以上チェックされません。同じ **permit** ステートメントまたは **deny** ステートメントでも、順序が異なる場合、ある状況では通過し、別の状況では拒否されるパケットが生じる可能性があります。
- アクセス リストを名前によって参照したときに、そのアクセス リストが存在しない場合は、すべてのパケットが通過します。インターフェイスまたはコマンドに空のアクセス リストを適用すると、ネットワークに対するすべてのトラフィックが許可されます。
- 標準のアクセス リストと拡張のアクセス リストの名前は同じにできません。
- パケットが発信インターフェイスにルーティングされる前に、着信アクセス リストがパケットを処理します。ネットワークへのパケット アクセスを拒否するフィルタ条件がある着信アクセス リストは、ルーティング ルックアップ時のオーバーヘッドを削減します。構成されたフィルタ基準に基づいてネットワークへのアクセスを許可されたパケットはルーティング処理されます。インバウンド アクセス リストの場合、**permit** ステートメントを構成するとパケットは受信後に処理され、**deny** ステートメントを構成するとパケットは破棄されます。
- アウトバウンドアクセス リストの場合、パケットの処理後にデバイスから送信されます。着信パケットはアウトバウンドインターフェイスにルーティングされてから、アウトバウ

ンドアクセス リストで処理されます。アウトバウンドアクセス リストの場合、**permit** ステートメントを構成するとパケットは出力バッファに送信され、**deny** ステートメントを構成するとパケットは破棄されます。

- アクセス リストで、デバイスに到達するトラフィック、またはデバイス経由で送信されるトラフィックは制御できますが、デバイスが送信元のトラフィックは制御できません。

ダイヤラリストのアクセスリストルール

次のアクセスリストルールは、Cisco ISR 4000 シリーズ プラットフォームにのみ適用されます。

- シリアルインターフェイス（BRI/PRI）のダイヤラインターフェイスは、出力 ACL を使用してダイヤルアウトします。そのため、ダイヤラリストの ACL 設定は出力 ACL である必要があります。
- ダイヤラのアイドルタイムアウトは、アウトバウンド方向で設定する必要があります。ダイヤラリストの入力 ACL リストを使用したインバウンド ダイヤラ アイドルタイムアウト設定により、セッションがアイドルタイムアウトになります。

IP アクセス リストを作成する際に役立つヒント

意図しない結果を回避し、より効率的で有効なアクセス リストを作成するために役立つヒントを紹介します。

- アクセス リストを作成してから、インターフェイス（または別の対象）に適用します。その理由は、存在しないアクセス リストをインターフェイスに適用してから、アクセス リストを設定すると、最初のステートメントが有効になり、それに続く暗黙的な **deny** ステートメントによってアクセスに緊急の問題が発生するおそれがあるためです。
- アクセス リストを設定してから適用するもう 1 つの理由は、空のアクセス リストが適用されたインターフェイスはすべてのトラフィックを許可するためです。
- すべてのアクセス リストには、少なくとも 1 つの **permit** ステートメントが必要です。permit がないと、すべてのパケットは拒否され、トラフィックはまったく通過しません。
- まだ拒否されていないその他のパケットすべてを許可する場合、ステートメント **permit any any** を使用します。ステートメント **permit any any** を使用すると、実質的に、アクセス リストの末尾にある暗黙的な deny ステートメントでその他すべてのパケットが拒否されることを防ぎます。最初のアクセス リスト エントリは **permit any any** にしないでください。すべてのトラフィックが通過し、以降のテストに到達するパケットがなくなります。**permit any any** を指定すると、まだ拒否されていないすべてのトラフィックが通過します。
- すべてのアクセス リストは暗黙的な **deny** ステートメントで終了しますが、明示的な **deny** ステートメント（たとえば **deny ip any any**）の使用を推奨します。ほとんどのプラットフォームでは、**show access-list** コマンドを発行して拒否されるパケット数を表示し、アクセス リストが許可していないパケットに関する詳細情報を調査できます。明示的な **deny**

ステートメントで拒否されたパケットのみがカウントされます。これは、明示的な **deny** ステートメントによって、より詳細なデータが生成されるためです。

- アクセス リストの作成中、または作成後に、エントリを削除する場合があります。
  - 番号付きアクセスリストからはエントリを削除できません。削除しようとすると、アクセス リスト全体が削除されます。エントリを削除する必要がある場合、アクセス リスト全体を削除してから最初から作り直す必要があります。
  - 名前付きアクセス リストからはエントリを削除できます。**no permit** または **no deny** コマンドを使用すると、適切なエントリが削除されます。
- 個々のステートメントの用途をひと目で確認および理解しやすくするために、**remark** コマンドを使用して、ステートメントの前後に役立つ注記を書き込むことができます。
- 特定のホストまたはネットワークに対するアクセスを拒否し、そのネットワークまたはホストの誰かがアクセスしようとしたかどうかを検出する場合、対応する **deny** ステートメントを指定した **log** キーワードを含めます。それによって、その送信元からの拒否されたパケットがログに記録されます。
- このヒントは、アクセスリストの配置に適用されます。リソースを保存しようとすると、インバウンドアクセスリストでは常にフィルタ条件を適用した後に、ルーティングテーブルの検索を行います。アウトバウンドアクセスリストではフィルタ条件を適用する前に、ルーティング テーブルの検索を行います。

名前付きまたは番号付きアクセス リスト

すべてのアクセス リストは、名前または番号で識別されます。名前付きアクセス リストは、番号付きアクセスリストよりも便利です。タスクを思いだしやすく関連性がある、わかりやすい名前を指定できるためです。名前付きアクセスリストでは、ステートメントの順序を変更したり、ステートメントを追加したりできます。

名前付きアクセスリストは、番号付きアクセスリストではサポートされない次の機能をサポートします。

- IP オプションのフィルタリング
- 非隣接ポート
- TCP フラグ フィルタリング
- **no permit** または **no deny** コマンドによるエントリの削除

（注） 番号付きアクセス リストを受け入れるコマンドの中には、名前付きアクセス リストを受け入れないコマンドがあります。たとえば、vty には番号付きアクセス リストだけを使用します。

標準または拡張アクセス リスト

すべてのアクセス リストは、標準または、拡張アクセス リストのいずれかになります。送信元アドレスでフィルタするだけの場合、より簡易な標準アクセスリストで十分です。送信元アドレス以外のアドレスをフィルタする場合、拡張アクセス リストが必要です。

- 名前付きアクセス リストは、**ip access-list** コマンド構文のキーワード **standard** または **extended** に基づいて標準か拡張かが決まります。
- 番号付きアクセス リストは、**access-list** コマンド構文の番号に基づいて標準か拡張かが決まります。標準 IP アクセス リストには 1 ～ 99 または 1300 ～ 1999 の番号が付けられ、拡張 IP アクセス リストには 100 ～ 199 または 2000 ～ 2699 の番号が付けられます。標準 IP アクセス リストの範囲は、当初は 1 ～ 99 のみでしたが、1300 ～ 1999 の範囲に拡張されました（間の番号は、他のプロトコルに割り当てられました）。拡張アクセスリストの範囲も同様に拡張されました。

（注） Cisco IOS XE 16.9.4 以降、オブジェクトグループベースの番号付き ACL を設定するには、**ip access-list** コマンドを使用します。

標準アクセス リスト

標準アクセス リストは、パケットの送信元アドレスのみをテストします（ただし 2 つの例外があります）。標準アクセスリストは送信元アドレスをテストするため、宛先の近くでトラフィックをブロックする際には効率的です。標準アクセス リストのアドレスが送信元アドレスではない例外が 2 つあります。

- アウトバウンド VTY アクセス リストでは、誰かが Telnet を実行しようとすると、アクセス リスト エントリのアドレスは、送信元アドレスではなく宛先アドレスとして使用されます。
- ルートをフィルタする場合、送信元アドレスではなくアドバタイズされたネットワークがフィルタされます。

拡張アクセス リスト

拡張アクセス リストは、任意の場所のトラフィックをブロックするために適しています。拡張アクセス リストは、送信元アドレス、宛先アドレス、およびその他の IP パケット データをテストします。たとえば、プロトコル、TCP または UDP ポート番号、タイプ オブ サービス（ToS）、優先順位、TCP フラグ、IP オプションなどです。また、拡張アクセス リストには、次のように標準アクセス リストにはない機能があります。

- IP オプションのフィルタリング
- TCP フラグのフィルタリング
- パケットの非初期フラグメントのフィルタリング（「Refining an IP Access List」モジュールを参照してください）

（注） 拡張アクセス リストの対象となるパケットは、自律的に切り替えられません。

アクセスを制御するためにフィルタできる IP パケット フィールド

拡張アクセスリストを使用すると、IPパケットに含まれる次の任意のフィールドについてフィルタできます。送信元アドレスおよび宛先アドレスは、アクセスリストの基礎として最もよく指定される 2 つのフィールドです。

- 送信元アドレス - 特定のネットワーキングデバイスまたはホストから送信されるパケットを制御するために、送信元アドレスを指定します。
- 宛先アドレス - 特定のネットワーキングデバイスまたはホストに対して送信されるパケットを制御するために、宛先アドレスを指定します。
- プロトコル - キーワード **eigrp**、**gre**、**icmp**、**igmp**、**ip**、**ipinip**、**nos**、**ospf**、**tcp**、または **udp** で示される IP プロトコル、あるいは 0 ～ 255 の範囲の整数（インターネット プロトコルを示す）で示されるIPプロトコルを指定します。トランスポート層プロトコル（**icmp**、**igmp**、**tcp**、または **udp**）を指定すると、コマンドは固有の構文になります。
  - ポートおよび非隣接ポート - ポート名またはポート番号で TCP または UDP ポートを指定します。ポート番号に非隣接ポート番号は指定できません。ポート番号は、Telnet トラフィックや HTTP トラフィックなどをフィルタする際に有効です。
  - TCP フラグ - TCP パケットに設定された任意のフラグまたはすべてのフラグにパケットが一致することを指定します。特定のフラグについてフィルタすることで、不正な同期パケットを回避できます。
- IP オプション - IP オプションを指定します。IP オプションに基づいてフィルタする理由の 1 つは、IP オプションを含む偽造パケットでルータが飽和状態にならないようにするためです。

アクセス リストのアドレスに対するワイルドカード マスク

アドレス フィルタリングでは、アクセス リスト エントリ内のアドレス ビットとアクセス リストに送信されるパケットを比較するときに、対応する IP アドレスを確認するか無視するかをソフトウェアに示すために、ワイルドカード マスクを使用します。注意してワイルドカード マスクを設定することで、許可または拒否テストのために 1 つまたは複数の IP アドレスを指定できます。

IP アドレス ビット用のワイルドカード マスクでは、数値 1 と数値 0 を使用して、対応する IP アドレス ビットをどのように扱うかを指定します。1 と 0 は、サブネット（ネットワーク）マスクで意味する内容が対照的なため、ワイルドカード マスクは逆マスクとも呼ばれます。

- ワイルドカード マスク ビット 0 は、対応するビット値を確認することを示します。ビット値は一致する必要があります。

- ワイルドカード マスク ビット 1 は、対応するビット値を無視することを示します。ビット値が一致する必要はありません。

アクセス リスト ステートメントの送信元アドレスまたは宛先アドレスでワイルドカード マスクを指定しない場合、0.0.0.0（すべての値が一致する必要があることを示します）という暗黙的なワイルドカード マスクが想定されます。

サブネットマスクでは、ネットワークとサブネットを示す隣接ビットをマスクにする必要がありますが、それとは異なり、ワイルドカード マスクではマスクに非隣接ビットを使用できます。

次の表に、アクセス リストの IP アドレスおよびマスクと、それに一致すると見なされる対応するアドレスの例を示します。

表 *47 : IP* アドレス、ワイルドカード マスク、および一致する結果の例

アドレス	ワイルドカード マスク	一致する結果
0.0.0.0	255.255.255.255	すべてのアドレスはアクセス リスト条件に一致します
172.18.0.0/16	0.0.255.255	ネットワーク 172.18.0.0
172.18.5.2/16	0.0.0.0	ホスト 172.18.5.2 のみが一致します
172.18.8.0	0.0.0.7	サブネット 172.18.8.0/29 のみが一致します
172.18.8.8	0.0.0.7	サブネット 172.18.8.8/29 のみが一致します
172.18.8.15	0.0.0.3	サブネット 172.18.8.15/30 のみが一致します
10.1.2.0	0.0.252.255（マスクの非隣接ビット）	10.1.2.0 ～ 10.1.254.0 に含まれる偶数のネットワークに一致します

アクセス リストのシーケンス番号

IP アクセス リスト エントリにシーケンス番号を適用する機能によって、アクセス リストの変更が簡易になります。IP アクセス リスト エントリ シーケンス番号機能の前には、アクセス リスト内のエントリの位置を指定する方法はありませんでした。以前は、既存のリストの途中にエントリを挿入する場合、目的の位置の後にあるすべてのエントリを削除してから、新しいエントリを追加し、削除したすべてのエントリを再入力する必要がありました。これは手間がかかり、エラーが起こりやすい方法です。

この新しい機能を使用すると、アクセス リスト エントリにシーケンス番号を追加し、順序を変更することができます。新しいエントリを追加する場合、アクセスリストの目的の位置に挿入されるようにシーケンス番号を指定します。必要に応じて、アクセスリストの現在のエントリを並べ替えて、新しいエントリを挿入できる場所を作成できます。

アクセス リストのロギング

Cisco IOS ソフトウェアには、単一の標準または拡張 IP アクセス リスト エントリで許可または拒否されたパケットに関するロギング メッセージ機能があります。つまり、パケットがエントリに一致する場合は常に、パケットに関する情報を提供するロギング メッセージがコンソールに送信されます。コンソールにロギングするメッセージのレベルは、**logging console** グローバル コンフィギュレーション コマンドで制御します。

アクセス リスト エントリをトリガーする最初のパケットによって、即時にロギング メッセージが作成され、表示またはロギングされるまで、以降のパケットは5分間隔で収集されます。ログ メッセージにはアクセス リスト番号、パケットの許可または拒否に関する状況、パケットの送信元 IP アドレス、および直前の 5 分間に許可または拒否された送信元からのパケット数が示されます。

ただし、**ip access-list log-update** コマンドを使用して、アクセス リストに一致する場合（さらに許可または拒否される場合）に、システムでログ メッセージを生成するパケットの数を設定できます。この手順を実行するのは、5分間隔よりも短い頻度でログ メッセージを受信する場合です。

注意 *number-of-matches* 引数を 1 に設定すると、ログ メッセージはキャッシングされずにただちに送信されます。この場合、アクセス リストに一致するパケットごとにログ メッセージが発生します。大量のログ メッセージでシステムが過負荷になる可能性があるため、1に設定することは推奨されません。

ip access-list log-update コマンドを使用する場合でも、5 分タイマーは有効なままなので、各キャッシュのメッセージ数に関係なく、5 分が経過すると各キャッシュは空になります。ログ メッセージを送信するタイミングに関係なく、しきい値が指定されていない場合と同様に、ログ メッセージのキャッシュは消去され、カウントは 0 にリセットされます。

（注） ロギング メッセージが多すぎて処理できない場合、または1秒以内に処理する必要があるロギング メッセージが複数ある場合、ロギング設備ではロギング メッセージ パケットの一部をドロップすることがあります。この動作によって、ロギングパケットが多すぎてルータがクラッシュすることを回避します。そのため、課金ツールや、アクセスリストと一致する数の正確な情報源としてロギング設備をを使用しないでください。

アクセス リスト ロギングの代替方法

ログ オプションを使用したACL内のエントリのパケット マッチングは代替のプロセスです。ACL でログ オプションを使用することは推奨されません。Null0 の宛先インターフェイスで NetFlowエクスポートおよびマッチングを使用することを推奨します。これはCEFパスで実行されます。Null0 の宛先インターフェイスは、ACL によってドロップされるすべてのパケット用に設定されます。

その他の IP アクセス リスト機能

標準または拡張アクセス リストを作成する基本手順以外に、次のようにアクセス リストを強化できます。これらの各方法の詳細については、「Refining an Access List」モジュールを参照してください。

- 拡張アクセス リストの **permit** ステートメントまたは **deny** ステートメントを有効にする日時を指定し、アクセス リストを細かくし、絶対的または定期的な期間に限定することができます。
- 名前付きアクセス リストの作成後は、エントリを追加したり、エントリの順序を変更したりできます（これはアクセス リストのシーケンス番号再割り当てとも呼ばれます）。
- パケットの非初期フラグメントについてフィルタすることで、パケットをフィルタするときにより細かい精度を達成できます。

RSP3 ポートの関連情報

発信アクセス リストは、RSP3 ではサポートされていません。

アクセス リストを適用する場所

アクセス リストは、デバイスの着信または発信インターフェイスに適用できます。アクセス リストを着信インターフェイスに適用すると、インターフェイスで着信するトラフィックが制御され、アクセス リストを発信インターフェイスに適用すると、インターフェイスから発信されるトラフィックが制御されます。

ソフトウェアは、着信インターフェイスでパケットを受信すると、アクセス リストで設定されているステートメントに対してパケットを検査します。アクセス リストがアドレスを許可している場合は、ソフトウェアはパケットを処理します。着信パケットをフィルタリングするためにアクセス リストを適用すると、フィルタリングされたパケットはデバイスに到達する前に廃棄されるため、デバイスのリソースを節約できます。

発信インターフェイスでは、アクセス リストはインターフェイスから転送（送信）されたパケットをフィルタリングします。発信インターフェイスで Rate-Based Satellite Control Protocol（RBSCP）の TCP アクセス コントロール リスト（ACL）を使用して、発信インターフェイスで TCP 確認応答（ACK）を受けるパケットの種類を制御できます。

debug コマンドを使用してアクセス リストを参照し、デバッグ ログの量を制限できます。たとえば、アクセス リストのフィルタリング基準または一致基準に基づいて、デバッグ ログを送信元または宛先のアドレスまたはプロトコルに制限できます。

アクセス リストを使用して、ルーティング アップデート、ダイヤルオンデマンド（DDR）、および Quality of Service（QoS）機能を制御することができます。

その他の参考資料

関連資料

関連項目	マニュアル タイトル
IP アクセス リスト コマンド：コマンド構文、コマンドモード、コマンド履歴、デフォルト設定、使用に関する注意事項および例	『Cisco IOS IP Addressing Services Command Reference』
送信元アドレス、宛先アドレス、またはプロトコルに基づくフィルタリング	『Creating an IP Access List and Applying It to an Interface』モジュール
IP オプション、TCP フラグ、非隣接ポート、または TTL に基づくフィルタリング	『Creating an IP Access List to Filter IP Options, TCP Flags, or Noncontiguous Ports』モジュール

標準

標準と RFC	タイトル
なし	—

MIB

MIB	MIB のリンク
なし	選択したプラットフォーム、Cisco IOS XE ソフトウェア リリース、およびフィーチャ セットの MIB の場所を検索しダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

シスコのテクニカル サポート

説明	リンク
右の URL にアクセスして、シスコのテクニカル サポートを最大限に活用してください。これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

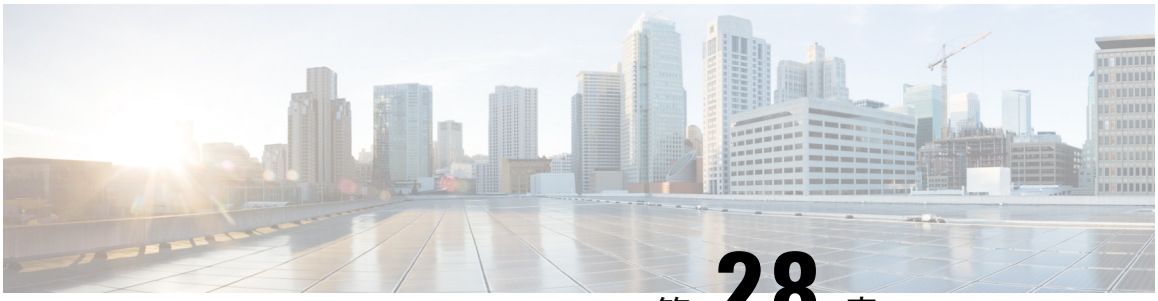
IP アクセス リストに関する機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *48 : IP* アクセス リストに関する機能情報

機能名	リリース	機能の設定情報
ACL - IP プロトコル	Cisco IOS XE リリース 3.16	Cisco IOS XE リリース 3.16 では、Cisco ASR 903 ルータのサポートが追加されました。



第 28 章

IP アクセス リストの作成とインターフェイスへの適用

IP アクセス リストには、ネットワークを保護し、Quality of Service（QoS）係数の設定や **debug** コマンド出力の制限などのセキュリティ以外の目標を達成する際に多数の利点があります。ここでは、標準、拡張、名前付き、および番号付き IP アクセス リストの作成方法について説明します。アクセス リストは、名前または番号で参照できます。標準アクセス リストは、IP パケットの送信元アドレスのみに基づいてフィルタできます。拡張アクセス リストは、IP パケットの送信元アドレス、宛先アドレス、および他のフィールドに基づいてフィルタできます。

アクセス リストの作成後に有効にするには、何かに適用する必要があります。このモジュールでは、アクセス リストをインターフェイスに適用する方法について説明します。ただし、アクセス リストにはその他にも多数の用途があり、このモジュールで言及していますが、他のモジュールでも説明しています。多様なテクノロジーについては、他のコンフィギュレーション ガイドを参照してください。

IP アクセス リストの作成およびインターフェイスへの適用の制限

IPv4 および IPv6 アクセス コントロール リスト（ACL）を設定する場合、次の制限事項が適用されます。

- Application Control Engine（ACE）固有のカウンタは、サポートされていません。
- レイヤ 3 IPv4 および Ipv6 ACL は、同じインターフェイスではサポートされません。

- レイヤ 3 Ipv4 または IPv6 ACL が適用されているイーサネット フローポイント（EFP）またはトランク EFP インターフェイスでは、MAC ACL はサポートされていません。
- IPv4 および IPv6 ACL は、EFP インターフェイスでは現在サポートされていません。IPv4 および IPv6 ACL は、物理インターフェイス、ブリッジ ドメイン インターフェイスおよびポート チャネル インターフェイスでサポートされています。
- レイヤ 4 ポートの範囲と機能は、Ternary Content Addressable Memory（TCAM）に展開されます。IPv4 ACL によって、レイヤ 1K TCAM に制限され、レイヤ 2 ACL スケールは、1K TCAM エントリに制限されます。
- オブジェクトグループ ACL（IPv4 および IPv6 ACL）は、Cisco ISR プラットフォームでサポートされています。
- **any options** コマンドはサポートされていません。
- Cisco IOS XE Cupertino リリース 17.7.1 以降、ACL は、管理インターフェイス Gigabit 0 でサポートされています。

IPアクセスリストの作成とインターフェイスへの適用に関する情報

IP アクセス リストを作成する際に役立つヒント

- アクセスリストを作成してから、インターフェイス（または別の対象）に適用します。その理由は、存在しないアクセス リストをインターフェイスに適用してから、アクセス リストを設定すると、最初のステートメントが有効になり、それに続く暗黙的な **deny** ステートメントによってアクセスに緊急の問題が発生するおそれがあるためです。
- アクセス リストを設定してから適用するもう 1 つの理由は、空のアクセス リストが適用されたインターフェイスはすべてのトラフィックを許可するためです。
- すべてのアクセス リストには、少なくとも 1 つの **permit** ステートメントが必要です。permit がないと、すべてのパケットは拒否され、トラフィックはまったく通過しません。
- ネットワークまたはサブネットのより具体的な参照が、より全般的な参照よりも前に出現するように、アクセス リストを構成します。
- パケットは、ACL の最初の ACE に一致します。したがって、**permit ip any any** はすべてのパケットに一致し、以降の ACE はすべて無視されます。
- すべてのアクセス リストは暗黙的な **deny** ステートメントで終了しますが、明示的な **deny** ステートメント（たとえば **deny ip any any**）の使用を推奨します。ほとんどのプラットフォームでは、**show access-list** コマンドを発行して拒否されるパケット数を表示し、アクセス リストが許可していないパケットに関する詳細情報を調査できます。明示的な **deny**

ステートメントで拒否されたパケットのみがカウントされます。これは、明示的な **deny** ステートメントによって、より詳細なデータが生成されるためです。

- アクセス リストの作成中、または作成後に、エントリを削除する場合があります。名前付きアクセス リストからはエントリを削除できます。**no permit** または **no deny** コマンドを使用すると、適切なエントリが削除されます。
- 個々のステートメントの用途をひと目で確認および理解しやすくするために、**remark** コマンドを使用して、ステートメントの前後に役立つ注記を書き込むことができます。
- 特定のホストまたはネットワークに対するアクセスを拒否し、そのネットワークまたはホストの誰かがアクセスしようとしたかどうかを検出する場合、対応する **deny** ステートメントを指定した **log** キーワードを含めます。それによって、その送信元からの拒否されたパケットがログに記録されます。
- このヒントは、アクセスリストの配置に適用されます。リソースを保存しようとすると、インバウンドアクセスリストでは常にフィルタ条件を適用した後に、ルーティングテーブルの検索を行います。アウトバウンドアクセスリストではフィルタ条件を適用する前に、ルーティング テーブルの検索を行います。

アクセス リストの注釈

任意のIPアクセス リストのエントリについて、コメントまたは注釈を含めることができます。アクセス リストの注釈は、アクセス リスト エントリの前後にあるオプションの注釈です。エントリの内容がわかるので、エントリの目的を解釈する必要はありません。各注釈の長さは 100 文字に制限されます。

コメントは、**permit** ステートメントまたは **deny** ステートメントの前後どちらにでも配置できます。注釈を追加する場所には一貫性があるようにしてください。注釈が関連する **permit** ステートメントや**deny** ステートメントの前にある場合と後にある場合とが混在すると、ユーザーが混乱する可能性があります。

後続の **deny** ステートメントの機能を説明する注釈の例を次に示します。

```
ip access-list extended telnetting
 remark Do not allow host1 subnet to telnet out
 deny tcp host 172.16.2.88 any eq telnet
```

その他の IP アクセス リスト機能

標準または拡張アクセス リストを作成する基本手順以外に、次のようにアクセス リストを強化できます。これらの各方法の詳細については、『*Refining an IP Access List module*』を参照してください。

- 拡張アクセス リストの **permit** ステートメントまたは **deny** ステートメントを有効にする日時を指定し、アクセスリストを細かくし、絶対的または定期的な期間に限定することができます。

- 名前付きまたは番号付きアクセスリストの作成後は、エントリを追加したり、エントリの順序を変更したりできます（これはアクセスリストのシーケンス番号再割り当てとも呼ばれます）。
- パケットの非初期フラグメントについてフィルタすることで、パケットをフィルタするときにより細かい精度を達成できます。

IPアクセス リストの作成とインターフェイスへの適用方法

ここでは、名前または番号を使用して、標準または拡張アクセス リストを作成する一般的な方法について説明します。アクセス リストには高い柔軟性があります。この作業では、単純に1つの **permit** コマンドと 1 つの **deny** コマンドを使用して、それぞれのコマンド構文を指定します。あとは、必要な **permit** および **deny** コマンドの数とその順序を決めるだけです。

（注） このモジュールの最初の 2 つの作業として、1 つのアクセス リストを作成します。適切に機能するように、アクセス リストを適用する必要があります。インターフェイスにアクセス リストを適用する場合は、「インターフェイスへのアクセス リストの適用」タスクを実行します。

送信元アドレスに基づいてフィルタする標準アクセス リストの作成

送信元アドレスのみに基づいてフィルタする場合、簡易な標準アクセス リストで十分です。標準アクセス リストには名前付きと番号付きという 2 種類があります。名前付きアクセス リストを使用すると、番号よりも直感的な名前を使用してアクセス リストを特定できます。また、番号付きアクセス リストよりもサポートする機能が多数です。

送信元アドレスに基づいてフィルタする名前付きアクセス リストの作成

送信元アドレスのみに基づいてフィルタする必要がある場合、標準の名前付きアクセス リストを使用します。この作業では、1 つの **permit** ステートメントと 1 つの **deny** ステートメントを使用しますが、使用する実際のステートメントとその順序は、フィルタまたは許可する内容によって変わります。フィルタリングの目標を達成するように、**permit** および **deny** ステートメントを定義します。

ステップ 1 **enable**

例：

```
Device> enable
```

特権 EXEC モードを有効にします。

- パスワードを入力します（要求された場合）。

ステップ 2 **configure terminal**

例：

```
Device# configure terminal
```

グローバル コンフィギュレーション モードを開始します。

ステップ 3 **ip access-list standard** *name*

例：

```
Device(config)# ip access-list standard R&D
```

名前を使用して標準IPアクセス リストを定義し、標準名前付きアクセス リストのコンフィギュレーション モードを開始します。

ステップ 4 **remark** *remark*

例：

```
Device(config-std-nacl)# remark deny Sales network
```

（任意）アクセス リスト エントリに関してユーザーにわかりやすいコメントを追加します。

- 注釈はアクセス リスト エントリの前または後に指定できます。
- この例の注釈では、後続のエントリがインターフェイスに対するSalesネットワークのアクセスを拒否することをネットワーク管理者に示しています（このアクセス リストは後でインターフェイスに適用される想定です）。

ステップ 5 **deny** {*source* [*source-wildcard*] | **any**} [**log**]

例：

```
Device(config-std-nacl)# deny 172.16.0.0 0.0.255.255 log
```

（任意）送信元アドレスおよびワイルドカード マスクに基づいて、指定した送信元を拒否します。

- *source-wildcard* を省略すると、0.0.0.0 というワイルドカード マスクが想定されます（つまり、すべての送信元アドレスに一致します）。
- 必要に応じて、*source source-wildcard* の代わりに、キーワード **any** を使用して、送信元と 0.0.0.0 255.255.255.255 の送信元ワイルドカードを指定できます。
- この例では、ネットワーク 172.16.0.0 のすべてのホストは、アクセス リストへの合格が拒否されます。
- この例では、送信元アドレスを明示的に拒否し、**log** キーワードを指定しているため、その送信元からのパケットが拒否されるとロギングされます。これは、ネットワークまたはホスト上の誰かがアクセスしようとしたことを通知する方法の 1 つです。

ステップ 6 **remark** *remark*

例：

```
Device(config-std-nacl)# remark Give access to Tester's host
```

（任意）アクセス リスト エントリに関してユーザーにわかりやすいコメントを追加します。

- 注釈はアクセス リスト エントリの前または後に指定できます。
- この注釈は、後続のエントリがインターフェイスに対する Tester のホスト アクセスを許可することをネットワーク管理者に示します。

ステップ 7 **permit** {*source* [*source-wildcard*] | **any**} [**log**]

例：

```
Device(config-std-nacl)# permit 172.18.5.22 0.0.0.0
```

送信元アドレスおよびワイルドカード マスクに基づいて、指定した送信元を許可します。

- 各アクセス リストには、少なくとも 1 つの **permit** ステートメントが必要です。ただし、最初のエントリにする必要はありません。
- *source-wildcard* を省略すると、0.0.0.0 というワイルドカード マスクが想定されます（つまり、すべての送信元アドレスに一致します）。
- 必要に応じて、*source source-wildcard* の代わりに、キーワード **any** を使用して、送信元と 0.0.0.0 255.255.255.255 の送信元ワイルドカードを指定できます。
- この例では、ホスト 172.18.5.22 がアクセス リストに合格できます。

ステップ 8 アクセス リストの基礎とする送信元の指定が完了するまで、ステップ 4 ～ 7 の手順を繰り返します。

明示的に許可されていないすべての送信元は、アクセス リストの末尾にある暗黙的な **deny** ステートメントで拒否されます。

ステップ 9 **end**

例：

```
Device(config-std-nacl)# end
```

標準の名前付きアクセス リスト コンフィギュレーション モードを終了し、特権 EXEC モードを開始します。

ステップ 10 **show ip access-list**

例：

```
Device# show ip access-list
```

（任意）現在の IP アクセス リストすべてのコンテンツが表示されます。

送信元アドレスに基づいてフィルタする番号付きアクセス リストの作成

送信元アドレスのみに基づいてフィルタする必要があり、名前付きアクセス リストを使用しない場合、標準の番号付きアクセス リストを設定します。

IP 標準アクセス リストには、1 ～ 99 または 1300 ～ 1999 の番号を付けます。この作業では、1 つの **permit** ステートメントと 1 つの **deny** ステートメントを使用しますが、使用する実際のステートメントとその順序は、フィルタまたは許可する内容によって変わります。フィルタリングの目標を達成するように、**permit** および **deny** ステートメントを定義します。

ステップ 1 **enable**

例：

```
Device> enable
```

特権 EXEC モードを有効にします。

- パスワードを入力します（要求された場合）。

ステップ 2 **configure terminal**

例：

```
Device# configure terminal
```

グローバル コンフィギュレーション モードを開始します。

ステップ 3 **access-list** *access-list-number permit* {*source* [*source-wildcard*] | **any**} [**log**]

例：

```
Device(config)# access-list 1 permit 172.16.5.22 0.0.0.0
```

送信元アドレスおよびワイルドカード マスクに基づいて、指定した送信元を許可します。

- 各アクセス リストには、少なくとも 1 つの permit ステートメントが必要です。ただし、最初のエントリにする必要はありません。
- 標準 IP アクセス リストには、1 ～ 99 または 1300 ～ 1999 の番号を付けます。
- source-wildcard を省略すると、0.0.0.0 というワイルドカード マスクが想定されます（つまり、すべての送信元アドレスに一致します）。
- 必要に応じて、source source-wildcard の代わりに、キーワード any を使用して、送信元と 0.0.0.0 255.255.255.255 の送信元ワイルドカードを指定できます。
- この例では、ホスト 172.16.5.22 がアクセス リストに合格できます。

ステップ 4 **access-list** *access-list-number* **deny** {*source* [*source-wildcard*] | **any**} [**log**]

例：

```
Device(config)# access-list 1 deny 172.16.7.34 0.0.0.0
```

送信元アドレスおよびワイルドカード マスクに基づいて、指定した送信元を拒否します。

- *source-wildcard* を省略すると、0.0.0.0 というワイルドカード マスクが想定されます（つまり、すべての送信元アドレスに一致します）。
- 必要に応じて、*source source-wildcard* の代わりに、省略形 **any** を使用して、送信元と 0.0.0.0 255.255.255.255 の送信元ワイルドカードを指定できます。
- この例では、ホスト 172.16.7.34 はアクセス リストへの合格が拒否されます。

ステップ 5 アクセス リストの基礎とする送信元の指定が完了するまで、ステップ 3 ～ 6 の手順を繰り返します。

明示的に許可されていないすべての送信元は、アクセス リストの末尾にある暗黙的な **deny** ステートメントで拒否されます。

ステップ 6 **end**

例：

```
Device(config)# end
```

グローバル コンフィギュレーション モードを終了し、特権 EXEC モードを開始します。

ステップ 7 **show ip access-list**

例：

```
Device# show ip access-list
```

（任意）現在の IP アクセス リストすべてのコンテンツが表示されます。

拡張アクセス リストの作成

送信元アドレス以外の要素に基づいてフィルタする場合、拡張アクセス リストを作成する必要があります。拡張アクセス リストには名前付きと番号付きという 2 種類があります。名前付きアクセス リストを使用すると、番号よりも直感的な名前を使用してアクセス リストを特定できます。また、サポートする機能が多数です。

送信元アドレスまたは宛先アドレス以外の要素をフィルタする方法の詳細については、コマンド リファレンス マニュアルの構文の説明を参照してください。

名前付き拡張アクセス リストの作成

送信元アドレス、宛先アドレス、またはアドレスと他の IP フィールドの組み合わせをフィルタする場合、名前付き拡張アクセス リストを作成します。

手順の概要

1. **enable**
2. **configure terminal**
3. **ip access-list extended** *name*
4. **deny** *protocol source* [*source-wildcard*] *destination* [*destination-wildcard*] [**option** *option-name*] [**precedence** *precedence*] [**tos** *tos*] [**established**] [**log** | **log-input**] [**time-range** *time-range-name*] [**fragments**]
5. **permit** *protocol source* [*source-wildcard*] *destination* [*destination-wildcard*] [**option** *option-name*] [**precedence** *precedence*] [**tos** *tos*] [**established**] [**log** | **log-input**] [**time-range** *time-range-name*] [**fragments**]
6. アクセス リストの基礎とするフィールドと値の指定が完了するまで、ステップ 4 ～ 7 の手順を繰り返します。
7. **end**
8. **show ip access-list**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ip access-list extended** *name* 例： `Device(config)# ip access-list extended acl1`	名前を使用して拡張 IP アクセス リストを定義し、拡張名前付きアクセス リストのコンフィギュレーション モードを開始します。
ステップ 4	**deny** *protocol source* [*source-wildcard*] *destination* [*destination-wildcard*] [**option** *option-name*] [**precedence** *precedence*] [**tos** *tos*] [**established**] [**log**	**log-input**] [**time-range** *time-range-name*] [**fragments**] 例： `Device(config-ext-nacl)# deny ip 172.18.0.0 0.0.255.255 host 172.16.40.10 log`	（任意）ステートメントに指定されたすべての条件に一致するすべてのパケットを拒否します。 • *source-wildcard* または *destination-wildcard* を省略すると、0.0.0.0 のワイルドカード マスクが想定されます。つまり、それぞれ送信元アドレスまたは宛先アドレスの全ビットへの一致を意味します。 • 必要に応じて、*source source-wildcard* または *destination destination-wildcard* の代わりに、キーワード **any** を使用して、アドレスと 0.0.0.0 255.255.255.255 の送信元ワイルドカードを指定できます。

	コマンドまたはアクション	目的
		• 必要に応じて、キーワード **host** *source* を使用し、*source* 0.0.0.0 の送信元と送信元ワイルドカードを表示して、省略形 **host** *destination* を使用し、*destination* 0.0.0.0 の宛先と宛先ワイルドカードを表示します。 • この例では、すべての送信元のパケットは、宛先ネットワーク 172.18.0.0 へのアクセスが拒否されます。アクセスリストによって許可または拒否されるパケットに関するロギング メッセージは、**logging facility** コマンドに設定された設備に送信されます（たとえば、コンソール、端末、syslog）。つまり、パケットがアクセス リストに一致する場合は常に、パケットに関する情報を提供するロギング メッセージが設定された設備に送信されます。コンソールにロギングするメッセージのレベルは、**logging console** コマンドで制御します。
ステップ 5	**permit** *protocol source* [*source-wildcard*] *destination* [*destination-wildcard*] [**option** *option-name*] [**precedence** *precedence*] [**tos** *tos*] [**established**] [**log** | **log-input**] [**time-range** *time-range-name*] [**fragments**] 例： `Device(config-ext-nacl)# permit tcp any any`	ステートメントに指定されたすべての条件に一致するすべてのパケットを許可します。 • 各アクセス リストには、少なくとも 1 つの permit ステートメントが必要です。 • *source-wildcard* または *destination-wildcard* を省略すると、0.0.0.0 のワイルドカードマスクが想定されます。つまり、それぞれ送信元アドレスまたは宛先アドレスの全ビットへの一致を意味します。 • 必要に応じて、*source source-wildcard* または *destination destination-wildcard* の代わりに、キーワード **any** を使用して、アドレスと 0.0.0.0 255.255.255.255 の送信元ワイルドカードを指定できます。 • この例では、任意の送信元から任意の宛先への TCP パケットが許可されています。 • **log-input** キーワードを使用して、ロギング出力に入力インターフェイス、送信元 MAC アドレス、または仮想回線を含めます。

	コマンドまたはアクション	目的
ステップ 6	アクセス リストの基礎とするフィールドと値の指定が完了するまで、ステップ 4 ～ 7 の手順を繰り返します。	明示的に許可されていないすべての送信元は、アクセス リストの末尾にある暗黙的な **deny** ステートメントで拒否されます。
ステップ 7	**end** 例： `Device(config-ext-nacl)# end`	標準の名前付きアクセス リスト コンフィギュレーション モードを終了し、特権 EXEC モードを開始します。
ステップ 8	**show ip access-list** 例： `Device# show ip access-list`	（任意）現在の IP アクセス リストすべてのコンテンツが表示されます。

RSP3 ポートの関連情報

ACL は、フラグメント化されたパケットに対してはサポートされていません。

番号付き拡張アクセス リストの作成

送信元アドレス、宛先アドレス、またはアドレスと他の IP フィールドの組み合わせに基づいてフィルタし、名前を使用しない場合、番号付き拡張アクセス リストを作成します。拡張 IP アクセス リストには、100 ～ 199 または 2000 ～ 2699 の番号を付けます。

手順の概要

1. **enable**
2. **configure terminal**
3. **access-list** *access-list-number* **remark** *remark*
4. **access-list** *access-list-number* **permit** *protocol* {*source* [*source-wildcard*] | **any**} {*destination* [*destination-wildcard*] | **any**} [**precedence** *precedence*] [**tos** *tos*] [**established**] [**log** | **log-input**] [**time-range** *time-range-name*] [**fragments**]
5. **access-list** *access-list-number* **remark** *remark*
6. **access-list** *access-list-number* **deny** *protocol* {*source* [*source-wildcard*] | **any**} {*destination* [*destination-wildcard*] | **any**} [**precedence** *precedence*] [**tos** *tos*] [**established**] [**log** | **log-input**] [**time-range** *time-range-name*] [**fragments**]
7. アクセス リストの基礎とするフィールドと値の指定が完了するまで、ステップ 3 ～ 6 の手順を繰り返します。
8. **end**
9. **show ip access-list**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**access-list** *access-list-number* **remark** *remark* 例： `Device(config)# access-list 107 remark allow Telnet packets from any source to network 172.69.0.0 (headquarters)`	（任意）アクセス リスト エントリに関してユーザーにわかりやすいコメントを追加します。 • 最大 100 文字の注釈をアクセス リスト エントリの前または後に指定できます。
ステップ 4	**access-list** *access-list-number* **permit** *protocol* {*source* [*source-wildcard*] | **any**} {*destination* [*destination-wildcard*] | **any**} [**precedence** *precedence*] [**tos** *tos*] [**established**] [**log** | **log-input**] [**time-range** *time-range-name*] [**fragments**] 例： `Device(config)# access-list 107 permit tcp any 172.69.0.0 0.0.255.255 eq telnet`	ステートメントに指定されたすべての条件に一致するすべてのパケットを許可します。 • 各アクセス リストには、少なくとも 1 つの **permit** ステートメントが必要です。ただし、最初のエントリにする必要はありません。 • 拡張 IP アクセス リストには、100 ～ 199 または 2000 ～ 2699 の番号を付けます。 • *source-wildcard* または *destination-wildcard* を省略すると、0.0.0.0 のワイルドカード マスクが想定されます。つまり、それぞれ送信元アドレスまたは宛先アドレスの全ビットへの一致を意味します。 • 必要に応じて、*source source-wildcard* または *destination destination-wildcard* の代わりに、キーワード **any** を使用して、アドレスと 0.0.0.0 255.255.255.255 の送信元ワイルドカードを指定できます。 • TCP と他のプロトコルでは、その他の構文も使用できます。複雑な構文の場合、コマンド リファレンスの **access-list** コマンドを参照してください。

	コマンドまたはアクション	目的
ステップ 5	**access-list** *access-list-number* **remark** *remark* 例： `Device(config)# access-list 107 remark deny all other TCP packets`	（任意）アクセス リスト エントリに関してユーザーにわかりやすいコメントを追加します。 • 最大 100 文字の注釈をアクセス リスト エントリの前または後に指定できます。
ステップ 6	**access-list** *access-list-number* **deny** *protocol* {*source* [*source-wildcard*] | **any**} {*destination* [*destination-wildcard*] | **any**} [**precedence** *precedence*] [**tos** *tos*] [**established**] [**log** | **log-input**] [**time-range** *time-range-name*] [**fragments**] 例： `Device(config)# access-list 107 deny tcp any any`	ステートメントに指定されたすべての条件に一致するすべてのパケットを拒否します。 • *source-wildcard* または *destination-wildcard* を省略すると、0.0.0.0 のワイルドカードマスクが想定されます。つまり、それぞれ送信元アドレスまたは宛先アドレスの全ビットへの一致を意味します。 • 必要に応じて、*source source-wildcard* または *destination destination-wildcard* の代わりに、キーワード **any** を使用して、アドレスと 0.0.0.0 255.255.255.255 の送信元ワイルドカードを指定できます。
ステップ 7	アクセス リストの基礎とするフィールドと値の指定が完了するまで、ステップ 3 ～ 6 の手順を繰り返します。	明示的に許可されていないすべての送信元は、アクセス リストの末尾にある暗黙的な **deny** ステートメントで拒否されます。
ステップ 8	**end** 例： `Device(config)# end`	グローバル コンフィギュレーション モードを終了し、特権 EXEC モードを開始します。
ステップ 9	**show ip access-list** 例： `Device# show ip access-list`	（任意）現在の IP アクセス リストすべてのコンテンツが表示されます。

物理インターフェイスへのアクセスリストの適用

手順の概要

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **ip access-group** {*access-list-number* | *access-list-name*} {**in** | **out**}
5. **ip access-list extended** *acl-name acl-number*

6. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface** *type number* 例：	インターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	**ip access-group** {*access-list-number* | *access-list-name*} {**in** | **out**} 例： `Device(config-if)# ip access-group acl1 in`	指定したアクセス リストをインバウンド インターフェイスに適用します。 • 送信元アドレスをフィルタリングするには、インバウンド インターフェイスにアクセス リストを適用します。
ステップ 5	**ip access-list extended** *acl-name acl-number* 例：	拡張 ACL コンフィギュレーション モードを有効にします。CLI は拡張 ACL コンフィギュレーション モードを開始します。このモードでは、後続のすべてのコマンドが現在の拡張アクセスリストに適用されます。 拡張 ACL コンフィギュレーション モードを有効にします。CLI は拡張 ACL コンフィギュレーション モードを開始します。このモードでは、後続のすべてのコマンドが現在の拡張アクセスリストに適用されます。 • ACL コンフィギュレーション モードから入力されたすべてのコマンドが適用されるアクセスリスト。英字で始まる最大 30 文字の英数字文字列を使用します。 • アクセス リスト コンフィギュレーション モードから入力されたすべてのコマンドが適用されるアクセスリスト。数字の識別子を使用します。拡張アクセスリストでは、有効範囲は 100 ～ 199 です。

	コマンドまたはアクション	目的
ステップ 6	**end** 例： `Device(config-if)# end`	インターフェイス コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

IP アクセスリストの作成と物理インターフェイスへの適用に関する設定例

例：ホスト送信元アドレスでのフィルタリング

次の例では、user1 に属するワークステーションがギガビットイーサネット 0/0/0 へのアクセスを許可され、user2 に属するワークステーションはアクセスを許可されていません。

```
interface gigabitethernet 0/0/0
 ip access-group workstations in
!
ip access-list standard workstations
 remark Permit only user1 workstation through
 permit 172.16.2.88
 remark Do not allow user2 workstation through
 deny 172.16.3.13
```

例：サブネット送信元アドレスでのフィルタリング

次の例では、user1 サブネットは、gigabitethernet インターフェイス 0/0/0 へのアクセスが許可されていませんが、Main サブネットは、アクセスが許可されています。

```
interface gigabitethernet 0/0/0
 ip access-group prevention in
!
ip access-list standard prevention
 remark Do not allow user1 subnet through
 deny 172.22.0.0 0.0.255.255
 remark Allow Main subnet
 permit 172.25.0.0 0.0.255.255
```

例：送信元と宛先のアドレスおよびIPプロトコルでのフィルタリング

次の設定例は、2 つのアクセス リストを持つインターフェイスを示します。一方のリストは発信パケット、もう一方のリストは着信パケットに適用されます。Internet-filter という標準アクセス リストは、送信元アドレスに基づいて発信パケットをフィルタします。インターフェイスから発信が許可されるパケットは、送信元が 172.16.3.4 である必要があります。

marketing-group という拡張アクセス リストは、着信パケットをフィルタします。このアクセス リストは、任意の送信元からネットワーク 172.26.0.0 への Telnet パケットを許可し、その他す

べての TCP パケットを拒否します。また、ICMP パケットはすべて許可します。1024 未満のポート番号を使用する、任意の送信元からネットワーク 172.26.0.0 への UDP パケットは拒否します。最後に、このアクセス リストはその他すべての IP パケットを拒否し、そのエントリによって許可または拒否されるパケットのロギングを実行します。

```
interface gigabitethernet 0/0/0
 ip address 172.20.5.1 255.255.255.0
 ip access-group Internet-filter out
 ip access-group marketing-group in
!
ip access-list standard Internet-filter
 permit 172.16.3.4
ip access-list extended marketing-group
 permit tcp any 172.26.0.0 0.0.255.255 eq telnet
 deny tcp any any
 permit icmp any any
 deny udp any 172.26.0.0 0.0.255.255 lt 1024
 deny ip any any
```

例：番号付きアクセスリストを使用した送信元アドレスでのフィルタリング

次の例では、ネットワーク 10.0.0.0 は、クラス A ネットワークで、2 番目のオクテットでサブネットを指定します。つまり、サブネット マスクは 255.255.0.0 です。ネットワーク 10.0.0.0 アドレスの 3 番目および 4 番目のオクテットで特定のホストを指定します。Cisco IOS XE ソフトウェアは、アクセス リスト 2 を使用して、サブネット 48 上の 1 つのアドレスを受け入れ、そのサブネット上のその他のアドレスはすべて拒否します。最後の行は、その他すべてのネットワーク 10.0.0.0 サブネット上のアドレスを受け入れることを示します。

```
interface gigabitethernet 0/0/0
 ip access-group 2 in
!
access-list 2 permit 10.48.0.3
access-list 2 deny 10.48.0.0  0.0.255.255
access-list 2 permit 10.0.0.0  0.255.255.255
```

例：サブネットへの Telnet アクセスの防止

次の例では、user1 サブネットは、ギガビット イーサネット インターフェイス 0/0/0 から Telnet にアクセスできません。

```
interface gigabitethernet 0/0/0
 ip access-group telnetting out
!
ip access-list extended telnetting
 remark Do not allow user1 subnet to telnet out
 deny tcp 172.20.0.0 0.0.255.255 any eq telnet
 remark Allow Top subnet to telnet out
 permit tcp 172.33.0.0 0.0.255.255 any eq telnet
```

例：ポート番号を使用した TCP および ICMP に基づくフィルタリング

次の例では、acl1 という名前の拡張アクセス リストの最初の行で、1023 よりも大きい宛先ポートを持つ着信 TCP 接続を許可しています。2 行目で、ホスト 172.28.1.2 の Simple Mail Transfer Protocol（SMTP）ポートへの着信 TCP 接続を許可しています。最後の行では、エラー フィードバックのための着信 ICMP メッセージを許可しています。

```
interface gigabitethernet 0/0/0
 ip access-group acl1 in
!
ip access-list extended acl1
 permit tcp any 172.28.0.0 0.0.255.255 gt 1023
 permit tcp any host 172.28.1.2 eq 25
 permit icmp any 172.28.0.0 255.255.255.255
```

例：SMTP 電子メールと確立済み TCP 接続の許可

インターネットに接続されているネットワークがあり、イーサネット上のホストでインターネット上の任意のホストに対して TCP 接続を構成するとします。ただし、専用のメール ホストのメール（SMTP）ポートを除き、IP ホストから gigabitethernet 上のホストに対する TCP 接続を構成できないようにします。

SMTP は、接続の一端では TCP ポート 25、もう一端ではランダムなポート番号を使用します。接続の存続中は、この同じ 2 つのポート番号が使用されます。インターネットから着信するメール パケットは、25 という宛先ポートを持ちます。発信パケットは、ポート番号が予約されています。ルータの背後にあるセキュア システムは、ポート 25 でメール接続を常に受け入れるため、着信および発信サービスを個別に制御できます。発信インターフェイスまたは着信インターフェイスで、アクセス リストを設定できます。

次の例で、gigabitethernet ネットワークはアドレスが 172.18.0.0 の クラス B ネットワークで、メール ホストのアドレスは 172.18.1.2 です。**established** キーワードを使用するのは、TCP プロトコルで確立済み接続を指定する場合のみです。TCP データグラムに ACK または RST ビットが設定されている場合に一致が発生します。これは、パケットが既存の接続に属することを示します。

```
interface gigabitethernet 0/0/0
 ip access-group 102 in
!
access-list 102 permit tcp any 172.18.0.0 0.0.255.255 established
access-list 102 permit tcp any host 172.18.1.2 eq 25
```

例：ポート名に基づくフィルタによる Web へのアクセス回避

次の例では、w1 および w2 ワークステーションは Web アクセスが許可されていません。ネットワーク 172.20.0.0 上のその他のホストは Web アクセスが許可されています。

```
interface gigabitethernet0/0/0
 ip access-group no-web out
!
ip access-list extended no-web
```

```
 remark Do not allow w1 to browse the web
 deny host 172.20.3.85 any eq http
 remark Do not allow w2 to browse the web
 deny host 172.20.3.13 any eq http
 remark Allow others on our network to browse the web
 permit 172.20.0.0 0.0.255.255 any eq http
```

例：送信元アドレスでのフィルタリングおよびパケットのロギング

次の例では、アクセス リスト 1 および 2 を定義します。いずれのリストもロギングが有効です。

```
interface gigabitethernet 0/0/0
 ip address 172.16.1.1 255.0.0.0
 ip access-group 1 in

!
access-list 1 permit 172.25.0.0 0.0.255.255 log
access-list 1 deny 172.30.0.0 0.0.255.255 log
!
access-list 2 permit 172.27.3.4 log
access-list 2 deny 172.17.0.0 0.0.255.255 log
```

インターフェイスが 172.25.7.7 から 10 パケットを受信し、172.17.23.21 から 14 パケットを受信する場合、最初のログは次のようになります。

```
list 1 permit 172.25.7.7 1 packet
list 2 deny 172.17.23.21 1 packet
```

5 分後、コンソールは、次のログを受信します。

```
list 1 permit 172.25.7.7 9 packets
list 2 deny 172.17.23.21 13 packets
```

例：デバッグ出力の制限

次の設定例では、アクセス リストを使用して、**debug** コマンドの出力を制限します。**debug** の出力を制限すると、データ量が絞られ、目的のデータを探しやすくなるため、時間とリソースを節約できます。

```
Device(config)# ip access-list acl1
Device(config-std-nacl)# remark Displays only advertisements for LDP peer in acl1
Device(config-std-nacl)# permit host 10.0.0.44

Device# debug mpls ldp advertisements peer-acl acl1

tagcon: peer 10.0.0.44:0 (pp 0x60E105BC): advertise 172.17.0.33
tagcon: peer 10.0.0.44:0 (pp 0x60E105BC): advertise 172.16.0.31
tagcon: peer 10.0.0.44:0 (pp 0x60E105BC): advertise 172.22.0.33
tagcon: peer 10.0.0.44:0 (pp 0x60E105BC): advertise 192.168.0.1
tagcon: peer 10.0.0.44:0 (pp 0x60E105BC): advertise 192.168.0.3
tagcon: peer 10.0.0.44:0 (pp 0x60E105BC): advertise 192.168.1.33
```

IPアクセスリストの作成とインターフェイスへの適用に関する追加参照資料

関連資料

関連項目	マニュアル タイトル
セキュリティ コマンド	• 『Cisco IOS Security Command Reference: Commands A to C』 • 『Cisco IOS Security Command Reference: Commands D to L』 • 『Cisco IOS Security Command Reference: Commands M to R』 • 『Cisco IOS Security Command Reference: Commands S to Z』
• アクセス リスト エントリの順序 • 日または週の時刻に基づくアクセス リスト エントリ • 非初期フラグメントを使用するパケット	『Refining an IP Access List』
IP オプション、TCP フラグ、または非隣接ポートに基づくフィルタリング	『Creating an IP Access List for Filtering』
ロギング関連のパラメータの制御	『Understanding Access Control List Loggingl』

標準および RFC

標準/RFC	タイトル
この機能によりサポートされる新規または変更された標準や RFC はありません。またこの機能による既存の標準や RFC のサポートに変更はありません。	—

シスコのテクニカル サポート

説明	リンク
右の URL にアクセスして、シスコのテクニカル サポートを最大限に活用してください。これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

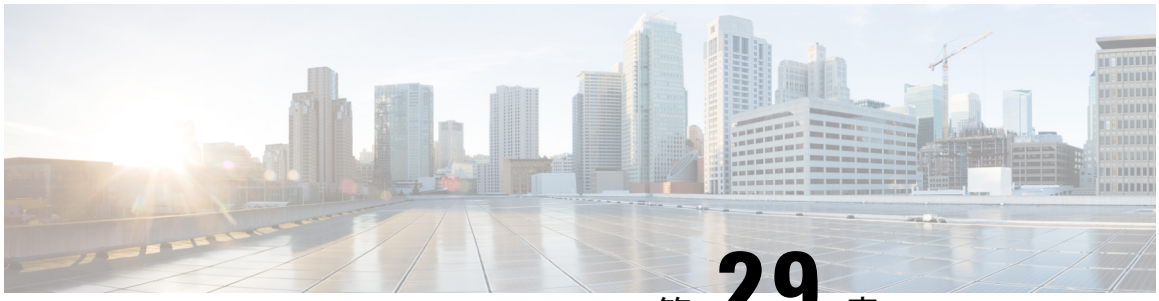
IPアクセス リストの作成とインターフェイスへの適用に関する機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *49 : IP* アクセス リストの作成とインターフェイスへの適用に関する機能情報

機能名	リリース	機能の設定情報
ACL - アクセス コントロール リスト内の送信元アドレスと宛先アドレスの一致	Cisco IOS XE リリース 3.5S	Cisco IOS XE リリース 3.5S では、Cisco ASR 903 ルータのサポートが追加されました。
ACL - ICMP コード	Cisco IOS XE リリース 3.5S	Cisco IOS XE リリース 3.5S では、Cisco ASR 903 ルータのサポートが追加されました。
ACL パフォーマンスの強化	Cisco IOS XE リリース 2.1	この機能は、Cisco ASR 1000 シリーズのアグリゲーション サービス ルータで導入されました。 この機能について導入または変更されたコマンドはありません。



第 29 章

IP オプション、TCP フラグ、非隣接ポート、をフィルタする IP アクセス リストの作成

このモジュールは、特定の IP オプション、TCP フラグ、非隣接ポート、を含む IP パケットをフィルタする IP アクセス リストの使用方法について説明します。

IP オプション、TCP フラグ、非隣接ポートをフィルタする IP アクセス リストの作成に関する前提条件

このモジュールのいずれかのタスクを実行する前に、次のモジュールの情報を把握しておく必要があります。

- 『IP アクセス リストの概要』
- 『IP アクセス リストの作成とインターフェイスへの適用』

IP オプション、TCP フラグ、非隣接ポートをフィルタする IP アクセス リストの作成に関する情報

IP オプション

IP は、サービスを提供するときに、タイプ オブ サービス、存続可能時間、オプション、およびヘッダー チェックサムという 4 つの主要メカニズムを使用します。

オプションは一般的に IP オプションと呼ばれ、一部の状況で必要な制御機能のために用意されていますが、ほとんどの一般的な通信では不要です。IP オプションには、タイム スタンプ、セキュリティ、および特殊なルーティングに関する条件が含まれます。

IP オプションはデータグラムに含まれる場合と含まれない場合があります。IP オプションはすべての IP モジュール（ホストとゲートウェイ）で実装する必要があります。オプションというのは、実装ではなく、任意の指定したデータグラムでの送信を指します。環境によっては、セキュリティ オプションがすべてのデータグラムで必要です。

オプション フィールドは長さが可変です。オプションの個数はゼロ個以上です。IP オプションには、次の 2 つの形式のいずれかを使用できます。

- 形式 1：単一オクテットの option-type
- 形式 2：1 つの option-type オクテット、option-length オクテット、および実際の option-data オクテット

option-length オクテットは、option-type オクテット、option-length オクテット、および option-data オクテットの数をカウントします。

option-type オクテットには、1 ビットのコピー済みフラグ、2 ビットのオプション クラス、および 5 ビットのオプション番号という 3 つのフィールドがあります。これらのフィールドは、オプション タイプ フィールドの 8 ビット値を構成します。IP オプションは、一般的にその 8 ビット値で参照されます。

IP オプションの詳細な一覧と説明については、次の URL の RFC 791『*Internet Protocol*』を参照してください。http://www.faqs.org/rfcs/rfc791.html

IP オプションをフィルタする利点

- ネットワークからの IP オプションを含むパケットをフィルタすることで、ダウンストリームのデバイスとホストにかかるオプション パケットの負荷が軽減されます。
- また、この機能によって、分散型システムでルート プロセッサ（RP）処理が必要な IP オプションを含むパケットについて、RP への負荷が最小限になります。以前は、パケットは常に RP CPU でルーティングまたは処理されていました。パケットをフィルタすることで、パケットの RP への影響を回避できます。

TCP フラグに基づいてフィルタする利点

ACL TCP フラグ フィルタリング機能には、TCP フラグに基づいてフィルタする柔軟なメカニズムが用意されています。以前は、パケットのいずれかの TCP フラグがアクセス コントロールエントリ（ACE）で指定されたフラグに一致する限り、着信パケットは一致していました。すべてのフラグが設定されたパケットがアクセス コントロール リスト（ACL）を通過する可能性があるため、この動作ではセキュリティの抜け穴を考慮しています。ACL TCP フラグ フィルタリング機能では、フィルタするフラグの任意の組み合わせを選択できます。設定されているフラグ、および設定されていないフラグに基づいてマッチングする機能によって、TCP フラグに基づくフィルタリングの制御性が向上するため、セキュリティが強化されます。

TCP パケットは偽造の同期パケットとして送信され、それがリスニング ポートで受け入れられる可能性があるため、ファイアウォールデバイスの管理者は、偽造の TCP パケットをドロップするフィルタリング ルールを設定することを推奨します。

アクセス リストを構成する ACE を設定し、特定のグループの TCP フラグが設定されているパケットのみ、または設定されていないパケットのみを許可することで、不正な TCP パケットを検出およびドロップできます。ACL TCP フラグ フィルタリング機能によって、次のようにパケット フィルタリングの制御性が向上します。

- フィルタする TCP パケットについて、TCP フラグの任意の組み合わせを選択できます。
- 設定されているフラグと設定されていないフラグに基づいてマッチングできるように、ACE を設定できます。

TCP フラグ

次の表は TCP フラグの一覧です。詳細については、RFC 793『*Transmission Control Protocol*』を参照してください。

表 *50 : TCP* フラグ

TCP フラグ	目的
ACK	Acknowledge フラグ：セグメントの acknowledgment フィールドが、このセグメントの送信元が受信を予測している番号の次のシーケンス番号を指定することを示します。
FIN	Finish フラグ：接続をクリアするために使用されます。
PSH	Push フラグ：呼び出しのデータを受信ユーザーに対してただちにプッシュする必要があることを示します。
RST	Reset フラグ：受信者が以降のやり取りなしで接続を削除する必要があることを示します。

TCP フラグ	目的
SYN	Synchronize フラグ：接続の確立に使用されます。
URG	Urgent フラグ：urgent フィールドが重要で、セグメント シーケンス番号に追加する必要があることを示します。

アクセス コントロール エントリ機能での非隣接ポートに関する名前付き ACL サポートを使用する利点

この機能によって、同じ送信元アドレス、宛先アドレス、およびプロトコルに関して複数のエントリを処理するために、アクセス コントロール リストで必要なアクセス コントロール エントリ（ACE）の数が大幅に削減されます。大量の ACE を保守している場合、可能な限り、新しいアクセス リスト エントリを作成するときは、この機能を使用して既存のアクセス リスト エントリのグループを統合します。非隣接ポートを使用するアクセス リスト エントリを設定すると、保守するアクセス リスト エントリ数が少なくなります。

TTL 値のフィルタリング方法

IPは、拡張名前付きおよび番号付きアクセスリストは、インターフェイスを発着信するパケットの TTL 値でフィルタリングできます。有効な TTL 値 0 ～ 255 のパケットを許可または拒否できます（フィルタリング）。その他のフィールド（送信元または宛先アドレスなど）でのフィルタリングと同様に、**ip access-group** コマンドは **in** または **out** を指定します。これにより、アクセスリストの入力または出力が行われ、それぞれ着信または発信パケットに適用されます。TTL 値は、アクセス リスト エントリで指定したプロトコル、アプリケーション、およびその他の設定とともにチェックされ、すべての条件を満たす必要があります。

入力インターフェイスに到達した TTL 値 0 または 1 のパケットに対する特別な処理

分散型シスコ エクスプレス フォワーディング（dCEF）、CEF、ファスト スイッチング、プロセス スイッチングなどのソフトウェア スイッチング パスは、通常、アクセス リスト ステートメントに基づいてパケットを許可または廃棄します。ただし、入力インターフェイスに到達したパケットの TTL 値が 0 または 1 であるときには、特別な処理が必要です。TTL 値が 0 または 1 のパケットは、CEF、dCEF、またはファスト スイッチング パスで入力アクセス リストがチェックされる前に、プロセス レベルに送信されます。入力アクセス リストは、TTL 値が 2 ～ 255 であるパケットに適用され、許可または拒否の決定が行われます。

TTL 値が 0 または 1 のパケットは、デバイスから外部に転送されることがないため、プロセス レベルに送信されます。プロセス レベルでは、各パケットがそのデバイス宛であるかどうか、および Internet Control Message Protocol（ICMP）TTL 値期限切れメッセージを返送する必要があるかどうかをチェックする必要があります。つまり、TTL が 0 または 1 のパケットをドロップする意図で TTL 値 0 または 1 のフィルタリングを設定した ACL が入力インターフェイスで設定されている場合でも、高速なパスではパケットのドロップが発生しないということです。代わりに、プロセスが ACL を適用するときに、プロセス レベルで発生します。これはハード

ウェア スイッチング プラットフォームについてもあてはまります。TTL 値が 0 または 1 のパケットはルート プロセッサ（RP）またはマルチレイヤ スイッチ フィーチャ カード（MSFC）のプロセス レベルに送信されます。

出力インターフェイスでは、TTL 値でのアクセス リスト フィルタリングは、その他のアクセス リスト機能と同じように動作します。チェックはデバイスで有効な最も高速なスイッチング パスで行われます。これは、より高速なスイッチング パスは出力インターフェイスですべての TTL 値（0 ～ 255）を均等に処理するためです。

TTL 値 0 と 1 でフィルタリングするためのコントロール プレーン ポリシング

TTL 値が 0 または 1 のパケットに対する特別な動作によって、デバイスの CPU 使用率が高くなります。0 または 1 の TTL 値 でフィルタリングする場合は、CPU が過負荷になることを防ぐためにコントロール プレーン ポリシング（CPP）を使用してください。CPP を活用するには、TTL 値 0 および 1 をフィルタリングすることに特化したアクセス リストを設定し、CPP を通じてそのアクセス リストを適用する必要があります。このアクセス リストは、その他のインターフェイス アクセス リストとは別のアクセス リストにします。CPP は個々のインターフェイスにおいてではなくシステム全体に対して機能するため、そのようなアクセスリストはデバイス全体に対して 1 つのみ設定する必要があります。このタスクは、セクション「TTL 値 0 と 1 でフィルタリングするコントロールプレーン ポリシングの有効化」で説明しています。

TTL 値に基づいてフィルタする利点

- 存続可能時間（TTL）値でのフィルタリングは、デバイスに到達できるパケット、またはデバイスに到達できないパケットを制御する方法を提供します。ネットワーク レイアウトを確認することで、特定のデバイスからのパケットをホップ数に基づいて許可するか拒否するかを選択できます。たとえば、小規模ネットワークでは、ホップ数が 3 より大きい場所からのパケットを拒否する可能性があります。TTL 値でのフィルタリングでは、トラフィックがネイバーデバイスから発信されたかどうかを検証できます。たとえば特定プロトコルの初期 TTL 値より 1 小さい TTL 値のパケットのみを受け入れることで、1 ホップで自分に到達するパケットのみを受け入れることができます。
- 多くのコントロール プレーン プロトコルはネイバーのみと通信しますが、パケットを誰からも受信します。TTL でフィルタリングするアクセス リストを受信側ルータに適用すると、不要なパケットをブロックできます。
- Cisco ソフトウェアが送信するすべてのパケットは、プロセス レベルに対して TTL 値が 0 または 1 です。デバイスは、Internet Control Message Protocol（ICMP）TTL 値期限切れメッセージを送信元に送信する必要があります。TTL 値が 0 ～ 2 であるパケットをフィルタリングすることで、プロセス レベルでの負荷を削減できます。

IP オプション、TCP フラグ、非隣接ポートをフィルタする IP アクセス リストの作成方法

IP オプションを含むパケットのフィルタリング

アクセス リストを設定して、IP オプションを含むパケットをフィルタし、アクセス リストが適切に設定されていることを確認するには、次の手順を完了します。

（注）
- IP オプションのフィルタリングに関する ACL のサポート機能は、名前付きの拡張 ACL でのみ使用できます。
- この機能を設定する場合、リソース予約プロトコル（RSVP）マルチプロトコル ラベル スイッチング トラフィック エンジニアリング（MPLS TE）、Internet Group Management Protocol バージョン 2（IGMPV2）、および IP オプション パケットを使用するその他のプロトコルは、ドロップまたは無視モードでは機能しない可能性があります。
- ほとんどの Cisco デバイスでは、IP オプションを含むパケットはハードウェアではスイッチされませんが、処理するコントロール プレーン ソフトウェアが必要です（主に、オプションを処理し、IP ヘッダーを書き直す必要があるため）。結果として、IP オプションを含むすべての IP パケットは、ソフトウェアでフィルタとスイッチが行われます。

ステップ 1 **enable**

例：

```
Device> enable
```

特権 EXEC モードを有効にします。

- パスワードを入力します（要求された場合）。

ステップ 2 **configure terminal**

例：

```
Device# configure terminal
```

グローバル コンフィギュレーション モードを開始します。

ステップ 3 **ip access-list extended** *access-list-name*

例：

```
Device(config)# ip access-list extended mylist1
```

名前で IP アクセス リストを指定し、名前付きアクセス リストのコンフィギュレーション モードを開始します。

ステップ 4 [*sequence-number*] **deny** *protocol source source-wildcard destination destination-wildcard* [**option** *option-value*] [**precedence** *precedence*] [**tos** *tos*] [**log**] [**time-range** *time-range-name*] [**fragments**]

例：

```
Device(config-ext-nacl)# deny ip any any option traceroute
```

（任意）名前付き IP アクセス リスト モードで **deny** ステートメントを指定します。

- このアクセス リストでは **deny** ステートメントを最初に使用していますが、必要なステートメントの順序に応じて、**permit** ステートメントが最初に使用される可能性もあります。
- **option** キーワードおよび *option-value* 引数を使用して、特定の IP オプションを含むパケットをフィルタします。
- この例では、traceroute IP オプションを含むすべてのパケットが除外されます。
- エントリを削除するには、このコマンドの **no** *sequence-number* 形式を使用します。

ステップ 5 [*sequence-number*] **permit** *protocol source source-wildcard destination destination-wildcard* [**option** *option-value*] [**precedence** *precedence*] [**tos** *tos*] [**log**] [**time-range** *time-range-name*] [**fragments**]

例：

```
Device(config-ext-nacl)# permit ip any any option security
```

名前付き IP アクセス リスト モードで **permit** ステートメントを指定します。

- この例では、セキュリティ IP オプションを含むすべてのパケット（まだフィルタされていないパケット）が許可されます。
- エントリを削除するには、このコマンドの **no** *sequence-number* 形式を使用します。

ステップ 6 必要に応じて、ステップ 4 またはステップ 5 を繰り返します。

アクセス リストは変更できます。

ステップ 7 **end**

例：

```
Device(config-ext-nacl)# end
```

（任意）名前付きアクセス リスト コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

ステップ 8 **show ip access-lists** *access-list-name*

例：

```
Device# show ip access-lists mylist1
```

（任意）IP アクセス リストの内容を表示します。

次の作業

アクセス リストをインターフェイスに適用するか、アクセス リストを受け入れるコマンドから参照します。

（注） IP オプションを含むすべてのパケットを効率的に除去するには、**ip options drop** グローバル コマンドを設定することを推奨します。

TCP フラグを含むパケットのフィルタリング

この作業では、アクセス リストを設定して、TCP フラグを含むパケットをフィルタし、アクセス リストが適切に設定されていることを確認します。

（注）
- TCP フラグのフィルタリングを使用できるのは、名前付きの拡張 ACL のみです。
- ACL TCP フラグ フィルタリング機能は、Cisco ACL の場合にのみサポートされます。
- 事前に、次のコマンドライン インターフェイス（CLI）形式を使用して、TCP フラグチェック メカニズムを設定できます。

permit tcp any any rst 同じ ACE を示す次の形式を使用できるようになりました。 **permit tcp any any match-any +rst** いずれの CLI 形式も使用できますが、新しいキーワード **match-all** または **match-any** を選択する場合、プレフィックスに「+」または「-」を付けた新しいフラグを次に指定する必要があります。単一の ACL では、古い形式のみ、または新しい形式のみを使用することを推奨します。CLI の古い形式と新しい形式の混在やマッチングを行うことはできません。

注意 新しい構文形式の ACE を持つデバイスを、ACL TCP フラグ フィルタリング機能をサポートしないシスコ ソフトウェアの以前のバージョンでリロードすると、ACE は適用されないため、セキュリティの抜け穴が発生する可能性があります。

ステップ 1 enable

例：

```
Device> enable
```

特権 EXEC モードを有効にします。

- パスワードを入力します（要求された場合）。

ステップ 2 configure terminal

例：

```
Device# configure terminal
```

グローバル コンフィギュレーション モードを開始します。

ステップ 3 **ip access-list extended** *access-list-name*

例：

```
Device(config)# ip access-list extended kmd1
```

名前で IP アクセス リストを指定し、名前付きアクセス リストのコンフィギュレーション モードを開始します。

ステップ 4 [*sequence-number*] **permit tcp** *source source-wildcard* [*operator* [*port*]] *destination destination-wildcard* [*operator* [*port*]] [**established**|{**match-any** | **match-all**} {**+** | **-**} *flag-name*] [**precedence** *precedence*] [**tos** *tos*] [**log**] [**time-range** *time-range-name*] [**fragments**]

例：

```
Device(config-ext-nacl)# permit tcp any any match-any +rst
```

名前付き IP アクセス リスト モードで **permit** ステートメントを指定します。

- このアクセス リストでは **permit** ステートメントを最初に使用していますが、必要なステートメントの順序に応じて、**deny** ステートメントが最初に使用される可能性もあります。
- **permit** コマンドの TCP コマンド構文を使用します。
- RST TCP ヘッダー フラグが設定されたすべてのパケットは一致し、ステップ 3 で名前付きアクセス リスト kmd1 に合格できます。

ステップ 5 [*sequence-number*] **deny tcp** *source source-wildcard* [*operator* [*port*]] *destination destination-wildcard* [*operator* [*port*]] [**established**|{**match-any** | **match-all**} {**+** | **-**} *flag-name*] [**precedence** *precedence*] [**tos** *tos*] [**log**] [**time-range** *time-range-name*] [**fragments**]

例：

```
Device(config-ext-nacl)# deny tcp any any match-all -ack -fin
```

（任意）名前付き IP アクセス リスト モードで **deny** ステートメントを指定します。

- このアクセス リストでは **permit** ステートメントを最初に使用していますが、必要なステートメントの順序に応じて、**deny** ステートメントが最初に使用される可能性もあります。
- **deny** コマンドの TCP コマンド構文を使用します。
- ACK フラグが設定されず、FIN フラグも設定されていないパケットは、ステップ 3 で名前付きアクセス リスト kmd1 に合格しません。
- 上位層プロトコル（ICMP、IGMP、TCP、およびUDP）を許可するその他のコマンド構文については、**deny**（IP）コマンドを参照してください。

ステップ 6 必要に応じてステップ 4 またはステップ 5 を繰り返し、計画したシーケンス番号でステートメントを追加します。エントリを削除するには、**no** *sequence-number* コマンドを使用します。

アクセス リストは変更できます。

ステップ 7 **end**

例：

```
Device(config-ext-nacl)# end
```

（任意）コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

ステップ 8 **show ip access-lists** *access-list-name*

例：

```
Device# show ip access-lists kmd1
```

（任意）IP アクセス リストの内容を表示します。

- 出力を見直して、アクセス リストに新しいエントリが含まれることを確認します。

次の作業

アクセス リストをインターフェイスに適用するか、アクセス リストを受け入れるコマンドから参照します。

非隣接ポートを使用するアクセス コントロール エントリの設定

非隣接 TCP または UDP ポート番号を使用するアクセス リスト エントリを作成するには、次の作業を実行します。この作業では TCP ポートを使用しますが、**permit** および **deny** コマンドの UDP 構文を使用して、非隣接 UDP ポートをフィルタすることもできます。

この作業では **permit** コマンドを最初に使用していますが、フィルタリングの目標に合わせた順序で、**permit** および **deny** コマンドを使用できます。

（注） ACL：アクセス コントロール エントリでの非隣接ポートに関する名前付き ACL サポート機能を使用できるのは、名前付きの拡張 ACL のみです。

ステップ 1 **enable**

例：

```
Device> enable
```

特権 EXEC モードを有効にします。

- パスワードを入力します（要求された場合）。

ステップ 2 **configure terminal**

例：

```
Device# configure terminal
```

グローバル コンフィギュレーション モードを開始します。

ステップ 3 **ip access-list extended** *access-list-name*

例：

```
Device(config)# ip access-list extended acl-extd-1
```

名前で IP アクセス リストを指定し、名前付きアクセス リストのコンフィギュレーション モードを開始します。

ステップ 4 [*sequence-number*] **permit tcp** *source source-wildcard* [*operator port* [*port*]] *destination destination-wildcard* [*operator* [*port*]] [**established** {**match-any** | **match-all**} {**+** | **-**} *flag-name*] [**precedence** *precedence*] [**tos** *tos*] [**log**] [**time-range** *time-range-name*] [**fragments**]

例：

```
Device(config-ext-nacl)# permit tcp any eq telnet ftp any eq 450 679
```

名前付き IP アクセス リスト コンフィギュレーション モードで **permit** ステートメントを指定します。

- 演算子には、**lt**（次の値より小さい）、**gt**（次の値より大きい）、**eq**（次の値に等しい）、**neq**（次の値に等しくない）**range**（次の範囲）があります。
- 演算子が source および source-wildcard 引数の後にある場合、送信元ポートに一致する必要があります。演算子が destination および destination-wildcard 引数の後にある場合、宛先ポートに一致する必要があります。
- **range** 演算子には 2 つのポート番号が必要です。**eq** および **neq** 演算子の後には、最大 10 個のポートを設定できます。他のすべての演算子は 1 つのポート番号が必要です。
- UDP ポートをフィルタするには、このコマンドの UDP 構文を使用します。

ステップ 5 [*sequence-number*] **deny tcp** *source source-wildcard* [*operator port* [*port*]] *destination destination-wildcard* [*operator* [*port*]] [**established** {**match-any** | **match-all**} {**+** | **-**} *flag-name*] [**precedence** *precedence*] [**tos** *tos*] [**log**] [**time-range** *time-range-name*] [**fragments**]

例：

```
Device(config-ext-nacl)# deny tcp any neq 45 565 632 any
```

（任意）名前付きアクセス リスト コンフィギュレーション モードで **deny** ステートメントを指定します。

- 演算子には、**lt**（次の値より小さい）、**gt**（次の値より大きい）、**eq**（次の値に等しい）、**neq**（次の値に等しくない）**range**（次の範囲）があります。
- 演算子が *source* および *source-wildcard* 引数の後にある場合、送信元ポートに一致する必要があります。演算子が *destination* および *destination-wildcard* 引数の後にある場合、宛先ポートに一致する必要があります。

- **range** 演算子には2つのポート番号が必要です。**eq** および **neq** 演算子の後には、最大10個のポートを設定できます。他のすべての演算子は1つのポート番号が必要です。
- UDP ポートをフィルタするには、このコマンドの UDP 構文を使用します。

ステップ6 必要に応じてステップ4またはステップ5を繰り返し、計画したシーケンス番号でステートメントを追加します。エントリを削除するには、**no** *sequence-number* コマンドを使用します。

アクセス リストは変更できます。

ステップ7 **end**

例：

```
Device(config-ext-nacl)# end
```

（任意）名前付きアクセス リスト コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

ステップ8 **show ip access-lists** *access-list-name*

例：

```
Device# show ip access-lists kmd1
```

（任意）アクセス リストの内容を表示します。

非隣接ポートを使用する複数アクセス リスト エントリの1つのアクセス リスト エントリへの統合

非隣接ポートを使用するアクセス リスト エントリ グループを1つのアクセス リスト エントリに統合するには、次の作業を実行します。

この作業では TCP ポートを使用しますが、**permit** および **deny** コマンドの UDP 構文を使用して、非隣接 UDP ポートをフィルタすることもできます。

この作業では **permit** コマンドを最初に使用していますが、フィルタリングの目標に合わせた順序で、**permit** および **deny** コマンドを使用できます。

ステップ1 **enable**

例：

```
Device> enable
```

特権 EXEC モードを有効にします。

- パスワードを入力します（要求された場合）。

ステップ2 **show ip access-lists** *access-list-name*

例：

```
Device# show ip access-lists mylist1
```

（任意）IP アクセス リストの内容を表示します。

- 出力を見直して、アクセス リスト エントリを統合できるかどうかを確認します。

ステップ 3 **configure terminal**

例：

```
Device# configure terminal
```

グローバル コンフィギュレーション モードを開始します。

ステップ 4 **ip access-list extended** *access-list-name*

例：

```
Device(config)# ip access-list extended mylist1
```

名前で IP アクセス リストを指定し、名前付きアクセス リストのコンフィギュレーション モードを開始します。

ステップ 5 **no** [*sequence-number*] **permit** *protocol source source-wildcard destination destination-wildcard*[**option** *option-name*] [**precedence** *precedence*][**tos** *tos*] [**log**] [**time-range** *time-range-name*] [**fragments**]

例：

```
Device(config-ext-nacl)# no 10
```

統合できる重複するアクセス リスト エントリを削除します。

- このステップを繰り返して、ポート番号のみが異なるために統合できるエントリを削除します。
- このステップを繰り返して、たとえばアクセス リスト エントリ 20、30、および 40 を削除した後は、1 つの **permit** ステートメントに統合されるため、これらのエントリは削除されます。
- *sequence-number* が指定された場合、その他のコマンド構文は任意です。

ステップ 6 [*sequence-number*] **permit** *protocol source source-wildcard*[*operator port*[*port*]] *destination destination-wildcard*[*operator port*[*port*]] [**option** *option-name*] [**precedence** *precedence*][**tos** *tos*] [**log**] [**time-range** *time-range-name*] [**fragments**]

例：

```
Device(config-ext-nacl)# permit tcp any neq 45 565 632 any eq 23 45 34 43
```

名前付きアクセス リスト コンフィギュレーション モードで **permit** ステートメントを指定します。

- このインスタンスでは、非隣接ポートを使用するアクセス リスト エントリ グループは、1 つの **permit** ステートメントに統合されました。
- **eq** および **neq** 演算子の後には、最大 10 個のポートを設定できます。

ステップ 7 必要に応じてステップ 5 と 6 を繰り返し、**permit** または **deny** ステートメントを追加して、可能な場合はアクセス リスト エントリを統合します。エントリを削除するには、**no** *sequence-number* コマンドを使用します。

アクセス リストは変更できます。

ステップ 8 **end**

例：

```
Device(config-std-nacl)# end
```

（任意）名前付きアクセス リスト コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

ステップ 9 **show ip access-lists** *access-list-name*

例：

```
Device# show ip access-lists mylist1
```

（任意）アクセス リストの内容を表示します。

次の作業

アクセス リストをインターフェイスに適用するか、アクセス リストを受け入れるコマンドから参照します。

TTL 値に基づいたパケットのフィルタリング

アクセス リストは柔軟性に優れているため、TTL 値に基づいてパケットをフィルタリングする **permit** と **deny** コマンドの組み合わせ 1 つだけでは定義することができません。次のタスクでは、TTL フィルタリングを実行する例を 1 つだけ示します。独自のフィルタリング プランを満たす **permit** と **deny** ステートメントを適切に設定します。

（注） デバイスで使用する Cisco のソフトウェア リリースに応じて、アクセス リストで演算子 EQ または NEQ を指定する場合、アクセス リストでは最大 10 個の TTL 値を指定できます。TTL 値の数は、シスコのソフトウェア リリースによって異なります。

手順の概要

1. **enable**
2. **configure terminal**
3. **ip access-list extended** *access-list-name*
4. [*sequence-number*] **permit** *protocol source source-wildcard destination destination-wildcard*[**option** *option-name*] [**precedence** *precedence*] [**tos** *tos*] [**ttl** *operator value*] [**log**] [**time-range** *time-range-name*] [**fragments**]
5. **permit** または **deny** ステートメントを続けて追加し、必要なフィルタリングを実現します。
6. **exit**
7. **interface** *type number*
8. **ip access-group** *access-list-name* {**in** | **out**}

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ip access-list extended** *access-list-name* 例： `Device(config)# ip access-list extended ttlfilter`	IP アクセス リストを名前で定義します。 • TTL 値でフィルタリングするアクセス リストは、拡張アクセス リストである必要があります。
ステップ 4	[*sequence-number*] **permit** *protocol source source-wildcard destination destination-wildcard*[**option** *option-name*] [**precedence** *precedence*] [**tos** *tos*] [**ttl** *operator value*] [**log**] [**time-range** *time-range-name*] [**fragments**] 例： `Device(config-ext-nacl)# permit ip host 172.16.1.1 any ttl lt 2`	パケットが名前付き IP アクセス リストを通過できる条件を設定します。 • すべてのアクセス リストには、**permit** ステートメントが 1 つ以上必要です。 • この例では、送信元 172.16.1.1 から TTL 値が 2 未満の接続先へのパケットが許可されています。
ステップ 5	**permit** または **deny** ステートメントを続けて追加し、必要なフィルタリングを実現します。	--
ステップ 6	**exit** 例： `Device(config-ext-nacl)# exit`	コンフィギュレーション モードを終了して、コマンドライン インターフェイス（CLI）モード階層で次に高いレベルのモードを開始します。
ステップ 7	**interface** *type number* 例： `Device(config)# interface ethernet 0`	インターフェイス タイプを設定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 8	**ip access-group** *access-list-name* {**in** | **out**} 例： `Device(config-if)# ip access-group ttlfilter in`	アクセス リストをインターフェイスに適用します。

TTL 値 0 と 1 でフィルタリングするコントロール プレーン ポリシングの有効化

TTL 値 0 または 1 に基づいて IP パケットをフィルタリングしたり、CPU の過負荷を防止したりするには、次のタスクを実行します。このタスクでは、TTL 値 0 と 1 で分類用のアクセス リストを設定し、モジュラ QoS コマンドライン インターフェイス（CLI）（MQC）を設定して、ポリシーマップをコントロールプレーンに適用します。アクセスリストを通過するパケットはドロップされます。この特別なアクセス リストは、他のインターフェイス アクセス リストとは異なります。

アクセス リストは柔軟性に優れているため、TTL 値に基づいてパケットをフィルタリングする **permit** と **deny** コマンドの組み合わせ 1 つだけでは定義することができません。次のタスクでは、TTL フィルタリングを実行する例を 1 つだけ示します。独自のフィルタリング プランを満たす **permit** と **deny** ステートメントを適切に設定します。

手順の概要

1. **enable**
2. **configure terminal**
3. **ip access-list extended** *access-list-name*
4. [*sequence-number*] **permit** *protocol source source-wildcard destination destination-wildcard* **ttl** *operator* value
5. **permit** または **deny** ステートメントを続けて追加し、必要なフィルタリングを実現します。
6. **exit**
7. **class-map** *class-map-name* [**match-all** | **match-any**]
8. **match access-group** {*access-group* | **name** *access-group-name*}
9. **exit**
10. **policy-map** *policy-map-name*
11. **class** {*class-name* | **class-default**}
12. **drop**
13. **exit**
14. **exit**
15. **control-plane**
16. **service-policy** {**input** | **output**} *policy-map-name*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。

	コマンドまたはアクション	目的
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ip access-list extended** *access-list-name* 例： `Device(config)# ip access-list extended ttlfilter`	IP アクセス リストを名前で定義します。 • TTL 値でフィルタリングするアクセス リストは、拡張アクセス リストである必要があります。
ステップ 4	[*sequence-number*] **permit** *protocol source source-wildcard destination destination-wildcard* **ttl** *operator* value 例： `Device(config-ext-nacl)# permit ip host 172.16.1.1 any ttl lt 2`	パケットが名前付き IP アクセス リストを通過できる条件を設定します。 • すべてのアクセス リストには、**permit** ステートメントが 1 つ以上必要です。 • この例では、送信元 172.16.1.1 から TTL 値が 2 未満の接続先へのパケットが許可されています。
ステップ 5	**permit** または **deny** ステートメントを続けて追加し、必要なフィルタリングを実現します。	アクセス リストを通過するパケットはドロップされます。
ステップ 6	**exit** 例： `Device(config-ext-nacl)# exit`	コンフィギュレーション モードを終了して、CLI モード階層で次に高いレベルのモードを開始します。
ステップ 7	**class-map** *class-map-name* [**match-all** | **match-any**] 例： `Device(config)# class-map acl-filtering`	指定したクラスへのパケットのマッチングに使用するクラス マップを作成します。
ステップ 8	**match access-group** {*access-group* | **name** *access-group-name*} 例： `Device(config-cmap)# match access-group name ttlfilter`	指定したアクセス コントロール リストに基づいて、クラス マップの一致基準を設定します
ステップ 9	**exit** 例： `Device(config-cmap)# exit`	コンフィギュレーション モードを終了して、CLI モード階層で次に高いレベルのモードを開始します。

	コマンドまたはアクション	目的
ステップ 10	**policy-map** *policy-map-name* 例： `Device(config)# policy-map acl-filter`	1 つ以上のインターフェイスに付加できるポリシーマップを作成または変更し、サービス ポリシーを指定します。
ステップ 11	**class** {*class-name* | **class-default**} 例： `Device(config-pmap)# class acl-filter-class`	作成または変更するポリシーのクラス名を指定するか、ポリシーを指定する前にデフォルト クラス（一般に class-default クラスといいます）を指定します。
ステップ 12	**drop** 例： `Device(config-pmap-c)# drop`	特定のクラスに属するパケットを廃棄するトラフィック クラスを設定します。
ステップ 13	**exit** 例： `Device(config-pmap-c)# exit`	コンフィギュレーション モードを終了して、CLI モード階層で次に高いレベルのモードを開始します。
ステップ 14	**exit** 例： `Device(config-pmap)# exit`	コンフィギュレーション モードを終了して、CLI モード階層で次に高いレベルのモードを開始します。
ステップ 15	**control-plane** 例： `Device(config)# control-plane`	デバイスのコントロール プレーンに関連する属性またはパラメータを関連付けたり、変更したりします。
ステップ 16	**service-policy** {**input** | **output**} *policy-map-name* 例： `Device(config-cp)# service-policy input acl-filter`	集約コントロール プレーン サービスのためにポリシーマップをコントロールプレーンに適用します。

IP オプション、TCP フラグ、非隣接ポートのフィルタリングの設定例

例：IP オプションを含むパケットのフィルタリング

次の例は、アクセス リスト エントリ（ACE）に指定されている IP オプションが含まれる場合にのみ、TCP パケットを許可するように設定された ACE を含む、mylist2 という拡張アクセス リストを示します。

```
ip access-list extended mylist2
 10 permit ip any any option eool
 20 permit ip any any option record-route
 30 permit ip any any option zsu
 40 permit ip any any option mtup
```

一致し、それによって許可されたパケットの数を示すため、**show access-list** コマンドが入力されました。

```
Device# show ip access-list mylist2
Extended IP access list test
10 permit ip any any option eool (1 match)
20 permit ip any any option record-route (1 match)
30 permit ip any any option zsu (1 match)
40 permit ip any any option mtup (1 match)
```

例：TCP フラグを含むパケットのフィルタリング

次のアクセス リストでは、TCP フラグ ACK および SYN が設定され、FIN フラグが設定されていない場合にのみ、TCP パケットを許可します。

```
ip access-list extended aaa
 permit tcp any any match-all +ack +syn -fin
 end
```

show access-list コマンドは、ACL を表示するために入力しました。

```
Device# show access-list aaa

Extended IP access list aaa
 10 permit tcp any any match-all +ack +syn -fin
```

例：非隣接ポートを使用するアクセス リスト エントリの作成

eq および **neq** 演算子の後に最大 10 ポートを入力できるため、次のアクセス リスト エントリを作成できます。

```
ip access-list extended aaa
```

```
 permit tcp any eq telnet ftp any eq 23 45 34
 end
```

show access-lists コマンドを入力して、新しく作成されたアクセス リスト エントリを表示します。

```
Device# show access-lists aaa

Extended IP access list aaa
 10 permit tcp any eq telnet ftp any eq 23 45 34
```

例：既存の複数のアクセス リスト エントリと非隣接ポートを使用する 1 つのアクセス リスト エントリの統合

show access-lists コマンドは、abc というアクセス リストについて、アクセス リスト エントリ グループを表示するために使用されます。

```
Device# show access-lists abc
Extended IP access list abc
 10 permit tcp any eq telnet any eq 450
 20 permit tcp any eq telnet any eq 679
 30 permit tcp any eq ftp any eq 450
 40 permit tcp any eq ftp any eq 679
```

エントリはすべて同じ **permit** ステートメント用であり、ポートのみが異なるため、1 つの新しいアクセス リスト エントリに統合できます。次の例では、重複するアクセス リスト エントリを削除し、以前に表示されていたアクセス リスト エントリ グループを統合する新しいアクセス リスト エントリを作成します。

```
ip access-list extended abc
 no 10
 no 20
 no 30
 no 40
 permit tcp any eq telnet ftp any eq 450 679
 end
```

show access-lists コマンドを再入力すると、統合されたアクセス リスト エントリが表示されます。

```
Device# show access-lists abc
Extended IP access list abc
 10 permit tcp any eq telnet ftp any eq 450 679
```

例：TTL 値のフィルタリング

次のアクセス リストは、存続可能時間（TTL）の値が 10 と 20 でタイプ オブ サービス（ToS）レベルが 3 の IP パケットをフィルタリングします。また、TTL が 154 を超える IP パケットをフィルタリングし、その規則を先頭以外のフラグメントにも適用します。フラッシュの優先レベルと 1 以外の TTL 値を持つ IP パケットを許可し、そのようなパケットのログ メッセージをコンソールに送信します。他のすべてのパケットは拒否されます。

```
ip access-list extended incomingfilter
 deny ip any any tos 3 ttl eq 10 20
 deny ip any any ttl gt 154 fragments
 permit ip any any precedence flash ttl neq 1 log
!
interface ethernet 0

ip access-group incomingfilter in
```

例：TTL 値 0 と 1 でフィルタリングするコントロール プレーン ポリシング

次の例では、acl-filter と呼ばれるポリシー マップで使用するために、acl-filter-class と呼ばれるトラフィック クラスを設定します。アクセス リストは、存続可能時間（TTL）値が 0 または 1 の送信元からの IP パケットを許可します。アクセス リストに一致するパケットがドロップされます。ポリシー マップはコントロール プレーンに結合されます。

```
ip access-list extended ttlfilter

 permit ip any any ttl eq 0 1

class-map acl-filter-class

 match access-group name ttlfilter

policy-map acl-filter

 class acl-filter-class

 drop

control-plane

 service-policy input acl-filter
```

その他の参考資料

関連資料

関連項目	マニュアル タイトル
セキュリティ コマンド	『*Cisco IOS Security Command Reference*』
no ip optionsコマンドを使用した、IP オプションを含むパケットをドロップまたは無視するためのデバイスの設定。	*ACL IP* オプションの選択的ドロップ

関連項目	マニュアル タイトル
アクセス リストに関する概要情報	*IP* アクセス リストの概要
IP アクセス リストの作成とインターフェイスへの適用に関する情報	*IP* アクセス リストの作成とインターフェイスへの適用
QoS コマンド	『*Cisco IOS Quality of Service Solutions Command Reference*』

RFC

RFC	タイトル
RFC 791	*Internet Protocol*（インターネット プロトコル） http://www.faqs.org/rfcs/rfc791.html
RFC 793	伝送制御プロトコル（*TCP*）
RFC 1393	『*Traceroute Using an IP Option*』

シスコのテクニカル サポート

説明	リンク
右の URL にアクセスして、シスコのテクニカル サポートを最大限に活用してください。これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

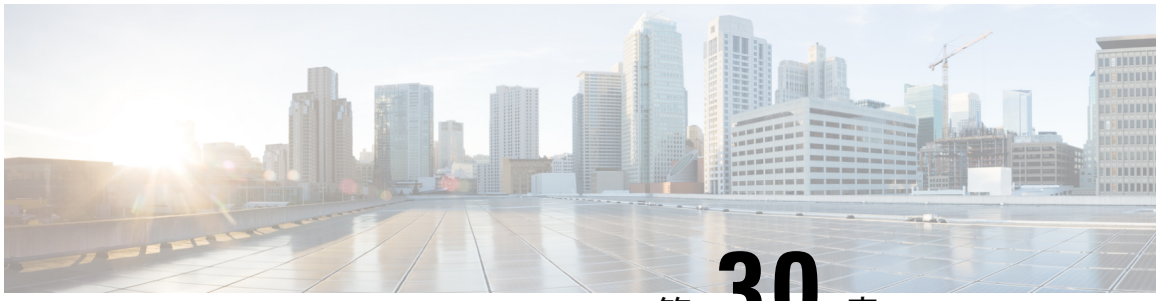
フィルタするための IP アクセス リストの作成に関する機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *51* : フィルタするための *IP* アクセス リストの作成に関する機能情報

機能名	リリース	機能の設定情報
ACL -- アクセス コントロールエントリでの非隣接ポートに関する名前付き ACL サポート	12.3(7)T 12.2(25)S	この機能を使用すると、1 つのアクセス コントロール エントリで非隣接ポートを指定できるため、複数のエントリが同じ送信元アドレス、宛先アドレス、およびプロトコルを持ち、ポートのみが異なる場合に、アクセス コントロール リストで必要なエントリ数を大幅に減らすことができます。
IP オプションのフィルタリングに関する ACL のサポート	12.3(4)T 12.2(25)S 15.2(2)S 15.4(1)S	この機能を使用すると、IP オプションを含むパケットをフィルタできます。その結果、ルータが偽造パケットで飽和状態にならないように防ぎます。 Cisco IOS リリース 15.4(1)S では、Cisco ASR 901S ルータのサポートが追加されました。
ACL TCP フラグ フィルタリング	12.3(4)T 12.2(25)S	この機能は、TCP フラグに基づくフィルタリングに柔軟なメカニズムを提供します。Cisco IOS リリース 12.3(4)T 以前は、パケット内のいずれかの TCP フラグがアクセス コントロール エントリ（ACE）で指定されたフラグに一致する限り、着信パケットは一致していました。すべてのフラグが設定されたパケットがアクセスコントロールリスト（ACL）を通過する可能性があるため、この動作ではセキュリティの抜け穴を考慮しています。ACL TCP フラグ フィルタリング機能では、フィルタするフラグの任意の組み合わせを選択できます。設定されているフラグ、および設定されていないフラグに基づいてマッチングする機能によって、TCP フラグに基づくフィルタリングの制御性が向上するため、セキュリティが強化されます。



第 30 章

FQDN ACL の設定

このドキュメントでは、完全修飾ドメイン名（FQDN）を使用したアクセスコントロールリスト（ACL）を設定する方法について説明します。FQDN ACL 機能を設定することによって、ドメイン名システム（DNS）に基づいて、ワイヤレスセッションに ACL を設定および適用することができます。ドメイン名を IP アドレスに解決されます。IP アドレスは、DNS 応答の一部としてクライアントに提供され、FQDN は、IP アドレスに基づいて、ACL にマッピングされます。

FQDN ACL の設定に関する制約事項

FQDN ACL 機能の設定は、IPv4 ワイヤレス セッションでのみサポートされます。

FQDN ACL の設定に関する情報

FQDN ACL の設定

アクセスコントロールリスト（ACL）が、完全修飾ドメイン名（FQDN）を使用して設定されている場合、宛先ドメイン名に基づいて ACL を適用できます。宛先のドメイン名はその後、DNS 応答の一部としてクライアントに提供される IP アドレスに解決されます。

ゲスト ユーザーは、FQDN ACL 名で構成されるパラメータ マップでネットワーク認証を使用してログインできます。

FQDN ACL を設定する前に、次の作業を実行してください。

- IP アクセス リストを設定します。
- IP ドメイン名のリストを設定します。
- ドメイン名と FQDN ACL をマッピングします。

コントローラに **fqdn-acl-name** AAA 属性を送信するように RADIUS サーバーを設定して、アクセス リストを特定のドメインに適用できます。オペレーティング システムは、パススルー ドメイン リストとそのマッピングを確認し、FQDN を許可します。FQDN ACL により、クライアントは認証なしで設定されたドメインのみにアクセスできます。

（注） デフォルトでは、IPアクセスリスト名は、パススルー ドメイン名と同じ名前で設定されます。デフォルト名を上書きするために、グローバル コンフィギュレーション モードで**access-session passthrou-access-group** *access-group-name* **passthrou-domain-list** *domain-list-name* コマンドを使用できます。

FQDN ACL の設定方法

IP アクセス リストの設定

手順の概要

1. **ip access-list extended** *name*
2. **permit ip any any**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**ip access-list extended** *name* 例： `Device (config)# ip access-list extended ABC`	IP アクセス リストを作成します。
ステップ 2	**permit ip any any** 例： `Device (config-ext-nacl)# permit ip any any`	ワイヤレス クライアントに許可されるドメインを指定します。ドメインはドメイン名リストで指定されます。

ドメイン名リストの設定

アクセス ポイントによる DNS スヌーピングが許可されたドメイン名のリストを含むドメイン名リストを設定できます。DNS ドメイン リスト名の文字列は、拡張アクセス リスト名と一致している必要があります。

手順の概要

1. **passthrou-domain-list** *name*
2. **match** *word*

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	**passthrou-domain-list** *name*
	例：
	`Device (config)# passthrou-domain-list abc`
	`Device (config-fqdn-acl-domains)#`
		パススルー ドメイン名リストを設定します。

ステップ 2	**match** *word*
	例：
	`Device (config-fqdn-acl-domains)# match play.google.com`
	`Device (config-fqdn-acl-domains)# match www.yahoo.com`
		パススルー ドメイン リストを設定します。クライアントがRADIUSサーバーを介して認証される必要なくアクセスの照会が許可されるWebサイトのリストを追加します。

ドメイン名と FQDN ACL のマッピング

手順の概要

1. **access-session passthrou-access-group** *access-group-name* **passthrou-domain-list** *domain-list-name*
2. **parameter-map type webauth** *domain-list-name* and **login-auth-bypass fqdn-acl-name** *acl-name* **domain-name** *domain-name*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**access-session passthrou-access-group** *access-group-name* **passthrou-domain-list** *domain-list-name* 例： `Device (config)# access-session passthrou-access-group abc passthrou-domain-list abc`	ドメイン名リストと FQDN ACL AAA 属性名をマッピングします。中央Web認証を設定する場合、このコマンドを使用します。
ステップ 2	**parameter-map type webauth** *domain-list-name* and **login-auth-bypass fqdn-acl-name** *acl-name* **domain-name** *domain-name* 例： `Device (config)# parameter-map type webauth abc SwitchControllerDevice`	ドメイン名リストと FQDN ACL 名をマッピングします。コントローラでローカル認証を設定する場合、このコマンドを使用します。 RADIUSサーバーは、認証されたユーザープロファイルの一部として FQDN ACL 名を返すように設定

	コマンドまたはアクション	目的
	`(config-params-parameter-map)# login-auth-bypass fqdn-acl-name abc domain-name abc`	できます。FQDN ACL がコントローラで定義される場合、コントローラは FQDN ACL をユーザーに動的に適用します。

FQDN ACL のモニタリング

次のコマンドを使用して FQDN ACL をモニターできます。

コマンド	目的
show access-session interface *interface-name* **details**	インターフェイスに設定された FQDN ACL 情報を表示します。
show access-session fqdn fqdn-maps	ドメイン名リストにマッピングされた FQDN ACL を表示します。
show access-session fqdn list-domain *domain-name*	ドメイン名を表示します。
show access-session fqdn passthru-domain-list	設定されているドメインを表示します。

FQDN ACL の設定例

例：FQDN ACL の設定

次に、IP アクセス リストを作成する例を示します。

```
# config terminal
(config)# ip access-list extended abc
(config-ext-nacl)# permit ip any any
(config-ext-nacl)# end
# show ip access-list abc
```

次に、ドメイン名のリストを設定する例を示します。

```
# config terminal
(config)# passthrou-domain-list abc
(config-fqdn-acl-domains)# match play.google.com
(config-fqdn-acl-domains)# end
# show access-session fqdn fqdn-maps
```

次に、中央集中型 Web 認証を使用してドメイン名と FQDN ACL をマッピングする例を示します。

```
# config terminal
```

```
(config)# access-session passthrou-access-group abc passthrou-domain-list abc
(config)# end
# show access-session interface vlan 20
```

次に、ローカル認証を使用してドメイン名と FQDN ACL をマッピングする例を示します。

```
# config terminal
(config)# parameter-map type webauth abc
(config-params-parameter-map)# login-auth-bypass fqdn-acl-name abc domain-name abc
(config-params-parameter-map)# end
# show access-session fqdn fqdn-maps
```

FQDN ACL の設定に関するその他の参考資料

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『Cisco IOS Master Command List, All Releases』
セキュリティ コマンド	• 『Cisco IOS Security Command Reference: Commands A to C』[英語] • 『Cisco IOS Security Command Reference: Commands D to L』[英語] • 『Cisco IOS Security Command Reference: Commands M to R』[英語] • 『Cisco IOS Security Command Reference: Commands S to Z』[英語]
ACL 設定ガイド	『セキュリティコンフィギュレーションガイド』の「アクセスコントロールリスト」

シスコのテクニカル サポート

説明	リンク
右の URL にアクセスして、シスコのテクニカル サポートを最大限に活用してください。これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

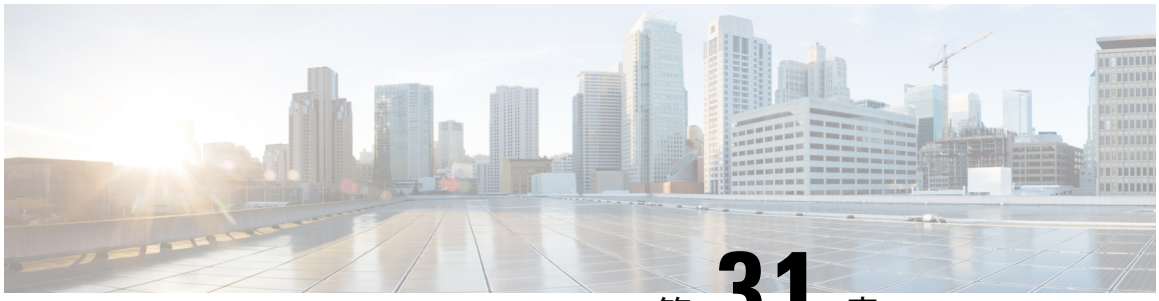
FQDN ACL の設定に関する機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *52 : FQDN ACL* の設定に関する機能情報

機能名	リリース	機能情報
FQDN ACL の設定		FQDN ACL 機能を設定することで、ドメイン名システム（DNS）に基づいてワイヤレス セッションにアクセス コントロール リスト（ACL）を設定、適用することができます。ドメイン名が IP アドレスが DNS 応答の一部として、クライアントに割り当てるられる IP アドレスに解決されます。次に FQDN が IP アドレスに基づいて ACL にマッピングされます。 次のコマンドが導入または変更されました。**access session passthrou access group**、**login-auth-bypass**、**parameter-map type webauth global**、 **pass throu domain list name**、**show access-session fqdn**



第 31 章

IP アクセス リストの精緻化

アクセス リストを作成している間、または作成した後に、アクセス リストを精緻化するにはいくつかの方法があります。アクセス リストのエントリの順序を変更したり、アクセス リストにエントリを追加したりできます。また、アクセス リスト エントリを日または週の特定の時間帯に制限したり、パケットの非初期フラグメントをフィルタリングすることでパケットをフィルタリングするときにより細かく設定することができます。

IP アクセス リストの精緻化に関する情報

アクセス リストのシーケンス番号

IP アクセス リスト エントリにシーケンス番号を適用する機能によって、アクセス リストの変更が簡易になります。IP アクセス リスト エントリ シーケンス番号機能の前には、アクセス リスト内のエントリの位置を指定する方法はありませんでした。以前は、既存のリストの途中にエントリを挿入する場合、目的の位置の後にあるすべてのエントリを削除してから、新しいエントリを追加し、削除したすべてのエントリを再入力する必要がありました。これは手間がかかり、エラーが起こりやすい方法です。

シーケンス番号を使用して、ユーザーはアクセス リスト エントリを追加し、それを並べ替えることができるようになりました。新しいエントリを追加する場合、アクセスリストの目的の位置に挿入されるようにシーケンス番号を指定します。必要に応じて、アクセスリストの現在のエントリを並べ替えて、新しいエントリを挿入できる場所を作成できます。

アクセス リスト シーケンス番号の利点

アクセス リスト シーケンス番号は、アクセス リストで **permit** または **deny** コマンドを開始する番号です。シーケンス番号により、エントリがアクセス リストに表示される順序が決定されます。IP アクセス リスト エントリにシーケンス番号を適用する機能によって、アクセス リストの変更が簡易になります。

シーケンス番号を設定する前に、アクセス リストの末尾にアクセス リスト エントリを追加できるため、アクセス リスト全体の再設定が必要になるリストの末尾以外の位置では、ステートメントの追加が必要になります。アクセス リスト内でのエントリの位置を指定する方法はありません。以前は、既存のリストの途中にエントリ（ステートメント）を挿入する場合、目的の位置の後にあるすべてのエントリを削除してから、新しいエントリを追加し、削除したすべてのエントリを再入力する必要がありました。これは手間がかかり、エラーが起こりやすい方法です。

この新しい機能を使用すると、アクセス リスト エントリにシーケンス番号を追加し、順序を変更することができます。新しいエントリを追加するとき、アクセス リストの目的の位置に配置されるように、シーケンス番号を選択します。必要に応じて、アクセス リストの現在のエントリを並べ替えて、新しいエントリを挿入できる場所を作成できます。シーケンス番号により、アクセス リストの変更を簡単に実行できるようになりました。

シーケンス番号の動作

- 以前のリリースとの下位互換性を保つため、シーケンス番号のないエントリが適用された場合には、最初のエントリにはシーケンス番号 10 が割り当てられます。連続してエントリを追加すると、シーケンス番号は10ずつ増分されます。最大シーケンス番号は2147483647です。生成したシーケンス番号がこの最大値を超えると、次のメッセージが表示されます。

```
Exceeded maximum sequence number.
```

- シーケンス番号のないエントリを入力すると、アクセス リストの最後のシーケンス番号に 10 を加えたシーケンス番号が割り当てられ、リストの末尾に配置されます。
- （シーケンス番号以外が）既存のエントリに一致するエントリを入力すると、何も変更されません。
- 既存のシーケンス番号を入力すると、次のエラー メッセージが表示されます。

```
Duplicate sequence number.
```

- グローバル コンフィギュレーション モードで新しいアクセス リストを入力すると、そのアクセス リストのシーケンス番号が自動的に生成されます。
- シーケンス番号が不揮発性生成（NVGEN）されることはありません。つまり、シーケンス番号自体は保存されません。システムのリロード時には、設定されたシーケンス番号はデフォルトのシーケンス開始番号と増分に戻されます。この機能は、シーケンス番号をサポートしないソフトウェア リリースとの下位互換性を保つために提供されています。

- この機能は、名前付きおよび番号付きの標準および拡張IPアクセス リストと連動します。

時間範囲の利点

時間範囲の利点および可能な使用法として、次のことが挙げられます。

- ネットワーク管理者は、リソースへのユーザーアクセスの許可または拒否の制御をより強化できます。これらのリソースとして、アプリケーション（IPアドレス/マスク ペアとポート番号によって特定されます）、ポリシールーティング、またはオンデマンドリンク（ダイヤラへの関連トラフィックとして認識されます）があります。
- ネットワーク管理者は、次に示すような、時刻ベースのセキュリティ ポリシーを設定できます。
  - アクセス リストを使用した境界セキュリティ
  - IP セキュリティ プロトコル（IPsec）を使用したデータの機密性保持
- プロバイダーのアクセス レートが一日の時間帯によって異なるときは、トラフィックは自動的にコスト効率よく再ルーティングすることが可能です。
- ネットワーク管理者は、ロギング メッセージを制御できます。アクセス リスト エントリは、一日の特定の時間帯にトラフィックをロギングすることはできますが、常にロギングすることはできません。したがって、管理者はピーク時間中に生成された多くのログを分析することなく、単にアクセスを拒否できます。

パケットの非初期フラグメントをフィルタリングする利点

パケットの初期フラグメントにとどまらず、より多くのトラフィックをブロックするには、拡張アクセス リストを使用してパケットの非初期フラグメントをフィルタリングします。まず、次の概念を理解しておく必要があります。

フラグメントを拒否する追加の IP アクセス リスト エントリで **fragments** キーワードが使用されている場合、フラグメント制御機能を使用すると、次のような利点があります。

追加のセキュリティ

パケットの初期フラグメントにとどまらず、より多くのトラフィックをブロックできます。不要なフラグメントは、受信側にリアセンブリ タイムアウトになるまで残りません。これは、このようなフラグメントは受信側に送信される前にブロックされるためです。不要なトラフィックを大量にブロックすることで、セキュリティが高まり、ハッカーから攻撃を受けるリスクが軽減されます。

コスト削減

パケットの不要な非初期フラグメントをブロックすると、ブロックしたいトラフィックに注意を払う必要がなくなります。

使用ストレージの削減

パケットの不要な非初期フラグメントが受信側に届かないようにブロックすることで、宛先はリアセンブリ タイムアウトになるまでフラグメントを保存する必要がなくなります。

予期される動作

非初期フラグメントは、初期フラグメントと同様に扱われます。予期されないポリシー ルーティング結果や、ルーティングされるべきでないパケットのフラグメントが生じる可能性も低くなります。

フラグメントのアクセス リスト処理

fragments キーワードを指定するかどうかによるアクセス リスト エントリの動作は、次のようにまとめることができます。

アクセス リスト エントリの状態...	結果

...**fragments** キーワードが指定されず（デフォルト）、すべてのアクセス リスト エントリ情報が一致する	レイヤ 3 情報のみを含むアクセス リスト エントリの場合：
	• エントリは、非フラグメント パケット、先頭フラグメント、先頭以外のフラグメントに適用されます。
	
	レイヤ 3 およびレイヤ 4 情報を含むアクセス リスト エントリの場合：
	• エントリは、非フラグメント パケットと先頭フラグメントに適用されます。
	  • エントリが **permit** ステートメントであると、パケットまたはフラグメントは許可されます。
	  • エントリが **deny** ステートメントであると、パケットまたはフラグメントは拒否されます。
	• エントリは、次の方法で先頭以外のフラグメントにも適用されます。非初期フラグメントにはレイヤ 3 情報のみが含まれているため、アクセス リスト エントリのレイヤ 3 の部分のみが適用されます。アクセス リスト エントリのレイヤ 3 の部分が一致し、
	  • エントリが **permit** ステートメントであると、非初期フラグメントは許可されます。
	  • エントリが **deny** ステートメントであると、次のアクセス リスト エントリが処理されます。
	
	（注） 非初期フラグメントと、非フラグメントまたは初期フラグメントの場合では、**deny** ステートメントの処理方法は異なります。

アクセス リスト エントリの状態...	結果
...**fragments** キーワードが指定され、すべてのアクセス リストエントリ情報が一致する	アクセス リスト エントリは、非初期フラグメントにのみ適用されます。 レイヤ 4 情報を含むアクセス リスト エントリに **fragments** キーワードは設定できません。

すべてのアクセス リスト エントリに **fragments** キーワードを追加することはできません。IP パケットの最初のフラグメントは非フラグメントとして見なされ、以降のフラグメントとは独立して扱われるためです。初期フラグメントは、アクセスリストの **fragments** キーワードが設定された **permit** または **deny** エントリとは一致しません。パケットは、**fragments** キーワードが設定されていないアクセス リスト エントリによって許可または拒否されるまで、次のアクセス リスト エントリと比較されます。したがって、**deny** エントリごとに、2 つのアクセス リスト エントリが必要になる場合があります。ペアの最初の **deny** エントリには **fragments** キーワードは含まれず、初期フラグメントに適用されます。ペアの 2 番目の **deny** エントリには **fragments** キーワードは含まれ、以降のフラグメントに適用されます。同じホストに複数の **deny** エントリがあり、レイヤ 4 ポートが異なる場合は、そのホストで **fragments** キーワードが設定された 1 つの **deny** アクセス リスト エントリを追加する必要があります。このように、パケットのすべてのフラグメントは、アクセス リストによって同様に扱われます。

IP データグラムのパケット フラグメントは個々のパケットと見なされ、それぞれ、アクセス リスト アカウンティングとアクセス リストの違反カウントの 1 つのパケットとして個別にカウントされます。

IP アクセス リストを精緻化する方法

このモジュールで説明する作業では、アクセスリストを精緻化するためのさまざまな方法を示します（アクセスリストを作成するときに精緻化しなかった場合に利用できます）。アクセス リスト エントリの順序変更、アクセス リストへのエントリの追加、日または週の特定の時間帯でのアクセス リスト エントリの制限などを実行できます。また、パケットの非初期フラグメントをフィルタリングすることでパケットをフィルタリングするときにより細かく設定することができます。

シーケンス番号を使用したアクセス リストの変更

既存のアクセスリストへのエントリの追加、エントリの順序変更、または（将来の変更に対応するための）アクセス リストのエントリの番号付けを行うには、次の手順を実行します。

（注） アクセス リストからエントリを削除する場合は、コマンドの **no deny** または **no permit** 形式を使用するか、あるいはステートメントにシーケンス番号がすでに指定されている場合は **no** *sequence-number* コマンドを使用するだけです。

（注）
- アクセス リスト シーケンス番号は、ダイナミック、リフレクシブ、またはファイアウォールのアクセス リストをサポートしていません。

手順の概要

1. **enable**
2. **configure terminal**
3. **ip access-list resequence** *access-list-name starting-sequence-number increment*
4. **ip access-list** {**standard**| **extended**} *access-list-name*
5. 次のいずれかを実行します。
   - *sequence-number* **permit** *source source-wildcard*
   - *sequence-number* **permit** *protocol source source-wildcard destination destination-wildcard* [**precedence** *precedence*][**tos** *tos*] [**log**] [**time-range** *time-range-name*] [**fragments**]
6. 次のいずれかを実行します。
   - *sequence-number* **deny** *source source-wildcard*
   - *sequence-number* **deny** *protocol source source-wildcard destination destination-wildcard* [**precedence** *precedence*][**tos** *tos*] [**log**] [**time-range** *time-range-name*] [**fragments**]
7. 必要に応じてステップ 5 とステップ 6 を繰り返し、目的とするシーケンス番号順にステートメントを追加します。エントリを削除するには、**no** *sequence-number* コマンドを使用します。
8. **end**
9. **show ip access-lists** *access-list-name*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ip access-list resequence** *access-list-name starting-sequence-number increment* 例：	開始シーケンス番号と、シーケンス番号の増分を使用して、指定した IP アクセス リストを並べ替えます。

	コマンドまたはアクション	目的
	`Router(config)# ip access-list resequence kmd1 100 15`	• この例では、kmd1 という名前のアクセス リストを並べ替えます。開始シーケンス番号は100、増分は 15 です。
ステップ 4	**ip access-list** {**standard**| **extended**} *access-list-name* 例： `Router(config)# ip access-list standard xyz123`	名前で IP アクセス リストを指定し、名前付きアクセス リストのコンフィギュレーション モードを開始します。 • **standard** を指定する場合は、その後に、標準アクセス リスト構文を使用して **permit** ステートメントまたは **deny** ステートメントを指定します。 • **extended** を指定する場合は、その後に、拡張アクセス リスト構文を使用して **permit** ステートメントまたは **deny** ステートメントを指定します。
ステップ 5	次のいずれかを実行します。 • *sequence-number* **permit** *source source-wildcard* • *sequence-number* **permit** *protocol source source-wildcard destination destination-wildcard* [**precedence** *precedence*][**tos** *tos*] [**log**] [**time-range** *time-range-name*] [**fragments**] 例： `Router(config-std-nacl)# 105 permit 10.5.5.5 0.0.0.255`	名前付き IP アクセス リスト モードで permit ステートメントを指定します。 • このアクセス リストでは **permit** ステートメントを最初に使用していますが、必要なステートメントの順序に応じて、**deny** ステートメントが最初に使用される可能性もあります。 • 上位層プロトコル（ICMP、IGMP、TCP、およびUDP）を許可するその他のコマンド構文については、**permit**（IP）コマンドを参照してください。 • エントリを削除するには、**no** *sequence-number* コマンドを使用します。 • プロンプトに示されるとおり、このアクセス リストは標準アクセス リストでした。ステップ 4 で **extended** を指定した場合は、このステップのプロンプトは Router(config-ext-nacl)# となり、拡張 **permit** コマンド構文を使用します。
ステップ 6	次のいずれかを実行します。 • *sequence-number* **deny** *source source-wildcard* • *sequence-number* **deny** *protocol source source-wildcard destination destination-wildcard* [**precedence** *precedence*][**tos** *tos*] [**log**] [**time-range** *time-range-name*] [**fragments**]	（任意）名前付き IP アクセス リスト モードで deny ステートメントを指定します。 • このアクセス リストでは **permit** ステートメントを最初に使用していますが、必要なステートメントの順序に応じて、**deny** ステートメントが最初に使用される可能性もあります。

	コマンドまたはアクション	目的
	例： `Router(config-std-nacl)# 110 deny 10.6.6.7 0.0.0.255`	• 上位層プロトコル（ICMP、IGMP、TCP、およびUDP）を許可するその他のコマンド構文については、**deny**（IP）コマンドを参照してください。 • エントリを削除するには、**no** *sequence-number* コマンドを使用します。 • プロンプトに示されるとおり、このアクセス リストは標準アクセス リストでした。ステップ 4 で **extended** を指定した場合は、このステップのプロンプトは Router(config-ext-nacl)# となり、拡張 **deny** コマンド構文を使用します。
ステップ 7	必要に応じてステップ 5 とステップ 6 を繰り返し、目的とするシーケンス番号順にステートメントを追加します。エントリを削除するには、**no** *sequence-number* コマンドを使用します。	アクセス リストは変更できます。
ステップ 8	**end** 例： `Router(config-std-nacl)# end`	（任意）コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。
ステップ 9	**show ip access-lists** *access-list-name* 例： `Router# show ip access-lists xyz123`	（任意）IP アクセス リストの内容を表示します。 • 出力を見直して、アクセス リストに新しいエントリが含まれることを確認します。

例

次に、**xyz123** アクセス リストを指定した場合の **show ip access-lists** コマンドの出力例を示します。

```
Router# show ip access-lists xyz123
Standard IP access list xyz123
100 permit 10.4.4.0, wildcard bits 0.0.0.255
105 permit 10.5.5.5, wildcard bits 0.0.0.255
115 permit 10.0.0.0, wildcard bits 0.0.0.255
130 permit 10.5.5.0, wildcard bits 0.0.0.255
145 permit 10.0.0.0, wildcard bits 0.0.0.255
```

日または週の特定の時間帯でのアクセス リスト エントリの制限

デフォルトで、アクセス リスト ステートメントは適用されたときに実行されます。ただし、時間範囲を定義し、各アクセス リスト ステートメントにおいて名前ごとに時間範囲を参照することで、**permit** ステートメントまたは **deny** ステートメントが有効になる日または週の時間帯を定義できます。IP および Internetwork Packet exchange（IPX）名前付きまたは番号付きの拡張アクセス リストは、時間範囲に対応します。

手順の概要

1. **enable**
2. **configure terminal**
3. **ip access-list extended** *name*
4. [*sequence-number*] **deny** *protocol source*[*source-wildcard*] [*operator port*[*port*]] *destination*[*destination-wildcard*] [*operator port*[*port*]]
5. [*sequence-number*] **deny** *protocol source*[*source-wildcard*][*operator port*[*port*]] *destination*[*destination-wildcard*] [*operator port*[*port*]] **fragments**
6. [*sequence-number*] **permit** *protocol source*[*source-wildcard*] [*operator port*[*port*]] *destination*[*destination-wildcard*] [*operator port*[*port*]]
7. アクセス リストの基本となる値を指定するまで、ステップ 4 ～ 6 を適宜組み合わせて繰り返します。
8. **end**
9. **show ip access-list**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ip access-list extended** *name* 例： `Router(config)# ip access-list extended rstrct4`	名前を使用して拡張 IP アクセス リストを定義し、拡張名前付きアクセス リストのコンフィギュレーション モードを開始します。
ステップ 4	[*sequence-number*] **deny** *protocol source*[*source-wildcard*] [*operator port*[*port*]] *destination*[*destination-wildcard*] [*operator port*[*port*]] 例：	（任意）ステートメントに指定されたすべての条件に一致するすべてのパケットを拒否します。 • このステートメントは、非フラグメント パケットと初期フラグメントに適用されます。

	コマンドまたはアクション	目的
	`Router(config-ext-nacl)# deny ip any 172.20.1.1`	
ステップ 5	[*sequence-number*] **deny** *protocol source*[*source-wildcard*][*operator port*[*port*]] *destination*[*destination-wildcard*] [*operator port*[*port*]] **fragments** 例： `Router(config-ext-nacl)# deny ip any 172.20.1.1 fragments`	（任意）ステートメントに指定されたすべての条件に一致するすべてのパケットを拒否します。 • このステートメントは、非初期フラグメントに適用されます。
ステップ 6	[*sequence-number*] **permit** *protocol source*[*source-wildcard*] [*operator port*[*port*]] *destination*[*destination-wildcard*] [*operator port*[*port*]] 例： `Router(config-ext-nacl)# permit tcp any any`	ステートメントに指定されたすべての条件に一致するすべてのパケットを許可します。 • 各アクセス リストには、少なくとも 1 つの **permit** ステートメントが必要です。 • *source-wildcard* または *destination-wildcard* を省略すると、0.0.0.0 のワイルドカードマスクが想定されます。つまり、それぞれ送信元アドレスまたは宛先アドレスの全ビットへの一致を意味します。 • 必要に応じて、*source source-wildcard* または *destination destination-wildcard* の代わりに、キーワード **any** を使用して、アドレスと 0.0.0.0 255.255.255.255 の送信元ワイルドカードを指定できます。
ステップ 7	アクセス リストの基本となる値を指定するまで、ステップ 4 ～ 6 を適宜組み合わせて繰り返します。	明示的に許可されていないすべての送信元は、アクセス リストの末尾にある暗黙的な **deny** ステートメントで拒否されます。
ステップ 8	**end** 例： `Router(config-ext-nacl)# end`	コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。
ステップ 9	**show ip access-list** 例： `Router# show ip access-list`	（任意）現在の IP アクセス リストすべてのコンテンツが表示されます。

次の作業

アクセス リストをインターフェイスに適用するか、アクセス リストを受け入れるコマンドから参照します。

（注） IP オプションを含むすべてのパケットを効率的に除去するには、**ip options drop** グローバル コマンドを設定することを推奨します。

IP アクセス リストの精緻化の設定例

例：アクセス リストのエントリの並べ替え

次に、並べ替える前と後のアクセス リストの例を示します。開始値は 1、増分値は 2 です。後続のエントリはユーザ指定の増分値に基づいて並べられています。範囲は 1 ～ 2147483647 です。

シーケンス番号のないエントリが入力されると、デフォルトで、アクセス リストの最後のエントリのシーケンス番号に 10 を加えたシーケンス番号が割り当てられます。

```
Router# show access-list carls
Extended IP access list carls
    10 permit ip host 10.3.3.3 host 172.16.5.34
    20 permit icmp any any
    30 permit tcp any host 10.3.3.3
    40 permit ip host 10.4.4.4 any
    50 Dynamic test permit ip any any
    60 permit ip host 172.16.2.2 host 10.3.3.12
    70 permit ip host 10.3.3.3 any log
    80 permit tcp host 10.3.3.3 host 10.1.2.2
    90 permit ip host 10.3.3.3 any
    100 permit ip any any
Router(config)# ip access-list extended carls
Router(config)# ip access-list resequence carls 1 2
Router(config)# end
Router# show access-list carls
Extended IP access list carls
    1 permit ip host 10.3.3.3 host 172.16.5.34
    3 permit icmp any any
    5 permit tcp any host 10.3.3.3
    7 permit ip host 10.4.4.4 any
    9 Dynamic test permit ip any any
    11 permit ip host 172.16.2.2 host 10.3.3.12
    13 permit ip host 10.3.3.3 any log
    15 permit tcp host 10.3.3.3 host 10.1.2.2
    17 permit ip host 10.3.3.3 any
    19 permit ip any any
```

例：シーケンス番号を指定したエントリの追加

次の例では、新しいエントリ（シーケンス番号 15）がアクセス リストに追加されます。

```
Router# show ip access-list
Standard IP access list tryon
2 permit 10.4.4.2, wildcard bits 0.0.255.255
5 permit 10.0.0.44, wildcard bits 0.0.0.255
10 permit 10.0.0.1, wildcard bits 0.0.0.255
20 permit 10.0.0.2, wildcard bits 0.0.0.255
Router(config)# ip access-list standard tryon
Router(config-std-nacl)# 15 permit 10.5.5.5 0.0.0.255
Router# show ip access-list
Standard IP access list tryon
2 permit 10.4.0.0, wildcard bits 0.0.255.255
5 permit 10.0.0.0, wildcard bits 0.0.0.255
10 permit 10.0.0.0, wildcard bits 0.0.0.255
15 permit 10.5.5.0, wildcard bits 0.0.0.255
20 permit 10.0.0.0, wildcard bits 0.0.0.255
```

例：シーケンス番号を指定しないエントリの追加

次に、シーケンス番号が指定されていないエントリをアクセス リストの末尾に追加する方法を示します。シーケンス番号のないエントリを追加すると、自動的にシーケンス番号が割り当てられ、アクセス リストの末尾に配置されます。デフォルトの増分値は 10 であるため、エントリには、既存のアクセス リストの最後のエントリのシーケンス番号に 10 を加えたシーケンス番号が割り当てられます。

```
Router(config)# ip access-list standard resources
Router(config-std-nacl)# permit 10.1.1.1 0.0.0.255
Router(config-std-nacl)# permit 10.2.2.2 0.0.0.255
Router(config-std-nacl)# permit 10.3.3.3 0.0.0.255
Router# show access-list
Standard IP access list resources
10 permit 10.1.1.1, wildcard bits 0.0.0.255
20 permit 10.2.2.2, wildcard bits 0.0.0.255
30 permit 10.3.3.3, wildcard bits 0.0.0.255
Router(config)# ip access-list standard resources
Router(config-std-nacl)# permit 10.4.4.4 0.0.0.255
Router(config-std-nacl)# end
Router# show access-list
Standard IP access list resources
10 permit 10.1.1.1, wildcard bits 0.0.0.255
20 permit 10.2.2.2, wildcard bits 0.0.0.255
30 permit 10.3.3.3, wildcard bits 0.0.0.255
40 permit 10.4.4.4, wildcard bits 0.0.0.255
```

例：IP アクセス リスト エントリに適用された時間範囲

次の例では、月曜日 ～ 金曜日の 8:00 am ～ 6:00 p.m に延長した、no-http と呼ばれる時間範囲を作成します。この時間帯は **deny** ステートメントに適用されるため、月曜日 ～ 金曜日の 8:00 am ～ 6:00 p.m の HTTP トラフィックが拒否されます。

udp-yes と呼ばれる時間範囲は、正午から 8:00 p.m までの週末を定義します。この時間範囲は **permit** ステートメントに適用されるため、土曜日 ～ 日曜日の正午から 8:00 p.m の UDP トラフィックのみが許可されます。両方のステートメントを含むアクセス リストは、ファストイーサネット インターフェイス 0/0/0 のインバウンド パケットに適用されます。

```
time-range no-http
 periodic weekdays 8:00 to 18:00
!
time-range udp-yes
 periodic weekend 12:00 to 20:00
!
ip access-list extended strict
 deny tcp any any eq http time-range no-http
 permit udp any any time-range udp-yes
!
interface fastethernet 0/0/0
 ip access-group strict in
```

例：IP パケット フラグメントのフィルタリング

次のアクセス リストでは、最初のステートメントはホスト 172.16.1.1 を宛先とする非初期フラグメントのみを拒否します。2 番目のステートメントは、ホスト 172.16.1.1 の TCP ポート 80 を宛先とする残りの非フラグメントと初期フラグメントのみを許可します。3 番目のステートメントは、その他のすべてのトラフィックを拒否します。すべての TCP ポートで非初期フラグメントをブロックするため、ホスト 172.16.1.1 のポート 80 をはじめとするすべての TCP ポートで非初期フラグメントをブロックする必要があります。つまり、非初期フラグメントにはレイヤ 4 ポート情報は含まれないため、指定のポートで該当するトラフィックをブロックするには、すべてのポートのフラグメントをブロックする必要があります。

```
access-list 101 deny ip any host 172.16.1.1 fragments
access-list 101 permit tcp any host 172.16.1.1 eq 80
access-list 101 deny ip any any
```

その他の参考資料

関連資料

関連項目	マニュアル タイトル
time-range コマンドを使用した時間範囲の指定	『*Cisco IOS XE Network Management Configuration Guide*』の「*Performing Basic System Management*」章
ネットワーク管理コマンドの説明	『*Cisco IOS Network Management Command Reference*』

標準

標準	タイトル
この機能でサポートされる新規の標準または変更された標準はありません。また、既存の標準のサポートは変更されていません。	--

MIB

MIB	MIB のリンク
この機能によってサポートされる新しい MIB または変更された MIB はありません。またこの機能による既存 MIB のサポートに変更はありません。	選択したプラットフォーム、Cisco IOS XE ソフトウェア リリース、およびフィーチャ セットの MIB の場所を検索しダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

RFC

RFC	タイトル
この機能によりサポートされた新規 RFC または改訂 RFC はありません。またこの機能による既存 RFC のサポートに変更はありません。	--

シスコのテクニカル サポート

説明	リンク
右の URL にアクセスして、シスコのテクニカル サポートを最大限に活用してください。これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

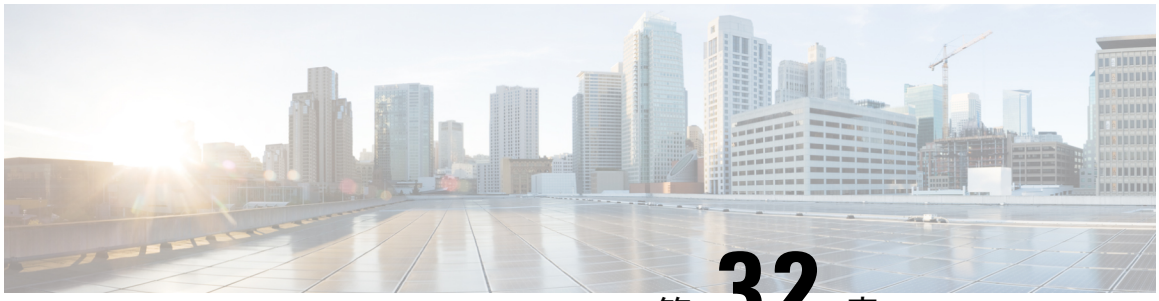
IP アクセス リストの精緻化に関する機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *53 : IP* アクセス リストの精緻化に関する機能情報

機能名	リリース	機能の設定情報
時刻ベースのアクセス リスト	Cisco IOS XE リリース 2.1	この機能は、Cisco ASR 1000 シリーズのアグリゲーション サービス ルータで導入されました。 この機能について導入または変更されたコマンドはありません。



第 32 章

IP 名前付きアクセス コントロール リスト

アクセス コントロール リスト（ACL）は、ネットワークを通過するパケットの動きを制御するためにパケット フィルタリングを実行します。パケット フィルタリングは、ネットワークへのトラフィックのアクセスを限定し、ユーザーおよびデバイスのネットワークに対するアクセスを制限し、トラフィックがネットワークから流出するのを防ぐことで、セキュリティを提供します。IP アクセス リストによって、スプーフィングやサービス妨害攻撃の可能性を軽減し、ファイアウォールを介した動的で一時的なユーザー アクセスが可能になります。

IP 名前付きアクセス コントロール リスト機能により、ネットワーク管理者は、管理するアクセス リストを識別するための名前を使用することができます。

このモジュールでは、IP 名前付きアクセス コントロール リスト、およびその設定方法について説明します。

IP 名前付きアクセス コントロール リストに関する情報

アクセス リストの定義

アクセス コントロール リスト（ACL）は、ネットワークを通過するパケットの動きを制御するためにパケット フィルタリングを実行します。パケット フィルタリングは、ネットワークへのトラフィックのアクセスを限定し、ユーザーおよびデバイスのネットワークに対するアクセスを制限し、トラフィックがネットワークから流出するのを防ぐことで、セキュリティを提供します。IP アクセス リストによって、スプーフィングやサービス妨害攻撃の可能性を軽減し、ファイアウォールを介した動的で一時的なユーザー アクセスが可能になります。

また、IP アクセス リストは、セキュリティ以外の用途にも使用できます。たとえば、帯域幅制御、ルーティング アップデートのコンテンツの制限、ルートの再配布、ダイヤルオンデマン

ド（DDR）呼び出しのトリガー、デバッグ出力の制限、Quality of Service（QoS）機能のトラフィックの識別と分類などです。

アクセス リストは、少なくとも 1 つの **permit** ステートメント、および任意の 1 つまたは複数の **deny** ステートメントで構成される順次リストです。IP アクセス リストの場合、これらのステートメントは IP アドレス、上位層の IP プロトコルなどの IP パケットのフィールドに適用できます。

アクセスリストは名前または番号で識別および参照されます。アクセスリストはパケットフィルタとして動作し、各アクセスリストに定義されている条件に基づいてパケットがフィルタされます。

アクセスリストを構成した後でアクセスリストを有効にするには、アクセスリストをインターフェイスに適用するか（**ip access-group** コマンドを使用）、vty に適用するか（**access-class** コマンドを使用）、またはアクセス リストを許容するあらゆるコマンドでアクセス リストを参照する必要があります。複数のコマンドから同じアクセス リストを参照できます。

次の構成では、branchoffices という名前の IP アクセス リストがファスト イーサネット インターフェイス 0/1/0 上で構成され、着信パケットに適用されます。発信元アドレスとマスクのペアで指定されているネットワーク以外は、ファスト イーサネット インターフェイス 0/1/0 にアクセスできません。ネットワーク 172.16.7.0 上の送信元から発信されるパケットの宛先に、制限はありません。ネットワーク 172.16.2.0 上の送信元から発信されるパケットの宛先は、172.31.5.4 にする必要があります。

```
ip access-list extended branchoffices
 10 permit 172.16.7.0 0.0.0.3 any
 20 permit 172.16.2.0 0.0.0.255 host 172.31.5.4
!
interface fastethernet 0/1/0
 ip access-group branchoffices in
```

名前付きまたは番号付きアクセス リスト

すべてのアクセス リストは、名前または番号で識別されます。名前付きアクセス リストは、番号付きアクセスリストよりも便利です。タスクを思いだしやすく関連性がある、わかりやすい名前を指定できるためです。名前付きアクセスリストでは、ステートメントの順序を変更したり、ステートメントを追加したりできます。

名前付きアクセスリストは、番号付きアクセスリストではサポートされない次の機能をサポートします。

- IP オプションのフィルタリング
- 非隣接ポート
- TCP フラグ フィルタリング
- **no permit** または **no deny** コマンドによるエントリの削除

（注） 番号付きアクセス リストを受け入れるコマンドの中には、名前付きアクセス リストを受け入れないコマンドがあります。たとえば、vty には番号付きアクセス リストだけを使用します。

IP アクセス リストの利点

アクセス コントロール リスト（ACL）は、ネットワークを通過するパケットのフローを制御するためにパケット フィルタリングを実行します。パケット フィルタリングによってユーザーおよびデバイスのネットワークに対するアクセスを制限し、セキュリティの手段として利用できます。アクセス リストによってトラフィック数を減らすことで、ネットワーク リソースを節約できます。アクセス リストを使用した場合の利点は次のとおりです。

- 着信 rsh および rcp 要求を認証する：アクセス リストは、デバイスへのアクセスを制御するように構成された認証データベース内のローカル ユーザー、リモート ホスト、およびリモート ユーザーの識別を簡素化できます。Cisco ソフトウェアは認証データベースを使用して、リモート シェル（rsh）およびリモート コピー（rcp）プロトコルの着信要求を受け取ることができます。
- 不要なトラフィックまたはユーザーをブロックする：アクセス リストを使用すると、インターフェイス上の着信パケットまたは発信パケットをフィルタできるため、送信元アドレス、宛先アドレス、またはユーザー認証に基づいてネットワークへのアクセスを制御できます。また、アクセス リストを使用して、デバイス インターフェイスで転送またはブロックするトラフィックの種類を決定することもできます。たとえば、電子メール トラフィックはネットワークでルーティングすることを許可し、すべての Telnet トラフィックはネットワークに入ることをブロックするようにアクセス リストを使用できます。
- vty へのアクセスを制御する：インバウンド vty（Telnet）でのアクセス リストは、デバイスへの回線にアクセスできるユーザーを制御できます。アウトバウンド vty でのアクセス リストは、デバイスからの回線が到達可能な宛先を制御できます。
- QoS 機能のトラフィックを特定または分類する：アクセス リストは、Weighted Random Early Detection（WRED）および専用アクセス レート（CAR）の IP プレシデンスを設定することで、輻輳回避を提供します。また、クラスベース均等化キューイング（CBWFQ）、プライオリティ キューイング、カスタム キューイングのために輻輳管理を提供します。
- debug コマンド出力を制限する：アクセス リストは、IP アドレスやプロトコルに基づいて debug 出力を制限できます。
- 帯域幅制御を提供する：低速リンクでのアクセス リストはネットワークでの過剰なトラフィックを防止できます。
- NAT 制御を提供する：アクセス リストによって、ネットワーク アドレス変換（NAT）が変換するアドレスを制御できます。
- DoS攻撃の可能性を低減する：アクセス リストは、サービス妨害（DoS）攻撃の可能性を低減させます。ホストからのトラフィック、ネットワーク、またはネットワークにアクセスするユーザーを制御するように IP 発信元アドレスを指定します。TCP インターセプト

機能を設定することで、接続に関する要求でサーバーにフラッディングが発生しないようにすることができます。

- ルーティング アップデートの内容を制限する：アクセス リストによって、ネットワーク内で送信、受信、または再配布されるルーティング アップデートを制御できます。
- ダイヤルオンデマンド コールをトリガーする：アクセス リストによって、ダイヤルおよび切断条件を適用できます。

アクセス リストのルール

アクセス リストには、次のルールが適用されます。

- 1 つのインターフェイス、1 つのプロトコル、1 つの方向につき、許可されるアクセス リストは 1 つだけです。
- アクセスリストには少なくとも 1 つの **permit** ステートメントが含まれる必要があります。そうしないと、ネットワークに入るすべてのパケットが拒否されます。
- アクセスリスト条件または一致基準の構成順序は重要です。パケットを転送するかブロックするかを決定するときに、シスコソフトウェアは、それぞれの条件ステートメントに対してステートメントの作成順にパケットをテストします。一致が見つかると、条件ステートメントはそれ以上チェックされません。同じ **permit** ステートメントまたは **deny** ステートメントでも、順序が異なる場合、ある状況では通過し、別の状況では拒否されるパケットが生じる可能性があります。
- アクセス リストを名前によって参照したときに、そのアクセス リストが存在しない場合は、すべてのパケットが通過します。インターフェイスまたはコマンドに空のアクセスリストを適用すると、ネットワークに対するすべてのトラフィックが許可されます。
- 標準のアクセス リストと拡張のアクセス リストの名前は同じにできません。
- パケットが発信インターフェイスにルーティングされる前に、着信アクセス リストがパケットを処理します。ネットワークへのパケットアクセスを拒否するフィルタ条件がある着信アクセス リストは、ルーティング ルックアップ時のオーバーヘッドを削減します。構成されたフィルタ基準に基づいてネットワークへのアクセスを許可されたパケットはルーティング処理されます。インバウンド アクセス リストの場合、**permit** ステートメントを構成するとパケットは受信後に処理され、**deny** ステートメントを構成するとパケットは破棄されます。
- アウトバウンドアクセスリストの場合、パケットの処理後にデバイスから送信されます。着信パケットはアウトバウンドインターフェイスにルーティングされてから、アウトバウンドアクセス リストで処理されます。アウトバウンドアクセス リストの場合、**permit** ステートメントを構成するとパケットは出力バッファに送信され、**deny** ステートメントを構成するとパケットは破棄されます。
- アクセスリストで、デバイスに到達するトラフィック、またはデバイス経由で送信されるトラフィックは制御できますが、デバイスが送信元のトラフィックは制御できません。

IP アクセス リストを作成する際に役立つヒント

意図しない結果を回避し、より効率的で有効なアクセス リストを作成するために役立つヒントを紹介します。

- アクセス リストを作成してから、インターフェイス（または別の対象）に適用します。その理由は、存在しないアクセス リストをインターフェイスに適用してから、アクセス リストを設定すると、最初のステートメントが有効になり、それに続く暗黙的な **deny** ステートメントによってアクセスに緊急の問題が発生するおそれがあるためです。
- アクセス リストを設定してから適用するもう 1 つの理由は、空のアクセス リストが適用されたインターフェイスはすべてのトラフィックを許可するためです。
- すべてのアクセス リストには、少なくとも 1 つの **permit** ステートメントが必要です。permit がないと、すべてのパケットは拒否され、トラフィックはまったく通過しません。
- 最初に（**permit** または **deny** ステートメントに対する）一致が見つかった後は条件のテストが終了するため、パケットが一致する可能性の高いステートメントをアクセス リストの先頭に配置すると処理にかかる時間とリソースが削減されます。最も頻繁に発生する条件を発生頻度の低い条件より前に配置します。
- ネットワークまたはサブネットのより具体的な参照が、より全般的な参照よりも前に出現するように、アクセス リストを構成します。
- まだ拒否されていないその他のパケットすべてを許可する場合、ステートメント **permit any any** を使用します。ステートメント **permit any any** を使用すると、実質的に、アクセス リストの末尾にある暗黙的な deny ステートメントでその他すべてのパケットが拒否されることを防ぎます。最初のアクセス リスト エントリは **permit any any** にしないでください。すべてのトラフィックが通過し、以降のテストに到達するパケットがなくなります。**permit any any** を指定すると、まだ拒否されていないすべてのトラフィックが通過します。
- すべてのアクセス リストは暗黙的な **deny** ステートメントで終了しますが、明示的な **deny** ステートメント（たとえば **deny ip any any**）の使用を推奨します。ほとんどのプラットフォームでは、**show access-list** コマンドを発行して拒否されるパケット数を表示し、アクセス リストが許可していないパケットに関する詳細情報を調査できます。明示的な **deny** ステートメントで拒否されたパケットのみがカウントされます。これは、明示的な **deny** ステートメントによって、より詳細なデータが生成されるためです。
- アクセス リストの作成中、または作成後に、エントリを削除する場合があります。
  - 番号付きアクセス リストからはエントリを削除できません。削除しようとすると、アクセス リスト全体が削除されます。エントリを削除する必要がある場合、アクセス リスト全体を削除してから最初から作り直す必要があります。
  - 名前付きアクセス リストからはエントリを削除できます。**no permit** または **no deny** コマンドを使用すると、適切なエントリが削除されます。
- 個々のステートメントの用途をひと目で確認および理解しやすくするために、**remark** コマンドを使用して、ステートメントの前後に役立つ注記を書き込むことができます。

- 特定のホストまたはネットワークに対するアクセスを拒否し、そのネットワークまたはホストの誰かがアクセスしようとしたかどうかを検出する場合、対応する **deny** ステートメントを指定した **log** キーワードを含めます。それによって、その送信元からの拒否されたパケットがログに記録されます。
- このヒントは、アクセスリストの配置に適用されます。リソースを保存しようとすると、インバウンドアクセスリストでは常にフィルタ条件を適用した後に、ルーティングテーブルの検索を行います。アウトバウンドアクセスリストではフィルタ条件を適用する前に、ルーティング テーブルの検索を行います。
- 新しい ACL ステートメントを追加する前に、パーサーが削除をクリーンアップする時間を確保します。

アクセス リストを適用する場所

アクセス リストは、デバイスの着信または発信インターフェイスに適用できます。アクセスリストを着信インターフェイスに適用すると、インターフェイスで着信するトラフィックが制御され、アクセスリストを発信インターフェイスに適用すると、インターフェイスから発信されるトラフィックが制御されます。

ソフトウェアは、着信インターフェイスでパケットを受信すると、アクセスリストで設定されているステートメントに対してパケットを検査します。アクセスリストがアドレスを許可している場合は、ソフトウェアはパケットを処理します。着信パケットをフィルタリングするためにアクセスリストを適用すると、フィルタリングされたパケットはデバイスに到達する前に廃棄されるため、デバイスのリソースを節約できます。

発信インターフェイスでは、アクセス リストはインターフェイスから転送（送信）されたパケットをフィルタリングします。発信インターフェイスで Rate-Based Satellite Control Protocol（RBSCP）の TCP アクセス コントロール リスト（ACL）を使用して、発信インターフェイスで TCP 確認応答（ACK）を受けるパケットの種類を制御できます。

debug コマンドを使用してアクセス リストを参照し、デバッグ ログの量を制限できます。たとえば、アクセス リストのフィルタリング基準または一致基準に基づいて、デバッグ ログを送信元または宛先のアドレスまたはプロトコルに制限できます。

アクセス リストを使用して、ルーティング アップデート、ダイヤルオンデマンド（DDR）、および Quality of Service（QoS）機能を制御することができます。

IP 名前付きアクセス コントロール リストの設定方法

IP 名前付きアクセス リストの作成

IP 名前付きアクセス リストを作成すると、発信元アドレスと宛先アドレス、またはアドレスと他の IP フィールドの組み合わせをフィルタリングすることができます。名前付きアクセスリストにより、分かりやすい名前の付いたアクセス リストを特定できます。

手順の概要

1. **enable**
2. **configure terminal**
3. **ip access-list extended** *name*
4. **remark** *remark*
5. **deny** *protocol* [*source source-wildcard*] {**any** | **host** {*address* | *name*} {*destination* [*destination-wildcard*] {**any** | **host** {*address* | *name*} [**log**]
6. **remark** *remark*
7. **permit** *protocol* [*source source-wildcard*] {**any** | **host** {*address* | *name*} {*destination* [*destination-wildcard*] {**any** | **host** {*address* | *name*} [**log**]
8. アクセス リストにステートメントをさらに指定するには、ステップ 4 ～ 7 を繰り返します。
9. **end**
10. **show ip access-lists**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ip access-list extended** *name* 例： `Device(config)# ip access-list extended acl1`	名前を使用して拡張 IP アクセス リストを定義し、拡張名前付きアクセス リストのコンフィギュレーション モードを開始します。
ステップ 4	**remark** *remark* 例： `Device(config-ext-nacl)# remark protect server by denying sales access to the acl1 network`	（任意）アクセス リスト ステートメントに説明を追加します。 • 注釈は IP アクセス リスト エントリの前または後に指定できます。 • この例では、**remark** コマンドによって、ステップ 5 で設定した **deny** コマンドがインターフェイスに対する Sales ネットワーク アクセスを拒否することをネットワーク管理者に示します。
ステップ 5	**deny** *protocol* [*source source-wildcard*] {**any**	**host** {*address*	*name*} {*destination* [*destination-wildcard*] {**any**	**host** {*address*	*name*} [**log**] 例：	（任意）注釈で指定されたすべての条件に一致するパケットをすべて拒否します。

	コマンドまたはアクション	目的
	`Device(config-ext-nacl)# deny ip 192.0.2.0 0.0.255.255 host 192.0.2.10 log`	
ステップ 6	**remark** *remark* 例： `Device(config-ext-nacl)# remark allow TCP from any source to any destination`	（任意）アクセス リスト ステートメントに説明を追加します。 • 注釈はIPアクセス リスト エントリの前または後に指定できます。
ステップ 7	**permit** *protocol* [*source source-wildcard*] {**any** | **host** {*address* | *name*} {*destination* [*destination-wildcard*] {**any** | **host** {*address* | *name*} [**log**] 例： `Device(config-ext-nacl)# permit tcp any any`	ステートメントで指定されたすべての条件に一致するパケットをすべて許可します。
ステップ 8	アクセス リストにステートメントをさらに指定するには、ステップ 4 ～ 7 を繰り返します。	（注） ステートメントによって明示的に許可されていないすべての送信元アドレスは、アクセス リストの末尾にある暗黙的なdenyステートメントで拒否されます。
ステップ 9	**end** 例： `Device(config-ext-nacl)# end`	拡張名前付きアクセス リストのコンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。
ステップ 10	**show ip access-lists** 例： `Device# show ip access-lists`	現在のすべてのIPアクセス リストの内容を表示します。

例：

次に、 **show ip access-lists** コマンドの出力例を示します。

```
Device# show ip access-lists acl1

Extended IP access list acl1
   permit tcp any 192.0.2.0 255.255.255.255 eq telnet
   deny tcp any any
   deny udp any 192.0.2.0 255.255.255.255 lt 1024
   deny ip any any log
```

物理インターフェイスへのアクセスリストの適用

手順の概要

1. **enable**

2. **configure terminal**
3. **interface** *type number*
4. **ip access-group** {*access-list-number* | *access-list-name*} {**in** | **out**}
5. **ip access-list extended** *acl-name acl-number*
6. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface** *type number* 例：	インターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	**ip access-group** {*access-list-number* | *access-list-name*} {**in** | **out**} 例： `Device(config-if)# ip access-group acl1 in`	指定したアクセス リストをインバウンド インターフェイスに適用します。 • 送信元アドレスをフィルタリングするには、インバウンド インターフェイスにアクセス リストを適用します。
ステップ 5	**ip access-list extended** *acl-name acl-number* 例：	拡張 ACL コンフィギュレーション モードを有効にします。CLI は拡張 ACL コンフィギュレーション モードを開始します。このモードでは、後続のすべてのコマンドが現在の拡張アクセスリストに適用されます。 拡張 ACL コンフィギュレーション モードを有効にします。CLI は拡張 ACL コンフィギュレーション モードを開始します。このモードでは、後続のすべてのコマンドが現在の拡張アクセスリストに適用されます。 • ACL コンフィギュレーション モードから入力されたすべてのコマンドが適用されるアクセス リスト。英字で始まる最大 30 文字の英数字文字列を使用します。 • アクセス リスト コンフィギュレーション モードから入力されたすべてのコマンドが適用されるアクセスリスト。数字の識別子を使用しま

	コマンドまたはアクション	目的
		す。拡張アクセスリストでは、有効範囲は 100 ～ 199 です。
ステップ 6	**end** 例： `Device(config-if)# end`	インターフェイス コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

IP 名前付きアクセス コントロール リストの設定例

例：IP 名前付きアクセス コントロール リストの作成

```
Device# configure terminal
Device(config)# ip access-list extended acl1
Device(config-ext-nacl)# remark protect server by denying sales access to the acl1 network
Device(config-ext-nacl)# deny ip 192.0.2.0 0.0.255.255 host 192.0.2.10 log
Device(config-ext-nacl)# remark allow TCP from any source to any destination
Device(config-ext-nacl)# permit tcp any any
```

例：インターフェイスへのアクセス リストの適用

```
Device# configure terminal

Device(config-if)# ip access-group acl1 in
```

IP 名前付きアクセス コントロール リストの追加情報

関連資料

関連項目	マニュアル タイトル
セキュリティ コマンド	• 『Cisco IOS Security Command Reference: Commands A to C』 • 『Cisco IOS Security Command Reference: Commands D to L』 • 『Cisco IOS Security Command Reference: Commands M to R』 • 『Cisco IOS Security Command Reference: Commands S to Z』

シスコのテクニカル サポート

説明	リンク
右の URL にアクセスして、シスコのテクニカル サポートを最大限に活用してください。これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

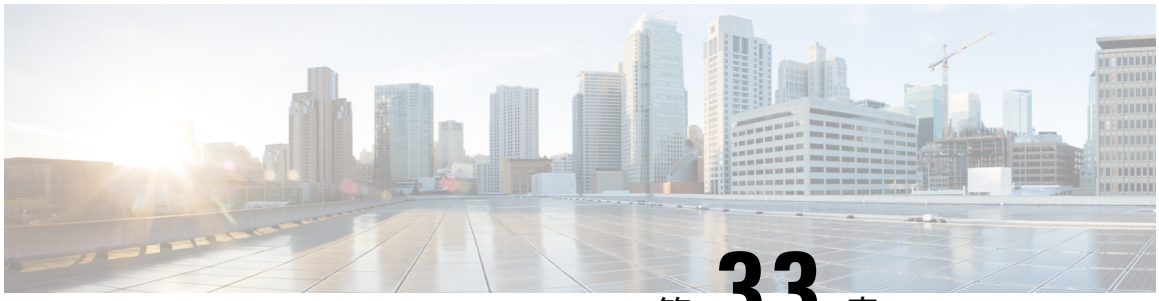
IP 名前付きアクセス コントロール リストに関する機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *54 : IP* 名前付きアクセス コントロール リストに関する機能情報

機能名	リリース	機能情報
IP 名前付きアクセス コントロール リスト		アクセス コントロール リスト（ACL）は、ネットワークを通過するパケットの動きを制御するためにパケット フィルタリングを実行します。パケット フィルタリングは、ネットワークへのトラフィックを限定し、ユーザーおよびデバイスのネットワークに対するアクセスを制限し、トラフィックがネットワークから流出するのを防ぐことで、セキュリティを提供します。IP アクセス リストによって、スプーフィングやサービス妨害攻撃の可能性を軽減し、ファイアウォールを介した動的で一時的なユーザー アクセスが可能になります。



第 33 章

注釈付きの IP アクセス リスト エントリ

注釈付きの IP アクセス リスト エントリ機能により、**deny** または**permit** 条件に関するコメントや注釈を IP アクセス リストに含めることができます。これらの注釈は、ネットワーク管理者がアクセス リストを理解するのを容易にします。各注釈の長さは 100 文字に制限されます。

このモジュールは、注釈付きの IP アクセス リスト エントリ機能に関する情報を提供します。

../トピック/注釈付きIPアクセスリストエントリに関する情報

IP アクセス リストの利点

アクセス コントロール リスト（ACL）は、ネットワークを通過するパケットのフローを制御するためにパケットフィルタリングを実行します。パケットフィルタリングによってユーザーおよびデバイスのネットワークに対するアクセスを制限し、セキュリティの手段として利用できます。アクセス リストによってトラフィック数を減らすことで、ネットワーク リソースを節約できます。アクセス リストを使用した場合の利点は次のとおりです。

- 着信 rsh および rcp 要求を認証する：アクセス リストは、デバイスへのアクセスを制御するように構成された認証データベース内のローカル ユーザー、リモート ホスト、およびリモート ユーザーの識別を簡素化できます。Cisco ソフトウェアは認証データベースを使用して、リモート シェル（rsh）およびリモート コピー（rcp）プロトコルの着信要求を受け取ることができます。

- 不要なトラフィックまたはユーザーをブロックする：アクセス リストを使用すると、インターフェイス上の着信パケットまたは発信パケットをフィルタできるため、送信元アドレ

ス、宛先アドレス、またはユーザー認証に基づいてネットワークへのアクセスを制御できます。また、アクセスリストを使用して、デバイスインターフェイスで転送またはブロックするトラフィックの種類を決定することもできます。たとえば、電子メールトラフィックはネットワークでルーティングすることを許可し、すべてのTelnetトラフィックはネットワークに入ることをブロックするようにアクセス リストを使用できます。

- vty へのアクセスを制御する：インバウンド vty（Telnet）でのアクセス リストは、デバイスへの回線にアクセスできるユーザーを制御できます。アウトバウンド vty でのアクセス リストは、デバイスからの回線が到達可能な宛先を制御できます。
- QoS 機能のトラフィックを特定または分類する：アクセス リストは、Weighted Random Early Detection（WRED）および専用アクセス レート（CAR）の IP プレシデンスを設定することで、輻輳回避を提供します。また、クラスベース均等化キューイング（CBWFQ）、プライオリティ キューイング、カスタム キューイングのために輻輳管理を提供します。
- debug コマンド出力を制限する：アクセス リストは、IP アドレスやプロトコルに基づいて debug 出力を制限できます。
- 帯域幅制御を提供する：低速リンクでのアクセス リストはネットワークでの過剰なトラフィックを防止できます。
- NAT 制御を提供する：アクセス リストによって、ネットワーク アドレス変換（NAT）が変換するアドレスを制御できます。
- DoS攻撃の可能性を低減する：アクセス リストは、サービス妨害（DoS）攻撃の可能性を低減させます。ホストからのトラフィック、ネットワーク、またはネットワークにアクセスするユーザーを制御するように IP 発信元アドレスを指定します。TCP インターセプト機能を設定することで、接続に関する要求でサーバーにフラッディングが発生しないようにすることができます。
- ルーティング アップデートの内容を制限する：アクセス リストによって、ネットワーク内で送信、受信、または再配布されるルーティング アップデートを制御できます。
- ダイヤルオンデマンド コールをトリガーする：アクセス リストによって、ダイヤルおよび切断条件を適用できます。

アクセス リストの注釈

任意のIPアクセスリストのエントリについて、コメントまたは注釈を含めることができます。アクセス リストの注釈は、アクセス リスト エントリの前後にあるオプションの注釈です。エントリの内容がわかるので、エントリの目的を解釈する必要はありません。各注釈の長さは 100 文字に制限されます。

コメントは、**permit** ステートメントまたは **deny** ステートメントの前後どちらにでも配置できます。注釈を追加する場所には一貫性があるようにしてください。注釈が関連する **permit** ステートメントや**deny**ステートメントの前にある場合と後にある場合とが混在すると、ユーザーが混乱する可能性があります。

後続の **deny** ステートメントの機能を説明する注釈の例を次に示します。

```
ip access-list extended telnetting
 remark Do not allow host1 subnet to telnet out
 deny tcp host 172.16.2.88 any eq telnet
```

注釈付き IP アクセス リスト エントリの設定方法

名前付きまたは番号付きアクセス リストへの注釈の書き込み

名前付きまたは番号付きアクセス リスト設定を使用できます。作業する設定用にアクセス リストを作成したら、アクセスリストをインターフェイスまたは端末回線に適用する必要があります。

手順の概要

1. **enable**
2. **configure terminal**
3. **ip access-list** {**standard** | **extended**} {*name* | *number*}
4. **remark** *remark*
5. **deny** *protocol* **host** *host-address* **any eq** *port*
6. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ip access-list** {**standard**	**extended**} {*name*	*number*} 例： `Device(config)# ip access-list extended telnetting`	名前または番号でアクセスリストを特定し、拡張名前付きアクセスリストコンフィギュレーションモードを開始します。
ステップ 4	**remark** *remark* 例： `Device(config-ext-nacl)# remark Do not allow host1 subnet to telnet out`	名前付き IP アクセス リストのエントリに注釈を追加します。 • 注釈は、**permit** または **deny** ステートメントの目的を示します。
ステップ 5	**deny** *protocol* **host** *host-address* **any eq** *port* 例：	パケットを拒否する名前付き IP アクセス リストの条件を設定します。

	コマンドまたはアクション	目的
	`Device(config-ext-nacl)# deny tcp host 172.16.2.88 any eq telnet`	
ステップ 6	**end** 例： `Device(config-ext-nacl)# end`	拡張名前付きアクセス リスト コンフィギュレーション モードを終了し、特権 EXEC モードを開始します。

注釈付き IP アクセス リスト エントリの設定例

例：IP アクセス リストの備考の書き込み

```
Device# configure terminal
Device(config)# ip access-list extended telnetting
Device(config-ext-nacl)# remark Do not allow host1 subnet to telnet out
Device(config-ext-nacl)# deny tcp host 172.16.2.88 any eq telnet
Device(config-ext-nacl)# end
```

注釈付き IP アクセス リスト エントリの追加情報

関連資料

関連項目	マニュアル タイトル
セキュリティ コマンド	• 『Cisco IOS Security Command Reference: Commands A to C』 • 『Cisco IOS Security Command Reference: Commands D to L』 • 『Cisco IOS Security Command Reference: Commands M to R』 • 『Cisco IOS Security Command Reference: Commands S to Z』

シスコのテクニカル サポート

説明	リンク
右の URL にアクセスして、シスコのテクニカル サポートを最大限に活用してください。これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

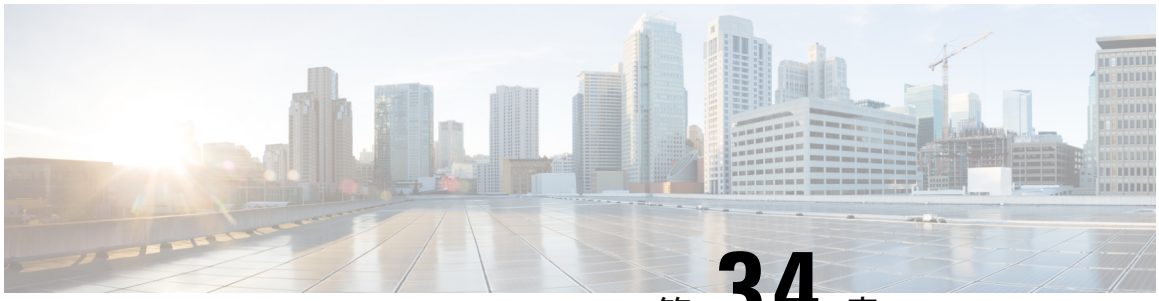
注釈付き IP アクセス リスト エントリに関する機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *55* : 注釈付き *IP* アクセス リスト エントリに関する機能情報

機能名	リリース	機能情報
注釈付きの IP アクセス リスト エントリ		注釈付きの IP アクセス リスト エントリ機能により、[deny] または [permit] 条件に関するコメントや備考をどの IP アクセスリストにも含めることができます。これらの注釈は、ネットワーク管理者がアクセス リストを理解するのを容易にします。各注釈の長さは 100 文字に制限されます。 次のコマンドが導入または変更されました。 **remark**



第 34 章

標準 IP アクセス リストのロギング

標準 IP アクセス リストのロギング機能は、標準 IP アクセス リストによって許可または拒否されるパケットに関するメッセージをロギングする機能を提供します。アクセス リストに一致するパケットによって、デバイス コンソールにあるパケットに関する情報メッセージがロギングされます。

このモジュールは、標準 IP アクセス リスト ロギングに関する情報を提供します。

標準 IP アクセス リストのロギングに関する制限事項

IP アクセス リスト ロギングは、ルーティング インターフェイスまたはルータ アクセス コントロール リスト（ACL）でのみサポートされます。

標準 IP アクセス リストのロギングに関する情報

標準 IP アクセス リストのロギング

標準 IP アクセス リストのロギング機能は、標準 IP アクセス リストによって許可または拒否されるパケットに関するメッセージをロギングする機能を提供します。アクセス リストに一致するパケットによって、デバイス コンソールに送信されるパケットに関する情報ロギング メッセージが生成されます。デバイス コンソールに記録されるメッセージのログ レベルは、**logging console** コマンドによって制御されます。

アクセス リストが最初に検査したパケットがアクセス リストをトリガーし、デバイス コンソールにメッセージをロギングします。後続のパケットは、5 分間隔で収集された後、表示または

ロギングされます。ログ メッセージには、アクセス リスト番号、パケットの送信元 IP アドレス、その送信元からの、直前の 5 分間隔に許可または拒否されたパケットの数、およびパケットが許可されたか拒否されたかに関する情報が含まれます。特定のアクセス リストによって許可または拒否された複数のパケットについて、各パケットの送信元アドレスなどをモニターすることができます。

標準 IP アクセス リストのロギングの設定方法

番号を使用した標準 IP アクセス リストの作成

手順の概要

1. **enable**
2. **configure terminal**
3. **access-list** *access-list-number* {**deny** | **permit**} **host** *address* [**log**]
4. **access-list** *access-list-number* {**deny** | **permit**} **any** [**log**]
5. **interface** *type number*
6. **ip access-group** *access-list-number* {**in** | **out**}
7. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**access-list** *access-list-number* {**deny** | **permit**} **host** *address* [**log**] 例： `Device(config)# access-list 1 permit host 10.1.1.1 log`	送信元アドレスとワイルドカードを使用して、標準の名前付き IP アクセス リストを定義し、デバイス コンソールでアクセス リスト エントリと一致したパケットに関する情報メッセージのロギングを設定します。
ステップ 4	**access-list** *access-list-number* {**deny** | **permit**} **any** [**log**] 例： `Device(config)# access-list 1 permit any log`	送信元の省略形および送信元マスク 0.0.0.0 255.255.255.255 を使用して、標準の 名前付き IP アクセス リストを定義します。
ステップ 5	**interface** *type number* 例：	インターフェイスを設定し、インターフェイス コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 6	**ip access-group** *access-list-number* {**in** | **out**} 例： `Device(config-if)# ip access-group 1 in`	指定した番号付きアクセス リストを着信または発信インターフェイスに適用します。 • 送信元アドレスに基づいてフィルタする場合、一般的に、着信インターフェイスにアクセス リストを適用します。
ステップ 7	**end** 例： `Device(config-if)# end`	インターフェイス コンフィギュレーション モードを終了し、特権 EXEC モードを開始します。

名前を使用した標準 IP アクセス リストの作成

手順の概要

1. **enable**
2. **configure terminal**
3. **ip access-list standard** *name*
4. {**deny** | **permit**} {**host** *address* | **any**} **log**
5. **exit**
6. **interface** *type number*
7. **ip access-group** *access-list-name* {**in** | **out**}
8. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ip access-list standard** *name* 例： `Device(config)# ip access-list standard acl1`	標準の IP アクセス リストを定義して、標準の名前付きアクセス リスト コンフィギュレーション モードを開始します。
ステップ 4	{**deny** | **permit**} {**host** *address* | **any**} **log** 例： `Device(config-std-nacl)# permit host 10.1.1.1 log`	パケットがネットワークに入らないように拒否したり、パケットがネットワークに入ることを許可したりする名前付き IP アクセス リストで条件を設定し、

	コマンドまたはアクション	目的
		デバイス コンソールでアクセス リスト エントリと一致するパケットに関する情報メッセージのロギングを設定します。
ステップ 5	**exit** 例： `Device(config-std-nacl)# exit`	標準の名前付きアクセス リスト コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードを開始します。
ステップ 6	**interface** *type number* 例：	インターフェイスを設定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 7	**ip access-group** *access-list-name* {**in** | **out**} 例： `Device(config-if)# ip access-group acl1 in`	指定したアクセス リストを着信または発信インターフェイスに適用します。 • 送信元アドレスに基づいてフィルタする場合、一般的に、着信インターフェイスにアクセス リストを適用します。
ステップ 8	**end** 例： `Device(config-if)# end`	インターフェイス コンフィギュレーション モードを終了し、特権 EXEC モードを開始します。

標準 IP アクセス リストのロギングの設定例

例：数字を使用した標準 IP アクセス リストの作成

```
Device# configure terminal
Device(config)# access-list 1 permit host 10.1.1.1 log
Device(config)# access-list 1 permit any log

Device(config-if)# ip access-group 1 in
```

例：名前を使用した標準 IP アクセス リストの作成

```
Device# configure terminal
Device(config)# ip access-list standard acl1
Device(config-std-nacl)# permit host 10.1.1.1 log
Device(config-std-nacl)# exit

Device(config-if)# ip access-group acl1 in
```

例：デバッグ出力の制限

次の設定例では、アクセス リストを使用して、**debug** コマンドの出力を制限します。**debug** の出力を制限すると、データ量が絞られ、目的のデータを探しやすくなるため、時間とリソースを節約できます。

```
Device(config)# ip access-list acl1
Device(config-std-nacl)# remark Displays only advertisements for LDP peer in acl1
Device(config-std-nacl)# permit host 10.0.0.44

Device# debug mpls ldp advertisements peer-acl acl1

tagcon: peer 10.0.0.44:0 (pp 0x60E105BC): advertise 172.17.0.33
tagcon: peer 10.0.0.44:0 (pp 0x60E105BC): advertise 172.16.0.31
tagcon: peer 10.0.0.44:0 (pp 0x60E105BC): advertise 172.22.0.33
tagcon: peer 10.0.0.44:0 (pp 0x60E105BC): advertise 192.168.0.1
tagcon: peer 10.0.0.44:0 (pp 0x60E105BC): advertise 192.168.0.3
tagcon: peer 10.0.0.44:0 (pp 0x60E105BC): advertise 192.168.1.33
```

標準 IP アクセス リストのロギングに関する追加情報

関連資料

関連項目	マニュアル タイトル
セキュリティ コマンド	• 『Cisco IOS Security Command Reference: Commands A to C』 • 『Cisco IOS Security Command Reference: Commands D to L』 • 『Cisco IOS Security Command Reference: Commands M to R』 • 『Cisco IOS Security Command Reference: Commands S to Z』

シスコのテクニカル サポート

説明	リンク
右の URL にアクセスして、シスコのテクニカル サポートを最大限に活用してください。これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

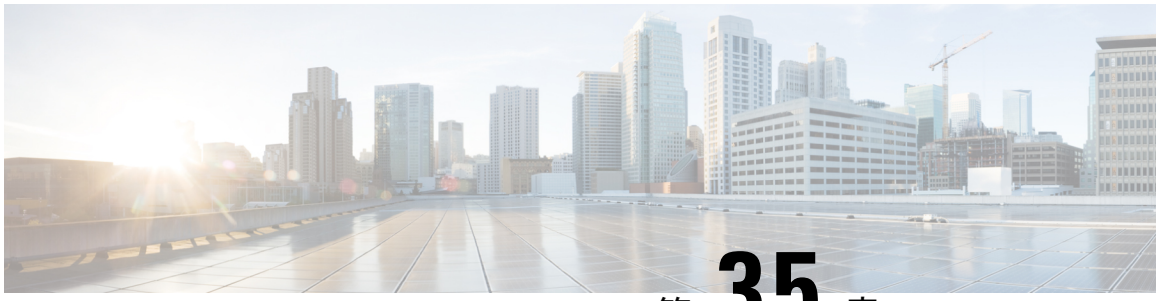
標準 IP アクセス リストのロギングに関する機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *56* : 標準 *IP* アクセス リストのロギングに関する機能情報

機能名	リリース	機能情報
標準 IP アクセス リストのロギング		標準 IP アクセス リストのロギング機能は、標準 IP アクセス リストによって許可または拒否されるパケットに関するメッセージをロギングする機能を提供します。アクセス リストに一致するパケットによって、デバイス コンソールにあるパケットに関する情報メッセージがロギングされます。



第 35 章

IP アクセス リスト エントリ シーケンス番号

IP アクセス リスト エントリ シーケンス番号機能により、**permit** または **deny** ステートメントにシーケンス番号を適用したり、名前付き IP アクセス リストでそのようなステートメントを順序変更、追加、削除することができます。IP アクセス リスト エントリ シーケンス番号機能を使用すると、IP アクセス リストを非常に簡単に変更することができます。この機能以前は、アクセス リストの末尾にしかアクセス リスト エントリを追加できませんでした。そのため、名前付き IP アクセス リストの末尾以外のどこかにステートメントを追加する必要がある場合、アクセス リスト全体の再設定が必要でした。

IP アクセス リストのエントリ シーケンス番号に関する制約事項

- この機能は、ダイナミック アクセス リスト、再帰アクセス リスト、またはファイアウォール アクセス リストをサポートしていません。
- また、名前付きアクセス リストよりも古くから存在する、旧式のスタイルで番号付けされたアクセス リストもサポートしていません。アクセス リストは番号で指定できるため、標準または拡張名前付きアクセス リスト（NACL）コンフィギュレーション モードでは番号を入力することができます。

IPアクセス リストのエントリ シーケンス番号に関する情報

IP アクセス リストの目的

アクセス リストは、パケット フィルタリングを実行して、ネットワークを介して移動するパケットとその場所を制御します。この処理は、ネットワーク トラフィックを制限し、ユーザやデバイスによるネットワークへのアクセスを制限するのに役立ちます。アクセス リストの用途は多様なので、多くのコマンドシンタックスでアクセス リストが参照されます。アクセス リストを使用して、次のようなことを実行できます。

- インターフェイスでの着信パケットのフィルタリング
- インターフェイスでの発信パケットのフィルタリング
- ルーティング アップデートの内容の制限
- アドレスまたはプロトコルに基づくデバッグ出力の制限
- 仮想端末回線アクセスの制御
- 輻輳回避、輻輳管理、プライオリティおよびカスタム キューイングなどの高度な機能に使用されるトラフィックの特定または分類
- ダイヤルオンデマンド ルーティング（DDR）呼び出しのトリガー

IP アクセス リストの機能

アクセス リストは、permit ステートメントと deny ステートメントで構成される順次リストです。これらのステートメントは、IP アドレス、場合によっては上位層 IP プロトコルに適用されます。アクセス リストには、参照に使用される名前があります。多くのソフトウェア コマンドは、構文の一部としてアクセス リストを受け取ります。

アクセス リストを設定して名前を付けることは可能ですが、アクセス リストを受け取るコマンドによってアクセス リストが参照されるまで、有効にはなりません。複数のコマンドから同じアクセス リストを参照できます。アクセス リストで、デバイスに到達するトラフィック、またはデバイス経由で送信されるトラフィックは制御できますが、デバイスが送信元のトラフィックは制御できません。

IP アクセス リストのプロセスとルール

- アクセス リストの条件に対してフィルタリングされる各パケットの送信元アドレスや宛先アドレス、またはプロトコルがテストされます。一度に 1 つの条件（**permit** ステートメントまたは **deny** ステートメント）がテストされます。

- パケットがアクセスリストのステートメントに一致しないと、そのパケットはリスト内の次のステートメントに対してテストされます。
- パケットとアクセス リスト ステートメントが一致すると、リスト内の残りのステートメントはスキップされ、パケットは一致したステートメントに指定されたとおりに許可または拒否されます。パケットが許可されるか拒否されるかは、パケットが一致する最初のエントリによって決まります。つまり、一致すると、それ以降のエントリは考慮されません。
- アクセスリストでアドレスまたはプロトコルが拒否されると、パケットは廃棄され、インターネット制御メッセージプロトコル（ICMP）ホスト到達不能メッセージが返されます。
- 一致する条件がない場合は、パケットはドロップされます。これは、各アクセスリストは暗黙の **deny** ステートメントで終了するためです。言い換えると、パケットが各ステートメントに対してテストされたときまでに許可されないと、このパケットは拒否されます。
- 最初に一致が見つかった後は条件のテストが終了するため、条件の順序は重要です。同じ **permit** ステートメントまたは **deny** ステートメントでも、順序が異なる場合、ある状況では通過し、別の状況では拒否されるパケットが生じる可能性があります。
- コマンドでアクセス リストを名前によって参照したときに、そのアクセス リストが存在しない場合は、すべてのパケットが通過します。
- 1 つのインターフェイス、1 つのプロトコル、1 つの方向につき、許可されるアクセス リストは 1 つだけです。
- インバウンドアクセスリストは、デバイスに到達するパケットを処理します。着信パケットの処理後に、アウトバウンドインターフェイスへのルーティングが行われます。インバウンドアクセスリストが効率的なのは、フィルタリングテストで拒否されたことでパケットが廃棄される場合、ルーティング検索のオーバーヘッドが抑えられるためです。パケットがテストで許可されると、そのパケットに対してルーティングの処理が実施されます。インバウンド リストの場合、**permit** とは、インバウンド インターフェイスでパケットの受信後に処理が続行されることを示します。**deny** とは、パケットが廃棄されることを示します。
- 発信アクセスリストの場合、パケットの処理後にデバイスから送信されます。着信パケットはアウトバウンド インターフェイスにルーティングされてから、アウトバウンド アクセス リストで処理されます。アウトバウンド リストの場合、**permit** とは、出力バッファに対して送信されることを示し、**deny** とは、パケットが廃棄されることを示します。

IP アクセス リストを作成する際に役立つヒント

意図しない結果を回避し、より効率的で有効なアクセスリストを作成するために役立つヒントを紹介します。

- アクセスリストを作成してから、インターフェイス（または別の対象）に適用します。その理由は、存在しないアクセス リストをインターフェイスに適用してから、アクセス リ

ストを設定すると、最初のステートメントが有効になり、それに続く暗黙的な **deny** ステートメントによってアクセスに緊急の問題が発生するおそれがあるためです。

- アクセス リストを設定してから適用するもう 1 つの理由は、空のアクセス リストが適用されたインターフェイスはすべてのトラフィックを許可するためです。
- すべてのアクセス リストには、少なくとも 1 つの **permit** ステートメントが必要です。permit がないと、すべてのパケットは拒否され、トラフィックはまったく通過しません。
- 最初に（**permit** または **deny** ステートメントに対する）一致が見つかった後は条件のテストが終了するため、パケットが一致する可能性の高いステートメントをアクセス リストの先頭に配置すると処理にかかる時間とリソースが削減されます。最も頻繁に発生する条件を発生頻度の低い条件より前に配置します。
- ネットワークまたはサブネットのより具体的な参照が、より全般的な参照よりも前に出現するように、アクセス リストを構成します。
- まだ拒否されていないその他のパケットすべてを許可する場合、ステートメント **permit any any** を使用します。ステートメント **permit any any** を使用すると、実質的に、アクセス リストの末尾にある暗黙的な deny ステートメントでその他すべてのパケットが拒否されることを防ぎます。最初のアクセス リスト エントリは **permit any any** にしないでください。すべてのトラフィックが通過し、以降のテストに到達するパケットがなくなります。**permit any any** を指定すると、まだ拒否されていないすべてのトラフィックが通過します。
- すべてのアクセス リストは暗黙的な **deny** ステートメントで終了しますが、明示的な **deny** ステートメント（たとえば **deny ip any any**）の使用を推奨します。ほとんどのプラットフォームでは、**show access-list**コマンドを発行して拒否されるパケット数を表示し、アクセス リストが許可していないパケットに関する詳細情報を調査できます。明示的な **deny** ステートメントで拒否されたパケットのみがカウントされます。これは、明示的な **deny** ステートメントによって、より詳細なデータが生成されるためです。
- アクセス リストの作成中、または作成後に、エントリを削除する場合があります。
  - 番号付きアクセス リストからはエントリを削除できません。削除しようとすると、アクセス リスト全体が削除されます。エントリを削除する必要がある場合、アクセス リスト全体を削除してから最初から作り直す必要があります。
  - 名前付きアクセス リストからはエントリを削除できます。**no permit**または **no deny** コマンドを使用すると、適切なエントリが削除されます。
- 個々のステートメントの用途をひと目で確認および理解しやすくするために、**remark** コマンドを使用して、ステートメントの前後に役立つ注記を書き込むことができます。
- 特定のホストまたはネットワークに対するアクセスを拒否し、そのネットワークまたはホストの誰かがアクセスしようとしたかどうかを検出する場合、対応する **deny** ステートメントを指定した **log** キーワードを含めます。それによって、その送信元からの拒否されたパケットがログに記録されます。
- このヒントは、アクセス リストの配置に適用されます。リソースを保存しようとすると、インバウンドアクセスリストでは常にフィルタ条件を適用した後に、ルーティングテーブ

ルの検索を行います。アウトバウンドアクセス リストではフィルタ条件を適用する前に、ルーティング テーブルの検索を行います。

- 新しい ACL ステートメントを追加する前に、パーサーが削除をクリーンアップする時間を確保します。

送信元アドレスと宛先アドレス

IP パケットの送信元アドレスと宛先アドレスのフィールドは、アクセス リストの基礎となる典型的な2つのフィールドです。送信元アドレスを指定して、特定のネットワーキング デバイスまたはホストから送信されるパケットを制御します。宛先アドレスを指定して、特定のネットワーキング デバイスまたはホストに送信されるパケットを制御します。

ワイルドカード マスクおよび暗黙のワイルドカード マスク

アドレス フィルタリングでは、アクセス リスト エントリ内のアドレス ビットとアクセス リストに送信されるパケットを比較する際、対応する IP アドレス ビットを確認するか無視するかを決定するために、ワイルドカード マスクが使用されます。管理者は、ワイルドカード マスクを慎重に設定することにより、許可または拒否のテストに 1 つまたは複数の IP アドレスを選択できます。

IP アドレス ビット用のワイルドカード マスクでは、数値 1 と数値 0 を使用して、対応する IP アドレス ビットをどのように扱うかを指定します。1 と 0 は、サブネット（ネットワーク）マスクで意味する内容が対照的なため、ワイルドカード マスクは逆マスクとも呼ばれます。

- ワイルドカード マスク ビット 0 は、対応するビット値を確認することを示します。
- ワイルドカード マスク ビット 1 は、対応するビット値を無視することを示します。

アクセス リスト ステートメントの送信元アドレスまたは宛先アドレスでワイルドカード マスクを指定しない場合、0.0.0.0 というデフォルトのワイルドカード マスクが想定されます。

サブネット マスクでは、ネットワークとサブネットを示す隣接ビットをマスクにする必要がありますが、それとは異なり、ワイルドカード マスクではマスクに非隣接ビットを使用できます。

トランスポート層の情報

トランスポート層の情報（パケットが TCP、UDP、Internet Control Message Protocol（ICMP）または Internet Group Management Protocol（IGMP）パケットであるか、などの情報）に基づいてパケットをフィルタできます。

利点：IP アクセス リスト エントリ シーケンス番号

IP アクセス リスト エントリにシーケンス番号を適用する機能によって、アクセス リストの変更が簡易になります。IP アクセス リスト エントリ シーケンス番号機能の前には、アクセス リ

スト内のエントリの位置を指定する方法はありませんでした。既存のリストの途中にエントリ（ステートメント）を挿入するには、目的の位置の後ろにあるすべてのエントリを削除する必要がありました。次に、新しいエントリを追加したら、先に削除したすべてのエントリを再入力する必要がありました。これは手間がかかり、エラーが起こりやすい方法です。

IP アクセス リスト エントリ シーケンス番号機能を使用すると、アクセス リスト エントリにシーケンス番号を追加し、リスト内のエントリを並べ替えることができます。新しいエントリを追加する場合、アクセスリストの目的の位置にエントリが挿入されるようにシーケンス番号を選択できます。必要に応じて、アクセスリストの現在のエントリを並べ替えて、新しいエントリを挿入できる場所を作成できます。

シーケンス番号の動作

- 以前のリリースとの下位互換性を保つため、シーケンス番号のないエントリが適用された場合には、最初のエントリにはシーケンス番号 10 が割り当てられます。連続してエントリを追加すると、シーケンス番号は10ずつ増分されます。最大シーケンス番号は2147483647です。生成したシーケンス番号がこの最大値を超えると、次のメッセージが表示されます。

```
Exceeded maximum sequence number.
```

- シーケンス番号のないエントリを1つ入力すると、アクセスリストの最後のシーケンス番号に 10 を加えたシーケンス番号が割り当てられ、リストの末尾に配置されます。
- （シーケンス番号以外が）既存のエントリに一致するエントリを入力すると、何も変更されません。
- 既存のシーケンス番号を入力すると、次のエラー メッセージが表示されます。

```
Duplicate sequence number.
```

- グローバル コンフィギュレーション モードで新しいアクセス リストを入力すると、そのアクセス リストのシーケンス番号が自動的に生成されます。
- 完全修飾32ビットホストアドレスを含むエントリは、リンクされずにハッシュされます。また、サブネットを定義するエントリは、ACL分類の迅速化のために、シーケンス番号でソートされたリンクリストで維持されます。パケットが標準 ACL と照合されると、送信元アドレスがハッシュされ、ハッシュテーブルと照合されます。一致するものが見つからない場合は、リンクリストで一致する可能性のあるものが検索されます。
- ルート プロセッサ（RP）のエントリとラインカード（LC）のエントリのシーケンス番号を常に同期できるように、分散機能がサポートされています。
- シーケンス番号が不揮発性生成（NVGEN）されることはありません。つまり、シーケンス番号自体は保存されません。システムのリロード時には、設定されたシーケンス番号はデフォルトのシーケンス開始番号とその番号からの増分に戻されます。この機能は、シーケンス番号をサポートしないソフトウェア リリースとの下位互換性を保つために提供されています。

- IP アクセス リスト エントリ シーケンス番号機能では、名前付き標準アクセス リストと拡張 IP アクセス リストが使用されます。アクセス リストの名前を番号として指定できるため、番号も使用できます。

IP アクセス リストでのシーケンス番号の使用法

アクセス リスト エントリの順序付けとアクセス リストの変更

ここでは、名前付き IP アクセス リストのエントリにシーケンス番号を割り当てる方法と、アクセス リストに対するエントリの追加または削除を行う方法を説明します。この作業を実行する場合は、次の点に注意してください。

- アクセス リスト エントリの並べ替えは任意です。この作業での並べ替えのステップは、機能の目的の 1 つであり、またその機能の説明が必要と思われることから、必要に応じて説明します。
- 次の手順で、**permit** コマンドはステップ 5 に、**deny** コマンドはステップ 6 に記載されています。ただし、その順番を入れ替えることもできます。設定のニーズに合わせた順番を使用します。

手順の概要

1. **enable**
2. **configure terminal**
3. **ip access-list resequence** *access-list-name starting-sequence-number increment*
4. **ip access-list** {**standard**| **extended**} *access-list-name*
5. 次のいずれかを実行します。
   - *sequence-number* **permit** *source source-wildcard*
   - *sequence-number* **permit** *protocol source source-wildcard destination destination-wildcard* [**precedence** *precedence*][**tos** *tos*] [**log**] [**time-range** *time-range-name*] [**fragments**]
6. 次のいずれかを実行します。
   - *sequence-number* **deny** *source source-wildcard*
   - *sequence-number* **deny** *protocol source source-wildcard destination destination-wildcard* [**precedence** *precedence*][**tos** *tos*] [**log**] [**time-range** *time-range-name*] [**fragments**]
7. 次のいずれかを実行します。
   - *sequence-number* **permit** *source source-wildcard*
   - *sequence-number* **permit** *protocol source source-wildcard destination destination-wildcard* [**precedence** *precedence*][**tos** *tos*] [**log**] [**time-range** *time-range-name*] [**fragments**]
8. 次のいずれかを実行します。
   - *sequence-number* **deny** *source source-wildcard*

- *sequence-number* **deny** *protocol source source-wildcard destination destination-wildcard* [**precedence** *precedence*][**tos** *tos*] [**log**] [**time-range** *time-range-name*] [**fragments**]

9. 必要に応じてシーケンス番号ステートメントを追加するには、ステップ 5 とステップ 6 を繰り返します。
10. **end**
11. **show ip access-lists** *access-list-name*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ip access-list resequence** *access-list-name starting-sequence-number increment* 例： `Device(config)# ip access-list resequence kmd1 100 15`	開始シーケンス番号と、シーケンス番号の増分を使用して、指定した IP アクセス リストを並べ替えます。
ステップ 4	**ip access-list** {**standard**| **extended**} *access-list-name* 例： `Device(config)# ip access-list standard kmd1`	名前で IP アクセス リストを指定し、名前付きアクセス リストのコンフィギュレーション モードを開始します。 • **standard** を指定する場合は、その後に、標準アクセス リスト構文を使用して **permit** ステートメントまたは **deny** ステートメントを指定します。 • **extended** を指定する場合は、その後に、拡張アクセス リスト構文を使用して **permit** ステートメントまたは **deny** ステートメントを指定します。
ステップ 5	次のいずれかを実行します。 • *sequence-number* **permit** *source source-wildcard* • *sequence-number* **permit** *protocol source source-wildcard destination destination-wildcard* [	名前付き IP アクセス リスト モードで permit ステートメントを指定します。 • このアクセス リストでは **permit** ステートメントを最初に使用していますが、必要なステート

	コマンドまたはアクション	目的
	precedence *precedence*][**tos** *tos*] [**log**] [**time-range** *time-range-name*] [**fragments**] 例： `Device(config-std-nacl)# 105 permit 10.5.5.5 0.0.0 255`	メントの順序に応じて、**deny** ステートメントが最初に使用される可能性もあります。 • プロンプトに示されるとおり、このアクセス リストは標準アクセス リストでした。ステップ4で**extended**を指定した場合は、このステップのプロンプトは Device(config-ext-nacl) となり、拡張 **permit** コマンドシンタックスを使用します。
ステップ6	次のいずれかを実行します。 • *sequence-number* **deny** *source source-wildcard* • *sequence-number* **deny** *protocol source source-wildcard destination destination-wildcard* [**precedence** *precedence*][**tos** *tos*] [**log**] [**time-range** *time-range-name*] [**fragments**] 例： `Device(config-std-nacl)# 105 deny 10.6.6.7 0.0.0 255`	（任意）名前付き IP アクセス リスト モードで deny ステートメントを指定します。 • このアクセス リストでは **permit** ステートメントを最初に使用していますが、必要なステートメントの順序に応じて、**deny** ステートメントが最初に使用される可能性もあります。 • プロンプトに示されるとおり、このアクセス リストは標準アクセス リストでした。ステップ4で**extended**を指定した場合は、このステップのプロンプトは Device(config-ext-nacl) となり、拡張 **deny** コマンドシンタックスを使用します。
ステップ7	次のいずれかを実行します。 • *sequence-number* **permit** *source source-wildcard* • *sequence-number* **permit** *protocol source source-wildcard destination destination-wildcard* [**precedence** *precedence*][**tos** *tos*] [**log**] [**time-range** *time-range-name*] [**fragments**] 例： `Device(config-ext-nacl)# 150 permit tcp any any log`	名前付き IP アクセス リスト モードで permit ステートメントを指定します。 • このアクセス リストでは **permit** ステートメントを最初に使用していますが、必要なステートメントの順序に応じて、**deny** ステートメントが最初に使用される可能性もあります。 • 上位層プロトコル（ICMP、IGMP、TCP、およびUDP）を許可するその他のコマンドシンタックスについては、permit（IP）コマンドを参照してください。 • エントリを削除するには、**no** *sequence-number* コマンドを使用します。
ステップ8	次のいずれかを実行します。 • *sequence-number* **deny** *source source-wildcard* • *sequence-number* **deny** *protocol source source-wildcard destination destination-wildcard* [	（任意）名前付き IP アクセス リスト モードで deny ステートメントを指定します。 • このアクセス リストでは **permit** ステートメントを最初に使用していますが、必要なステート

	コマンドまたはアクション	目的
	precedence *precedence*][**tos** *tos*] [**log**] [**time-range** *time-range-name*] [**fragments**] 例： `Device(config-ext-nacl)# 150 deny tcp any any log`	メントの順序に応じて、**deny** ステートメントが最初に使用される可能性もあります。 • 上位層プロトコル（ICMP、IGMP、TCP、およびUDP）を許可するその他のコマンドシンタックスについては、deny（IP）コマンドを参照してください。 • エントリを削除するには、**no** *sequence-number* コマンドを使用します。
ステップ 9	必要に応じてシーケンス番号ステートメントを追加するには、ステップ 5 とステップ 6 を繰り返します。	アクセス リストは変更できます。
ステップ 10	**end** 例： `Device(config-std-nacl)# end`	（任意）コンフィギュレーションモードを終了し、特権 EXEC モードに戻ります。
ステップ 11	**show ip access-lists** *access-list-name* 例： `Device# show ip access-lists kmd1`	（任意）IP アクセス リストの内容を表示します。

例

アクセス リストに新しいエントリが含まれていることを確認するには、**show ip access-lists** コマンドの出力を確認します。

```
Device# show ip access-lists kmd1

Standard IP access list kmd1
100 permit 10.4.4.0, wildcard bits 0.0.0.255
105 permit 10.5.5.0, wildcard bits 0.0.0.255
115 permit 10.0.0.0, wildcard bits 0.0.0.255
130 permit 10.5.5.0, wildcard bits 0.0.0.255
145 permit 10.0.0.0, wildcard bits 0.0.0.255
```

IP アクセス リスト エントリ シーケンス番号の設定例

例：アクセス リストのエントリの並べ替え

次に、アクセス リストを並べ替える例を示します。開始値は 1、増分値は 2 です。後続のエントリは指定の増分値に基づいて並べられています。範囲は 1 ～ 2147483647 です。

シーケンス番号のないエントリが入力されると、デフォルトで、アクセス リストの最後のエントリのシーケンス番号に 10 を加えたシーケンス番号が割り当てられます。

```
Device# show access-list 150

Extended IP access list 150
    10 permit ip host 10.3.3.3 host 172.16.5.34
    20 permit icmp any any
    30 permit tcp any host 10.3.3.3
    40 permit ip host 10.4.4.4 any
    50 Dynamic test permit ip any any
    60 permit ip host 172.16.2.2 host 10.3.3.12
    70 permit ip host 10.3.3.3 any log
    80 permit tcp host 10.3.3.3 host 10.1.2.2
    90 permit ip host 10.3.3.3 any
    100 permit ip any any

Device(config)# ip access-list extended 150
Device(config)# ip access-list resequence 150 1 2
Device(config)# exit

Device# show access-list 150

Extended IP access list 150
    1 permit ip host 10.3.3.3 host 172.16.5.34
    3 permit icmp any any
    10 permit tcp any any eq 22 log
    5 permit tcp any host 10.3.3.3
    7 permit ip host 10.4.4.4 any
    9 Dynamic test permit ip any any
    11 permit ip host 172.16.2.2 host 10.3.3.12
    13 permit ip host 10.3.3.3 any log
    15 permit tcp host 10.3.3.3 host 10.1.2.2
    17 permit ip host 10.3.3.3 any
    19 permit ip any any
```

例：シーケンス番号を持つエントリの追加

次に、指定のアクセス リストに新しいエントリを追加する例を示します。

```
Device# show ip access-list

Standard IP access list tryon
2 permit 10.4.4.2, wildcard bits 0.0.255.255
5 permit 10.0.0.44, wildcard bits 0.0.0.255
10 permit 10.0.0.1, wildcard bits 0.0.0.255
20 permit 10.0.0.2, wildcard bits 0.0.0.255
```

```
Device(config)# ip access-list standard tryon
Device(config-std-nacl)# 15 permit 10.5.5.5 0.0.0.255
Device(config-std-nacl)# exit
Device(config)# exit
Device# show ip access-list

Standard IP access list tryon
2 permit 10.4.0.0, wildcard bits 0.0.255.255
5 permit 10.0.0.0, wildcard bits 0.0.0.255
10 permit 10.0.0.0, wildcard bits 0.0.0.255
15 permit 10.5.5.0, wildcard bits 0.0.0.255
20 permit 10.0.0.0, wildcard bits 0.0.0.255
```

例：シーケンス番号のないエントリ

次に、シーケンス番号が指定されていないエントリをアクセス リストの末尾に追加する方法を示します。シーケンス番号のないエントリを追加すると、自動的にシーケンス番号が割り当てられ、アクセス リストの末尾に配置されます。デフォルトの増分値は 10 であるため、エントリには、既存のアクセス リストの最後のエントリのシーケンス番号に 10 を加えたシーケンス番号が割り当てられます。

```
Device(config)# ip access-list standard 1
Device(config-std-nacl)# permit 10.1.1.1 0.0.0.255
Device(config-std-nacl)# permit 10.2.2.2 0.0.0.255
Device(config-std-nacl)# permit 10.3.3.3 0.0.0.255
Device(config-std-nacl)## exit
Device# show access-list

Standard IP access list 1
10 permit 0.0.0.0, wildcard bits 0.0.0.255
20 permit 0.0.0.0, wildcard bits 0.0.0.255
30 permit 0.0.0.0, wildcard bits 0.0.0.255

Device(config)# ip access-list standard 1
Device(config-std-nacl)# permit 10.4.4.4 0.0.0.255
Device(config-std-nacl)# end
Device(config-std-nacl)## exit
Device# show access-list

Standard IP access list 1
10 permit 0.0.0.0, wildcard bits 0.0.0.255
20 permit 0.0.0.0, wildcard bits 0.0.0.255
30 permit 0.0.0.0, wildcard bits 0.0.0.255
40 permit 0.0.0.0, wildcard bits 0.0.0.255
```

その他の参考資料

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『Cisco IOS Master Commands List, All Releases』

関連項目	マニュアル タイトル
セキュリティ コマンド：コマンド構文の詳細、コマンド モード、コマンド履歴、デフォルト設定、使用上のガイドライン、および例	『*Cisco IOS Security Command Reference*』
セキュア シェル	セキュア シェルおよびセキュア シェル バージョン 2 サポート設定の機能モジュール。
認証と認可の設定	認証設定、認可設定、およびアカウンティング設定の機能モジュール。

標準

標準	タイトル
なし	--

MIB

MIB	MIB のリンク
なし	選択したプラットフォーム、Cisco ソフトウェア リリース、およびフィーチャ セットの MIB を検索してダウンロードする場合は、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

RFC

RFC	タイトル
この機能によりサポートされた新規 RFC または改訂 RFC はありません。またこの機能による既存 RFC のサポートに変更はありません。	--

シスコのテクニカル サポート

説明	リンク
右の URL にアクセスして、シスコのテクニカル サポートを最大限に活用してください。これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

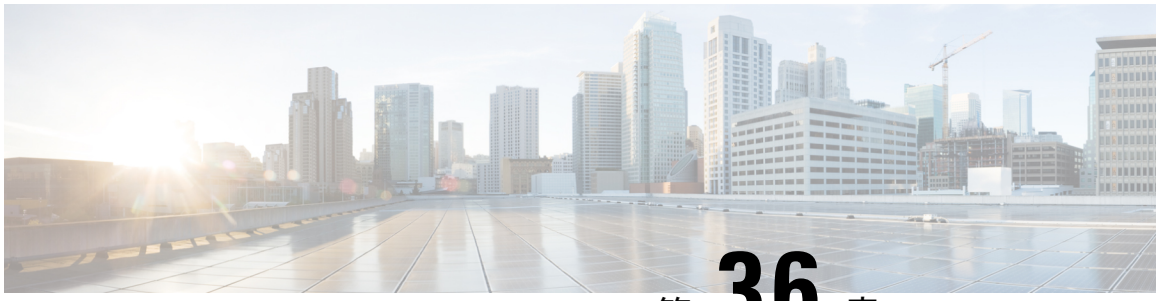
IP アクセス リスト エントリ シーケンス番号に関する機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *57 : IP* アクセス リスト エントリ シーケンス番号に関する機能情報

機能名	リリース	機能情報
IP アクセス リスト エントリ シーケンス番号		**permit** または **deny** ステートメントにシーケンス番号を適用し、名前付き IP アクセス リストで、該当するステートメントの再整理、追加、または削除を行うことができます。この機能により、IP アクセス リストを簡単に変更できるようになります。この機能が実装される前は、アクセス リストの最後にエントリを追加することしかできませんでした。そのため、末尾以外の任意の場所にステートメントを追加する必要があるときは、アクセス リスト全体を再設定する必要がありました。 では、Cisco Catalyst 3850 シリーズ スイッチのサポートが追加されました。 次のコマンドが導入または変更されました。**deny (IP)**、**ip access-list resequence deny (IP), permit (IP)**



第 36 章

ロック アンド キー セキュリティの設定（ダイナミックアクセス リスト）

機能の履歴

リリース	変更内容
Cisco IOS	Cisco IOS ソフトウェアの機能サポートに関する情報については、Cisco Feature Navigator を使用してください。

この章では、ルータでロックアンドキー セキュリティを設定する方法について説明します。ロック アンド キーは、IP プロトコルで使用可能なトラフィック フィルタリング セキュリティ機能です。

ロック アンド キー コマンドの詳細な説明については、『*Cisco IOS* セキュリティ コマンド リファレンス』を参照してください。この章で使用されたその他のコマンドの詳細については、コマンド リファレンス マスタ インデックスを使用するか、オンラインで検索してください。

機能に関連付けられたハードウェア プラットフォームまたはソフトウェア イメージの情報を識別するには、Cisco.com の Feature Navigator を使用して機能についての情報を検索するか、特定のリリースのソフトウェア リリースノートを参照してください。

ロック アンド キーの設定の必須条件

ロック アンド キーは、IP 拡張アクセス リストを使用します。ロック アンド キーを設定しようとする前に、アクセス リストを使用してトラフィックをフィルタする方法について確実に理

解する必要があります。アクセス リストについては、「アクセス コントロール リスト：概要および指針」を参照してください。

ロックアンドキーは、Ciscoの認証、許可、アカウンティング（AAA）の枠組みで実装されているように、ユーザー認証と認可を使用します。ロック アンド キーを設定する前に、AAA ユーザー認証、許可、アカウンティングの設定方法について理解する必要があります。ユーザー認証および認可は、本書の「認証、認可、アカウンティング（AAA）」のセクションで説明します。

ロック アンド キーは、理解する必要のある **autocommand** コマンドを使用します。このコマンドは、『Cisco IOS Terminal *Services* コマンド リファレンス』を参照してください。

ロック アンド キー セキュリティ（ダイナミック アクセス リスト）の設定に関する情報

ロック アンド キーについて

ロック アンド キーは、IP プロトコル トラフィックを動的にフィルタするトラフィック フィルタリング セキュリティ機能です。ロック アンド キーは、IP ダイナミック拡張アクセス リストを使用して設定されます。ロック アンド キーは、その他の標準アクセス リストとスタティック拡張アクセス リストと共に使用できます。

ロック アンド キーが設定されると、IP トラフィックが通常ルータではブロックされる指定されたユーザーは、ルータ経由で一時的なアクセスを得ることができます。起動されると、ロック アンド キーは、指定されたユーザーに指定されたホストに到達することを許可するよう、インターフェイスの既存の IP アクセス リストを再設定します。その後、ロック アンド キーは、インターフェイスを元の状態に戻すよう、再設定します。

ユーザーがロック アンド キーが設定されたルータを介してホストへのアクセスできるようにするため、ユーザーは、最初にルータに Telnet セッションを開く必要があります。ユーザーがルータに標準 Telnet セッションを開始すると、ロック アンド キーは、自動的にユーザーを認証しようとします。ユーザーが認証されると、ルータを通じて、一時的なアクセスを取得し、宛先ホストに到達できます。

ロック アンド キーの利点

ロックアンドキーは、標準およびスタティック拡張アクセスリストと同じ利点があります（これらの利点については、「アクセス コントロール リスト：概要および指針」で説明します）。ただし、ロック アンド キーには、標準およびスタティック拡張アクセス リストに比べ、次の利点もあります。

- ロック アンド キーは、個々のユーザーを認証するために実験機能を使用します。
- ロック アンド キーは、より大きなインターネットワークにおけるより簡素な管理を提供します。

- 多くの場合、ロック アンド キーは、アクセス リストに必要なルータ処理の量を減らします。
- ロック アンド キーは、ネットワーク ハッカーが、ネットワークへの侵入する可能性を減らします。

ロック アンド キーを使用すると、送信元および宛先がホストとなるアクセスをどのユーザーに許可するかを指定できます。これらのユーザーは、指定されたホストへのアクセスが許可される前に、ユーザー認証プロセスをパスする必要があります。ロック アンド キーは、その他の設定されたセキュリティ制約事項を損なうことなく、ファイアウォールを通じてダイナミック ユーザー アクセスを作成します。

ロック アンド キーを使用するタイミング

ロック アンド キーを使用するタイミングの 2 つの例を以下に示します。

- 特定のリモート ユーザー（またはリモート ユーザーのグループに）が、インターネットを介して、そのリモートホストから接続して、ネットワーク内のホストへのアクセスを必要とする場合。ロック アンド キーは、ユーザーを認証し、次に、個々のホストまたはサブネットに対して、限られた時間の間、ファイアウォールを介した限られたアクセスを許可します。
- ローカル ネットワーク上のホストのサブセットがファイアウォールによって保護されたリモート ネットワーク上のホストにアクセスする必要がある場合。ロック アンド キーを使用すると、ローカル ユーザーが必要とするホストのセットに対してのみリモート ホストへのアクセスを有効にすることができます。ロック アンド キーは、ホストがリモート ホスト リモートへアクセスすることを許可する前に、ユーザーが TACACS+ サーバー、もしくはその他のサーバーを通じて、認証を行うことを必要とします。

ロック アンド キーの機能

次のプロセスは、ロック アンド キー アクセスの動作を説明します。

1. ユーザーは、ロック アンド キー用に設定された境界（ファイアウォール）ルータへの Telnet セッションを開きます。ユーザーは、ルータ上の仮想端末ポートを介して接続します。
2. Cisco IOS ソフトウェアは、Telnet パケットを受信し、Telnet セッションを開いてパスワードを要求し、ユーザー認証プロセスを実行します。ユーザーは、ルータを介したアクセスが許可される前に、認証をパスする必要があります。認証プロセスは、ルータ、または TACACS+ または RADIUS サーバーなどの中央アクセス セキュリティ サーバーで実行することもできます。
3. ユーザーが認証をパスすると、Telnet セッションからログアウトし、ソフトウェアがダイナミック アクセス リストに一時的なエントリを作成します。（設定ごとに、この一時エントリは、ユーザーが一時的なアクセスを与えられるネットワークの範囲を制限できます。）

4. ユーザーは、ファイアウォール経由でのデータを交換します。
5. ソフトウェアは、設定されているタイムアウトに到達するか、システム管理者が手動でクリアした場合に、一時的なアクセス リスト エントリを削除します。設定されているタイムアウトは、アイドルタイムアウトまたは絶対タイムアウトのいずれかになることがあります。

（注） ユーザーがセッションを終了させた場合、一時アクセス リスト エントリは、自動的に削除されません。一時アクセスリストのエントリは、設定されているタイムアウトに到達するか、システム管理者がクリアされるまで保持されます。

Cisco IOS リリース 11.1 以前のリリースとの互換性

access-list コマンドの拡張機能は、ロック アンド キーに使用されます。これらの機能拡張は、下位互換性があります。Cisco IOS リリース 11.1 以前のリリースから新しいリリースに移行する場合、アクセスリストは、機能拡張を反映するために、自動的に変換されます。ただし、次の注意の項で説明されているように、Cisco IOS リリース 11.1 以前のリリースでロック アンド キーを使用しようとすると、問題が発生する可能性があります。

注意 Cisco IOS リリース 11.1 以前のリリースは、ロック アンド キー アクセス リスト拡張機能と互換性がありません。そのため、リリース 11.1 以前のソフトウェアでアクセス リストを保存し、このソフトウェアを使用する場合、作成されたアクセスリストは、正しく解釈されません。これによって、深刻なセキュリティ上の問題が発生する可能性があります。これらのファイルと共に画像をブートする前に、Cisco IOS リリース 11.1 以降のソフトウェアを使用して、古い設定ファイルを保存する必要があります。

ロック アンド キーによるスプーフィングのリスク

注意 ロック アンド キー アクセスを使用すると、外部イベント（Telnet セッション）がファイアウォールに穴を開けることができます。この穴がある間、ルータは、送信元アドレスのスプーフィングを受ける可能性があります。

ロック アンド キー が起動されると、ユーザー アクセスを許可するインターフェイスを一時的に再設定することで、ファイアウォール内に動的な穴が作成されます。この穴がある間は、別のホストが認証済みのユーザーのアドレスを偽装し、ファイアウォールの裏でのアクセスを獲得する可能性があります。ロック アンド キーは、アドレス スプーフィングの問題を発生させません。この問題は、ユーザーの関心事としてここに特定されるだけです。スプーフィングは、すべてのアクセス リストに伴う問題であり、ロック アンド キーは、この問題に具体的に対処していません。

スプーフィングを防ぐには、リモート ホストからのトラフィックがセキュアなリモート ルータで暗号化され、ロック アンド キーを提供するルータ インターフェイス上でローカルで復号化されるように暗号化を設定します。ルータの入力時に、ロック アンド キーを使用して、すべてのトラフィックを暗号化したい場合、ハッカーは、それらが暗号化を複製できないか、暗号化のセットアップ プロセスの必要な部分として認証できないため、送信元アドレスをスプーフィングすることはできません。

ロック アンド キーによるルータのパフォーマンスへの影響

ロック アンド キーを設定すると、ルータのパフォーマンスは、次のように影響を受ける場合があります。

- ロック アンド キーが起動されると、ダイナミック アクセス リストは、シリコン スイッチング エンジン（SSE）上でのアクセス リストの再構成が強制されます。これによって、SSE スイッチング パスが一瞬低速になります。
- ダイナミック アクセス リストは、アイドル タイムアウト機能（タイムアウトがデフォルトになったとしても）を必要とし、SSE スイッチングにすることはできません。これらのエントリは、プロトコル ファスト スイッチング パスで処理する必要があります。
- リモート ユーザーが境界ルータでロック アンド キーを起動すると、追加のアクセス リスト エントリが境界ルータ インターフェイスで作成されます。インターフェイスのアクセス リストが動的に拡大および縮小します。エントリは、アイドル タイムアウトまたは最大タイムアウト期間が経過すると、動的に削除されます。アクセス リストが大きくなると、パケット交換のパフォーマンスが低下し、パフォーマンスの問題の劣化を通知する場合、ロック アンド キーによって生成された一時アクセス リスト エントリを削除するかどうかを確認するために、境界ルータの設定を確認する必要があります。

ロック アンド キーの保守

ロック アンド キーを使用中の場合、ダイナミック アクセス リストは、認証エントリの追加および削除に伴って動的に増減します。エントリが存在しても、スプーフィング攻撃のリスクがあるため、タイムリーにエントリが削除されていることを確認する必要があります。また、エントリの数が増えれば、ルータのパフォーマンスへの影響も大きくなります。

アイドルまたは絶対タイムアウトを設定していない場合、エントリは、ダイナミック アクセス リスト エントリを手動で削除するまで維持されます。この場合、エントリの削除について配慮してください。

ダイナミック アクセス リスト

ダイナミック アクセス リストを設定する場合は、次のガイドラインを参照してください。

- いずれか 1 つのアクセス リストに対して複数のダイナミック アクセス リストを作成しないで下さい。ソフトウェアは、定義された最初のダイナミック アクセス リストだけを参照します。

- 別のアクセス リストに同じ名前を割り当てないで下さい。そうすることで、既存のリストを再利用するように、ソフトウェアに指示します。すべての名前付きエントリは、設定内でグローバルに一意である必要があります。
- スタティック アクセス リストに属性を割り当てるのと同じ方法で、ダイナミック アクセス リストに属性を割り当てます。一時アクセス リスト エントリは、このリストに割り当てられているアトリビュートを継承します。
- ルータ経由でのアクセスが許可される前に、ユーザーが認証する必要があるルータに対する Telnet セッションを開く必要があるよう、プロトコルとして Telnet を設定します。
- 今度は、**autocommand** 内の **access-enable** コマンド内の **timeout** キーワードで、アイドル タイムアウトを定義するか、後で、**access-list** コマンドで絶対タイムアウト値を定義します。アイドル タイムアウトまたは絶対タイムアウトを定義する必要があります。そうしないと、一時的なアクセス リスト エントリは、管理者が手動でエントリを削除するまで（ユーザーがセッションを終了した後でも）、インターフェイスで永久に設定されたままになります。（必要に応じて、アイドル タイムアウトと絶対タイムアウトの両方を設定することもできます）。
- アイドル タイムアウトを設定する場合、アイドル タイムアウト値は、WAN アイドル タイムアウト値と等しくなる必要があります。
- アイドル タイムアウトと絶対タイムアウトの両方を設定する場合、アイドル タイムアウト値は、絶対タイムアウト値未満である必要があります。
- ジョブが ACL の絶対タイマーを超えて動作していることを認識した場合、**access-list dynamic-extend** コマンドを使用して、6 分ほどダイナミック ACL の絶対タイマーを拡張します。このコマンドにより、ロック アンド キーを使用して、自身を再認証するため、ルータに新しい Telnet セッションを開くことができます。
- 一時的なエントリで置換される唯一の値は、入力アクセス リストまたは出力アクセス リスト内にアクセス リストがあったかどうかに応じて、送信元または宛先アドレスになります。ポートなどの他の属性はすべて、メインのダイナミック アクセス リストから引き継がれます。
- ダイナミック リストへの追加はそれぞれ、ダイナミック リストの先頭に常に配置されます。一時アクセス リスト エントリの順序を指定することはできません。
- 一時アクセス リスト エントリが NVRAM には書き込まれません。
- ダイナミック アクセス リストを手動でクリアまたは表示するには、この章で後述される「ロック アンド キーの維持」を参照して下さい。

ロック アンド キー認証

認証問い合せプロセスを設定するには、3 つの方法があります。この項では、これら 3 つの方法について説明します。

（注） Cisco は、認証問い合せプロセスには、TACACS+ サーバーを使用することを推奨します。TACACS+ は、認証、許可、アカウンティング サービスを提供します。また、プロトコル サポート、プロトコル仕様、および中央集中型セキュリティデータベースも提供します。TACACS+ サーバーの使用については、次項「方法 1 -- セキュリティ サーバーの設定」で説明します。

TACACS+ サーバーなどのネットワーク アクセス セキュリティ サーバーを使用します。この方法には、TACACS+ サーバーでの追加設定手順が必要になりますが、より厳しい認証問い合わせとより高度な追跡機能が可能になります。

```
Router(config-line)# login tacacs
```

username コマンドを使用します。この方法では、認証はユーザー単位で決定するため、効果的です。

```
Router(config)# username

name
 {nopassword
 |
password
 {
mutual-password
 |
encryption-type

encryption-password
}}
```

password および **login** コマンドを使用します。この方法は、パスワードがユーザーではなく、このポートに設定されているため、有効でありません。そのため、パスワードを知っているすべてのユーザーが正常に認証できます。

```
R
outer(config-line)# password

password
Router(config-line)# login local
```

autocommand コマンド

autocommand コマンドは、ユーザーが特定の回線に接続する際に、システムが指定されている特権 EXEC コマンドを自動的に実行するように設定します。**autocommand** コマンドの設定のための次のガイドラインを使用します。

- ユーザーを認証するために TACACS+ サーバーを使用する場合、TACACS+ サーバー上で、ユーザーごとの autocommand として、**autocommand** コマンドを設定する必要があります。ローカル認証を使用する場合、回線上で **autocommand** コマンドを使用します。
- 同じ **autocommand** コマンドで、すべての仮想端末（VTY）ポートを設定します。VYT ポートで **autocommand** コマンドを省略すると、任意のホストがルータの特権 EXEC モー

ドへのアクセスを許可し、ダイナミック アクセス リスト内の一時アクセス リスト エントリを作成しません。

- **autocommand access-enable** コマンドでアイドル タイムアウトを定義しない場合、**access-list** コマンドで絶対タイムアウトを定義する必要があります。アイドル タイムアウトまたは絶対タイムアウトを定義する必要があります。そうしないと、一時的なアクセス リスト エントリは、エントリが管理者によって手動で削除されるまで（ユーザーがセッションを終了した後も）インターフェイスで永久に設定されたままになります。（必要に応じて、アイドル タイムアウトと絶対タイムアウトの両方を設定することもできます）。
- アイドル タイムアウトと絶対タイムアウトの両方を設定する場合、絶対タイムアウト値は、アイドル タイムアウト値よりも大きくする必要があります。

ロック アンド キーセキュリティ（ダイナミック アクセス リスト）の設定方法

ロック アンド キーの設定

ロック アンド キーを設定するには、グローバル コンフィギュレーション モードで次のコマンドを使用します。次の手順を実行する際、この章の「ロック アンド キー設定のガイドライン」に記載されているガイドラインに従っていることを確認します。

手順の概要

1. Router(config)# **access-list** *access-list-number* [**dynamic** *dynamic-name* [**timeout** *minutes*]] {**deny** | **permit**} **telnet** *source source-wildcard destination destination-wildcard*[**precedence** *precedence*] [**tos** *tos*] [**established**] [**log**]
2. Router(config)# **access-list dynamic-extend**
3. Router(config)# **interface** *type number*
4. Router(config-if)# **ip access-group** *access-list-number*
5. Router(config-if)# **exit**
6. Router(config)# **line vty** *line-number* [*ending-line-number*]
7. 次のいずれかを実行します。
   - Router(config-line)# **login tacacs**
   -
   - Router(config-line)# **password** *password*
8. 次のいずれかを実行します。
   - Router(config-line)# **autocommand access-enable** [**host]** [**timeout** *minutes*]
   -
   - Router# **access-enable** [**host]** [**timeout** *minutes*]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	Router(config)# **access-list** *access-list-number* [**dynamic** *dynamic-name* [**timeout** *minutes*]] {**deny** | **permit**} **telnet** *source source-wildcard destination destination-wildcard*[**precedence** *precedence*] [**tos** *tos*] [**established**] [**log**]	一時アクセス リスト エントリのテンプレートとプレースホルダとして動作するダイナミック アクセス リストを設定します。
ステップ 2	Router(config)# **access-list dynamic-extend**	（任意）ロック アンド キーを使用して、自分の再認証を実行するようにルータに別の Telnet セッションを開く際に、6 分ごとのダイナミック ACL の絶対タイマーを拡張します。ジョブが ACL の絶対タイマー前を実行する場合に、このコマンドを使用します。
ステップ 3	Router(config)# **interface** *type number*	インターフェイスを設定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	Router(config-if)# **ip access-group** *access-list-number*	アクセス リストをインターフェイスに適用します。
ステップ 5	Router(config-if)# **exit**	インターフェイス コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードに入ります。
ステップ 6	Router(config)# **line vty** *line-number* [*ending-line-number*]	1 つ以上の仮想端末（VTY）ポートを定義し、ライン コンフィギュレーション モードを開始します。複数の VTY ポートを指定する場合、ソフトウェアがラウンドロビン ベースで使用可能な VTY ポートをハントするため、個別に設定する必要があります。ロック アンド キー アクセスに対して、すべての VTY ポートを設定しない場合、ロック アンド キー サポートに対してのみ、VTY ポートのグループを指定できます。

ステップ 7	次のいずれかを実行します。
	• Router(config-line)# **login tacacs**
	•
	• Router(config-line)# **password** *password*
	例：
	`Router(config-line)# login local`
	例：
	`Router(config-line)# exit`
	例：
		回線またはグローバル コンフィギュレーション モードでユーザー認証を設定します。

	コマンドまたはアクション	目的
	then 例： Router(config)# **username** *name* **password** *secret*	
ステップ 8	次のいずれかを実行します。 • Router(config-line)# **autocommand access-enable** [**host**] [**timeout** *minutes*] • • Router# **access-enable** [**host**] [**timeout** *minutes*]	回線設定または特権EXECモードの一時アクセス リスト エントリを作成できます。 回線設定モードで **access-enable** コマンドとともに **autocommand** を使用して、回線が接続されたときに、自動的にダイナミック アクセス リスト上の一時アクセス リスト エントリを作成するようシステムを設定します。 任意の **host** キーワードを指定しないと、ネットワーク全体のすべてのホストが一時アクセス リスト エントリを設定できます。ダイナミック アクセス リストには、新しいネットワーク接続を許可するためのネットワーク マスクが含まれます。 任意の **timeout** キーワードを指定すると、一時アクセス リストに対するアイドル タイムアウトを定義します。 有効値の範囲は 1 ～ 9999（分）です。

ロック アンド キーの設定の確認

ユーザーに接続をテストするように求めることで、ロック アンド キーがルータで正しく設定されていることを確認できます。ユーザーは、ダイナミック アクセス リストで許可されるホストである必要があり、ユーザーは、AAA 認証および許可を設定する必要があります。

接続をテストするには、ユーザーは、ルータへの Telnet 接続を行い、Telnet セッションを閉じる許可をし、ルータの反対側のホストへのアクセスを試みる必要があります。このホストは、ダイナミック アクセス リストによって許可されているものである必要があります。ユーザーは、IPプロトコルを使用するアプリケーションのあるホストにアクセスする必要があります。

次の例は、エンドユーザーが正常に認証された場合に、何が見えるかを示しています。パスワードが入力され、認証された後に、Telnet 接続は閉じられます。一時アクセス リスト エントリが作成され、Telnet セッションを開始したホストがファイアウォールの内側のホストにアクセスします。

```
Router% telnet corporate
Trying 172.21.52.1 ...
Connected to corporate.example.com.
Escape character is '^]'.
```

```
User Access Verification
Password:Connection closed by foreign host.
```

ユーザーは、ルータで **show access-lists** コマンドを使用して、ルータを介して、ユーザーのアクセスを許可する別のエントリを含む、ダイナミック アクセス リストを表示できます。

ダイナミック アクセス リスト エントリの表示

一時アクセス リスト エントリは、使用中に表示できます。一時アクセス リスト エントリがユーザーまたは絶対またはアイドル タイムアウト パラメータによってクリアされた後は表示されなくなります。表示される一致の数は、アクセス リスト エントリがヒットした回数を示します。

現在確立されているダイナミック アクセス リスト エントリ リストおよび一時アクセス リスト エントリ リストを表示するには、特権 EXEC モードで次のコマンドを使用します。

コマンド	目的
Router# **show access-lists** [*access-list-number*]	ダイナミック アクセス リストおよび一時アクセス リスト エントリを表示します。

ダイナミック アクセス リスト エントリの手動削除

一時アクセス リスト エントリを手動で削除するには、特権 EXEC モードで次のコマンドを使用します。

コマンド	目的
Router# **clear access-template** [*access-list-number* | *name*] [*dynamic-name*] [*source*] [*destination*]	ダイナミック アクセス リストを削除します。

ロック アンド キーの設定例

ローカル認証を使用したロック アンド キーの例

この例は、ルータで局所的に生じた認証を使って、ロック アンド キー アクセスを設定する方法を示しています。ロック アンド キーは、Ethernet 0 インターフェイスとして設定されます。

```
interface ethernet0
 ip address 172.18.23.9 255.255.255.0
 ip access-group 101 in
access-list 101 permit tcp any host 172.18.21.2 eq telnet
access-list 101 dynamic mytestlist timeout 120 permit ip any any
line vty 0
```

```
login local
autocommand access-enable timeout 5
```

最初の access-list エントリは、ルータに Telnet だけを許可します。2 番目のアクセス リスト エントリは、ロック アンド キーがトリガーされるまで常に無視されます。

access-list コマンドでは、タイムアウトは絶対タイムアウトです。この例では、mytestlist ACL の有効期間は、120 分です。つまり、ユーザーがログインし、**access-enable** コマンドを有効にすると、120 分間（最大絶対時間）有効なダイナミック ACL が作成されます。セッションは使用者の有無に関係なく、120 分後に閉じられます。

access-enable コマンドでは、タイムアウトは、アイドル タイムアウトです。この例では、ユーザーがログインまたは認証するたびに 5 分間セッションがあります。アクティビティがないと、セッションは 5 分後に終了し、ユーザーを再認証する必要があります。ユーザーが接続を使用すると、絶対時間が作用し、セッションは 120 分後に終了します。

ユーザーがルータへの Telnet セッションを開いた後、ルータはユーザーを認証しようとします。認証に成功すると、**autocommand** が実行され、Telnet セッションが終了します。**autocommand** は、2 番目のアクセス リスト エントリ（mytestlist）に基づいて、イーサネット 0 インターフェイスで一時的な着信アクセス リスト エントリを作成します。アクティビティがない場合、タイムアウトで規定されているように、この一時エントリは 5 分後に無効となります。

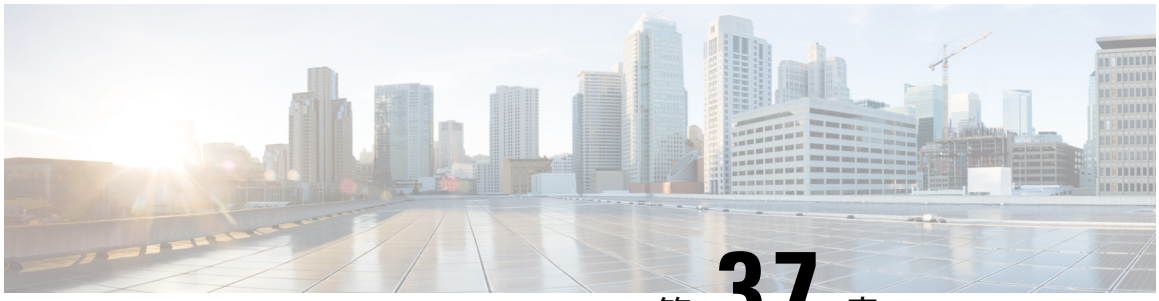
TACACS+ 認証を使用したロック アンド キーの例

Cisco は、認証に TACACS+ サーバーを使用することを推奨します。以下の例を参照して下さい。

以下の例は、TACACS+ サーバーでの認証を使用して、ロック アンド キーを設定する方法について説明しまています。ロック アンド キー アクセスは、BRI0 インターフェイスで設定されます。4 つのポートは、VTY パスワード「password1」として定義されています。

```
aaa authentication login default group tacacs+ enable
aaa accounting exec stop-only group tacacs+
aaa accounting network stop-only group tacacs+
enable password ciscotac
!
isdn switch-type basic-dms100
!
interface ethernet0
ip address 172.18.23.9 255.255.255.0
!
interface BRI0
 ip address 172.18.21.1 255.255.255.0
 encapsulation ppp
 dialer idle-timeout 3600
 dialer wait-for-carrier-time 100
 dialer map ip 172.18.21.2 name dialermapname
 dialer-group 1
 isdn spid1 2036333715291
 isdn spid2 2036339371566
 ppp authentication chap
 ip access-group 102 in
!
access-list 102 permit tcp any host 172.18.21.2 eq telnet
```

```
access-list 102 dynamic testlist timeout 5 permit ip any any
!
!
ip route 172.18.250.0 255.255.255.0 172.18.21.2
priority-list 1 interface BRI0 high
tacacs-server host 172.18.23.21
tacacs-server host 172.18.23.14
tacacs-server key test1
tftp-server rom alias all
!
dialer-list 1 protocol ip permit
!
line con 0
 password password1
line aux 0
 line VTY 0 4
 autocommand access-enable timeout 5
 password password1
!
```



第 37 章

ACL IP オプションの選択的ドロップ

ACL IP オプションの選択的ドロップ機能を使用すると、Cisco ルータが IP オプションが設定されたパケットをフィルタしたり、ルータまたはダウンストリーム ルータ上での IP オプションの影響を軽減したりすることができるようになります。これは、これらのパケットをドロップするか、IP オプションの処理を無視することによって行われます。

ACL IP オプションの選択的ドロップの制約事項

リソース予約プロトコル（RSVP）（マルチプロトコル ラベル スイッチング トラフィック エンジニアリング（MPLS TE））、Internet Group Management Protocol バージョン 2（IGMPv2）、および IP オプション パケットを使用するその他のプロトコルは、ドロップまたは無視モードでは機能しない可能性があります。

ACL IP オプションの選択的ドロップに関する情報

ACL IP オプションの選択的ドロップの使用

ACL IP オプションの選択的ドロップ機能を使用すると、IP オプションが設定されたパケットをルータでフィルタできるようになります。これにより、これらのパケットのルータまたはダウンストリーム ルータへの影響を軽減し、次の手順を実行できます。

- 受信した IP オプション パケットをすべてドロップし、オプションがネットワークの奥深くまで入り込まないようにします。

- そのルータ宛ての IP オプション パケットを無視し、IP オプションが設定されていないものとして扱います。

多くのユーザーにとっては、パケットのドロップが最善策であると言えます。ただし、正規の IP オプションが存在する可能性のある環境では、ルータ上のパケットのロード処理を減らすだけで十分です。したがって、ルータ上のオプション処理をスキップしたうえで、ピュア IP であるかのようにパケットを転送することができます。

ACL IP オプションの選択的ドロップを使用する利点

- ドロップ モードでは、ネットワークからのパケットをフィルタすることで、オプション パケットからロードするというダウンストリームルータおよびホストの負荷を軽減できます。
- ドロップ モードでは、分散システム上でのルート プロセッサ（RP）処理が必要となるオプションの RP へのロードが最小限に抑えられます。以前は、パケットは常に RP CPU でルーティングまたは処理されていました。現在は、無視またはドロップすることで、パケットが RP パフォーマンスに影響を及ぼすことを回避できます。

ACL IP オプションの選択的ドロップの設定方法

ACL IP オプションの選択的ドロップの設定

ここでは、ACL IP オプションの選択的ドロップ機能を設定する方法について説明します。

手順の概要

1. **enable**
2. **configure terminal**
3. **ip options** {**drop** | **ignore**}
4. **exit**
5. **show ip traffic**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例：	グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
	`Router# configure terminal`	
ステップ 3	**ip options** {**drop** | **ignore**} 例： `Router(config)# ip options drop`	ルータに送信されたIPオプションパケットをドロップまたは無視します。
ステップ 4	**exit** 例： `Router(config)# exit`	特権 EXEC モードに戻ります。
ステップ 5	**show ip traffic** 例： `Router# show ip traffic`	（任意）IP トラフィックの統計情報を表示します。

ACL IP オプションの選択的ドロップの設定例

例：ACL IP オプションの選択的ドロップの設定

次に、ネットワークに入ったすべてのオプションパケットをドロップするように、ルータ（およびダウンストリーム ルータ）を設定する例を示します。

```
Router(config)# ip options drop
% Warning:RSVP and other protocols that use IP Options packets may not function in drop
 or ignore modes.
end
```

例：ACL IP オプションの選択的ドロップの確認

この出力例は、**ip options drop** コマンドを使用した後に表示されます。

```
Router# show ip traffic
IP statistics:
  Rcvd:  428 total, 323 local destination
         0 format errors, 0 checksum errors, 0 bad hop count
         0 unknown protocol, 0 not a gateway
         0 security failures, 0 bad options, 0 with options
  Opts:  0 end, 0 nop, 0 basic security, 0 loose source route
         0 timestamp, 0 extended security, 0 record route
         0 stream ID, 0 strict source route, 0 alert, 0 cipso, 0 ump
         0 other, 30 ignored
  Frags: 0 reassembled, 0 timeouts, 0 couldn't reassemble
         0 fragmented, 0 fragments, 0 couldn't fragment
  Bcast: 0 received, 0 sent
```

```
Mcast: 323 received, 809 sent
Sent:  809 generated, 591 forwarded
Drop:  0 encapsulation failed, 0 unresolved, 0 no adjacency
       0 no route, 0 unicast RPF, 0 forced drop, 0 unsupported-addr
       0 options denied, 0 source IP address zero
```

IP アクセス リスト エントリ シーケンス番号の追加情報

ここでは、IP アクセス リストに関する関連資料について説明します。

関連資料

関連項目	マニュアル タイトル
IP アクセス リストの設定	『Creating an IP Access List and Applying It to an Interface』
IP アクセス リスト コマンド	• 『Cisco IOS Security Command Reference: Commands A to C』 • 『Cisco IOS Security Command Reference: Commands D to L』 • 『Cisco IOS Security Command Reference: Commands M to R』 • 『Cisco IOS Security Command Reference: Commands S to Z』

シスコのテクニカル サポート

説明	リンク
シスコのサポート Web サイトでは、シスコの製品やテクノロジーに関するトラブルシューティングにお役立ていただけるように、マニュアルやツールをはじめとする豊富なオンライン リソースを提供しています。 お使いの製品のセキュリティ情報や技術情報を入手するために、Cisco Notification Service（Field Notice からアクセス）、Cisco Technical Services Newsletter、Really Simple Syndication（RSS）フィードなどの各種サービスに加入できます。 シスコのサポート Web サイトのツールにアクセスする際は、Cisco.com のユーザ ID およびパスワードが必要です。	http://www.cisco.com/en/US/support/index.html

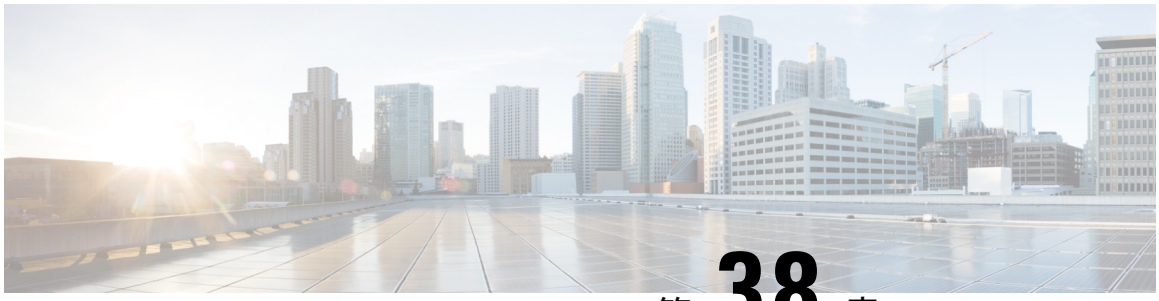
ACL IP オプションの選択的ドロップに関する機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *58 : ACL IP* オプションの選択的ドロップに関する機能情報

機能名	リリース	機能情報
ACL IP オプションの選択的ドロップ	Cisco IOS XE リリース 2.1	ACL IP オプションの選択的ドロップ機能を使用すると、Cisco ルータが IP オプションが設定されたパケットをフィルタしたり、ルータまたはダウンストリームルータ上での IP オプションの影響を軽減したりすることができるようになります。これは、これらのパケットをドロップするか、IP オプションの処理を無視することによって行われます。 この機能は、Cisco ASR 1000 シリーズのアグリゲーション サービス ルータで導入されました。 次のコマンドが導入されました。**ip options**



第 38 章

ACL 管理性を使用した IP アクセス リスト データの表示及びクリア

このモジュールでは、IP アクセス リスト内のエントリおよび各エントリに一致したパケットの数の表示方法について説明します。ユーザーは、ACL 管理性機能を使用して、グローバルに、または、インターフェイスごとのおよび着信または発信トラフィック方向ごとにこれらの統計情報を取得できます。ネットワーク デバイスのさまざまなインターフェイス上の着信または発信トラフィックパターンの詳細表示は、特定のインターフェイスへの攻撃に対してデバイスの保護に役立ちます。このモジュールでは、また、アクセス リスト エントリに一致するパケットの数が 0 から再開されるカウンタをクリアする方法について説明します。

ACL 管理性を使用した IP アクセス リスト データの表示及びクリアに関する情報

ACL 管理性の利点

Cisco IOS リリース 12.4(6)T 以前では、Cisco IOS ソフトウェア内の ACL インフラストラクチャは、ACL 内の各 ACE に対するグローバル統計情報を維持するだけでした。この方法によって、1 つの ACL が複数のインターフェイスに適用される場合、維持された ACE 統計情報は、その ACL が適用されるすべてのインターフェイス上で一致（ヒット）する着信および発信パケットの合計数となります。

ただし、ACEの統計情報がインターフェイスごとおよび着信または発信トラフィック方向ごとに維持される場合、ネットワークデバイスの様々なインターフェイスにおける着信および発信トラフィックパターンの特定の詳細およびACEの効率性を表示できます。このような情報は、特定のインターフェイス上に着信する攻撃に対するデバイスの保護に役立ちます。

インターフェイス レベルの ACL 統計情報のサポート

Cisco IOS リリース 12.4(6)T により、Cisco IOS ソフトウェア内の ACL インフラストラクチャは、インターフェイスごとの、および ACL に対する着信または発信トラフィック方向ごとの ACE 統計情報の保守、表示、およびクリアをサポートするよう、拡張されます。このサポートは、『インターフェイス レベルの統計情報のサポート』と呼ばれます。

（注） 同じアクセス グループ ACL が他の機能によっても使用された場合、保持されているインターフェイス統計情報は、パケット一致が他の機能によって検出される際に、更新されません。この例では、ACL のために維持される、すべてのインターフェイス レベル統計情報の合計は、その ACL に対するグローバル統計情報を集約していない場合があります。

IP アクセス リスト データを表示およびクリアする方法

この項には、IPアクセスリストおよび各リストに一致（ヒット）するパケットの数を表示し、IP アクセス リスト カウンタをクリアするための次の手順が含まれます。

（注） 特定のホストまたはネットワークに対するアクセスを拒否し、そのネットワークまたはホストの誰かがアクセスしようとしたかどうかを検出する場合、対応する **deny** ステートメントを指定した **log** キーワードを含めます。それによって、その送信元からの拒否されたパケットがログに記録されます。詳細については、「IP アクセス リストの概要」の「IP アクセス リスト ロギング」を参照して下さい。

グローバル IP ACL 統計情報の表示

ルータ上のすべての IP アクセス リストと一致したパケット数を表示するには、次の作業を実行します。

手順の概要

1. **enable**
2. **show ip access-list** [*access-list-number* | *access-list-name*]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**show ip access-list** [*access-list-number* | *access-list-name*] 例： `Router# show ip access-list limited`	IP アクセス リスト情報を表示します。 • この例では、「名前付きアクセス リストを指定します」を使用するすべてのインターフェイスの統計情報を表示します。

インターフェイス レベル IP ACL 統計情報の表示

このセクションでは、インターフェイスに ACL 用の着信または発信トラフィック方向ごとの IP ACE の統計情報を表示する方法について説明します。この機能は、ACL 管理性と呼ばれています。

（注）
- ACL 管理性サポート対象：
  - 非分散型プラットフォーム ソフトウェアでスイッチングされるだけです。
  - 標準と拡張の静的に設定された ACL と脅威緩和サービス（TMS）ダイナミック ACE です。
- ACL 管理性サポート対象外：
  - ファイアウォールおよび認証プロキシなど、再帰かつユーザー設定のダイナミック ACL およびダイナミック ACE ブロック。
  - 仮想テンプレートおよび仮想アクセス インターフェイス。

>

手順の概要

1. **enable**
2. **show ip access-list interface** *interface-name* [**in**| **out**]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例：	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。

	コマンドまたはアクション	目的
	`Router> enable`	
ステップ 2	**show ip access-list interface** *interface-name* [**in**| **out**] 例： `Router# show ip access-list interface FastEthernet 0/0 in`	IP アクセス リスト情報を表示します。 • この例では、FastEthernet インターフェイスに着信するトラフィックに関する統計情報を表示します。 • ACL のインターフェイス レベルの統計情報に関するデバッグ情報を表示するには、**debug ip access-list intstats** コマンドを使用します。

アクセス リスト カウンタのクリア

システムは、アクセス リストの各行に一致（ヒット）するパケットの数を数えます。カウンタは、**show access-lists** EXEC コマンドで表示されます。この作業を行い、アクセス リストのカウンタをクリアします。アクセスリストに一致するゼロから始まるパケットの数を決定しようとする場合に、これを行うことができます。

手順の概要

1. **enable**
2. **clear ip access-list counters** {*access-list-number* | *access-list-name}*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**clear ip access-list counters** {*access-list-number* | *access-list-name}* 例： `Router# clear access-list counters corpmark`	IP アクセス リストのカウンタをクリアします。

ACL 管理性を使用した IP アクセス リスト データの表示及びクリアのための設定例

グローバル IP ACL 統計情報を表示する例

次に、ACL 150 のグローバル統計情報を表示する例を示します。

```
Router# show ip access-list 150

Extended IP access list 150
   10 permit ip host 10.1.1.1 any (3 matches)
   30 permit ip host 10.2.2.2 any (27 matches)
```

入力統計情報を表示する例

次の例は、アクセス リスト 150（ACL 番号）に関連付けられているインターフェイス FastEthernet 0/1 から集めた着信パケットの統計情報を示しています。

```
Router#
 show ip access-list interface FastEthernet 0/1 in
Extended IP access list 150 in
   10 permit ip host 10.1.1.1 any (3 matches)
   30 permit ip host 10.2.2.2 any (12 matches)
```

出力統計情報を表示する例

次の例は、FastEthernet 0/0 インターフェイスから集めた出力パケットに関する統計情報を示しています。

```
Router#
 show ip access-list interface FastEthernet 0/0 out
Extended IP access list myacl out
    5 deny ip any 10.1.0.0 0.0.255.255
    10 permit udp any any eq snmp (6 matches)
```

入出力統計情報を表示する例

（注） 方向を指定しないと、そのインターフェイスに適用された入出力 ACL が表示されます。

次の例の表示から集めた入出力統計情報は、FastEthernet 0/0 を実行します。

```
Router#
 show ip access-list interface FastEthernet 0/0
```

```
Extended IP access list 150 in
   10 permit ip host 10.1.1.1 any
   30 permit ip host 10.2.2.2 any (15 matches)
Extended IP access list myacl out
    5 deny ip any 10.1.0.0 0.0.255.255
    10 permit udp any any eq snmp (6 matches)
```

IPアクセスリスト用のグローバルおよびインターフェイス統計情報のクリアの例

次の例では、IP ACL 150 のグローバルおよびインターフェイスの統計情報をクリアします。

```
Router#
 clear ip access-list counters 150
```

すべての IP アクセス リスト用のグローバルおよびインターフェイス統計情報のクリアの例

次の例では、すべての IP ACL のグローバルおよびインターフェイスの統計情報をクリアします。

```
Router#
 clear ip access-list counters
```

その他の参考資料

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『Cisco IOS Master Commands List, All Releases』
セキュリティ コマンド	『*Cisco IOS Security Command Reference*』

標準

標準	タイトル
この機能がサポートする新しい規格または変更された規格はありません。	--

MIB

MIB	MIB のリンク
この機能によってサポートされる新しい MIB または変更された MIB はありません。	選択したプラットフォーム、Cisco IOS リリース、およびフィーチャ セットに関する MIB を探してダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

RFC

RFC	タイトル
この機能でサポートされる新規の標準または変更された標準はありません。また、既存の標準のサポートは変更されていません。	--

シスコのテクニカル サポート

説明	リンク
右の URL にアクセスして、シスコのテクニカル サポートを最大限に活用してください。これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

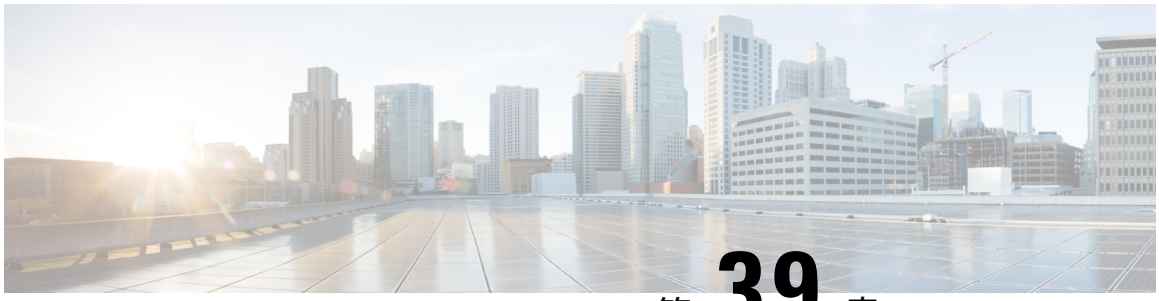
IP アクセス リスト情報の表示およびカウンタのクリアに関する機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *59 : ACL* 管理性を使用した *IP* アクセス リスト データの表示及びクリアのための機能情報

機能名	リリース	機能情報
ACL 管理性	Cisco IOS XE Release 3.9S	ACL 管理性機能により、ユーザーは、インターフェイスおよびアクセス コントロール リスト（ACL）に対する入力や出力トラフィック方向ごとのアクセス コントロール エントリ（ACE）の統計情報を表示およびクリアすることができます。



第 39 章

ACL Syslog 相関

アクセス コントロール リスト（ACL）Syslog 相関機能では、アクセス コントロール エントリ（ACE）Syslog エントリにタグ（ユーザー定義の Cookie またはデバイスが生成した MD5 ハッシュ値）を追加します。このタグは Syslog エントリを生成した ACL 内で ACE を一意に特定します。

ACL Syslog 相関の前提条件

ACL Syslog 相関機能を設定する前に、「IP アクセス リストの概要」モジュールでその概念を理解する必要があります。

ACL Syslog 相関機能は、ユーザー定義の cookie またはデバイスで生成されるハッシュ値を syslog 内の ACE メッセージに追加します。ログ オプションが ACE に対してイネーブルになっている場合、これらの値は ACE メッセージにのみ追加されます。

ACL Syslog 相関に関する情報

ACL Syslog 相関タグ

ACL Syslog 相関機能では、アクセス コントロール エントリ（ACE）Syslog エントリにタグ（ユーザー定義の Cookie またはデバイスが生成した MD5 ハッシュ値）を追加します。このタグは Syslog エントリを生成した ACE を一意に特定します。

ネットワーク管理ソフトウェアでは、どの ACE が特定の Syslog イベントを生成したかを特定するためにタグを使用できます。たとえば、ネットワーク管理者はネットワーク管理アプリ

ケーションでACE規則を選択し、次にそのACEルールに対応するSyslogイベントを表示できます。

Syslogメッセージにタグを追加するには、Syslogイベントを生成するACEでログ オプションが有効になっている必要があります。システムは各メッセージに1つのタイプのタグ（ユーザー定義のCookieまたはデバイスで生成したMD5ハッシュ値）のみを追加します。

ユーザー定義のCookieタグを指定するには、ユーザーはACEログ オプションを構成する際にCookie値を入力する必要があります。Cookieは英数字形式である必要があります。64文字以上にはできず、16進数表記（0xなど）で始めることはできません。

デバイスで生成したMD5ハッシュ値タグを指定するには、ハッシュ生成機能をデバイスで有効にする必要があります。また、ACEログ オプションを構成するときにユーザーはCookie値を入力してはいけません。

ACE Syslog メッセージ

パケットがACL内のアクセス コントロール エントリ（ACE）と一致すると、そのイベントのログ オプションが有効になっているかどうかシステムでチェックされます。ログ オプションが有効な場合、ACL Syslog相関機能がデバイスで構成されていると、システムはsyslogメッセージにタグを付けます。タグは、標準情報に加えてsyslogメッセージの最後に表示されます。

次は、ユーザー定義のCookieタグを示すサンプルsyslogメッセージです。

```
Jun 5 12:55:44.359: %SEC-6-IPACCESSLOGP: list logacl permitted tcp 192.168.16.1(38402)
-> 192.168.16.2(23), 1 packet [User_permiited_ACE]
```

次は、ハッシュ値タグを示すサンプルsyslogメッセージです。

```
Jun 5 12:55:44.359: %SEC-6-IPACCESSLOGP: list logacl permitted tcp 192.168.16.1(38402)
-> 192.168.16.2(23), 1 packet [0x723E6E12]
```

ACL Syslog 相関の設定方法

デバイスでのハッシュ値生成の有効化

ユーザー定義Cookieを使用して設定されていないシステム内でログをイネーブルにした各アクセス コントロール エントリ（ACE）のMD5ハッシュ値を生成するデバイスを設定するには、このタスクを実行します。

ハッシュ値生成設定をイネーブルにすると、システムは既存のすべてのACEをチェックし、ハッシュ値を必要とする各ACEのハッシュ値を生成します。ハッシュ値生成の設定をディセーブルにすると、これまでに生成されたすべてのハッシュ値がシステムから削除されます。

手順の概要

1. **enable**

2. **configure terminal**
3. **ip access-list logging hash-generation**
4. **end**
5. 次のいずれかを実行します。
   - **show ip access-list** *access-list-number*
   - **show ip access-list** *access-list-name*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ip access-list logging hash-generation** 例： `Device(config)# ip access-list logging hash-generation`	デバイスでハッシュ値生成を有効にします。 • ログを有効にした ACE があり、ハッシュ値を必要とする場合、デバイスは自動的に値を生成し、コンソールでその値を表示します。
ステップ 4	**end** 例： `Device(config)# end`	（任意）グローバル コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

ステップ 5	次のいずれかを実行します。
	• **show ip access-list** *access-list-number*
	• **show ip access-list** *access-list-name*
	例：
	`Device# show ip access-list 101`
	例：
	`Device# show ip access-list acl`
		（任意）番号付きまたは名前付き IP アクセス リストの内容を表示します。
		• ログをイネーブルにした ACE のアクセス リストに生成したハッシュ値が含まれることを確認するには、出力を見直します。

デバイスでのハッシュ値生成の無効化

デバイスでのハッシュ値生成をディセーブルにするには、このタスクを実行します。ハッシュ値生成の設定をディセーブルにすると、これまでに生成されたすべてのハッシュ値がシステムから削除されます。

手順の概要

1. **enable**
2. **configure terminal**
3. **no ip access-list logging hash-generation**
4. **end**
5. 次のいずれかを実行します。
   - **show ip access-list** *access-list-number*
   - **show ip access-list** *access-list-name*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**no ip access-list logging hash-generation** 例： `Device(config)# no ip access-list logging hash-generation`	デバイスでのハッシュ値生成をディセーブルにします。 • これまでに作成されたハッシュ値がシステムから削除されます。
ステップ 4	**end** 例： `Device(config)# end`	（任意）グローバル コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。
ステップ 5	次のいずれかを実行します。 • **show ip access-list** *access-list-number* • **show ip access-list** *access-list-name* 例：	（任意）IP アクセス リストの内容を表示します。 • ログをイネーブルにした ACE のアクセス リストに生成したハッシュ値が含まれないことを確認するには、出力を見直します。

	コマンドまたはアクション	目的

	`Device# show ip access-list 101`
	例：
	`Device# show ip access-list acl`	

ユーザー定義 Cookie を使用した ACL Syslog 相関の設定

syslog メッセージ タグとしてユーザー定義の Cookie クッキーを使用し、特定のアクセス リストのデバイス上の ACL syslog 相関機能を設定するには、このタスクを実行します。

このセクションでは、番号付きアクセス リストのユーザー定義の Cookie を使用して、ACL Syslog 相関機能を設定する方法について例を示します。ただし、番号付きおよび名前付きアクセス リストの両方、標準および拡張アクセス リストの両方について、ユーザー定義の Cookie を使用し、ACL Syslog 相関機能を設定できます。

（注） 次の制限事項は、ユーザー定義の Cookie 値を選択する場合に適用されます。

- 最大文字数は 64 です。
- Cookie は 16 進表記（0x など）で始めることはできません。
- Cookie は、**reflect**、**fragment**、**time-range** といったキーワードと同じまたはその一部を使用することはできません。たとえば、reflect と refは無効な値です。ただし、これらのキーワードを先頭に使用することはできます。たとえば、reflectedACE と fragment_33 は有効な値です。
- Cookie に設定できるのは英数字のみです。

>

手順の概要

1. **enable**
2. **configure terminal**
3. **access-list** *access-list-number* **permit** *protocol source destination* **log** *word*
4. **end**
5. **show ip access-list** *access-list-number*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例：	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。

	コマンドまたはアクション	目的
	`Device> enable`	
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**access-list** *access-list-number* **permit** *protocol source destination* **log** *word* 例： `Device(config)# access-list 101 permit tcp host 10.1.1.1 host 10.1.1.2 log UserDefinedValue`	拡張 IP アクセス リストとユーザー定義の Cookie 値を定義します。 • Cookie 値の引数として *word* を入力します。
ステップ 4	**end** 例： `Device(config)# end`	（任意）グローバル コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。
ステップ 5	**show ip access-list** *access-list-number* 例： `Device# show ip access-list 101`	（任意）IP アクセス リストの内容を表示します。 • 出力を見直して、アクセス リストにユーザー定義の Cookie 値が含まれることを確認します。

例

次に、ユーザー定義の Cookie 値を使用したアクセス リストに **show ip access-list** コマンドを使用した際の出力例を示します。

```
Device# show ip access-list
101
Extended IP access list 101
30 permit tcp host 10.1.1.1 host 10.1.1.2 log (tag = UserDefinedValue)
```

ハッシュ値を使用した ACL Syslog 相関の設定

syslog メッセージ タグとしてデバイスで生成されたハッシュ値を使用し、特定のアクセス リストのデバイス上の ACL Syslog 相関機能を設定するには、このタスクを実行します。

このセクションでは、番号付きアクセス リストのデバイスで生成されたハッシュ値を使用して、ACL Syslog 相関機能を設定する方法についてステップを示します。ただし、番号付きおよび名前付きアクセス リストの両方、標準および拡張アクセス リストの両方について、デバイスで生成されたハッシュ値を使用し、ACL Syslog 相関機能を設定できます。

手順の概要

1. **enable**
2. **configure terminal**
3. **ip access-list logging hash-generation**
4. access-list *access-list-number* **permit** *protocol source destination* **log**
5. **end**
6. **show ip access-list** *access-list-number*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ip access-list logging hash-generation** 例： `Device(config)# ip access-list logging hash-generation`	デバイスでハッシュ値生成を有効にします。 • ログを有効にした ACE があり、ハッシュ値を必要とする場合、デバイスは自動的に値を生成し、コンソールでその値を表示します。
ステップ 4	access-list *access-list-number* **permit** *protocol source destination* **log** 例： `Device(config)# access-list 102 permit tcp host 10.1.1.1 host 10.1.1.2 log`	拡張 IP アクセス リストを定義します。 • アクセス リストのログ オプションを有効にしますが、Cookie 値は指定しないでください。 • デバイスが、新たに定義したアクセス リストのハッシュ値を自動的に生成します。
ステップ 5	**end** 例： `Device(config)# end`	（任意）グローバル コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。
ステップ 6	**show ip access-list** *access-list-number* 例： `Device# show ip access-list 102`	（任意）IP アクセス リストの内容を表示します。 • 出力を見直して、アクセス リストにルータが生成したハッシュ値が含まれることを確認します。

例

次に、デバイスで生成されたハッシュ値を使用したアクセス リストに**show ip access-list** コマンドを使用した際の出力例を示します。

```
Device# show ip access-list
102
Extended IP access list 102
10 permit tcp host 10.1.1.1 host 10.1.1.2 log (hash = 0x7F9CF6B9)
```

ACL Syslog 相関タグ値の変更

ユーザー定義の Cookie の値を変更したり、ユーザー定義の Cookie とデバイスで生成したハッシュ値を置き換えたりするには、このタスクを実行します。

この手順は、番号付きアクセス リストの ACL Syslog 相関タグ値を変更する方法について示しています。ただし、番号付きおよび名前付きアクセス リストの両方と、標準および拡張アクセス リストの両方について、ACL Syslog 相関タグ値を変更できます。

手順の概要

1. **enable**
2. show access-list
3. **configure terminal**
4. access-list *access-list-number* **permit** *protocol source destination* **log** *word*
5. **end**
6. **show ip access-list** *access-list-number*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	show access-list 例： `Device(config)# show access-list`	（任意）アクセス リストの内容を表示します。
ステップ 3	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的

ステップ 4	access-list *access-list-number* **permit** *protocol source destination* **log** *word*
	例：
	`Device(config)# access-list 101 permit tcp host 10.1.1.1 host 10.1.1.2 log NewUDV`
	例：
	`OR`
	例：
	例：
	`Device(config)# access-list 101 permit tcp any any log replacehash`
		Cookie を修正したり、ハッシュ値を Cookie に変更したりします。
		• アクセス リスト コンフィギュレーション コマンド全体を入力し、前のタグ値を新しいタグ値で置き換える必要があります。

ステップ 5	**end** 例： `Device(config)# end`	（任意）グローバル コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。
ステップ 6	**show ip access-list** *access-list-number* 例： `Device# show ip access-list 101`	（任意）IP アクセス リストの内容を表示します。 • 変更を確認するために出力結果を見直します。

トラブルシューティングのヒント

アクセス リストのデバッグ情報を表示するには、**debug ip access-list hash-generation** コマンドを使用します。**debug** コマンドの出力例を次に示します。

```
Device# debug ip access-list hash-generation
 Syslog hash code generation debugging is on
Device# show debug
IP ACL:
 Syslog hash code generation debugging is on
Device# no debug ip access-list hash-generation

 Syslog hash code generation debugging is off
Device# show debug
Device#
```

ACL Syslog 相関の設定例

例：ユーザー定義 Cookie を使用した ACL Syslog 相関の設定

次に、ユーザー定義 Cookie を使用して、デバイス上で ACL Syslog 相関機能を設定する方法について説明します。

```
Device#
Device# debug ip access-list hash-generation
Syslog MD5 hash code generation debugging is on
Device# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Device(config)# access-list 33 permit 10.10.10.6 log cook_33_std
Device(config)# do show ip access 33
Standard IP access list 33
10 permit 10.10.10.6 log (tag = cook_33_std)
Device(config)# end
```

例：ハッシュ値を使用した ACL Syslog 相関の設定

次の例では、デバイスで生成されたハッシュ値を使用して、デバイス上で ACL Syslog 相関機能を設定する方法について説明します。

```
Device# debug ip access-list hash-generation
Syslog MD5 hash code generation debugging is on
Device# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Device(config)# access-list 33 permit 10.10.10.7 log
Device(config)#
*Nov 7 13:51:23.615: %IPACL-HASHGEN: Hash Input: 33 standard permit 10.10.10.7
Hash Output: 0xCE87F535
Device(config)#
do show ip access 33

Standard IP access list 33
    10 permit 10.10.10.6 log (tag = cook_33_std)
    20 permit 10.10.10.7 log (hash = 0xCE87F535)
```

例：ACL Syslog 相関タグ値の変更

次に、既存のアクセス リストのユーザー定義 Cookie と新しい Cookie 値を交換する方法と、デバイス生成ハッシュ値とユーザー定義 Cookie 値を交換する方法について示します。

```
Device# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Device(config)# do show ip access-list 101
Extended IP access list 101
    10 permit tcp host 10.1.1.1 host 10.1.1.2 log (tag = MyCookie)
    20 permit tcp any any log (hash = 0x75F078B9)
Device(config)# access-list 101 permit tcp host 10.1.1.1 host 10.1.1.2 log NewUDV
Device(config)# do show access-list
```

```
Extended IP access list 101
    10 permit tcp host 10.1.1.1 host 10.1.1.2 log (tag = NewUDV)
    20 permit tcp any any log (hash = 0x75F078B9)
Device(config)# access-list 101 permit tcp any any log replacehash
Device(config)# do show access-list
Extended IP access list 101
    10 permit tcp host 10.1.1.1 host 10.1.1.2 log (tag = NewUDV)
    20 permit tcp any any log (tag = replacehash)
```

IPv6 IOS ファイアウォールの追加情報

関連資料

関連項目	マニュアル タイトル
セキュリティ コマンド	• 『*Cisco IOS Security Command Reference: Commands A to C*』[英語] • 『*Cisco IOS Security Command Reference: Commands D to L*』[英語] • 『*Cisco IOS Security Command Reference: Commands M to R*』[英語] • 『*Cisco IOS Security Command Reference: Commands S to Z*』[英語]
IPv6 コマンド	『*Cisco IOS IPv6 Command Reference*』
IPv6 アドレッシングと接続	『*IPv6 Configuration Guide*』
Cisco IOS IPv6 機能	『*Cisco IOS IPv6 Feature Mapping*』

標準および RFC

標準/RFC	タイトル
IPv6 に関する RFC	*IPv6 RFCs*

シスコのテクニカル サポート

説明	リンク
右の URL にアクセスして、シスコのテクニカル サポートを最大限に活用してください。これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

ACL Syslog 相関に関する機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *60 : ACL Syslog* 相関に関する機能情報

機能名	リリース	機能情報
ACL Syslog 相関	Cisco IOS XE リリース 3.6S	ACL Syslog 相関機能は、ACE Syslog エントリにタグ（ユーザー定義の Cookie またはデバイスが生成した MD5 ハッシュ値）を追加します。このタグは Syslog エントリを生成した ACL 内で ACE を一意に特定します。

第 40 章

IPv6 アクセス コントロール リスト

アクセス リストによって、デバイス インターフェイスでブロックされるトラフィックおよび転送されるトラフィックが決定され、送信元アドレスと宛先アドレスに基づくトラフィックのフィルタリング、および特定のインターフェイスへの着信および発信トラフィックのフィルタリングを行うことができます。標準の IPv6 ACL 機能が拡張されて、IPv6 オプション ヘッダー、および任意でより細かい制御を行うための上位層プロトコル タイプ情報に基づくトラフィック フィルタリングがサポートされています。標準の IPv6 ACL 機能が拡張されて、IPv6 オプション ヘッダー、および任意でより細かい制御を行うための上位層プロトコル タイプ情報に基づくトラフィック フィルタリングがサポートされています。

このモジュールは、仮想端末回線へのアクセスを制御する IPv6 トラフィック フィルタリングの設定方法について説明します。

RSP3 ポートの関連情報

IPv6 ACL は、RSP3 ではサポートされていません

IPv6 アクセス コントロール リストに関する情報

IPv6 トラフィック フィルタリングのアクセス コントロール リスト

IPv6 での標準 ACL 機能は、IPv4 での標準 ACL に似ています。アクセス リストによって、デバイスインターフェイスでブロックされるトラフィックおよび転送されるトラフィックが決定され、送信元アドレスと宛先アドレスに基づいて、特定のインターフェイスへの着信と発信をフィルタリングできます。各アクセス リストの末尾には、暗黙的な deny 文があります。IPv6

ACLを定義し、拒否条件と許可条件を設定するには、グローバルコンフィギュレーションモードで **deny** キーワードと **permit** キーワードを指定して **ipv6 access-list** コマンドを使用します。

IPv6 で拡張された ACL では標準 IPv6 ACL 機能を強化して、IPv6 オプション ヘッダー、および任意でより細かい制御を行うための上位層プロトコルタイプ情報に基づくトラフィック フィルタリングがサポートされています（IPv4 における拡張 ACL に類似した機能です）。

IPv6 パケット インスペクション

ヘッダーフィールド（トラフィック クラス、フローラベル、ペイロード長、次ヘッダー、ホップ リミット、および送信元 IP アドレスや宛先 IP アドレス）は、IPv6 インスペクション用に使用されます。IPv6 ヘッダー フィールドの詳細および説明については、RFC 2474 を参照してください。

IPv6 でのアクセス クラス フィルタリング

IPv6 ACL に基づく、デバイスとの間の着信接続と発信接続のフィルタリングは、ライン コンフィギュレーション モードで **ipv6 access-class** コマンドを使用して実行します。**ipv6 access-class** コマンドは、IPv6 ACL が名前で定義される点を除き、**access-class** コマンドに似ています。IPv6 ACL が着信トラフィックに適用される場合、ACL 内の送信元アドレスは、着信接続の送信元アドレスと照合され、ACL 内の宛先アドレスは、インターフェイス上のローカル デバイス アドレスと照合されます。IPv6 ACL が発信トラフィックに適用される場合、ACL 内の送信元アドレスは、インターフェイス上のローカル デバイス アドレスと照合され、ACL 内の宛先アドレスは、発信接続の送信元アドレスと照合されます。ユーザーが任意の接続を試行できるように、すべての仮想端末回線で同じ制限を設定することを推奨します。

IPv6 アクセス コントロール リストの設定方法

IPv6 トラフィック フィルタリングの設定

トラフィック フィルタリング用の IPv6 ACL の作成および設定

（注） Cisco ASR 1000 プラットフォームの IPv6 ACL には、暗黙の許可ルールは含まれません。IPv6 ネイバー探索プロセスでは、IPv6 ネットワーク層サービスを使用します。したがって、IPv6 ネイバー探索をイネーブルにするには、IPv6 ネイバー探索パケットのインターフェイス上での送受信が許可されるように IPv6 ACL を追加する必要があります。IPv4 では、IPv6 ネイバー探索プロセスと同等のアドレス解決プロトコル（ARP）は、別のデータリンク層プロトコルを使用します。したがってデフォルトでは、IPv4 ACL により、ARP パケットのインターフェイス上での送受信が暗黙的に許可されます。

手順の概要

1. **enable**
2. **configure terminal**
3. **ipv6 access-list** *access-list-name*
4. 次のいずれかを実行します。
   - **permit protocol** {*source-ipv6-prefix/prefix-length* | **any** | **host** *source-ipv6-address*} [*operator* [*port-number*]] {*destination-ipv6-prefix / prefix-length* | **any** | **host** *destination-ipv6-address*} [**operator** [*port-number*]] [**dest-option-type** [*doh-number* | *doh-type*]] [**dscp** *value*] [**flow-label** *value*] [**fragments**] [**log**] [**log-input**] [**mobility**] [**mobility-type** [*mh-number* | *mh-type*]] [**routing**] [**routing-type** *routing-number*] [**sequence** *value*] [**time-range** *name*]
   - **deny** *protocol* {*source-ipv6-prefix*/*prefix-length* | **any** | **host** *source-ipv6-address*} [*operator port-number*]] {*destination-ipv6-prefix/prefix-length* | **any** | **host** *destination-ipv6-address*} [*operator* [*port-number*]] [**dest-option-type** [*doh-number* | *doh-type*]] [**dscp** *value*] [**flow-label** *value*] [**fragments**] [**log**] [**log-input**] [**mobility**] [**mobility-type** [*mh-number* | *mh-type*]] [**routing**] [**routing-type** *routing-number*] [**sequence** *value*] [**time-range** *name*] [**undetermined-transport**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ipv6 access-list** *access-list-name* 例： `Device(config)# ipv6 access-list inbound`	IPv6 ACL を定義し、IPv6 アクセス リスト コンフィギュレーション モードを開始します。 • *access-listname* 引数は、IPv6 ACL の名前を指定します。IPv6 ACL の名前にスペースまたは引用符を含めることはできません。また、先頭を数字にすることはできません。
ステップ 4	次のいずれかを実行します。 • **permit protocol** {*source-ipv6-prefix/prefix-length*	**any**	**host** *source-ipv6-address*} [*operator* [*port-number*]] {*destination-ipv6-prefix / prefix-length*	**any**	**host** *destination-ipv6-address*} [**operator** [*port-number*]] [**dest-option-type** [*doh-number*	*doh-type*]] [**dscp** *value*] [**flow-label** *value*] [**fragments**] [**log**] [**log-input**] [**mobility**] [**mobility-type** [*mh-number*	*mh-type*]] [**routing**]	IPv6 ACL の許可条件または拒否条件を指定します。

	コマンドまたはアクション	目的

	[**routing-type** *routing-number*] [**sequence** *value*] [**time-range** *name*]
	• **deny** *protocol* {*source-ipv6-prefix*/*prefix-length* | **any** | **host** *source-ipv6-address*} [*operator port-number*]] {*destination-ipv6-prefix/prefix-length* | **any** | **host** *destination-ipv6-address*} [*operator* [*port-number*]] [**dest-option-type** [*doh-number* | *doh-type*]] [**dscp** *value*] [**flow-label** *value*] [**fragments**] [**log**] [**log-input**] [**mobility**] [**mobility-type** [*mh-number* | *mh-type*]] [**routing**] [**routing-type** *routing-number*] [**sequence** *value*] [**time-range** *name*] [**undetermined-transport**
	例：
	`Device(config-ipv6-acl)# permit tcp 2001:DB8:0300:0201::/32 eq telnet any`
	例：
	`Device(config-ipv6-acl)# deny tcp host 2001:DB8:1::1 any log-input`	

インターフェイスへの IPv6 ACL の適用

手順の概要

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **ipv6 traffic-filter** *access-list-name* {**in**| **out**}

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 3	**interface** *type number* 例： `Device(config)# interface gigabitethernet 0/0/0`	インターフェイスのタイプおよび番号を指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	**ipv6 traffic-filter** *access-list-name* {**in**| **out**} 例： `Device(config-if)# ipv6 traffic-filter inbound in`	指定した IPv6 アクセス リストを、前のステップで指定したインターフェイスに適用します。

vty へのアクセスの制御

IPv6 ACL の作成によるアクセス クラス フィルタリングの提供

手順の概要

1. **enable**
2. **configure terminal**
3. **ipv6 access-list** *access-list-name*
4. 次のいずれかを実行します。
   - **permit protocol** {*source-ipv6-prefix/prefix-length* | **any** | **host** *source-ipv6-address*} [*operator* [*port-number*]] {*destination-ipv6-prefix / prefix-length* | **any** | **host** *destination-ipv6-address*} [*operator* [*port-number*]] [**dest-option-type** [*doh-number* | *doh-type*]] [**dscp** *value*] [**flow-label** *value*] [**fragments**] [**log**] [**log-input**] [**mobility**] [**mobility-type** [*mh-number* | *mh-type*]] [**routing**] [**routing-type** *routing-number*] [**sequence** *value*] [**time-range** *name*
   - **deny** *protocol* {*source-ipv6-prefix*/*prefix-length* | **any** | **host** *source-ipv6-address*} [*operator port-number*]] {*destination-ipv6-prefix/prefix-length* | **any** | **host** *destination-ipv6-address*} [*operator* [*port-number*]] [**dest-option-type** [*doh-number* | *doh-type*]] [**dscp** *value*] [**flow-label** *value*] [**fragments**] [**log**] [**log-input**] [**mobility**] [**mobility-type** [*mh-number* | *mh-type*]] [**routing**] [**routing-type** *routing-number*] [**sequence** *value*] [**time-range** *name*] [**undetermined-transport**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 3	**ipv6 access-list** *access-list-name* 例： `Device(config)# ipv6 access-list cisco`	IPv6 ACL を定義し、IPv6 アクセス リスト コンフィギュレーション モードを開始します。

ステップ 4	次のいずれかを実行します。
	• **permit protocol** {*source-ipv6-prefix/prefix-length* | **any** | **host** *source-ipv6-address*} [*operator* [*port-number*]] {*destination-ipv6-prefix / prefix-length* | **any** | **host** *destination-ipv6-address*} [*operator* [*port-number*]] [**dest-option-type** [*doh-number* | *doh-type*]] [**dscp** *value*] [**flow-label** *value*] [**fragments**] [**log**] [**log-input**] [**mobility**] [**mobility-type** [*mh-number* | *mh-type*]] [**routing**] [**routing-type** *routing-number*] [**sequence** *value*] [**time-range** *name*
	• **deny** *protocol* {*source-ipv6-prefix*/*prefix-length* | **any** | **host** *source-ipv6-address*} [*operator port-number*]] {*destination-ipv6-prefix/prefix-length* | **any** | **host** *destination-ipv6-address*} [*operator* [*port-number*]] [**dest-option-type** [*doh-number* | *doh-type*]] [**dscp** *value*] [**flow-label** *value*] [**fragments**] [**log**] [**log-input**] [**mobility**] [**mobility-type** [*mh-number* | *mh-type*]] [**routing**] [**routing-type** *routing-number*] [**sequence** *value*] [**time-range** *name*] [**undetermined-transport**
	例：
	`Device(config-ipv6-acl)# permit ipv6 host 2001:DB8:0:4::32 any`
	例：
	`Device(config-ipv6-acl)# deny ipv6 host 2001:DB8:0:6::6 any`
		IPv6 ACL の許可条件または拒否条件を指定します。

仮想端末回線への IPv6 ACL の適用

手順の概要

1. **enable**
2. **configure terminal**
3. **line** [**aux**| **console**| **tty**| **vty**] *line-number*[*ending-line-number*]
4. **ipv6 access-class** *ipv6-access-list-name* {**in**| **out**}

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**line** [**aux**| **console**| **tty**| **vty**] *line-number*[*ending-line-number*] 例： `Device(config)# line vty 0 4`	設定する特定の回線を識別し、ライン コンフィギュレーション モードを開始します。 • この例では、**vty** キーワードを使用して、リモート コンソール アクセス用の仮想端末回線を指定します。
ステップ 4	**ipv6 access-class** *ipv6-access-list-name* {**in**| **out**} 例： `Device(config-line)# ipv6 access-class cisco in`	IPv6 ACL に基づいて、デバイスとの間の着信接続と発信接続をフィルタリングします。

IPv6 アクセス コントロール リストの設定例

例：IPv6 ACL 設定の確認

次の例では、**show ipv6 access-list** コマンドを使用して、IPv6 ACL が正しく設定されていることを確認します。

```
Device> show ipv6 access-list

IPv6 access list inbound
    permit tcp any any eq bgp (8 matches) sequence 10
    permit tcp any any eq telnet  (15 matches) sequence 20
    permit udp any any  sequence 30

IPv6 access list Virtual-Access2.1#427819008151 (per-user)
    permit tcp host 2001:DB8:1::32 eq bgp host 2001:DB8:2::32 eq 11000 sequence 1
    permit tcp host 2001:DB8:1::32 eq telnet host 2001:DB8:2::32 eq 11001 sequence 2
```

例：IPv6 ACL の作成と適用

次に、HTTP アクセスを日中の特定の時間に制限し、許可されていない時間のアクティビティを記録する方法について例を示します。

```
Device# configure terminal
Device(config)# time-range lunchtime
Device(config-time-range)# periodic weekdays 12:00 to 13:00
Device(config-time-range)# exit
Device(config)# ipv6 access-list INBOUND
Device(config-ipv6-acl)# permit tcp any any eq www time-range lunchtime
Device(config-ipv6-acl)# deny tcp any any eq www log-input
Device(config-ipv6-acl)# permit tcp 2001:DB8::/32 any
Device(config-ipv6-acl)# permit udp 2001:DB8::/32 any
Device(config-ipv6-acl)# end
```

例：vty へのアクセスの制御

次の例では、仮想端末回線 0 ～ 4 に着信する接続は、acl1 という名前の IPv6 アクセス リストに基づいてフィルタリングされます。

```
ipv6 access-list acl1
 permit ipv6 host 2001:DB8:0:4::2/32 any
!
line vty 0 4
 ipv6 access-class acl1 in
```

IPv6 アクセス コントロール リストに関する機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *61 : IPv6* アクセス コントロール リストに関する機能情報

機能名	リリース	機能情報
IPv6 サービス：拡張アクセス コントロール リスト	Cisco IOS XE リリース 2.1	標準の IPv6 ACL 機能が拡張されて、IPv6 オプション ヘッダー、および任意でより細かい制御を行うための上位層プロトコル タイプ情報に基づくトラフィック フィルタリングがサポートされています。

第 41 章

IPv6 ACL 未決定トランスポートサポート

IPv6 ACL 未決定トランスポートサポート機能は、完全な上位層ヘッダーが存在しない、誤設定されたパケットをドロップするのに役立ちます。

IPv6 ACL 未決定トランスポートサポートの制約事項

- 未決定トランスポート オプションは拒否アクションと IPv6 プロトコルの Cisco Application Control Engine（ACE）でのみサポートされています。
- 未決定トランスポートが nonfirst パケットのフラグメントには適用されません。

IPv6 ACL 未決定トランスポートサポートに関する情報

IPv6 ACL 未決定トランスポートサポート

ユーザーによる意図しない設定ミスまたはネットワーク上の悪意のある攻撃によって、ネットワーク上のホストに対する運用上の問題が発生する可能性があります。

上位層ヘッダーは、RFC 2460 に説明されているように、IPv6 パケット内の拡張ヘッダー（EH）チェーンの拡張の最後に置かれます。完全な上位層ヘッダーが Ipv6 パケット内にない場合、ルータは、パケットを処理できません。これらのパケットは、誤設定、破損または悪意がある可能性があります。

未決定トランスポートオプションのある IPv6 ACL を使用して、これらのパケットをドロップするよう選択できます。

IPv6 ACL 未決定トランスポートサポートの設定方法

IPv6 ACL 未決定トランスポートサポートの設定

手順の概要

1. **enable**
2. **configure terminal**
3. **ipv6 access-list** *acl-name*
4. **deny ipv6** {*src-addr* | **any**} {*dest-addr* | **any**} [**undetermined-transport**]
5. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ipv6 access-list** *acl-name* 例： `Device(config)# ipv6 access-list acl1`	IPv6 アクセス リストを設定します。
ステップ 4	**deny ipv6** {*src-addr*	**any**} {*dest-addr*	**any**} [**undetermined-transport**] 例： `Device(config-ipv6-acl)# deny ipv6 2001:DB8:0300:0201::/32 2001:DB8:1:1::/64 undetermined-transport`	未決定トランスポートとして、IPv6アクセス リストに対して、拒否状態を設定します。
ステップ 5	**end** 例： `Device(config-ipv6-acl)# end`	特権 EXEC モードに戻ります。

例：IPv6 ACL 未決定トランスポートサポートの例

例：IPv6 ACL 未決定トランスポートサポートの例

```
Device> enable
Device# configure terminal
Device(config)# ipv6 access-list acl1
Device(config-ipv6-acl)# deny ipv6 2001:DB8:0300:0201::/32 2001:DB8:1:1::/64
undetermined-transport
Device(config-ipv6-acl)# end
```

IPv6 ACL 未決定トランスポートサポートのその他の参考資料

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『Cisco IOS Master Command List, All Releases』
IP アクセス リスト コマンド	『*Cisco IOS Security Command Reference*』
IP アクセス リストの設定	『Creating an IP Access List and Applying It to an Interface』

標準および RFC

標準/RFC	タイトル
RFC 2460	インターネット プロトコル、バージョン 6（IPv6）仕様

シスコのテクニカル サポート

説明	リンク
右の URL にアクセスして、シスコのテクニカル サポートを最大限に活用してください。これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

ACL テンプレートに関する機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *62 : ACL* テンプレートに関する機能情報

機能名	リリース	機能情報
IPv6 ACL 未決定トランスポートサポート	Cisco IOS XE リリース 3.15	IPv6 ACL 未決定トランスポートサポート機能は、完全な上位層ヘッダーが存在していない誤って設定されたパケットをドロップするのに役立ちます。 追加または変更されたコマンドはありません。

第 42 章

テンプレート ACL の設定

ユーザー プロファイルが RADIUS 属性 242 またはベンダー固有属性（VSA ）Cisco AVPairs を使用して設定されると、同様のユーザーごとのアクセス コントロール リスト（ACL）は、単一のテンプレート ACL に置き換えられることがあります。つまり、1 つの ACL で多数の類似した ACL を表します。IPv6 テンプレート ACL を使用することで、ACL をサポートするために必要なメモリおよび Ternary Content Addressable Memory（TCAM）リソースを最小限に抑えながら、1 ユーザーあたりの ACL の合計数を増やすことができます。

各サブスクライバが独自の ACL を所有するネットワークでは、ユーザーの IP アドレスを除いて、ACL をユーザーごとに同じとするのが普通です。テンプレート ACL 機能は、システム リソースを節約する 1 つの ACL に多くの一般的なアクセス コントロール要素（ACE ）で ACL をグループ化します。

テンプレート ACL の前提条件

- Cisco ASR 1000 シリーズ ルータ
- Cisco IOS XE リリース 2.4 以降のリリース

テンプレート ACL の制約事項

テンプレート ACL は、RADIUS 属性 242 または VSA Cisco-AVPairs（ip:inacl/outacl）を通じて設定されたユーザーごとの ACL に対してのみ有効になります。その他のタイプの ACL は、テンプレート ACL 機能によって処理されません。

テンプレート ACL 機能は、IPv4 ACL でのみ使用できます。

テンプレート ACL 機能は、ユーザーごとの ACL の次のタイプには利用はできません。

- 時間ベース ACL
- ダイナミック ACL
- 評価 ACL
- 再帰 ACL
- ISG IP セッションで設定された ACL
- IPv6 ACL

テンプレート ACL 機能の無効化

テンプレート ACL 機能を無効にすると、システムは、すべての既存のテンプレート ACL インスタンスを ACL と置き換えます。システムに必要な数の ACL を設定するための十分なリソース（具体的には、TCAM リソース）がない場合、システムは、エラー メッセージを生成し、テンプレート ACL 機能を無効にする要求は失敗します。

テンプレート ACL の設定に関する情報

テンプレート ACL 機能設計

サービス プロバイダーが、AAA サーバーを使用して、RADIUS 属性 242 または Cisco VSA AVPairs を使用する、権限のあるセッションに対する ACL を設定する場合、セッション数は、システムで許容される最大の ACL 数を簡単に上回ります。

各サブスクライバが ACL を有するネットワークでは、ユーザーの IP アドレスを除いて、ACL が各ユーザーに対して同じになることは普通です。テンプレート ACL は、システム リソースを高速で編集し、多くの共通 ACE を持つ ACL を節約する 1 つの ACL にグループ化することで、この問題を軽減します。

テンプレート ACL 機能は、デフォルトで有効になっており、RADIUS 属性 242 または Cisco VSA AVPairs VSA を使用した ACL 設定は、テンプレート ステータスの対象となります。

テンプレート ACL 機能を有効にすると、システムは、すべての設定済みセッション単位の ACL をスキャンおよび評価して、必要なテンプレート ACL を作成します。

テンプレート ACL の無効化

テンプレート ACL 機能を無効にすると、システムは、すべての既存のテンプレート ACL インスタンスを ACL と置き換えます。システムに必要な数の ACL を設定するための十分なリソース（特に TCAM リソース）がない場合、システムは、エラーメッセージを生成し、テンプレート ACL 機能を無効にする要求が失敗します。

そのため、テンプレート ACL 機能を無効にする前に、**show access-list template summary** コマンドを使用して、システム内のテンプレート ACL の数を表示し、この数がシステムの制限を超えているかを確認します。

テンプレート ACL 機能を無効にすると、新しい ACL は、テンプレーティングの対象にはなりません。

複数の ACL

テンプレート ACL 機能を有効にすると、システムは、2 ユーザーごとの ACL が類似している場合を特定し、2 つのユーザーごとの ACL を 1 つのテンプレート ACL に統合します。

たとえば、次の例は、2 人の個別のユーザーに対する 2 つの ACL を示します。

```
ip access-list extended Virtual-Access1.1#1 (PeerIP: 10.1.1.1)
permit igmp any host 10.1.1.1
permit icmp host 10.1.1.1 any
deny ip host 10.31.66.36 host 10.1.1.1
deny tcp host 10.1.1.1 host 10.31.66.36
permit udp any host 10.1.1.1
permit udp host 10.1.1.1 any
permit udp any host 192.168.2.1
permit udp any host 192.168.222.1
permit icmp host 10.55.15.4 host 192.168.2.1
permit udp 10.22.11.0 0.0.0.255 host 192.168.211.2
permit tcp any host 192.168.222.1
permit ip host 10.55.15.4 host 192.168.2.1
permit tcp 10.22.11.0 0.0.0.255 host 192.168.211.2
ip access-list extended Virtual-Access1.1#2 (PeerIP: 10.13.11.2)
permit igmp any host 10.13.11.2
permit icmp host 10.13.11.2 any
deny ip host 10.31.66.36 host 10.13.11.2
deny tcp host 10.13.11.2 host 10.31.66.36
permit udp any host 10.13.11.2
permit udp host 10.13.11.2 any
permit udp any host 192.168.2.1
permit udp any host 192.168.222.1
permit icmp host 10.55.15.4 host 192.168.2.1
permit udp 10.22.11.0 0.0.0.255 host 192.168.211.2
permit tcp any host 192.168.222.1
permit ip host 10.55.15.4 host 192.168.2.1
permit tcp 10.22.11.0 0.0.0.255 host 192.168.211.2
```

テンプレート ACL 機能を有効にすると、システムは、これら 2 つの ACL が類似していることを認識し、次のように、テンプレート ACL を作成します。

```
ip access-list extended Template_1
permit igmp any host <PeerIP>
permit icmp host <PeerIP> any
deny ip host 10.31.66.36 host <PeerIP>
deny tcp host <PeerIP> 10.31.66.36
permit udp any host <PeerIP>
permit udp host <PeerIP> any
permit udp any host 192.168.2.1
permit udp any host 192.168.222.1
permit icmp host 10.55.15.4 host 192.168.2.1
permit udp 10.22.11.0 0.0.0.255 host 192.168.211.2
permit tcp any host 192.168.222.1
```

```
permit ip host 10.55.15.4 host 192.168.2.1
permit tcp 10.22.11.0 0.0.0.255 host 192.168.211.2
```

この例では、ピアの IP アドレスは次のように関連付けられています。

- Virtual-Access1.1#1 10.1.1.1
- Virtual-Access1.1#2 10.13.11.2

2 つの ACL は、1 つのテンプレート ACL に統合され、次のように参照されます。

Template_1(10.1.1.1) への Virtual-Access1.1#1 マップ

Template_1(10.13.11.2) への Virtual-Access1.1#2 マップ

VSA Cisco-AVPairs

テンプレート ACL 処理は、Cisco-AVPairs を使用して設定される ACL に対して発生します。ACL 番号を使用して定義される AVPairs のみが、テンプレーティングプロセスの対象になります。

テンプレーティングの対象となるために、入力 ACL のための AVPairs は、次の形式に従う必要があります。

ip:inacl#number={standard-access-control-list | extended-access-control-list}

例：ip:inacl#10=deny ip any 10.13.16.0 0.0.0.255

テンプレーティングの対象になるためには、出力 ACL のための AVPairs は、次の形式に従う必要があります:

ip:outacl#number={standard-access-control-list | extended-access-control-list}

例：ip:outacl#200=permit ip any any

Cisco-AVPairs の詳細については、『Cisco IOS ISG RADIUS CoA インターフェイス ガイド』の「Cisco ベンダー固有 AVPair Attributes」のセクションを参照してください。

RADIUS 属性 242

RADIUS 属性 242 を使用して設定される ACL に対して、テンプレート ACL 処理が発生します。属性 242 は、IP データ フィルタに対して、次の形式があります。

Ascend-Data-Filter = “ip <dir> <action> [dstip <dest_ipaddr\subnet_mask>] [srcp <src_ipaddr\subnet_mask>] [<proto> [dstport <cmp> <value>] [srcport <cmp> <value>] [<est>]]”

次の表で、IP データ フィルタの属性 242 エントリ内の要素について説明します。

表 *63 : IP* データ フィルタ構文要素

要素	説明
ip	IP アドレスを指定します。

要素	説明
<dir>	フィルタの方向を指定します。有効値は、**in**（ルータに着信するパケットのフィルタリング）または、**out**（ルータから発信するパケットのフィルタリング）です。
<action>	ルータがフィルタに一致したパケットに取るべきアクションを指定します。有効な値は **forward** または **drop** です。
dstip <dest_ipaddr\subnet_mask>	宛先 IP アドレス フィルタリングを有効にします。宛先アドレスが **<dest_ipaddr>** の値に一致するパケットに適用されます。アドレスのサブネット マスクの部分が存在する場合、ルータはマスクされたビットのみを比較します。0.0.0.0 に **<dest_ipaddr>** を設定するか、またはこのキーワードがなければ、フィルタは、すべての IP パケットに一致します。
srcp<src_ipaddr\subnet_mask>	送信元 IP アドレス フィルタリングを有効にします。送信元アドレスが **<src_ipaddr>** の値に一致するパケットに適用されます。アドレスのサブネット マスクの部分が存在する場合、ルータはマスクされたビットのみを比較します。0.0.0.0 に **<src_ipaddr>** を設定するか、またはこのキーワードがなければ、フィルタは、すべての IP パケットに一致します。
<proto>	名前または番号として指定するプロトコルを指定します。プロトコル フィールドがこの値に一致するパケットに適用されます。使用できる名前と番号は **icmp**（**1**）、**tcp**（**6**）、**udp**（**17**）、および **ospf**（**89**）です。この値をゼロ（0）に設定すると、フィルタは、一切のプロトコルに一致します。
dstport <cmp> <value>	宛先ポートフィルタリングを有効にします。このキーワードは、**<proto>** が **tcp**（**6**）または **udp**（**17**）に設定されている場合に限り有効です。宛先ポートを指定しないと、フィルタは、一切のポートと一致します。 **<cmp>** は、指定された **<value>** と実際の宛先ポートとを比較する方法を定義します。この値として **<**、**=**、**>**、または **!** を使用できます。 **<value>** 名前も番号も使用可能です。使用できる名前と番号は **ftp-data (20)**、**ftp (21)**、**telnet (23)**、**nameserver (42)**、**domain (53)**、**tftp (69)**、**gopher (70)**、**finger (79)**、**www (80)**、**kerberos (88)**、**hostname (101)**、**nntp (119)**、**ntp (123)**、**exec (512)**、**login (513)**、**cmd (514)**、および **talk (517)** です。
srcport <cmp> <value>	送信元ポートフィルタリングを有効にします。このキーワードは、**<proto>** が **tcp**（**6**）または **udp**（**17**）に設定されている場合に限り有効です。送信元ポートを指定しないと、フィルタは、一切のポートと一致します。 **<cmp>** は、指定された **<value>** と実際の宛先ポートとを比較する方法を定義します。この値として **<**、**=**、**>**、または **!** を使用できます。 **<value>** 名前も番号も使用可能です。使用できる名前と番号は **ftp-data**（**20**）、**ftp**（**21**）、**telnet**（**23**）、**nameserver**（**42**）、**domain**（**53**）、**tftp**（**69**）、**gopher**（**70**）、**finger**（**79**）、**www**（**80**）、**kerberos**（**88**）、**hostname**（**101**）、**nntp**（**119**）、**ntp**（**123**）、**exec**（**512**）、**login**（**513**）、**cmd**（**514**）、および **talk**（**517**）です。

要素	説明
<est>	1 に設定すると、TCP セッションがすでに確立されている場合にのみ、パケット フィルタと一致していると指定します。この引数は、**<proto>** が **tcp (6)** に設定されている場合に限り有効です。

「RADIUS 属性 242 IP データ フィルタ エントリ」は、4 つの属性 242 IP データフィルタエントリを示します。

RADIUS 属性 242 IP データフィルタエントリ

```
Ascend-Data-Filter=”ip in drop”
Ascend-Data-Filter=”ip out forward tcp”
Ascend-Data-Filter=”ip out forward tcp dstip 10.0.200.3/16 srcip 10.0.200.25/16
dstport!=telnet”
Ascend-Data-Filter=”ip out forward tcp dstip 10.0.200.3/16 srcip 10.0.200.25/16 icmp”
```

テンプレート ACL の設定方法

ACL が RADIUS 属性 242 または VSA Cisco-AVPairs を使用して設定されると、ACL は、デフォルトでは有効になりません。

テンプレート ACL の最大サイズの設定

デフォルトでは、テンプレートの ACL ステータスは 100 台以下のルールの ACL に限定されます。ただし、この制限を低い値に設定できます。テンプレート ACL とみなされるため、既存の ACL は、以下のようなルールの最大数を設定するには、このセクションの手順を実行してください:

手順の概要

1. **enable**
2. **configure terminal**
3. **access-list template** *number*
4. **exit**
5. **show access-list template summary**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。

	コマンドまたはアクション	目的
ステップ 2	**configure terminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**access-list template** *number* 例： `Router(config)# access-list template 50`	テンプレート ACL の処理をイネーブルにします。 指定された数のルール（またはより少ないルール）の ACL だけがテンプレートのステータスの対象となります。
ステップ 4	**exit** 例： `Router(config)# exit`	グローバル コンフィギュレーション モードを終了します。
ステップ 5	**show access-list template summary** 例： `Router# show access-list template summary`	（任意）ACL テンプレートに関する要約情報が表示されます。

トラブルシューティングのヒント

次のコマンドを使用すると、テンプレート ACL をトラブルシューティングできます。

- **show access-list template**
- show platform hardware qfp active classification class-group-manager class-group client acl all
- **show platform hardware qfp active feature acl** {**control** | **node** *acl-node-id*}
- show platform software access-list

テンプレート ACL の設定例

テンプレート ACL の最大サイズの例

次の例では、テンプレートのステータスを 50 と対象するために ACL が含むことができるルールの最大数の設定方法を示しています。ルールの数は同じか、または 50 よりも少ない ACL のみがテンプレート ステータスの対象となります。

```
Router> enable

Router# configure terminal
```

```
Router(config)# access-list template 50
Router(config)# exit
```

ACL のテンプレートの概要情報を示す例

以下の例は、システム内の全 ACL 用の要約情報を表示する方法を示しています。このコマンドからの出力には、次の情報が含まれています。

- テンプレート ACL ごとのルールの最大数
- 発見されたアクティブなテンプレート数
- これらのテンプレートによって置き換えられた ACL 数
- レッドブラックツリー内の要素数

```
Router# show access-list template summary
Maximum rules per template ACL = 100
Templates active = 9
Number of ACLs those templates represent = 14769
Number of tree elements = 13
```

レッドブラックツリー要素

ツリー要素の数は、レッドブラックツリー内の要素の数です。各テンプレートは、レッドブラックツリー内の一意のエントリを 1 つ含みます。システムは、ピア IP アドレスをマスクする各 ACL 上の巡回冗長検査（CRC）を計算し、レッドブラックツリーに CRC を送信します。次に例を示します。

システムに 9 つのテンプレート（14769 個の ACL を表す）、および 13 のツリーの要素があります。レッドブラックツリー内で各テンプレートに一意のエントリが 1 つしかない場合、その他 4 つのツリー要素は、システムには、テンプレート化されていない 4 個のユーザーあたりの ACL が含まれているということです。

ACL のテンプレート ツリー情報を示す例

以下の例は、システム内の全 ACL 用のレッドブラックツリー情報を表示する方法を示しています。

このコマンドからの出力には、次の情報が含まれています。

- レッドブラックツリー上の ACL 名
- 元の CRC32 値
- ACL のユーザー数
- 計算された CRC32 値

```
Router# show access-list template tree
```

```
ACL name      OrigCRC   Count  CalcCRC
4Temp_1073741891108      59DAB725   98  59DAB725
```

その他の参考資料

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『Cisco IOS Master Commands List, All Releases』
セキュリティ コマンド：コマンド構文の詳細、コマンド モード、コマンド履歴、デフォルト設定、使用上のガイドライン、および例	『*Cisco IOS Security Command Reference*』
セキュア シェル	セキュア シェルおよびセキュア シェル バージョン 2 サポート設定の機能モジュール。
認証と認可の設定	認証設定、認可設定、およびアカウンティング設定の機能モジュール。

標準

標準	タイトル
なし	--

MIB

MIB	MIB のリンク
なし	選択したプラットフォーム、Cisco ソフトウェア リリース、およびフィーチャ セットの MIB を検索してダウンロードする場合は、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

RFC

RFC	タイトル
この機能によりサポートされた新規 RFC または改訂 RFC はありません。またこの機能による既存 RFC のサポートに変更はありません。	--

シスコのテクニカル サポート

説明	リンク
右の URL にアクセスして、シスコのテクニカル サポートを最大限に活用してください。これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

ACL テンプレートに関する機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *64 : ACL* テンプレートに関する機能情報

機能名	リリース	機能情報
ACL テンプレート	12.2(28) SB 12.2(31) SB2 Cisco IOS XE リリース 2.4	12.2(28)SB では、この機能が Cisco 10000 シリーズ ルータで追加されました。 12.2(31)SB2 では、PRE3 のサポートが追加されました。 この機能は、Cisco IOS XE Release 2.4 で、Cisco ASR 1000 シリーズ ルータに実装されました。 次のコマンドが導入または変更されました。**access-list template, show access-list template**

第 43 章

IPv6 テンプレート ACL

ベンダー固有属性（VSA）の Cisco AV ペアを使用してユーザー プロファイルが設定されている場合は、類似した 1 ユーザー単位の IPv6 ACL を 1 つのテンプレート ACL で置き換えることができます。つまり、1 つの ACL で多数の類似した ACL を表します。IPv6 テンプレート ACL を使用することで、ACL をサポートするために必要なメモリおよび Ternary Content Addressable Memory（TCAM）リソースを最小限に抑えながら、1 ユーザーあたりの ACL の合計数を増やすことができます。

IPv6 テンプレート ACL 機能では、次の ACL フィールドを使用してテンプレートを作成します。

- IPv6 の送信元アドレスおよび宛先アドレス
- すべての関連ポート（0 ～ 65535）を含む TCP および UDP
- ICMP ネイバー探索アドバタイズメントおよび要請
- 指定した DSCP 値による IPv6 DSCP

この機能により、ACL の名前はたとえば次のように動的に生成されます。

- 6Temp_#152875854573 - 親 ACL のテンプレートとして動的に生成されたテンプレート名の例
- Virtual-Access2.32135#152875854573 - 子 ACL またはテンプレートの一部とされていない ACL の例。

IPv6 ACL に関する情報：テンプレート ACL

IPv6 テンプレート ACL

ベンダー固有属性（VSA）の Cisco AV ペアを使用してユーザー プロファイルが設定されている場合は、類似した 1 ユーザー単位の IPv6 ACL を 1 つのテンプレート ACL で置き換えることができます。つまり、1 つの ACL で多数の類似した ACL を表します。IPv6 テンプレート ACL を使用することで、ACL をサポートするために必要なメモリおよび Ternary Content Addressable Memory（TCAM）リソースを最小限に抑えながら、1 ユーザーあたりの ACL の合計数を増やすことができます。

IPv6 テンプレート ACL 機能では、次の ACL フィールドを使用してテンプレートを作成します。

- IPv6 の送信元アドレスおよび宛先アドレス
- すべての関連ポート（0 ～ 65535）を含む TCP および UDP
- ICMP ネイバー探索アドバタイズメントおよび要請
- 指定した DSCP 値による IPv6 DSCP

この機能により、ACL の名前はたとえば次のように動的に生成されます。

- 6Temp_#152875854573 - 親 ACL のテンプレートとして動的に生成されたテンプレート名の例
- Virtual-Access2.32135#152875854573 - 子 ACL またはテンプレートの一部とされていない ACL の例。

IPv6 ACL を有効にする方法：テンプレート ACL

IPv6 テンプレートの処理の有効化

手順の概要

1. **enable**
2. **configure terminal**
3. **access-list template** [*number-of-rules*]
4. **exit**
5. **show access-list template** {**summary** | *aclname* | **exceed** *number* | **tree**}

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**access-list template** [*number-of-rules*] 例： `Router(config)# access-list template 50`	テンプレート ACL の処理をイネーブルにします。 • このタスクの例では、50以下のルールを設定した ACL がテンプレート ACL ステータスとして見なされるように指定しています。 • *number-of-rules* 引数のデフォルトは 100 です。
ステップ 4	**exit** 例： `Router(config)# exit`	グローバル コンフィギュレーション モードを終了して、ルータを特権 EXEC モードにします。
ステップ 5	**show access-list template** {**summary** | *aclname* | **exceed** *number* | **tree**} 例： `Router# show access-list template summary`	ACL テンプレートの情報を表示します。

IPv6 ACL の設定例：テンプレート ACL

例：IPv6 テンプレート ACL の処理

この例では、内容は同じでも、名前が ACL1 と ACL2 で異なります。

```
ipv6 access-list extended ACL1 (PeerIP: 2001:1::1/64)
permit igmp any                  2003:1::1/64
permit icmp 2002:5::B/64         any
permit udp  any                  host 2004:1::5
permit udp  any                  host 2002:2BC::a
permit icmp host 2001:BC::7      host 2003:3::7
ipv6 access-list extended ACL2 (PeerIP: 2007:2::7/64)
permit igmp any                  2003:1::1/64
permit icmp 2002:5::B/64         any
```

```
permit udp  any                 host 2004:1::5
permit udp  any                 host 2002:2BC::a
permit icmp host 2001:BC::7     host 2003:3::7
```

これらの ACL のテンプレートは次のとおりです。

```
ipv6 access-list extended Template_1
permit igmp any                 2003:1::1/64
permit icmp 2002:5::B/64        any
permit udp  any                 host 2004:1::5
permit udp  any                 host 2002:2BC::a
permit icmp host 2001:BC::7     host 2003:3::7
```

その他の参考資料

関連資料

関連項目	マニュアル タイトル
IPv6 アドレッシングと接続	『*IPv6 Configuration Guide*』
IPv6 コマンド	『*Cisco IOS IPv6 Command Reference*』
Cisco IOS IPv6 機能	『*Cisco IOS IPv6 Feature Mapping*』

標準および RFC

標準/RFC	タイトル
IPv6 に関する RFC	*IPv6 RFCs*

MIB

選択したプラットフォーム、Cisco IOS リリース、およびフィーチャ セットに関する MIB を探してダウンロードするには、次の URL にある Cisco MIB Locator を使用します。

http://www.cisco.com/go/mibs

シスコのテクニカル サポート

説明	リンク
右の URL にアクセスして、シスコのテクニカル サポートを最大限に活用してください。これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

IPv6 ACL - テンプレート ACL に関する機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *65 : IPv6 ACL* - テンプレート *ACL* に関する機能情報

機能名	リリース	機能情報
IPv6 ACL - テンプレート ACL	Cisco IOS XE リリース 3.2S	この機能により、類似のユーザーごとの IPv6 ACL を単一のテンプレート ACL に置き換えることができます。 次のコマンドが導入または変更されました。**access-list template**、**show access-list template**

第 44 章

IPv4 ACL チェーニング サポート

マルチアクセス コントロール リストとも呼ばれる ACL チェーニングにより、アクセス コントロール リスト（ACL）を分割することができます。このモジュールでは、IPv4 ACL チェーニング サポートによって ACL を共通 ACL とユーザー専用 ACL に明示的に分割する方法、および両 ACL をデバイスでのトラフィック フィルタリングのためにバインドする方法について説明します。この方法では、Ternary Content Addressable Memory（TCAM）内の共通 ACL は複数のターゲットにより共有され、これによりリソース使用量が削減されます。

IPv4 ACL チェーニング サポートの制限事項

- 単一のアクセス コントロール リスト（ACL）を、同じ方向の同じターゲットに対する共通、標準の両 ACL に使用することはできません。
- ACL チェーニングはセキュリティ ACL にのみ適用されます。サービス品質（QoS）、ファイアウォール サービス モジュール（FW）、ポリシーベース ルーティング（PBR）などのフィーチャ ポリシーではサポートされません。
- 共通 ACL ではターゲットごとの統計情報はサポートされません。

IPv4 ACL チェーニング サポートに関する情報

ACL チェーニングの概要

パケット フィルタリング プロセスは、1 つのインターフェイスの 1 つの方向および 1 つのプロトコルごとに適用される単一のアクセス コントロール リスト（ACL）のみをサポートします。そのため、多数のインターフェイスに共通 ACL エントリが必要な場合、管理性と拡張性の問題が生じます。そのようなインターフェイスにはすべて重複アクセス コントロール エントリ（ACE）が設定されており、共通 ACE の変更はすべての ACL で行われる必要があります。

インターネット サービス プロバイダー（ISP）のエッジ ボックスの典型的な ACL には次の 2 組の ACE が含まれます。

- 共通 ISP 専用 ACE
- 顧客/インターフェイス専用 ACE

これらのアドレスブロックは、ISPの保護されたインフラストラクチャ ネットワークへのアクセスを拒否するため、および顧客の送信元アドレスブロックのみを許可することでスプーフィングを防ぐために行われます。この結果、インターフェイスごとに一意の ACL が設定され、ほとんどの ACE がデバイス上のすべての ACL で共通になります。ACL をプロビジョニングし、変更するのは非常に面倒ですが、ACEを変更すれば全ターゲットに影響を及ぼすことができます。

IPv4 ACL チェーニング サポート

IPv4 ACL チェーニング サポートを使用して、アクセス コントロール リスト（ACL）を共通 ACL と顧客専用 ACL に分割したり、両 ACL を共通セッションにアタッチすることができます。この方法では、共通 ACL を 1 コピーのみ Ternary Content Addressable Memory（TCAM）にアタッチしこれを全ユーザーで共有することで、共通 ACE の維持が簡略化されます。

IPv4 ACL チェーニング機能により、次の 2 つの IPv4 ACL を 1 方向ごとに 1 つのインターフェイスでアクティブにできます。

- 共通
- 標準
- 共通と標準

（注） 1 つのインターフェイスで共通と標準の両 ACL を設定している場合、共通 ACL が標準 ACL に優先されます。

IPv4 ACL チェーニング サポートの設定方法

ACL チェーニングは、**ip traffic filter** コマンドの拡張によりサポートされます。

ip traffic filter コマンドは追加式ではありません。このコマンドを使用すると、このコマンドの以前のインスタンスが置き換えられます。

詳細については、『Security Configuration Guide: Access Control Lists Configuration Guide』の「*IPv6 ACL Chaining with a Common ACL*」セクションを参照してください。

共通 ACL を受け入れるインターフェイスの設定

このタスクを実行すると、インターフェイス固有のACLとともに、共通のアクセス コントロール リスト（ACL）を受け入れるようにインターフェイスを設定できます。

手順の概要

1. **enable**
2. **configure terminal**
3. **interface** *type number*}
4. **ip access-group** {**common** {*common-access-list-name* {*regular-access-list* | **acl**}} {**in** | **out**}}
5. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface** *type number*} 例： `Device(config)# interface gigabitethernet 0/0/0`	インターフェイス（この場合、gigabitethernet interface）を設定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	**ip access-group** {**common** {*common-access-list-name* {*regular-access-list*	**acl**}} {**in**	**out**}} 例： `Device(config)# ipv4 access-group common acl-p acl1 in`	インターフェイス固有の ACL とともに、共通 ACL を受け入れるようにインターフェイスを設定します。

	コマンドまたはアクション	目的
ステップ 5	**end** 例： `Device(config-if)# end`	（任意）コンフィギュレーションモードを終了し、特権 EXEC モードに戻ります。

IPv4 ACL チェーニング サポートの設定例

ここでは、共通アクセス コントロール リスト（ACL）の設定例を示します。

例：共通 ACL を受け入れるインターフェイスの設定

次に、ACL を明示的に削除しないでインターフェイスで設定したアクセス コントロール リスト（ACL）を交換する方法例を示します。

```
interface gigabitethernet 0/0/0
ipv4 access-group common  C_acl ACL1 in
end
replace interface acl ACL1 by ACL2
interface gigabitethernet 0/0/0
ipv4 access-group common  C_acl ACL2 in
end
```

次に、インターフェイスから共通 ACL を明示的に削除しないと、共通 ACL をインターフェイスで交換できない方法例を示します。

```
interface gigabitethernet 0/0/0
ipv4 access-group common  C_acl1 ACL1 in
end
change the common acl to C_acl2
interface gigabitethernet 0/0/0
no ipv4 access-group common  C_acl1  ACL1 in
end
interface gigabitethernet 0/0/0
ipv4 access-group common  C_acl2  ACL1 in
end
```

（注） 共通 ACL を再設定する際、ライン カードの他のインターフェイスが共通 ACL に取り付けられないことを確認する必要があります。

（注） 共通 ACL とインターフェイス ACL の両方をインターフェイスに取り付け、その一方をインターフェイスで再構成すると、他は自動的に削除されます。

次に、インターフェイス ACL の削除方法を示します。

```
interface gigabitethernet 0/0/0
ipv4 access-group common C_acl1 ACL1 in
end
```

IPv4 ACL チェーニング サポートの追加参考資料

関連資料

関連項目	マニュアル タイトル
IPv6 ACL チェーニング サポート	
セキュリティ コマンド	• 『Cisco IOS Security Command Reference: Commands A to C』 • 『Cisco IOS Security Command Reference: Commands D to L』 • 『Cisco IOS Security Command Reference: Commands M to R』 • 『Cisco IOS Security Command Reference: Commands S to Z』

シスコのテクニカル サポート

説明	リンク
シスコのサポート Web サイトでは、シスコの製品やテクノロジーに関するトラブルシューティングにお役立ていただけるように、マニュアルやツールをはじめとする豊富なオンライン リソースを提供しています。 お使いの製品のセキュリティ情報や技術情報を入手するために、Cisco Notification Service（Field Notice からアクセス）、Cisco Technical Services Newsletter、Really Simple Syndication（RSS）フィードなどの各種サービスに加入できます。 シスコのサポート Web サイトのツールにアクセスする際は、Cisco.com のユーザ ID およびパスワードが必要です。	http://www.cisco.com/support

IPv4 ACL チェーニング サポートに関する機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *66 : IPv4 ACL* チェーニング サポートに関する機能情報

機能名	リリース	機能情報
IPv4 ACL チェーニング サポート	Cisco IOS XE リリース 3.11S Cisco IOS XE リリース 3.6E	IPv4 ACL チェーニング サポートは、アクセス コントロール リスト（ACL ）を明示的に共通およびユーザー固有の ACL に分割して、両方の ACL をデバイス上でのトラフィック フィルタリングのためのセッションにバインドする方法について説明します。この方法では、Ternary Content Addressable Memory（TCAM）内の共通 ACL は複数のターゲットにより共有され、これによりリソース使用量が削減されます。 次のコマンドが導入または変更されました。**ip access-group command**

第 45 章

共通 ACL による IPv6 ACL チェーニング

マルチアクセス コントロール リストとも呼ばれる ACL チェーニングにより、ACL を分割することができます。このマニュアルでは、IPv6 ACL チェーニング サポートによって ACL を共通 ACL とユーザー専用 ACL に明示的に分割する方法、および両 ACL をデバイスでのトラフィック フィルタリングのためにバインドする方法について説明します。この方法では、Ternary Content Addressable Memory（TCAM）内の共通 ACL は複数のターゲットにより共有され、これによりリソース使用量が削減されます。

共通 ACL による IPv6 ACL チェーニングに関する情報

ACL チェーニングの概要

パケット フィルタリング プロセスは、1 つのインターフェイスの 1 つの方向および 1 つのプロトコルごとに適用される単一のアクセス コントロール リスト（ACL）のみをサポートします。そのため、多数のインターフェイスに共通 ACL エントリが必要な場合、管理性と拡張性の問題が生じます。そのようなインターフェイスにはすべて重複アクセス コントロール エントリ（ACE）が設定されており、共通 ACE の変更はすべての ACL で行われる必要があります。

インターネット サービス プロバイダー（ISP）のエッジ ボックスの典型的な ACL には次の 2 組の ACE が含まれます。

- 共通 ISP 専用 ACE
- 顧客/インターフェイス専用 ACE

これらのアドレスブロックは、ISP の保護されたインフラストラクチャ ネットワークへのアクセスを拒否するため、および顧客の送信元アドレスブロックのみを許可することでスプーフィングを防ぐために行われます。この結果、インターフェイスごとに一意の ACL が設定され、

ほとんどの ACE がデバイス上のすべての ACL で共通になります。ACL をプロビジョニングし、変更するのは非常に面倒ですが、ACE を変更すれば全ターゲットに影響を及ぼすことができます。

共通 ACL による IPv6 ACL チェーニング

IPv6 ACL チェーニングを使用して、トラフィック フィルタを次の ACL とチェーニングできます。

- 共通 ACL
- 専用 ACL
- 共通 ACL と専用 ACL

各アクセス コントロール リスト（ACL）は順に照合されます。たとえば、共通 ACL と専用 ACL の両方を指定している場合、パケットはまず共通 ACL に対して照合され、一致が見つからなければ専用 ACL に対して照合されます。

（注） 任意の IPv6 ACL を共通または専用 ACL としてトラフィック フィルタで設定できます。ただし、同じ ACL を同じトラフィック フィルタで共通と専用の両方として指定することはできません。

共通 ACL による IPv6 ACL チェーニングの設定方法

始める前に

IPv6 ACL チェーニングは、既存の IPv6 トラフィック フィルタ コマンド **ipv6 traffic-filter** [**common** *common-acl*] [*specific-acl*] [**in** | **out**] の拡張機能を使用して、インターフェイス上で設定します。

（注） 次のいずれかを設定できます。

- 共通 ACL のみ。例：**ipv6 traffic-filter common** *common-acl*
- 特定の ACL のみ。例：**ipv6 traffic-filter** *common-acl*
- 両方の ACL。例：**ipv6 traffic-filter common** *common-acl specific-acl*

ipv6 traffic-filter コマンドは追加式ではありません。このコマンドを使用すると、このコマンドの以前のインスタンスが置き換えられます。たとえば、コマンド シーケンス **ipv6 traffic-filter** [**common** *common-acl*] [*specific-acl*] **in** **ipv6 traffic-filter** [*specific-acl*] **in** は、共通 ACL とトラフィック フィルタをバインディングし、共通 ACL を削除してから、特定の ACL をバインディングします。

インターフェイスへの IPv6 ACL の設定

このタスクを実行すると、インターフェイス固有のACLとともに、共通のアクセスコントロール リスト（ACL）を受け入れるようにインターフェイスを設定できます。

手順の概要

1. **enable**
2. **configure terminal**
3. **interface** *type number*}
4. **ipv6 traffic filter** {*common-access-list-name* {**in** | **out**}}
5. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface** *type number*} 例： `Device(config)# interface gigabitethernet 0/0/0`	インターフェイスのタイプおよび番号を指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	**ipv6 traffic filter** {*common-access-list-name* {**in**	**out**}} 例： `Device(config)# ipv6 traffic-filter outbound out`	指定した IPv6 アクセス リストを、前のステップで指定したインターフェイスに適用します。
ステップ 5	**end** 例： `Device(config-if)# end`	（任意）コンフィギュレーションモードを終了し、特権 EXEC モードに戻ります。

共通 ACL による IPv6 ACL チェーニングの設定例

特定の順序でなくても、次の組み合わせを設定できます。

- 共通 ACL。例： **ipv6 traffic-filter common** *common-acl* **in**
- 特定の ACL。例： **ipv6 traffic-filter** *specific-acl* **in**

- 両方の ACL。例： **ipv6 traffic-filter common** *common-acl* *specific-acl* **in**

例：共通 ACL を受け入れるインターフェイスの設定

次に、ACL を明示的に削除しないでインターフェイスで設定したアクセス コントロール リスト（ACL）を交換する方法例を示します。

```
interface gigabitethernet 0/0/0
ipv6 access-group common  C_acl ACL1 in
end
replace interface acl ACL1 by ACL2
interface gigabitethernet 0/0/0
ipv6 access-group common  C_acl ACL2 in
end
```

次の例では、共通 ACL をインターフェイスから削除する方法を示します。インターフェイスから共通 ACL を明示的に削除しないと、共通 ACL をインターフェイスで交換できません。

```
interface gigabitethernet 0/0/0
ipv6 access-group common  C_acl1 ACL1 in
end
change the common acl to C_acl2
interface gigabitethernet 0/0/0
no ipv6 access-group common  C_acl1  ACL1 in
end
interface gigabitethernet 0/0/0
ipv6 access-group common  C_acl2  ACL1 in
end
```

（注） 共通 ACL を再設定する際、ライン カードの他のインターフェイスが共通 ACL に取り付けられないことを確認する必要があります。

（注） 共通 ACL とインターフェイス ACL の両方をインターフェイスに取り付け、その一方をインターフェイスで再構成すると、他は自動的に削除されます。

次に、インターフェイス ACL を削除する方法を示します。

```
interface gigabitethernet 0/0/0
ipv6 access-group common C_acl1 ACL1 in
end
```

共通 ACL による IPv6 ACL チェーニングの追加情報

関連資料

関連項目	マニュアル タイトル
IPv4 ACL チェーニング サポート	『Security Configuration Guide: Access Control Lists, Cisco IOS XE Release 3S』
セキュリティ コマンド	• 『Cisco IOS Security Command Reference: Commands A to C』 • 『Cisco IOS Security Command Reference: Commands D to L』 • 『Cisco IOS Security Command Reference: Commands M to R』 • 『Cisco IOS Security Command Reference: Commands S to Z』

シスコのテクニカル サポート

説明	リンク
シスコのサポート Web サイトでは、シスコの製品やテクノロジーに関するトラブルシューティングにお役立ていただけるように、マニュアルやツールをはじめとする豊富なオンライン リソースを提供しています。 お使いの製品のセキュリティ情報や技術情報を入手するために、Cisco Notification Service（Field Notice からアクセス）、Cisco Technical Services Newsletter、Really Simple Syndication（RSS）フィードなどの各種サービスに加入できます。 シスコのサポート Web サイトのツールにアクセスする際は、Cisco.com のユーザ ID およびパスワードが必要です。	http://www.cisco.com/support

共通 ACL による IPv6 ACL チェーニングに関する機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *67 :* 共通 *ACL* による *IPv6 ACL* チェーニングに関する機能情報

機能名	リリース	機能情報
共通 ACL による IPv6 ACL チェーニング	Cisco IOS XE リリース 3.11S Cisco IOS XE リリース 3.6E	ACL チェーニング機能（別名、マルチ ACL）により、IPv6 トラフィック フィルタのアクセス コントロール リスト（ACL ）を明示的にコモンおよびセッション単位の ACL に分割できます。このように、使用される共通のアクセス コントロール エントリ（ACE）は、Ternary Content Addressable Memory（TCAM）内のセッションごとに各 ACL エントリのリソース使用量を減らします。 次のコマンドが導入または変更されました。**ip access-group common**

第 46 章

ホップ バイ ホップ フィルタリングに対応するための IPv6 ACL の拡張

ホップ バイ ホップ フィルタリングに対応するための IPv6 ACL の拡張機能により、ホップ バイ ホップ拡張ヘッダーを含む可能性がある IPv6 トラフィックを制御することができます。アクセス コントロール リスト（ACL）を設定して、すべてのホップ バイ ホップ トラフィックを拒否するか、またはプロトコルに基づいて選択的にトラフィックを許可することができます。

ホップバイ ホップフィルタリングに対応するための IPv6 ACL の拡張に関する情報

ACL およびトラフィック転送

IPv6 アクセス コントロール リスト（ACL）は、デバイス インターフェイスでブロックされるトラフィックと転送されるトラフィックを決定します。ACL を使用すると、特定のインターフェイスへの着信および発信を、送信元アドレスと宛先アドレスに基づいてフィルタリングできます。**ipv6 access-list** コマンドを使用して IPv6 ACL を定義し、**deny** および **permit** コマンドを使用してその条件を構成します。

ホップ バイ ホップ フィルタリングに対応するための IPv6 ACL の拡張機能は、上位層プロトコル タイプでのトラフィック フィルタリングをサポートするために RFC 2460 を実装します。

ホップバイ ホップ フィルタリングに対応するための IPv6 ACL の拡張の設定方法

ホップ バイ ホップ フィルタリングに対応するための IPv6 ACL の拡張の設定

手順の概要

1. **enable**
2. **configure terminal**
3. **ipv6 access-list** *access-list-name*
4. **permit** *protocol* {*source-ipv6-prefix/prefix-length* | **any** | **host** *source-ipv6-address* | **auth**} [*operator* [*port-number*]] {*destination-ipv6-prefix/prefix-length* | **any** | **host** *destination-ipv6-address* | **auth**} [*operator* [*port-number*]] [**dest-option-type** [*header-number* | *header-type*]] [**dscp** *value*] [**flow-label** *value*] [**fragments**] [**hbh**] [**log**] [**log-input**] [**mobility**] [**mobility-type** [*mh-number* | *mh-type*]] [**reflect** *name* [**timeout** *value*]] [**routing**] [**routing-type** *routing-number*] [**sequence** *value*] [**time-range** *name*]
5. **deny** *protocol* {*source-ipv6-prefix/prefix-length* | **any** | **host** *source-ipv6-address* | **auth**} [*operator* [*port-number*]] {*destination-ipv6-prefix/prefix-length* | **any** | **host** *destination-ipv6-address* | **auth**} [*operator* [*port-number*]] [**dest-option-type** [*header-number* | *header-type*]] [**dscp** *value*] [**flow-label** *value*] [**fragments**] [**hbh**] [**log**] [**log-input**] [**mobility**] [**mobility-type** [*mh-number* | *mh-type*]] [**routing**] [**routing-type** *routing-number*] [**sequence** *value*] [**time-range** *name*] [**undetermined-transport**]
6. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ipv6 access-list** *access-list-name* 例： `Device(config)# ipv6 access-list hbh-acl`	IPv6 ACL を定義し、IPv6 アクセス リスト コンフィギュレーション モードを開始します。
ステップ 4	**permit** *protocol* {*source-ipv6-prefix/prefix-length*	**any**	**host** *source-ipv6-address*	**auth**} [*operator* [*port-number*]] {*destination-ipv6-prefix/prefix-length*	**any**	IPv6 ACL の許可条件を設定します。

	コマンドまたはアクション	目的
	| **host** *destination-ipv6-address* | **auth**} [*operator* [*port-number*]] [**dest-option-type** [*header-number* | *header-type*]] [**dscp** *value*] [**flow-label** *value*] [**fragments**] [**hbh**] [**log**] [**log-input**] [**mobility**] [**mobility-type** [*mh-number* | *mh-type*]] [**reflect** *name* [**timeout** *value*]] [**routing**] [**routing-type** *routing-number*] [**sequence** *value*] [**time-range** *name*] 例： `Device(config-ipv6-acl)# permit icmp any any dest-option-type`	
ステップ 5	**deny** *protocol* {*source-ipv6-prefix*/*prefix-length* | **any** | **host** *source-ipv6-address* | **auth**} [*operator* [*port-number*]] {*destination-ipv6-prefix*/*prefix-length* | **any** | **host** *destination-ipv6-address* | **auth**} [*operator* [*port-number*]] [**dest-option-type** [*header-number* | *header-type*]] [**dscp** *value*] [**flow-label** *value*] [**fragments**] [**hbh**] [**log**] [**log-input**] [**mobility**] [**mobility-type** [*mh-number* | *mh-type*]] [**routing**] [**routing-type** *routing-number*] [**sequence** *value*] [**time-range** *name*] [**undetermined-transport**] 例： `Device(config-ipv6-acl)# deny icmp any any dest-option-type`	IPv6 ACL の拒否条件を設定します。
ステップ 6	**end** 例： `Device (config-ipv6-acl)# end`	特権EXECコンフィギュレーションモードに戻ります。

ホップバイ ホップ フィルタリングに対応するための IPv6 ACL の拡張の設定例

例：ホップ バイ ホップ フィルタリングに対応するための IPv6 ACL の拡張

```
Device(config)# ipv6 access-list hbh_acl
Device(config-ipv6-acl)# permit tcp any any hbh
Device(config-ipv6-acl)# permit tcp any any
Device(config-ipv6-acl)# permit udp any any
Device(config-ipv6-acl)# permit udp any any hbh
Device(config-ipv6-acl)# permit hbh any any
Device(config-ipv6-acl)# permit any any
```

```
Device(config-ipv6-acl)# hardware statistics
Device(config-ipv6-acl)# exit

! Assign an IP address and add the ACL on the interface.

Device(config)# interface FastEthernet3/1
Device(config-if)# ipv6 address 1001::1/64
Device(config-if)# ipv6 traffic-filter hbh_acl in
Device(config-if)# exit
Device(config)# exit
Device# clear counters
Clear "show interface" counters on all interfaces [confirm]
Device#

! Verify the configurations.

Device# show running-config interface FastEthernet3/1

Building configuration...

Current configuration : 114 bytes
!
interface FastEthernet3/1
no switchport
ipv6 address 1001::1/64
ipv6 traffic-filter hbh_acl
end
```

その他の参考資料

関連資料

関連項目	マニュアル タイトル
IPv6 アドレッシングと接続	『*IPv6 Configuration Guide*』
IPv6 コマンド	『*Cisco IOS IPv6 Command Reference*』
Cisco IOS IPv6 機能	『*Cisco IOS IPv6 Feature Mapping*』

標準および RFC

標準/RFC	タイトル
IPv6 に関する RFC	*IPv6 RFCs*

MIB

選択したプラットフォーム、Cisco IOS リリース、およびフィーチャ セットに関する MIB を探してダウンロードするには、次の URL にある Cisco MIB Locator を使用します。

http://www.cisco.com/go/mibs

シスコのテクニカル サポート

説明	リンク
右の URL にアクセスして、シスコのテクニカル サポートを最大限に活用してください。これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

ホップバイ ホップ フィルタリングに対応するための IPv6 ACL の拡張に関する機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *68* : ホップ バイ ホップ フィルタリングに対応するための *IPv6 ACL* の拡張に関する機能情報

機能名	リリース	機能情報
ホップ バイ ホップ フィルタリングに対応するための IPv6 ACL の拡張	Cisco IOS リリース XE 3.4S Cisco IOS リリース XE 3.5S Cisco IOS リリース XE 3.6S Cisco IOS リリース XE 3.3SG	これによって、ホップ バイ ホップ拡張ヘッダーを含む IPv6 トラフィックを制御できます。 次のコマンドが導入または変更されました。**deny**（IPv6）、**permit**（IPv6）。

第 47 章

セキュリティ（ACL）の拡張機能

セキュリティ（ACL）の拡張機能では、1つのボックスで設定できるACL、ACE、またはこれらの両方の数を制限するオプションが用意されています。ボックスでACLまたはACEの数を制限することにより、ボックスのパフォーマンスに悪影響を与える可能性のあるTCAMスペースの枯渇または過使用を防ぐことができます。

機能制限

- acl-ace-limit の設定は、ACL ごとであり、ボックスのすべての ACL に適用されます。
- acl-limit および acl-ace-limit は、global-ace-limit と同時に使用できません。acl-limit と acl-ace-limt が設定されている場合、global-ace-limit は設定できず、global-ace-limit が設定されている場合、acl-limit と acl-ace-limt は設定できません。

  設定する制限は、ボックスの既存の ACL/ACE の数未満にはできません。
- acl-limit、acl-ace-limit、または global-ace-limit 設定は、デバイスの起動中に内部で作成された ACL/ACE に適用されます。
- オブジェクト グループ ACE（ogace）拡張を備えた ACL は、このリリースではサポートされていません。お客様の要件に基づいて、これは詳しく調査できます。各 ogace は 1 つの ace としてカウントされます。
- acl-limit、acl-ace-limit、または global-ace-limit 設定は、すべての静的 ACL および動的に作成されたすべての ACL に適用されます（ただし、テンプレート ACL は除きます）。
- 設定可能な acl-limit、acl-ace-limit、または global-ace-limit によって、TCAM スペースの過使用や枯渇が発生しなくなるという訳ではありません。ラボでの事前テストから、ボックスでサポートできる正確な設定可能制限を認知しておく必要があります。

- ボックスで設定されているすべての ACL がインターフェイスに適用されるということが前提であり、これは TCAM スペースに影響します。
- ボックスが設定可能な acl-limit、acl-ace-limit、または global-ace-limit に到達し、かつクライアントが動的 ACL/ACE を作成しようとすると、その要求は拒否され、syslog エラーメッセージが出力されます。これに応じて障害を処理するのはユーザーの責任です。

セキュリティ（ACL）の拡張機能の設定

V4 および V6 に対して ACL および ACE 制限を設定するには：

```
enable
configure terminal
 access-list acl-limit 10
 access-list acl-ace-limit 12
 access-list global-ace-limit 14
 end
```

（注） acl-limit および acl-ace-limit は、global-ace-limit と同時に使用できません。

特記事項

- 設定可能な最大 ACL 制限の範囲は 1 ～ 2^{16} です。
- 設定可能な ACL あたりの最大 ACE 制限の範囲は 1 ～ 2^{32} です。
- 設定可能な最大グローバル ACE 制限の範囲は 1 ～ 2^{32} です。
- acl-ace-limit 設定は、すでに設定されているすべての ACL、およびこれから設定されるすべての ACL に適用されます。

セキュリティ（ACL）の拡張機能の設定の確認

show access-list acl-limit コマンドを使用すると、設定されている ACL と ACE の数を表示できます。

```
Device# show access-list acl-limit
Max ACLs configurable:       50
Number of ACLs configured:   10

Max aces/ACL configurable:   10

Max aces configurable:       100
Number of aces configured:   67
```

ホップバイ ホップ フィルタリングに対応するための IPv6 ACL の拡張に関する機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *69* : ホップ バイ ホップ フィルタリングに対応するための *IPv6 ACL* の拡張に関する機能情報

機能名	リリース	機能情報
ホップ バイ ホップ フィルタリングに対応するための IPv6 ACL の拡張	Cisco IOS リリース XE 3.4S Cisco IOS リリース XE 3.5S Cisco IOS リリース XE 3.6S Cisco IOS リリース XE 3.3SG	これによって、ホップ バイ ホップ拡張ヘッダーを含む IPv6 トラフィックを制御できます。 次のコマンドが導入または変更されました。**deny**（IPv6）、**permit**（IPv6）。

第 48 章

ACL の IPv6 オブジェクトグループ

ACL の IPv6 オブジェクトグループ機能を使用して、ユーザー、デバイス、またはプロトコルをグループに分類し、これらのグループをアクセスコントロールリスト（ACL）に適用してグループのアクセス コントロール ポリシーを作成できます。この機能により、従来の ACL で使用される個々の IP アドレス、プロトコル、ポートではなく、オブジェクト グループを使用できるようになります。この機能は、複数のアクセス コントロール エントリ（ACE）を許可しますが、各 ACE を使用して、ユーザーのグループ全体に対してサーバーまたはサービスのグループへのアクセスを許可または禁止できます。

大規模なネットワークでは、ACL の行数が大量（数百行）になり、特に ACL が頻繁に変更される場合は ACL の設定および管理が困難になります。オブジェクトグループベースの ACL は、従来の ACL よりも小さく、読みやすく、設定と管理が容易であるため、Cisco IOS ルータでの大規模なユーザーアクセス環境での静的および動的な ACL の導入が簡素化されます。

Cisco IOS ファイアウォールでは、オブジェクトグループはポリシーの作成を簡素化することから（たとえば、グループ A にグループ A サービスへのアクセスを許可するなど）オブジェクトグループによるメリットが得られます。

ACL の IPv6 オブジェクトグループに関する制約事項

- オブジェクトグループベースの ACL は、レイヤ 3 インターフェイス（ルーテッドインターフェイスや VLAN インターフェイスなど）のみをサポートします。オブジェクトグループベースの ACL は、VLAN ACL（VACL）やポート ACL（PACL）などのレイヤ 2 機能をサポートしません。
- オブジェクトグループベースの ACL は、IPsec ではサポートされていません。
- ACL でサポートされるオブジェクトグループベースの ACE の最大数は 2048 です。

- 空のオブジェクトグループは自動的に削除されます。
- オブジェクトグループは、アクセスリストで参照する前に作成する必要があります。オブジェクトグループは、アクセスリストなどの他の機能によって参照されている場合は削除できません。
- パケットフローに対して ACL 照合が実行される場合、ACL エントリを含むオブジェクトグループはスキップされます。

ACL の IPv6 オブジェクトグループに関する情報

従来型のアクセス制御エントリ（ACE）を設定し、複数の ACE が同じ ACL 内のオブジェクトグループを参照するように設定できます。

オブジェクトグループベースの ACL は、Quality of Service（QoS）一致基準、Cisco IOS ファイアウォール、Dynamic Host Configuration Protocol（DHCP）、およびその他の拡張 ACL を使用する機能で使用できます。さらに、マルチキャストトラフィックでオブジェクトグループベースの ACL を使用することもできます。

大規模な設定では、ACE でオブジェクトグループを使用する場合、アドレスとプロトコルのペアごとに個別の ACE を定義する必要がなくなるため、NVRAM に必要なストレージを削減できます。

オブジェクト グループ

オブジェクトグループには、単一のオブジェクト（単一の IP アドレス、ネットワーク、またはサブネットなど）または複数のオブジェクト（複数の IP アドレスの組み合わせ、ネットワーク、またはサブネットなど）を含めることができます。

一般的なアクセス コントロール エントリ（ACE）では、ユーザーのグループが特定のサーバーグループにのみアクセスできます。オブジェクトグループベースのアクセスコントロールリスト（ACL）では、多数の ACE を作成する（各 ACE に異なる IP アドレスが必要）代わりに、オブジェクトグループ名を使用する単一の ACE を作成できます。同様のオブジェクトグループ（プロトコルポートグループなど）を拡張して、ユーザーグループの一連のアプリケーションのみアクセス可能にできます。ACE には、送信元のみ、宛先のみ、なし、または両方のオブジェクトグループを含めることができます。

オブジェクトグループを使用して、ACE のコンポーネントの所有権を分離できます。たとえば、組織内の各部門がそのグループメンバーシップを制御し、管理者が ACE 自体を所有して、どの部門が相互に通信できるかを制御します。

IPv6 アドレスおよびサービス（プロトコル）はオブジェクトとして扱われ、その後、必要に応じてさまざまなオブジェクトグループにグループ化されます。オブジェクトグループには、v6-network オブジェクトグループ（アドレス用）と v6-service オブジェクトグループ（プロトコル用）の 2 種類があります。必要に応じて、オブジェクトグループをネストできます。

オブジェクトグループは、IPv6 ACE の設定時に、プロトコルや送信元アドレスまたは宛先アドレスの代わりに参照できます。オブジェクトグループを含む ACE は、個別の ACE（各オブジェクトの）に展開され、ハードウェアにプログラムされます。

IPv6 ネットワークおよびサービス オブジェクト グループには、オブジェクトが追加される独自のコンフィギュレーション サブモードがあります。

Cisco Policy Language（CPL）クラスマップを使用する機能でオブジェクトグループを使用できます。

この機能は、ACL パラメータをグループ化するために、ネットワーク オブジェクト グループとサービス オブジェクト グループの 2 種類のオブジェクトグループをサポートします。これらのオブジェクトグループを使用して、IP アドレス、プロトコル、プロトコルサービス（ポート）、および Internet Control Message Protocol（ICMP）タイプをグループ化します。

ネットワーク オブジェクト グループで許可されるオブジェクト

ネットワーク オブジェクト グループは、次のいずれかのオブジェクトのグループです。

- IPv6 アドレス
- ホスト IPv6 アドレス
- その他のネットワーク オブジェクト グループ
- サブネット

サービス オブジェクト グループで許可されるオブジェクト

サービス オブジェクト グループは、次のいずれかのオブジェクトのグループです。

- 送信元および宛先プロトコル ポート（Telnet や Simple Network Management Protocol（SNMP）など）
- Internet Control Message Protocol（ICMP）タイプ（エコー、エコー応答、到達不能など）
- トップレベル プロトコル（Encapsulating Security Payload（ESP）、TCP、UDP など）
- その他のサービス オブジェクト グループ

オブジェクト グループに基づく ACL

従来のアクセス コントロール リスト（ACL）を使用または参照する機能はすべて、オブジェクト グループ ベースの ACL と互換性があり、従来の ACL の機能インタラクションはオブジェクト グループ ベース ACL と同じです。この機能により、オブジェクト グループ ベースの ACL をサポートできるように従来の ACL が拡張され、新しいキーワードと、送信元アドレス、宛先アドレス、送信元ポート、および宛先ポートが追加されます。

オブジェクト グループ メンバーシップ リストでは、（オブジェクト グループを削除および再定義せずに）オブジェクトを動的に追加、削除、または変更できます。また、オブジェクト グループ メンバーシップ リストでは、オブジェクト グループを使用する ACL アクセス コント

ロールエントリ（ACE）を再定義せずに、オブジェクトを追加、削除、または変更できます。グループにオブジェクトを追加してから、グループからオブジェクトを削除することで、ACL をインターフェイスに再適用せずに、オブジェクト グループ ベースの ACL 内で変更が正しく機能することを確認できます。

ソース グループのみ、宛先グループのみ、またはソース グループと宛先グループの両方を使用して、オブジェクト グループ ベースの ACL を複数回設定できます。

ACL 内またはクラス ベース ポリシー言語（CPL）ポリシー内で使用されているオブジェクト グループは削除できません。

ACL のオブジェクト グループの設定方法

ACL のオブジェクト グループを設定するには、最初に 1 つ以上のオブジェクト グループを作成します。作成するオブジェクトグループは、ネットワーク オブジェクト グループ（ホストアドレスやネットワークアドレスなどのオブジェクトが含まれるグループ）またはサービスオブジェクト グループ（ポート番号に **lt**、**eq**、**gt**、**neq**、**range** などの演算子を使用するグループ）を任意に組み合わせることができます。オブジェクトグループを作成した後、それらのグループにポリシー（**permit** または **deny** など）を適用するアクセス コントロール エントリ（ACE）を作成します。

IPv6 オブジェクトグループの設定

オブジェクト グループ

次のオブジェクトグループが追加されています。

```
Device# enable
Device# configure terminal
Device(config)# object-group ?
network     network group
security    security group
service     service group
v6-network  IPv6 network group
v6-service  IPv6 service group
```

IPv6 ACL でのオブジェクトグループの使用

オブジェクトグループは、プロトコル、送信元 IPv6 アドレス、および宛先 IPv6 アドレスの 3 つの位置にあるアクセスリストで使用できます。

次のオブジェクト グループ オプションが既存のプロトコル/アドレスオプションに追加されています。

```
Device(config-v6network-group)#?

Device(config-ipv6-acl)# [no] { permit | deny } [ <protocol options> | object-group
<v6service og name> ] { <source address options> | object-group <v6network OG
name> } { <destination address options> | object-group <v6network OG name> }
```

IPv6 ネットワーク オブジェクト グループの作成

単一のオブジェクト（単一の IP アドレス、ホスト名、別のネットワーク オブジェクト グループ、またはサブネットなど）または複数のオブジェクトを含むネットワーク オブジェクト グループには、オブジェクトのアクセス制御ポリシーを作成するための、ネットワーク オブジェクト グループ ベース ACL が関連付けられています。

IPv6 ネットワーク オブジェクト グループを作成するには、次の手順を実行します。

```
Device> enable
Device# configure terminal
Device(config)# object-group v6-network name
Device(config-v6network-group)# [no] { description <desc> | <x.x.x.x::x/prefix_len> |
host <x.x.x.x::x> | group-object <nested OG name> }


Device(config)#object-group v6-net ognet1
Device(config-v6network-group)#?


V6-Network object group configuration commands:
X:X:X:X::X/<0-128>  - IPv6 network address/prefix length
description         - Network object group description
exit                - Exit from object group configuration mode
group-object        - Nested object group
host                - Host address of group member
no                  - Negate or set default values of a command
```

IPv6 サービス オブジェクト グループの作成

TCP または UDP ポートまたはポート範囲を指定するにはサービス オブジェクト グループを使用します。サービス オブジェクト グループがアクセス コントロール リスト（ACL）に関連付けられると、このサービス オブジェクト グループ ベースの ACL はポートへのアクセスを制御できます。

IPv6 サービス オブジェクト グループを作成するには、次の手順を実行します。

```
Device> enable
Device# configure terminal
Device(config)# object-group v6-service <name>
Device(config-v6service-group)# [no] {description <desc> | <0-255> | ahp | esp | hbh
|icmp [<message type>]
| ipv6 | pcp | { <sctp | tcp | udp | tcp-udp> [source <src port options>]}
[<dest port options>] | group-object <nested OG name> }
Device(config-service-group)# end
```

```
Device# (config-v6service-group)#?
IPv6 Service object group configuration commands:
<0-255>         -  An IP protocol number
ahp             - Authentication Header Protocol
description     - Service object group description
esp             - Encapsulation Security Payload
exit            - Exit from object-group configuration mode
group-object    - Nested object group
hbh             - Hop by Hop options header
icmp            - Internet Control Message Protocol
ipv6            - Any Internet Protocol (v6)
no              - Negate or set default values of a command
pcp             - Payload Compression Protocol
sctp            - Streams Control Transmission Protocol
```

```
tcp             - Transmission Control Protocol
tcp-udp         - TCP or UDP protocol
udp             - User Datagram Protocol
```

ACL の IPv6 オブジェクトグループの確認

ACL の IPv6 オブジェクトグループを確認するには、次の手順を実行します。

```
Device# enable
Device# show running int <name>-------to check if ACL is applied on the interface
Device# show object-group object-group-name --------to check if configured object groups
 are referenced
Device# show ipv6 access-list --------to check the configured ACL
```

上記の show コマンドは、名前付きまたは番号付きアクセスリストまたはオブジェクトグループベース ACL（名前が入力されていない場合はすべてのアクセスリストおよびオブジェクトグループベース ACL）の内容を表示します。

ACL 用オブジェクト グループの設定例

例：IPv6 ネットワーク オブジェクト グループの作成

次に、v6-network ognet1 という名前の IPv6 ネットワーク オブジェクト グループを作成する例を示します。

```
Device> enable
Device# configure terminal
Device(config)# object-group v6-network ognet1
Device(config-v6-network-group)# 1:1:2::0/32
Device(config-v6-network-group)# host AB:233::23D5
Device(config-v6-network-group)# exit
```

次に、1 つのホスト、1 つのサブネット、および既存のオブジェクトグループ（子）をオブジェクトとして含む、v6-network ognet2 という名前のネットワーク オブジェクト グループを作成する例を示します。

```
Device> enable
Device# configure terminal
Device(config)# object-group network v6-network ognet2
Device(config-v6network-group)# 1:2:3::4/36
Device(config-v6network-group)# host AABB::CCDD
Device(config-v6network-group)# group-object ognet1
Device(config-v6network-group)# exit
```

例：IPv6 サービス オブジェクト グループの作成

次に、複数の ICMP、TCP、UDP、および TCP-UDP プロトコルをオブジェクトとして含む、v6-service ogserv1 という名前のサービス オブジェクト グループを作成する例を示します。

```
Device> enable
Device# configure terminal
Device(config)# object-group service v6-service ogserv1
Device(config-v6service-group)# icmp unreachable
Device(config-v6service-group)# tcp smtp
Device(config-v6service-group)# tcp telnet
Device(config-v6service-group)# tcp source range 3000 4000 telnet
Device(config-v6service-group)# pcp
Device(config-v6service-group)# udp domain
Device(config-v6service-group)# hph
Device(config-v6service-group)# exit
```

例：IPv6 オブジェクトグループベースの ACL の作成

次に、パケットを許可する IPv6 オブジェクトグループベース ACL を作成する例を示します。

```
Device> enable
Device# configure terminal
Device(config)# ipv6 access-list ogacl1
Device(config-ipv6-acl)# permit object-group ogserv1 5:6:7::5/56 object-group ognet1
Device(config-ipv6-acl)# deny ip object-group ognet2 object-group ognet3
Device(config-ipv6-acl)# permit ipv6 any any
Device(config-ipv6-acl)# exit
```

例：ACL 用 IPv6 オブジェクトグループの確認

次に、すべてのオブジェクト グループを表示する例を示します。

```
Device# show object-group

V6-Network object group ognet1
1:1:2::/32
host AB:233::23D5
V6-Network object group ognet2
1:2:3::4/36
host AABB::CCDD
group-object ognet1
V6-Network object group ognet3
host 1::1
host 1::2
host 1::3
V6-Service object group ogserv1
icmp unreachable
tcp source range 3000 4000 eq telnet
pcp
hbh
```

次に、IPv6 オブジェクトグループベース ACL に関する情報を表示する例を示します。

```
Device# show ipv6 access-list
IPv6 access list ogacl1
      permit object-group ogserv1 5:6:7::/56 object-group ognet1 sequence 10
      deny ipv6 object-group ognet2 object-group ognet3 sequence 20
```

```
permit ipv6 any any sequence 30
```

ACL 用オブジェクト グループに関する追加情報

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『Cisco IOS Master Command List, All Releases』
セキュリティ コマンド	• 『Cisco IOS Security Command Reference: Commands A to C』[英語] • 『Cisco IOS Security Command Reference: Commands D to L』[英語] • 『Cisco IOS Security Command Reference: Commands M to R』[英語] • 『Cisco IOS Security Command Reference: Commands S to Z』[英語]
ACL 設定ガイド	『セキュリティコンフィギュレーションガイド』の「アクセスコントロールリスト」

シスコのテクニカル サポート

説明	リンク
右の URL にアクセスして、シスコのテクニカル サポートを最大限に活用してください。これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

ACL 用 IPv6 オブジェクトグループに関する機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだ

けを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *70 : ACL* 用オブジェクト グループに関する機能情報

機能名	リリース	機能情報
ACL の IPv6 オブジェクトグループ	Cisco IOS XE リリース 16.11.1	ACL 用 IPv6 オブジェクトグループ機能を使用すれば、ユーザー、デバイス、またはプロトコルをグループに分類して、それらをアクセス制御リスト（ACL）に適用し、そのグループ用のアクセス制御ポリシーを作成することができます。この機能により、従来の ACL で使用される個々の IP アドレス、プロトコル、ポートではなく、オブジェクトグループを使用できるようになります。この機能は、複数のアクセス コントロール エントリ（ACE）を許可しますが、各 ACE を使用して、ユーザーのグループ全体に対してサーバーまたはサービスのグループへのアクセスを許可または禁止できます。

第 IV 部

RADIUS

第 49 章

RADIUS の設定

RADIUS セキュリティ システムは、不正なアクセスからネットワークのセキュリティを保護する分散クライアント/サーバ システムです。シスコの実装では、RADIUS クライアントはシスコ デバイス上で実行され、すべてのユーザ認証およびネットワーク サービス アクセス情報を持つ中央の RADIUS サーバに認証要求を送信します。

RADIUS の前提条件

シスコ デバイスまたはアクセス サーバーで RADIUS を設定するには、次のタスクを実行する必要があります。

- **aaa new-model** グローバル コンフィギュレーション コマンドを使用して、認証、認可、およびアカウンティング（AAA）をイネーブルにします。RADIUS を使用する予定がある場合、AAA を設定する必要があります。
- **aaa authentication** グローバル コンフィギュレーション コマンドを使用して、RADIUS 認証の方式リストを定義します。
- **line** および **interface** コマンドを使用して、使用する定義済みの方式リストをイネーブルにします。

RadSec の制限（RADIUS セキュリティ）

RadSec は、シスコ エンタープライズ ルーティング プラットフォームではサポートされていません。

RADIUS の概要

RADIUS ネットワーク環境

シスコは、認証、認可、およびアカウンティング（AAA）セキュリティ パラダイムに基づいて RADIUS をサポートします。RADIUS は、TACACS+、Kerberos、ローカル ユーザー名の検索など、他の AAA セキュリティ プロトコルと併用できます。RADIUS はすべての Cisco プラットフォームでサポートされますが、RADIUS でサポートされる一部の機能は、指定されたプラットフォームだけで実行されます。

RADIUS は、リモート ユーザーのネットワーク アクセスを維持すると同時に高度なレベルのセキュリティを必要とするさまざまなネットワーク環境に実装されています。

RADIUS は、アクセスのセキュリティが必要な次のネットワーク環境で使用できます。

- それぞれが RADIUS をサポートする、マルチベンダー アクセス サーバによるネットワーク。たとえば、複数のベンダーのアクセス サーバが、1 つの RADIUS サーバベース セキュリティ データベースを使用します。複数ベンダーのアクセス サーバからなる IP ベースのネットワークでは、ダイヤルイン ユーザは RADIUS サーバを通じて認証されます。RADIUS サーバは、Kerberos セキュリティ システムで動作するようにカスタマイズされています。
- アプリケーションが RADIUS プロトコルをサポートするターンキー ネットワーク セキュリティ環境。たとえば、スマート カード アクセス コントロール システムを使用するアクセス環境。その例として、ユーザーの検証とネットワーク リソースへのアクセス許可に、RADIUS が Enigma のセキュリティ カードとともに使用されています。
- すでに RADIUS を使用中のネットワーク。RADIUS 機能を持つ Cisco デバイスをネットワークに追加できます。これが TACACS+ サーバーへの移行の最初のステップとなることもあります。
- ユーザーが単一のサービスにだけアクセスする必要があるネットワーク。RADIUS を使用すると、単一ホスト、単一ユーティリティ（Telnet など）、または単一プロトコル（PPP など）に対するユーザー アクセスを制御できます。たとえば、ユーザーがログインすると、RADIUS は、IP アドレス 10.2.3.4 を使用してそのユーザーが PPP を実行する権限を持っていることを識別し、定義済みのアクセス リストが開始されます。
- リソース アカウンティングが必要なネットワーク。RADIUS アカウンティングは、RADIUS 認証または RADIUS 認可とは個別に使用できます。RADIUS アカウンティング機能を使用すると、サービスの開始および終了時に、セッション中に使用したリソース（時間、パケット、バイトなど）の量を示すデータを送信できます。ISP は、RADIUS アクセス コン

トロールおよびアカウンティング ソフトウェアのフリーウェア バージョンを使用して、特殊なセキュリティおよび課金に対するニーズを満たすこともできます。

- 事前認証をサポートしているネットワーク。ネットワークにRADIUSサーバーを導入すると、AAA 事前認証を設定し、事前認証のプロファイルを設定できます。サービス プロバイダーが事前認証を使用すると、既存のRADIUSソリューションを使用するポートの管理性が向上し、共有リソースを効率的に管理して、各種のサービスレベル契約を提供できるようになります。

RADIUS は、次のようなネットワーク セキュリティ状況には適していません。

- マルチプロトコル アクセス環境。RADIUS は次のプロトコルをサポートしていません。
  - AppleTalk Remote Access（ARA）
  - NetBIOS Frame Control Protocol（NBFCP）
  - NetWare Asynchronous Services Interface（NASI）
  - X.25 Packet Assemblers/Disassemblers（PAD）接続
- デバイスからデバイスへの状況。RADIUSは、双方向認証を行いません。RADIUSは、他社製のデバイスがRADIUS認証を必要とする場合に、あるデバイスから他社製のデバイスへの認証に使用できます。
- 各種のサービスを使用するネットワーク。RADIUS は、一般に 1 人のユーザを 1 つのサービス モデルにバインドします。

RADIUS の動作

ユーザーがログインを試行し、RADIUSを使用してアクセスサーバーから認証を受ける場合、次の手順が発生します。

1. ユーザー名とパスワードの入力を求めるプロンプトが表示されます。
2. ユーザ名および暗号化されたパスワードが、ネットワーク経由でRADIUSサーバに送信されます。
3. ユーザは、RADIUS サーバから次のいずれかの応答を受信します。
   1. ACCEPT：ユーザーが認証されたことを表します。
   2. CHALLENGE：RADIUSサーバーによってチャレンジが発行されます。チャレンジは、ユーザーから追加データを収集します。
   3. CHANGE PASSWORD：RADIUS サーバーからユーザーに対して新しいパスワードの選択を求める要求が発行されます。
   4. REJECT：ユーザーは認証されず、ユーザー名とパスワードの再入力を求められるか、アクセスを拒否されます。

ACCEPT応答またはREJECT応答には、EXEC許可またはネットワーク許可に使用される追加データが含まれています。RADIUS認可を使用するには、まずRADIUS認証を完了する必要があります。ACCEPTまたはREJECTパケットに含まれる追加データの内容は次のとおりです。

- ユーザーがアクセスできるサービス。Telnet、rlogin、またはローカルエリア トランスポート（LAT）などの接続や、PPP、Serial Line Internet Protocol（SLIP）、または EXEC サービスなどのサービスを含む。
- ホストまたはクライアントの IP アドレス、アクセス リスト、ユーザータイムアウトなどの接続パラメータ。

RADIUS 属性

ネットワーク アクセス サーバーは、各ユーザー プロファイルで RADIUS 属性で定義されている RADIUS 認可機能およびアカウンティング機能をモニターします。

ベンダー独自の RADIUS 属性

RADIUS の Internet Engineering Task Force（IETF）標準規格には、ネットワーク アクセス サーバーと RADIUS サーバーの間でベンダー独自の情報を伝達する際の方式が規定されています。さらに、一部のベンダーが固有の方法で RADIUS 属性を拡張しています。Cisco ソフトウェアは、ベンダー独自仕様の RADIUS 属性のサブセットをサポートしています。

RADIUS トンネル属性

RADIUS は、元は Livingston, Inc. が開発したセキュリティ サーバーの AAA プロトコルです。RADIUS は属性値（AV）ペアを使用して、セキュリティ サーバーとネットワーク アクセス サーバーの間で通信します。

RFC 2138 と RFC 2139 では、RADIUS の基本機能と、AAA 情報の送信に使用される IETF 標準規格の AV ペアの初期セットについて説明しています。「RADIUS Attributes for Tunnel Protocol Support」および「RADIUS Accounting Modifications for Tunnel Protocol Support」という 2 つの IETF 標準規格は、VPN 固有の属性を含むように IETF が定義した AV ペア セットを拡張します。これらの属性は、RADIUS サーバーとトンネル イニシエータの間でトンネリング情報を伝送するために使用されます。

RFC 2865 と RFC 2868 は IETF が定義した AV ペア セットを拡張して、VPN の強制トンネリングに固有の属性を追加しています。この属性を使用して、ユーザーはネットワーク アクセス サーバーおよび RADIUS サーバーの認証名を指定できます。

シスコ デバイスとアクセス サーバーでは、新しい RADIUS IETF 標準規格の仮想プライベート ダイヤルアップ ネットワーク（VPDN）トンネル属性がサポートされています。

RADIUS サーバー上の事前認証

RADIUS 属性は、事前認証の動作を指定するために RADIUS 事前認証プロファイルで設定されています。シスコ デバイスで事前認証を設定するだけでなく、RADIUS サーバーでも事前認証プロファイルを設定する必要があります。

DNIS または CLID 事前認証のための RADIUS プロファイル

RADIUS 事前認証プロファイルを設定するには、着信番号識別サービス（DNIS）または発信側回線 ID（CLID）の番号をユーザー名として使用し、**dnis** または **clid** コマンドで定義されたパスワードをパスワードとして使用します。

（注） 事前認証プロファイルのサービス タイプは常に「outbound」になります。これは、パスワードがネットワーク アクセス サーバー（NAS）で事前定義されているためです。この方法で事前認証プロファイルを設定することで、DNIS 番号、CLID 番号、またはコール タイプのユーザー名と、わかりやすいパスワードを使用してユーザーが NAS にログインする操作を回避できます。「outbound」サービス タイプは、RADIUS サーバーに送信される Access-Request パケットにも含まれます。

コール タイプの事前認証のための RADIUS プロファイル

RADIUS 事前認証プロファイルを設定するには、コール タイプ文字列をユーザー名として使用し、**ctype** コマンドで定義したパスワードをパスワードとして使用します。以下の表に、事前認証プロファイルで使用できるコール タイプ文字列の一覧を示します。

表 *71 :* 事前認証で使用されるコール タイプ文字列

コール タイプ ストリング	ISDN ベアラ機能
digital	無制限のデジタル、制限付きのデジタル。
speech	音声、3.1 kHz オーディオ、7 kHz オーディオ。 （注） これは個別線信号方式（CAS）で使用できる唯一のコール タイプです。
v.110	V.110 ユーザー情報レイヤがある任意のコール。
v.120	V.120 ユーザー情報レイヤがある任意のコール。

（注） 事前認証プロファイルのサービス タイプは必ず「outbound」になります。これは、パスワードが NAS で事前定義されているためです。この方法で事前認証プロファイルを設定することで、DNIS 番号、CLID 番号、またはコール タイプのユーザー名と、わかりやすいパスワードを使用してユーザーが NAS にログインする操作を回避できます。「outbound」サービス タイプは、RADIUS サーバーに送信された Access-Request パケットにも含まれます。また、RADIUS サーバーがチェックイン アイテムをサポートする場合、チェックイン アイテムにする必要があります。

コールバック用の事前認証の機能拡張のための RADIUS プロファイル

在宅勤務者などのリモート ネットワーク ユーザーは、コールバックを使用すると課金を受けずにNASにダイヤルインできます。コールバックが必要な場合、NASは現在の通話を終了し、呼び出し元にダイヤルします。NASがコールバックを実行する場合は、発信接続の情報だけが適用されます。事前認証 access-accept メッセージからの残りの属性は廃棄されます。

（注） RADIUS サーバーからのコールバックに宛先の IP アドレスは必要ありません。

次に、コールバック番号が 555-0101 でサービス タイプが outbound に設定された RADIUS プロファイル設定の例を示します。cisco-avpair = “preauth:send-name=<string>” では文字列 “user1” を使用し、cisco-avpair = “preauth:send-secret=<string>” ではパスワード “cisco” を使用します。

```
5550101 password = “cisco”, Service-Type = Outbound
Service-Type = Callback-Framed
Framed-Protocol = PPP,
Dialback-No = “5550119”
Class = “ISP12”
cisco-avpair = “preauth:send-name=user1”
cisco-avpair = “preauth:send-secret=cisco”
```

大規模なダイヤルアウトに使用するリモート ホスト名の RADIUS プロファイル

次の例では、正しい電話番号をコールして誤ったデバイスにアクセスするアクシデントを防ぐために、大規模なダイヤルアウトで使用するリモート デバイスの名前を指定しています。

```
5550101 password = "PASSWORD1", Service-Type = Outbound
       Service-Type = Callback-Framed
       Framed-Protocol = PPP,
       Dialback-No = "5550190"
       Class = "ISP12"
       cisco-avpair = "preauth:send-name=user1"
       cisco-avpair = "preauth:send-secret=PASSWORD1"
       cisco-avpair = "preauth:remote-name=Device2"
```

モデム管理用の RADIUS プロファイル

DNIS、CLID、またはコール タイプの事前認証を使用する場合、NAS の RADIUS サーバーからの肯定応答には、ベンダー固有属性（VSA）26 を介して、モデム管理用のモデム文字列を含めることができます。モデム管理 VSA の構文は次のとおりです。

```
cisco-avpair = “preauth:modem-service=modem min-speed <
x
> max-speed <
y
>
modulation <
z
> error-correction <
a
> compression <
```

```
b
>"
```

以下の表に、VSA 内のモデム管理文字列要素の一覧を示します。

表 *72*：モデム管理文字列

コマンド	引数
min-speed	300 ～ 56000、any
max-speed	300 ～ 56000、any
modulation	K56Flex、v22bis、v32bis、v34、v90、any
error-correction	lapm、mnp4
compression	mnp5、v42bis

VSA の形式で RADIUS サーバーからモデム管理文字列を受信すると、その情報は Cisco ソフトウェアに渡され、コールごとに適用されます。Modem ISDN Channel Aggregation（MICA）モデムには、コール設定時にメッセージを送信できるコントロール チャネルがあります。そのため、このモデム管理機能をサポートするのは、MICA モデムだけです。この機能は Microcom モデムではサポートされません。

後続の認証のための RADIUS プロファイル

事前認証に成功すると、事前認証プロファイルのベンダー独自の RADIUS 属性 201（Require-Auth）を使用して、後続の認証を実行するかどうかを決定できます。access-accept メッセージで返される属性 201 の値が 0 の場合、後続の認証は実行されません。属性 201 の値が 1 の場合、後続の認証は通常どおり実行されます。

属性 201 の構文は次のとおりです。

```
cisco-avpair = "preauth:auth-required=<
n
>"
```

ここで、<*n*> は、属性 201と同じ値の範囲です（つまり、0 または 1）。

事前認証プロファイルに属性 201 が含まれない場合、値 1 と仮定され、後続の認証が実行されます。

（注） 後続の認証を実行する前に、事前認証プロファイルに加えて、通常のユーザープロファイルを設定する必要があります。

後続の認証タイプのための RADIUS プロファイル

事前認証プロファイルに後続の認証を指定した場合、後続の認証に使用する認証タイプも指定する必要があります。後続の認証で使用できる認証タイプを指定するには、次の VSA を使用します。

```
cisco-avpair = "preauth:auth-type=<
string
>"
```

以下の表に、<*string*> 要素で使用できる値の一覧を示します。

表 *73 : <string>* 要素の値

文字列	説明
chap	PPP 認証の Challenge Handshake Authentication Protocol（CHAP）のユーザー名とパスワードが必要です。
ms-chap	PPP 認証の MS-CHAP のユーザー名とパスワードが必要です。
pap	PPP 認証の Password Authentication Protocol（PAP）のユーザー名とパスワードが必要です。

複数の認証タイプを許可するように指定するには、事前認証プロファイルでこの VSA の複数インスタンスを設定できます。事前認証プロファイルに指定する認証タイプ VSA の順序は、PPP ネゴシエーションに使用する認証タイプの順序にもなるため、重要です。

この VSA はユーザー別の属性であり、**ppp authentication** インターフェイス コンフィギュレーション コマンドで指定された認証タイプ リストを置き換えます。

（注） これは後続の認証用の認証タイプを指定する VSA なので、後続の認証が必要な場合にだけ使用してください。

ユーザー名を含めるための RADIUS プロファイル

コールの認証に事前認証のみを使用する場合、発信するときに NAS がユーザー名を見つけられない可能性があります。RADIUS は、NAS が RADIUS 属性 1（User-Name）または Access-Accept パケットで返される VSA を介して使用するユーザー名を提供できます。ユーザー名を指定する VSA の構文は次のとおりです。

```
cisco-avpair = "preauth:username=<
string
>"
```

ユーザー名を指定しない場合、DNIS 番号、CLID 番号、またはコール タイプが使用されます。これは、設定した最後の事前認証コマンドによって変わります（たとえば、**clid** が最後に設定された事前認証コマンドの場合、CLID 番号がユーザー名として使用されます）。

後続の認証を使用してコールを認証する場合、2つのユーザー名が存在する可能性があります。RADIUSから提供されたユーザー名と、ユーザーが指定したユーザー名です。この場合、ユーザーが指定したユーザー名は、RADIUS事前認証プロファイルに含まれているユーザー名を上書きします。ユーザーが指定したユーザー名は、認証およびアカウンティングの両方に使用されます。

双方向認証のための RADIUS プロファイル

双方向認証の場合、発信側のネットワーク デバイスはNASを認証する必要があります。PAPのユーザー名とパスワードやCHAPのユーザー名とパスワードをNAS上でローカルに設定する必要はありません。代わりに、事前認証のAccess-Acceptメッセージにユーザー名とパスワードを含めることができます。

（注） **radius** コマンドを使用する場合、**ppp authentication** コマンドは設定しないでください。

PAPをセットアップする場合、インターフェイスで **ppp pap sent-name password** コマンドは設定しないでください。VSA「preauth:send-name」および「preauth:send-secret」は、アウトバウンド認証のPAPユーザー名とPAPパスワードとして使用されます。

CHAPの場合、「preauth:send-name」はアウトバウンド認証だけでなく、インバウンド認証にも使用されます。CHAPインバウンドの場合、NASは、発信側のネットワーク デバイスに対するチャレンジ パケットで「preauth:send-name」に定義されている名前を使用します。CHAPアウトバウンドの場合、「preauth:send-name」と「preauth:send-secret」の両方が応答パケットで使用されます。

次に、双方向認証を指定する設定の例を示します。

```
5550101 password = "PASSWORD2", Service-Type = Outbound
Service-Type = Framed-User
cisco-avpair = "preauth:auth-required=1"
cisco-avpair = "preauth:auth-type=pap"
cisco-avpair = "preauth:send-name=user1"
cisco-avpair = "preauth:send-secret=PASSWORD2"
class = "<some class>"
```

（注） リソース プーリングをイネーブルにする場合、双方向認証は機能しません。

認可をサポートするための RADIUS プロファイル

事前認証のみが設定されている場合、後続の認証はバイパスされます。ユーザー名とパスワードを使用できないため、認可もバイパスされます。ただし、事前認証プロファイルにauthorization属性を含めてユーザー別の属性を適用することで、認可のために後でRADIUSに処理を戻す必要がなくなります。認可プロセスを開始するには、NASで **aaa authorization network** コマンドも設定する必要があります。

事前認証プロファイルに authorization 属性を設定できますが、service-type 属性（属性 6）という 1 つの例外があります。service-type 属性は、事前認証プロファイルで VSA に変換する必要があります。この VSA の構文は次のとおりです。

```
cisco-avpair = "preauth:service-type=<
n
>"
```

ここで、<*n*> は、属性 6 に関する標準の RFC 2865 値の 1 つです。

（注） 後続の認証が必要な場合、事前認証プロファイルの authorization 属性は適用されません。

RADIUS 認証

RADIUS サーバーを指定し、RADIUS 認証キーを定義した後は、RADIUS 認証の方式リストを定義する必要があります。AAA によって RADIUS 認証が容易になるため、**aaa authentication** コマンドを入力し、認証方式として RADIUS を指定する必要があります。

RADIUS 許可

AAA 認可を使用すると、ユーザーのアクセスをそのネットワークに制限するパラメータを設定できます。RADIUS を使用する認可は、1 回限りの認可や各サービスに対する認可、各ユーザーに対するアカウントリストおよびプロファイル、ユーザー グループのサポート、IP、IPX、AppleTalk Remote Access（ARA）、および Telnet のサポートなど、リモート アクセスをコントロールするための方法を提供します。AAA によって RADIUS 認可は容易になるため、認可方式として RADIUS を指定して、**aaa authorization** コマンドを入力する必要があります。

RADIUS アカウンティング

AAAアカウンティング機能を使用すると、ユーザーがアクセスしているサービスや、ユーザーが消費しているネットワーク リソース量を追跡できます。AAA によって RADIUS アカウンティングは容易になるため、アカウンティング方式としてRADIUSを指定して、**aaa accounting** コマンドを入力する必要があります。

RADIUS Login-IP-Host

ネットワーク アクセス サーバー（NAS）が、ダイヤルイン ユーザーに対する接続を試行するときに複数のログイン ホストを試行できるようにするため、RADIUS サーバーのユーザー プロファイルに 3 つの Login-IP-Host エントリを入力できます。次に、ユーザー *user1* 用に 3 つの Login-IP-Host インスタンスを設定し、接続に TCP-Clear を使用する例を示します。

```
user1 Password = xyz
        Service-Type = Login,
        Login-Service = TCP-Clear,
```

```
Login-IP-Host = 10.0.0.0,
Login-IP-Host = 10.2.2.2,
Login-IP-Host = 10.255.255.255,
Login-TCP-Port = 23
```

ホストの入力順は、試行される順序になります。**ip tcp synwait-time** コマンドを使用して、NAS がリストの次のホストに対して接続を試行するまでに待機する秒数を設定します。デフォルトは 30 秒です。

使用している RADIUS サーバーが 4 つ以上の Login-IP-Host エントリを許可していても、NAS が Access-Accept パケットでサポートするのは 3 つのホストだけです。

RADIUS Prompt

Access-Challenge パケットに対するユーザーの応答を画面にエコーするかどうかを制御するには、RADIUS サーバーのユーザー プロファイルで Prompt 属性を設定します。この属性は、Access-Challenge パケットにだけ含まれます。次に、No-Echo に設定された Prompt 属性の例を示します。この設定で、ユーザーの応答はエコーされません。

```
user1 Password = xyz
Service-Type = Login,
Login-Service = Telnet,
Prompt = No-Echo,
Login-IP-Host = 172.31.255.255
```

ユーザーの応答をエコーするには、この属性を Echo に設定します。Prompt 属性をユーザー プロファイルに含めない場合、デフォルトで応答はエコーされま。

この属性は、アクセス サーバーに設定されている **radius-server challenge-noecho** コマンドの動作よりも優先されます。たとえば、アクセス サーバーがエコーを表示しないように設定され、個人のユーザー プロファイルではエコーを許可している場合、ユーザー応答はエコーされます。

（注） Prompt 属性を使用する場合、Access-Challenge パケットをサポートするように RADIUS サーバーを設定する必要があります。

ベンダー固有の RADIUS 属性

IETF 標準規格では、ネットワーク アクセス サーバーと RADIUS サーバーの間で、ベンダー固有属性（属性 26）を使用してベンダー固有の情報を伝達する方法を指定しています。各ベンダーは、Vendor-Specific Attribute（VSA）を使用することによって、一般的な用途には適さない独自の拡張属性をサポートできます。シスコの RADIUS 実装は、この仕様で推奨される形式を使用して、1 つのベンダー固有オプションをサポートしています。シスコのベンダー ID は 9 で、サポートされるオプションはベンダータイプ 1、名前は「cisco-avpair」です。この値は、次のフォーマットのストリングです。

```
protocol : attribute sep value *
```

「protocol」は、特定の認可タイプに対するシスコの「protocol」属性の値です。使用可能なプロトコルには、IP、Internetwork Packet Exchange（IPX）、VPDN、VoIP、セキュア シェル（SSH）、Resource Reservation Protocol（RSVP）、シリアル インターフェイス プロセッサ（SIP）、AirNet、およびアウトバウンドなどがあります。「attribute」と「value」は、Cisco TACACS+ 仕様で定義されている適切な AV ペアで、「sep」は、必須属性では「=」、省略可能な属性では「*」です。この設定により、TACACS+ 認可で使用できる機能一式を RADIUS でも使用できるようになります。

たとえば、次の AV ペアにより、シスコの「複数の名前付き IP アドレス プール」機能が、IP 認可中（PPP のインターネット プロトコル制御プロトコル（IPCP）アドレスの割り当て中）に有効化されます。

```
cisco-avpair= ”ip:addr-pool=first“
```

「*」を挿入すると、AV ペア「ip:addr-pool=first」は省略可能になります。任意の AV ペアを省略可能にすることができます。

```
cisco-avpair= ”ip:addr-pool*first“
```

次に、ネットワーク アクセス サーバからユーザがログインしたときに、すぐに EXEC コマンドを実行する方法の例を示します。

```
cisco-avpair= ”shell:priv-lvl=15“
```

他のベンダーには、そのベンダー固有の ID、オプション、関連 VSA があります。

RADIUS サーバーのスタティック ルートと IP アドレス

RADIUS のベンダー固有実装の一部では、ネットワーク内にある個々のネットワーク アクセス サーバーの代わりに、ユーザーが RADIUS サーバーのスタティック ルートおよび IP プールを定義できます。各ネットワーク アクセス サーバーは、スタティック ルートと IP プール情報について RADIUS サーバーに照会します。

シスコ デバイスが起動したときに、そのデバイスまたはアクセス サーバーがスタティック ルートと IP プール定義を RADIUS サーバーに照会するには、**radius-server configure-nas** コマンドを使用します。

radius-server configure-nas コマンドは、シスコ デバイスの起動時に実行されるため、**copy system:running-config nvram:startup-config** コマンドを入力するまで有効になりません。

RADIUS の設定方法

ベンダー独自の RADIUS サーバーとの通信に関するデバイス設定

IETF の RADIUS 標準規格では、ネットワーク アクセス サーバーと RADIUS サーバーの間でベンダー独自の情報を受け渡す方法を指定していますが、一部のベンダーはRADIUS 属性セッ

トを独自の方法で拡張しています。Cisco ソフトウェアは、ベンダー独自仕様の RADIUS 属性のサブセットをサポートしています。

RADIUS を設定するには（ベンダー独自または IETF 準拠のいずれの場合も）、**radius-server** コマンドを使用して、RADIUS サーバーデーモンを実行しているホストと、そのホストがシスコ デバイスと共有する秘密テキスト文字列を指定する必要があります。RADIUS サーバーが RADIUS のベンダー独自実装を使用していることを示すには、**radius-server host non-standard** コマンドを使用します。**radius-server host non-standard** コマンドを使用しないと、ベンダー独自の属性はサポートされません。

手順の概要

1. **enable**
2. **configure terminal**
3. **radius-server vsa send** [**accounting** | **authentication**]
4. **radius server** *server-name*
5. **address ipv4** *ip-address*
6. **non-standard**
7. **key** {**0** *string* | **7** *string* | *string*}
8. **exit**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**radius-server vsa send** [**accounting**	**authentication**] 例： `Device(config)# radius-server vsa send`	RADIUS IETF 属性 26 の定義に従って、ネットワーク アクセス サーバーが VSA を認識および使用できるようにします。
ステップ 4	**radius server** *server-name* 例：	RADIUS サーバーの名前を指定します。

	コマンドまたはアクション	目的
	`Device(config)# radius server rad1`	（注） **radius-server host** コマンドは、Cisco IOS リリース 15.4(2)S 以降では廃止されています。IPv4 または IPv6 RADIUS サーバーを設定するには、**radius server** *name* コマンドを使用します。 **radius server** コマンドの詳細については、『*Cisco IOS Security Command Reference: Commands M to R*』を参照してください。
ステップ 5	**address ipv4** *ip-address* 例： `Device(config-radius-server)# address ipv4 10.45.1.2`	RADIUS サーバーに IP アドレスを割り当てます。
ステップ 6	**non-standard** 例： `Device(config-radius-server)# non-standard`	セキュリティ サーバーが RADIUS のベンダー独自の実装を使用していることを示します。
ステップ 7	**key** {**0** *string* | **7** *string* | *string*} 例： `Device(config-radius-server)# key myRaDIUSpassword`	デバイスとベンダー独自仕様の RADIUS サーバーとの間で使用される共有秘密テキスト文字列を指定します。 • デバイスと RADIUS サーバーはこのテキスト文字列を使用してパスワードを暗号化し、応答を交換します。
ステップ 8	**exit** 例： `Device(config)# exit`	特権 EXEC モードに戻ります。

ネットワーク アクセス サーバーのポート情報を拡張するためのデバイス設定

コール自体が着信したインターフェイスとは別のインターフェイスで PPP 認証またはログイン認証が発生する場合があります。たとえば、V.120 ISDN コールでは、ログイン認証または PPP 認証は仮想非同期インターフェイス「ttt」で発生しますが、コール自体は ISDN インターフェイスのチャネルの 1 つで発生します。

radius-server attribute nas-port extended コマンドは、RADIUS を設定して NAS-Port 属性（RADIUS IETF 属性 5）フィールドのサイズを 32 ビットに拡張します。NAS-Port 属性の上位 16 ビットは、制御インターフェイスの種類と番号を示します。下位 16 ビットは、インターフェイスで実行中の認証を示します。

（注） **radius-server attribute nas-port format** コマンドは、**radius-server extended-portnames** コマンドおよび **radius-server attribute nas-port extended** コマンドの代わりに使用します。

手順の概要

1. **enable**
2. **configure terminal**
3. **radius-server configure-nas**
4. **radius-server attribute nas-port format**
5. **exit**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**radius-server configure-nas** 例： `Device(config)# radius-server configure-nas`	（任意）シスコ デバイスまたはアクセス サーバーが、そのドメイン内で使用するスタティック ルートと IP プール定義について RADIUS サーバーに照会するように指定します。 （注） **radius-server configure-nas** コマンドは、シスコ デバイスの起動時に使用されるため、**copy system:running-config nvram:startup-config** コマンドを発行するまで有効になりません。
ステップ 4	**radius-server attribute nas-port format** 例： `Device(config)# radius-server attribute nas-port format`	NAS-Port 属性のサイズを 16 ビットから 32 ビットに拡張して、拡張インターフェイス情報を表示できるようにします。
ステップ 5	**exit** 例：	特権 EXEC モードに戻ります。

	コマンドまたはアクション	目的
	`Device(config)# exit`	

NAS-Port 属性の RADIUS 属性への置き換え

各スロットに複数のインターフェイス（ポート）があるプラットフォームの場合、シスコの RADIUS 実装では、インターフェイスを区別できる固有の NAS-Port 属性を提供しません。たとえば、スロット 1 にデュアル PRI がある場合、RADIUS IETF NAS-Port 属性に関連付けられた 16 ビット フィールド サイズ制限により、Serial1/0:1 と Serial1/1:1 の両方でのコールが NAS-Port = 20101 として表示されます。この場合、NAS-Port 属性を VSA（RADIUS IETF 属性 26）に置き換えることができます。シスコのベンダー ID は 9 で、Cisco-NAS-Port 属性はサブタイプ 2 です。VSA を有効にするには、**radius-server vsa send** コマンドを入力します。ベンダー固有属性のポート情報を提供および設定するには、**aaa nas port extended** コマンドを使用します。

標準の NAS-Port 属性（RADIUS IETF 属性 5）が送信されます。この情報を送信しない場合、**no radius-server attribute nas-port** コマンドを使用して停止できます。このコマンドを設定すると、標準の NAS-Port 属性は送信されなくなります。

手順の概要

1. **enable**
2. **configure terminal**
3. **radius-server vsa send** [**accounting** | **authentication**]
4. **aaa nas port extended**
5. **exit**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**radius-server vsa send** [**accounting**	**authentication**] 例： `Device(config)# radius-server vsa send`	RADIUS IETF 属性 26 の定義に従って、ネットワーク アクセス サーバーがベンダー固有属性を認識および使用できるようにします。

	コマンドまたはアクション	目的
ステップ 4	**aaa nas port extended** 例： `Device(config)# aaa nas port extended`	VSA NAS-Port フィールドのサイズを 16 ビットから 32 ビットに拡張して、拡張インターフェイス情報を表示できるようにします。
ステップ 5	**exit** 例： `Device(config)# exit`	特権 EXEC モードに戻ります。

RADIUS のモニタリングとメンテナンス

手順の概要

1. **enable**
2. **debug radius**
3. **show radius statistics**
4. **show aaa servers**
5. **exit**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**debug radius** 例： `Device# debug radius`	RADIUS 関連の情報を表示します。
ステップ 3	**show radius statistics** 例： `Device# show radius statistics`	アカウンティングパケットと認証パケットについての RADIUS 統計情報を示します。 （注） RADIUS にエフェメラル送信元ポートを使用する IOS プロセスはほとんどなく、ポート番号は毎回異なる場合があります。
ステップ 4	**show aaa servers** 例：	AAA サーバー MIB によって解釈される、すべてのパブリックおよびプライベート AAA RADIUS サー

	コマンドまたはアクション	目的
	`Device# show aaa servers`	バーとの間で送受信されるパケットのステータスと数を表示します。
ステップ 5	**exit** 例： `Device# exit`	デバイス セッションを終了します。

RADIUS の設定例

例：RADIUS の認証と認可

次に、RADIUS を使用して認証および認可を行うようにデバイスを設定する例を示します。

```
aaa authentication login use-radius group radius local
aaa authentication ppp user-radius if-needed group radius
aaa authorization exec default group radius
aaa authorization network default group radius
```

この RADIUS 認証および認可設定のサンプル行は、次のように定義されます。

- **aaa authentication login use-radius group radius local** コマンドを実行すると、デバイスは、ログインプロンプトで認証にRADIUSを使用するように設定されます。RADIUSがエラーを返すと、ユーザーはローカル データベースを使用して認証されます。この例では、**use-radius** は方式リストの名前であり、RADIUS を指定し、次にローカル認証を指定します。
- **aaa authentication ppp user-radius if-needed group radius** コマンドで、ユーザーがまだ認可されていない場合に、CHAP または PAP による PPP を使用する回線に RADIUS 認証を使用するように Cisco ソフトウェアを設定します。EXEC ファシリティによってユーザーが認証済みの場合、RADIUS 認証は実行されません。この例では、**user-radius** は、if-needed 認証方式として RADIUS を定義する方式リストの名前です。
- **aaa authorization exec default group radius** コマンドで、EXEC 認可、autocommand、およびアクセス リストに使用する RADIUS 情報を設定します。
- **aaa authorization network default group radius** コマンドを実行すると、ネットワーク認可、アドレス割り当て、アクセス リストに RADIUS が設定されます。

例：RADIUS 認証、許可、アカウンティング

次に、AAA コマンドを設定して RADIUS を使用する一般的な設定例を示します。

```
radius-server host 10.45.1.2
```

```
radius-server key myRaDiUSpassWoRd
username root password ALongPassword
aaa authentication ppp dialins group radius local
aaa authorization network default group radius local
aaa accounting network default start-stop group radius
aaa authentication login admins local
aaa authorization exec default local
line 1 16
 autoselect ppp
 autoselect during-login
 login authentication admins
 modem ri-is-cd
interface group-async 1
 encaps ppp
 ppp authentication pap dialins
```

この例の RADIUS 認証、許可、アカウンティングの回線は、次のように定義されます。

- **radius-server host** コマンドは、RADIUS サーバー ホストの IP アドレスを定義します。
- **radius-server key** コマンドは、ネットワーク アクセス サーバーと RADIUS サーバー ホストの間の共有秘密テキスト文字列を定義します。
- **aaa authentication ppp dialins group radius local** コマンドで、まず RADIUS 認証を指定する認証方式リスト「dialins」を定義します。次に、（RADIUS サーバーが応答しない場合）PPP を使用するシリアル回線でローカル認証が使用されます。
- **aaa authorization network default group radius local** コマンドは、アドレスと他のネットワーク パラメータを RADIUS ユーザーに割り当てるために使用されます。
- **aaa accounting network default start-stop group radius** コマンドは、PPP の使用状況を追跡します。
- **aaa authentication login admins local** コマンドは、ログイン認証に別の方式リスト「admins」を定義します。
- **login authentication admins** コマンドは、ログイン認証に「admins」方式リストを適用します。
- **ppp authentication pap dialins** コマンドは「dialins」方式リストを指定した回線に適用します。

例：ベンダー固有の RADIUS 設定

次に、AAA コマンドを設定してベンダー固有の RADIUS を使用する一般的な設定例を示します。

（注） **radius-server host** コマンドは、Cisco IOS リリース 15.4(2)S 以降では廃止されています。IPv4 または IPv6 RADIUS サーバーを設定するには、**radius server** *name* コマンドを使用します。**radius server** コマンドの詳細については、『*Cisco IOS Security Command Reference: Commands M to R*』を参照してください。

```
radius server myserver
radius server address ipv4 192.0.2.2
non-standard
key 7 any key
radius-server configure-nas
username root password ALongPassword
aaa authentication ppp dialins group radius local
aaa authorization network default group radius local
aaa accounting network default start-stop group radius
aaa authentication login admins local
aaa authorization exec default local
```

この RADIUS 認証、認可、アカウンティング設定例の行は、次のように定義されます。

- **non-standard** コマンドは、RADIUS サーバー ホストの名前を定義し、この RADIUS ホストがベンダー独自バージョンの RADIUS を使用することを指定します。
- **key** コマンドは、ネットワーク アクセス サーバーと RADIUS サーバー ホストの間の共有秘密テキスト文字列を定義します。
- **configure-nas** コマンドは、シスコ デバイスが最初に起動したときに、そのデバイスまたはアクセス サーバーがスタティック ルートと IP プール定義について RADIUS サーバーに照会するように定義します。
- **aaa authentication ppp dialins group radius local** コマンドで、まず RADIUS 認証を指定する認証方式リスト「dialins」を定義します。次に、（RADIUS サーバーが応答しない場合）PPP を使用するシリアル回線でローカル認証が使用されます。
- **aaa authorization network default group radius local** コマンドは、アドレスと他のネットワーク パラメータを RADIUS ユーザーに割り当てます。
- **aaa accounting network default start-stop group radius** コマンドは、PPP の使用状況を追跡します。
- **aaa authentication login admins local** コマンドは、ログイン認証に別の方式リスト「admins」を定義します。

例：同じサーバー IP アドレスを持つ複数の RADIUS サーバー エントリ

次に、同じ IP アドレスを持つ複数の RADIUS ホスト エントリを認識するように、ネットワーク アクセス サーバーを設定する例を示します。同じ RADIUS サーバー上にある 2 つのホスト エントリは、同じサービス（認証とアカウンティング）のために設定されています。設定されている 2 番めのホスト エントリは、1 番めのエントリのフェールオーバー バックアップとして動作します（試行される RADIUS ホスト エントリの順番は、設定されている順序に従います）。

```
! This command enables AAA.
aaa new-model
! The next command configures default RADIUS parameters.
aaa authentication ppp default group radius
! The next set of commands configures multiple host entries for the same IP address.
radius-server host 172.20.0.1 auth-port 1000 acct-port 1001
radius-server host 172.20.0.1 auth-port 2000 acct-port 2001
```

その他の参考資料

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『*Cisco IOS Master Command List, All Releases*』
AAA コマンドと RADIUS コマンド	『*Cisco IOS Security Command Reference*』
RADIUS 属性	『*RADIUS Attributes Configuration Guide*』（Securing User Services Configuration Library の一部）
AAA	『*Authentication, Authorization, and Accounting Configuration Guide*』（Securing User Services Configuration Library の一部）
L2TP、VPN、または VPDN	『*Dial Technologies Configuration Guide*』および『*VPDN Configuration Guide*』
モデムの設定と管理	『*Dial Technologies Configuration Guide*』
PPP の RADIUS ポートの識別	『*Wide-Area Networking Configuration Guide*』

RFC

RFC	タイトル
RFC 2138	『*Remote Authentication Dial In User Service (RADIUS)*』
RFC 2139	『*RADIUS Accounting*』
RFC 2865	『*RADIUS*』
RFC 2867	『*RADIUS Accounting Modifications for Tunnel Protocol Support*』
RFC 2868	『*RADIUS Attributes for Tunnel Protocol Support*』

シスコのテクニカル サポート

説明	リンク
右の URL にアクセスして、シスコのテクニカル サポートを最大限に活用してください。これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

RADIUS の設定に関する機能情報

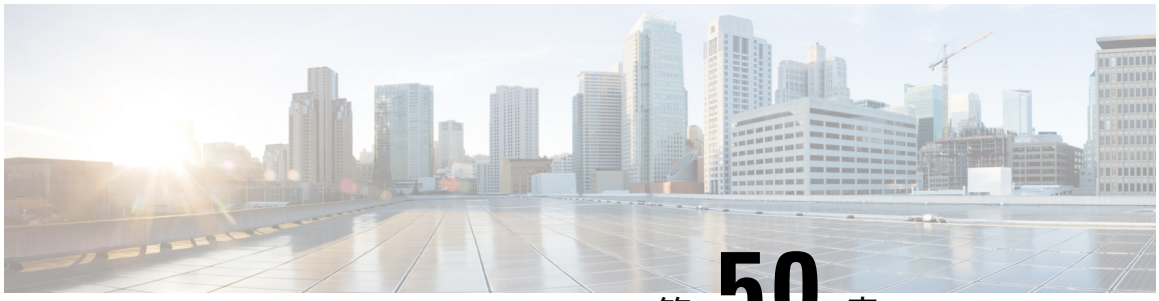
次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *74 : RADIUS* の設定に関する機能情報

機能名	リリース	機能情報
RADIUS の設定		RADIUS セキュリティ システムは、不正なアクセスからネットワークのセキュリティを保護する分散クライアント/サーバ システムです。シスコの実装では、RADIUS クライアントはシスコデバイス上で実行され、すべてのユーザ認証およびネットワーク サービス アクセス情報を持つ中央の RADIUS サーバに認証要求を送信します。 • Catalyst 3850 シリーズ スイッチ • Cisco 5760 Wireless LAN Controller • Catalyst 3650 シリーズ スイッチ

機能名	リリース	機能情報
SNMP を介する RADIUS 統計情報		この機能は、RADIUS トラフィックおよびプライベート RADIUS サーバーに関連する統計情報を提供します。 • Catalyst 3850 シリーズ スイッチ • Cisco 5760 Wireless LAN Controller • Catalyst 3650 シリーズ スイッチ 次のコマンドが導入または変更されました。**show aaa servers**、**show radius statistics**



第 50 章

複数の UDP ポート用の RADIUS

RADIUS セキュリティ サーバーは、ホスト名または IP アドレス、ホスト名と特定の UDP ポート番号、または IP アドレスと特定の UDP ポート番号により識別されます。IP アドレスと UDP ポート番号を組み合わせることによって、異なるポートを特定の認証、認可、およびアカウンティング（AAA）サービスを提供する RADIUS ホストとして個別に定義できます。この一意の ID を使用することによって、同じ IP アドレスにあるサーバー上の複数の UDP ポートに、RADIUS 要求を送信できます。同じ RADIUS サーバー上の異なる 2 つのホスト エントリに同じサービス（たとえば認証など）を設定した場合、2 番めに設定されたホスト エントリは、最初に設定されたホスト エントリのフェールオーバー バックアップとして動作します。最初のホスト エントリがアカウンティング サービスの提供に失敗すると、ネットワーク アクセス サーバーは同じデバイスに設定されている 2 番めのホスト エントリを使用してアカウンティング サービスを提供するように試行します。

複数の UDP ポート用の RADIUS の前提条件

シスコ デバイスまたはアクセス サーバーで RADIUS を設定するには、次のタスクを実行する必要があります。

- **aaa new-model** グローバル コンフィギュレーション コマンドを使用して、AAA をイネーブルにします。RADIUS を使用する予定がある場合、AAA を設定する必要があります。
- **aaa authentication** グローバル コンフィギュレーション コマンドを使用して、RADIUS 認証の方式リストを定義します。
- **line** および **interface** コマンドを使用して、使用する定義済みの方式リストをイネーブルにします。

複数の UDP ポート用の RADIUS に関する情報

デバイスと RADIUS サーバーの通信

通常、RADIUS ホストは、シスコ（CiscoSecure ACS）、Livingston、Merit、Microsoft、または他のソフトウェア プロバイダーの RADIUS サーバー ソフトウェアを実行するマルチユーザー システムです。RADIUS サーバーとの通信のためにデバイスを設定するには、次のような要素があります。

- ホスト名または IP アドレス
- 認証の宛先ポート
- アカウンティングの宛先ポート
- タイムアウト時間
- 再送信回数
- キー文字列

RADIUS セキュリティ サーバーは、ホスト名または IP アドレス、ホスト名と特定の UDP ポート番号、または IP アドレスと特定の UDP ポート番号により識別されます。固有の識別情報は、IP アドレスと UDP ポート番号の組み合わせで構成されます。これにより、RADIUS ホストとして定義されているさまざまなポートが、固有の AAA サービスを提供できるようになります。この一意の ID を使用することによって、同じ IP アドレスにあるサーバー上の複数の UDP ポートに、RADIUS 要求を送信できます。同じ RADIUS サーバー上の異なる 2 つのホストエントリに同じサービス（たとえば認証など）を設定した場合、2 番めに設定されたホストエントリは、最初に設定されたホスト エントリのフェールオーバー バックアップとして動作します。最初のホストエントリがアカウンティング サービスの提供に失敗すると、ネットワーク アクセス サーバーは同じデバイスに設定されている 2 番めのホスト エントリを使用してアカウンティング サービスを提供するように試行します。（試行される RADIUS ホスト エントリの順番は、設定されている順序に従います）。

RADIUS サーバーとシスコ デバイスは、共有秘密テキスト文字列を使用して、パスワードの暗号化および応答の交換を行います。RADIUS で AAA セキュリティ コマンドを使用するように設定するには、RADIUS サーバー デーモンが稼働するホストと、そのホストがデバイスと共有する秘密テキスト（キー）文字列を指定する必要があります。

タイムアウト値、再送信値、および暗号キー値には、すべての RADIUS サーバーを対象にしたグローバル設定、サーバー別設定、またはグローバル設定とサーバー別設定の組み合わせを使用できます。デバイスと通信するすべての RADIUS サーバーにこのような設定をグローバルに適用するには、**radius-server timeout**、**radius-server retransmit**、および **radius-server key** という 3 つの固有なグローバル コマンドを使用します。特定の RADIUS サーバーにこれらの値を適用するには、**radius-server host** コマンドをグローバル コンフィギュレーション モードで使用します。

（注） 同じシスコ製ネットワーク アクセス サーバーで、タイムアウト、再送信、およびキー値のコマンドを同時に設定（グローバル設定およびサーバー別設定）できます。デバイスにグローバル機能とサーバー別機能の両方を設定する場合、サーバー別のタイマー、再送信、およびキー値のコマンドが、グローバルのタイマー、再送信、およびキー値のコマンドよりも優先されます。

複数の UDP ポート用の RADIUS を設定する方法

デバイスと RADIUS サーバーの通信の設定

手順の概要

1. **enable**
2. **configure terminal**
3. **radius server** *server-name*
4. **address ipv4** *ip-address*
5. **key** {**0** *string* | **7** *string* | *string*}
6. **retransmit** *retries*
7. **timeout** *seconds*
8. **exit**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**radius server** *server-name* 例： `Device(config)# radius server rad1`	RADIUS サーバーの名前を指定します。
ステップ 4	**address ipv4** *ip-address* 例：	RADIUS サーバーに IP アドレスを割り当てます。

	コマンドまたはアクション	目的
	`Device(config-radius-server)# address ipv4 10.45.1.2`	
ステップ 5	**key** {**0** *string* | **7** *string* | *string*} 例： `Device(config-radius-server)# key myRaDIUSpassword`	デバイスとRADIUSサーバーの間で使用する共有秘密テキスト文字列を指定します。 （注） この手順では、暗号キーの値は、すべての RADIUS サーバーに対してグローバルに設定されます。 • **0** *string* オプションを使用して、暗号化されていない共有秘密を設定します。**7** *string* オプションを使用して、暗号化された共有秘密を設定します。
ステップ 6	**retransmit** *retries* 例： `Device(config-radius-server)# retransmit 25`	デバイスからサーバーに対して各RADIUS要求を送信する回数の上限を指定します（デフォルトは 3 です）。 （注） この手順では、再送信の値は、すべてのRADIUSサーバーに対してグローバルに設定されます。
ステップ 7	**timeout** *seconds* 例： `Device(config-radius-server)# timeout 6`	デバイスがRADIUS要求に対する応答を待機して、要求を再送信するまでの時間（秒数）を指定します。 （注） この手順では、タイムアウト値は、すべての RADIUS サーバーに対してグローバルに設定されます。
ステップ 8	**exit** 例： `Device(config)# exit`	特権 EXEC モードに戻ります。

複数の UDP ポート用の RADIUS の設定例

例：デバイスと RADIUS サーバーの通信

次に、固有のタイムアウト、再送信、およびキー値を指定した2つのRADIUSサーバーを設定する例を示します。この例では、**aaa new-model** コマンドを使用してデバイス上の AAA サービスを有効化し、特定の AAA コマンドで AAA サービスを定義します。**retransmit** コマンド

で、すべての RADIUS サーバーについて、グローバル再送信値を 4 に変更します。**host** コマンドで、IP アドレスが 172.16.1.1 と 172.29.39.46 の RADIUS サーバー ホストについて、特定のタイムアウト、再送信、およびキーの値を設定します。

```
! Enable AAA services on the device and define those services.
aaa new-model
aaa authentication login default group radius
aaa authentication login console-login none
aaa authentication ppp default group radius
aaa authorization network default group radius
aaa accounting exec default start-stop group radius
aaa accounting network default start-stop group radius
enable password tryit1
!
Device(config)# radius server rad1
Device(config-radius-server)# address ipv4 10.45.1.2
Device(config-radius-server)# key myRaDIUSpassword
Device(config-radius-server)# retransmit 25
Device(config-radius-server)# timeout 6
Device(config)# exit
```

例：サーバー固有の値を指定した RADIUS サーバー

次に、172.31.39.46 という IP アドレスの RADIUS サーバーについて、サーバー固有のタイムアウト、再送信、およびキー値を設定する例を示します。

```
radius-server host 172.31.39.46 timeout 6 retransmit 5 key rad123
```

その他の参考資料

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『Cisco IOS Master Command List, All Releases』
セキュリティ コマンド	• 『Cisco IOS Security Command Reference: Commands A to C』[英語] • 『Cisco IOS Security Command Reference: Commands D to L』[英語] • 『Cisco IOS Security Command Reference: Commands M to R』[英語] • 『Cisco IOS Security Command Reference: Commands S to Z』[英語]
AAA	『*Authentication, Authorization, and Accounting Configuration Guide*』（Securing User Services Configuration Library の一部）

シスコのテクニカル サポート

説明	リンク
右の URL にアクセスして、シスコのテクニカル サポートを最大限に活用してください。これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

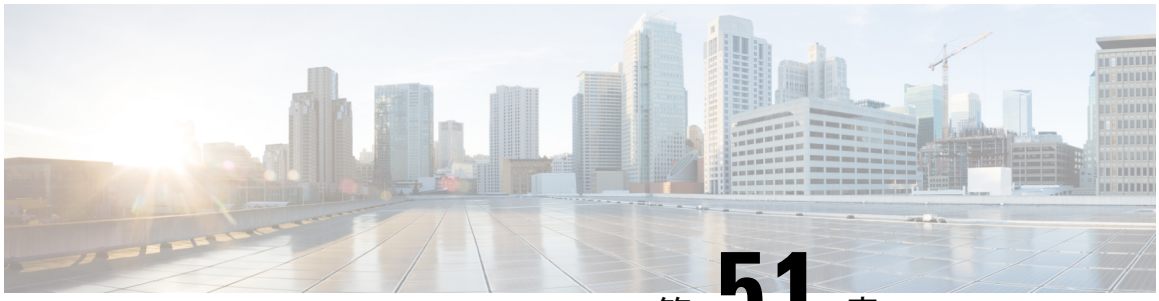
複数の UDP ポート用の RADIUS の機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *75* : 複数の *UDP* ポート用の *RADIUS* の機能情報

機能名	リリース	機能情報
複数の UDP ポート用の RADIUS		RADIUS セキュリティ サーバーは、ホスト名または IP アドレス、ホスト名と特定の UDP ポート番号、または IP アドレスと特定の UDP ポート番号により識別されます。固有の識別情報は、IP アドレスと UDP ポート番号の組み合わせで構成されます。これにより、RADIUS ホストとして定義されているさまざまなポートが、固有の AAA サービスを提供できるようになります。この一意の ID を使用することによって、同じ IP アドレスにあるサーバー上の複数の UDP ポートに、RADIUS 要求を送信できます。 • Catalyst 3850 シリーズ スイッチ • Catalyst 3650 シリーズ スイッチ 次のコマンドが導入または変更されました。**radius-server host**



第 51 章

許可用の AAA Dialed Number Information Service（DNIS）マップ

許可用の AAA DNIS マップ機能を使用すると、着信番号識別サービス（DNIS）番号を特定の認証、許可、およびアカウンティング（AAA）サーバー グループに割り当てることができます。これによって、サーバー グループは、その DNIS を使用して、ネットワークにダイヤルインするユーザーの認証、許可、アカウンティングの要求を処理できます。すべての電話回線（通常の自宅電話または商用の T1/PRI 回線）を、複数の電話番号と関連付けることができます。DNIS 番号は、ユーザー宛てに発信された番号を示します。

許可用の AAA DNIS マップの前提条件

- サーバー グループの DNIS に基づいて特定の AAA サーバー グループを選択するようにデバイスを設定する前に、RADIUS サーバー ホストと AAA サーバー グループの一覧を設定する必要があります。
- AAA 事前認証を設定する前に、**aaa new-model** コマンドを設定して、サポートする事前認証アプリケーションが使用中のネットワークの RADIUS サーバーで実行されていることを確認する必要があります。

許可用の AAA DNIS マップに関する情報

DNIS に基づく AAA サーバー グループの選択

Cisco ソフトウェアを使用すると、DNIS 番号を特定の AAA サーバ グループに割り当てることができます。これによって、サーバ グループは、その DNIS を使用して、ネットワークにダイヤルインするユーザの認証、認可、アカウンティングの要求を処理できます。すべての電話回線（通常の自宅電話または商用の T1/PRI 回線）を、複数の電話番号と関連付けることができます。DNIS 番号は、ユーザー宛てに発信された番号を示します。

たとえば、複数の顧客で同じ電話番号を共有する場合に、電話を受ける前に発信元を知りたいことがあります。DNIS を使用すると、応答するときに発信元の顧客がわかるため、電話に応答する方法をカスタマイズできます。

ISDN または内部モデムと接続するシスコ デバイスは、DNIS 番号を受信できます。この機能を使用すると、顧客ごとに異なる RADIUS サーバー グループを割り当て可能です（つまり、DNIS 番号ごとに異なる RADIUS サーバー）。さらに、サーバー グループを使用して、複数の AAA サービスに同じサーバー グループを指定できます。また、各 AAA サービスに個別のサーバー グループを指定できます。

Cisco ソフトウェアには、認証サービスとアカウンティング サービスを複数の方法で実装できる柔軟性があります。

- グローバル：AAA サービスは、グローバル コンフィギュレーション アクセス リスト コマンドを使用して定義され、特定のネットワーク アクセス サーバー上のすべてのインターフェイスに、全般的に適用されます。
- インターフェイス別：AAA サービスは、インターフェイス コンフィギュレーション コマンドを使用して定義され、特定のネットワーク アクセス サーバーに設定されているインターフェイスにだけ適用されます。
- DNIS マッピング：DNIS を使用して、AAA サーバーが AAA サービスを提供するように指定します。

このような複数の AAA コンフィギュレーション方式を同時に設定できるため、シスコでは、AAA サービスを提供するサーバまたはサーバ グループを決定するために、優先順位を設定しました。優先順位は次のとおりです。

- DNIS 別：DNIS を使用し、AAA サービスを提供するサーバ グループを指定または決定するようにネットワーク アクセス サーバを設定している場合、この方式がその他の AAA 選択方式よりも優先されます。
- インターフェイス別：サーバーから AAA サービスを提供する方法を決定するために、インターフェイス別にネットワーク アクセス サーバーを設定してアクセス リストを使用する場合、この方式は、他のグローバル コンフィギュレーション AAA アクセス リストよりも優先されます。

- グローバル：セキュリティ サーバーが AAA サービスを提供する方法を決定するために、グローバル AAA アクセス リストを使用してネットワーク アクセス サーバーを設定する場合、この方式には最も低い優先度が使用されます。

AAA 事前認証

ISDN PRI または個別線信号方式（CAS）による AAA 事前認証を設定すると、サービス プロバイダーは、既存の RADIUS ソリューションを使用するポートの管理性を改善し、共有リソースの使用を効率的に管理して、各種のサービスレベル契約を提供できるようになります。ISDN PRI または CAS によって、着信コールに関する情報をネットワーク アクセス サーバー（NAS）で使用してから、コールを接続できます。使用できるコール情報は次のとおりです。

- 着信番号識別サービス（DNIS）番号（着信者番号とも呼ばれます）
- 発呼回線 ID（CLID）番号（発番号とも呼ばれます）
- コール タイプ（ベアラ機能とも呼ばれます）

AAA 事前認証の機能を使用すると、Cisco NAS で、DNIS 番号、CLID 番号、またはコール タイプに基づいて着信コールを接続するかどうかを決定することができます。（ISDN PRI を使用する場合、ユーザーの認証と認可を行ってから、コールに応答できます。CAS を使用する場合、コールに応答する必要はありますが、事前認証に失敗した場合、コールをドロップできます）。

パブリック ネットワーク スイッチからコールを着信し、まだ接続前の場合、AAA 事前認証によって、NAS から DNIS 番号、CLID 番号、およびコール タイプを RADIUS サーバーに送信し、認可を受けることができます。サーバーがコールを認可すると、NAS はコールを許可します。サーバーがコールを認可しない場合、NAS からパブリック ネットワーク スイッチに接続解除メッセージが送信され、コールが拒否されます。

RADIUS サーバー アプリケーションが使用不能になった場合、または応答が遅くなった場合、NAS でガード タイマーを設定できます。タイマーが期限切れになると、NAS は設定可能なパラメータを使用して、認可されなかった着信コールを許可または拒否します。

AAA 事前認証の機能では、事前認証の動作を指定するために、RADIUS サーバー アプリケーションによる属性 44 の使用、および RADIUS 事前認証プロファイルに設定されている RADIUS 属性の使用がサポートされています。また、これらの属性は、たとえば、以降の認証を実行するかどうか、また実行する場合、どの認証方式を使用するかを指定するためにも使用できます。

ISDN PRI および CAS による AAA 事前認証には、次の制約事項が適用されます。

- 属性 44 は、事前認証またはリソース プーリングをイネーブルにした CAS コールにだけ使用できます。
- マルチシャーシ マルチリンク PPP（MMP）は、ISDN PRI では使用できません。
- AAA 事前認証は、一部のハードウェア プラットフォームでのみ使用できます。
- ISDN PRI は、一部のハードウェア プラットフォームでのみサポートされています。

コール処理のガード タイマー

事前認証要求および認可要求の応答時間はさまざまなので、ガードタイマーを使用してコールの処理を制御できます。ガードタイマーは、DNISがRADIUSサーバーに送信されると開始されます。ガード タイマーが期限切れになる前にNASがAAAから応答を受信しない場合、タイマーの設定に基づいてコールを許可または拒否します。

許可用の AAA DNIS マップの設定方法

AAA DNIS 事前認証の設定

DNIS 事前認証を使用すると、着信番号に基づいてコール設定時に事前認証を実行できます。DNIS 番号は、コールの着信時にセキュリティ サーバーに直接送信されます。コールが AAA によって認証されると、そのコールは許可されます。

手順の概要

1. **enable**
2. **configure terminal**
3. **aaa preauthorization**
4. **group** {**radius** | **tacacs+** | *server-group*}
5. **dnis** [**password** *string*]
6. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**aaa preauthorization** 例： `Device(config)# aaa preauthorization`	AAA 事前認証コンフィギュレーション モードを開始します。
ステップ 4	**group** {**radius**	**tacacs+**	*server-group*} 例：	（任意）AAA事前認証要求に使用するセキュリティ サーバーを選択します。

	コマンドまたはアクション	目的
	`Device(config-preauth)# group radius`	• デフォルトは RADIUS です。
ステップ 5	**dnis** [**password** *string*] 例： `Device(config-preauth)# dnis password dnispass`	DNIS を使用して事前認証をイネーブルにし、必要に応じてAccess-Requestパケットに使用するパスワードを指定します。
ステップ 6	**end** 例： `Device(config-preauth)# end`	AAA 事前認証コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

DNIS に基づく AAA サーバー グループの選択の設定

サーバー グループの DNIS に基づいて特定の AAA サーバー グループを選択するようにデバイスを設定するには、DNIS マッピングを設定します。DNIS 番号を使用してサーバー グループをグループ名とマッピングするには、次のタスクを実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **aaa dnis map enable**
4. **aaa dnis map** *dnis-number* **authentication ppp group** *server-group-name*
5. **aaa dnis map** *dnis-number* **authorization network group** *server-group-name*
6. **aaa dnis map** *dnis-number* **accounting network** [**none** | **start-stop** | **stop-only**] **group** *server-group-name*
7. **exit**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**aaa dnis map enable** 例：	DNIS マッピングをイネーブルにします。

	コマンドまたはアクション	目的
	`Device(config)# aaa dnis map enable`	
ステップ 4	**aaa dnis map** *dnis-number* **authentication ppp group** *server-group-name* 例： `Device(config)# aaa dnis map 7777 authentication ppp group sg1`	DNIS 番号を定義済みの AAA サーバー グループにマッピングします。このサーバー グループのサーバーは、認証に使用されます。
ステップ 5	**aaa dnis map** *dnis-number* **authorization network group** *server-group-name* 例： `Device(config)# aaa dnis map 7777 authorization network group sg1`	DNIS 番号を定義済みの AAA サーバー グループにマッピングします。このサーバー グループのサーバーは、認可に使用されます。
ステップ 6	**aaa dnis map** *dnis-number* **accounting network** [**none** | **start-stop** | **stop-only**] **group** *server-group-name* 例： `Device(config)# aaa dnis map 8888 accounting network stop-only group sg2`	DNIS 番号を定義済みの AAA サーバー グループにマッピングします。このサーバー グループのサーバーは、アカウンティングに使用されます。
ステップ 7	**exit** 例： `Device(config)# exit`	グローバル コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

AAA 事前認証の設定

手順の概要

1. **enable**
2. **configure terminal**
3. **aaa preauthorization**
4. **group** *server-group*
5. **clid** [**if-avail** | **required**] [**accept-stop**] [**password** *string*]
6. **ctype** [**if-avail** | **required**] [**accept-stop**] [**password** *string*]
7. **dnis** [**if-avail** | **required**] [**accept-stop**] [**password** *string*]
8. **dnis bypass** *dnis-group-name*
9. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**aaa preauthorization** 例： `Device(config)# aaa preauthorization`	AAA 事前認証コンフィギュレーション モードを開始します。
ステップ 4	**group** *server-group* 例： `Device(config-preauth)# group sg2`	事前認証に使用する AAA RADIUS サーバー グループを指定します。
ステップ 5	**clid** [**if-avail** | **required**] [**accept-stop**] [**password** *string*] 例： `Device(config-preauth)# clid required`	CLID 番号に基づいて、コールを事前認証します。
ステップ 6	**ctype** [**if-avail** | **required**] [**accept-stop**] [**password** *string*] 例： `Device(config-preauth)# ctype required`	コール タイプに基づいて、コールを事前認証します。
ステップ 7	**dnis** [**if-avail** | **required**] [**accept-stop**] [**password** *string*] 例： `Device(config-preauth)# dnis required`	DNIS 番号に基づいて、コールを事前認証します。
ステップ 8	**dnis bypass** *dnis-group-name* 例： `Device(config-preauth)# dnis bypass group1`	事前認証をバイパスする DNIS 番号のグループを指定します。
ステップ 9	**end** 例：	事前認証コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

	コマンドまたはアクション	目的
	`Device(config-preauth)# end`	

ガード タイマーの設定

RADIUS サーバーが認証要求または事前認証要求に応答できなかった場合にコールを許可または拒否するようにガード タイマーを設定するには、次のタスクを実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **isdn guard-timer** *milliseconds* [**on-expiry** {**accept** | **reject**}]
5. **call guard-timer** *milliseconds* [**on-expiry** {**accept** | **reject**}]
6. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface** *type number* 例： `Device(config)# interface serial 1/0/0:23`	インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	**isdn guard-timer** *milliseconds* [**on-expiry** {**accept** | **reject**}] 例： `Device(config-if)# isdn guard-timer 8000 on-expiry reject`	RADIUS サーバーが事前認証要求に応答できなかった場合にコールを許可または拒否できる ISDN ガード タイマーを設定します。
ステップ 5	**call guard-timer** *milliseconds* [**on-expiry** {**accept** | **reject**}] 例：	RADIUS サーバーが事前認証要求に応答できなかった場合にコールを許可または拒否できる CAS ガード タイマーを設定します。

	コマンドまたはアクション	目的
	`Device(config-if)# call guard-timer 2000 on-expiry accept`	
ステップ 6	**end** 例： `Device(config-if)# end`	インターフェイス コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

許可用の AAA DNIS マップの設定例

例：DNIS に基づく AAA サーバー グループの選択

次に、特定の AAA サービスを提供するために、DNIS に基づいて RADIUS サーバー グループを選択する例を示します。

```
! This command enables AAA.
aaa new-model
!
! The following set of commands configures the RADIUS attributes for each server
! that will be associated with one of the defined server groups.
radius-server host 172.16.0.1 auth-port 1645 acct-port 1646 key cisco1
radius-server host 172.17.0.1 auth-port 1645 acct-port 1646 key cisco2
radius-server host 172.18.0.1 auth-port 1645 acct-port 1646 key cisco3
radius-server host 172.19.0.1 auth-port 1645 acct-port 1646 key cisco4
radius-server host 172.20.0.1 auth-port 1645 acct-port 1646 key cisco5
! The following commands define the sg1 RADIUS server group and associate servers
! with it.
aaa group server radius sg1
  server 172.16.0.1
  server 172.17.0.1
! The following commands define the sg2 RADIUS server group and associate a server
! with it.
aaa group server radius sg2
  server 172.18.0.1
! The following commands define the sg3 RADIUS server group and associate a server
! with it.
aaa group server radius sg3
  server 172.19.0.1
! The following commands define the default-group RADIUS server group and associate
! a server with it.
aaa group server radius default-group
  server 172.20.0.1
! The next set of commands configures default-group RADIUS server group parameters.
aaa authentication ppp default group default-group
aaa accounting network default start-stop group default-group
!
! The next set of commands enables DNIS mapping and maps DNIS numbers to the defined
! RADIUS server groups. In this configuration, all PPP connection requests using
! DNIS 7777 are sent to the sg1 server group. The accounting records for these
! connections (specifically, start-stop records) are handled by the sg2 server group.
! Calls with a DNIS of 8888 use server group sg3 for authentication and server group
! default-group for accounting. Calls with a DNIS of 9999 use server group
```

```
! default-group for authentication and server group sg3 for accounting records
! (stop records only). All other calls with DNIS other than the ones defined use the
! server group default-group for both authentication and stop-start accounting records.
aaa dnis map enable
aaa dnis map 7777 authentication ppp group sg1
aaa dnis map 7777 accounting network start-stop group sg2
aaa dnis map 8888 authentication ppp group sg3
aaa dnis map 9999 accounting network stop-only group sg3
```

例：AAA 事前認証

次に、事前認証に DNIS 番号を指定する単純な設定を示します。

```
aaa preauthentication
 group radius
 dnis required
```

次に、事前認証に DNIS 番号と CLID 番号の両方を使用する設定の例を示します。DNIS 事前認証が先に実行され、次に CLID 事前認証が実行されます。

```
aaa preauthentication
 group radius
 dnis required
 clid required
```

次に、「dnis-group1」という DNIS グループに指定されている 2 つの DNIS 番号を除き、すべての DNIS 番号について事前認証を実行することを指定する例を示します。

```
aaa preauthentication
 group radius
 dnis required
 dnis bypass dnis-group1
dialer dnis group dnis-group1
 number 12345
 number 12346
```

次に、DNIS 事前認証を使用する AAA 設定の例を示します。

```
aaa new-model
aaa authentication login CONSOLE none
aaa authentication login RADIUS_LIST group radius
aaa authentication login TAC_PLUS group tacacs+ enable
aaa authentication login V.120 none
aaa authentication enable default enable group tacacs+
aaa authentication ppp RADIUS_LIST if-needed group radius
aaa authorization exec RADIUS_LIST group radius if-authenticated
aaa authorization exec V.120 none
aaa authorization network default group radius if-authenticated
aaa authorization network RADIUS_LIST if-authenticated group radius
aaa authorization network V.120 group radius if-authenticated
aaa accounting suppress null-username
aaa accounting exec default start-stop group radius
aaa accounting commands 0 default start-stop group radius
aaa accounting network default start-stop group radius
aaa accounting connection default start-stop group radius
aaa accounting system default start-stop group radius
aaa preauthentication
 dnis password Cisco-DNIS
aaa nas port extended
```

```
!
radius-server configure-nas
radius-server host 10.0.0.0 auth-port 1645 acct-port 1646 non-standard
radius-server host 10.255.255.255 auth-port 1645 acct-port 1646 non-standard
radius-server retransmit 2
radius-server deadtime 1
radius-server attribute nas-port format c
radius-server unique-ident 18
radius-server key MyKey
```

（注） 事前認証を設定するには、RADIUS サーバーでも事前認証プロファイルを設定する必要があります。

例：ISDN および CAS のガード タイマー

次に、8,000 ミリ秒に設定された ISDN ガード タイマーの例を示します。事前認証要求に対して RADIUS サーバーが応答しないまま、タイマーが期限切れになった場合、コールは拒否されます。

```
interface serial 1/0/0:23
 isdn guard-timer 8000 on-expiry reject
aaa preauthentication
 group radius
 dnis required
```

次に、20,000 ミリ秒に設定された CAS ガード タイマーの例を示します。事前認証要求に対して RADIUS サーバーが応答しないまま、タイマーが期限切れになった場合、コールは許可されます。

```
controller T1 0
 framing esf
 clock source line primary
 linecode b8zs
 ds0-group 0 timeslots 1-24 type e&m-fgb dtmf dnis
 cas-custom 0
 call guard-timer 20000 on-expiry accept
aaa preauthentication
group radius
dnis required
```

その他の参考資料

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『Cisco IOS Master Command List, All Releases』

関連項目	マニュアル タイトル
セキュリティ コマンド	• 『Cisco IOS Security Command Reference: Commands A to C』[英語] • 『Cisco IOS Security Command Reference: Commands D to L』[英語] • 『Cisco IOS Security Command Reference: Commands M to R』[英語] • 『Cisco IOS Security Command Reference: Commands S to Z』[英語]
AAA	『*Authentication, Authorization, and Accounting Configuration Guide*』（Securing User Services Configuration Library の一部）

シスコのテクニカル サポート

説明	リンク
右の URL にアクセスして、シスコのテクニカル サポートを最大限に活用してください。これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

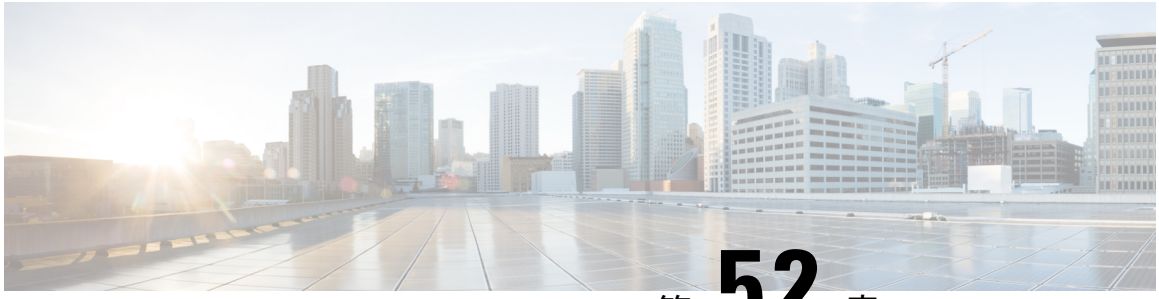
許可用の AAA DNIS マップの機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *76 :* 許可用の *AAA DNIS* マップの機能情報

機能名	リリース	機能情報
許可用の AAA Dialed Number Information Service（DNIS）マップ	12.1(1)T 12.2(2)T 12.2(27)SBA Cisco IOS XE Release 2.3	許可用の AAA DNIS マップ機能を使用すると、着信番号識別サービス（DNIS）番号を特定の AAA サーバー グループに割り当てることができます。これによって、サーバー グループは、その DNIS を使用して、ネットワークにダイヤルインするユーザーの認証、認可、およびアカウンティングの要求を処理できます。すべての電話回線（通常の自宅電話または商用の T1/PRI 回線）を、複数の電話番号と関連付けることができます。DNIS 番号は、ユーザー宛てに発信された番号を示します。 次のコマンドが導入または変更されました。**aaa dnis enable**、**aaa dnis map authentication group**、**aaa dnis map authorization network group**、および **aaa dnis map accounting network**



第 52 章

AAA サーバグループ

認証、認可、およびアカウンティング（AAA）サーバー グループを使用するようにデバイスを設定すると、既存のサーバーホストをグループ化できます。既存のサーバーホストをグループ化すると、設定したサーバーホストのサブセットを選択し、それを特定のサービスに使用できます。サーバー グループ内でデッドタイムを設定することで、AAA トラフィックを、異なる動作特性を持つ別のサーバー グループに送信できます。この機能モジュールでは、AAA サーバー グループとデッドタイマーを設定する方法について説明します。

AAA サーバー グループに関する情報

AAA サーバグループ

AAA サーバー グループを使用するようにデバイスを設定すると、既存のサーバー ホストをグループ化できます。既存のサーバー ホストをグループ化すると、設定したサーバー ホストのサブセットを選択し、それを特定のサービスに使用できます。サーバー グループは、グローバル サーバー ホストの一覧と一緒に使用されます。サーバー グループには、選択したサーバー ホストの IP アドレスが一覧表示されます。

また、サーバー グループには、各エントリが一意の ID を持っていれば、同一サーバーに複数のホスト エントリを組み込むことができます。固有の識別情報は、IP アドレスと UDP ポート番号の組み合わせで構成されます。これにより、RADIUS ホストとして定義されているさまざまなポートが、固有の AAA サービスを提供できるようになります。この一意の ID により、同じ IP アドレスでサーバーの異なる UDP ポートに RADIUS の要求を送ることができるようになります。同じ RADIUS サーバー上の異なる 2 つのホスト エントリに同じサービス（たとえばアカウンティングなど）を設定した場合、2 番目に設定されたホスト エントリは、最初に設定されたホスト エントリのフェールオーバー バックアップとして動作します。最初のホスト エ

ントリがアカウンティング サービスの提供に失敗すると、ネットワーク アクセス サーバは同じデバイスに設定されている 2 番めのホスト エントリを使用してアカウンティング サービスを提供するように試行します。（試行される RADIUS ホスト エントリの順番は、設定されている順序に従います）。

AAA サーバー グループのデッドタイマー

サーバー名を指定してサーバーホストを設定したら、**deadtime** コマンドを使用して、サーバーグループごとに各サーバーを設定できます。サーバー グループ内でデッドタイムを設定することで、AAA トラフィックを、異なる動作特性を持つ別のサーバー グループに送信できます。

デッドタイムの設定は、グローバル コンフィギュレーションに限定されません。すべてのサーバー グループの各サーバー ホストには、個別のタイマーがあります。そのため、サーバーが応答せず、再送信とタイムアウトが何度も発生する場合、そのサーバーは動作していない（デッド状態）と見なされます。すべてのサーバー グループの各サーバーホストに付属するタイマーが開始されます。基本的に、タイマーがチェックされ、サーバーに対する以降の要求は（デッド状態と見なされた場合）、（設定されていれば）代替タイマーに送信されます。ネットワーク アクセス サーバーがサーバーからの応答を受信すると、すべてのサーバー グループのそのサーバーに関するすべての設定済みタイマー（実行中の場合）が停止されます。

タイマーが期限切れになると、タイマーが付属しているサーバーは応答可能（アライブ状態）と見なされます。このサーバーは、タイマーが属するサーバー グループを使用して後で AAA 要求のために試行できる唯一のサーバーになります。

（注） 1 つのサーバーが複数のタイマーを持ち、異なるデッドタイム値がサーバー グループに設定されることがあるため、同時刻の同じサーバーでも複数の状態（デッドとアライブ）になる可能性があります。

（注） サーバーの状態を変更するには、すべてのサーバー グループですべての設定済みタイマーを起動および終了する必要があります。

新しいタイマーと deadtime 属性が追加されるため、サーバー グループのサイズはやや増えます。構造の全体的な影響は、サーバー グループの数と規模、およびその設定でサーバー グループ内でサーバーを共有する方法によって変わります。

AAA サーバー グループの設定方法

AAA サーバー グループの設定

サーバー グループ名を使用してサーバー ホストを定義するには、グローバル コンフィギュレーション モードで次のコマンドを使用します。一覧のサーバーは、グローバル コンフィギュレーション モードに存在します。

始める前に

グループの各サーバーは、**radius-server host** コマンドを使用して事前に定義する必要があります。

手順の概要

1. **enable**
2. **configure terminal**
3. **radius server** *server-name*
4. **aaa group server** {**radius** | **tacacs+**} *group-name*
5. **server** *ip-address* [**auth-port** *port-number*] [**acct-port** *port-number*]
6. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**radius server** *server-name* 例： `Device(config)# radius server rad1`	RADIUS サーバーの名前を指定します。
ステップ 4	**aaa group server** {**radius**	**tacacs+**} *group-name* 例： `Device(config)# aaa group server radius group1`	グループ名を使用して、AAA サーバー グループを定義します。 • グループのすべてのメンバは、タイプを同じにする必要があります。つまり、RADIUS または

	コマンドまたはアクション	目的
		TACACS+ です。このコマンドを実行すると、デバイスはサーバー グループRADIUSコンフィギュレーション モードへ移行します。
ステップ5	**server** *ip-address* [**auth-port** *port-number*] [**acct-port** *port-number*] 例： `Device(config-sg-radius)# server 172.16.1.1 acct-port 1616`	特定の RADIUS サーバーを定義済みのサーバー グループと関連付けます。 • セキュリティ サーバーは、IP アドレスと UDP ポート番号で識別されます。 • AAA サーバー グループの RADIUS サーバーごとに、このステップを繰り返します。
ステップ6	**end** 例： `Device(config-sg-radius)# end`	サーバー グループ RADIUS コンフィギュレーション モードを終了し、特権EXECモードに戻ります。

AAA サーバー グループのデッドタイマーの設定

手順の概要

1. **enable**
2. **configure terminal**
3. **aaa group server radius** *group*
4. **deadtime** *minutes*
5. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • プロンプトが表示されたらパスワードを入力します。
ステップ2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 3	**aaa group server radius** *group* 例： `Device(config)# aaa group server radius group1`	RADIUS タイプ サーバー グループを定義し、サーバー グループ RADIUS コンフィギュレーション モードを開始します。
ステップ 4	**deadtime** *minutes* 例： `Device(config-sg-radius)# deadtime 1`	デッドタイム値（分）を設定および定義します。 （注） ローカル サーバー グループのデッドタイムは、グローバル コンフィギュレーションよりも優先されます。ローカル サーバー グループ コンフィギュレーションでデッドタイム値を省略した場合は、プライマリ リストから継承されます。
ステップ 5	**end** 例： `Device(config-sg-radius)# end`	サーバーグループ RADIUS コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

AAA サーバー グループの設定例

例：AAA サーバー グループ

次に、3 つの RADIUS サーバ メンバを持ち、各メンバがデフォルトの認証ポート（1645）とアカウンティング ポート（1646）を使用するサーバ グループ radgroup1 を作成する例を示します。

```
aaa group server radius radgroup1
 server 172.16.1.11
 server 172.17.1.21
 server 172.18.1.31
```

次に、3 つの RADIUS サーバ メンバを持ち、各メンバが IP アドレスは同じでも認証ポートとアカウンティング ポートはそれぞれ異なるサーバ グループ radgroup2 を作成する例を示します。

```
aaa group server radius radgroup2
 server 172.16.1.1 auth-port 1000 acct-port 1001
 server 172.16.1.1 auth-port 2000 acct-port 2001
 server 172.16.1.1 auth-port 3000 acct-port 3001
```

例：AAA サーバー グループを使用する複数の RADIUS サーバー エントリ

次に、2 つの RADIUS サーバー グループを認識するようにネットワーク アクセス サーバーを設定する例を示します。一方のグループである group1 には、同じ RADIUS サーバー上に同じサービス用に設定された 2 つのホスト エントリがあります。設定されている 2 番めのホスト エントリは、1 番めのエントリのフェールオーバー バックアップとして動作します各グループのデッドタイムは個々に設定されています。group 1 のデッドタイムは 1 分で、group 2 のデッドタイムは 2 分です。

（注） グローバル コマンドと **server** コマンドの両方を使用する場合、**server** コマンドがグローバル コマンドよりも優先されます。

```
! This command enables AAA.
aaa new-model
! The next command configures default RADIUS parameters.
aaa authentication ppp default group group1
! The following commands define the group1 RADIUS server group and associate servers
! with it and configures a deadtime of one minute.
aaa group server radius group1
 server 10.1.1.1 auth-port 1645 acct-port 1646
 server 10.2.2.2 auth-port 2000 acct-port 2001
 deadtime 1
! The following commands define the group2 RADIUS server group and associate servers
! with it and configures a deadtime of two minutes.
aaa group server radius group2
 server 10.2.2.2 auth-port 2000 acct-port 2001
 server 10.3.3.3 auth-port 1645 acct-port 1646
 deadtime 2
! The following set of commands configures the RADIUS attributes for each host entry
! associated with one of the defined server groups.
radius-server host 10.1.1.1 auth-port 1645 acct-port 1646
radius-server host 10.2.2.2 auth-port 2000 acct-port 2001
radius-server host 10.3.3.3 auth-port 1645 acct-port 1646
```

その他の参考資料

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『*Cisco IOS Master Command List, All Releases*』
AAA コマンドと RADIUS コマンド	『*Cisco IOS Security Command Reference*』
RADIUS 属性	『*RADIUS Attributes Configuration Guide*』（Securing User Services Configuration Library の一部）

関連項目	マニュアル タイトル
AAA	『*Authentication, Authorization, and Accounting Configuration Guide*』（Securing User Services Configuration Library の一部）
L2TP、VPN、または VPDN	『*Dial Technologies Configuration Guide*』および『*VPDN Configuration Guide*』
モデムの設定と管理	『*Dial Technologies Configuration Guide*』
PPP の RADIUS ポートの識別	『*Wide-Area Networking Configuration Guide*』

RFC

RFC	タイトル
RFC 2138	『*Remote Authentication Dial In User Service (RADIUS)*』
RFC 2139	『*RADIUS Accounting*』
RFC 2865	『*RADIUS*』
RFC 2867	『*RADIUS Accounting Modifications for Tunnel Protocol Support*』
RFC 2868	『*RADIUS Attributes for Tunnel Protocol Support*』

シスコのテクニカル サポート

説明	リンク
右の URL にアクセスして、シスコのテクニカル サポートを最大限に活用してください。これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

AAA サーバー グループの機能情報

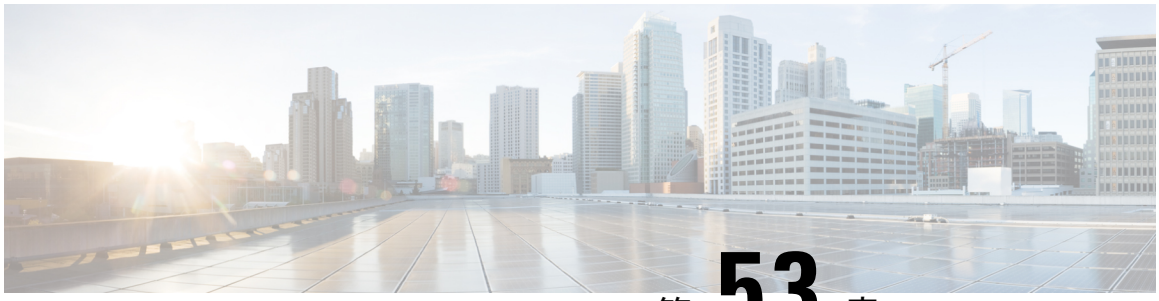
次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 77：AAA サーバー グループの機能情報

機能名	リリース	機能情報
AAA Server Group		AAA サーバー グループを使用するようにデバイスを設定すると、既存のサーバー ホストをグループ化できます。これによって、設定したサーバー ホストのサブセットを選択し、それを特定のサービスに使用できます。サーバー グループは、グローバル サーバー ホストの一覧と一緒に使用されます。サーバー グループには、選択したサーバー ホストの IP アドレスが一覧表示されます。 • Catalyst 3850 シリーズ スイッチ • Cisco 5760 Wireless LAN Controller • Catalyst 3650 シリーズ スイッチ 次のコマンドが導入または変更されました。**aaa group server radius**、**aaa group server tacacs+**、および **server**（RADIUS）。

機能名	リリース	機能情報
AAA サーバー グループの拡張機能		AAA サーバー グループの拡張機能により、サーバー グループ内のサーバーの完全な設定が可能です。 • Catalyst 3850 シリーズ スイッチ • Cisco 5760 Wireless LAN Controller • Catalyst 3650 シリーズ スイッチ
AAA サーバー グループ デッドタイマー		サーバー グループ内でデッドタイムを設定することで、AAA トラフィックを、異なる動作特性を持つ別のサーバーグループに送信できます。 • Catalyst 3850 シリーズ スイッチ • Cisco 5760 Wireless LAN Controller • Catalyst 3650 シリーズ スイッチ 次のコマンドが導入または変更されました。**deadtime**



第 53 章

RADIUS アカウンティング内の Framed-Route

RADIUS アカウンティング内の Framed-Route 機能は、RADIUS Accounting-Request アカウンティング レコードに Framed-Route（RADIUS 属性 22）情報を挿入します。Framed-Route 情報は、Accounting-Request パケットで RADIUS サーバーに返されます。Framed-Route 情報を使用すれば、ユーザー単位ルートがネットワーク アクセス サーバー（NAS）上の特定の静的 IP 顧客に適用されているかどうかを確認できます。

RADIUS アカウンティング内の Framed-Route の前提条件

認証、許可、アカウンティング（AAA）、RADIUS サーバー、および RADIUS 属性スクリーニングの設定に精通している必要があります。

RADIUS アカウンティング内の Framed-Route に関する情報

Framed-Route 属性 22

インターネット技術特別調査委員会（IETF）標準の RFC 2865 で属性 22 として定義されている Framed-Route は、NAS 上のユーザーに対して設定すべきルーティング情報を提供します。通常、Framed-Route 属性情報は、Access-Accept パケットで RADIUS サーバーから NAS に送信されます。この属性は複数挿入できます。

RADIUS アカウンティング パケット内の Framed-Route

RADIUS アカウンティング パケット内の Framed-Route 属性情報は、NAS 上の特定の静的 IP 顧客に適用されたユーザー単位ルートを表します。現在は、Framed-Route 属性情報が Access-Accept パケットで送信されます。Framed-Route 属性情報は、Access-Accept パケットに挿入され、正常に適用されていれば、Accounting-Request パケットでも送信されます。Accounting-Request パケットには、0 個以上の Framed-Route 属性を挿入できます。

（注） Access-Accept パケット内に複数の Framed-Route 属性が存在する場合は、Accounting-Request 内にも複数の Framed-Route 属性を挿入できます。

Framed-Route 情報は、accounting Delay-Start の設定時に、Stop および Interim アカウンティング レコードと Start アカウンティング レコードで返されます。

Frame-Route 属性情報を RADIUS アカウンティング パケットで返すための設定は不要です。

RADIUS アカウンティング内の Framed-Route のモニター方法

debug radius コマンドを使用して、Framed-Route（属性 22）の情報が RADIUS Accounting-Request パケットで送信されているかどうかをモニターします。

RADIUS アカウンティング内の Framed-Route の設定例

debug radius コマンドの出力例

次の例では、**debug radius** コマンドを使用して、Framed-Route（属性 22）情報が Accounting-Request パケットで送信されているかどうかを確認します（00:06:23: RADIUS: Framed-Route [22] 26 "10.80.0.1 255.255.255.255 10.60.0.1 100" の行を参照）。

```
Router# debug radius
00:06:23: RADIUS:  Send to unknown id 0 10.1.0.2:1645, Access-Request, len 126
00:06:23: RADIUS:  authenticator 40 28 A8 BC 76 D4 AA 88 - 5A E9 C5 55 0E 50 84 37
00:06:23: RADIUS:  Framed-Protocol     [7]   6   PPP                       [1]
00:06:23: RADIUS:  User-Name           [1]   14  "nari@trw1001"
00:06:23: RADIUS:  CHAP-Password       [3]   19  *
00:06:23: RADIUS:  NAS-Port            [5]   6   1
00:06:23: RADIUS:  Vendor, Cisco       [26]  33
00:06:23: RADIUS:  Cisco AVpair        [1]   27  "interface=Virtual-Access1"
00:06:23: RADIUS:  NAS-Port-Type       [61]  6   Virtual                   [5]
00:06:23: RADIUS:  Service-Type        [6]   6   Framed                    [2]
00:06:23: RADIUS:  NAS-IP-Address      [4]   6   12.1.0.1
00:06:23: RADIUS:  Acct-Session-Id     [44]  10  "00000002"
00:06:23: RADIUS:  Received from id 0 10.1.0.2:1645, Access-Accept, len 103
```

```
00:06:23: RADIUS:  authenticator 5D 2D 9F 25 11 15 45 B2 - 54 BB 7F EB CE 79 20 3B
00:06:23: RADIUS:  Vendor, Cisco       [26]  33
00:06:23: RADIUS:  Cisco AVpair        [1]   27  "interface=Virtual-Access1"
00:06:23: RADIUS:  Service-Type        [6]   6   Framed                    [2]
00:06:23: RADIUS:  Framed-Protocol     [7]   6   PPP                      [1]
00:06:23: RADIUS:  Framed-IP-Netmask   [9]   6   255.255.255.255
00:06:23: RADIUS:  Framed-IP-Address   [8]   6   10.60.0.1
00:06:23: RADIUS:  Framed-Route        [22]  26  "10.80.0.1 255.255.255.255 10.60.0.1
100"        <=======
00:06:23: RADIUS:  Received from id 2
00:06:24: %LINEPROTO-5-UPDOWN: Line protocol on Interface Virtual-Access1, changed state
 to up
00:06:25: AAA/AUTHOR:  Processing PerUser AV route
00:06:25: Vi1 AAA/PERUSER/ROUTE: route string: IP route  10.80.0.1 255.255.255.255
10.60.0.1 100
00:06:25: RADIUS/ENCODE(00000002): Unsupported AAA attribute timezone
00:06:25: RADIUS(00000002): sending
00:06:25: RADIUS:  Send to unknown id 1 10.1.0.2:1646, Accounting-Request, len 278
00:06:25: RADIUS:  authenticator E0 CC 99 EB 49 18 B9 78 - 4A 09 60 0F 4E 92 24 C6
00:06:25: RADIUS:  Acct-Session-Id     [44]  10  "00000002"
00:06:25: RADIUS:  Tunnel-Server-Endpoi[67]  12  00:"10.1.1.1"
00:06:25: RADIUS:  Tunnel-Client-Endpoi[66]  12  00:"10.1.1.2"
00:06:25: RADIUS:  Tunnel-Assignment-Id[82]  15  00:"from_isdn101"
00:06:25: RADIUS:  Tunnel-Type         [64]  6   00:L2TP                  [3]
00:06:25: RADIUS:  Acct-Tunnel-Connecti[68]  12  "2056100083"
00:06:25: RADIUS:  Tunnel-Client-Auth-I[90]  10  00:"isdn101"
00:06:25: RADIUS:  Tunnel-Server-Auth-I[91]  6   00:"lns"
00:06:25: RADIUS:  Framed-Protocol     [7]   6   PPP                      [1]
00:06:25: RADIUS:  Framed-Route        [22]  39  "10.80.0.1 255.255.255.255 10.60.0.1
100"          <========
00:06:25: RADIUS:  Framed-IP-Address   [8]   6   10.60.0.1
00:06:25: RADIUS:  Vendor, Cisco       [26]  35
00:06:25: RADIUS:  Cisco AVpair        [1]   29  "connect-progress=LAN Ses Up"
00:06:25: RADIUS:  Authentic           [45]  6   RADIUS                   [1]
00:06:25: RADIUS:  User-Name           [1]   14  "username1@example.com"
00:06:25: RADIUS:  Acct-Status-Type    [40]  6   Start                    [1]
00:06:25: RADIUS:  NAS-Port            [5]   6   1
00:06:25: RADIUS:  Vendor, Cisco       [26]  33
00:06:25: RADIUS:  Cisco AVpair        [1]   27  "interface=Virtual-Access1"
00:06:25: RADIUS:  NAS-Port-Type       [61]  6   Virtual                  [5]
00:06:25: RADIUS:  Service-Type        [6]   6   Framed                   [2]
00:06:25: RADIUS:  NAS-IP-Address      [4]   6   10.1.0.1
00:06:25: RADIUS:  Acct-Delay-Time     [41]  6   0
```

その他の参考資料

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『Cisco IOS Master Commands List, All Releases』
セキュリティ コマンド：コマンド構文の詳細、コマンドモード、コマンド履歴、デフォルト設定、使用上のガイドライン、および例	『*Cisco IOS Security Command Reference*』

関連項目	マニュアル タイトル
RADIUS	「Configuring RADIUS」機能モジュール。

標準

標準	タイトル
この機能でサポートされる新規の標準または変更された標準はありません。また、既存の標準のサポートは変更されていません。	--

MIB

MIB	MIB のリンク
なし。	選択したプラットフォーム、Cisco ソフトウェア リリース、およびフィーチャ セットの MIB を検索してダウンロードする場合は、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

RFC

RFC	タイトル
RFC 2865	『Remote Authentication Dial In User Service (RADIUS)』
RFC 3575	『IANA Considerations for RADIUS (Remote Authentication Dial In User Service)』

シスコのテクニカル サポート

説明	リンク
シスコのサポート Web サイトでは、シスコの製品やテクノロジーに関するトラブルシューティングにお役立ていただけるように、マニュアルやツールをはじめとする豊富なオンライン リソースを提供しています。 お使いの製品のセキュリティ情報や技術情報を入手するために、Cisco Notification Service（Field Notice からアクセス）、Cisco Technical Services Newsletter、Really Simple Syndication（RSS）フィードなどの各種サービスに加入できます。 シスコのサポート Web サイトのツールにアクセスする際は、Cisco.com のユーザ ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

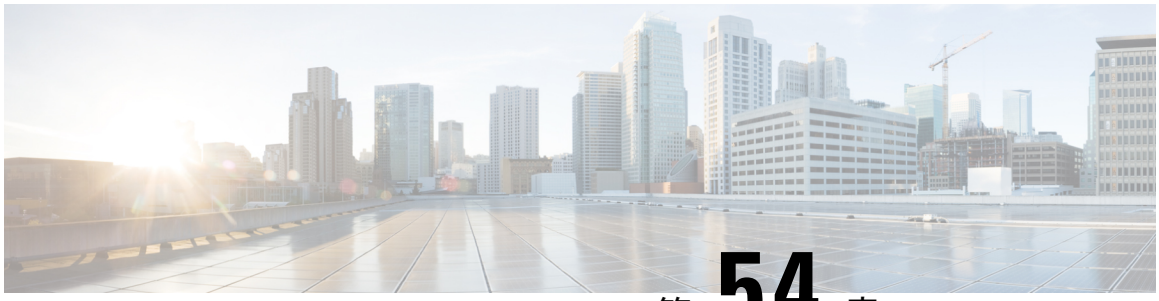
RADIUS アカウンティング内の Framed-Route の機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *78 : RADIUS* アカウンティング内の *Framed-Route* の機能情報

機能名	リリース	機能情報
RADIUS アカウンティング内の Framed-Route	Cisco IOS XE Release 2.1	RADIUS アカウンティング内の Framed-Route 機能は、RADIUS Accounting-Request アカウンティング レコードに Framed-Route（RADIUS 属性 22）情報を挿入します。 この機能は、Cisco IOS XE Release 2.1 で、Cisco ASR 1000 シリーズ アグリゲーション サービス ルータに導入されました。



第 54 章

RFC-2867 RADIUS トンネル アカウンティング

RFC-2867 RADIUS トンネル アカウンティングは、6 つの新しい RADIUS アカウンティング タイプを導入しています。これらのタイプは、アカウンティング要求がユーザー サービスの始まり（開始）と終わり（終了）のどちらを表しているかを示す、RADIUS アカウンティング属性の Acct-Status-Type（属性 40）と一緒に使用されます。

また、この機能は、ユーザーによる VPDN セッション イベントのトラブルシューティングを支援する 2 つの新しい仮想プライベート ダイヤルアップ ネットワーク（VPDN）コマンドを導入しています。

RFC-2867 RADIUS トンネル アカウンティングの制約事項

RADIUS トンネル アカウンティングは、L2TP トンネル サポートがなければ動作しません。

RFC-2867 RADIUS トンネル アカウンティングに関する情報

RFC-2867 RADIUS トンネル アカウンティングの利点

ユーザーが tunnel-link ステータスの変化を判断できるようにするネットワーク アカウンティングを使用した VPDN では、RADIUS トンネル アカウンティングがサポートされていないため、

使用可能なすべての属性がアカウンティング レコード ファイルに書き込まれませんでした。現在は使用可能なすべての属性を表示できるため、ユーザーはアカウンティング レコードをインターネット サービス プロバイダー（ISP）に確認しやすくなりました。

RADIUS トンネル アカウンティングのための RADIUS 属性サポート

以下の表に、ダイヤルアップ ネットワーク内の Compulsory Tunneling のプロビジョンをサポートするように設計された新しい RADIUS アカウンティング タイプの概要を示します。これらの属性タイプを使用すると、トンネル ステータスの変化をより適切に追跡できます。

（注） アカウンティング タイプは 2 つのトンネル タイプに分けられるため、ユーザーは、トンネル タイプが必要なのか、tunnel-link タイプが必要なのか、両方のアカウンティング タイプが必要なのかを判断できます。

表 *79 : Acct-Status-Type* 属性用の *RADIUS* アカウンティング タイプ

タイプ名	ケース	説明	追加属性[1]
Tunnel-Start	9	別のノードとのトンネルセットアップの始まりを示します。	• User-Name（1）：クライアントから • NAS-IP-Address（4）：AAA から • Acct-Delay-Time（41）：AAA から • Event-Timestamp（55）：AAA から • Tunnel-Type（64）：クライアントから • Tunnel-Medium-Type（65）：クライアントから • Tunnel-Client-Endpoint（66）：クライアントから • Tunnel-Server-Endpoint（67）：クライアントから • Acct-Tunnel-Connection（68）：クライアントから

タイプ名	ケース	説明	追加属性[1]
Tunnel-Stop	10	別のノードへの、または別のノードからのトンネル接続の終わりを示します。	• User-Name（1）：クライアントから • NAS-IP-Address（4）：AAA から • Acct-Delay-Time（41）：AAA から • Acct-Input-Octets（42）：AAA から • Acct-Output-Octets（43）：AAA から • Acct-Session-Id（44）：AAA から • Acct-Session-Time（46）：AAA から • Acct-Input-Packets（47）：AAA から • Acct-Output-Packets（48）：AAA から • Acct-Terminate-Cause（49）：AAA から • Acct-Multi-Session-Id（51）：AAA から • Event-Timestamp（55）：AAA から • Tunnel-Type（64）：クライアントから • Tunnel-Medium-Type（65）：クライアントから • Tunnel-Client-Endpoint（66）：クライアントから • Tunnel-Server-Endpoint（67）：クライアントから • Acct-Tunnel-Connection（68）：クライアントから • Acct-Tunnel-Packets-Lost（86）：クライアントから

タイプ名	ケース	説明	追加属性[1]
Tunnel-Reject	11	別のノードとのトンネルセットアップの拒否を示します。	• User-Name（1）：クライアントから • NAS-IP-Address（4）：AAA から • Acct-Delay-Time（41）：AAA から • Acct-Terminate-Cause（49）：クライアントから • Event-Timestamp（55）：AAA から • Tunnel-Type（64）：クライアントから • Tunnel-Medium-Type（65）：クライアントから • Tunnel-Client-Endpoint（66）：クライアントから • Tunnel-Server-Endpoint（67）：クライアントから • Acct-Tunnel-Connection（68）：クライアントから
Tunnel-Link-Start	12	トンネル リンクの構築を示します。一部のトンネル タイプ（レイヤ 2 トランスポート プロトコル（L2TP）しか、トンネル当たりの複数リンクをサポートしていません。この値は、トンネル当たりの複数リンクをサポートしているトンネル タイプのアカウンティング パケット以外には含めないでください。	• User-Name（1）：クライアントから • NAS-IP-Address（4）：AAA から • NAS-Port（5）：AAA から • Acct-Delay-Time（41）：AAA から • Event-Timestamp（55）：AAA から • Tunnel-Type（64）：クライアントから • Tunnel-Medium-Type（65）：クライアントから • Tunnel-Client-Endpoint（66）：クライアントから • Tunnel-Server-Endpoint（67）：クライアントから • Acct-Tunnel-Connection（68）：クライアントから

タイプ名	ケース	説明	追加属性[1]
Tunnel-Link-Stop	13	トンネル リンクの終わりを示します。一部のトンネル タイプ（L2TP）しか、トンネル当たりの複数リンクをサポートしていません。この値は、トンネル当たりの複数リンクをサポートしているトンネル タイプのアカウンティング パケット以外には含めないでください。	• User-Name（1）：クライアントから • NAS-IP-Address（4）：AAA から • NAS-Port（5）：AAA から • Acct-Delay-Time（41）：AAA から • Acct-Input-Octets（42）：AAA から • Acct-Output-Octets（43）：AAA から • Acct-Session-Id（44）：AAA から • Acct-Session-Time（46）：AAA から • Acct-Input-Packets（47）：AAA から • Acct-Output-Packets（48）：AAA から • Acct-Terminate-Cause（49）：AAA から • Acct-Multi-Session-Id（51）：AAA から • Event-Timestamp（55）：AAA から • NAS-Port-Type（61）：AAA から • Tunnel-Type（64）：クライアントから • Tunnel-Medium-Type（65）：クライアントから • Tunnel-Client-Endpoint（66）：クライアントから • Tunnel-Server-Endpoint（67）：クライアントから • Acct-Tunnel-Connection（68）：クライアントから • Acct-Tunnel-Packets-Lost（86）：クライアントから

タイプ名	ケース	説明	追加属性[1]
Tunnel-Link-Reject	14	既存のトンネル内の新しいリンクに対するトンネルセットアップの拒否を示します。一部のトンネル タイプ（L2TP）しか、トンネル当たりの複数リンクをサポートしていません。この値は、トンネル当たりの複数リンクをサポートしているトンネル タイプのアカウンティング パケット以外には含めないでください。	• User-Name（1）：クライアントから • NAS-IP-Address（4）：AAA から • Acct-Delay-Time（41）：AAA から • Acct-Terminate-Cause（49）：AAA から • Event-Timestamp（55）：AAA から • Tunnel-Type（64）：クライアントから • Tunnel-Medium-Type（65）：クライアントから • Tunnel-Client-Endpoint（66）：クライアントから • Tunnel-Server-Endpoint（67）：クライアントから • Acct-Tunnel-Connection（68）：クライアントから

[1] 指定されたトンネル タイプが使用されている場合は、これらの属性もアカウンティング要求パケットに含める必要があります。

RADIUS トンネル アカウンティングの設定方法

トンネル タイプ アカウンティング レコードの有効化

このタスクを使用して、トンネル レコードと tunnel-link アカウンティング レコードを RADIUS サーバーに送信するように LAC を設定します。

vpdn セッション アカウンティング ネットワーク（tunnel-link-type レコード）と vpdn トンネル アカウンティング ネットワーク（tunnel-type レコード）という 2 つの新しいコマンドライン インターフェイス（CLI）が、次のイベントの特定を支援するためにサポートされています。

- VPDN トンネルが構築または破壊された。
- VPDN トンネルの作成要求が拒否された。
- VPDN トンネル内のユーザー セッションが起動または停止された。
- ユーザー セッション作成要求が拒否された。

（注） 最初の 2 つのイベントは、tunnel-type アカウンティング レコードです。認証、許可、アカウンティング（AAA）が、Tunnel-Start、Tunnel-Stop、または Tunnel-Reject アカウンティング レコードを RADIUS サーバーに送信します。次の 2 つのイベントは、tunnel-link-type アカウンティング レコードです。AAA が、Tunnel-Link-Start、Tunnel-Link-Stop、または Tunnel-Link-Reject アカウンティング レコードを RADIUS サーバーに送信します。

手順の概要

1. **enable**
2. **configure terminal**
3. Router(config)# **aaa accounting network default** *list-name*} {**start-stop** | **stop-only** | **wait-start** | **none group** *groupname*
4. Router(config)# **vpdn enable**
5. Router(config)# **vpdn tunnel accounting network** *list-name*
6. Router(config)# **vpdn session accounting network** *list-name*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	Router(config)# **aaa accounting network default** *list-name*} {**start-stop** | **stop-only** | **wait-start** | **none group** *groupname* 例： 例： 例： 例： 例：	ネットワーク アカウンティングを有効にします。 • **default** ：デフォルトのネットワーク アカウンティングの方式リストが設定され、インターフェイス上でどの追加のアカウンティング設定も有効になっていない場合は、デフォルトで、ネットワーク アカウンティングが有効になります。 **vpdn session accounting network** コマンドまたは **vpdn tunnel accounting network** コマンドが **default** 方式リストにリンクされている場合、すべてのトンネルおよびトンネルリンク アカウンティング レコードが、これらのセッションで有効になります。

	コマンドまたはアクション	目的
	例： 例： 例： 例： 例： 例： `Router(config)# aaa accounting network m1 start-stop group radius`	• *list-name* ：**aaa accounting** コマンドで定義された *list-name* は、VPDN コマンドで定義された *list-name* と同一である必要があります。そうでない場合、アカウンティングは発生しません。
ステップ 4	Router(config)# **vpdn enable** 例： `Router(config)# vpdn enable`	ルータ上のバーチャル プライベート ダイヤルアップ ネットワーキングを有効にして、ルータにローカル データベースとリモート認可サーバー（該当する場合）上でトンネル定義を検索するように指示します。
ステップ 5	Router(config)# **vpdn tunnel accounting network** *list-name* 例： `Router(config)# vpdn tunnel accounting network m1`	Tunnel-Start、Tunnel-Stop、および Tunnel-Reject アカウンティング レコードを有効にします。 • *list-name* ：*list-name* は、**aaa accounting** コマンドで定義された *list-name* と一致している必要があります。そうでない場合、ネットワーク アカウンティングは発生しません。
ステップ 6	Router(config)# **vpdn session accounting network** *list-name* 例： `Router(config)# vpdn session accounting network m1`	Tunnel-Link-Start、Tunnel-Link-Stop、および Tunnel-Link-Reject アカウンティング レコードを有効にします。 • *list-name* ：*list-name* は、**aaa accounting** コマンドで定義された *list-name* と一致している必要があります。そうでない場合、ネットワーク アカウンティングは発生しません。

次の作業

RADIUS トンネル アカウンティングを有効にしたら、次のオプション タスク「RADIUS トンネル アカウンティングの確認」で設定を確認できます。

RADIUS トンネル アカウンティングの確認

次のオプション手順のどちらかまたは両方を使用して、RADIUS トンネルアカウンティング設定を確認します。

手順の概要

1. **enable**
2. Router# **show accounting**
3. Router# **show vpdn** [**session**] [**tunnel**]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	Router# **show accounting** 例： `Router# show accounting`	ネットワーク上でアクティブなアカウント可能イベントを表示して、アカウンティング サーバー上でのデータ消失イベント時の情報収集を支援します。
ステップ 3	Router# **show vpdn** [**session**] [**tunnel**] 例： 例： 例： 例： `Router# show vpdn session`	VPDN 内のアクティブな L2TP トンネルとメッセージ識別子に関する情報を表示します。 • **session** ：すべてのアクティブなトンネルのステータス サマリーを表示します。 • **tunnel** ：すべてのアクティブな L2TP トンネルに関する情報をサマリー形式で表示します。

RADIUS トンネル アカウンティングの設定例

LAC 上での RADIUS トンネル アカウンティングの設定例

次の例は、トンネル レコードと tunnel-link アカウンティング レコードを RADIUS サーバーに送信するように L2TP アクセス コンセントレータ（LAC）を設定する方法を示しています。

```
aaa new-model
!
!
aaa authentication ppp default group radius
aaa authorization network default local
aaa accounting network m1 start-stop group radius
aaa accounting network m2 stop-only group radius
aaa session-id common
enable secret 5 $1$IDjH$iL7puCja1RM1yOM.JAeuf/
enable password lab
!
username ISP_LAC password 0 tunnelpass
!
!
resource-pool disable
!
!
ip subnet-zero
ip cef
no ip domain-lookup
ip host dirt 172.16.1.129
!
vpdn enable
vpdn tunnel accounting network m1
vpdn session accounting network m1
vpdn search-order domain dnis
!
vpdn-group 1
 request-dialin
  protocol l2tp
  domain cisco.com
 initiate-to ip 10.1.26.71
 local name ISP_LAC
!
mta receive maximum-recipients 0
!
interface GigabitEthernet0/0/0
 ip address 10.1.27.74 255.255.255.0
 no ip mroute-cache
 duplex half
 speed auto
 no cdp enable
!
interface FastEthernet0/0/1
 no ip address
 no ip mroute-cache
 shutdown
 duplex auto
 speed auto
 no cdp enable
!
ip default-gateway 10.1.27.254
ip classless
ip route 0.0.0.0 0.0.0.0 10.1.27.254
no ip http server
ip pim bidir-enable
!
no cdp run
!
!
radius-server host 172.19.192.26 auth-port 1645 acct-port 1646 key rad123
radius-server retransmit 3
```

```
call rsvp-sync
!
```

LNS 上での RADIUS トンネル アカウンティングの設定例

次の例は、トンネル レコードと tunnel-link アカウンティング レコードを RADIUS サーバーに送信するように L2TP ネットワーク サーバー（LNS）を設定する方法を示しています。

```
aaa new-model
!
!
aaa accounting network m1 start-stop group radius
aaa accounting network m2 stop-only group radius
aaa session-id common
enable secret 5 $1$ftf.$wE6Q5Yv6hmQiwL9pizPCg1
!
username ENT_LNS password 0 tunnelpass
username user1@cisco.com password 0 lab
username user2@cisco.com password 0 lab
spe 1/0 1/7
 firmware location system:/ucode/mica_port_firmware
spe 2/0 2/9
 firmware location system:/ucode/mica_port_firmware
!
!
resource-pool disable
clock timezone est 2
!
ip subnet-zero
no ip domain-lookup
ip host CALLGEN-SECURITY-V2 172.24.80.28 10.47.0.0
ip host dirt 172.16.1.129
!
vpdn enable
vpdn tunnel accounting network m1
vpdn session accounting network m1
!
vpdn-group 1
accept-dialin
  protocol l2tp
  virtual-template 1
 terminate-from hostname ISP_LAC
 local name ENT_LNS
!
mta receive maximum-recipients 0
!
interface Loopback0
 ip address 192.168.70.101 255.255.255.0
!
interface Loopback1
 ip address 192.168.80.101 255.255.255.0
!
interface FastEthernet0/0/0
 ip address 10.1.26.71 255.255.255.0
 no ip mroute-cache
 no cdp enable
!
interface Virtual-Template1
 ip unnumbered Loopback0
 peer default ip address pool vpdn-pool1
 ppp authentication chap
```

```
!
interface Virtual-Template2
 ip unnumbered Loopback1
 peer default ip address pool vpdn-pool2
 ppp authentication chap
!
interface FastEthernet0/0/1
 no ip address
 no ip mroute-cache
 shutdown
 duplex auto
 speed auto
 no cdp enable
!
ip local pool vpdn-pool1 192.168.70.1 192.168.70.100
ip local pool vpdn-pool2 192.168.80.1 192.168.80.100
ip default-gateway 10.1.26.254
ip classless
ip route 0.0.0.0 0.0.0.0 10.1.26.254
ip route 10.90.1.2 255.255.255.255 10.1.26.254
no ip http server
ip pim bidir-enable
!
no cdp run
!
radius-server host 172.19.192.80 auth-port 1645 acct-port 1646 key rad123
radius-server retransmit 3
call rsvp-sync
```

その他の参考資料

次の項で、RFC-2867 RADIUS トンネル アカウンティングに関する参考資料を紹介します。

関連資料

関連項目	マニュアル タイトル
RADIUS 属性	『*Cisco IOS XE Security Configuration Guide: Securing User Services* , Release 2』の「RADIUS Attributes Overview and RADIUS IETF Attributes」
VPDN	『*Cisco IOS XE VPDN Configuration Guide* , Release 2』
ネットワーク アカウンティング	『*Cisco IOS XE Security Configuration Guide: Securing User Services* , Release 2』の「Configuring Accounting」
コマンド	• 『*Cisco IOS Security Command Reference*』 • 『*Cisco IOS VPDN Command Reference*』

標準

標準	タイトル
この機能でサポートされる新規の標準または変更された標準はありません。また、既存の標準のサポートは変更されていません。	--

MIB

MIB	MIB のリンク
この機能がサポートする新しいMIBまたは変更されたMIBはありません。また、この機能で変更された既存規格のサポートはありません。	選択したプラットフォーム、Cisco IOS XE ソフトウェア リリース、およびフィーチャ セットの MIB の場所を検索しダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

RFC

RFC	タイトル
RFC 2867	『*RADIUS Accounting Modifications for Tunnel Protocol Support*』

シスコのテクニカル サポート

説明	リンク
シスコのサポート Web サイトでは、シスコの製品やテクノロジーに関するトラブルシューティングにお役立ていただけるように、マニュアルやツールをはじめとする豊富なオンライン リソースを提供しています。 お使いの製品のセキュリティ情報や技術情報を入手するために、Cisco Notification Service（Field Notice からアクセス）、Cisco Technical Services Newsletter、Really Simple Syndication（RSS）フィードなどの各種サービスに加入できます。 シスコのサポート Web サイトのツールにアクセスする際は、Cisco.com のユーザ ID およびパスワードが必要です。	http://www.cisco.com/en/US/support/index.html

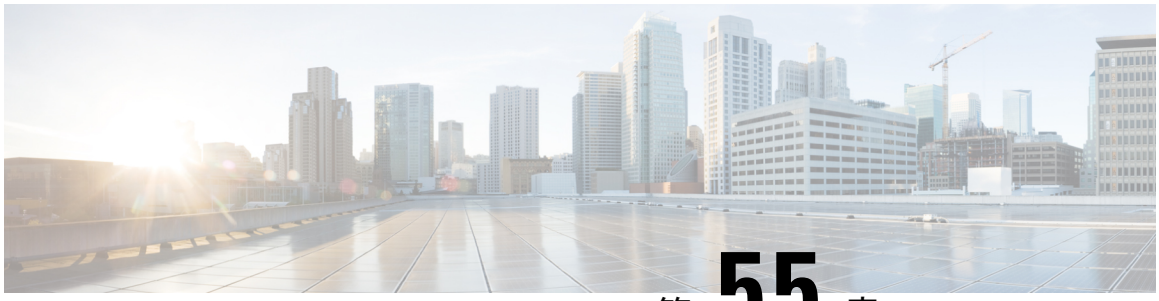
RFC-2867 RADIUS トンネル アカウンティングの機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *80 : RFC-2867 RADIUS* トンネル アカウンティングの機能情報

機能名	リリース	機能情報
RFC-2867 RADIUS トンネル アカウンティング	Cisco IOS XE Release 2.1	RFC-2867 RADIUS トンネル アカウンティングは、6 つの新しい RADIUS アカウンティング タイプを導入しています。これらのタイプは、アカウンティング要求がユーザー サービスの始まり（開始）と終わり（終了）のどちらを表しているかを示す、RADIUS アカウンティング属性の Acct-Status-Type（属性 40）と一緒に使用されます。 また、この機能は、ユーザーによる VPDN セッション イベントのトラブルシューティングを支援する 2 つの新しい仮想プライベート ダイヤルアップ ネットワーク（VPDN）コマンドを導入しています。 この機能は、Cisco IOS XE Release 2.1 で Cisco ASR 1000 シリーズ アグリゲーション サービス ルータに導入されました。 次のコマンドが導入または変更されました。**aaa accounting**、**vpdn session accounting network**、**vpdn tunnel accounting network**



第 55 章

RADIUS 論理回線 ID

論理回線 ID（LLID）ブロッキング機能としても知られる RADIUS 論理回線 ID 機能を使用すれば、管理者は、顧客コールが発信された物理回線に基づいて顧客を追跡できます。管理者は、顧客が物理回線を移動しても変化しない仮想ポートを使用します。この仮想ポートは、管理者の顧客プロファイルデータベースのメンテナンスを容易にし、管理者が顧客に対して追加のセキュリティ チェックを実施できるようにします。

RADIUS 論理回線 ID の前提条件

この機能は任意の RADIUS サーバーと一緒に使用できますが、RADIUS サーバーによっては、Access-Accept メッセージで Calling-Station-ID 属性を返せるようにディレクトリ ファイルを変更する必要があります。たとえば、「ATTRIBUTE Calling-Station-Id 31 string (*, *)」のようにディクショナリを変更しなければ、Merit RADIUS サーバーで LLID ダウンロードはサポートされません。

RADIUS 論理回線 ID の制約事項

RADIUS 論理回線 ID 機能は RADIUS のみをサポートしています。TACACS+ はサポートしていません。

この機能は、PPP over Ethernet over ATM（PPPoEoATM）コールと PPP over Ethernet over VLAN（PPPoEoVLAN）（Dot1Q）コールにしか適用できません。ISDN などのその他のコールは使用できません。

RADIUS 論理回線 ID に関する情報

事前認可

LLID は、加入者線の論理識別を表す英数字文字列です（1 ～ 253 文字にする必要があります）。また、LLID は、RADIUS サーバー上の顧客プロファイル データベース上に保存されます。顧客プロファイルデータベースがアクセスルータから事前認可要求を受け取ると、RADIUS サーバーが LLID を Calling-Station-ID 属性（属性 31）としてルータに送信します。

レイヤ 2 トンネリング プロトコル（L2TP）アクセス コンセントレータ（LAC）が、事前認可用に設定されている場合に、事前認可要求を顧客プロファイル データベースに送信します。**subscriber access** コマンドを使用して、LAC を事前認可用に設定します。

（注） LLID のダウンロードは「事前認可」と呼ばれています。これは、サービス（ドメイン）認可またはユーザー認証および認可の前に実施されるためです。

RADIUS サーバー上の顧客プロファイルデータベースは、ルータに接続された物理ネットワーク アクセス サーバー（NAS）ごとのユーザー プロファイルで構成されています。各ユーザー プロファイルには、ルータ上の物理ポートを表すユーザー名（属性 1）と一致したプロファイルが格納されています。ルータは、事前認可用に設定されている場合に、接続先の物理 NAS ポートの代表ユーザー名を使用して顧客プロファイルデータベースに問い合わせます。顧客プロファイルデータベース内で一致するものが見つかると、顧客プロファイルデータベースが、ユーザー プロファイル内の LLID を含む Access-Accept メッセージを返します。LLID は、Calling-Station-ID 属性として Access-Accept レコード内に定義されています。

事前認可プロセスは、認証に使用される実際のユーザー名を RADIUS サーバーに提供することもできます。物理 NAS ポート情報がユーザー名（属性 1）として使用されるため、RADIUS 属性 77（Connect-Info）を認証ユーザー名を含めるように設定できます。この設定によって、RADIUS サーバーは、LLID をルータに返す前に、選択した認可要求に対して追加の検証（プライバシー ルールに対するユーザー名の分析など）を実施できます。

RADIUS 論理回線 ID の設定方法

事前認可の設定

LLID をダウンロードして、LAC を事前認可用に設定するには、次の手順を実行します。

手順の概要

1. **enable**
2. **configure terminal**

3. **ip radius source-interface** *interface-name*
4. **subscriber access** {**pppoe** | **pppoa**} **pre-authorize nas-port-id** [**default** | *list-name*] [**send username**]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ip radius source-interface** *interface-name* 例： 例： `Router (config)# ip radius source-interface Loopback1`	事前認可要求用のユーザー名の IP アドレス部分を指定します。
ステップ 4	**subscriber access** {**pppoe**	**pppoa**} **pre-authorize nas-port-id** [**default**	*list-name*] [**send username**] 例： 例： `Router (config)# subscriber access pppoe pre-authorize nas-port-id mlist_llid send username`	LLID のダウンロードを可能にして、ルータを事前認可用に設定できるようにします。 **send username** オプションは、Access-Request メッセージ内の Connect-Info（属性 77）にセッションの認証ユーザー名を含めるように指定します。

RADIUS ユーザー プロファイル内の LLID の設定

ユーザー プロファイルを事前認可用に設定するには、顧客プロファイル データベースに NAS ポート ユーザーを追加して、ユーザー プロファイルに RADIUS インターネット技術特別調査委員会（IETF）属性 31（Calling-Station-ID）を追加します。

手順の概要

1. UserName=nas_port: ip-address:slot/module/port/vpi.vci
2. User-Name=nas-port: ip-address:slot/module/port/vlan-id
3. Calling-Station-Id = “string (*,*)”

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	UserName=nas_port: ip-address:slot/module/port/vpi.vci	（任意）PPPoE over ATM NAS ポート ユーザーを追加します。
ステップ 2	User-Name=nas-port: ip-address:slot/module/port/vlan-id	（任意）PPPoE over VLAN NAS ポート ユーザーを追加します。
ステップ 3	Calling-Station-Id = “string (*,*)”	ユーザー プロファイルに属性 31 を追加します。 • String：ユーザーがかけてきた電話番号を含む 1 つ以上のオクテット。

論理回線 ID の確認

機能を確認するには、次の手順を実行します。

手順の概要

1. **enable**
2. **debug radius**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**debug radius** 例： `Router# debug radius`	RADIUS 属性 31 が、LAC 上の Accounting-Request と、LNS 上の Access-Request および Accounting-Request 内の LLID であることを確認します。

RADIUS 論理回線 ID の設定例

事前認可用の LAC 設定例

次の例は、LLID をダウンロードすることによって、LAC を事前認可用に設定する方法を示しています。

```
aaa new-model
aaa group server radius sg_llid
 server 172.31.164.106 auth-port 1645 acct-port 1646
aaa group server radius sg_water
 server 172.31.164.106 auth-port 1645 acct-port 1646
aaa authentication ppp default group radius
aaa authorization confg-commands
aaa authorization network default group sg_water
aaa authorization network mlist_llid group sg_llid
aaa session-id common
!
username s7200_2 password 0 lab
username s5300 password 0 lab
username sg_water password 0 lab
vpdn enable
!
vpdn-group 2
 request-dialin
 protocol l2tp
 domain example.com
 domain example.com#184
 initiate-to ip 10.1.1.1
 local name s7200_2
 l2tp attribute clid mask-method right * 255 match #184
!
vpdn-group 3
 accept dialin
  protocol pppoe
  virtual-template 1
!
!
Enable the LLID to be downloaded.
subscriber access pppoe pre-authorize nas-port-id mlist_llid send username
!
interface Loopback0
 ip address 10.1.1.2 255.255.255.0
!
interface Loopback1
 ip address 10.1.1.1 255.255.255.0
!
interface FastEthernet1/0/0
 ip address 10.1.1.8 255.255.255.0 secondary
 ip address 10.0.58.111 255.255.255.0
 no cdp enable
!
interface ATM4/0/0
 no ip address
 no atm ilmi-keepalive
!
interface ATM4/0/0.1 point-to-point
 pvc 1/100
```

```
  encapsulation aa15snap
  protocol pppoe
!
interface virtual-template1
 no ip unnumbered Loopback0
 no peer default ip address
 ppp authentication chap
!
radius-server host 172.31.164.120 auth-port 1645 acct-port 1646 key rad123
radius-server host 172.31.164.106 auth-port 1645 acct-port 1646 key rad123
ip radius source-interface Loopback1
```

LLID 用の RADIUS ユーザー プロファイルの例

次の例は、ユーザー プロファイルを PPPoEoVLAN および PPPoEoATM に対する LLID 問い合わせ用に設定する方法と属性 31 の追加方法を示しています。

```
pppoeovlan
----------
nas-port:10.1.0.3:6/0/0/0    Password = "password1",
    Service-Type = Outbound,
    Calling-Station-ID = "cat-example"
pppoeoa
--------
nas-port:10.1.0.3:6/0/0/1.100    Password = "password1",
    Service-Type = Outbound,
    Calling-Station-ID = "cat-example"
```

その他の参考資料

次の項で、RADIUS EAP サポート機能に関する参考資料を紹介します。

関連資料

関連項目	マニュアル タイトル
AAA を使用した ppp 認証の設定	「Configuring Authentication」モジュール。
RADIUS の設定	「Configuring RADIUS」モジュール。
PPP の設定	「Configuring Asynchronous SLIP and PPP」モジュール。
ダイヤル テクノロジー コマンド	『*Cisco IOS Dial Technologies Command Reference*』
セキュリティ コマンド	『*Cisco IOS Security Command Reference*』

標準

標準	タイトル
なし	--

MIB

MIB	MIB のリンク
なし	選択したプラットフォーム、Cisco IOS リリース、およびフィーチャ セットに関する MIB を探してダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

RFC

RFC	タイトル
RFC 2284	『*PPP Extensible Authentication Protocol (EAP)*』
RFC 1938	『*A One-Time Password System*』
RFC 2869	『*RADIUS Extensions*』

シスコのテクニカル サポート

説明	リンク
シスコのサポート Web サイトでは、シスコの製品やテクノロジーに関するトラブルシューティングにお役立ていただけるように、マニュアルやツールをはじめとする豊富なオンライン リソースを提供しています。 お使いの製品のセキュリティ情報や技術情報を入手するために、Cisco Notification Service（Field Notice からアクセス）、Cisco Technical Services Newsletter、Really Simple Syndication（RSS）フィードなどの各種サービスに加入できます。 シスコのサポート Web サイトのツールにアクセスする際は、Cisco.com のユーザ ID およびパスワードが必要です。	http://www.cisco.com/en/US/support/index.html

RADIUS 論理回線 ID の機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *81 : RADIUS* 論理回線 *ID* の機能情報

機能名	リリース	機能情報
RADIUS 論理回線 ID	Cisco IOS XE Release 2.1	論理回線 ID（LLID）ブロッキング機能としても知られる RADIUS 論理回線 ID 機能を使用すれば、管理者は、顧客コールが発信された物理回線に基づいて顧客を追跡できます。 この機能は、Cisco IOS XE Release 2.1 で、Cisco ASR 1000 シリーズ アグリゲーション サービス ルータに導入されました。 この機能により、次のコマンドが導入または変更されました。**subscriber access**
発信側ステーション ID 属性 31	Cisco IOS XE Release 2.1	この機能は、Cisco ASR 1000 シリーズ ルータに追加されました。
LLID ブロッキング	Cisco IOS XE Release 2.1	この機能は、Cisco ASR 1000 シリーズ ルータに追加されました。

用語集

attribute ：RADIUS Internet Engineering Task Force（IETF）属性は、クライアントとサーバーの間で認証、認可、およびアカウンティング（AAA）情報を通信するために使用される 255 個の標準属性からなるオリジナル セットの 1 つです。IETF 属性は標準であるため、属性データは事前定義されてその内容も認識されています。このため、IETF 属性を介して AAA 情報を交換するすべてのクライアントとサーバーは、属性の厳密な意味や各属性値の一般的な限界などの属性データを一致させる必要があります。

CHAP ：チャレンジ ハンドシェイク認証プロトコル。PPP カプセル化を使用した回線上でサポートされ、不正アクセスを防止するセキュリティ機能。CHAPそれ自体が不正アクセスを防止するわけではなく、単に、リモートエンドを識別するだけです。その後で、ルータまたはアクセス サーバーがそのユーザーのアクセスを許可するかどうかを決定します。

EAP ：拡張認証プロトコル。認証フェーズ（Link Control Protocol（LCP）フェーズではなく）でネゴシエートされる複数の認証メカニズムをサポートする PPP 認証プロトコル。EAP を使用すれば、汎用のインターフェイスを介して、サードパーティ製の認証サーバーと PPP 実装の間でデータのやり取りができます。

LCP ：リンク制御プロトコル。PPP で使用するためのデータ リンク接続を確立して、設定し、テストするプロトコル。

MD5 (HMAC variant) ：Message Digest 5。パケット データの認証に使用するハッシュ アルゴリズム。HMAC は、メッセージ認証用の重要なハッシングです。

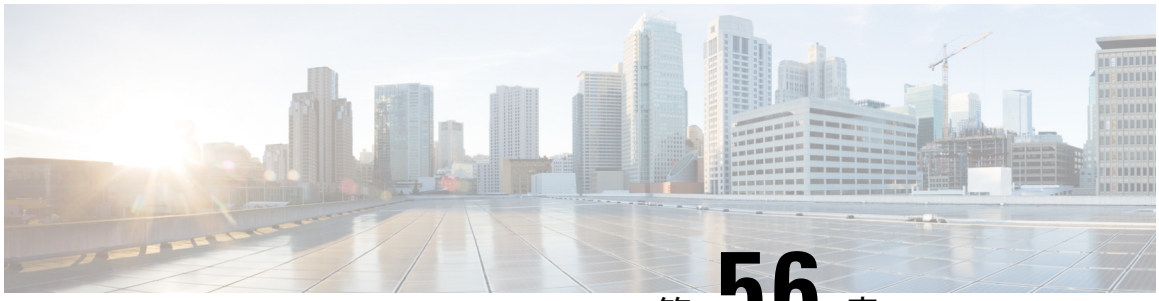
NAS ：ネットワーク アクセス サーバー。公衆電話交換網（PSTN）などのリモート アクセス ネットワーク上でユーザーにローカル ネットワーク アクセスを提供するデバイス。

PAP ：パスワード認証プロトコル。PPP ピアの相互認証を可能にする認証プロトコル。ローカル ルータに接続を試みているリモート ルータは、認証要求を送信するように要求されます。CHAP と違って、PAP はパスワードとホスト名またはユーザー名をクリア テキスト（暗号化なし）で渡します。PAP それ自体が不正アクセスを防止するわけではなく、単に、リモート エンドを識別するだけです。ルータまたはアクセス サーバーがそのユーザーのアクセスを許可するかどうかを決定します。PAP は、PPP 回線上でのみサポートされます。

PPP ：ポイントツーポイント プロトコル。ポイントツーポイント リンク上でネットワーク層プロトコル情報をカプセル化するプロトコル。PPP は RFC 1661 で規定されています。

RADIUS ：リモート認証ダイヤルイン ユーザー サービス。モデムおよび ISDN 接続の認証、および接続のトラッキングのためのデータベースです。

このマニュアルで使用している IP アドレスおよび電話番号は、実際のアドレスおよび電話番号を示すものではありません。マニュアル内の例、コマンド出力、ネットワークトポロジ図、およびその他の図は、説明のみを目的として使用されています。説明の中に実際のアドレスおよび電話番号が使用されていたとしても、それは意図的なものではなく、偶然の一致によるものです。



第 56 章

RADIUS ルート ダウンロード

RADIUS ルート ダウンロード機能を使用すれば、RADIUS 認可を転送するようにネットワーク アクセス サーバー（NAS）を設定できます。

RADIUS ルート ダウンロードの前提条件

この機能でタスクを実行する前に、AAA ネットワーク セキュリティを有効にする必要があります。

RADIUS ルート ダウンロードに関する情報

RADIUS ルート ダウンロード機能を使用すれば、RADIUS 認可を転送するようにネットワーク アクセス サーバー（NAS）を設定できます。ユーザーは、NAS から認証、許可、アカウンティング（AAA）に送信されるスタティック ルート ダウンロード要求用として、もう一つの名前付き方式リスト（デフォルトの方式リストに加えて）を設定できます。

この機能以前は、スタティック ルート ダウンロード要求用の RADIUS 認可が、デフォルトの方式リストで指定された AAA サーバーにのみ送信されていました。

この機能では、AAA サーバーへのスタティック ルート ダウンロード要求の転送に使用される方式リストの名前を指定できるように **aaa route download** コマンドの機能が拡張されています。**aaa route download** コマンドは、スタティック ルートをダウンロードするためのもう 1 つの方式リストを指定するために使用できます。この方式リストは、**aaa authorization configuration** コマンドを使用して追加できます。

RADIUS ルート ダウンロードの設定方法

RADIUS ルート ダウンロードの設定

名前付き方式リストで指定されたサーバーにスタティック ルート ダウンロード要求を送信するようにNASを設定するには、グローバル コンフィギュレーション モードで次のコマンドを使用します。

手順の概要

1. Router(config)# **aaa authorization configuration** *method-name* **[radius | tacacs+ | group** *group-name* **]**
2. Router(config)# **aaa route download** [*time*] [**authorization** *method-list*]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	Router(config)# **aaa authorization configuration** *method-name* **[radius | tacacs+ | group** *group-name* **]**	RADIUS を使用して AAA サーバーからスタティック ルート設定情報をダウンロードします。
ステップ 2	Router(config)# **aaa route download** [*time*] [**authorization** *method-list*]	スタティック ルート ダウンロード機能を有効にします。**authorization** *method-list* 属性を使用して、スタティック ルート ダウンロード用の RADIUS 認可要求が送信される名前付き方式リストを指定します。

RADIUS ルート ダウンロードの確認

インストールされているルートを確認するには、EXEC モードで **show ip route** コマンドを使用します。

RADIUS に関連付けられた情報を表示するには、特権 EXEC モードで **debug radius** コマンドを使用します。

RADIUS ルート ダウンロードの設定例

RADIUS ルート ダウンロード設定例

次の例は、スタティック ルート ダウンロード要求を「list1」という名前の方式リストで指定されたサーバーに送信するように NAS を設定する方法を示しています。

```
aaa new-model
aaa group server radius rad1
server 10.2.2.2 auth-port 1645 acct-port 1646
!
aaa group server tacacs+ tac1
server 172.17.3.3
!
aaa authorization configuration default group radius
aaa authorization configuration list1 group rad1 group tac1
aaa route download 1 authorization list1
tacacs-server host 172.17.3.3
tacacs-server key cisco
tacacs-server administration
!
radius-server host 10.2.2.2 auth-port 1645 acct-port 1646
radius-server key cisco
```

その他の参考資料

次の項で、RADIUS ルート ダウンロードに関する参考資料を紹介します。

関連資料

関連項目	マニュアル タイトル
セキュリティ コマンド	『*Cisco IOS Security Command Reference*』

標準

標準	タイトル
この機能でサポートされる新規の標準または変更された標準はありません。また、既存の標準のサポートは変更されていません。	--

MIB

MIB	MIB のリンク
この機能によってサポートされる新しい MIB または変更された MIB はありません。またこの機能による既存 MIB のサポートに変更はありません。	選択したプラットフォーム、Cisco IOS XE ソフトウェア リリース、およびフィーチャ セットの MIB の場所を検索しダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

RFC

RFC	タイトル
この機能によりサポートされた新規 RFC または改訂 RFC はありません。またこの機能による既存 RFC のサポートに変更はありません。	--

シスコのテクニカル サポート

説明	リンク
シスコのサポート Web サイトでは、シスコの製品やテクノロジーに関するトラブルシューティングにお役立ていただけるように、マニュアルやツールをはじめとする豊富なオンライン リソースを提供しています。 お使いの製品のセキュリティ情報や技術情報を入手するために、Cisco Notification Service（Field Notice からアクセス）、Cisco Technical Services Newsletter、Really Simple Syndication（RSS）フィードなどの各種サービスに加入できます。 シスコのサポート Web サイトのツールにアクセスする際は、Cisco.com のユーザ ID およびパスワードが必要です。	http://www.cisco.com/en/US/support/index.html

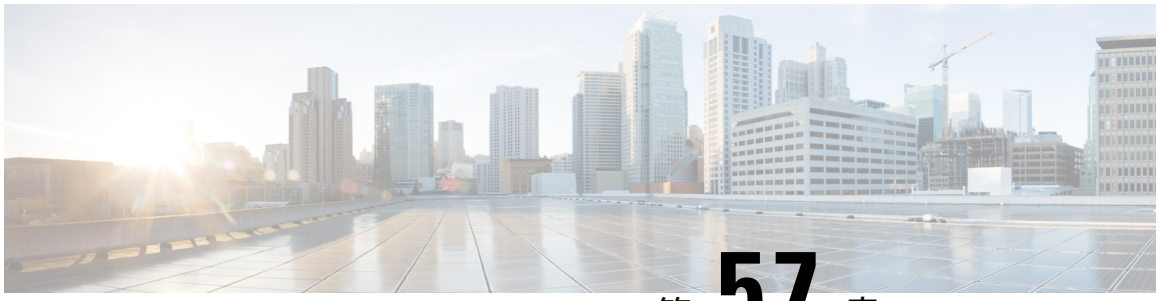
RADIUS ルート ダウンロードの機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *82 : RADIUS* ルート ダウンロードの機能情報

機能名	リリース	機能情報
RADIUS ルート ダウンロード	Cisco IOS XE Release 2.1	RADIUS ルート ダウンロード機能を使用すれば、RADIUS 認可を転送するようにネットワーク アクセス サーバー（NAS）を設定できます。ユーザーは、NAS から認証、許可、アカウンティング（AAA）に送信されるスタティック ルート ダウンロード要求用として、もう一つの名前付き方式リスト（デフォルトの方式リストに加えて）を設定できます。 この機能は、Cisco IOS XE Release 2.1 で、Cisco ASR 1000 シリーズアグリゲーション サービス ルータに導入されました。 次のコマンドが導入されました。 **aaa route download**



第 57 章

RADIUS サーバ ロード バランシング

RADIUS サーバー ロード バランシング機能は、認証、認可、およびアカウンティング（AAA）の認証トランザクションとアカウンティング トランザクションをサーバー グループ内の RADIUS サーバーに分配します。これらのサーバーは、AAA トランザクションの負荷を共有することで、着信要求に迅速に応答できるようになります。

このモジュールでは、RADIUS サーバー ロード バランシング機能について説明します。

RADIUS サーバ ロード バランシングの前提条件

- 認証、認可、およびアカウンティング（AAA）を RADIUS サーバーに設定する必要があります。
- AAA RADIUS サーバー グループを設定する必要があります。
- 認証、アカウンティング、スタティック ルート ダウンロードなどの機能用に RADIUS を設定する必要があります。

RADIUS サーバ ロード バランシングの制約事項

- パケット オブ ディスコネクト（POD）要求などの着信 RADIUS 要求はサポートされていません。

RADIUS サーバ ロード バランシングに関する情報

RADIUS サーバ ロード バランシングの概要

ロードバランシングは、トランザクションのバッチをサーバー グループ内のRADIUSサーバーに分配します。ロードバランシングにより、トランザクションの各バッチは、キュー内の未処理トランザクション数が最も少ないサーバーに割り当てられます。トランザクションのバッチの割り当てプロセスは次のとおりです。

1. 最初のトランザクションが新しいバッチとして受信されます。
2. すべてのサーバー トランザクション キューがチェックされます。
3. 最小番号の未処理トランザクションを持つサーバーが特定されます。
4. 特定されたサーバーが、トランザクションの次のバッチに割り当てられます。

バッチ サイズはユーザー設定のパラメータです。バッチ サイズを変更すると、CPU の負荷やネットワークのスループットに影響する可能性があります。バッチサイズが大きくなるほど、CPU の負荷が減少し、ネットワークのスループットが増加します。ただし、バッチ サイズが大きくても、使用可能なすべてのサーバー リソースが使い果たされることはありません。バッチ サイズが小さくなるほど、CPU の負荷が増加し、ネットワークのスループットが減少します。

（注） 大きなバッチ サイズまたは小さなバッチ サイズに関する設定数はありません。50 を超えるトランザクションを含むバッチは大きいと見なされ、25 より少ないトランザクションを含むバッチは、小さいと見なされます。

（注） サーバー グループに 10 以上のサーバーが含まれている場合、CPU の負荷を軽減するために高いバッチ サイズを設定することを推奨します。

RADIUS サーバ グループ全体のトランザクションのロード バランシング

名前付き RADIUS サーバー グループごとに、またはグローバル RADIUS サーバー グループに対してロード バランシングを設定できます。ロード バランシング サーバー グループは、認証、認可、およびアカウンティング（AAA）方式リストで「radius」として参照される必要があります。RADIUS サーバー グループの一部であるすべてのパブリック サーバーは、その後、ロード バランシングされます。

同じRADIUSサーバーを使用するか、または別のサーバーを使用するように認証およびアカウンティングを設定できます。1 つのサーバーをセッションの事前認証、認証、またはアカウンティング トランザクションに使用することもできます。内部設定であり、デフォルトとして設定される優先サーバーが、サーバー コストに関係なく、セッションの開始レコードと終了レコードに対して同じサーバーを使用するよう AAA に指示します。優先サーバー設定を使用する場合は、初期トランザクション（認証など）に使用されるサーバー、つまり優先サーバーが、以降のトランザクション（アカウンティングなど）に使用される他のサーバー グループにも属するようにします。

優先サーバーは、次のいずれかの条件が真である場合は使用されません。

- **load-balance method least-outstanding ignore-preferred-server** コマンドが使用されている。
- 優先サーバーが停止中である。
- 優先サーバーが隔離中である。
- 必要サーバー フラグがセットされている場合は、優先サーバー設定が無効になります。

内部設定である必要サーバー フラグは、サーバー コストに関係なく、マルチステージ トランザクションのすべてのステージに対して同じサーバーを使用する必要がある場合に使用されます。必要サーバーが使用できない場合は、トランザクションが失敗します。

次のいずれかの設定がある場合、**load-balance method least-outstanding ignore-preferred-server** コマンドを使用できます。

- 専用の認証サーバーと別の専用のアカウンティング サーバー
- 開始レコードと終了レコード、および別のサーバーに保存されたレコードなど、すべての通話レコード統計情報と通話レコード詳細を追跡可能なネットワーク

認証サーバーをアカウンティング サーバーのスーパーセットとして設定している場合、優先サーバーは使用されません。

RADIUS サーバー ステータスと自動テスト

RADIUS サーバー ロード バランシング機能では、バッチを割り当てるときにサーバー ステータスを考慮します。トランザクションのバッチは、稼働中のサーバーのみに送信されます。あまり使用されていないサーバー（バックアップ サーバーなど）を含む、すべてのRADIUSロード バランシング サーバーのステータスをテストすることを推奨します。

停止中としてマークされたサーバーにはトランザクションが送信されません。隔離状態になったサーバーは、タイマーが切れるまで停止中としてマークされます。RADIUS自動テスタ機能によって動作中であることが確認されるまでサーバーは隔離中になります。

サーバーが稼働中でトランザクションを処理できるかどうかを確認するために、RADIUS自動テスターは、テスト ユーザー ID で要求を定期的にサーバーに送信します。サーバーがAccess-Rejectメッセージを返した場合、サーバーは稼働中です。それ以外の場合、サーバーは停止中または隔離中です。

未応答のサーバーに送信されたトランザクションは、未応答のサーバーが停止中としてマークされる前に、次の使用可能なサーバーにフェールオーバーされます。失敗したトランザクションには再試行順序変更モードを使用することを推奨します。

RADIUS 自動テスターを使用する場合、認証、認可、およびアカウンティング（AAA）サーバーが、ネットワーク アクセス サーバー（NAS）によって送信されるテスト パケットに応答していることを確認します。サーバーが正しく設定されていない場合は、パケットが破棄され、サーバーが誤って停止中としてマークされる可能性があります。

注意 RADIUS サーバー上で定義されていないテスト ユーザーを RADIUS サーバー自動テストに使用して、テストユーザーが正しく設定されていない場合に発生するセキュリティ上の問題を解決することを推奨します。

（注） ロード バランシング トランザクションを確認するには、**test aaa group** コマンドを使用します。

（注） Cisco IOS XE Bengaluru 17.4.1 以降では、VRF を認識するように自動テスターを設定できます。**automate-tester** コマンドで **vrf** キーワードを使用すると、デフォルト以外の VRF の自動テスト機能を有効化します。

VRF 対応の自動テスターを機能させるには、**global config ipv4/ipv6 source interface** *interface-name* **vrf** *vrf-name* コマンドを設定する必要があります。

RADIUS サーバ ロード バランシングの設定方法

名前付き RADIUS サーバ グループのロード バランシングの有効化

手順の概要

1. **enable**
2. **configure terminal**
3. **aaa group server radius** *group-name*
4. **server ip-address [auth-port port-number] [acct-port port-number]**
5. **load-balance method least-outstanding** [**batch-size** *number*] [**ignore-preferred-server**]
6. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**aaa group server radius** *group-name* 例： `Device(config)# aaa group server radius rad-sg`	サーバー グループ コンフィギュレーション モードに入ります。
ステップ 4	**server ip-address [auth-port port-number] [acct-port port-number]** 例： `Device (config-sg-radius)server 192.0.2.238 auth-port 2095 acct-port 2096`	グループ サーバー用の RADIUS サーバーの IP アドレスを設定します。
ステップ 5	**load-balance method least-outstanding** [**batch-size** *number*] [**ignore-preferred-server**] 例： `Device(config-sg-radius)# load-balance method least-outstanding batch-size 30`	名前付きサーバー グループに対して最小未処理ロード バランシングを有効にします。
ステップ 6	**end** 例： `Device(config-sg)# end`	サーバー グループ コンフィギュレーション モードを終了し、特権 EXEC モードを開始します。

グローバル RADIUS サーバー グループのロード バランシングの有効化

グローバル RADIUS サーバー グループは、認証、認可、およびアカウンティング（AAA）方式リストで「radius」として参照されます。

手順の概要

1. **enable**
2. **configure terminal**
3. **radius-server host** {*hostname* | *ip-address*} [**test username** *name*] [**auth-port** *number*] [**ignore-auth-port**] [**acct-port** *number*] [**ignore-acct-port**] [**idle-time** *seconds*]
4. **radius-server load-balance method least-outstanding** [**batch-size** *number*] [**ignore-preferred-server**]
5. **load-balance method least-outstanding** [**batch-size** *number*] [**ignore-preferred-server**]

6. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**radius-server host** {*hostname* | *ip-address*} [**test username** *name*] [**auth-port** *number*] [**ignore-auth-port**] [**acct-port** *number*] [**ignore-acct-port**] [**idle-time** *seconds*] 例： `Device(config)# radius-server host 192.0.2.1 test username test1 idle-time 1`	RADIUS 自動テストを有効にします。
ステップ 4	**radius-server load-balance method least-outstanding** [**batch-size** *number*] [**ignore-preferred-server**] 例： `Device(config)# radius-server load-balance method least-outstanding`	グローバル RADIUS サーバー グループに対して最小未処理ロードバランシングを有効にし、サーバー グループ コンフィギュレーション モードを開始します。 • デフォルトのバッチ サイズは 25 です。バッチ サイズの範囲は 1 ～ 2147483647 です。
ステップ 5	**load-balance method least-outstanding** [**batch-size** *number*] [**ignore-preferred-server**] 例： `Device(config-sg)# load-balance method least-outstanding batch-size 5`	グローバル名前付きサーバー グループに対して最小未処理ロード バランシングを有効にします。
ステップ 6	**end** 例： `Device(config-sg)# end`	サーバー グループ コンフィギュレーション モードを終了し、特権 EXEC モードを開始します。

RADIUS サーバ ロード バランシングのトラブルシューティング

RADIUS サーバー ロード バランシング機能を設定した後は、アイドル タイマー、デッド タイマー、ロード バランシング サーバーの選択をモニターしたり、手動テスト コマンドを使用してサーバー ステータスを確認したりできます。

手順の概要

1. **debug aaa test** コマンドを使用して、アイドル タイマーやデッド タイマーが期限切れになった日時、テスト パケットが送信された日時、およびサーバー ステータスを特定し、サーバーの状態を確認します。
2. **debug aaa sg-server selection** コマンドを使用して、ロード バランシング用に選択されたサーバーを特定します。
3. **test aaa group** コマンドを使用して、RADIUS ロード バランシング サーバーのステータスを手動で確認します。

手順の詳細

ステップ 1 **debug aaa test** コマンドを使用して、アイドル タイマーやデッド タイマーが期限切れになった日時、テスト パケットが送信された日時、およびサーバー ステータスを特定し、サーバーの状態を確認します。

アイドル タイマーは、サーバー ステータスのチェックに使用され、着信要求の有無に関係なく更新されます。アイドル タイマーをモニターすると、未応答のサーバーが存在するかどうかを判断し、RADIUS サーバーのステータスを最新の状態に保つことができるため、利用可能なリソースを効率的に利用できます。たとえば、アイドル タイマーが更新されていれば、着信要求が動作中のサーバーに送信されていることを簡単に確認できます。

デッド タイマーは、サーバーが停止中であることを特定したり、停止中のサーバーのステータスを適切に更新したりするために使用します。

サーバの選択をモニタすると、サーバの選択が変更される頻度を特定するのに役立ちます。サーバの選択は、ボトルネック、つまり、キュー内に大量の要求が存在するかどうかや、特定のサーバのみが着信要求を処理しているかどうかを分析するのに有効です。

debug aaa test コマンドの次のサンプル出力は、アイドル タイマーが期限切れになった日時を示しています。

例：

```
Device# debug aaa test

Jul 16 00:07:01: AAA/SG/TEST: Server (192.0.2.245:1700,1701) quarantined.
Jul 16 00:07:01: AAA/SG/TEST: Sending test request(s) to server (192.0.2.245:1700,1701)
Jul 16 00:07:01: AAA/SG/TEST: Sending 1 Access-Requests, 1 Accounting-Requests in current batch.
Jul 16 00:07:01: AAA/SG/TEST(Req#: 1): Sending test AAA Access-Request.
Jul 16 00:07:01: AAA/SG/TEST(Req#: 1): Sending test AAA Accounting-Request.
Jul 16 00:07:01: AAA/SG/TEST: Obtained Test response from server (192.0.2.245:1700,1701)
Jul 16 00:07:01: AAA/SG/TEST: Obtained Test response from server (192.0.2.245:1700,1701)
Jul 16 00:07:01: AAA/SG/TEST: Necessary responses received from server (192.0.2.245:1700,1701)
Jul 16 00:07:01: AAA/SG/TEST: Server (192.0.2.245:1700,1701) marked ALIVE. Idle timer set for 60
sec(s).
Jul 16 00:07:01: AAA/SG/TEST: Server (192.0.2.245:1700,1701) removed from quarantine.
```

ステップ 2 **debug aaa sg-server selection** コマンドを使用して、ロード バランシング用に選択されたサーバーを特定します。

debug aaa sg-server selection コマンドの次のサンプル出力は、5 つのアクセス要求がバッチ サイズ 3 のサーバー グループに送信されていることを示しています。

例：

```
Device# debug aaa sg-server selection

Jul 16 03:15:05: AAA/SG/SERVER_SELECT: Obtaining least loaded server.
Jul 16 03:15:05: AAA/SG/SERVER_SELECT: [3] transactions remaining in batch. Reusing server.
Jul 16 03:15:05: AAA/SG/SERVER_SELECT: Obtaining least loaded server.
Jul 16 03:15:05: AAA/SG/SERVER_SELECT: [2] transactions remaining in batch. Reusing server.
Jul 16 03:15:05: AAA/SG/SERVER_SELECT: Obtaining least loaded server.
Jul 16 03:15:05: AAA/SG/SERVER_SELECT: [1] transactions remaining in batch. Reusing server.
Jul 16 03:15:05: AAA/SG/SERVER_SELECT: Obtaining least loaded server.
Jul 16 03:15:05: AAA/SG/SERVER_SELECT: No more transactions in batch. Obtaining a new server.
Jul 16 03:15:05: AAA/SG/SERVER_SELECT: Obtaining a new least loaded server.
Jul 16 03:15:05: AAA/SG/SERVER_SELECT: Server[0] load: 3
Jul 16 03:15:05: AAA/SG/SERVER_SELECT: Server[1] load: 0
Jul 16 03:15:05: AAA/SG/SERVER_SELECT: Server[2] load: 0
Jul 16 03:15:05: AAA/SG/SERVER_SELECT: Selected Server[1] with load 0
Jul 16 03:15:05: AAA/SG/SERVER_SELECT: [3] transactions remaining in batch.
Jul 16 03:15:05: AAA/SG/SERVER_SELECT: Obtaining least loaded server.
Jul 16 03:15:05: AAA/SG/SERVER_SELECT: [2] transactions remaining in batch. Reusing server.
```

ステップ 3 **test aaa group** コマンドを使用して、RADIUS ロード バランシング サーバーのステータスを手動で確認します。

次のサンプル出力は、ユーザー名「test」がユーザー プロファイルと一致しない場合の動作中の RADIUS ロード バランシング サーバーからの応答を示しています。**test aaa group** コマンドを使用して生成された認証、認可、およびアカウンティング（AAA）パケットに対し、サーバーが Access-Reject 応答を発行する場合、そのサーバーは動作中であることが確認されます。

例：

```
Device# test aaa group SG1 test lab new-code

00:06:07: RADIUS/ENCODE(00000000):Orig. component type = INVALID
00:06:07: RADIUS/ENCODE(00000000): dropping service type, "radius-server attribute 6 on-for-login-auth"
 is off
00:06:07: RADIUS(00000000): Config NAS IP: 192.0.2.4
00:06:07: RADIUS(00000000): sending
00:06:07: RADIUS/ENCODE: Best Local IP-Address 192.0.2.141 for Radius-Server 192.0.2.176
00:06:07: RADIUS(00000000): Send Access-Request to 192.0.2.176:1645 id 1645/1, len 50
00:06:07: RADIUS:  authenticator CA DB F4 9B 7B 66 C8 A9 - D1 99 4E 8E A4 46 99 B4
00:06:07: RADIUS:  User-Password       [2]   18  *
00:06:07: RADIUS:  User-Name           [1]   6   "test"
00:06:07: RADIUS:  NAS-IP-Address      [4]   6   192.0.2.141
00:06:07: RADIUS: Received from id 1645/1 192.0.2.176:1645, Access-Reject, len 44
00:06:07: RADIUS:  authenticator 2F 69 84 3E F0 4E F1 62 - AB B8 75 5B 38 82 49 C3
00:06:07: RADIUS:  Reply-Message       [18]  24
00:06:07: RADIUS:   41 75 74 68 65 6E 74 69 63 61 74 69 6F 6E 20 66  [Authentication f]
00:06:07: RADIUS:   61 69 6C 75 72 65                               [failure]
00:06:07: RADIUS(00000000): Received from id 1645/1
00:06:07: RADIUS/DECODE: Reply-Message fragments, 22, total 22 bytes
```

RADIUS サーバ ロード バランシングの設定例

例：グローバル RADIUS サーバー グループのロード バランシングの有効化

次の例は、グローバル RADIUS サーバー グループのロード バランシングを有効化する方法を示しています。これらの例は、RADIUS コマンド出力の現在の設定、デバッグ出力、認証、認可、およびアカウンティング（AAA）サーバーのステータス情報という 3 つの部分からなります。区切り文字を使用して、設定の関連する部分を表示できます。

次の例は、関連する RADIUS 設定を示しています。

```
Device# show running-config | include radius

aaa authentication ppp default group radius
aaa accounting network default start-stop group radius
radius-server host 192.0.2.238 auth-port 2095 acct-port 2096 key cisco
radius-server host 192.0.2.238 auth-port 2015 acct-port 2016 key cisco
radius-server load-balance method least-outstanding batch-size 5
```

上記の RADIUS コマンド出力のうち、現在の設定に関する行は次のように定義されます。

- **aaa authentication ppp** コマンドは RADIUS を使用してすべての PPP ユーザーを認証します。
- **aaa accounting** コマンドは、クライアントが認証された後に **start-stop** キーワードを使用して切断されたときに、すべてのアカウンティング要求を AAA サーバーに送信できるようにします。
- **radius-server host** コマンドは、指定された認可ポートおよびアカウンティング ポートと、特定された認証および暗号キーを使用して、RADIUS サーバー ホストの IP アドレスを定義します。
- **radius-server load-balance** コマンドは、バッチ サイズが指定されたグローバル RADIUS サーバー グループのロード バランシングを有効化します。

下の **show debug** サンプル出力は、設定に関する優先サーバーの選択と要求の処理を示しています。

```
Device# show debug

General OS:
  AAA server group server selection debugging is on
#
<sending 10 pppoe requests>
Device#
*Feb 28 13:40:32.199:AAA/SG/SERVER_SELECT(00000014):No preferred server available.
*Feb 28 13:40:32.199:AAA/SG/SERVER_SELECT:Obtaining least loaded server.
*Feb 28 13:40:32.199:AAA/SG/SERVER_SELECT:No more transactions in batch. Obtaining a new
 server.
*Feb 28 13:40:32.199:AAA/SG/SERVER_SELECT:Obtaining a new least loaded server.
*Feb 28 13:40:32.199:AAA/SG/SERVER_SELECT:Server[0] load:0
```

```
*Feb 28 13:40:32.199:AAA/SG/SERVER_SELECT:Server[1] load:0
*Feb 28 13:40:32.199:AAA/SG/SERVER_SELECT:Selected Server[0] with load 0
*Feb 28 13:40:32.199:AAA/SG/SERVER_SELECT:[5] transactions remaining in batch.
*Feb 28 13:40:32.199:AAA/SG/SERVER_SELECT(00000014):Server (192.0.2.238:2095,2096) now
being used as preferred server
*Feb 28 13:40:32.199:AAA/SG/SERVER_SELECT(00000015):No preferred server available.
*Feb 28 13:40:32.199:AAA/SG/SERVER_SELECT:Obtaining least loaded server.
*Feb 28 13:40:32.199:AAA/SG/SERVER_SELECT:[4] transactions remaining in batch. Reusing
server.
*Feb 28 13:40:32.199:AAA/SG/SERVER_SELECT(00000015):Server (192.0.2.238:2095,2096) now
being used as preferred server
*Feb 28 13:40:32.199:AAA/SG/SERVER_SELECT(00000016):No preferred server available.
*Feb 28 13:40:32.199:AAA/SG/SERVER_SELECT:Obtaining least loaded server.
*Feb 28 13:40:32.199:AAA/SG/SERVER_SELECT:[3] transactions remaining in batch. Reusing
server.
*Feb 28 13:40:32.199:AAA/SG/SERVER_SELECT(00000016):Server (192.0.2.238:2095,2096) now
being used as preferred server
*Feb 28 13:40:32.199:AAA/SG/SERVER_SELECT(00000017):No preferred server available.
*Feb 28 13:40:32.199:AAA/SG/SERVER_SELECT:Obtaining least loaded server.
*Feb 28 13:40:32.199:AAA/SG/SERVER_SELECT:[2] transactions remaining in batch. Reusing
server.
*Feb 28 13:40:32.199:AAA/SG/SERVER_SELECT(00000017):Server (192.0.2.238:2095,2096) now
being used as preferred server
*Feb 28 13:40:32.199:AAA/SG/SERVER_SELECT(00000018):No preferred server available.
*Feb 28 13:40:32.199:AAA/SG/SERVER_SELECT:Obtaining least loaded server.
*Feb 28 13:40:32.199:AAA/SG/SERVER_SELECT:[1] transactions remaining in batch. Reusing
server.
*Feb 28 13:40:32.199:AAA/SG/SERVER_SELECT(00000018):Server (192.0.2.238:2095,2096) now
being used as preferred server
*Feb 28 13:40:32.199:AAA/SG/SERVER_SELECT(00000019):No preferred server available.
*Feb 28 13:40:32.199:AAA/SG/SERVER_SELECT:Obtaining least loaded server.
*Feb 28 13:40:32.199:AAA/SG/SERVER_SELECT:No more transactions in batch. Obtaining a new
 server.
*Feb 28 13:40:32.199:AAA/SG/SERVER_SELECT:Obtaining a new least loaded server.
*Feb 28 13:40:32.199:AAA/SG/SERVER_SELECT:Server[1] load:0
*Feb 28 13:40:32.199:AAA/SG/SERVER_SELECT:Server[0] load:5
*Feb 28 13:40:32.199:AAA/SG/SERVER_SELECT:Selected Server[1] with load 0
*Feb 28 13:40:32.199:AAA/SG/SERVER_SELECT:[5] transactions remaining in batch.
*Feb 28 13:40:32.199:AAA/SG/SERVER_SELECT(00000019):Server (192.0.2.238:2015,2016) now
being used as preferred server.
```

show aaa servers コマンドの次のサンプル出力は、グローバル RADIUS サーバー グループ設定に対する AAA サーバーのステータスを示しています。

このサンプル出力は、2 つの RADIUS サーバーのステータスを示しています。両方のサーバーが稼働しており、最後の 2 分間に次の要求が正常に処理されました。

- 6 件の認証要求のうち 5 件
- 5 件のアカウンティング要求のうち 5 件

```
Device# show aaa servers

RADIUS:id 4, priority 1, host 192.0.2.238, auth-port 2095, acct-port 2096
     State:current UP, duration 3175s, previous duration 0s
     Dead:total time 0s, count 0
     Quarantined:No
     Authen:request 6, timeouts 1
             Response:unexpected 1, server error 0, incorrect 0, time 1841ms
             Transaction:success 5, failure 0
     Author:request 0, timeouts 0
             Response:unexpected 0, server error 0, incorrect 0, time 0ms
             Transaction:success 0, failure 0
```

```
     Account:request 5, timeouts 0
             Response:unexpected 0, server error 0, incorrect 0, time 3303ms
             Transaction:success 5, failure 0
     Elapsed time since counters last cleared:2m
RADIUS:id 5, priority 2, host 192.0.2.238, auth-port 2015, acct-port 2016
     State:current UP, duration 3175s, previous duration 0s
     Dead:total time 0s, count 0
     Quarantined:No
     Authen:request 6, timeouts 1
             Response:unexpected 1, server error 0, incorrect 0, time 1955ms
             Transaction:success 5, failure 0
     Author:request 0, timeouts 0
             Response:unexpected 0, server error 0, incorrect 0, time 0ms
             Transaction:success 0, failure 0
     Account:request 5, timeouts 0
             Response:unexpected 0, server error 0, incorrect 0, time 3247ms
             Transaction:success 5, failure 0
     Elapsed time since counters last cleared:2m
```

例：サーバー設定とグローバル RADIUS サーバー グループに対するロード バランシングの有効化

次の例は、関連する RADIUS 設定を示しています。

```
Device# show running-config | include radius

aaa authentication ppp default group radius
aaa accounting network default start-stop group radius
radius-server host 192.0.2.238 auth-port 2095 acct-port 2096 key cisco
radius-server host 192.0.2.238 auth-port 2015 acct-port 2016 key cisco
radius-server load-balance method least-outstanding batch-size 5
```

上記の RADIUS コマンド出力のうち、現在の設定に関する行は次のように定義されます。

- **aaa authentication ppp** コマンドは RADIUS を使用してすべての PPP ユーザーを認証します。
- **aaa accounting** コマンドは、クライアントが認証された後に **start-stop** キーワードを使用して切断されたときに、すべてのアカウンティング要求を認証、認可、およびアカウンティング（AAA）サーバーに送信できるようにします。
- **radius-server host** コマンドは、指定された認可ポートおよびアカウンティング ポートと、特定された認証および暗号キーを使用して、RADIUS サーバー ホストの IP アドレスを定義します。
- **radius-server load-balance** コマンドは、バッチ サイズが指定されたグローバル RADIUS サーバー グループのロード バランシングを有効化します。

例：グローバル RADIUS サーバー グループのデバッグ出力

下の **debug** コマンドの出力は、設定に関する優先サーバーの選択と要求の処理を示しています。

```
Device# show debug

General OS:
  AAA server group server selection debugging is on
```

```
#
<sending 10 pppoe requests>
Device#
*Feb 28 13:40:32.199:AAA/SG/SERVER_SELECT(00000014):No preferred server available.
*Feb 28 13:40:32.199:AAA/SG/SERVER_SELECT:Obtaining least loaded server.
*Feb 28 13:40:32.199:AAA/SG/SERVER_SELECT:No more transactions in batch. Obtaining a new
 server.
*Feb 28 13:40:32.199:AAA/SG/SERVER_SELECT:Obtaining a new least loaded server.
*Feb 28 13:40:32.199:AAA/SG/SERVER_SELECT:Server[0] load:0
*Feb 28 13:40:32.199:AAA/SG/SERVER_SELECT:Server[1] load:0
*Feb 28 13:40:32.199:AAA/SG/SERVER_SELECT:Selected Server[0] with load 0
*Feb 28 13:40:32.199:AAA/SG/SERVER_SELECT:[5] transactions remaining in batch.
*Feb 28 13:40:32.199:AAA/SG/SERVER_SELECT(00000014):Server (192.0.2.238:2095,2096) now
being used as preferred server
*Feb 28 13:40:32.199:AAA/SG/SERVER_SELECT(00000015):No preferred server available.
*Feb 28 13:40:32.199:AAA/SG/SERVER_SELECT:Obtaining least loaded server.
*Feb 28 13:40:32.199:AAA/SG/SERVER_SELECT:[4] transactions remaining in batch. Reusing
server.
*Feb 28 13:40:32.199:AAA/SG/SERVER_SELECT(00000015):Server (192.0.2.238:2095,2096) now
being used as preferred server
*Feb 28 13:40:32.199:AAA/SG/SERVER_SELECT(00000016):No preferred server available.
*Feb 28 13:40:32.199:AAA/SG/SERVER_SELECT:Obtaining least loaded server.
*Feb 28 13:40:32.199:AAA/SG/SERVER_SELECT:[3] transactions remaining in batch. Reusing
server.
*Feb 28 13:40:32.199:AAA/SG/SERVER_SELECT(00000016):Server (192.0.2.238:2095,2096) now
being used as preferred server
*Feb 28 13:40:32.199:AAA/SG/SERVER_SELECT(00000017):No preferred server available.
*Feb 28 13:40:32.199:AAA/SG/SERVER_SELECT:Obtaining least loaded server.
*Feb 28 13:40:32.199:AAA/SG/SERVER_SELECT:[2] transactions remaining in batch. Reusing
server.
*Feb 28 13:40:32.199:AAA/SG/SERVER_SELECT(00000017):Server (192.0.2.238:2095,2096) now
being used as preferred server
*Feb 28 13:40:32.199:AAA/SG/SERVER_SELECT(00000018):No preferred server available.
*Feb 28 13:40:32.199:AAA/SG/SERVER_SELECT:Obtaining least loaded server.
*Feb 28 13:40:32.199:AAA/SG/SERVER_SELECT:[1] transactions remaining in batch. Reusing
server.
*Feb 28 13:40:32.199:AAA/SG/SERVER_SELECT(00000018):Server (192.0.2.238:2095,2096) now
being used as preferred server
*Feb 28 13:40:32.199:AAA/SG/SERVER_SELECT(00000019):No preferred server available.
*Feb 28 13:40:32.199:AAA/SG/SERVER_SELECT:Obtaining least loaded server.
*Feb 28 13:40:32.199:AAA/SG/SERVER_SELECT:No more transactions in batch. Obtaining a new
 server.
*Feb 28 13:40:32.199:AAA/SG/SERVER_SELECT:Obtaining a new least loaded server.
*Feb 28 13:40:32.199:AAA/SG/SERVER_SELECT:Server[1] load:0
*Feb 28 13:40:32.199:AAA/SG/SERVER_SELECT:Server[0] load:5
*Feb 28 13:40:32.199:AAA/SG/SERVER_SELECT:Selected Server[1] with load 0
*Feb 28 13:40:32.199:AAA/SG/SERVER_SELECT:[5] transactions remaining in batch.
*Feb 28 13:40:32.199:AAA/SG/SERVER_SELECT(00000019):Server (192.0.2.238:2015,2016) now
being used as preferred server.
```

例：グローバル RADIUS サーバー グループのサーバー ステータス情報

show aaa server コマンドの次のサンプル出力は、グローバル RADIUS サーバー グループ設定に対する AAA サーバーのステータスを示しています。

```
Device# show aaa server

RADIUS:id 4, priority 1, host 192.0.2.238, auth-port 2095, acct-port 2096
     State:current UP, duration 3175s, previous duration 0s
     Dead:total time 0s, count 0
     Quarantined:No
     Authen:request 6, timeouts 1
             Response:unexpected 1, server error 0, incorrect 0, time 1841ms
```

```
            Transaction:success 5, failure 0
     Author:request 0, timeouts 0
            Response:unexpected 0, server error 0, incorrect 0, time 0ms
            Transaction:success 0, failure 0
     Account:request 5, timeouts 0
            Response:unexpected 0, server error 0, incorrect 0, time 3303ms
            Transaction:success 5, failure 0
     Elapsed time since counters last cleared:2m
RADIUS:id 5, priority 2, host 192.0.2.238, auth-port 2015, acct-port 2016
     State:current UP, duration 3175s, previous duration 0s
     Dead:total time 0s, count 0
     Quarantined:No
     Authen:request 6, timeouts 1
            Response:unexpected 1, server error 0, incorrect 0, time 1955ms
            Transaction:success 5, failure 0
     Author:request 0, timeouts 0
            Response:unexpected 0, server error 0, incorrect 0, time 0ms
            Transaction:success 0, failure 0
     Account:request 5, timeouts 0
            Response:unexpected 0, server error 0, incorrect 0, time 3247ms
            Transaction:success 5, failure 0
     Elapsed time since counters last cleared:2m
```

このサンプル出力は、2 つの RADIUS サーバーのステータスを示しています。両方のサーバーが稼働しており、最後の 2 分間に次の要求が正常に処理されました。

- 6 つの認証要求のうち 5 つ
- 5 つのアカウンティング要求のうち 5 つ

例：名前付き RADIUS サーバ グループのロード バランシングの有効化

次の例は、名前付き RADIUS サーバー グループで有効化されたロード バランシングを示しています。これらの例は、RADIUS コマンド出力の現在の設定、デバッグ出力、認証、認可、およびアカウンティング（AAA）サーバーのステータス情報という 3 つの部分からなります。

次のサンプル出力は、関連する RADIUS 設定を示しています。

```
Device# show running-config
.
.
.
aaa group server radius server-group1
 server 192.0.2.238 auth-port 2095 acct-port 2096
 server 192.0.2.238 auth-port 2015 acct-port 2016
 load-balance method least-outstanding batch-size 5
!
aaa authentication ppp default group server-group1
aaa accounting network default start-stop group server-group1
.
.
.
Device(config-sg-radius)# load-balance method least-outstanding batch-size 30
```

上記の RADIUS コマンド出力のうち、現在の設定に関する行は次のように定義されます。

- **aaa group server radius** コマンドは、2 つのメンバー サーバーからなるサーバー グループの設定を表示します。

- **load-balance** コマンドは、バッチ サイズが指定されたグローバル RADIUS サーバー グループのロード バランシングを有効化します。
- **aaa authentication ppp** コマンドは RADIUS を使用してすべての PPP ユーザーを認証します。
- **aaa accounting** コマンドは、クライアントが認証された後に **start-stop** キーワードを使用して切断されたときに、すべてのアカウンティング要求を AAA サーバーに送信できるようにします。

下の show debug サンプル出力は、前の設定に関する優先サーバーの選択と要求の処理を示しています。

```
Device# show debug

*Feb 28 13:51:16.019:AAA/SG/SERVER_SELECT(0000002C):No preferred server available.
*Feb 28 13:51:16.019:AAA/SG/SERVER_SELECT:Obtaining least loaded server.
*Feb 28 13:51:16.019:AAA/SG/SERVER_SELECT:No more transactions in batch. Obtaining a new
 server.
*Feb 28 13:51:16.019:AAA/SG/SERVER_SELECT:Obtaining a new least loaded server.
*Feb 28 13:51:16.019:AAA/SG/SERVER_SELECT:Server[0] load:0
*Feb 28 13:51:16.019:AAA/SG/SERVER_SELECT:Server[1] load:0
*Feb 28 13:51:16.019:AAA/SG/SERVER_SELECT:Selected Server[0] with load 0
*Feb 28 13:51:16.019:AAA/SG/SERVER_SELECT:[5] transactions remaining in batch.
*Feb 28 13:51:16.019:AAA/SG/SERVER_SELECT(0000002C):Server (192.0.2.238:2095,2096) now
being used as preferred server
*Feb 28 13:51:16.019:AAA/SG/SERVER_SELECT(0000002D):No preferred server available.
*Feb 28 13:51:16.019:AAA/SG/SERVER_SELECT:Obtaining least loaded server.
*Feb 28 13:51:16.019:AAA/SG/SERVER_SELECT:[4] transactions remaining in batch. Reusing
server.
*Feb 28 13:51:16.019:AAA/SG/SERVER_SELECT(0000002D):Server (192.0.2.238:2095,2096) now
being used as preferred server
*Feb 28 13:51:16.019:AAA/SG/SERVER_SELECT(0000002E):No preferred server available.
*Feb 28 13:51:16.019:AAA/SG/SERVER_SELECT:Obtaining least loaded server.
*Feb 28 13:51:16.019:AAA/SG/SERVER_SELECT:[3] transactions remaining in batch. Reusing
server.
*Feb 28 13:51:16.019:AAA/SG/SERVER_SELECT(0000002E):Server (192.0.2.238:2095,2096) now
being used as preferred server
*Feb 28 13:51:16.019:AAA/SG/SERVER_SELECT(0000002F):No preferred server available.
*Feb 28 13:51:16.019:AAA/SG/SERVER_SELECT:Obtaining least loaded server.
*Feb 28 13:51:16.019:AAA/SG/SERVER_SELECT:[2] transactions remaining in batch. Reusing
server.
*Feb 28 13:51:16.019:AAA/SG/SERVER_SELECT(0000002F):Server (192.0.2.238:2095,2096) now
being used as preferred server
*Feb 28 13:51:16.019:AAA/SG/SERVER_SELECT(00000030):No preferred server available.
*Feb 28 13:51:16.019:AAA/SG/SERVER_SELECT:Obtaining least loaded server.
*Feb 28 13:51:16.019:AAA/SG/SERVER_SELECT:[1] transactions remaining in batch. Reusing
server.
*Feb 28 13:51:16.019:AAA/SG/SERVER_SELECT(00000030):Server (192.0.2.238:2095,2096) now
being used as preferred server
*Feb 28 13:51:16.023:AAA/SG/SERVER_SELECT(00000031):No preferred server available.
*Feb 28 13:51:16.023:AAA/SG/SERVER_SELECT:Obtaining least loaded server.
*Feb 28 13:51:16.023:AAA/SG/SERVER_SELECT:No more transactions in batch. Obtaining a new
 server.
*Feb 28 13:51:16.023:AAA/SG/SERVER_SELECT:Obtaining a new least loaded server.
*Feb 28 13:51:16.023:AAA/SG/SERVER_SELECT:Server[1] load:0
*Feb 28 13:51:16.023:AAA/SG/SERVER_SELECT:Server[0] load:5
*Feb 28 13:51:16.023:AAA/SG/SERVER_SELECT:Selected Server[1] with load 0
*Feb 28 13:51:16.023:AAA/SG/SERVER_SELECT:[5] transactions remaining in batch.
*Feb 28 13:51:16.023:AAA/SG/SERVER_SELECT(00000031):Server (192.0.2.238:2015,2016) now
being used as preferred server
```

```
*Feb 28 13:51:16.023:AAA/SG/SERVER_SELECT(00000032):No preferred server available.
*Feb 28 13:51:16.023:AAA/SG/SERVER_SELECT:Obtaining least loaded server.
*Feb 28 13:51:16.023:AAA/SG/SERVER_SELECT:[4] transactions remaining in batch. Reusing
server.
.
.
.
```

show aaa servers コマンドの次のサンプル出力は、名前付き RADIUS サーバー グループ設定に対する AAA サーバーのステータスを示しています。

このサンプル出力は、2 つの RADIUS サーバーのステータスを示しています。両方のサーバーが動作中ですが、カウンタが 0 分前にクリアされて以降は、どの要求も処理されていません。

```
Device# show aaa servers

RADIUS:id 8, priority 1, host 192.0.2.238, auth-port 2095, acct-port 2096
     State:current UP, duration 3781s, previous duration 0s
     Dead:total time 0s, count 0
     Quarantined:No
     Authen:request 0, timeouts 0
             Response:unexpected 0, server error 0, incorrect 0, time 0ms
             Transaction:success 0, failure 0
     Author:request 0, timeouts 0
             Response:unexpected 0, server error 0, incorrect 0, time 0ms
             Transaction:success 0, failure 0
     Account:request 0, timeouts 0
             Response:unexpected 0, server error 0, incorrect 0, time 0ms
             Transaction:success 0, failure 0
     Elapsed time since counters last cleared:0m
RADIUS:id 9, priority 2, host 192.0.2.238, auth-port 2015, acct-port 2016
     State:current UP, duration 3781s, previous duration 0s
     Dead:total time 0s, count 0
     Quarantined:No
     Authen:request 0, timeouts 0
             Response:unexpected 0, server error 0, incorrect 0, time 0ms
             Transaction:success 0, failure 0
     Author:request 0, timeouts 0
             Response:unexpected 0, server error 0, incorrect 0, time 0ms
             Transaction:success 0, failure 0
     Account:request 0, timeouts 0
             Response:unexpected 0, server error 0, incorrect 0, time 0ms
             Transaction:success 0, failure 0
     Elapsed time since counters last cleared:0m
```

例：サーバー設定と名前付き RADIUS サーバー グループに対するロード バランシングの有効化

次のサンプル出力は、関連する RADIUS 設定を示しています。

```
Device# show running-config
.
.
.
aaa group server radius server-group1
 server 192.0.2.238 auth-port 2095 acct-port 2096
 server 192.0.2.238 auth-port 2015 acct-port 2016
 load-balance method least-outstanding batch-size 5
!
aaa authentication ppp default group server-group1
aaa accounting network default start-stop group server-group1
.
```

.
.

上記の RADIUS コマンド出力のうち、現在の設定に関する行は次のように定義されます。

- **aaa group server radius** コマンドは、2 つのメンバー サーバーからなるサーバー グループの設定を表示します。
- **load-balance** コマンドは、バッチ サイズが指定されたグローバル RADIUS サーバー グループのロード バランシングを有効化します。
- **aaa authentication ppp** コマンドは RADIUS を使用してすべての PPP ユーザーを認証します。
- **aaa accounting** コマンドは、クライアントが認証された後に **start-stop** キーワードを使用して切断されたときに、すべてのアカウンティング要求を AAA サーバーに送信できるようにします。

例：名前付き RADIUS サーバー グループのデバッグ出力

下のデバッグ サンプル出力は、上の設定に関する優先サーバーの選択と要求の処理を示しています。

```
Device# show debug

*Feb 28 13:51:16.019:AAA/SG/SERVER_SELECT(0000002C):No preferred server available.
*Feb 28 13:51:16.019:AAA/SG/SERVER_SELECT:Obtaining least loaded server.
*Feb 28 13:51:16.019:AAA/SG/SERVER_SELECT:No more transactions in batch. Obtaining a new
 server.
*Feb 28 13:51:16.019:AAA/SG/SERVER_SELECT:Obtaining a new least loaded server.
*Feb 28 13:51:16.019:AAA/SG/SERVER_SELECT:Server[0] load:0
*Feb 28 13:51:16.019:AAA/SG/SERVER_SELECT:Server[1] load:0
*Feb 28 13:51:16.019:AAA/SG/SERVER_SELECT:Selected Server[0] with load 0
*Feb 28 13:51:16.019:AAA/SG/SERVER_SELECT:[5] transactions remaining in batch.
*Feb 28 13:51:16.019:AAA/SG/SERVER_SELECT(0000002C):Server (192.0.2.238:2095,2096) now
being used as preferred server
*Feb 28 13:51:16.019:AAA/SG/SERVER_SELECT(0000002D):No preferred server available.
*Feb 28 13:51:16.019:AAA/SG/SERVER_SELECT:Obtaining least loaded server.
*Feb 28 13:51:16.019:AAA/SG/SERVER_SELECT:[4] transactions remaining in batch. Reusing
server.
*Feb 28 13:51:16.019:AAA/SG/SERVER_SELECT(0000002D):Server (192.0.2.238:2095,2096) now
being used as preferred server
*Feb 28 13:51:16.019:AAA/SG/SERVER_SELECT(0000002E):No preferred server available.
*Feb 28 13:51:16.019:AAA/SG/SERVER_SELECT:Obtaining least loaded server.
*Feb 28 13:51:16.019:AAA/SG/SERVER_SELECT:[3] transactions remaining in batch. Reusing
server.
*Feb 28 13:51:16.019:AAA/SG/SERVER_SELECT(0000002E):Server (192.0.2.238:2095,2096) now
being used as preferred server
*Feb 28 13:51:16.019:AAA/SG/SERVER_SELECT(0000002F):No preferred server available.
*Feb 28 13:51:16.019:AAA/SG/SERVER_SELECT:Obtaining least loaded server.
*Feb 28 13:51:16.019:AAA/SG/SERVER_SELECT:[2] transactions remaining in batch. Reusing
server.
*Feb 28 13:51:16.019:AAA/SG/SERVER_SELECT(0000002F):Server (192.0.2.238:2095,2096) now
being used as preferred server
*Feb 28 13:51:16.019:AAA/SG/SERVER_SELECT(00000030):No preferred server available.
*Feb 28 13:51:16.019:AAA/SG/SERVER_SELECT:Obtaining least loaded server.
*Feb 28 13:51:16.019:AAA/SG/SERVER_SELECT:[1] transactions remaining in batch. Reusing
server.
*Feb 28 13:51:16.019:AAA/SG/SERVER_SELECT(00000030):Server (192.0.2.238:2095,2096) now
being used as preferred server
```

```
*Feb 28 13:51:16.023:AAA/SG/SERVER_SELECT(00000031):No preferred server available.
*Feb 28 13:51:16.023:AAA/SG/SERVER_SELECT:Obtaining least loaded server.
*Feb 28 13:51:16.023:AAA/SG/SERVER_SELECT:No more transactions in batch. Obtaining a new
 server.
*Feb 28 13:51:16.023:AAA/SG/SERVER_SELECT:Obtaining a new least loaded server.
*Feb 28 13:51:16.023:AAA/SG/SERVER_SELECT:Server[1] load:0
*Feb 28 13:51:16.023:AAA/SG/SERVER_SELECT:Server[0] load:5
*Feb 28 13:51:16.023:AAA/SG/SERVER_SELECT:Selected Server[1] with load 0
*Feb 28 13:51:16.023:AAA/SG/SERVER_SELECT:[5] transactions remaining in batch.
*Feb 28 13:51:16.023:AAA/SG/SERVER_SELECT(00000031):Server (192.0.2.238:2015,2016) now
being used as preferred server
*Feb 28 13:51:16.023:AAA/SG/SERVER_SELECT(00000032):No preferred server available.
*Feb 28 13:51:16.023:AAA/SG/SERVER_SELECT:Obtaining least loaded server.
*Feb 28 13:51:16.023:AAA/SG/SERVER_SELECT:[4] transactions remaining in batch. Reusing
server.
.
.
.
```

例：名前付き RADIUS サーバー グループのサーバー ステータス情報

show aaa servers コマンドの次のサンプル出力は、名前付き RADIUS サーバー グループ設定に対する AAA サーバーのステータスを示しています。

```
Device# show aaa servers

RADIUS:id 8, priority 1, host 192.0.2.238, auth-port 2095, acct-port 2096
     State:current UP, duration 3781s, previous duration 0s
     Dead:total time 0s, count 0
     Quarantined:No
     Authen:request 0, timeouts 0
             Response:unexpected 0, server error 0, incorrect 0, time 0ms
             Transaction:success 0, failure 0
     Author:request 0, timeouts 0
             Response:unexpected 0, server error 0, incorrect 0, time 0ms
             Transaction:success 0, failure 0
     Account:request 0, timeouts 0
             Response:unexpected 0, server error 0, incorrect 0, time 0ms
             Transaction:success 0, failure 0
     Elapsed time since counters last cleared:0m
RADIUS:id 9, priority 2, host 192.0.2.238, auth-port 2015, acct-port 2016
     State:current UP, duration 3781s, previous duration 0s
     Dead:total time 0s, count 0
     Quarantined:No
     Authen:request 0, timeouts 0
             Response:unexpected 0, server error 0, incorrect 0, time 0ms
             Transaction:success 0, failure 0
     Author:request 0, timeouts 0
             Response:unexpected 0, server error 0, incorrect 0, time 0ms
             Transaction:success 0, failure 0
     Account:request 0, timeouts 0
             Response:unexpected 0, server error 0, incorrect 0, time 0ms
             Transaction:success 0, failure 0
     Elapsed time since counters last cleared:0m
```

このサンプル出力は、2 つの RADIUS サーバーのステータスを示しています。両方のサーバーが動作中ですが、カウンタが 0 分前にクリアされて以降は、どの要求も処理されていません。

例：アイドル タイマーのモニタリング

次の例は、名前付き RADIUS サーバー グループに対して有効にされたロード バランシングに関するアイドル タイマーと関連するサーバー状態を示しています。RADIUS コマンド出力と debug コマンド出力の現在の設定も表示されます。

次のサンプル出力は、関連する RADIUS 設定を示しています。

```
Device# show running-config | include radius

aaa group server radius server-group1
radius-server host 192.0.2.238 auth-port 2095 acct-port 2096 test username junk1 idle-time
 1 key cisco
radius-server host 192.0.2.238 auth-port 2015 acct-port 2016 test username junk1 idle-time
 1 key cisco
radius-server load-balance method least-outstanding batch-size 5
```

上記の RADIUS コマンド出力のうち、現在の設定に関する行は次のように定義されます。

- **aaa group server radius** コマンドは、サーバー グループの設定を表示します。
- **radius-server host** コマンドは、指定された認可ポートおよびアカウンティング ポートと、特定された認証および暗号キーを使用して、RADIUS サーバー ホストの IP アドレスを定義します。
- **radius-server load-balance** コマンドは、バッチ サイズが指定された RADIUS サーバーのロード バランシングを有効化します。

下の **show debug** サンプル出力は、サーバーに送信されるテスト要求を示しています。サーバーに送信されたテスト要求に対する応答が受信され、必要に応じて、隔離からサーバーが除外され、サーバーが動作中としてマークされてから、アイドル タイマーがリセットされます。

```
Device# show debug

*Feb 28 13:52:20.835:AAA/SG/TEST:Server (192.0.2.238:2015,2016) quarantined.
*Feb 28 13:52:20.835:AAA/SG/TEST:Sending test request(s) to server (192.0.2.238:2015,2016)
*Feb 28 13:52:20.835:AAA/SG/TEST:Sending 1 Access-Requests, 1 Accounting-Requests in
current batch.
*Feb 28 13:52:20.835:AAA/SG/TEST(Req#:1):Sending test AAA Access-Request.
*Feb 28 13:52:20.835:AAA/SG/TEST(Req#:1):Sending test AAA Accounting-Request.
*Feb 28 13:52:21.087:AAA/SG/TEST:Obtained Test response from server (192.0.2.238:2015,2016)
*Feb 28 13:52:22.651:AAA/SG/TEST:Obtained Test response from server (192.0.2.238:2015,2016)
*Feb 28 13:52:22.651:AAA/SG/TEST:Necessary responses received from server
(192.0.2.238:2015,2016)
*Feb 28 13:52:22.651:AAA/SG/TEST:Server (192.0.2.238:2015,2016) marked ALIVE. Idle timer
 set for 60 secs(s).
*Feb 28 13:52:22.651:AAA/SG/TEST:Server (192.0.2.238:2015,2016) removed from quarantine.
.
.
.
```

例：サーバー設定とアイドル タイマー モニタリングに対するロード バランシングの有効化

次のサンプル出力は、関連する RADIUS 設定を示しています。

```
Device# show running-config | include radius
```

```
aaa group server radius server-group1
radius-server host 192.0.2.238 auth-port 2095 acct-port 2096 test username junk1 idle-time
 1 key cisco
radius-server host 192.0.2.238 auth-port 2015 acct-port 2016 test username junk1 idle-time
 1 key cisco
radius-server load-balance method least-outstanding batch-size 5
```

上記の RADIUS コマンド出力のうち、現在の設定に関する行は次のように定義されます。

- **aaa group server radius** コマンドは、サーバー グループの設定を表示します。
- **radius-server host** コマンドは、指定された認可ポートおよびアカウンティング ポートと、特定された認証および暗号キーを使用して、RADIUS サーバー ホストの IP アドレスを定義します。
- **radius-server load-balance** コマンドは、バッチ サイズが指定された RADIUS サーバーのロード バランシングを有効化します。

例：アイドル タイマー モニタリングのデバッグ出力

下の **debug** コマンドの出力は、サーバーに送信されるテスト要求を示しています。サーバーに送信されたテスト要求に対する応答が受信され、必要に応じて、隔離からサーバーが除外され、動作中としてマークされてから、アイドル タイマーがリセットされます。

```
Device# show debug
*Feb 28 13:52:20.835:AAA/SG/TEST:Server (192.0.2.238:2015,2016) quarantined.
*Feb 28 13:52:20.835:AAA/SG/TEST:Sending test request(s) to server (192.0.2.238:2015,2016)
*Feb 28 13:52:20.835:AAA/SG/TEST:Sending 1 Access-Requests, 1 Accounting-Requests in
current batch.
*Feb 28 13:52:20.835:AAA/SG/TEST(Req#:1):Sending test AAA Access-Request.
*Feb 28 13:52:20.835:AAA/SG/TEST(Req#:1):Sending test AAA Accounting-Request.
*Feb 28 13:52:21.087:AAA/SG/TEST:Obtained Test response from server (192.0.2.238:2015,2016)
*Feb 28 13:52:22.651:AAA/SG/TEST:Obtained Test response from server (192.0.2.238:2015,2016)
*Feb 28 13:52:22.651:AAA/SG/TEST:Necessary responses received from server
(192.0.2.238:2015,2016)
*Feb 28 13:52:22.651:AAA/SG/TEST:Server (192.0.2.238:2015,2016) marked ALIVE. Idle timer
 set for 60 secs(s).
*Feb 28 13:52:22.651:AAA/SG/TEST:Server (192.0.2.238:2015,2016) removed from quarantine.
.
.
.
```

例：認証サーバと認可サーバが同じ優先サーバの設定

次の例は、サーバーの 209.165.200.225 と 209.165.200.226 を共有する認証サーバー グループと認可サーバー グループを示しています。両方のサーバー グループで優先サーバー フラグが有効になっています。

```
aaa group server radius authentication-group
   server 209.165.200.225 key radkey1
   server 209.165.200.226 key radkey2
aaa group server radius accounting-group
   server 209.165.200.225 key radkey1
   server 209.165.200.226 key radkey2
```

あるセッションで優先サーバーが選択されると、そのセッションのすべてのトランザクションでオリジナルの優先サーバーの使用が継続されます。サーバーの 209.165.200.225 と

209.165.200.226は、トランザクションではなく、セッションに基づいてロードバランシングされます。

例：認証サーバと認可サーバが別々の優先サーバの設定

次の例は、サーバーの 209.165.200.225 と 209.165.200.226 を使用する認証サーバー グループとサーバーの 209.165.201.1 と 209.165.201.2 を使用する認可サーバー グループを示しています。両方のサーバー グループで優先サーバー フラグが有効になっています。

```
aaa group server radius authentication-group
   server 209.165.200.225 key radkey1
   server 209.165.200.226 key radkey2
aaa group server radius accounting-group
   server 209.165.201.1 key radkey3
   server 209.165.201.2 key radkey4
```

認証サーバー グループとアカウンティング サーバー グループはどの共通サーバーも共有しません。アカウンティング トランザクションでは優先サーバーは検出されないため、認証サーバーとアカウンティング サーバーはトランザクションに基づいてロードバランシングされます。1 つのセッションで開始レコードと終了レコードが同じサーバーに送信されます。

例：認証サーバと認可サーバが重複している優先サーバの設定

次の例は、サーバーの209.165.200.225、209.165.200.226、および209.165.201.1を使用する認証サーバー グループとサーバーの 209.165.201.1 と 209.165.201.2 を使用する認可サーバー グループを示しています。両方のサーバー グループで優先サーバー フラグが有効になっています。

```
aaa group server radius authentication-group
   server 209.165.200.225 key radkey1
   server 209.165.200.226 key radkey2
   server 209.165.201.1 key radkey3
aaa group server radius accounting-group
   server 209.165.201.1 key radkey3
   server 209.165.201.2 key radkey4
```

すべてのサーバーのトランザクション処理能力が同じ場合は、すべての認証トランザクションの 1/3 がサーバーの 209.165.201.1 に転送されます。したがって、すべてのアカウンティング トランザクションの 1/3 もサーバーの 209.165.201.1 に転送されます。アカウンティング トランザクションの残りの 2/3 は、サーバーの 209.165.201.1 と 209.165.201.2 の間で均等にロードバランシングされます。サーバーの209.165.201.1に未処理のアカウンティング トランザクションがあるため、サーバーの 209.165.201.1 が受信する認証トランザクション数は減少します。

例：認証サーバが認可サーバのサブセットである優先サーバの設定

次の例は、サーバーの209.165.200.225と209.165.200.226を使用する認証サーバー グループと、サーバーの209.165.200.225、209.165.200.226、および209.165.201.1を使用する認可サーバー グループを示しています。両方のサーバー グループで優先サーバー フラグが有効になっています。

```
aaa group server radius authentication-group
   server 209.165.200.225 key radkey1
   server 209.165.200.226 key radkey2
```

```
aaa group server radius accounting-group
  server 209.165.200.225 key radkey1
   server 209.165.200.226 key radkey2
   server 209.165.201.1 key radkey3
```

すべての認証トランザクションの半分がサーバーの 209.165.200.225 に送信され、残りの半分がサーバーの 209.165.200.226 に送信されます。サーバーの 209.165.200.225 と 209.165.200.226 は、認証およびアカウンティング トランザクションの優先サーバーです。そのため、認証およびアカウンティング トランザクションは、サーバーの 209.165.200.225 と 209.165.200.226 に均等に分配されます。サーバーの 209.165.201.1 は相対的に使用されません。

例：認証サーバが認可サーバのスーパーセットである優先サーバの設定

次の例は、サーバーの 209.165.200.225、209.165.200.226、および 209.165.201.1 を使用する認証サーバー グループとサーバーの 209.165.200.225 と 209.165.200.226 を使用する認可サーバー グループを示しています。両方のサーバー グループで優先サーバー フラグが有効になっています。

```
aaa group server radius authentication-group
   server 209.165.200.225 key radkey1
   server 209.165.200.226 key radkey2
   server 209.165.201.1 key radkey3
aaa group server radius accounting-group
  server 209.165.200.225 key radkey1
   server 209.165.200.226 key radkey2
```

最初に、認証トランザクションの 1/3 が認可サーバー グループ内の各サーバーに割り当てられます。追加のセッションに対してアカウンティング トランザクションが生成されますが、優先サーバー フラグがオンになっているため、アカウンティング トランザクションはサーバーの 209.165.200.225 と 209.165.200.226 に送信されます。サーバーの 209.165.200.225 と 209.165.200.226 がトランザクションの処理を開始しますが、認証トランザクションはサーバーの 209.165.201.1 に送信されます。サーバーの 209.165.201.1 で認証されたトランザクション要求は、どの優先サーバー設定も含まず、サーバーの 209.165.200.225 と 209.165.200.226 に分配されるため、優先サーバー フラグの使用が無効になります。この設定は慎重に使用する必要があります。

RADIUS サーバ ロード バランシングのその他の参考資料

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『Cisco IOS Master Command List, All Releases』

関連項目	マニュアル タイトル
セキュリティ コマンド	• 『Security Command Reference: Commands A to C』 • 『Security Command Reference: Commands D to L』 • 『Security Command Reference: Commands M to R』 • 『Security Command Reference: Commands S to Z』
AAA および RADIUS	『*Authentication, Authorization, and Accounting Configuration Guide*』
AAA サーバー グループと RADIUS 設定	『*RADIUS Configuration Guide*』の「Configuring RADIUS」モジュール
フェールオーバー再試行順序変更モード	『*RADIUS Configuration Guide*』の「RADIUS Server Reorder on Failure」モジュール

シスコのテクニカル サポート

説明	リンク
シスコのサポート Web サイトでは、シスコの製品やテクノロジーに関するトラブルシューティングにお役立ていただけるように、マニュアルやツールをはじめとする豊富なオンライン リソースを提供しています。 お使いの製品のセキュリティ情報や技術情報を入手するために、Cisco Notification Service（Field Notice からアクセス）、Cisco Technical Services Newsletter、Really Simple Syndication（RSS）フィードなどの各種サービスに加入できます。 シスコのサポート Web サイトのツールにアクセスする際は、Cisco.com のユーザ ID およびパスワードが必要です。	http://www.cisco.com/en/US/support/index.html

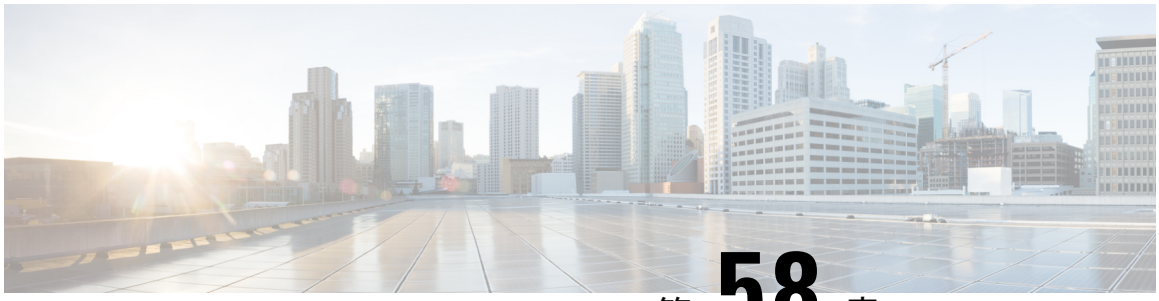
RADIUS サーバー ロード バランシングの機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *83 : RADIUS* サーバー ロード バランシングの機能情報

機能名	リリース	機能情報
RADIUS サーバー ロード バランシング	12.2(28)SB 12.4(11)T 12.2(33)SRC	RADIUS サーバー ロード バランシング機能は、認証、認可、およびアカウンティング（AAA）の認証トランザクションとアカウンティング トランザクションをサーバー グループ内のサーバーに分配します。これらのサーバーは、トランザクションの負荷を分担し、空いているサーバーを効率的に使用して着信要求に対するより迅速な応答を実現します。 この機能は、Cisco IOS Release 12.2(28)SB に統合されました。 この機能は、Cisco IOS Release 12.4(11)T に統合されました。 この機能は、Cisco IOS Release 12.2(33)SRC に統合されました。 次のコマンドが導入または変更されました。**debug aaa sg-server selection**、**debug aaa test**、**load-balance (server-group)**、**radius-server host**、**radius-server load-balance**、**test aaa group.**
RADIUS サーバー ロード バランシング ポーティング	Cisco IOS XE Release 2.1	この機能は、Cisco ASR 1000 シリーズ ルータで導入されました。



第 58 章

RADIUS サーバー障害発生時順序変更

RADIUS サーバー障害発生時順序変更機能は、高負荷期間またはサーバーで障害が発生した場合に、サーバー グループ内の別のサーバーへのフェールオーバーを提供します。障害発生後は、すべての RADIUS トラフィックが新しいサーバーに転送されます。新しいサーバーからサーバー グループ内の別のサーバーにトラフィックが切り替えられるのは、新しいサーバーでも障害が発生した場合に限られます。トラフィックが自動的に最初にサーバーに戻されることはありません。

RADIUS トランザクションを複数のサーバーに分散させることによって、認証要求とアカウンティング要求がより迅速に処理されます。

RADIUS サーバー障害発生時順序変更の前提条件

- 障害発生時に順序変更を実行するように RADIUS サーバーを設定する前に、**aaa new-model** コマンドを使用して、認証、認可、およびアカウンティング（AAA）を有効にする必要があります。
- 認証、アカウンティング、スタティック ルート ダウンロードなどの機能用に RADIUS を設定する必要もあります。

RADIUS サーバー障害発生時順序変更の制約事項

- サーバー グループごとに新しい 4 バイトのメモリが消費されます。ただし、ほとんどのサーバーは少数のサーバー グループのみに設定されているため、追加の4バイトはそれほど性能に影響しない可能性があります。
- Cisco IOS XE ソフトウェアセット内の RADIUS 機能によっては、この機能を使用できない場合があります。RADIUS機能でRADIUSサーバ障害発生時順序変更機能を使用できない場合は、順序変更機能が設定されていないかのようにサーバが動作します。

RADIUS サーバー障害発生時順序変更に関する情報

RADIUS サーバーの障害

RADIUS サーバー障害発生時順序変更機能が設定されていない状態でサーバーの障害が発生した場合：

1. 新しい RADIUS トランザクションを実行する必要があります。
2. トランザクション用のRADIUSパケットが、グループ内で停止中としてマークされていない（設定されたデッドタイムに従って）最初のサーバーに送信され、設定された再送回数だけ再送されます。
3. 再送のすべてがタイムアウトした（設定されたタイムアウトに従って）場合は、ルータがそのパケットをリストで次の非停止中サーバーに設定された再送回数だけ送信します。
4. ステップ 3 は、トランザクションごとに指定された最大送信回数に達するまで繰り返されます。最大送信回数に到達する前にリストの最後に到達した場合は、ルータがリストの先頭に戻ってそこから処理を継続します。

このプロセスのどの時点でも、サーバーが停止中サーバーの検出基準（設定不可。使用されている Cisco IOS XE ソフトウェアのバージョンによって異なる）を満たした場合は、設定されたデッドタイムに合わせてサーバーが停止中としてマークされます。

RADIUS サーバー障害発生時順序変更機能の動作方法

RADIUS サーバー障害発生時順序変更機能を設定した場合は、次のように、初期サーバーとして使用する RADIUS サーバーが決定されます。

- ネットワーク アクセス サーバー（NAS）は、トランスミッションが送信される最初のサーバーである「フラグ設定された」サーバーのステータスを保持します。
- フラグ設定されたサーバーにトランスミッションが送信された後は、設定された再送回数だけ、フラグ設置されたサーバーにトラフィックが再送されます。

- その後は、NASが、フラグ設定されたサーバーの次にリストされたサーバーから始めて、設定されたトランザクションの最大再試行回数に到達するか、応答が返されるまで、サーバー グループ内の非停止中サーバーのリストの順にトランスミッションを送信します。
- 起動時は、**radius-server host** コマンドを使用して設定されたように、フラグ設定されたサーバーがサーバー グループ リストで最初のサーバーになります。
- フラグ設定されたサーバーが停止中としてマークされている場合は（デッドタイムが0の場合でも）、フラグ設定されたサーバーの次にリストされた最初の非停止中サーバーがフラグ設定されたサーバーになります。
- フラグ設定されたサーバーが、リスト内の最後のサーバーで、停止中としてマークされている場合は、フラグ設定されたサーバーがリスト内で停止中としてマークされていない最初のサーバーになります。
- すべてのサーバーが停止中としてマークされている場合は、トランザクションが失敗して、フラグ設定されたサーバーへの変更が実施されません。
- フラグ設定されたサーバーが停止中としてマークされており、デッドタイマーが切れた場合は、何も行われません。

（注） トランスミッションのタイプ（チャレンジハンドシェーク認証プロトコル（CHAP）、Microsoft CHAP（MS-CHAP）、拡張可能認証プロトコル（EAP））によっては、1 つのサーバーを何度も往復しなければならない場合があります。これらの特別なトランザクションでは、サーバーのラウンドトリップの全シーケンスは、1つのトランスミッションと同じように処理されます。

RADIUS サーバーが停止中の場合

次の 1 と 2 の基準が満たされた場合に、サーバーを停止中としてマークすることができます。

1. **radius-server transaction max-tries** コマンドで指定された再送信回数を超えてサーバーが応答しなかった場合。
2. 設定されたタイムアウトまでどの要求にもサーバーが応答しなかった場合。両方の基準（これと上の基準）が満たされた場合にのみ、サーバーが停止中としてマークされます。デッドタイムが 0 の場合でも、サーバーを停止中としてマークすると、RADIUS サーバーの再試行方式順序変更システムに重大な影響を及ぼします。

RADIUS サーバー障害発生時順序変更の設定方法

RADIUS サーバー障害発生時順序変更の設定

このタスクを実行して、サーバー グループ内のあるサーバーを、最初のサーバーで障害が発生した場合に別のサーバーにトラフィックを転送するように設定します。

手順の概要

1. **enable**
2. **configure terminal**
3. **aaa new-model**
4. **radius-server retry method reorder**
5. **radius-server retransmit** {*retries*}
6. **radius-server transaction max-tries {** *number* **}**
7. **radius-server host { *hostname* | *ip-address* } [key *string*]**
8. **radius-server host { *hostname* | *ip-address* } [key *string*]**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**aaa new-model** 例： `Router (config)# aaa new-model`	AAA アクセス コントロール モデルをイネーブルにします。
ステップ 4	**radius-server retry method reorder** 例： 例： `Router (config)# radius-server retry method reorder`	サーバー グループ内の RADIUS トラフィック エントリの順序変更を指定します。
ステップ 5	**radius-server retransmit** {*retries*} 例： `Router (config)# radius-server retransmit 1`	Cisco IOS XE ソフトウェアが RADIUS サーバー ホストのリストを検索する回数の最大値を指定します。 *retries* 引数は、再送信の最大試行回数です。デフォルトは 3 回に設定されています。
ステップ 6	**radius-server transaction max-tries {** *number* **}** 例： `Router (config)# radius-server transaction max-tries 3`	RADIUS サーバー上で試行可能なトランザクション当たりのトランスミッション数の最大値を指定します。

	コマンドまたはアクション	目的
		number 引数は、トランザクション当たりのトランスミッション数の総数です。このコマンドが設定されなかった場合のデフォルトは 8 トランスミッションです。 （注） このコマンドは、特定のトランザクションに関係するすべての RADIUS サーバーに適用されます。
ステップ 7	**radius-server host { *hostname* | *ip-address* } [key *string*]** 例： `Router (config)# radius-server host 10.2.3.4 key radi23`	RADIUS サーバー ホストを指定します。 （注） **radius-server key** コマンドを発行することによって、サーバー単位キーが設定されていないすべての RADIUS サーバーのグローバル キーを設定することもできます。
ステップ 8	**radius-server host { *hostname* | *ip-address* } [key *string*]** 例： `Router (config)# radius-server host 10.5.6.7 key rad234`	RADIUS サーバー ホストを指定します。 （注） 少なくとも 2 つのサーバーを設定する必要があります。

RADIUS サーバー障害発生時順序変更のモニタリング

ルータ上でサーバー障害発生時順序変更プロセスをモニターするには、次のコマンドを使用します。

手順の概要

1. **enable**
2. **debug aaa sg-server selection**
3. **debug radius**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。

	コマンドまたはアクション	目的
ステップ 2	**debug aaa sg-server selection** 例： `Router# debug aaa sg-server selection`	ルータ内の RADIUS および TACACS+ サーバー グループ システムが特定のサーバーを選択している理由に関する情報を表示します。
ステップ 3	**debug radius** 例： `Router# debug radius`	ルータが特定の RADIUS サーバーを選択している理由に関する情報を表示します。

例

デバッグ 1

デバッグ 2

次の 2 つのデバッグ出力は、RADIUS サーバー障害発生時順序変更機能の動作を示しています。

次のサンプル出力では、RADIUS サーバー障害発生時順序変更機能が設定されています。サーバーの再送は0（したがって、次に設定されたサーバーへのフェールオーバー前に、各サーバーが一度だけ試行される）に設定され、トランザクション当たりのトランスミッション数は4（3回めのフェールオーバーでトランスミッション終了）に設定されています。サーバー グループ内で 3 番めのサーバー（10.107.164.118）が、3 回めのトランスミッション（2 回めのフェールオーバー）のトランザクションを受け入れています。

```
00:38:35: %SYS-5-CONFIG-I: Configured from console by console
00:38:53: RADIUS/ENCODE(OOOOOOOF) : ask "Username: "
00:38:53: RADIUS/ENCODE (0000000F) : send packet; GET-USER
00:38:58: RADIUS/ENCODE (0000000F) : ask "Password: "
00:38:58: RADIUS/ENCODE(0000000F) : send packet; GET-PASSWORD
00:38:59: RADIUS: AAA Unsupported [152] 4
00:38:59: RADIUS: 7474 [tt]
00:38:59: RADIUS (0000000F) : Storing nasport 2 in rad-db
00:38:59: RADIUS/ENCODE(0000000F) : dropping service type, "radius-server attribute 6
on-for-login-auth" is off
00:38:59: RADIUS (0000000F) : Config NAS IP: 0.0.0.0
00:38:59: RADIUS/ENCODE (0000000F) : acct-session-id: 15
00:38:59: RADIUS (0000000F) : sending
00:38:59: RADIUS/ENCODE: Best Local IP-Address 10.0.1.130 for Radius-Server 192.1.1.1
00:38:59: RAPIUS(0000000F) : Send Access-Request to 10.10.10.10:1645 id 21645/11, len
78
00:38:59: RADIUS:: authenticator 4481 E6 65 2D 5F 6F OA -lE F5 81 8F 4E 1478 9C
00:38:59: RADIUS: User-Name [1] 7 "username1"
00:38:59: RADIUS: User-Password [2] 18 *
00:38:59: RADIUS: NAS-Port fSl 6 2
00:~8:59: RADIUS: NAS-Port-Type [61] 6 Virtual [5]
00:38:59: RADIUS: Calling-Station-Id [31] 15 "10.19.192.23"
00:39:00: RADIUS: NAS-IP-Address [4] 6 10.0.1.130
```

```
00:39:02: RADIUS: Fail-over to (10.2.2.2:1645,1646) for id 21645/11
00:39:02: RADIUS/ENCODE: Best Local IP-Address 10.0.1.130 for Radius-Server 192.2.2.2
00:39:04: RADIUS: Fail-over to (10.107.164.118:1645,1646) for id 21645/11
00:39:04: RADIUS/ENCODE: Best Local IP-Address 10.0.1.130 for Radius-Server 128.107.164.118
00:39:05: RADIUS: Received from id 21645/11 10.107.164.118:1645, Access-Accept, len 26
00:39:05: RADIUS: authenticator 5609 56 F9 64 4E DF 19- F3 A2 DD 73 EE 3F 9826
00:39:05: RADIUS: Service-Type [6] 6 Login [1]
```

次のサンプル出力では、RADIUS サーバー障害発生時順序変更機能が設定されています。サーバーの再送は 0 に設定され、トランザクション当たりのトランスミッション数は 8 に設定されています。このトランザクションでは、サーバー 10.10.10.0 へのトランスミッションが 8 回めで失敗します。

```
00:42:30: RADIUS(00000011): Received from id 21645/13
00:43:34: RADIUS/ENCODE(00000012) : ask "Username: "
00:43:34: RADIUS/ENCODE(00000012) : send packet; GET-USER
00:43:39: RADIUS/ENCODE(00000012) : ask "Password: "
00:43:39: RADIUS/ENCODE(00000012) : send packet; GET-PASSWORD
00:43:40: RADIUS: AAA Unsupported [152] 4
00:43:40: RADIUS: 7474 [tt]
00:43:40: RADIUS(00000012) : Storing nasport 2 in rad-db
00:43:40: RADIUS/ENCODE(00000012): dropping service type, "radius-server attribute 6
on-for-login-auth" is off
00:43:40: RADIUS(00000012) : Co~fig NAS IP: 0.0.0.0
00:43:40: RADIUS/ENCODE(00000012) : acct-session-id: 18
00:43:40: RADIUS(00000012) : sending
00:43:40: RADIUS/ENCODE: Best Local IP-Address 10.0.1.130 for Radius-Server 10.107.164.118
 00:43:40: RADIUS(00000012) : Send Access-Request to 10.107.164.118:1645 id 21645/14,
len 78 00:43:40: RADIUS: authenticator B8 OA 51 3A AF A6 0018 -B3 2E 94 5E 07 OB 2A IF
00:43:40: RADIUS: User-Name [1] 7 "username1" 00:43:40: RADIUS: User-Password [2] 18 *
00:43:40: RADIUS: NAS-Port [5] 6 2
00:43:40: RADIUS: NAS-Port-Type [61] 6 Virtual [5] 00:43:40: RADIUS: Calling-Station-]d
 [31] 15 "172.19.192.23" 00:43:40: RADIUS: NAS-IP-Address [4] 6 10.0.1.130
00:43:42: RADIUS: Fail-over to (10.10.10.10:1645,1646) for id 21645/14
00:43:42: RADIUS/ENCODE: Best Local IP-Address 10.0.1.130 for Radius-Server 10.1.1.1
00:43:44: RADius: Fail-over to (10.2.2.2:1645,1646) for id 21645/14
00:43:44: RADIUS/ENCODE: Best Local IP-Address 10.0.1.130 for Radius-Server 10.2.2.2
00:43:46: RADIUS: Fail-over to (10.107.164.118:1645,1646) for id 21645/14
00:43:46: RADIUS/ENCODE: Best Local IP-Address 10.0.1.130 for Radius-Server 10.107.164.118
 00:43:48: RADIUS: Fail-over to (10.10.10.10:1645,1646) for id 21645/14
00:43:48: RADIUS/ENCODE: Best Local IP-Address 10.0.1.130 for Radius-Server 10.1.1.1
00:43:50: RADIUS: Fail-over to (10.2.2.2:1645,1646) for id 21645/14
00:43:50: RADIUS/ENCODE: Best Local IP-Address 10.0.1.130 for Radius-Server 10.2.2.2
00:43:52: RADIUS: Fail-over to (10.107.164.118:1645,1646) for id 21645/14
00:43:52: RADIUS/ENCODE: Best Local IP-Address 10.0.1.130 for Radius-Server 10.107.164.118
 00:43:54: RADIUS: Fail-over to (10.10.10.10:1645,1646) for id 21645/14
00:43:54: RADIUS/ENCODE: Best Local IP-Address 10.0.1.130 for Radius-Server 10.1.1.1
00:43:56: RADIUS: No response from (10.10.10.10:1645,1646) for id 21645/14 00:43:56:
RADIUS/DECODE: parse response no app start; FAIL 00:43:56: RADIUS/DECODE: parse response;
 FAIL
```

RADIUS サーバー障害発生時順序変更の設定例

RADIUS サーバーで障害発生時の順序変更を設定する例

次の設定例は、RADIUSサーバーが障害発生時に順序変更されるように設定されます。RADIUSサーバー上で試行可能なトランザクション当たりのトランスミッション数の最大値は6です。

```
aaa new-model

radius-server retry method reorder

radius-server retransmit 0

radius-server transaction max-tries 6

radius-server host 10.2.3.4 key rad123

radius-server host 10.5.6.7 key rad123
```

RADIUS サーバーが停止中の送信順序の決定

起動時に次のように設定し、

```
Router(config)# aaa new-model
Router(config)# radius-server retry method reorder
Router(config)# radius-server retransmit 0
Router(config)# radius-server transaction max-tries 6
Router(config)# radius-server host 10.2.3.4
Router(config)# radius-server host 10.5.6.7
```

両方のサーバーがダウンしているが、まだ、停止中としてマークされていない場合は、最初のトランザクションで、次のようなトランスミッションが見られます。

```
10.2.3.4
10.5.6.7
10.2.3.4
10.5.6.7
10.2.3.4
10.5.6.7
```

順序変更を次のように設定し、

```
Router(config)# aaa new-model
Router(config)# radius-server retry method reorder
Router(config)# radius-server retransmit 1
Router(config)# radius-server transaction max-tries 3
Router(config)# radius-server host 10.2.3.4
Router(config)# radius-server host 10.4.5.6
```

両方の RADIUS サーバーが RADIUS パケットに応答していないが、まだ、停止中としてマークされていない（NASの起動後のため）場合は、最初のトランザクションのトランスミッションが次のようになります。

```
10.2.3.4
10.2.3.4
10.4.5.6
```

以降のトランザクションは、別のパターンに従って転送されます。トランスミッションは、どちらか（または両方）のサーバーを停止中としてマークする基準が満たされているかどうかと、前述したサーバーのフラグ設定パターンによって異なります。

順序変更を次のように設定し、

```
Router(config)# aaa new-model
Router(config)# radius-server retry method reorder
Router(config)# radius-server retransmit 1
Router(config)# radius-server max-tries-per-transaction 8
Router(config)# radius-server host 10.1.1.1
Router(config)# radius-server host 10.2.2.2
Router(config)# radius-server host 10.3.3.3
Router(config)# radius-server timeout 3
```

RADIUS サーバー 10.1.1.1 が RADIUS パケットに応答していないが、まだ、停止中としてマークされておらず、残りの 2 つの RADIUS サーバーが動作中の場合は、次のように表示されます。

最初のトランザクションの場合：

```
10.1.1.1
10.1.1.1
10.2.2.2
```

サーバーが停止中としてマークされる前に任意のトランスミッションに対して開始された追加のトランザクションの場合：

```
10.1.1.1
10.1.1.1
10.2.2.2
```

その後開始されたトランザクションの場合：

```
10.2.2.2
```

その後で、サーバーの 10.2.2.2 と 10.3.3.3 もダウンした場合は、サーバーの 10.2.2.2 と 10.3.3.3 が停止中としてマークされる基準を満たすまで、次のようなトランスミッションが見られます。

```
10.2.2.2
10.2.2.2
10.3.3.3
10.3.3.3
10.1.1.1
10.1.1.1
10.2.2.2
10.2.2.2
```

この後に、トランスミッションが失敗し、方式リスト内で次の方式が使用されます（存在する場合）。

サーバーの 10.2.2.2 と 10.3.3.3 がダウンしたが、同時に、サーバー 10.1.1.1 が復旧した場合は、次のようになります。

```
10.2.2.2
10.2.2.2
10.3.3.3
10.3.3.3
10.1.1.1
```

その後で、サーバーの 10.2.2.2 と 10.3.3.3 が停止中としてマークされると、次のようになります。

```
10.1.1.1
```

その他の参考資料

関連資料

関連項目	マニュアル タイトル
RADIUS	『*Cisco IOS XE Security Configuration Guide: Securing User Services* , Release 2』の「Configuring RADIUS」
AAA コマンドと RADIUS コマンド	『*Cisco IOS Security Command Reference*』
AAA の有効化	『*Cisco IOS XE Security Configuration Guide: Securing User Services* , Release 2』の「Authentication, Authorization, and Accounting (AAA)」
セキュリティ コマンド	『*Cisco IOS* セキュリティ コマンド リファレンス』

標準

標準	タイトル
この機能でサポートされる新規の標準または変更された標準はありません。また、既存の標準のサポートは変更されていません。	--

MIB

MIB	MIB のリンク
この機能によってサポートされる新しい MIB または変更された MIB はありません。またこの機能による既存 MIB のサポートに変更はありません。	選択したプラットフォーム、Cisco IOS XE ソフトウェア リリース、およびフィーチャ セットの MIB の場所を検索しダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

RFC

RFC	タイトル
この機能によりサポートされた新規 RFC または改訂 RFC はありません。またこの機能による既存 RFC のサポートに変更はありません。	--

シスコのテクニカル サポート

説明	リンク
シスコのサポート Web サイトでは、シスコの製品やテクノロジーに関するトラブルシューティングにお役立ていただけるように、マニュアルやツールをはじめとする豊富なオンライン リソースを提供しています。 お使いの製品のセキュリティ情報や技術情報を入手するために、Cisco Notification Service（Field Notice からアクセス）、Cisco Technical Services Newsletter、Really Simple Syndication（RSS）フィードなどの各種サービスに加入できます。 シスコのサポート Web サイトのツールにアクセスする際は、Cisco.com のユーザ ID およびパスワードが必要です。	http://www.cisco.com/en/US/support/index.html

RADIUS サーバー障害発生時順序変更の機能情報

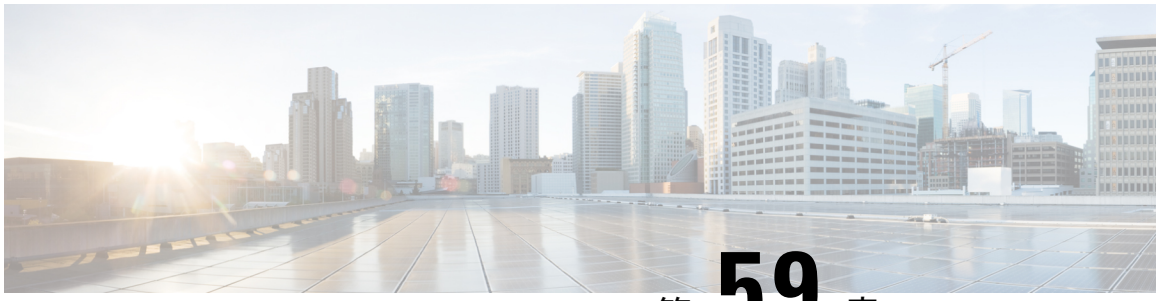
次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだ

けを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *84 : RADIUS* サーバー障害発生時順序変更の機能情報

機能名	リリース	機能情報
RADIUS サーバー障害発生時順序変更	Cisco IOS XE Release 2.1	RADIUS サーバー障害発生時順序変更機能は、高負荷期間またはサーバーで障害が発生した場合に、サーバー グループ内の別のサーバーへのフェールオーバーを提供します。 この機能は、Cisco IOS XE Release 2.1 で Cisco ASR 1000 シリーズ アグリゲーション サービス ルータに導入されました。 この機能により、次のコマンドが導入または変更されました。 **debug aaa sg-server selection, radius-server retry method reorder, radius-server transaction max-tries.**



第 59 章

アカウンティングの RADIUS 個別再送信カウンタ

RADIUS：アカウンティングの個別再送信カウンタ機能を使用すると、指数バックオフ再送信を設定することができます。つまり、標準設定された再送信が再試行された後に、ルータは、設定された最大間隔に達するまで各再送信の失敗ごとに間隔を2倍にして試行を継続します。この機能により、RADIUSサーバが復旧したときにサーバに負荷をかけすぎることなく、長時間にわたってアカウンティング要求を再送信することができます。

アカウンティングの RADIUS 個別再送信カウンタの制約事項

次のタスクでは、ルータのメモリが過剰に消費されます。

- ルータ上でこの機能を高い発信レートで設定。
- **aaa accounting send stop-record authentication failure** コマンドを設定：これにより、RADIUSサーバーがダウンしている間、認証に失敗する各ユーザーに対してアカウンティングレコードと RADIUS パケットが生成されます。
- 中間アカウンティングの設定：新しいアカウンティング レコードが生成され、ルータに保存されます。

アカウンティングの RADIUS 個別再送信カウンタに関する情報

多くの環境では、認証およびアカウンティングに単一のRADIUSサーバーが使用されます。このサーバーが約24時間にわたってダウンすると、認証、認可、およびアカウンティング（AAA）がすべての再送信を行った後に、ルータ上に保持されているユーザーのアカウンティング レコードは失われます。この機能を導入する前に、再送信の再試行が最大100回に設定され、タイムアウトが 1,000 秒に設定されている可能性があります。このような設定では、ルータ上のアカウンティング レコードが24時間保持されますが、タイムアウトが1,000秒の設定は、ネットワークの輻輳が原因でRADIUSサーバーに接続できないときに問題が発生するため、適切ではありません。

RADIUS：アカウンティングの個別再送信カウンタ機能を使用すると、指数バックオフ再送信を設定することができます。つまり、標準設定された再送信が再試行された後に、ルータは、設定された最大間隔に達するまで各再送信の失敗ごとに間隔を2倍にして試行を継続します。この機能により、RADIUSサーバーが復旧したときにサーバーに負荷をかけすぎることなく、長時間にわたってアカウンティング要求を再送信することができます。

この機能は、グローバルに設定（**radius-server backoff exponential** コマンドを使用）、サーバーごとに設定（**radius-server host** コマンドを使用）、またはグループごとに設定（**backoff exponential** コマンドを使用）できます。

利点

この機能を使用すると、RADIUSサーバーまたはサーバーへの接続がダウンし、アカウンティング応答の確認がない場合に、RADIUS クライアント（ルータ）がアカウンティング要求をRADIUSサーバーに送信する時間を延長できます。この機能により、アカウンティング レコードを最大 24 時間、ルータ上に保持できます。

アカウンティングの RADIUS 個別再送信カウンタの設定方法

アカウンティングの再送信カウンタのグローバル設定または RADIUS ホストごとの設定

拡張された期間での RADIUS 再送信の指数バックオフをグローバルおよびRADIUS ホストごとに設定するには、次の手順を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. Router(config)# **radius-server backoff exponential** [**max-delay** *minutes*] [**backoff-retry** *retransmits*
4. Router(config)# **radius-server host** {*hostname* | *ip-address*} [**test username** *user-name*] [**auth-port** *port-number*] [**ignore-auth-port**] [**acct-port** *port-number*] [**ignore-acct-port**] [**timeout** *seconds*] [**retransmit** *retries*] [**key** *string*] [**alias** {*hostname* | *ip-address*}] [**idle-time** *seconds*] [**backoff exponential** {**backoff-retry** *number-of-retransmits* | **key** *encryption-key* | **max-delay** *minutes*}]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードを開始します。 パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	Router(config)# **radius-server backoff exponential** [**max-delay** *minutes*] [**backoff-retry** *retransmits* 例： `Router (config)# radius-server backoff exponential max-delay 60 backoff-retry 32`	アカウンティング要求の指数バックオフ再送信をルータで設定します。
ステップ 4	Router(config)# **radius-server host** {*hostname* | *ip-address*} [**test username** *user-name*] [**auth-port** *port-number*] [**ignore-auth-port**] [**acct-port** *port-number*] [**ignore-acct-port**] [**timeout** *seconds*] [**retransmit** *retries*] [**key** *string*] [**alias** {*hostname* | *ip-address*}] [**idle-time** *seconds*] [**backoff exponential** {**backoff-retry** *number-of-retransmits* | **key** *encryption-key* | **max-delay** *minutes*}] 例： `Router (config)# radius-server host 192.0.2.1 test username test1 auth-port 1645 acct-port 1646`	RADIUS サーバー ホストを指定し、アカウンティング要求の指数バックオフ再送信を行うように設定します。

アカウンティングの再送信カウンタの RADIUS サーバー グループごとの設定

RADIUS サーバー グループごとに拡張された期間で RADIUS 再送信の指数バックオフを設定するには、次の手順を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. Router(config)# **aaa group server radius** *group-name*
4. Router(config -sg-radius)# **backoff exponential max-delay** *minutes*] [**backoff-retry** *retransmits*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードを開始します。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Router (config)# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	Router(config)# **aaa group server radius** *group-name*	異なる RADIUS サーバー ホストを別々のリストと方式にグループ化し、server-group RADIUS コンフィギュレーション モードを開始します。
ステップ 4	Router(config -sg-radius)# **backoff exponential max-delay** *minutes*] [**backoff-retry** *retransmits*	RADIUS サーバー グループごとのアカウンティング要求の指数バックオフ再送信をルータで設定します。

再送信設定の確認

機能を確認するには、次のいずれかの EXEC コマンドを使用します。

手順の概要

1. **enable**
2. **debug radius**
3. **show accounting**
4. **show radius statistics**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードを開始します。 • パスワードを入力します（要求された場合）。
ステップ 2	**debug radius** 例： `Router# debug radius`	RADIUS 関連の情報を表示します。
ステップ 3	**show accounting** 例： `Router# show accounting`	すべてのアクティブセッションを表示し、アカウントがアクティブな機能のすべてのアカウンティングレコードを出力します。
ステップ 4	**show radius statistics** 例： `Router# show radius statistics`	アカウンティング パケットについての RADIUS 統計情報を表示します。

アカウンティングの RADIUS 個別再送信カウンタの設定例

アカウンティングの再送信カウンタの包括的な設定例

次の例は、ルータでアカウンティング要求の指数バックオフ再送信を設定する方法を示します。この例では、指数バックオフはグローバル（**radius-server backoff exponential** コマンドを使用）および RADIUS サーバーホスト「172.107.164.206」（**radius-server host** コマンドを使用）に設定されています。

```
aaa new-model
aaa authentication login default group radius
aaa authentication ppp default group radius
aaa authorization exec default group radius
aaa authorization network default group radius
aaa accounting send stop-record authentication failure
aaa accounting update periodic 1
aaa accounting network default start-stop group radius
!
interface BRI1/0
 ip address 10.0.0.2 255.0.0.0
 encapsulation ppp
 no ip mroute-cache
```

```
 dialer idle-timeout 0
 dialer-group 1
 isdn switch-type basic-5ess
!
radius-server host 172.107.164.206 auth-port 1645 acct-port 1646 backoff exponential
max-delay 60 backoff-retry 32
radius-server backoff exponential max-delay 60 backoff-retry 32
radius-server retransmit 3
radius-server key rad123
end
```

サーバーごとの設定例

次に、サーバー単位で指数バックオフ再送信を有効化する例を示します。この例では、再送信は3回の再試行に設定され、タイムアウトは5秒に設定されると想定します。つまり、RADIUS要求は 5 秒間の遅延で 3 回送信されます。その後、ルータは、再試行が 32 回になるまで、各再試行時に遅延間隔を2倍にしてRADIUS要求の再送信を継続します。ルータは、再送信間隔が設定された 60 分を超えると、間隔を 2 倍にする操作を中止し、その後は 60 分ごとに送信します。

```
radius-server host foo.xyz.com backoff exponential max-delay 60 backoff-retry 32
```

このコマンドを有効にすると、次のように再送信が実行されます（「t」は秒単位）。

```
t = 0 req sent
t = 5 retrans 1
t = 10 retrans 2
t = 15 retrans 3
t = 25 retrans 4
t = 45 retrans 5
t = 85 retrans 6
t = 165 retrans 7
t = 325 retrans 8
t = 645 retrans 9
t = 1285 retrans 10
t= 2565 retrans 11
t = 5125 retrans 12
t = 8725 retrans 13 (The interval has stabilized to 60 minutes here).
t = 12325 retrans 14 till retransmit 35
```

すべての再送信が完了すると、RADIUS要求は、通常の再送信がすべて完了したときと同じパスに従います。

その他の参考資料

次の項で、RADIUS：アカウンティングの個別再送信カウンタに関する参考資料を紹介します。

関連資料

関連項目	マニュアル タイトル
RADIUSおよびAAAアカウンティング設定のタスクとコマンド	• 「Configuring RADIUS」および「Configuring Accounting」機能モジュール。 • 『*CiscoOS Security Command Reference*』

標準

標準	タイトル
なし	--

MIB

MIB	MIB のリンク
なし	選択したプラットフォーム、Cisco IOS リリース、およびフィーチャ セットに関する MIB を探してダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

RFC

RFC	タイトル
この機能でサポートが追加または変更された RFC はありません。	--

シスコのテクニカル サポート

説明	リンク
シスコのサポート Web サイトでは、シスコの製品やテクノロジーに関するトラブルシューティングにお役立ていただけるように、マニュアルやツールをはじめとする豊富なオンライン リソースを提供しています。 お使いの製品のセキュリティ情報や技術情報を入手するために、Cisco Notification Service（Field Notice からアクセス）、Cisco Technical Services Newsletter、Really Simple Syndication（RSS）フィードなどの各種サービスに加入できます。 シスコのサポート Web サイトのツールにアクセスする際は、Cisco.com のユーザ ID およびパスワードが必要です。	http://www.cisco.com/en/US/support/index.html

アカウンティングの RADIUS 個別再送信カウンタの機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *85 : RADIUS* の機能情報：アカウンティングの個別再送信カウンタ

機能名	リリース	機能情報
RADIUS：アカウンティングの個別再送信カウンタ	12.2(15)B 12.2(33)SRC	RADIUS：アカウンティングの個別再送信カウンタ機能を使用すると、指数バックオフ再送信を設定することができます。つまり、標準設定された再送信が再試行された後に、ルータは、設定された最大間隔に達するまで各再送信の失敗ごとに間隔を 2 倍にして試行を継続します。この機能により、RADIUS サーバーが復旧したときにサーバーに負荷をかけすぎることなく、長時間にわたってアカウンティング要求を再送信することができます。 次のコマンドが導入または変更されました。**backoff exponential**、**radius-server host**、**radius-server backoff exponential**

第 60 章

RADIUS VC ロギング

RADIUS 仮想回線（VC）ロギングを使用すると、着信サブスクライバ セッションの仮想パス インターフェイス（VPI）と仮想回線インターフェイス（VCI）を Cisco IOS XE で正確に記録できます。

RADIUS VC ロギングを有効にすると、RADIUS ネットワーク アクセス サーバー（NAS）のポート フィールドが拡張され、VPI/VCI 情報を伝送するように変更されます。この情報は、セッションの起動時に作成された RADIUS アカウンティング レコードに記録されます。

RADIUS VC ロギングの設定方法

NSP での NME インターフェイス IP アドレスの設定

RADIUS アカウンティング パケットの NAS-IP-Address フィールドには、NME がシャットダウンされた場合でも、ネットワーク サービス プロバイダー（NSP）のネットワーク管理イーサネット（NME）ポートの IP アドレスが含まれています。IP アドレスを取得するためにネットワーク ルート プロセッサ（NRP）で DHCP サーバーを使用しない場合、静的 IP アドレスを設定する必要があります。次の手順を実行して、静的に結合された NME IP アドレスを設定します。

手順の概要

1. **enable**
2. **configure terminal**
3. **interface BVI** *bridge-group*
4. **ip address** *address subnet*
5. **exit**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface BVI** *bridge-group* 例： `Router(config)# interface BVI1`	結合されたブリッジグループ仮想インターフェイス（BVI）NME インターフェイスを選択して、インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	**ip address** *address subnet* 例： `Router(config-if)# ip address 209.165.200.225 255.255.255.224`	静的 IP アドレスとサブネットワーク アドレスを設定します。
ステップ 5	**exit** 例： `Router(config)# exit`	インターフェイス コンフィギュレーション モードを終了します。

NME IP アドレスの設定

結合された NME インターフェイスの代わりに、ギガビット イーサネット ポートを別の NME インターフェイスとして使用できます。次の手順を実行して NME IP アドレスを設定します。

手順の概要

1. **enable**
2. **configure terminal**
3. **interface GigabitEthernet** *number*
4. **ip address** *address mask*
5. **exit**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface GigabitEthernet** *number* 例： `Router(config)# interface GigabitEthernet 0/0/0`	NME インターフェイスを選択します。
ステップ 4	**ip address** *address mask* 例： `Router(config-if)# ip address 209.165.200.225 255.255.255.224`	静的 IP アドレスとサブネットワーク アドレスを設定します。 （注） NRP で PVC を設定する前に、NME IP アドレスを設定する必要があります。そうしないと、RADIUS アカウンティング パケットの NAS-IP-Address フィールドに正しくない IP アドレスが含まれます。
ステップ 5	**exit** 例： `Router(config)# exit`	設定モードを終了します。

NRP での RADIUS VC ロギングの設定

次の手順を実行して RADIUS VC ロギングを設定します。

手順の概要

1. **enable**
2. **configure terminal**
3. **radius-server attribute nas-port format d**
4. **exit**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**radius-server attribute nas-port format d** 例： `Router(config)# radius-server attribute nas-port format d`	NAS ポート フィールドに ATM VC（仮想回線）拡張形式を選択します。
ステップ 4	**exit** 例： `Router(config)# exit`	インターフェイス コンフィギュレーション モードを終了します。

NME インターフェイス IP アドレスの確認

NME IP アドレスを確認するには、NSP で **show interface bvi1** または **show interface e0/0/0** EXEC コマンドを入力します。インターネット アドレス ステートメント（矢印で示されます）を確認します。

```
Router# show interface bvi1BVI1 is up, line protocol is up
  Hardware is BVI, address is 0010.7ba9.c783 (bia 0000.0000.0000)
    MTU 1500 bytes, BW 10000 Kbit, DLY 5000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  ARP type:ARPA, ARP Timeout 04:00:00
  Last input never, output never, output hang never
  Last clearing of "show interface" counters never
  Queueing strategy:fifo
  Output queue 0/0, 0 drops; input queue 0/75, 0 drops
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     1540 packets input, 302775 bytes, 0 no buffer
     Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
     545 packets output, 35694 bytes, 0 underruns
     0 output errors, 0 collisions, 0 interface resets
     0 output buffer failures, 0 output buffers swapped out
```

NRP での RADIUS VC ロギングの確認

RADIUS サーバー上の RADIUS VC ロギングを確認するには、RADIUS アカウンティング パケットを検査します。RADIUS VC ロギングが Cisco IOS XE ソフトウェアで有効になっている場合、RADIUS アカウンティング パケットは次の例のように表示されます。

```
Wed Jun 16 13:57:31 1999
NAS-IP-Address = 192.168.100.192
NAS-Port = 268566560
NAS-Port-Type = Virtual
User-Name = "cisco"
Acct-Status-Type = Start
Service-Type = Framed
Acct-Session-Id = "1/0/0/2.32_00000009"
Framed-Protocol = PPP
Framed-IP-Address = 172.16.7.254
Acct-Delay-Time = 0
```

NAS-Port フィールドは、RADIUS VC ロギングが有効であることを示します。この行が出力に表示されない場合、RADIUS VC ロギングは Cisco IOS XE ソフトウェアで有効になっていません。

また、Acct-Session-Id フィールドでは、着信 NSP インターフェイスと VPI/VCI 情報を次の形式で識別します。

```
Acct-Session-Id = "slot/subslot/port/VPI.VCI_acct-session-id"
```

RADIUS VC ロギングの設定例

NSP での NME インターフェイス IP アドレスの設定例

次に、ブリッジグループ仮想インターフェイスの静的 IP およびサブネットワーク アドレスを設定する例を示します。

```
Router> enable
Router# configure terminal
Router(config)# interface BVI1
ip address 209.165.200.225 255.255.255.224
Router(config)# exit
```

NME IP アドレスの設定例

次に、GigabitEthernet インターフェイスを設定する例を示します。

```
Router> enable
Router# configure terminal
Router(config)# interface GigabitEthernet 0/0/0
Router(config-if)# ip address 209.165.200.225 255.255.255.224
Router(config)# exit
```

NRP での RADIUS VC ロギングの設定例

次に、NRP で RADIUS VC ロギングを設定する例を示します。

```
Router> enable
Router# configure terminal
Router(config)# radius-server attribute nas-port format d
Router(config)# exit
```

その他の参考資料

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『*Cisco IOS Master Security Commands List, All Releases*』

MIB

MIB	MIB のリンク
なし	選択したプラットフォーム、Cisco IOS XE ソフトウェア リリース、およびフィーチャセットの MIB の場所を検索しダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

RFC

RFC	タイトル

シスコのテクニカル サポート

説明	リンク
シスコのサポート Web サイトでは、シスコの製品やテクノロジーに関するトラブルシューティングにお役立ていただけるように、マニュアルやツールをはじめとする豊富なオンライン リソースを提供しています。 お使いの製品のセキュリティ情報や技術情報を入手するために、Cisco Notification Service（Field Notice からアクセス）、Cisco Technical Services Newsletter、Really Simple Syndication（RSS）フィードなどの各種サービスに加入できます。 シスコのサポート Web サイトのツールにアクセスする際は、Cisco.com のユーザ ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

RADIUS VC ロギングの機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *86 :* ゾーンベース ポリシー ファイアウォールの機能情報

機能名	リリース	機能の設定情報
RADIUS VC ロギング	Cisco IOS XE Release 3.1S	RADIUS 仮想回線（VC）ロギングを使用すると、着信サブスクライバ セッションの仮想パス インターフェイス（VPI）と仮想回線インターフェイス（VCI）を Cisco IOS XE ソフトウェアで正確に記録できます。

第 61 章

RADIUS 集中型フィルタ管理

RADIUS 集中型フィルタ管理機能は、ACL の設定と管理を容易にするフィルタ サーバーを導入しています。このフィルタ サーバーは、集中型 RADIUS リポジトリおよび管理ポイントとして機能します。ユーザーは、アクセス コントロール リスト（ACL）フィルタを集中的に管理および設定できます。

RADIUS 集中型フィルタ管理の前提条件

- 新しい RADIUS VSA をサポートしていないサーバーにディレクトリ ファイルを追加しなければならない場合があります。サンプルのディクショナリとベンダー ファイルについては、このドキュメントの後半にある「RADIUS ディクショナリとベンダー ファイルの例」を参照してください。

ディレクトリ ファイルを追加する必要がある場合は、RADIUS サーバーが非標準であり、新しく導入された VSA を送信可能であること確認してください。

- リモート ユーザーがダイヤルインして IP 接続を確立できるように、RADIUS ネットワーク認証をセットアップすることができます。

RADIUS 集中型フィルタ管理の制約事項

この機能では複数の方式リストがサポートされていません。単一のグローバル フィルタ方式リストが設定できるだけです。

RADIUS 集中型フィルタ管理に関する情報

RADIUS 集中型フィルタ管理機能以前は、ホールセール プロバイダー（ACL などの顧客サービスに対して特別料金を課している）が、顧客の網羅的な ACL の適用を阻止できました。この行為は、ルータの性能や他の顧客に影響を与える可能性があります。この機能では、ACL 管理用の集中型管理ポイント（フィルタ サーバー）が導入されます。フィルタ サーバーは、ACL 設定用の集中型 RADIUS リポジトリとして機能します。

フィルタ サーバーとして使用されている RADIUS サーバーがアクセス認証に使用されているサーバーと同じかどうかに関係なく、ネットワーク アクセス サーバー（NAS）はフィルタ サーバーに対して別のアクセス要求を開始します。設定されていれば、NAS は、認証ユーザー名と 2 つめのアクセス要求用のフィルタ サーバー パスワードとして、フィルタ ID 名を使用します。RADIUS サーバーは、フィルタ ID 名を認証して、access-accept 応答内に必要なフィルタリング設定を返そうとします。

ACL のダウンロードには時間がかかるため、NAS 上でローカル キャッシュが維持されます。ローカル キャッシュ上に ACL 名が存在する場合は、フィルタ サーバーに問い合わせることなくその設定が使用されます。

（注） キャッシュが適切に設定されていれば、遅延は最小限に抑えられるはずです。ただし、フィルタが必要な最初のダイヤルイン ユーザーは必ず待たされることになります。これは、初めての場合は、ACL 設定が読み込まれるためです。

キャッシュ管理

グローバル フィルタ キャッシュは最後に ACL をダウンロードした NAS 上で維持されます。そのため、ユーザーは、過負荷状態の RADIUS サーバーに対して同じ ACL 設定情報を何度も要求する必要がありません。ユーザーは、次の基準が満たされている場合にキャッシュをフラッシュする必要があります。

- エントリが新しいアクティブ コールに関連付けられた後に、そのエントリに関連付けられたアイドル タイマーがリセットされる（そのように設定されている場合）。
- アイドル時間スタンプの期限が切れたエントリが削除される。
- グローバル キャッシュのエントリが指定された最大数に到達した後に、アイドル タイマーがアイドル時間限界に最も近いエントリが削除される。

1 つのタイマーがすべてのキャッシュ エントリの管理に使用されます。このタイマーは、最初のキャッシュ エントリの作成時に開始され、リブートされるまで定期的に実行されます。タイマーの期間は、キャッシュ アイドル タイマーの設定時に指定された最小粒度に対応し、毎分期限切れになります。タイマーが 1 つしかないことによって、ユーザーは、キャッシュ エントリごとに別々のタイマーを管理する必要がありません。

（注） 単一のタイマーは、タイマーの期限切れの精度に欠けます。約 50% のタイマー粒度に平均誤差が含まれています。タイマー粒度を下げると平均誤差も下がりますが、性能が低下する可能性があります。キャッシュ管理には正確なタイミングが必要ないため、誤差遅延を受け入れる必要があります。

新しいベンダー固有属性のサポート

この機能は、次の 2 つのカテゴリに分類可能な 3 つの新しいベンダー固有属性（VSA）のサポートを導入しています。

- ユーザー プロファイルの拡張
  - Filter-Required（50）：指定されたフィルタが見つからなかった場合にコールを許可するかどうかを指定します。存在する場合は、この属性が、すべての認証、許可、アカウンティング（AAA）フィルタ方式リストの後に適用されます。
- 疑似ユーザー プロファイルの拡張
  - Cache-Refresh（56）：エントリが新しいセッションから参照されるたびにキャッシュ エントリを更新するかどうかを指定します。この属性は、**cache refresh** コマンドに対応します。
  - Cache-Time（57）：キャッシュ エントリのアイドル タイムアウトを分単位で指定します。この属性は、**cache clear age** コマンドに対応します。

（注） すべての RADIUS 属性が、すべてのコマンドライン インターフェイス（CLI）設定よりも優先されます。

RADIUS 用の集中型フィルタ管理の設定方法

RADIUS ACL フィルタ サーバーの設定

RADIUS ACL フィルタ サーバーを有効にするには、グローバル コンフィギュレーション モードで次のコマンドを使用します。

コマンド	目的
`Router(config)# aaa authorization cache filterserver default methodlist[methodlist2...]`	AAA 認可キャッシュと、RADIUS フィルタ サーバーからの ACL 設定のダウンロードを有効にします。 • **default** ：デフォルト認可リスト。 • *methodlist* [*methodlist2...*] : **password** コマンド ページに列挙されたキーワードの 1 つ。

フィルタ キャッシュの設定

この項の次の手順に従って、AAA フィルタ キャッシュを設定します。

手順の概要

1. **enable**
2. **configure terminal**
3. Router(config)# **aaa cache filter**
4. Router(config-aaa-filter)# **password 0 7**} *password*
5. Router(config-aaa-filter)# **cache disable**
6. Router(config-aaa-filter)# **cache clear age** *minutes*
7. Router(config-aaa-filter)# **cache refresh**
8. Router(config-aaa-filter)# **cache max** *number*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	Router(config)# **aaa cache filter**	フィルタ キャッシュ設定を有効にして、AAA フィルタ コンフィギュレーション モードに入ります。
ステップ 4	Router(config-aaa-filter)# **password 0 7**} *password*	（任意）フィルタ サーバー認証要求に使用されるオプション パスワードを指定します。 **0** ：暗号化されていないパスワードが後に続くことを示します。

	コマンドまたはアクション	目的
		7 ：非表示パスワードが後に続くことを示します。 *password* ：暗号化されていない（クリア テキスト）パスワード。 （注） パスワードが指定されなかった場合は、デフォルト パスワード（「cisco」）が有効になります。
ステップ 5	Router(config-aaa-filter)# **cache disable**	（任意）キャッシュを無効にします。
ステップ 6	Router(config-aaa-filter)# **cache clear age** *minutes*	（任意）キャッシュ エントリの期限が切れ、キャッシュがクリアされるタイミングを分単位で指定します。 *minutes* ：0 ～ 4294967295 の任意の値。 （注） 時間が指定されなかった場合は、デフォルト（1400 分（1 日））が有効になります。
ステップ 7	Router(config-aaa-filter)# **cache refresh**	（任意）新しいセッションの開始時点でキャッシュ エントリをリフレッシュします。このコマンドは、デフォルトでイネーブルになっています。この機能をディセーブルにするには、**no cache refresh** コマンドを使用します。
ステップ 8	Router(config-aaa-filter)# **cache max** *number*	（任意）キャッシュで特定のサーバー用に維持できるエントリの絶対数を制限します。 *number* ：キャッシュに含めることが可能なエントリの最大数。0 ～ 4294967295 の任意の値。 （注） 数値が指定されなかった場合は、デフォルト（100 エントリ）が有効になります。

フィルタ キャッシュの確認

キャッシュ ステータスを表示するには、**show aaa cache filterserver** EXEC コマンドを使用します。次に、**show aaa cache filterserver** コマンドの出力例を示します。

```
Router# show aaa cache filterserver
Filter     Server          Age Expires Refresh Access-Control-Lists
-------------------------------------------------------------------------------
aol        10.2.3.4          0    1440     100 ip in icmp drop
                                                ip out icmp drop
                                                ip out forward tcp dstip 1.2.3...
```

```
msn         10.3.3.4          N/A   Never       2 ip in tcp drop
msn2        10.4.3.4          N/A   Never       2 ip in tcp drop
vone        10.5.3.4          N/A   Never       0 ip in tcp drop
```

（注） **show aaa cache filterserver** コマンドは、特定のフィルタが参照またはリフレッシュされた回数を表示します。この機能は、実際に使用されるフィルタを決定するために管理者が使用します。

トラブルシューティングのヒント

フィルタ キャッシュ設定のトラブルシューティングを支援するために、**debug aaa cache filterserver** 特権 EXEC コマンドを使用します。**debug aaa cache filterserver** コマンドのサンプル出力を確認するには、このドキュメントの後半にある「デバッグ出力の例」を参照してください。

フィルタ キャッシュのモニタリングと維持

フィルタ キャッシュをモニターおよび維持するには、次の EXEC コマンドの少なくとも 1 つを使用します。

コマンド	目的
Router# **clear aaa cache filterserver acl** [*filter-name*	特定のフィルタまたはすべてのフィルタのキャッシュ ステータスをクリアします。
Router# **show aaa cache filterserver**	キャッシュ ステータスを表示します。

RADIUS 集中型フィルタ管理の設定例

NAS の設定例

次の例は、キャッシュ フィルタリング用の NAS の設定方法を示しています。この例では、最初に、サーバー グループの「mygroup」に接続されます。応答がない場合は、デフォルト RADIUS サーバーに接続されます。それでも応答がない場合は、ローカル フィルタ ケアに接続されます。最終的に、フィルタが解決できなければ、コールが受け入れられます。

```
aaa authorization cache filterserver group mygroup group radius local none
!
aaa group server radius mygroup
 server 10.2.3.4
 server 10.2.3.5
!
radius-server host 10.1.3.4
```

```
!
aaa cache filter
 password mycisco
 no cache refresh
 cache max 100
!
```

RADIUS サーバーの設定例

次の例は、NAS にダイヤルしているリモート ユーザー「user1」のサンプル RADIUS 設定です。

```
myfilter Password = "cisco"
Service-Type = Outbound,
Ascend:Ascend-Call-Filter = "ip in drop srcip 10.0.0.1/32 dstip 10.0.0.10/32 icmp",
Ascend:Ascend-Call-Filter = "ip in drop srcip 10.0.0.1/32 dstip 10.0.0.10/32 tcp dstport
 = telnet",
Ascend:Ascend-Cache-Refresh = Refresh-No,
Ascend:Ascend-Cache-Time = 15
user1 Password = "cisco"
Service-Type = Framed,
Filter-Id = "myfilter",
Ascend:Ascend-Filter-Required = Filter-Required-Yes,
```

RADIUS ディクショナリとベンダー ファイルの例

次の例は、新しい VSA 用のサンプル RADIUS 辞書ファイルです。この例では、辞書ファイルが Merit サーバー用です。

```
dictionary file:
Ascend.attr Ascend-Filter-Required 50 integer (*, 0, NOENCAPS)
Ascend.attr Ascend-Cache-Refresh   56 integer (*, 0, NOENCAPS)
Ascend.attr Ascend-Cache-Time      57 integer (*, 0, NOENCAPS)
Ascend.value Ascend-Cache-Refresh Refresh-No  0
Ascend.value Ascend-Cache-Refresh Refresh-Yes 1
Ascend.value Ascend-Filter-Required  Filter-Required-No  0
Ascend.value Ascend-Filter-Required  Filter-Required-Yes 1
vendors file:
50     50
56     56
57     57
```

デバッグ出力例

次に、**debug aaa cache filterserver** コマンドの出力例を示します。

```
Router# debug aaa cache filterserver

AAA/FLTSV: need "myfilter" (fetch), call 0x612DAC64
AAA/FLTSV: send req, call 0x612DAC50
AAA/FLTSV: method SERVER_GROUP myradius
AAA/FLTSV: recv reply, call 0x612DAC50 (PASS)
AAA/FLTSV: create cache
AAA/FLTSV: add attr "call-inacl"
AAA/FLTSV: add attr "call-inacl"
```

```
AAA/FLTSV: add attr "call-inacl"
AAA/FLTSV: skip attr "filter-cache-refresh"
AAA/FLTSV: skip attr "filter-cache-time"
AAA/CACHE: set "AAA filtserv cache" entry "myfilter" refresh? no
AAA/CACHE: set "AAA filtserv cache" entry "myfilter" cachetime 15
AAA/FLTSV: add attr to list "call-inacl" call 0x612DAC64
AAA/FLTSV: add attr to list "call-inacl" call 0x612DAC64
AAA/FLTSV: add attr to list "call-inacl" call 0x612DAC64
AAA/FLTSV: PASS call 0x612DAC64
AAA/CACHE: timer "AAA filtserv cache", next in 10 secs (0 entries)
AAA/CACHE: timer "AAA filtserv cache", next in 10 secs (1 entry)
AAA/CACHE: destroy "AAA filtserv cache" entry "myfilter"
AAA/CACHE: timer "AAA filtserv cache", next in 10 secs (0 entries)
```

その他の参考資料

次の項で、RADIUS 集中型フィルタ管理に関する参考資料を紹介します。

関連資料

関連項目	マニュアル タイトル
認可の設定	「Configuring Authorization」機能モジュール。
RADIUS の設定	「Configuring RADIUS」機能モジュール
認可コマンド	『*Cisco IOS Security Command Reference*』

標準

標準	タイトル
なし	--

MIB

MIB	MIB のリンク
なし	選択したプラットフォーム、Cisco IOS リリース、およびフィーチャ セットに関する MIB を探してダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

RFC

RFC	タイトル
なし	--

シスコのテクニカル サポート

説明	リンク
シスコのサポート Web サイトでは、シスコの製品やテクノロジーに関するトラブルシューティングにお役立ていただけるように、マニュアルやツールをはじめとする豊富なオンライン リソースを提供しています。 お使いの製品のセキュリティ情報や技術情報を入手するために、Cisco Notification Service（Field Notice からアクセス）、Cisco Technical Services Newsletter、Really Simple Syndication（RSS）フィードなどの各種サービスに加入できます。 シスコのサポート Web サイトのツールにアクセスする際は、Cisco.com のユーザ ID およびパスワードが必要です。	http://www.cisco.com/en/US/support/index.html

RADIUS 集中型フィルタ管理の機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *87 : RADIUS* 集中型フィルタ管理の機能情報

機能名	リリース	機能情報
RADIUS集中型フィルタ管理	Cisco IOS XE Release 3.9S	RADIUS集中型フィルタ管理機能は、ACLの設定と管理を容易にするフィルタ サーバーを導入しています。このフィルタ サーバーは、集中型RADIUSリポジトリおよび管理ポイントとして機能します。ユーザーは、アクセス コントロール リスト（ACL）フィルタを集中的に管理および設定できます。 この機能により、次のコマンドが導入または変更されました。**aaa authorization cache filterserver**、**aaa cache filter, cache clear age, cache disable, cache refresh**、**clear aaa cache filterserver acl**、**debug aaa cache filterserver**、**password**、**show aaa cache filterserver.**

第 62 章

RADIUS EAP サポート

RADIUS EAP サポート機能は、ユーザーに PPP 内でのクライアント認証方式（独自の認証を含む）の適用を可能にします。この認証方式は、ネットワーク アクセス サーバー（NAS）ではサポートされない可能性があり、拡張可能認証プロトコル（EAP）を通して実現されます。この機能が導入される前は、PPP接続用のさまざまな認証方式をサポートするために、特別なベンダー固有設定と、クライアントと NAS に対する変更が必要でした。RADIUS EAP サポートを使用すれば、トークンカードや公開キーなどの認証スキームでネットワークに対するエンド ユーザーとデバイスの認証対象アクセスを補強できます。

RADIUS EAP サポートの前提条件

クライアント上で EAP RADIUS を有効化する前に、次のタスクを実行する必要があります。

- **interface** コマンドを使用してインターフェイス タイプを設定し、インターフェイス コンフィギュレーション モードを開始します。
- **encapsulation** コマンドを使用して、PPP をカプセル化するためのインターフェイスを設定します。

これらのタスクの実行方法については、「Configuring Asynchronous SLIP and PPP」モジュールを参照してください。

RADIUS EAP サポートの制約事項

EAP がプロキシ モードで動作中に、認証時間が大幅に増加する可能性があります。これは、ピアからのすべてのパケットを RADIUS サーバーに送信する必要があり、RADIUS サーバーからのすべての EAP パケットをクライアントに送り返す必要があるためです。この追加処理は遅延の原因になりますが、**ppp timeout authentication** コマンドを使用して、デフォルトの認証タイムアウト値を増やすことができます。

RADIUS EAP サポートに関する情報

EAP は、認証フェーズ（Link Control Protocol（LCP）フェーズではなく）でネゴシエートされる複数の認証メカニズムをサポートする PPP 用の認証プロトコルです。EAP を使用すると、汎用のインターフェイスを介して、サードパーティ製の認証サーバーと PPP 実装の間でデータのやり取りができます。

EAP のしくみ

デフォルトでは、EAP はプロキシモードで実行されます。このため、EAP では、RADIUS サーバーに存在するバックエンドサーバー、または RADIUS サーバーを介してアクセスできるバックエンド サーバーに対する認証プロセス全体を、NAS によってネゴシエートすることができます。LCP の交換中にクライアントと NAS の間で EAP がネゴシエートされると、その後のすべての認証メッセージは、クライアントとバックエンド サーバーの間で透過的に送信されます。NAS は認証プロセスに直接関与しなくなります。つまり、NAS はプロキシとして機能し、リモート ピア間で EAP メッセージを送信します。

（注） EAP は、ローカル モードでも実行できます。その場合、セッションは Message Digest 5（MD5）アルゴリズムを使用して認証され、Challenge Handshake Authentication Protocol（CHAP）と同じ認証ルールに従います。プロキシ モードを無効にしてローカルで認証するには、**ppp eap local** コマンドを使用する必要があります。

新しくサポートされた属性

RADIUS EAP サポート機能では、次の RADIUS 属性のサポートが追加されています。

番号	IETF 属性	説明
79	EAP-Message	PPP type、request-id、length、および EAP-type の各フィールドを含む EAP メッセージの 1 つのフラグメントをカプセル化します。

番号	IETF 属性	説明
80	Message Authenticator	メッセージの発信元整合性を保証します。無効なチェックサムを伴って受信されたすべてのメッセージは、通知されることなく両端で破棄されます。この属性には、RADIUS要求または応答メッセージ全体の HMAC-MD5 チェックサムが含まれており、キーとして RADIUS サーバー シークレットが使用されます。

RADIUS EAP サポートの設定方法

EAP の設定

このタスクを実行して、PPP カプセル化用に設定されたインターフェイス上で EAP を設定します。

手順の概要

1. **enable**
2. **configure terminal**
3. **ppp authentication eap**
4. **ppp eap identity** *string*
5. **ppp eap password** [*number*] *string*
6. **ppp eap local**
7. **ppp eap wait**
8. **ppp eap refuse** [**callin**]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ppp authentication eap** 例：	認証プロトコルとして EAP を有効にします。

	コマンドまたはアクション	目的
	`Router(config-if)# ppp authentication eap`	
ステップ 4	**ppp eap identity** *string* 例： `Router(config-if)# ppp eap identity user`	（任意）ピアから要求されたときの EAP ID を指定します。
ステップ 5	**ppp eap password** [*number*] *string* 例： `Router(config-if)# ppp eap password 7 141B1309`	（任意）ピア認証用の EAP パスワードを設定します。 このコマンドは、クライアント上でのみ設定する必要があります。
ステップ 6	**ppp eap local** 例： `Router(config-if)# ppp eap local`	（任意）RADIUS バックエンドサーバーを使用する代わりにローカルで認証します。これはデフォルトの設定です。 （注） このコマンドは、NAS 上でのみ設定する必要があります。
ステップ 7	**ppp eap wait** 例： `Router(config-if)# ppp eap wait`	（任意）発信者が自分自身を最初に認証するのを待機します。デフォルトでは、クライアントの方が発信者よりも先に自分自身を認証します。 （注） このコマンドは、NAS 上でのみ設定する必要があります。
ステップ 8	**ppp eap refuse** [**callin**] 例： `Router(config-if)# ppp eap refuse`	（任意）EAP を使用した認証を拒否します。**callin** キーワードが有効になっている場合は、着信コールのみが認証されません。 （注） このコマンドは、NAS 上でのみ設定する必要があります。

EAP の確認

クライアントまたは NAS 上の EAP 設定を確認するには、特権 EXEC コンフィギュレーションモードで次のコマンドの少なくとも 1 つを使用します。

コマンド	目的
`Router# show users`	ルータのアクティブ回線に関する情報を表示します。
`Router# show interfaces`	ルータまたはアクセス サーバーで設定されているすべてのインターフェイスの統計情報を表示します。

コマンド	目的
Router# **show running-config**	使用している設定が実行コンフィギュレーションの一部として表示されていることを確認します。

設定例

クライアント上の EAP ローカル設定例

次の例は、EAP 用に設定されたクライアントのサンプル設定です。

```
interface Ethernet0/0
 ip address 10.1.1.202 255.255.255.0
 no ip mroute-cache
 half-duplex
!
interface BRI0/0
 ip address 192.168.101.100 255.255.255.0
 encapsulation ppp
 no ip mroute-cache
 dialer map ip 192.168.101.101 56167
 dialer-group 1
 isdn switch-type basic-5ess
 ppp eap identity user
 ppp eap password 7 141B1309
!
!
ip default-gateway 10.1.1.1
ip classless
ip route 192.168.101.101 255.255.255.255 BRI0/0
no ip http server
!
dialer-list 1 protocol ip permit
```

NAS 用の EAP プロキシ設定例

次の例は、EAP プロキシを使用するように設定された NAS のサンプル設定です。

```
aaa authentication login default group radius
aaa authentication login NOAUTH none
aaa authentication ppp default if-needed group radius
aaa session-id common
enable secret 5 $1$x5D0$cfTL/D8Be.34PgTbdGdgl/
!
username dtw5 password 0 lab
username user password 0 lab
ip subnet-zero
no ip domain-lookup
ip host lab24-boot 172.19.192.254
ip host lb 172.19.192.254
!
isdn switch-type primary-5ess
!
```

```
controller T1 3
 framing esf
 linecode b8zs
 pri-group timeslots 1-24
!
interface Ethernet0
 ip address 10.1.1.108 255.255.255.0
 no ip route-cache
 no ip mroute-cache
!
interface Serial3:23
 ip address 192.168.101.101 255.255.255.0
 encapsulation ppp
 dialer map ip 192.168.101.100 60213
 dialer-group 1
 isdn switch-type primary-5ess
 isdn T321 0
 ppp authentication eap
 ppp eap password 7 011F0706
!
!
ip default-gateway 10.0.190.1
ip classless
ip route 192.168.101.0 255.255.255.0 Serial3:23
no ip http server
!
dialer-list 1 protocol ip permit
!
radius-server host 10.1.1.201 auth-port 1645 acct-port 1646 key lab
radius-server retransmit 3
call rsvp-sync
!
mgcp profile default
!
!
line con 0
 exec-timeout 0 0
 logging synchronous
 login authentication NOAUTH
line 1 48
line aux 0
ine vty 0 4
lpassword lab
```

その他の参考資料

次の項で、RADIUS EAP サポート機能に関する参考資料を紹介します。

関連資料

関連項目	マニュアル タイトル
AAA を使用した ppp 認証の設定	「Configuring Authentication」モジュール。
RADIUS の設定	「Configuring RADIUS」モジュール。
PPP の設定	「Configuring Asynchronous SLIP and PPP」モジュール。

関連項目	マニュアル タイトル
ダイヤル テクノロジー コマンド	『*Cisco IOS Dial Technologies Command Reference*』
セキュリティ コマンド	『*Cisco IOS Security Command Reference*』

標準

標準	タイトル
なし	--

MIB

MIB	MIB のリンク
なし	選択したプラットフォーム、Cisco IOS リリース、およびフィーチャ セットに関する MIB を探してダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

RFC

RFC	タイトル
RFC 2284	『*PPP Extensible Authentication Protocol (EAP)*』
RFC 1938	『*A One-Time Password System*』
RFC 2869	『*RADIUS Extensions*』

シスコのテクニカル サポート

説明	リンク
シスコのサポート Web サイトでは、シスコの製品やテクノロジーに関するトラブルシューティングにお役立ていただけるように、マニュアルやツールをはじめとする豊富なオンライン リソースを提供しています。 お使いの製品のセキュリティ情報や技術情報を入手するために、Cisco Notification Service（Field Notice からアクセス）、Cisco Technical Services Newsletter、Really Simple Syndication（RSS）フィードなどの各種サービスに加入できます。 シスコのサポート Web サイトのツールにアクセスする際は、Cisco.com のユーザ ID およびパスワードが必要です。	http://www.cisco.com/en/US/support/index.html

RADIUS EAP サポートの機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *88 : RADIUS EAP* サポートの機能情報

機能名	リリース	機能情報
RADIUS EAP サポート	Cisco IOS XE Release 3.9S	RADIUS EAP サポート機能は、ユーザーに PPP 内でのクライアント認証方式（独自の認証を含む）の適用を可能にします。この認証方式は、ネットワーク アクセス サーバー（NAS）ではサポートされない可能性があり、拡張可能認証プロトコル（EAP）を通して実現されます。この機能が導入される前は、PPP 接続用のさまざまな認証方式をサポートするために、特別なベンダー固有設定と、クライアントと NAS に対する変更が必要でした。RADIUS EAP サポートを使用すれば、トークン カードや公開キーなどの認証スキームでネットワークに対するエンドユーザーとデバイスの認証対象アクセスを補強できます。 次のコマンドが導入または変更されました。**ppp authentication**、**ppp eap identity, ppp eap local**、**ppp eap password**、**ppp eap refuse**、**ppp eap wait**

用語集

attribute ：RADIUS Internet Engineering Task Force（IETF）属性は、クライアントとサーバーの間で認証、認可、およびアカウンティング（AAA）情報を通信するために使用される 255 個の標準属性からなるオリジナル セットの 1 つです。IETF 属性は標準であるため、属性データは事前定義されてその内容も認識されています。このため、IETF 属性を介して AAA 情報を交換するすべてのクライアントとサーバーは、属性の厳密な意味や各属性値の一般的な限界などの属性データを一致させる必要があります。

CHAP ：チャレンジ ハンドシェイク認証プロトコル。PPP カプセル化を使用した回線上でサポートされ、不正アクセスを防止するセキュリティ機能。CHAP それ自体が不正アクセスを防止するわけではなく、単に、リモートエンドを識別するだけです。その後で、ルータまたはアクセス サーバーがそのユーザーのアクセスを許可するかどうかを決定します。

EAP ：拡張認証プロトコル。認証フェーズ（Link Control Protocol（LCP）フェーズではなく）でネゴシエートされる複数の認証メカニズムをサポートする PPP 認証プロトコル。EAP を使用すれば、汎用のインターフェイスを介して、サードパーティ製の認証サーバーと PPP 実装の間でデータのやり取りができます。

LCP ：リンク制御プロトコル。PPP で使用するためのデータ リンク接続を確立して、設定し、テストするプロトコル。

MD5 (HMAC variant) ：Message Digest 5。パケット データの認証に使用するハッシュ アルゴリズム。HMAC は、メッセージ認証用の重要なハッシングです。

NAS ：ネットワーク アクセス サーバー。公衆電話交換網（PSTN）などのリモート アクセス ネットワーク上でユーザーにローカル ネットワーク アクセスを提供するデバイス。

PAP ：パスワード認証プロトコル。PPP ピアの相互認証を可能にする認証プロトコル。ローカル ルータに接続を試みているリモート ルータは、認証要求を送信するように要求されます。CHAP と違って、PAP はパスワードとホスト名またはユーザー名をクリアテキスト（暗号化なし）で渡します。PAP それ自体が不正アクセスを防止するわけではなく、単に、リモート エンドを識別するだけです。ルータまたはアクセス サーバーがそのユーザーのアクセスを許可するかどうかを決定します。PAP は、PPP 回線上でのみサポートされます。

PPP ：ポイントツーポイント プロトコル。ポイントツーポイント リンク上でネットワーク層プロトコル情報をカプセル化するプロトコル。PPP は RFC 1661 で規定されています。

RADIUS ：リモート認証ダイヤルイン ユーザー サービス。モデムおよび ISDN 接続の認証、および接続のトラッキングのためのデータベースです。

このマニュアルで使用している IP アドレスおよび電話番号は、実際のアドレスおよび電話番号を示すものではありません。マニュアル内の例、コマンド出力、ネットワークトポロジ図、およびその他の図は、説明のみを目的として使用されています。説明の中に実際のアドレスおよび電話番号が使用されていたとしても、それは意図的なものではなく、偶然の一致によるものです。

第 63 章

コール接続時の RADIUS 暫定アップデート

コール接続時の RADIUS 暫定アップデート機能では、課金サーバーにコール接続のタイムスタンプを提供する追加のアカウンティング レコードが生成されます。

コール接続時の RADIUS 暫定アップデートに関する情報

コール接続時の RADIUS 暫定アップデート機能を有効にすると、Cisco IOS ソフトウェアは、コール レッグが接続されたときに、追加の更新済み中間アカウンティング レコードを生成してアカウンティング サーバーに送信します。コール レッグは、Voice over IP（VoIP）ネットワーク内のコール接続の別個のセグメントであり、ルータと、ベアラ チャネルを介したテレフォニー エンドポイントまたはセッション プロトコルを使用した別のエンドポイントとの間の論理的な接続です。コール接続時に使用可能なすべての属性（h323-connect-time や backward-call-indicators など）がこの更新済み中間アカウンティング レコードによって送信されます。

コール接続時の RADIUS 暫定アップデート機能を有効化する方法

次のタスクを実行して、コール レッグが接続されたときに、Cisco IOS で追加の更新済み中間アカウンティング レコードを生成してアカウンティング サーバーに送信できるようにします。

手順の概要

1. **enable**
2. **configure terminal**
3. **aaa new-model**

4. **gw-accounting aaa**
5. **aaa accounting update newinfo**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**aaa new-model** 例： `Router(config)# aaa new-model`	認証、認可、およびアカウンティング（AAA）を有効化します。
ステップ 4	**gw-accounting aaa** 例： `Router(config)# gw-accounting aaa`	AAA システムを通じてアカウンティングを有効化し、コール詳細レコード（CDR）をベンダー固有属性（VSA）の形式で RADIUS サーバーに送信します。
ステップ 5	**aaa accounting update newinfo** 例： `Router(config)# aaa accounting update newinfo`	問題のユーザーに関する新しいアカウンティング情報が生成されるたびに、一時アカウンティング レコードを定期的にアカウンティング サーバーに送信できるようにします。

その他の参考資料

次の項で、コール接続時の RADIUS 暫定アップデート機能に関する参考資料を紹介します。

関連資料

関連項目	マニュアル タイトル
認証、許可、アカウンティング（AAA）	「Configuring Authentication」、「Configuring Authorization」、および「Configuring Accounting」モジュール。
RADIUS ベンダー固有属性	「RADIUS Vendor-Proprietary Attributes」モジュール。

関連項目	マニュアル タイトル
ダイナミック プロンプトの設定、アカウンティングテンプレートのカスタマイズ、および音声ゲートウェイへの AAA 要求の転送	『*Cisco IOS Dial Technologies Configuration Guide* , Release 12.4T』および『*Cisco IOS VPDN Configuration Guide* , Release 12.4T』。

標準

標準	タイトル
なし。	--

MIB

MIB	MIB のリンク
なし。	選択したプラットフォーム、Cisco IOS リリース、およびフィーチャ セットに関する MIB を探してダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

RFC

RFC	タイトル
RFC 2138	『*Remote Authentication Dial In User Service (RADIUS)*』
RFC 2139	『*RADIUS Accounting*』

シスコのテクニカル サポート

説明	リンク
シスコのサポート Web サイトでは、シスコの製品やテクノロジーに関するトラブルシューティングにお役立ていただけるように、マニュアルやツールをはじめとする豊富なオンライン リソースを提供しています。 お使いの製品のセキュリティ情報や技術情報を入手するために、Cisco Notification Service（Field Notice からアクセス）、Cisco Technical Services Newsletter、Really Simple Syndication（RSS）フィードなどの各種サービスに加入できます。 シスコのサポート Web サイトのツールにアクセスする際は、Cisco.com のユーザ ID およびパスワードが必要です。	http://www.cisco.com/en/US/support/index.html

コール接続時の RADIUS 暫定アップデートの機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *89 :* コール接続時の *RADIUS* 暫定アップデートの機能情報

機能名	リリース	機能情報
コール接続時の RADIUS 暫定アップデート	Cisco IOS XE Release 3.9S	コール接続時の RADIUS 暫定アップデート機能では、課金サーバーにコール接続のタイムスタンプを提供する追加のアカウンティング レコードが生成されます。 次のコマンドが導入または変更されました。**gw-accounting aaa** および **aaa accounting update**

第 64 章

ロード バランシングおよびフェールオーバー用の RADIUS トンネル プリファレンス

ロード バランシングおよびフェールオーバー用の RADIUS トンネル プリファレンス機能は、シスコ独自のベンダー固有属性（VSA）を使用せずに、業界標準のロードバランシング機能とフェールオーバー機能を Layer 2 Tunneling Protocol ネットワーク サーバー（LNS）に提供します。この機能は、RFC 2868 で規定されているマルチベンダー ネットワーク環境に使用すべきトンネル属性に適合しているため、複数のベンダーで製造されたネットワーク アクセス サーバー（NAS）間の相互運用性の問題を解決します。

前提条件

VPDN と HGW グループの設定はこのマニュアルの範囲を超えています。詳細については、「関連資料」を参照してください。

機能制限

次の制約および制限が、ロード バランシングおよびフェールオーバー用の RADIUS トンネル プリファレンス機能に適用されます。

- この機能は、VPDN ダイヤルアウト ネットワークをサポートしていません。ダイヤルイン アプリケーション専用に設計されています。
- ネットワーク上で許容される LNS の最大数は、タグ属性グループ当たり 50 ずつの合計 1550 で、タグは 31 までに制限されています。
- この機能には、RFC 2868 をサポートする RADIUS サーバー実装が必要です。

ロードバランシングおよびフェールオーバー用の RADIUS トンネル プリファレンスに関する情報

ロード バランシングおよびフェールオーバー用の RADIUS トンネル プリファレンス機能は、ロード バランシングおよびフェールオーバーの仮想プライベート ダイヤルアップ ネットワーク（VPDN）ホーム ゲートウェイ（HGW）グループを標準化された方式で提供します。この機能は、新しいソフトウェア機能を導入しています。この機能に関連付けられた新しいコマンドはありません。

独自の属性ではなく、業界標準の属性

Cisco IOS Release 12.2(4)T までは、LNS のロード バランシングおよびフェールオーバー機能が、シスコ独自の VSA によって提供されていました。マルチベンダー ネットワーク環境で、RADIUS 上の VSA を使用した場合は、複数のベンダーによって製造された NAS 間で相互運用性の問題が発生する可能性があります。特定の RADIUS サーバー実装が要求元の NAS で解読可能な VSA を送信可能な場合でも、ユーザーが同じ目的で複数の VSA をシングル サービス プロファイルに保存しておく必要があります。

マルチベンダー ネットワーク環境で使用すべきトンネル属性に関する合意は RFC 2868 で規定されています。RFC 2868 では、Tunnel-Server-Endpoint と Tunnel-Medium-Type を組み合わせて、NAS が新しいセッションを開始すべきアドレスが指定されます。複数の Tunnel-Server-Endpoint 属性が 1 つのタグ付き属性グループ内で定義されている場合は、equal-cost load-balancing HGW として解釈されます。

RFC 2868 で規定されている Tunnel-Preference 属性は、ロードバランシングおよびフェールオーバー HGW グループを形成する手段として使用できます。複数のタグ付き属性グループの Tunnel-Preference 値が同じ場合は、他に指定されていなければ、それらの属性グループの Tunnel-Server-Endpoint が同じ優先順位に設定されていると見なされます。一部の属性グループの Tunnel-Preference 値が他の属性グループよりも高い（プリファレンスが低い）場合は、それらの Tunnel-Server-Endpoint 属性の優先順位が上になります。ある属性グループの優先順位値

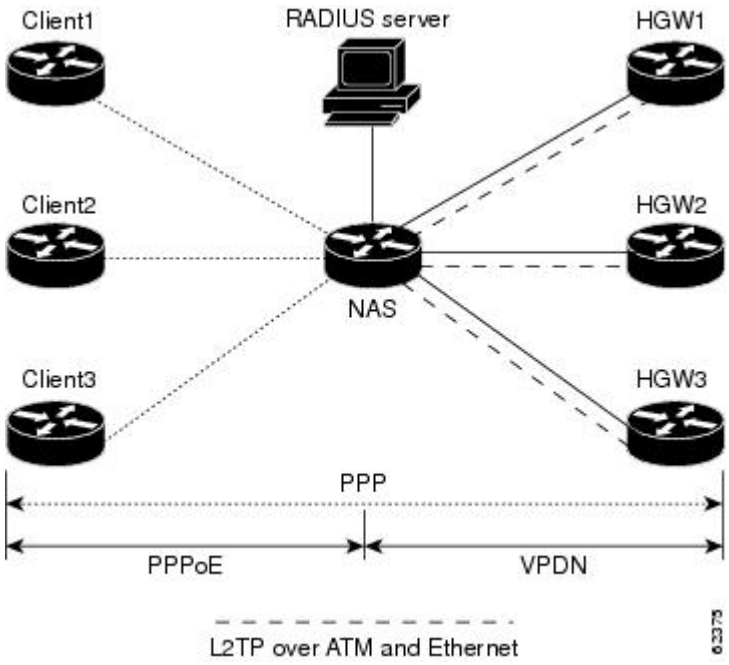
が高い場合は、それより優先順位値が低い属性グループが接続に使用できない場合に、その属性グループがフェールオーバーに使用されます。

Cisco IOS Release 12.2(4)T までは、特別に書式設定された文字列が Cisco VSA の「vpdn:ip-addresses」文字列内で NAS に転送され、HGW のロード バランシングおよびフェールオーバーに使用されていました。たとえば、10.0.0.1 10.0.0.2 10.0.0.3/2.0.0.1 2.0.0.2 は、ロード バランシング用の最初のグループに関する IP アドレスの 10.0.0.1、10.0.0.2、および 10.0.0.3 として解釈されます。新しいセッションは、least-load-first アルゴリズムに基づいて、この 3 つのアドレスに送出されます。このアルゴリズムは、ローカルな知識を利用して、新しいセッションを開始する負荷が最低の HGW を選択します。この例では、2 番めのグループ内のアドレスの 2.0.0.1 と 2.0.0.2 が、優先順位が低く、最初のグループ内で指定されたすべての HGW が新しい接続要求に対する応答に失敗した場合にのみ適用可能になります。そのため、2.0.0.1 と 2.0.0.2 がフェールオーバー アドレスになります。RADIUS トンネル プロファイル内でのこのようなフェールオーバー アドレスの設定方法の例については、ロード バランシングおよびフェールオーバー用の RADIUS トンネル プリファレンスの設定例（764 ページ）を参照してください。

マルチベンダー ネットワークにおけるロード バランシングとフェールオーバー

ロード バランシングおよびフェールオーバー用の RADIUS トンネル プリファレンス機能は、以下の図に示す構成のように、ATM および Ethernet などの WAN リンクを経由して VPDN レイヤ 2 トンネルを使用する大規模なマルチベンダー ネットワーク向けに設計されています。

図 *9:* マルチベンダー ネットワークにおける代表的なロード バランシングとフェールオーバー



上の図に示す構成では、NAS が RADIUS サーバーからダウンロードされたトンネル プロファイルを使用して、ロード バランシングおよびフェールオーバー用の VPDN レイヤ 2 トンネルを構築します。Point-to-Point over Ethernet（PPPoE）プロトコルが、PPP セッションを生成するクライアントとして使用されます。

関連機能およびテクノロジー

ロード バランシングおよびフェールオーバー用の RADIUS トンネル プリファレンス機能は、VPDN で使用されます。加えて、次のテクノロジーとプロトコルに精通していることが求められます。

- ATM
- イーサネット
- L2TP と L2F
- PPP と PPPoE
- RADIUS サーバー

ロードバランシングおよびフェールオーバー用の RADIUS トンネル プリファレンスの設定方法

この機能には新しいコンフィギュレーション コマンドはありません。ただし、RADIUS トンネル プロファイル内でのロード バランシングおよびフェールオーバー用の RADIUS トンネル プリファレンス機能の実装方法の例については、次の項を参照してください。

ロードバランシングおよびフェールオーバー用の RADIUS トンネル プリファレンスの設定例

次の例は、RADIUS トンネル プロファイルの作成方法を示しています。

```
net3 Password = "cisco" Service-Type = Outbound
        Tunnel-Type = :0:L2TP,
        Tunnel-Medium-Type = :0:IP,
        Tunnel-Server-Endpoint = :0:"1.1.3.1",
        Tunnel-Assignment-Id = :0:"1",
        Tunnel-Preference = :0:1,
        Tunnel-Password = :0:"welcome"
        Tunnel-Type = :1:L2TP,
        Tunnel-Medium-Type = :1:IP,
        Tunnel-Server-Endpoint = :1:"1.1.5.1",
        Tunnel-Assignment-Id = :1:"1",
        Tunnel-Preference = :1:1,
        Tunnel-Password = :1:"welcome"
```

```
Tunnel-Type = :2:L2TP,
Tunnel-Medium-Type = :2:IP,
Tunnel-Server-Endpoint = :2:"1.1.4.1",
Tunnel-Assignment-Id = :2:"1",
Tunnel-Preference = :2:1,
Tunnel-Password = :2:"welcome"
Tunnel-Type = :3:L2TP,
Tunnel-Medium-Type = :3:IP,
Tunnel-Server-Endpoint = :3:"1.1.6.1",
Tunnel-Assignment-Id = :3:"1",
Tunnel-Preference = :3:1,
Tunnel-Password = :3:"welcome"
```

これらのプロファイル内でフェールオーバーアドレスがどのように選択されるかの詳細については、ロード バランシングおよびフェールオーバー用の RADIUS トンネル プリファレンスに関する情報 （762 ページ）を参照してください。

その他の参考資料

次の項で、ロード バランシングおよびフェールオーバー用の RADIUS トンネル プリファレンス機能に関する参考資料を紹介します。

関連資料

関連項目	マニュアル タイトル
RADIUS	「Configuring RADIUS」モジュール。
RADIUS 属性	「RADIUS Attributes Overview and RADIUS IETF Attributes」モジュール。
バーチャル プライベート ダイヤルアップ ネットワーク（VPDN）のロードマップ	『*Cisco IOS VPDN Configuration Guide* , Release 15.0』
ダイヤル テクノロジー	『*Cisco IOS Dial Technologies Configuration Guide* , Release 12.4T』
ブロードバンドアクセス：PPP とルーテッド ブリッジ エンカプセレーション	『*Cisco IOS Broadband Access Aggregation and DSL Configuration Guide* , Release 12.4T』

標準

標準	タイトル
なし。	--

MIB

MIB	MIB のリンク
なし。	選択したプラットフォーム、Cisco IOS リリース、およびフィーチャ セットに関する MIB を探してダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

RFC

RFC	タイトル
RFC 2868	『RADIUS Attributes for Tunnel Protocol Support』

ロードバランシングおよびフェールオーバー用の RADIUS トンネル プリファレンスの機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *90*：ロード バランシングおよびフェールオーバー用の *RADIUS* トンネル プリファレンスの機能情報

機能名	リリース	機能情報
ロードバランシングおよびフェールオーバー用の RADIUS トンネル プリファレンス	Cisco IOS XE Release 3.9S	ロード バランシングおよびフェールオーバー用の RADIUS トンネル プリファレンス機能は、シスコ独自のベンダー固有属性（VSA）を使用せずに、業界標準のロード バランシング機能とフェールオーバー機能を Layer 2 Tunneling Protocol ネットワーク サーバー（LNS）に提供します。この機能は、RFC 2868 で規定されているマルチベンダー ネットワーク環境に使用すべきトンネル属性に適合しているため、複数のベンダーで製造されたネットワーク アクセス サーバー（NAS）間の相互運用性の問題を解決します。

用語集

HGW ：ホーム ゲートウェイ。L2TP などのレイヤ 2 トンネリング プロトコルを終端するゲートウェイ。

home gateway ：「HGW」を参照してください。

L2TP ：レイヤ 2 トンネル プロトコル。PPP のトンネリングを提供する RFC 2661 で規定されたインターネット技術特別調査委員会（IETF）標準トラック プロトコル。L2F と PPTP の最良の機能に基づいて、L2TP が、VPDN を実装するための業界全体で相互運用可能な方式を提供します。

L2TP ネットワーク サーバー：LNS を参照してください。

Layer 2 Tunnel Protocol ：「L2TP」を参照してください。

LNS ：L2TP ネットワーク サーバー。L2TP トンネル エンドポイントの一方の側として機能し、NAS または L2TP アクセス コンセントレータ（LAC）に対するピアであるノード。LNS は、アクセス サーバーによってリモート システムからトンネル化されている PPP セッションの論理的終端点です。レイヤ 2 フォワーディング（L2F）HGW に似ています。

NAS ：ネットワーク アクセス サーバー。パケットの世界（インターネットなど）と回線の世界（公衆電話交換網など）をインターフェイスするシスコ プラットフォームまたはプラットフォームの集合。

network access server ：「NAS」を参照してください。

Request for Comments ：「RFC」を参照してください。

RFCs ：コメント要求。インターネット技術特別調査委員会（IETF）によって収集されたインターネットに関する各種規約。1969 年に発足した IETF は、インターネット アーキテクチャの発展に携わっているネットワーク設計者、運営業者、ベンダー、および研究者の大規模でオープンな国際的コミュニティです。RFC は、ネットワーキング プロトコル、手続き、プログラム、および概念に焦点を当てた、コンピュータ通信のさまざまな側面を規定しています。

virtual private dialup network ：「VPDN」を参照してください。

VPDN ：バーチャル プライベート ダイヤルアップ ネットワーク。ネットワーク間のトラフィックをすべて暗号化することにより、パブリック TCP/IP ネットワーク経由でも IP トラフィックをセキュアに転送できます。

このマニュアルで使用している IP アドレスおよび電話番号は、実際のアドレスおよび電話番号を示すものではありません。マニュアル内の例、コマンド出力、ネットワークトポロジ図、およびその他の図は、説明のみを目的として使用されています。説明の中に実際のアドレスおよび電話番号が使用されていたとしても、それは意図的なものではなく、偶然の一致によるものです。

第 V 部

RADIUS 属性

第 65 章

『RADIUS Attributes Overview and RADIUS IETF Attributes』

Remote Authentication Dial-In User Service（RADIUS）属性は、RADIUS プログラムに保存されたユーザ プロファイル内の特定の認証、認可、およびアカウンティング（AAA）要素を定義するために使用されます。この章では、サポートされる RADIUS 属性を示します。

RADIUS 属性の概要

IETF 属性と VSA の比較

RADIUS インターネット技術特別調査委員会（IETF）属性は、255 個の標準属性で構成されるオリジナルのセットで、クライアントとサーバ間での AAA 情報の伝達に使用されます。IETF 属性は標準であり、属性のデータは事前に定義されています。IETF 属性を使用して AAA 情報を交換するクライアントとサーバは、属性の正確な意味や各属性値の一般的な範囲など、属性データについて合意する必要があります。

RADIUS ベンダー固有属性（VSA）は、ベンダー固有 IETF 属性（属性 26）に由来しています。属性 26 を使用して、ベンダーは 255 種の属性を追加作成できます。つまり、ベンダーは、IETF 属性のデータとは異なる属性を作成して、属性 26 の背後でカプセル化することができます。新しく作成された属性は、ユーザが属性 26 を受け入れる場合に受信されます。

VSA の詳細については、「RADIUS ベンダー固有属性および RADIUS Disconnect-Cause 属性値」の章を参照してください。

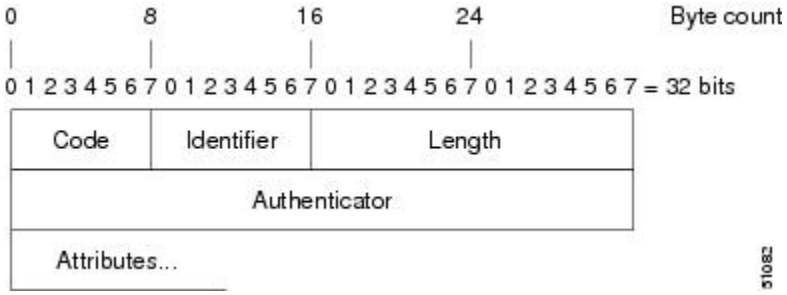
RADIUS パケットのフォーマット

RADIUS サーバと RADIUS クライアント間のデータは、RADIUS パケットで交換されます。データ フィールドは左から右に転送されます。

次の図に、RADIUS パケット内のフィールドを示します。

（注） VSA の図については、「RADIUS ベンダー固有属性および RADIUS Disconnect-Cause 属性値」の章の図 1 を参照してください。

図 *10 : RADIUS* パケット図



各 RADIUS パケットには、次の情報が含まれています。

- コード：コード フィールドは 1 オクテットです。次の RADIUS パケットのタイプを識別します。
  - Access-Request（1）
  - Access-Accept（2）
  - Access-Reject（3）
  - Accounting-Request（4）
  - Accounting-Response（5）
- 識別子：識別子フィールドは 1 オクテットです。RADIUS サーバの要求と応答の照合を支援し、重複した要求を検出します。
- 長さ：長さフィールドは 2 オクテットです。パケット全体の長さを示します。
- オーセンティケータ：オーセンティケータ フィールドは 16 オクテットです。最上位オクテットが最初に転送されます。RADIUS サーバからの応答の認証に使用されます。オーセンティケータには次の 2 つのタイプがあります。
  - Request-Authentication：Access-Request パケットと Accounting-Request パケットで使用できます。
  - Response-Authenticator：Access-Accept、Access-Reject、Access-Challenge、および Accounting-Response パケットで使用できます。

RADIUS パケット タイプ

次のリストは、属性情報を含むさまざまなタイプの RADIUS パケットをまとめたものです。

Access-Request：クライアントから RADIUS サーバに送信されます。このパケットには、ユーザにアクセスを許可している特定のネットワーク アクセス サーバ（NAS）へのアクセスを許可するかどうかを RADIUS サーバが判断するための情報が含まれています。認証を実行しているユーザは、Access-Request パケットを提出する必要があります。RADIUS サーバは、Access-Request パケットを受信した後、応答を返す必要があります。

Access-Accept：RADIUS サーバは、Access-Request パケットを受信した後、Access-Request パケット内のすべての属性値が受け入れ可能な場合に、Access-Accept パケットを送信する必要があります。Access-Accept パケットには、クライアントからユーザにサービスを提供するために必要な設定情報が含まれています。

Access-Reject：RADIUS サーバは、Access-Request パケットを受信した後、どの属性値も受け入れ可能でなかった場合に、Access-Reject パケットを送信する必要があります。

Access-Challenge：RADIUS サーバは、Access-Accept パケットの受信後、応答が必要な Access-Challenge パケットをクライアントに送信できます。クライアントで応答の仕方がわからない場合、または、パケットが無効な場合は、 RADIUS サーバがそのパケットを破棄します。クライアントがパケットに応答する場合は、オリジナルの Access-Request パケットと一緒に新しい Access-Request パケットを送信する必要があります。

Accounting-Request：クライアントから RADIUS アカウンティング サーバに送信され、アカウンティング情報を提供します。RADIUS サーバが正常に Accounting-Request パケットを記録したら、Accounting-Response パケットを提出する必要があります。

Accounting-Response：RADIUS アカウンティング サーバからクライアントに送信され、Accounting-Request が正常に受信および記録されたことが伝えられます。

RADIUS ファイル

クライアントからサーバに AAA 情報を伝送するためには、RADIUS で使用されるファイルのタイプを理解しておくことが重要です。各ファイルには、ユーザの認証や認可のレベルが定義されています。ディレクトリ ファイルには、ユーザの NAS が実装できる属性が定義され、クライアント ファイルには、RADIUS サーバに要求を行えるユーザが定義され、ユーザ ファイルには、セキュリティおよび構成データに基づいて RADIUS サーバが認証するユーザ要求が定義されます。

ディレクトリ ファイル

ディレクトリ ファイルには、NAS でサポートされている属性に依存する属性のリストが格納されています。ただし、独自の属性のセットをカスタム ソリューション用のディレクトリに追加できます。このファイルでは属性値が定義されるため、構文解析要求などの属性出力を解釈できます。ディレクトリ ファイルには次の情報が含まれています。

- 名前：User-Name などの属性の ASCII 文字列「名」
- ID：属性の数値「名」。たとえば、User-Name 属性は属性 1 です。

- 値型：属性は次の値型のいずれかとして指定できます。
  - abinary：0 ～ 254 オクテット
  - date：ビッグエンディアン順の 32 ビット値。たとえば、1970 年 1 月 1 日 00:00:00 GMT 以降の秒数。
  - ipaddr：ネットワーク バイト順の 4 オクテット
  - integer：ビッグエンディアン順による 32 ビット値（上位バイトが先頭）
  - string：0 ～ 253 オクテット

特定の属性のデータ型が整数の場合は、オプションで、整数を拡張して何らかの文字列と一致させることができます。次のサンプル辞書には、整数ベースの属性と対応する値が含まれています。

```
# dictionary sample of integer entry
#
ATTRIBUTE       Service-Type            6                       integer
VALUE           Service-Type            Login                      1
VALUE           Service-Type            Framed                     2
VALUE           Service-Type            Callback-Login             3
VALUE           Service-Type            Callback-Framed            4
VALUE           Service-Type            Outbound                   5
VALUE           Service-Type            Administrative             6
VALUE           Service-Type            NAS-Prompt                 7
VALUE           Service-Type            Authenticate-Only          8
VALUE           Service-Type            Callback-NAS-Prompt        9
VALUE           Service-Type            Call-Check                 10
VALUE           Service-Type            Callback-Administrative    11
```

クライアント ファイル

クライアントファイルには、RADIUS サーバへの認証要求とアカウンティング要求の送信を許可された RADIUS クライアントのリストが含まれています。認証を受けるには、クライアントからサーバに送信された名前と認証キーがクライアントファイル内のデータと完全一致する必要があります。

クライアントファイルの例を次に示します。この例に示すキーは、**radius-server key***SomeSecret* コマンドと同じにする必要があります。

```
#Client Name        Key
#----------------  ---------------
10.1.2.3:256        test
nas01               bananas
nas02               MoNkEys
nas07.foo.com       SomeSecret
```

ユーザ ファイル

RADIUS ユーザ ファイルには、RADIUS サーバが認証するユーザごとのエントリが含まれています。ユーザプロファイルとも呼ばれるエントリごとに、そのユーザがアクセス可能な属性が設定されます。

ユーザプロファイルの最初の行は、常に、「ユーザアクセス」行です。つまり、サーバはユーザにアクセス許可を出す前に、最初の行の属性をチェックする必要があります。最初の行には

ユーザの名前が含まれています。この名前は、最大252文字にすることができ、後ろにユーザのパスワードなどの認証情報が続きます。

ユーザアクセス行に関連付けられたその他の行は、要求元のクライアントまたはサーバに送信される属性応答を表します。応答内で送信される属性は、ディレクトリファイルで定義する必要があります。ユーザ ファイルを調べるときは、等号（=）文字の左側のデータがディレクトリ ファイルで定義された属性で、等号文字の右側のデータが構成データであることに注意してください。

（注） 空白行はユーザ プロファイルのどの場所にも挿入できません。

RADIUS ユーザ プロファイル（Merit Daemon フォーマット）の例を次に示します。この例では、ユーザ名が company.com、パスワードが user1 で、ユーザは 5 つのトンネル属性にアクセスできます。

```
# This user profile includes RADIUS tunneling attributes
company.com  Password="user1" Service-Type=Outbound
     Tunnel-Type = :1:L2TP
     Tunnel-Medium-Type = :1:IP
     Tunnel-Server-Endpoint = :1:10.0.0.1
     Tunnel-Password = :1:"welcome"
     Tunnel-Assignment-ID = :1:"nas"
```

RADIUS IETF 属性

（注） RADIUS トンネル属性では、L2TP に 32 個のタグ付きトンネル セットがサポートされます。

サポートされている RADIUS IETF 属性

表 1 に、シスコがサポートしている IETF RADIUS 属性とそれらが実装されている Cisco IOS リリースを示します。属性がセキュリティ サーバ固有の形式の場合は、この形式が指定されます。

リスト内の属性の説明については、表 2 を参照してください。

（注） 特別な（AA）リリースまたは初期開発（T）リリースで実装された属性が次のメインライン イメージに追加されています。

表 *91 :* サポートされている *RADIUS IETF* 属性

番号	IETF 属性	11.1	11.2	11.3	11.3 AA	11.3T	12.0	12.1	12.2
1	User-Name	あり	あり	あり	あり	あり	あり	あり	あり
2	User-Password	あり	あり	あり	あり	あり	あり	あり	あり
3	CHAP-Password	あり	あり	あり	あり	あり	あり	あり	あり
4	NAS-IP Address	あり	あり	あり	あり	あり	あり	あり	あり
5	NAS-Port	あり	あり	あり	あり	あり	あり	あり	あり
6	Service-Type	あり	あり	あり	あり	あり	あり	あり	あり
7	Framed-Protocol	あり	あり	あり	あり	あり	あり	あり	あり
8	Framed-IP-Address	あり	あり	あり	あり	あり	あり	あり	あり
9	Framed-IP-Netmask	あり	あり	あり	あり	あり	あり	あり	あり
10	Framed-Routing	あり	あり	あり	あり	あり	あり	あり	あり
11	Filter-Id	あり	あり	あり	あり	あり	あり	あり	あり
12	Framed-MTU	あり	あり	あり	あり	あり	あり	あり	あり
13	Framed-Compression	あり	あり	あり	あり	あり	あり	あり	あり
14	Login-IP-Host	あり	あり	あり	あり	あり	あり	あり	あり
15	Login-Service	あり	あり	あり	あり	あり	あり	あり	あり
16	Login-TCP-Port	あり	あり	あり	あり	あり	あり	あり	あり
18	Reply-Message	あり	あり	あり	あり	あり	あり	あり	あり
19	Callback-Number	いいえ（No）	いいえ（No）	いいえ（No）	いいえ（No）	いいえ（No）	いいえ（No）	あり	あり
20	Callback-ID	いいえ（No）	いいえ（No）	いいえ（No）	いいえ（No）	いいえ（No）	いいえ（No）	いいえ（No）	いいえ（No）
22	Framed-Route	あり	あり	あり	あり	あり	あり	あり	あり
23	Framed-IPX-Network	いいえ（No）	いいえ（No）	いいえ（No）	いいえ（No）	いいえ（No）	いいえ（No）	いいえ（No）	いいえ（No）

番号	IETF 属性	11.1	11.2	11.3	11.3 AA	11.3T	12.0	12.1	12.2
24	状態	あり	あり	あり	あり	あり	あり	あり	あり
25	Class	あり	あり	あり	あり	あり	あり	あり	あり
26	Vendor-Specific	あり	あり	あり	あり	あり	あり	あり	あり
27	Session-Timeout	あり	あり	あり	あり	あり	あり	あり	あり
28	Idle-Timeout	あり	あり	あり	あり	あり	あり	あり	あり
29	Termination-Action	いいえ（No）	いいえ（No）	いいえ（No）	いいえ（No）	いいえ（No）	いいえ（No）	いいえ（No）	いいえ（No）
30	Called-Station-Id	あり	あり	あり	あり	あり	あり	あり	あり
31	Calling-Station-Id	あり	あり	あり	あり	あり	あり	あり	あり
32	NAS-Identifier	いいえ（No）	いいえ（No）	いいえ（No）	いいえ（No）	いいえ（No）	いいえ（No）	いいえ（No）	あり
33	Proxy-State	いいえ（No）	いいえ（No）	いいえ（No）	いいえ（No）	いいえ（No）	いいえ（No）	いいえ（No）	いいえ（No）
34	Login-LAT-Service	あり	あり	あり	あり	あり	あり	あり	あり
35	Login-LAT-Node	いいえ（No）	いいえ（No）	いいえ（No）	いいえ（No）	いいえ（No）	いいえ（No）	いいえ（No）	あり
36	Login-LAT-Group	いいえ（No）	いいえ（No）	いいえ（No）	いいえ（No）	いいえ（No）	いいえ（No）	いいえ（No）	いいえ（No）
37	Framed-AppleTalk-Link	いいえ（No）	いいえ（No）	いいえ（No）	いいえ（No）	いいえ（No）	いいえ（No）	いいえ（No）	いいえ（No）
38	Framed-AppleTalk-Network	いいえ（No）	いいえ（No）	いいえ（No）	いいえ（No）	いいえ（No）	いいえ（No）	いいえ（No）	いいえ（No）
39	Framed-AppleTalk-Zone	いいえ（No）	いいえ（No）	いいえ（No）	いいえ（No）	いいえ（No）	いいえ（No）	いいえ（No）	いいえ（No）

番号	IETF 属性	11.1	11.2	11.3	11.3 AA	11.3T	12.0	12.1	12.2
40	Acct-Status-Type	あり	あり	あり	あり	あり	あり	あり	あり
41	Acct-Delay-Time	あり	あり	あり	あり	あり	あり	あり	あり
42	Acct-Input-Octets	あり	あり	あり	あり	あり	あり	あり	あり
43	Acct-Output-Octets	あり	あり	あり	あり	あり	あり	あり	あり
44	Acct-Session-Id	あり	あり	あり	あり	あり	あり	あり	あり
45	Acct-Authentic	あり	あり	あり	あり	あり	あり	あり	あり
46	Acct-Session-Time	あり	あり	あり	あり	あり	あり	あり	あり
47	Acct-Input-Packets	あり	あり	あり	あり	あり	あり	あり	あり
48	Acct-Output-Packets	あり	あり	あり	あり	あり	あり	あり	あり
49	Acct-Terminate-Cause	いいえ（No）	いいえ（No）	いいえ（No）	あり	あり	あり	あり	あり
50	Acct-Multi-Session-Id	いいえ（No）	あり	あり	あり	あり	あり	あり	あり
51	Acct-Link-Count	いいえ（No）	あり	あり	あり	あり	あり	あり	あり
52	Acct-Input-Gigawords	いいえ（No）	いいえ（No）	いいえ（No）	いいえ（No）	いいえ（No）	いいえ（No）	いいえ（No）	いいえ（No）
53	Acct-Output-Gigawords	いいえ（No）	いいえ（No）	いいえ（No）	いいえ（No）	いいえ（No）	いいえ（No）	いいえ（No）	いいえ（No）
55	Event-Timestamp	いいえ（No）	いいえ（No）	いいえ（No）	いいえ（No）	いいえ（No）	いいえ（No）	いいえ（No）	あり
60	CHAP-Challenge	あり	あり	あり	あり	あり	あり	あり	あり
61	NAS-Port-Type	あり	あり	あり	あり	あり	あり	あり	あり
62	Port-Limit	あり	あり	あり	あり	あり	あり	あり	あり
63	Login-LAT-Port	いいえ（No）	いいえ（No）	いいえ（No）	いいえ（No）	いいえ（No）	いいえ（No）	いいえ（No）	いいえ（No）

番号	IETF 属性	11.1	11.2	11.3	11.3 AA	11.3T	12.0	12.1	12.2
64	Tunnel-Type[2]	いいえ（No）	いいえ（No）	いいえ（No）	いいえ（No）	いいえ（No）	いいえ（No）	あり	あり
65	Tunnel-Medium-Type 1	いいえ（No）	いいえ（No）	いいえ（No）	いいえ（No）	いいえ（No）	いいえ（No）	あり	あり
66	Tunnel-Client-Endpoint	いいえ（No）	いいえ（No）	いいえ（No）	いいえ（No）	いいえ（No）	いいえ（No）	あり	あり
67	Tunnel-Server-Endpoint 1	いいえ（No）	いいえ（No）	いいえ（No）	いいえ（No）	いいえ（No）	いいえ（No）	あり	あり
68	Acct-Tunnel-Connection-ID	いいえ（No）	いいえ（No）	いいえ（No）	いいえ（No）	いいえ（No）	いいえ（No）	あり	あり
69	Tunnel-Password 1	いいえ（No）	いいえ（No）	いいえ（No）	いいえ（No）	いいえ（No）	いいえ（No）	あり	あり
70	ARAP-Password	いいえ（No）	いいえ（No）	いいえ（No）	いいえ（No）	いいえ（No）	いいえ（No）	いいえ（No）	いいえ（No）
71	ARAP-Features	いいえ（No）	いいえ（No）	いいえ（No）	いいえ（No）	いいえ（No）	いいえ（No）	いいえ（No）	いいえ（No）
72	ARAP-Zone-Access	いいえ（No）	いいえ（No）	いいえ（No）	いいえ（No）	いいえ（No）	いいえ（No）	いいえ（No）	いいえ（No）
73	ARAP-Security	いいえ（No）	いいえ（No）	いいえ（No）	いいえ（No）	いいえ（No）	いいえ（No）	いいえ（No）	いいえ（No）
74	ARAP-Security-Data	いいえ（No）	いいえ（No）	いいえ（No）	いいえ（No）	いいえ（No）	いいえ（No）	いいえ（No）	いいえ（No）

番号	IETF 属性	11.1	11.2	11.3	11.3 AA	11.3T	12.0	12.1	12.2
75	Password-Retry	いいえ（No）	いいえ（No）	いいえ（No）	いいえ（No）	いいえ（No）	いいえ（No）	いいえ（No）	いいえ（No）
76	Prompt	いいえ（No）	いいえ（No）	いいえ（No）	いいえ（No）	いいえ（No）	いいえ（No）	あり	あり
77	Connect-Info	いいえ（No）	いいえ（No）	いいえ（No）	いいえ（No）	いいえ（No）	いいえ（No）	いいえ（No）	あり
78	Configuration-Token	いいえ（No）	いいえ（No）	いいえ（No）	いいえ（No）	いいえ（No）	いいえ（No）	いいえ（No）	いいえ（No）
79	EAP-Message	いいえ（No）	いいえ（No）	いいえ（No）	いいえ（No）	いいえ（No）	いいえ（No）	いいえ（No）	いいえ（No）
80	Message-Authenticator	いいえ（No）	いいえ（No）	いいえ（No）	いいえ（No）	いいえ（No）	いいえ（No）	いいえ（No）	いいえ（No）
81	Tunnel-Private-Group-ID	いいえ（No）	いいえ（No）	いいえ（No）	いいえ（No）	いいえ（No）	いいえ（No）	いいえ（No）	いいえ（No）
82	Tunnel-Assignment-ID 1	いいえ（No）	いいえ（No）	いいえ（No）	いいえ（No）	いいえ（No）	いいえ（No）	あり	あり
83	Tunnel-Preference	いいえ（No）	いいえ（No）	いいえ（No）	いいえ（No）	いいえ（No）	いいえ（No）	いいえ（No）	あり
84	ARAP-Challenge-Response	いいえ（No）	いいえ（No）	いいえ（No）	いいえ（No）	いいえ（No）	いいえ（No）	いいえ（No）	いいえ（No）
85	Acct-Interim-Interval	いいえ（No）	いいえ（No）	いいえ（No）	いいえ（No）	いいえ（No）	いいえ（No）	あり	あり

番号	IETF 属性	11.1	11.2	11.3	11.3 AA	11.3T	12.0	12.1	12.2
86	Acct-Tunnel-Packets-Lost	いいえ（No）	いいえ（No）	いいえ（No）	いいえ（No）	いいえ（No）	いいえ（No）	いいえ（No）	いいえ（No）
87	NAS-Port-ID	いいえ（No）	いいえ（No）	いいえ（No）	いいえ（No）	いいえ（No）	いいえ（No）	いいえ（No）	いいえ（No）
88	Framed-Pool	いいえ（No）	いいえ（No）	いいえ（No）	いいえ（No）	いいえ（No）	いいえ（No）	いいえ（No）	いいえ（No）
90	Tunnel-Client-Auth-ID [3]	いいえ（No）	いいえ（No）	いいえ（No）	いいえ（No）	いいえ（No）	いいえ（No）	いいえ（No）	あり
91	Tunnel-Server-Auth-ID	いいえ（No）	いいえ（No）	いいえ（No）	いいえ（No）	いいえ（No）	いいえ（No）	いいえ（No）	あり
200	IETF-Token-Immediate	いいえ（No）	いいえ（No）	いいえ（No）	いいえ（No）	いいえ（No）	いいえ（No）	いいえ（No）	いいえ（No）

[2] このRADIUS属性は、2つのドラフトIETF文書、RFC 2868『RADIUS Attributes for Tunnel Protocol Support』とRFC 2867『RADIUS Accounting Modifications for Tunnel Protocol Support』に基づきます。

[3] このRADIUS属性は、RFC 2865およびRFC 2868に基づきます。

RADIUS 属性解説の包括的リスト

次の表に、IETF RADIUS属性とその説明を示します。属性がセキュリティ サーバ固有の形式の場合は、この形式が指定されます。

表 *92 : RADIUS IETF* 属性

番号	IETF 属性	説明
1	User-Name	RADIUS サーバで認証されるユーザの名前を示します。
2	User-Password	Access-Challenge の後に続くユーザのパスワードとユーザ入力を示します。16文字を超えるパスワードは、RFC 2865の仕様により暗号化されます。

番号	IETF 属性	説明
3	CHAP-Password	Access-Challenge に対する応答で PPP Challenge Handshake Authentication Protocol（CHAP）ユーザが入力した応答値を示します。
4	NAS-IP Address	認証を要求しているネットワーク アクセス サーバの IP アドレスを示します。デフォルト値は 0.0.0.0/0 です。
5	NAS-Port	ユーザを認証しているネットワーク アクセス サーバの物理ポート番号を示します。NAS-Port 値（32 ビット）は、1 つまたは 2 つの 16 ビット値（**radius-server extended-portnames** コマンドの設定に依存）で構成されます。各 16 ビットの数値は、次のように、解釈用の 5 桁の 10 進整数として表示されるはずです。 非同期端末回線、非同期ネットワーク インターフェイス、および仮想非同期インターフェイスの場合、この値は **00ttt** です。ここで、**ttt** は回線番号または非同期インターフェイスユニット番号です。 • 通常の同期ネットワーク インターフェイスの場合、この値は **10xxx** です。 • プライマリレート ISDN インターフェイス上のチャネルの場合、この値は **2ppcc** です。 • 基本レート ISDN インターフェイス上のチャネルの場合、この値は **3bb0c** です。 • 他のタイプのインターフェイスの場合、値は **6nnss** です。

番号	IETF 属性	説明
6	Service-Type	要求されたサービスのタイプまたは指定されたサービスのタイプを示します。 • 要求内： 既知の PPP または Serial Line Internet Protocol（SLIP）接続の場合にフレーム化。**enable** コマンドの場合は Administrative-user。 • 応答内： Login：接続を確立します。Framed：SLIP または PPP を開始します。Administrative User：EXEC または **enable ok** を開始します。 Exec User：EXEC セッションを開始します。 サービス タイプは、次のような特定の数値で示されます。 • 1：Login • 2：Framed • 3：Callback-Login • 4：Callback-Framed • 5：Outbound • 6：Administrative • 7：NAS-Prompt • 8：Authenticate Only • 9：Callback-NAS-Prompt

番号	IETF 属性	説明
7	Framed-Protocol	フレーム化アクセスに使用されるフレーム構成を示します。他のフレーム構成は許可されません。 フレーム構成は次のように数値で指定されます。 • 1：PPP • 2：SLIP • 3：ARA • 4：Gandalf 独自のシングルリンク/マルチリンク プロトコル • 5：Xylogics 独自の IPX/SLIP
8	Framed-IP-Address	access-request 内でユーザの IP アドレスを RADIUS サーバに送信することによって、ユーザに対して設定する IP アドレスを示します。このコマンドを有効にするには、グローバル コンフィギュレーション モードで **radius-server attribute 8 include-in-access-req** コマンドを使用します。
9	Framed-IP-Netmask	ユーザがネットワーク上でデバイスを使用している場合に、ユーザに対して設定する IP ネットマスクを示します。この属性値によって、指定されたマスクを使用して Framed-IP-Address にスタティック ルートが追加されることになります。

番号	IETF 属性	説明
10	Framed-Routing	ユーザがネットワーク上でデバイスを使用している場合に、ユーザに対するルーティング方式を示します。この属性に対してサポートされている値は、「None」と「Send and Listen」だけです。 ルーティング方式は次のように数値で指定されます。 • 0：なし • 1：ルーティング パケットの送信 • 2：ルーティング パケットのリッスン • 3：ルーティング パケットの送信とリッスン
11	Filter-Id	ユーザのフィルタ リストの名前を示し、%d、%d.in、または %d.out としてフォーマットされます。この属性は、最近のサービス タイプ コマンドに関連付けられます。ログインと EXEC の場合は、0 ～ 199 の回線アクセス リスト値として %d または %d.out を使用します。フレーム化サービスの場合は、インターフェイス出力アクセス リストとして %d または %d.out を使用し、入力アクセス リストとして %d.in を使用します。この番号は、参照しているプロトコルに対する自己符号化です。
12	Framed-MTU	最大伝送ユニット（MTU）が PPP でネゴシエートされない場合に、ユーザに対して設定可能な MTU を示します。

番号	IETF 属性	説明
13	Framed-Compression	リンクに使用される圧縮プロトコルを示します。この属性により、EXEC認可時に生成される PPP または SLIP オートコマンドに「/compress」が追加されます。これは EXEC 認可以外には実装されていません。 圧縮プロトコルは次のように数値で指定されます。 • 0：なし • 1：VJ-TCP/IP ヘッダー圧縮 • 2：IPX ヘッダー圧縮
14	Login-IP-Host	Login-Service 属性が含まれている場合に、ユーザが接続するホストを示しますこの動作はログイン直後に開始されます。
15	Login-Service	ユーザをログイン ホストに接続するために使用すべきサービスを示します。 サービスは次のように数値で指定されます。 • 0：Telnet • 1：Rlogin • 2：TCP-Clear • 3：PortMaster • 4：LAT
16	Login-TCP-Port	Login-Service 属性も存在する場合に、ユーザを接続すべき TCP ポートを定義します。
18	Reply-Message	RADIUS サーバを使用してユーザに表示される可能性のあるテキストを示します。この属性はユーザ ファイルに含めることができますが、プロファイル当たりの Reply-Message エントリ数を 16 以下にする必要があります。

番号	IETF 属性	説明
19	Callback-Number	コールバックに使用するダイヤリング文字列を定義します。
20	Callback-ID	呼び出される場所の名前、つまり、ネットワーク アクセス サーバによって解釈される場所の名前（1つ以上のオクテットからなる）を定義します。
22	Framed-Route	このネットワーク アクセス サーバ上のユーザに対して設定するルーティング情報を指定します。RADIUS RFC 形式（net/bits [router [metric]]）と従来のドット区切りのマスク（net mask [router [metric]]）がサポートされています。デバイス フィールドを省略するか、0 にした場合は、ピア IP アドレスが使用されます。現在、メトリックは無視されます。この属性は access-request パケットです。
23	Framed-IPX-Network	ユーザに対して設定される IPX ネットワーク番号を定義します。
24	状態	ネットワーク アクセス サーバと RADIUS サーバ間で状態情報の保持を可能にします。この属性は CHAP チャレンジにしか適用できません。
25	Class	（アカウンティング）RADIUS サーバで入力された場合に、このユーザに関するすべてのアカウンティング パケットにネットワーク アクセス サーバで追加される任意の値

番号	IETF 属性	説明

26	Vendor-Specific	ベンダーに一般使用に適さない独自の拡張属性の使用を許可します。シスコの RADIUS 実装は、この仕様で推奨される形式を使用して、1つのベンダー固有オプションをサポートしています。シスコのベンダー ID は 9 であり、サポート対象のオプションはベンダータイプ 1（名前は「cisco-avpair」）です。値は、次の形式のストリングです。
		
		`protocol : attribute sep value`
		
		「protocol」は、特定の認可タイプに使用するシスコの「protocol」属性の値です。「attribute」および「value」は、シスコの TACACS+ 仕様で定義されている適切な AV ペアです。「sep」は、必須の属性の場合は「=」、任意指定の属性の場合は「*」です。これにより、TACACS+認可で使用できるすべての機能を RADIUS にも使用できるようになります。次に例を示します。
		
		`cisco-avpair= ”ip:addr-pool=first“`
		`cisco-avpair= ”shell:priv-lvl=15“`
		
		1つめの例は、IP認可の際（PPP の IPCP アドレスの割り当て中）にシスコの「Multiple Named ip address Pools」機能を有効化します。2つめの例は、ネットワーク アクセス サーバからのユーザ ログイン直後に EXEC コマンドにアクセスできるようにします。
		
		表 1 に、サポートされているベンダー固有 RADIUS 属性（IETF 属性 26）を示します。

27	Session-Timeout	セッションを終了する前に、ユーザにサービスを提供する最大秒数を設定します。この属性値は、ユーザ単位の絶対タイムアウトになります。

番号	IETF 属性	説明
28	Idle-Timeout	セッションが終了する前にユーザに許可されるアイドル接続の最大秒数を設定します。この属性値は、ユーザ単位のセッションタイムアウトになります。
29	Termination-Action	終了は次のように数値で指定されます。 • 0：デフォルト • 1：RADIUS 要求
30	Called-Station-Id	（アカウンティング）ネットワーク アクセス サーバから、ユーザが Access-Request パケットの一部として呼び出した電話番号を送信できるようにします（着信番号識別サービス（DNIS）または同様の技術を使用）。この属性は、ISDN と、PRI と一緒に使用された場合の Cisco AS5200 上のモデム コールに対してのみサポートされます。
31	Calling-Station-Id	（アカウンティング）ネットワーク アクセス サーバから、コールが Access-Request パケットの一部として発信された電話番号を送信できるようにします（自動番号識別または同様の技術を使用）。この属性の値は、TACACS+ の「remote-addr」の値と同じです。この属性は、ISDN と、PRI と一緒に使用された場合の Cisco AS5200 上のモデム コールに対してのみサポートされます。
32	NAS-Identifier	Access-Request を送信したネットワーク アクセス サーバを識別する文字列。**radius-server attribute 32 include-in-access-req** グローバル コンフィギュレーション コマンドを使用して、Access-Request または Accounting-Request 内で RADIUS 属性 32 を送信します。フォーマットが指定されなかった場合は、デフォルトで、完全修飾ドメイン名（FQDN）が属性内で送信されます。

番号	IETF 属性	説明
33	Proxy-State	Access-Request の転送時にプロキシ サーバから別のサーバに送信可能な属性。この属性は、Access-Accept、Access-Reject、または Access-Challenge 内でそのまま返され、ネットワーク アクセス サーバに応答が送信される前にプロキシ サーバで削除される必要があります。
34	Login-LAT-Service	ユーザをローカル エリア トランスポート（LAT）で接続すべきシステムを示します。この属性は、EXEC モードでのみ使用できます。
35	Login-LAT-Node	ユーザが LAT で自動的に接続されるノードを示します。
36	Login-LAT-Group	ユーザに使用が認可されている LAT グループ コードを識別します。
37	Framed-AppleTalk-Link	AppleTalk デバイスであるシリアル リンクに使用すべき別の AppleTalk のネットワーク番号を示します。
38	Framed-AppleTalk- Network	ユーザに AppleTalk ノードを割り当てるためにネットワーク アクセス サーバで使用される AppleTalk ネットワーク番号を示します。
39	Framed-AppleTalk-Zone	ユーザに使用すべき AppleTalk デフォルト ゾーンを示します。
40	Acct-Status-Type	（アカウンティング）この Accounting-Request がユーザ サービスの始まり（開始）または終わり（終了）をマークするかどうかを示します。
41	Acct-Delay-Time	（アカウンティング）クライアントが特定のレコードの送信を試みる秒数を示します。
42	Acct-Input-Octets	（アカウンティング）このサービスの提供中にポートから受信されたオクテット数を示します。

番号	IETF 属性	説明
43	Acct-Output-Octets	（アカウンティング）このサービスの配信中にポートに送信されたオクテット数を示します。
44	Acct-Session-Id	（アカウンティング）ログ ファイル内の開始レコードと終了レコードのマッチングを容易にする一意のアカウンティング識別子。Acct-Session ID の番号は、デバイスの電源を入れ直したり、ソフトウェアをリロードしたりするたびに、1 から再開します。この属性を access-request パケット内で送信するには、グローバル コンフィギュレーション モードで **radius-server attribute 44 include-in-access-req** コマンドを使用します。
45	Acct-Authentic	（アカウンティング）ユーザがどのように認証されたか、RADIUS、ネットワーク アクセス サーバ自体、およびその他のリモート認証プロトコルのどれで認証されたかを示します。この属性は、RADIUS で認証されたユーザの場合は「radius」に、TACACS+ と Kerberos の場合は「remote」に、local、enable、line、および if-needed 方式の場合は「local」に設定されます。その他のすべての方式の場合は、この属性が省略されます。
46	Acct-Session-Time	（アカウンティング）ユーザがサービスを受信していた時間（秒数）を示します。
47	Acct-Input-Packets	（アカウンティング）このサービスのフレーム化ユーザへの提供中にポートから受信されたパケット数を示します。
48	Acct-Output-Packets	（アカウンティング）このサービスのフレーム化ユーザへの配信中にポートに送信されたパケット数を示します。

番号	IETF 属性	説明
49	Acct-Terminate-Cause	（アカウンティング）接続が終了した理由の詳細を報告します。終了の理由は次のように数値で指定されます。 **1.** ユーザ要求 **2.** 搬送が失われた **3.** サービスの消失 **4.** アイドル タイムアウト **5.** セッション タイムアウト **6.** 管理リセット **7.** 管理リブート **8.** ポート エラー **9.** NAS エラー **10.** NAS 要求 **11.** NAS リブート **12.** ポートの不要化 **13.** ポートの横取り **14.** ポートの保留 **15.** 使用できないサービス **16.** コールバック **17.** ユーザー エラー **18.** ホスト要求 （注） 属性49に関して、シスコは1 ～ 6、8、9、12、および15 ～ 18 の値をサポートしています。

番号	IETF 属性	説明
50	Acct-Multi-Session-Id	（アカウンティング）ログ ファイル内の複数の関連セッションをリンクするために使用される一意のアカウンティング識別子。 マルチリンク セッション内でリンクされたセッションごとに、一意の Acct-Session-Id 値が割り当てられますが、Acct-Multi-Session-Id は共有されます。
51	Acct-Link-Count	（アカウンティング）アカウンティング レコードが生成された時点で特定のマルチリンク セッション内で認識されていたリンク数を示します。ネットワーク アクセス サーバは、複数のリンクが含まれる任意のアカウンティング要求内にこの属性を追加できます。
52	Acct-Input-Gigawords	サービスの提供中に Acct-Input-Octets カウンタが一周（2 の 32 乗）した回数を示します。
53	Acct-Output-Gigawords	サービスの配信中に Acct-Output-Octets カウンタが一周（2 の 32 乗）した回数を示します。

番号	IETF 属性	説明
55	Event-Timestamp	NAS 上でイベントが発生した時刻を記録します。属性 55 内で送信されるタイムスタンプは、1970 年 1 月 1 日 00:00 UTC 以降の秒数です。アカウンティングパケット内で RADIUS 属性 55 を送信するには、**radius-server attribute 55 include-in-acct-req** コマンドを使用します。 （注） アカウンティング パケット内で Event-Timestamp 属性を送信するには、ネットワーク デバイスのクロックを設定する必要があります（ネットワーク デバイスのクロックの設定方法については、ネットワーク管理の設定ガイドの「基本システム管理」の章の「基本システム管理の実行」を参照してください）。ネットワークデバイスがリロードされるたびにネットワークデバイスのクロックを設定するのを避けるには、**clock calendar-valid** コマンドを有効にします。（このコマンドの詳細については、ネットワーク管理の設定ガイドの「基本システム管理」の章の「時刻およびカレンダーサービスの設定」を参照してください）。
60	CHAP-Challenge	ネットワーク アクセス サーバから PPP CHAP ユーザに送信されたチャレンジ ハンドシェーク認証プロトコル チャレンジが保存されます。

番号	IETF 属性	説明
61	NAS-Port-Type	ユーザを認証するためにネットワーク アクセス サーバで使用されている物理ポートのタイプを示します。物理ポートは、次のように数値で示されます。 • 0：非同期 • 1：同期 • 2：ISDN 同期 • 3：ISDN 非同期（V.120） • 4：ISDN 非同期（V.110） • 5：仮想
62	Port-Limit	NAS からユーザに提供される最大ポート数を設定します。
63	Login-LAT-Port	ユーザを LAT で接続すべきポートを定義します。
64	Tunnel-Type[4]	使用されているトンネリング プロトコルを示します。シスコのソフトウェアでは、この属性の値として L2TP がサポートされます。
65	Tunnel-Medium-Type1	トンネルの作成に使用される転送メディア タイプを示します。この属性には、このリリースで使用可能な値（IP）が 1 つしかありません。この属性に値を設定しなかった場合は、デフォルトとして IP が使用されます。

番号	IETF 属性	説明
66	Tunnel-Client-Endpoint	トンネルの開始側端のアドレスが含まれています。Access-Request と Access-Accept の両方のパケットに含めて、新しいトンネルを開始するアドレスを示すこともできます。 Tunnel-Client-Endpoint 属性が Access-Request パケットに含まれている場合、RADIUS サーバはその値を指示として取得する必要があります。この属性は、Accounting-Request パケットに含める必要があります。このパケットには、トンネルが開始されたアドレスを示す場合に Start と Stop のどちらかの値を伴う Acct-Status-Type 属性が含まれています。この属性は、Tunnel-Server-Endpoint 属性や Acct-Tunnel-Connection-ID 属性と一緒に使用して、アカウンティングと監査の目的でトンネルを特定する、グローバルで一意の手段を提供できます。 次のように、この属性の 127.0.0.X の値を受け入れるためにネットワーク アクセス サーバの機能が拡張されています。 127.0.0.0 は loopback0 の IP アドレスを使用する必要があることを示し、127.0.0.1 は loopback1 の IP アドレスを使用する必要があることを示します。127.0.0.X は、実際のトンネル クライアント エンドポイントの IP アドレスに loopbackX の IP アドレスを使用する必要があることを示します。この機能拡張によって、複数のネットワーク アクセス サーバ全体のスケーラビリティが向上します。

番号	IETF 属性	説明
67	Tunnel-Server-Endpoint1	トンネルのサーバ端のアドレスを示します。この属性のフォーマットは、Tunnel-Medium-Type の値によって異なります。リリースによっては、トンネル メディア タイプとして IP のみがサポートされ、IP アドレスまたは LNS のホスト名がこの属性に使用できる場合があります。
68	Acct-Tunnel-Connection-ID	トンネル セッションに割り当てられた識別子を示します。この属性は、Start、Stop、または上記のいずれかを値として持つ Acct-Status-Type 属性と一緒に Accounting-Request パケットに含める必要があります。この属性は、Tunnel-Client-Endpoint 属性や Tunnel-Server-Endpoint 属性と一緒に使用して、監査の目的でトンネルセッションを一意に特定する手段を提供できます。
69	Tunnel-Password1	リモート サーバの認証に使用されるパスワードを定義します。この属性は、Tunnel-Type の値（AAA_ATTR_l2tp_tunnel_pw (L2TP)、AAA_ATTR_nas_password (L2F)、および AAA_ATTR_gw_password (L2F)）に基づいて、さまざまな AAA 属性に変換されます。 デフォルトで、受信されたすべてのパスワードが暗号化されます。そのため、NAS が暗号化されていないパスワードを復号化しようとすると、認可エラーが発生する可能性があります。属性 69 を有効にして、暗号化されていないパスワードを受信できるようにするには、グローバル コンフィギュレーション モードで **radius-server attribute 69 clear** コマンドを使用します。
70	ARAP-Password	AppleTalk Remote Access Control（ARAP）の Framed-Protocol を含む Access-Request パケットを識別します。

番号	IETF 属性	説明
71	ARAP-Features	ARAP feature flags パケットで NAS からユーザに送信する必要のあるパスワード情報が含まれています。
72	ARAP-Zone-Access	ユーザの ARAP ゾーン リストの使用方法を示します。
73	ARAP-Security	Access-Challenge パケット内で使用すべき ARAP セキュリティ モジュールを示します。
74	ARAP-Security-Data	Access-Challenge および Access-Request パケットに実際のセキュリティモジュールのチャレンジまたは応答が含まれています。
75	Password-Retry	ユーザが切断されるまでに認証を試みることができる回数を示します。
76	Prompt	ユーザの応答をエコーすべきか否かを NAS に指示します（0 = エコーなし、1 = エコーあり）。
77	Connect-Info	モデム コールに関する追加情報を提供します。この属性は start と stop のアカウンティング レコード内で生成されます。
78	Configuration-Token	使用するユーザ プロファイルのタイプを示します。この属性は、プロキシに基づく大規模な分散認証ネットワークで使用する必要があります。 Access-Accept 内で RADIUS プロキシ サーバから RADIUS プロキシ クライアントに送信されます。NAS には送信しないでください。
79	EAP-Message	Extended Access Protocol（EAP）プロトコルを理解していなくても、NAS で EAP を使用してダイヤルイン ユーザを認証できるように EAP パケットをカプセル化します。
80	Message-Authenticator	CHAP、ARAP、または EAP 認証方式を使用して Access-Requests のスプーフィングを阻止します。

番号	IETF 属性	説明
81	Tunnel-Private-Group-ID	特定のトンネル化されたセッションのグループ ID を示します。
82	Tunnel-Assignment-ID1	セッションが割り当てられた特定のトンネル イニシエータを示します。
83	Tunnel-Preference	各トンネルに割り当てられた相対プリファレンスを示します。この属性は、RADIUS サーバからトンネルイニシエータに複数のトンネリング属性のセットが返される場合に含める必要があります。
84	ARAP-Challenge-Response	ダイヤルイン クライアントのチャレンジに対する応答が含まれています。
85	Acct-Interim-Interval	この特定のセッションの一時更新間隔を秒数で示します。この値は、Access-Accept メッセージにのみ含めることができます。
86	Acct-Tunnel-Packets-Lost	特定のリンク上で失われたパケット数を示します。この属性は、Tunnel-Link-Stop の値を持つ Acct-Status-Type 属性と一緒に Accounting-Request パケットに含める必要があります。
87	NAS-Port-ID	ユーザを認証している NAS のポートを識別するテキスト文字列が含まれています。
88	Framed-Pool	ユーザにアドレスを割り当てるために使用すべき、割り当て済みのアドレス プールの名前が含まれています。NAS が複数のアドレス プールをサポートしていない場合は、この属性を無視する必要があります。
90	Tunnel-Client-Auth-ID	トンネル セットアップをトンネル ターミネータで認証するときに、トンネル イニシエータ（NAS とも呼ばれる）で使用される名前を示します。L2F プロトコルと L2TP プロトコルをサポートします。

番号	IETF 属性	説明
91	Tunnel-Server-Auth-ID	トンネル セットアップをトンネル イニシエータで認証するときに、トンネル ターミネータ（ホーム ゲートウェイとも呼ばれる）で使用される名前を示します。L2F プロトコルと L2TP プロトコルをサポートします。
200	IETF-Token-Immediate	ファイル エントリがハンドヘルド セキュリティ カード サーバを示しているログインユーザから受け取ったパスワードを RADIUS でどのように処理するかを決定します。 この属性の値は次のように数値で指定されます。 • 0：No - パスワードは無視されます。 • 1：Yes - パスワードが認証に使用されます。

[4] この RADIUS 属性は、2 つのドラフト IETF 文書、RFC 2868『RADIUS Attributes for Tunnel Protocol Support』と RFC 2867『RADIUS Accounting Modifications for Tunnel Protocol Support』に基づきます。

その他の参考資料

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『Master Commands List, All Releases』

関連項目	マニュアル タイトル
セキュリティ コマンド	• 『Security Command Reference: Commands A to C』 • 『Security Command Reference: Commands D to L』 • 『Security Command Reference: Commands M to R』 • 『Security Command Reference: Commands S to Z』

RFC

RFC	タイトル
RFC 2865	『Remote Authentication Dial In User Service (RADIUS)』
RFC 2866	『RADIUS Accounting』
RFC 2867	『RADIUS Accounting Modifications for Tunnel Protocol Support』
RFC 2868	『RADIUS Attributes for Tunnel Protocol Support』
RFC 2869	『RADIUS Extensions』

シスコのテクニカル サポート

説明	リンク
右の URL にアクセスして、シスコのテクニカル サポートを最大限に活用してください。これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

RADIUS 属性の概要と RADIUS IETF 属性の機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *93 : RADIUS* 属性の概要と *RADIUS IETF* 属性の機能情報

機能名	リリース	機能情報
RADIUS IETF 属性	Cisco IOS Release 11.1	この機能は、Cisco IOS Release 11.1 で導入されました。

第 66 章

RADIUS ベンダー固有属性

IETF ドラフト標準には、RADIUS でのネットワーク アクセス サーバと RADIUS サーバ間でベンダー固有情報を通信する方式が規定されています。ただし、ベンダーには固有のアプリケーション向けに拡張した RADIUS 属性セットを持つものがあります。このマニュアルでは、これらベンダー固有 RADIUS 属性の Cisco IOS XE でのサポート情報について記載します。

サポートされるベンダー固有 RADIUS 属性

次の表に、シスコがサポートしているベンダー固有 RADIUS 属性およびこれらを実装している Cisco IOS XE リリースを示します。属性がセキュリティ サーバ固有の形式の場合は、この形式が指定されます。それぞれの説明については、ベンダー固有 RADIUS 属性の表を参照してください。

表 *94* : サポートされるベンダー固有 *RADIUS* 属性

番号	ベンダー固有属性	IOS XE 2.1
17	Change-Password	yes
21	Password-Expiration	yes
68	Tunnel-ID	yes
108	My-Endpoint-Disc-Alias	no
109	My-Name-Alias	no
110	Remote-FW	no
111	Multicast-GLeave-Delay	no
112	CBCP-Enable	no

番号	ベンダー固有属性	IOS XE 2.1
113	CBCP-Mode	no
114	CBCP-Delay	no
115	CBCP-Trunk-Group	no
116	Appletalk-Route	no
117	Appletalk-Peer-Mode	no
118	Route-Appletalk	no
119	FCP-Parameter	no
120	Modem-PortNo	no
121	Modem-SlotNo	no
122	Modem-ShelfNo	no
123	Call-Attempt-Limit	no
124	Call-Block-Duration	no
125	Maximum-Call-Duration	no
126	Router-Preference	no
127	Tunneling-Protocol	no
128	Shared-Profile-Enable	no
129	Primary-Home-Agent	no
130	Secondary-Home-Agent	no
131	Dialout-Allowed	no
133	BACP-Enable	no
134	DHCP-Maximum-Leases	no
135	Primary-DNS-Server	yes
136	Secondary-DNS-Server	yes
137	Ascend-Client-Assign-DNS	no
138	User-Acct-Type	no
139	User-Acct-Host	no
140	User-Acct-Port	no

番号	ベンダー固有属性	IOS XE 2.1
141	User-Acct-Key	no
142	User-Acct-Base	no
143	User-Acct-Time	no
144	Assign-IP-Client	no
145	Assign-IP-Server	no
146	Assign-IP-Global-Pool	no
147	DHCP-Reply	no
148	DHCP-Pool-Number	no
149	Expect-Callback	no
150	Event-Type	no
151	Ascend-Session-Svr-Key	yes
152	Ascend-Multicast-Rate-Limit	yes
153	IF-Netmask	no
154	h323-Remote-Address	no
155	Ascend-Multicast-Client	yes
156	FR-Circuit-Name	no
157	FR-LinkUp	no
158	FR-Nailed-Grp	no
159	FR-Type	no
160	FR-Link-Mgt	no
161	FR-N391	no
162	FR-DCE-N392	no
163	FR-DTE-N392	no
164	FR-DCE-N393	no
165	FR-DTE-N393	no
166	FR-T391	no
167	FR-T392	no

番号	ベンダー固有属性	IOS XE 2.1
168	Bridge-Address	no
169	TS-Idle-Limit	no
170	TS-Idle-Mode	no
171	DBA-Monitor	no
172	Base-Channel-Count	no
173	Minimum-Channels	no
174	IPX-Route	no
175	FT1-Caller	no
176	Ipsec-Backup-Gateway	yes
177	rm-Call-Type	yes
178	Group	no
179	FR-DLCI	no
180	FR-Profile-Name	no
181	Ara-PW	no
182	IPX-Node-Addr	no
183	Home-Agent-IP-Addr	no
184	Home-Agent-Password	no
185	Home-Network-Name	no
186	Home-Agent-UDP-Port	no
187	Multilink-ID	yes
188	Ascend-Num-In-Multilink	yes
189	First-Dest	no
190	Pre-Bytes-In	yes
191	Pre-Bytes-Out	yes
192	Pre-Paks-In	yes
193	Pre-Paks-Out	yes
194	Maximum-Time	yes

番号	ベンダー固有属性	IOS XE 2.1
195	Disconnect-Cause	yes
196	Connect-Progress	yes
197	Data-Rate	yes
198	PreSession-Time	yes
199	Token-Idle	no
201	Require-Auth	no
202	Number-Sessions	no
203	Authen-Alias	no
204	Token-Expiry	no
205	Menu-Selector	no
206	Menu-Item	no
207	PW-Warntime	no
208	PW-Lifetime	yes
209	IP-Direct	yes
210	PPP-VJ-Slot-Compression	yes
211	PPP-VJ-1172	no
212	PPP-Async-Map	no
213	Third-Prompt	no
214	Send-Secret	yes
215	Receive-Secret	no
216	IPX-Peer-Mode	no
217	IP-Pool	yes
218	Static-Addr-Pool	yes
219	FR-Direct	no
220	FR-Direct-Profile	no
221	FR-Direct-DLCI	no
222	Handle-IPX	no

番号	ベンダー固有属性	IOS XE 2.1
223	Netware-Timeout	no
224	IPX-Alias	no
225	Metric	no
226	PRI-Number-Type	no
227	Dial-Number	yes
228	Route-IP	yes
229	Route-IPX	no
230	Bridge	no
231	Send-Auth	yes
232	Send-Passwd	no
233	Link-Compression	yes
234	Target-Util	yes
235	Maximum-Channels	yes
236	Inc-Channel-Count	no
237	Dec-Channel-Count	no
238	Seconds-of-History	no
239	History-Weigh-Type	no
240	Add-Seconds	no
241	Remove-Seconds	no
242	Data-Filter	yes
243	Call-Filter	no
244	Idle-Limit	yes
245	Preempt-Limit	no
246	Callback	no
247	Data-Service	yes
248	Force-56	yes
249	Billing Number	no

番号	ベンダー固有属性	IOS XE 2.1
250	Call-By-Call	no
251	Transit-Number	no
252	Host-Info	no
253	PPP-Address	no
254	MPP-Idle-Percent	no
255	Xmit-Rate	yes

ベンダー固有 RADIUS 属性の説明に関する包括的なリスト

次の表に、既知のベンダー固有 RADIUS 属性の一覧と説明を示します。

表 *95 :* ベンダー固有 *RADIUS* 属性

番号	ベンダー固有属性	説明
17	Change-Password	ユーザのパスワード変更要求を指定します。
21	Password-Expiration	ユーザのファイル エントリのユーザ パスワードの有効期限を指定します。
68	Tunnel-ID	（Ascend 5）CLID または DNIS トンネリングを使用する各セッションで、RADIUS により割り当てられるストリングを指定します。アカウンティングが実装されている場合、この値はアカウンティングに使用されます。
108	My-Endpoint-Disc-Alias	（Ascend 5）説明はありません。
109	My-Name-Alias	（Ascend 5）説明はありません。
110	Remote-FW	（Ascend 5）説明はありません。
111	Multicast-GLeave-Delay	（Ascend 5）説明はありません。
112	CBCP-Enable	（Ascend 5）説明はありません。
113	CBCP-Mode	（Ascend 5）説明はありません。
114	CBCP-Delay	（Ascend 5）説明はありません。

番号	ベンダー固有属性	説明
115	CBCP-Trunk-Group	（Ascend 5）説明はありません。
116	Appletalk-Route	（Ascend 5）説明はありません。
117	Appletalk-Peer-Mode	（Ascend 5）説明はありません。
118	Route-Appletalk	（Ascend 5）説明はありません。
119	FCP-Parameter	（Ascend 5）説明はありません。
120	Modem-PortNo	（Ascend 5）説明はありません。
121	Modem-SlotNo	（Ascend 5）説明はありません。
122	Modem-ShelfNo	（Ascend 5）説明はありません。
123	Call-Attempt-Limit	（Ascend 5）説明はありません。
124	Call-Block-Duration	（Ascend 5）説明はありません。
125	Maximum-Call-Duration	（Ascend 5）説明はありません。
126	Router-Preference	（Ascend 5）説明はありません。
127	Tunneling-Protocol	（Ascend 5）説明はありません。
128	Shared-Profile-Enable	（Ascend 5）説明はありません。
129	Primary-Home-Agent	（Ascend 5）説明はありません。
130	Secondary-Home-Agent	（Ascend 5）説明はありません。
131	Dialout-Allowed	（Ascend 5）説明はありません。
133	BACP-Enable	（Ascend 5）説明はありません。
134	DHCP-Maximum-Leases	（Ascend 5）説明はありません。
135	Primary-DNS-Server	Microsoft PPP クライアントにより IPCP ネゴシエーション中にネットワーク アクセス サーバから要求される可能性がある、プライマリ DNS サーバを特定します。
136	Secondary-DNS-Server	Microsoft PPP クライアントにより IPCP ネゴシエーション中にネットワーク アクセス サーバから要求される可能性がある、セカンダリ DNS サーバを特定します。
137	Client-Assign-DNS	説明はありません。
138	User-Acct-Type	説明はありません。

番号	ベンダー固有属性	説明
139	User-Acct-Host	説明はありません。
140	User-Acct-Port	説明はありません。
141	User-Acct-Key	説明はありません。
142	User-Acct-Base	説明はありません。
143	User-Acct-Time	説明はありません。
144	Assign-IP-Client	説明はありません。
145	Assign-IP-Server	説明はありません。
146	Assign-IP-Global-Pool	説明はありません。
147	DHCP-Reply	説明はありません。
148	DHCP-Pool-Number	説明はありません。
149	Expect-Callback	説明はありません。
150	Event-Type	説明はありません。
151	Session-Svr-Key	説明はありません。
152	Multicast-Rate-Limit	説明はありません。
153	IF-Netmask	説明はありません。
154	Remote-Addr	説明はありません。
155	Multicast-Client	説明はありません。
156	FR-Circuit-Name	説明はありません。
157	FR-LinkUp	説明はありません。
158	FR-Nailed-Grp	説明はありません。
159	FR-Type	説明はありません。
160	FR-Link-Mgt	説明はありません。
161	FR-N391	説明はありません。
162	FR-DCE-N392	説明はありません。
163	FR-DTE-N392	説明はありません。

番号	ベンダー固有属性	説明
164	FR-DCE-N393	説明はありません。
165	FR-DTE-N393	説明はありません。
166	FR-T391	説明はありません。
167	FR-T392	説明はありません。
168	Bridge-Address	説明はありません。
169	TS-Idle-Limit	説明はありません。
170	TS-Idle-Mode	説明はありません。
171	DBA-Monitor	説明はありません。
172	Base-Channel-Count	説明はありません。
173	Minimum-Channels	説明はありません。
174	IPX-Route	説明はありません。
175	FT1-Caller	説明はありません。
176	Backup	説明はありません。
177	Call-Type	説明はありません。
178	Group	説明はありません。
179	FR-DLCI	説明はありません。
180	FR-Profile-Name	説明はありません。
181	Ara-PW	説明はありません。
182	IPX-Node-Addr	説明はありません。
183	Home-Agent-IP-Addr	Ascend Tunnel Management Protocol（ATMP）を使用する際に、ホーム エージェントの IP アドレスをドット付き 10 進表記で示します。
184	Home-Agent-Password	ATMP で、外部のエージェントが自身の認証に使用するパスワードを指定します。
185	Home-Network-Name	ATMP で、ホーム エージェントがすべてのパケットを送信する接続プロファイルの名前を示します。

番号	ベンダー固有属性	説明
186	Home-Agent-UDP-Port	外部のエージェントが ATMP メッセージをホーム エージェントに送信する際に使用する UDP ポート番号を示します。
187	Multilink-ID	セッションが終了した時のマルチリンク バンドルの ID 番号をレポートします。この属性は、マルチリンク バンドルの一部のセッションに適用されます。Multilink-ID 属性は、認証応答パケットに送信されます。
188	Num-In-Multilink	アカウンティング終了パケットでレポートされたセッションが終了したときにマルチリンク バンドルに残っているセッション数をレポートします。この属性は、マルチリンク バンドルの一部のセッションに適用されます。Num-In-Multilink 属性は、認証応答パケットと一部のアカウンティング要求パケットで送信されます。
189	First-Dest	認証後最初に受信したパケットの宛先 IP アドレスを記録します。
190	Pre-Bytes-In	認証前の入力バイト数を記録します。Pre-Bytes-In 属性は、アカウンティング終了記録で送信されます。
191	Pre-Bytes-Out	認証前の出力バイト数を記録します。Pre-Bytes-Out 属性は、アカウンティング終了記録で送信されます。
192	Pre-Paks-In	認証前の入力パケット数を記録します。Pre-Paks-In 属性は、アカウンティング終了記録で送信されます。
193	Pre-Paks-Out	認証前の出力パケット数を記録します。Pre-Paks-Out 属性は、アカウンティング終了記録で送信されます。
194	Maximum-Time	任意のセッションで許可される最大時間長を秒で指定します。セッションがこの制限した時間に達すると、接続がドロップします。
195	Disconnect-Cause	接続がオフラインになった理由を特定します。Disconnect-Cause 属性は、アカウンティング終了記録で送信されます。また、この属性で、認証が実行される前に接続が切断された場合、最初に開始レコードを生成せずに終了レコードが生成されます。意味の詳細については、ベンダー固有属性（VSA）およびRADIUS Disconnect-Cause 属性値の説明を参照してください。
196	Connect-Progress	接続が切断される前の接続状態を示します。
197	Data-Rate	接続のライフタイムでの平均ビット/秒値を指定します。Data-Rate 属性は、アカウンティング終了記録で送信されます。

番号	ベンダー固有属性	説明
198	PreSession-Time	コールが最初に接続された時から認証が完了した時までの時間長を秒で指定します。PreSession-Time 属性は、アカウンティング終了記録で送信されます。
199	Token-Idle	キャッシュされたトークンが認証間での接続を持続できる最長時間を分で示します。
201	Require-Auth	CLID 認証が行われたクラスで、追加認証が必要かどうかを定義します。
202	Number-Sessions	RADIUS アカウンティング サーバにレポートするクラスごとのアクティブ セッション数を指定します。
203	Authen-Alias	PPP 認証中の RADIUS サーバのログイン名を定義します。
204	Token-Expiry	キャッシュされたトークンのライフタイムを定義します。
205	Menu-Selector	ユーザにデータの入力を指示するために使用するストリングを定義します。
206	Menu-Item	ユーザプロファイルの単一メニュー項目を指定します。プロファイルごとに最大 20 のメニュー項目を割り当てられます。
207	PW-Warntime	（Ascend 5）説明はありません。
208	PW-Lifetime	ユーザ単位ベースで、パスワードの有効日数を指定できます。
209	IP-Direct	この属性をユーザのファイル エントリに含めると、フレームルートがルーティングおよびブリッジング テーブルにインストールされます。 （注） パケット ルーティングは、この新しくインストールしたエントリだけではなくテーブル全体に依存しています。この属性を含めても、すべてのパケットが指定の IP アドレスに送信されるとは限りません。したがって、この属性は、完全にサポートされていません。このような属性の制限は、Cisco ルータが内部ルーティングやブリッジング テーブルを一部しかバイパスできず、指定した IP アドレスにパケットを送信できないために起こります。
210	PPP-VJ-Slot-Comp	VJ 圧縮パケットを PPP リンク経由で送信する際に、Cisco ルータでスロット圧縮しないように指示します。
211	PPP-VJ-1172	PPP で、VJ 圧縮に 0x0037 値を使用するように指示します。

番号	ベンダー固有属性	説明
212	PPP-Async-Map	Ciscoルータに、PPPセッション用の非同期制御文字マップを提供します。指定した制御文字は、PPP リンク経由でデータとして渡され、リンク上で起動しているアプリケーションで使用されます。
213	Third-Prompt	ユーザ名とパスワードの次の、ユーザが追加で入力する 3 番めのプロンプトを定義します。
214	Send-Secret	アウトダイヤルパスワードの通常のパスワードの代わりに暗号化パスワードを使用できるようにします。
215	Receive-Secret	暗号化パスワードを RADIUS サーバで検証できるようにします。
216	IPX-Peer-Mode	（Ascend 5）説明はありません。
217	IP-Pool-Definition	アドレスのプールを X a.b.c Z の形式で定義します。ここで、X はプール インデックス番号、a.b.cはプールの開始IPアドレス、Z はプールの IP アドレス数です。たとえば、3 10.0.0.1 5 は、10.0.0.1 から 10.0.0.5 までをダイナミック割り当てに割り当てます。
218	Assign-IP-Pool	ルータに、ユーザおよび IP アドレスを IP プールから割り当てるよう指示します。
219	FR-Direct	フレーム リレー リダイレクト モードで接続プロファイルを処理するかどうかを定義します。
220	FR-Direct-Profile	この接続をフレーム リレー スイッチまで伝送するフレーム リレー プロファイルの名前を定義します。
221	FR-Direct-DLCI	この接続をフレーム リレー スイッチまで伝送する DLCI を示します。
222	Handle-IPX	NCP のウォッチドッグ要求の処理方法を示します。
223	Netware-Timeout	RADIUS サーバが NCP ウォッチドッグ パケットに応答する時間を分で定義します。
224	IPX-Alias	番号が付いたインターフェイスが必要な IPX ルータでエイリアスを定義できます。
225	Metric	説明はありません。
226	PRI-Number-Type	説明はありません。
227	Dial-Number	ダイヤルする番号を定義します。

番号	ベンダー固有属性	説明
228	Route-IP	IP ルーティングがユーザのファイルエントリで許可されているかどうかを示します。
229	Route-IPX	IPX ルーティングをイネーブルにできます。
230	Bridge	説明はありません。
231	Send-Auth	CLID 認証に続く、username-password 認証で使用するプロトコル（PAP または CHAP）を定義します。
232	Send-Passwd	RADIUS サーバで、発信コールの接続のリモートエンドに送信するパスワードを指定できます。
233	Link-Compression	PPP リンクで「stac」圧縮をオンまたはオフのどちらにするかを定義します。 リンク圧縮は、次のように、数値で定義します。 • 0：なし • 1：Stac • 2：Stac-Draft-9 • 3：MS-Stac
234	Target-Util	PPP マルチリンクが定義されている場合に、追加チャネルを立ち上げる負荷しきい値を割合で指定します。
235	Maximum-Channels	割り当て済み/割り当て可能な最大チャネル数を指定します。
236	Inc-Channel-Count	説明はありません。
237	Dec-Channel-Count	説明はありません。
238	Seconds-of-History	説明はありません。
239	History-Weigh-Type	説明はありません。
240	Add-Seconds	説明はありません。
241	Remove-Seconds	説明はありません。

番号	ベンダー固有属性	説明
242	Data-Filter	ユーザごとの IP データ フィルタを定義します。これらのフィルタは、コールが RADIUS 発信プロファイルを使用して発信された場合か、RADIUS 着信プロファイルを使用して応答した場合にのみ取得されます。最初に一致したフィルタのエントリが適用されます。したがって、フィルタのエントリの入力順が重要です。
243	Call-Filter	ユーザごとの IP データ フィルタを定義します。Cisco ルータでは、この属性は Data-Filter 属性と同一です。
244	Idle-Limit	セッションがアイドル状態を持続できる最大時間を秒で指定します。セッションがこのアイドル時間に達すると、接続がドロップします。
245	Preempt-Limit	説明はありません。
246	Callback	コールバックをイネーブルまたはディセーブルにできます。
247	Data-Svc	説明はありません。
248	Force-56	チャネルの 64 K すべてが使用可能に見える場合でも、ネットワーク アクセス サーバが 56 K の部分のみを使用するかどうかを指定します。
249	Billing Number	説明はありません。
250	Call-By-Call	説明はありません。
251	Transit-Number	説明はありません。
252	Host-Info	説明はありません。
253	PPP-Address	PPP IPCP ネゴシエーション中に発信ユニットにレポートされた IP アドレスを示します。
254	MPP-Idle-Percent	説明はありません。
255	Xmit-Rate	（Ascend 5）説明はありません。

ベンダー固有 RADIUS 属性の詳細については、「RADIUS の設定」機能モジュールを参照してください。

RADIUS ベンダー固有属性の機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *96 : RADIUS* ベンダー固有属性の機能情報

機能名	リリース	機能情報
RADIUS ベンダー固有属性	Cisco IOS XE Release 2.1	IETF ドラフト標準には、RADIUS でのネットワーク アクセス サーバと RADIUS サーバ間でベンダー固有情報を通信する方式が規定されています。ただし、ベンダーには固有のアプリケーション向けに拡張した RADIUS 属性セットを持つものがあります。このマニュアルでは、これらベンダー固有 RADIUS 属性の Cisco IOS XE でのサポート情報について記載します。 Cisco IOS XE Release 2.1 では、Cisco ASR 1000 シリーズ Aggregation Services Router にこの機能が実装されました。

第 67 章

RADIUS ベンダー固有属性および RADIUS Disconnect-Cause 属性値

インターネット技術特別調査委員会（IETF）ドラフト標準には、ネットワーク アクセス サーバと RADIUS サーバの間でベンダー固有属性（属性 26）を使用してベンダー固有の情報を伝達する方法が規定されています。属性26はベンダー固有属性をカプセル化します。このため、ベンダーは一般的な用途に適さない独自の拡張属性をサポートできます。

RADIUS ベンダー固有属性および RADIUS Disconnect-Cause 属性値に関する情報

シスコの RADIUS 実装は、この仕様で推奨される形式を使用して、1 つのベンダー固有オプションをサポートしています。シスコのベンダー ID は 9 であり、サポート対象のオプションはベンダータイプ 1（名前は「cisco-avpair」）です。値は、次の形式のストリングです。

```
protocol : attribute sep value *
```

「Protocol」は、特定の認可タイプを表すシスコの「protocol」属性です。使用可能なプロトコルには、IP、IPX、VPDN、VOIP、SHELL、RSVP、SIP、AIRNET、OUTBOUND があります。「attribute」および「value」は、シスコの TACACS+ 仕様で定義されている適切な属性値（AV）ペアです。「sep」は、必須の属性の場合は「=」、任意指定の属性の場合は「*」です。これにより、TACACS+ 認可で使用できるすべての機能を RADIUS にも使用できるようになります。

たとえば、次の AV ペアは IP 許可の際（PPP の IPCP アドレス割り当ての際）、シスコの「multiple named ip address pools」機能を起動します。

```
cisco-avpair= ”ip:addr-pool=first“
```

「*」を挿入すると、AV ペア「ip:addr-pool=first」は任意指定になります。AV ペアはオプションにできることに注意してください。

```
cisco-avpair= ”ip:addr-pool*first“
```

次に、ネットワーク アクセス サーバからユーザがログインしたときに、すぐに EXEC コマンドを実行する方法の例を示します。

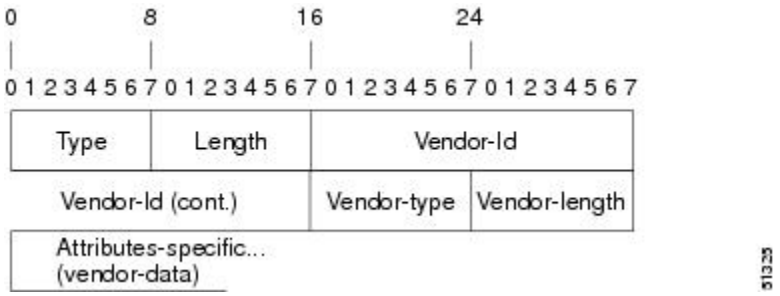
```
cisco-avpair= ”shell:priv-lvl=15“
```

属性 26 には、次の 3 つの要素が含まれています。

- タイプ
- 長さ
- ストリング（またはデータ）
  - Vendor-Id
  - Vendor-Type
  - Vendor-Length
  - Vendor-Data

次の図は、属性 26 の「背後で」カプセル化される VSA のパケット形式を示します。

図 *11* : 属性 *26* の背後でカプセル化される *VSA*



（注） VSA の形式はベンダーが指定します。Attribute-Specific フィールド（Vendor-Data とも呼ばれる）は、ベンダーによるその属性の定義によって異なります。

次の表に、「ベンダー固有 RADIUS IETF 属性テーブル」（次の 2 番目の表）で表示される重要なフィールドを示します。これは、サポート対象のベンダー固有 RADIUS 属性（IETF 属性 26）を表示します。

表 *97* : ベンダー固有属性表のフィールドの説明

フィールド	説明
番号	次の表に示されるすべての属性は、IETF 属性 26 の拡張です。
ベンダー固有のコマンドコード	特定のベンダーの識別に使用する定義されたコード。コード 9 は Cisco VSA、311 は Microsoft VSA、529 は Ascend VSA を定義します。
サブタイプ番号	属性 ID 番号。この番号は、属性 26 の背後でカプセル化される「2 番めのレイヤ」の ID 番号であること以外、IETF 属性の ID 番号に似ています。
属性	属性の ASCII ストリング名。
説明	属性の説明。

表 *98* : ベンダー固有 *RADIUS IETF* 属性

番号	ベンダー固有の企業コード	サブタイプ番号	属性	説明
MS-CHAP 属性				
26	311	1	MSCHAP-Response	PPP MS-CHAP ユーザがチャレンジに対する応答で提供するレスポンス値が含まれます。Access-Request パケットでしか使用されません。この属性は、PPP CHAP ID と同じです（RFC 2548）。
26	311	11	MSCHAP-Challenge	ネットワーク アクセス サーバが MS-CHAP ユーザに送信するチャレンジが含まれます。これは、Access-Request パケットと Access-Challenge パケットの両方で使用できます。（RFC 2548）。
VPDN 属性				
26	9	1	l2tp-busy-disconnect	LNS の vpdn-group で、事前にコピーするよう設定された仮想テンプレートを使用している場合、この属性は、接続先の事前にコピーされたインターフェイスが検索されない、新しい L2TP セッションのディスポジションを制御します。属性が true（デフォルト）の場合、セッションが LNS により切断されます。そうでない場合は、新しいインターフェイスが仮想テンプレートからコピーされます。
26	9	1	l2tp-cm-local-window-size	L2TP 制御メッセージの最大受信ウィンドウ サイズを指定します。この値は、トンネルの確立中にピアにアドバタイズされます。

番号	ベンダー固有の企業コード	サブタイプ番号	属性	説明
26	9	1	l2tp-drop-out-of-order	正しくない順序で受信したデータ パケットをドロップして、シーケンス番号を順守します。これは受信した場合の処理方法であって、データ パケット上でシーケンス番号が送信されるわけではありません。
26	9	1	l2tp-hello-interval	hello キープアライブ インターバルの秒数を指定します。ここで指定した秒数、トンネルでデータが送信されないと、hello パケットが送信されます。
26	9	1	l2tp-hidden-avp	イネーブルにすると、L2TP 制御メッセージで、大文字小文字を区別する AVP にスクランブルがかけられるか、または非表示になります。
26	9	1	l2tp-nosession-timeout	タイムアウトおよびシャットダウンまでに、セッションなしでトンネルがアクティブのままになる秒数を指定します。
26	9	1	tunnel-tos-reflect	LNS でトンネルに入るパケットに対して、IP ToS フィールドを各ペイロード パケットの IP ヘッダーからトンネル パケットの IP ヘッダーにコピーします。
26	9	1	l2tp-tunnel-authen	この属性を設定すると、L2TP トンネル認証が実行されます。
26	9	1	l2tp-tunnel-password	L2TP トンネル認証および AVP 隠蔽に使用される共有秘密。
26	9	1	l2tp-udp-checksum	これは認可属性で、L2TP がデータ パケットに対して UDP チェックサムを実行する必要があるかどうかを定義します。有効な値は「yes」と「no」です。デフォルトは「no」です。
H323 属性				
26	9	23	Remote-Gateway-ID（h323-remote-address）	リモート ゲートウェイの IP アドレスを示します。
26	9	24	Connection-ID（h323-conf-id）	会議 ID を識別します。
26	9	25	Setup-Time（h323-setup-time）	以前、グリニッジ標準時（GMT）およびズール タイムと呼ばれていた協定世界時（UTC）でのこの接続のセットアップ時間を示します。

番号	ベンダー固有の企業コード	サブタイプ番号	属性	説明
26	9	26	Call-Origin（h323-call-origin）	ゲートウェイに対するコールの発行元を示します。有効値は、originating および terminating です（回答）。
26	9	27	Call-Type（h323-call-type）	コールのレグ タイプを示します。使用可能な値は **telephony** と **VoIP** です。
26	9	28	Connect-Time（h323-connect-time）	このコール レッグの UTC での接続時間を示します。
26	9	29	Disconnect-Time（h323-disconnect-time）	このコール レッグが UTC で接続解除された時間を示します。
26	9	30	Disconnect-Cause（h323-disconnect-cause）	Q.931 仕様によって、接続がオフラインにされた理由を示します。
26	9	31	Voice-Quality（h323-voice-quality）	コールの音声品質に影響する Impairment Factor（ICPIF）を指定します。
26	9	33	Gateway-ID（h323-gw-id）	下位のゲートウェイの名前を示します。
大規模のダイヤルアウト属性				
26	9	1	callback-dialstring	コールバックに使用するダイヤリング文字列を定義します。
26	9	1	data-service	説明はありません。
26	9	1	dial-number	ダイヤルする番号を定義します。
26	9	1	force-56	チャネルの 64 K すべてが使用可能に見える場合でも、ネットワーク アクセス サーバが 56 K の部分のみを使用するかどうかを指定します。
26	9	1	map-class	ユーザ プロファイルに、ダイヤルアウトするネットワーク アクセス サーバ上で同じ名前のマップ クラスで設定される情報の参照を許可します。
26	9	1	send-auth	CLID 認証に続く、username-password 認証で使用するプロトコル（PAP または CHAP）を定義します。

番号	ベンダー固有の企業コード	サブタイプ番号	属性	説明
その他の属性				
26	9	2	Cisco-NAS-Port	NAS-Port アカウンティングに追加的なベンダー固有属性（VSA）を指定します。属性値ペア（AVPair）ストリングの形式で追加的な NAS-Port 情報を指定するには、radius-server vsa send グローバル コンフィギュレーション コマンドを使用します。 （注） この VSA は、通常アカウンティングで使用されますが認証（Access-Request）パケットで使用される場合もあります。
26	9	1	min-links	MLP に対するリンクの最小数を設定します。
26	9	1	proxyacl#<n>	ダウンロード可能なユーザ プロファイル（ダイナミック ACL）を、認証プロキシを使用して設定でき、これにより設定されたインターフェイスのトラフィックの通過を許可するよう、認証を設定できます。
26	9	1	spi	登録中にホーム エージェントがモバイル ノードの認証で必要とする認証情報を伝送します。この情報は、**ip mobile secure host <addr>** コンフィギュレーション コマンドと同じ構文です。基本的に、この文字列に続く残りのコンフィギュレーション コマンドはそのまま含まれます。これにはセキュリティ パラメータ インデックス（SPI）、キー、認証アルゴリズム、認証モード、およびリプレイ保護タイムスタンプ範囲が含まれています。
26	9	1	client-mac-address	PPPoE クライアントの MAC アドレスが含まれます。 （注） この属性は、PPP over Ethernet（PPPoE）または PPP over ATM（PPPoA）にのみ適用できます。

NAS を設定して VSA を認識し使用する方法については、「RADIUS の設定」機能モジュールの「ベンダー固有RADIUS属性を使用するためのルータの設定」セクションを参照してください。

RADIUS Disconnect-Cause 属性値

Disconnect-cause 属性値は、接続がオフラインにされた理由を指定します。属性値は、アカウンティング要求パケットで送信されます。セッションの認証が失敗しても、これらの値は、セッションの終了時に送信されます。セッションが認証されないと、属性が開始レコードを生成せずに終了レコードを発生させる可能性があります。

次の表に、Disconnect-Cause（195）属性の原因コード、値、および説明を示します。

（注） Disconnect-Cause は、RADIUS AVPairs で使用されるごとに 1000 ずつ増分されます。たとえば、disc-cause 4 は 1004 になります。

表 *99 : Disconnect-Cause* 属性値

原因コード	値	説明
2	Unknown	理由は不明。
4	CLID-Authentication-Failure	calling-party 数の認証の失敗。
10	No-Carrier	キャリアが検出されない。 （注） 最初のモデム接続中に接続解除があると、コード 10、11、および 12 が送信される場合があります。
11	Lost-Carrier	キャリアの喪失。
12	No-Detected-Result-Codes	モデム結果コード検出の失敗。
20	User-Ends-Session	ユーザがセッションを終了した。 （注） コード 20、22、23、24、25、26、27、および 28 は、EXEC セッションに適用されます。
21	Idle-Timeout	ユーザ入力待機中のタイムアウト。 コード 21、100、101、102、および 120 は、すべてのセッション タイプに適用されます。
22	Exit-Telnet-Session	既存の Telnet セッションによる接続解除。
23	No-Remote-IP-Addr	SLIP/PPP への切り替え不能。リモート エンドに IP アドレスがない。
24	Exit-Raw-TCP	既存の raw TCP による接続解除。
25	Password-Fail	間違ったパスワード。

原因コード	値	説明
26	Raw-TCP-Disabled	Raw TCP がディセーブルにされた。
27	Control-C-Detected	Control-C が検出された。
28	EXEC-Process-Destroyed	EXEC プロセスが破棄された。
40	Timeout-PPP-LCP	PPP LCP ネゴシエーションがタイムアウトした。 （注） コード 40、41、42、43、44、45、および 46 は、PPP セッションに適用されます。
41	Failed-PPP-LCP-Negotiation	PPP LCP ネゴシエーションが失敗した。
42	Failed-PPP-PAP-Auth-Fail	PPP PAP 認証が失敗した。
43	Failed-PPP-CHAP-Auth	PPP CHAP 認証が失敗した。
44	Failed-PPP-Remote-Auth	PPP リモート認証が失敗した。
45	PPP-Remote-Terminate	PPP がリモート エンドから Terminate Request を受信した。
46	PPP-Closed-Event	上位層がセッションの終了を要求した。
63	PPP-Echo-Replies	TCP 接続が終了した。
100	Session-Timeout	セッションがタイムアウトした。
101	Session-Failed-Security	セキュリティ上の理由から、セッションが失敗した。
102	Session-End-Callback	コールバックにより、セッションが終了した。
120	Invalid-Protocol	検出されたプロトコルがディセーブルにされていたため、コールが拒否された。
600	VPN-User-Disconnect	クライアントによってコールが接続解除された（PPP 経由）。 LNS がクライアントから PPP terminate request を受信するとコードが送信されます。
601	VPN-Carrier-Loss	キャリアの喪失。これは回線が物理的に普通になった結果である場合があります。 クライアントがダイヤラを使用してダイヤルアウトできない場合、コードが送信されます。
602	VPN-No-Resources	コールの処理に使用できるリソースがない。 クライアントがメモリを割り当てることができない場合、コードが送信されます（メモリの不足）。

原因コード	値	説明
603	VPN-Bad-Control-Packet	L2TP または L2F 制御パケットが間違っている。 このコードは、必須の属性値ペア（AVP）が欠落しているなど、ピアから受信した制御パケットが無効な場合に送信されます。L2TP を使用すると、コードは 6 回の再送信後に送信されます。L2F を使用すると、再送信の回数はユーザ設定が可能です。 （注） トンネルにアクティブなセッションがある場合は、VPN-Tunnel-Shut が送信されます。
604	VPN-Admin-Disconnect	管理上の接続解除。これは、VPN ソフトシャットダウンの結果である場合があります。これは、クライアントが最大セッション制限に達するか、最大ホップカウントを超過した場合に発生します。 トンネルが、**clear vpdn tunnel** コマンドの発行によってダウンした場合に、コードが送信されます。
605	VPN-Tunnel-Shut	トンネルのティアダウン、またはトンネルのセットアップが失敗した。 トンネルにアクティブなセッションがあり、トンネルがダウンした場合にコードが送信されます。 （注） このコードはトンネルの認証が失敗した場合は、送信されません。
606	VPN-Local-Disconnect	LNS PPP モジュールによって、コールが接続解除された。 LNS がクライアントに PPP terminate request を送信するとコードが送信されます。これは通常の PPP 接続解除が LNS によって開始されたことを示します。
607	VPN-Session-Limit	VPN ソフト シャットダウンがイネーブルになった。 前述したソフト シャットダウンの制約事項のいずれかによってコールが拒否されると、コードが送信されます。
611	VPDN-Tunnel-In-Resync	VPDN トンネルは HA 再同期中です。

その他の参考資料

ここでは、RADIUS ベンダー固有属性（VSA）および RADIUS Disconnect-Cause 属性値に関する関連資料について説明します。

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『Cisco IOS Master Commands List, All Releases』
セキュリティ コマンド	『*Cisco IOS Security Command Reference*』
セキュリティ機能	『*Cisco IOS XE Security Configuration Guide: Securing User Services*, Release 2』
セキュリティ サーバ プロトコル	『*Cisco IOS XE Security Configuration Guide: Securing User Services*, Release 2』の「セキュリティ サーバ プロトコル」の項
RADIUS Configuration	「RADIUS の設定」機能モジュール。

標準

標準	タイトル
インターネット技術特別調査委員会（IETF）インターネット ドラフト：Network Access Servers Requirements	「Network Access Servers Requirements: Extended RADIUS Practices」

MIB

MIB	MIB のリンク
なし。	選択したプラットフォーム、Cisco ソフトウェア リリース、およびフィーチャ セットの MIB を検索してダウンロードする場合は、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

RFC

RFC	タイトル
RFC 2865	『Remote Authentication Dial In User Service (RADIUS)』

シスコのテクニカル サポート

説明	リンク
シスコのサポート Web サイトでは、シスコの製品やテクノロジーに関するトラブルシューティングにお役立ていただけるように、マニュアルやツールをはじめとする豊富なオンライン リソースを提供しています。 お使いの製品のセキュリティ情報や技術情報を入手するために、Cisco Notification Service（Field Notice からアクセス）、Cisco Technical Services Newsletter、Really Simple Syndication（RSS）フィードなどの各種サービスに加入できます。 シスコのサポート Web サイトのツールにアクセスする際は、Cisco.com のユーザ ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

RADIUS ベンダー固有属性および RADIUS Disconnect-Cause 属性値の機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *100 : RADIUS* ベンダー固有属性（*VSA*）および *RADIUS Disconnect-Cause* 属性値の機能情報

機能名	リリース	機能情報
VPDN Disconnect Cause のアカウンティング	Cisco IOS XE Release 2.1	この機能は、Cisco ASR 1000 シリーズ ルータに追加されました。

機能名	リリース	機能情報
ベンダー固有の RADIUS 属性	Cisco IOS XE Release 2.1	このマニュアルは、ネットワーク アクセス サーバと RADIUS サーバの間でベンダー固有属性（属性 26）を使用してベンダー固有の情報を伝達する方法を規定するインターネット技術特別調査委員会（IETF）ドラフト標準を扱います。属性 26 はベンダー固有属性をカプセル化します。このため、ベンダーは一般的な用途に適さない独自の拡張属性をサポートできます。 Cisco IOS XE Release 2.1 では、Cisco ASR 1000 シリーズ Aggregation Services Router にこの機能が実装されました。

第 68 章

Connect-Info RADIUS 属性 77

Connect-Info RADIUS 属性 77 機能を使用すれば、ネットワーク アクセス サーバ（NAS）から、RADIUS クライアント（ダイヤルイン モデム）に送信される RADIUS アカウンティング「start」および「stop」レコード内で Connect-Info（属性 77）を報告できます。これらのレコードを使用すれば、送受信の接続速度、変調、および圧縮を比較することによって、接続端（ネゴシエーション後）での速度がさまざまなダイヤルイン モデム上のユーザ セッションを分析できます。

ネットワーク アクセス サーバ（NAS）からアカウンティング「start」および「stop」レコード内で属性 77 を送信したときの接続レートをプラットフォーム上で測定できます。「送信」速度（NAS モデムが情報を送信する速度）と「受信」速度（NAS が情報を受信する速度）を記録することによって、ユーザモデム接続でセッションの開始直後に速度を落とすようにネゴシエーションをやり直すかどうかを判断できます。送信速度と受信速度が異なる場合は、属性 77 が両方の速度を報告します。これによって、顧客ごとにセッションからモデム接続速度を取得できます。

属性 77 は、PPPoX などのブロードバンド接続用のクラス文字列、ダイヤルアクセス用の物理接続速度、および **ip vrf forwarding** コマンドで定義されたルータインターフェイス上のセッションに関する VRF 文字列の送信にも使用されます。

（注） この機能は設定が不要です。

Connect-Info RADIUS 属性 77 の前提条件

リリースおよびプラットフォーム サポートの詳細については、Connect-Info RADIUS 属性 77 の機能情報 （837 ページ）を参照してください。

NASからアカウンティング「start」および「stop」レコード内で属性77を送信できるようにするには、次の作業を実行する必要があります。

- NAS を認証、認可、およびアカウンティング（AAA）用に設定し、着信モデム コールを受け入れるように設定します。
- グローバル コンフィギュレーション モードで **aaa accounting network default start-stop group radius** コマンドを使用して、AAA アカウンティングを有効にします。
- グローバル コンフィギュレーション モードで **modem link-info poll time** コマンドを使用して、モデムポーリングタイマーを変更します。

（注） モデム ポーリング タイマーの変更は、Cisco ASR 1000 シリーズ アグリゲーション サービス ルータ上で必要です。

Connect-Info RADIUS 属性 77 に関する情報

設定可能な Connect-Info 属性機能により、RADIUS 属性 77（Connect-Info）のサポートが導入されました。これにより、RADIUS アカウンティング「start」および「stop」レコードを使用して、モデム ダイヤルイン接続の接続速度、変調、圧縮に関する情報が提供されます。

イーサネット接続での属性 77 のカスタマイズ

イーサネット接続での属性 77 をカスタマイズするには、イーサネット サブインターフェイスに適用されるサービス ポリシーの名前として接続情報を入力します。ルータはそのポリシー名を取得して、属性 77 にコピーします。

たとえば、次の設定で、speed:eth:25100:5100:19/0 という名前のアウトバウンド サービス ポリシーが、QinQ ギガビット イーサネット サブインターフェイス 1/0/0.2696 に適用されます。ルータはそのポリシー名を属性 77 にコピーし、これを Access-Request、Accounting-Start、または Accounting-Stop メッセージで RADIUS サーバに送信します。

```
interface GigabitEthernet1/0/0.2696
encapsulation dot1q 2696 second-dot1q 256
pppoe enable group global
no snmp trap link-status
service-policy input set_precedence_to_0
```

service-policy output speed:eth:25100:5100:19/0

ATM 接続での属性 77 のカスタマイズ

ATM 接続の属性 77 をカスタマイズするには、次のコンフィギュレーション モードで **aaa connect-info** *string* コマンドを設定します。

- PVC（特定の PVC の場合）
- PVC 範囲（一定範囲の PVC の場合）
- PVC-in-range（一定範囲の PVC の特定 PVC の場合）
- VC クラス（特定の **class-vc** コマンドの指定による）

ルータは、 **class-vc** コマンドで指定した VC クラスの名前、または **aaa connect-info** *string* コマンドで指定した文字列を取得して、属性 77 にコピーします。

たとえば、次の設定では、ATM PVC 10/42 と 10/43 の両方で **class-vc** コマンドが設定され、PVC 10/42 で **aaa connect-info** コマンドが設定されます。

```
interface ATM1/0/0.1 multipoint
description TDSL clients - default TDSL 1024 no ip mroute-cache
class-int speed:ubr:1184:160:10
range pvc 10/41 10/160
!
pvc-in-range 10/42
class-vc speed:ubr:2303:224:10
aaa connect-info speed:ubr:2303:224:10:isp-specific-descr
!
pvc-in-range 10/43
class-vc speed:ubr:2303:224:10
```

PVC 10/42 の場合、ルータは、**aaa connect-info** コマンドで指定された文字列（speed:ubr:2303:224:10:isp-specific-descr）を取得し、属性 77 にコピーします。サブインターフェイスで **aaa connect-info** コマンドが設定されない場合、ルータは **class-vc** コマンドで指定されたクラス名（speed:ubr:2303:224:10）を取得し、属性 77 にコピーします。

PVC 10/43 の場合、ルータは **class-vc** コマンドで指定されたクラス名（speed:ubr:2303:224:10）を取得し、属性 77 にコピーします。

Connect-Info RADIUS 属性 77 の確認方法

Connect-Info RADIUS 属性 77 の確認

アカウンティング「start」および「stop」レコード内の属性 77 を確認するには、特権 EXEC モードで **debug radius** コマンドを使用します。

手順の概要

1. **enable**
2. **debug radius**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**debug radius** 例： `Router# debug radius`	RADIUS 関連の情報を表示します。

例

次の例は、Connect-Info [77] アカウンティング属性を示しています。

```
Router# debug radius
Sep 8 21:53:05.242: RADIUS/ENCODE(00007D34):Orig. component type = PPPoE
Sep 8 21:53:05.242: RADIUS: AAA Unsupported Attr: interface [208] 10
Sep 8 21:53:05.242: RADIUS: 30 2F 31 2F 30 2F 39 2E [ 0/1/0/9.]
Sep 8 21:53:05.242: RADIUS: AAA Unsupported Attr: client-mac-address[45] 14
Sep 8 21:53:05.242: RADIUS: 30 30 30 30 2E 63 30 30 31 2E 30 31 [ 0000.c001.01]
Sep 8 21:53:05.242: RADIUS(00007D34): Config NAS IP: 0.0.0.0
Sep 8 21:53:05.242: RADIUS/ENCODE(00007D34): acct_session_id: 32042
Sep 8 21:53:05.242: RADIUS(00007D34): sending
Sep 8 21:53:05.242: RADIUS/ENCODE: Best Local IP-Address 10.3.8.2 for Radius-Server
10.3.1.107
Sep 8 21:53:05.242: RADIUS(00007D34): Send Access-Request to 10.3.1.107:1645 id 1645/1,
 len 116
Sep 8 21:53:05.242: RADIUS: authenticator FC 82 50 DB 65 8F 21 A9 - F3 0A A8 09 29 E5
56 65
Sep 8 21:53:05.242: RADIUS: Framed-Protocol [7] 6 PPP [1]
Sep 8 21:53:05.242: RADIUS: User-Name [1] 8 ''user1''
Sep 8 21:53:05.242: RADIUS: User-Password [2] 18 *
Sep 8 21:53:05.242: RADIUS: NAS-Port-Type [61] 6 Virtual [5]
Sep 8 21:53:05.242: RADIUS: NAS-Port [5] 6 0
Sep 8 21:53:05.242: RADIUS: NAS-Port-Id [87] 12 ''0/1/0/9.32''
Sep 8 21:53:05.242: RADIUS: Connect-Info [77] 28 ''speed:ubr:3456:448:10/0000''
Sep 8 21:53:05.242: RADIUS: Service-Type [6] 6 Framed [2]
Sep 8 21:53:05.242: RADIUS: NAS-IP-Address [4] 6 10.3.8.2
Sep 8 21:53:05.242: RADIUS(00007D34): Started 5 sec timeout
Sep 8 21:53:05.244: RADIUS: Received from id 1645/1 10.3.1.107:1645, Access-Accept, len
 32
Sep 8 21:53:05.244: RADIUS: authenticator 9A F1 29 01 66 53 17 CB - 73 FB 1B CE 7D 80
04 F2
Sep 8 21:53:05.244: RADIUS: Service-Type [6] 6 Framed [2]
Sep 8 21:53:05.244: RADIUS: Framed-Protocol [7] 6 PPP [1]
Sep 8 21:53:05.244: RADIUS(00007D34): Received from id 1645/1
Sep 8 21:53:05.248: RADIUS/ENCODE(00007D34):Orig. component type = PPPoE
Sep 8 21:53:05.248: RADIUS(00007D34): Config NAS IP: 0.0.0.0
Sep 8 21:53:05.248: RADIUS(00007D34): sending
Sep 8 21:53:05.248: RADIUS/ENCODE: Best Local IP-Address 10.3.8.2 for Radius-Server
5.3.1.107
Sep 8 21:53:05.248: RADIUS(00007D34): Send Accounting-Request to 10.3.1.107:1646 id
1646/3, len 126
```

```
Sep 8 21:53:05.248: RADIUS: authenticator 71 6E 73 9B FD 7E 82 81 - 10 2A CD 83 A8 BD
D2 F0
Sep 8 21:53:05.248: RADIUS: Acct-Session-Id [44] 10 ''00007D2A''
Sep 8 21:53:05.248: RADIUS: Framed-Protocol [7] 6 PPP [1]
Sep 8 21:53:05.248: RADIUS: User-Name [1] 8 ''user1''
Sep 8 21:53:05.248: RADIUS: Acct-Authentic [45] 6 RADIUS [1]
Sep 8 21:53:05.248: RADIUS: Acct-Status-Type [40] 6 Start [1]
Sep 8 21:53:05.248: RADIUS: NAS-Port-Type [61] 6 Virtual [5]
Sep 8 21:53:05.248: RADIUS: NAS-Port [5] 6 0
Sep 8 21:53:05.248: RADIUS: NAS-Port-Id [87] 12 ''0/1/0/9.32''
Sep 8 21:53:05.248: RADIUS: Connect-Info [77] 28 ''speed:ubr:3456:448:10/0000
```

Connect-Info RADIUS 属性 77 の設定例

AAA と着信モデム コール用の NAS の設定例

次の例は、AAA と着信モデム コール用の NAS 設定のサンプルです。

```
interface Serial0:15
  no ip address
  isdn switch-type primary-net5
  isdn incoming-voice modem
!
interface Async1
  ip address 192.0.2.2 255.255.255.0
  encapsulation ppp
  async default routing
  async mode interactive
  no peer default ip address
  ppp authentication chap
!
line 1
  modem InOu
  transport preferred none
  transport input all
  autoselect ppp
!
```

その他の参考資料

次の項で、Connect-Info RADIUS 属性 77 機能に関連する参考資料を紹介します。

関連資料

関連項目	マニュアル タイトル
IOS ダイヤル テクノロジー	『Cisco IOS XE Dial Technologies Configuration Guide, Release 2』
	『*Cisco IOS Dial Technologies Command Reference*』
セキュリティ コマンド	『*Cisco IOS Security Command Reference*』

標準

標準	タイトル
この機能でサポートされる新規の標準または変更された標準はありません。また、既存の標準のサポートは変更されていません。	--

MIB

MIB	MIB のリンク
この機能によってサポートされる新しい MIB または変更された MIB はありません。またこの機能による既存MIBのサポートに変更はありません。	選択したプラットフォーム、Cisco IOS リリース、およびフィーチャ セットに関する MIB を探してダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

RFC

RFC	タイトル
RFC 2869	『RADIUS Extensions』

シスコのテクニカル サポート

説明	リンク
シスコのサポート Web サイトでは、シスコの製品やテクノロジーに関するトラブルシューティングにお役立ていただけるように、マニュアルやツールをはじめとする豊富なオンライン リソースを提供しています。 お使いの製品のセキュリティ情報や技術情報を入手するために、Cisco Notification Service（Field Notice からアクセス）、Cisco Technical Services Newsletter、Really Simple Syndication（RSS）フィードなどの各種サービスに加入できます。 シスコのサポート Web サイトのツールにアクセスする際は、Cisco.com のユーザ ID およびパスワードが必要です。	http://www.cisco.com/en/US/support/index.html

Connect-Info RADIUS 属性 77 の機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *101 : Connect-Info RADIUS* 属性 *77* の機能情報

機能名	リリース	機能情報
Connect-Info RADIUS 属性 77	Cisco IOS XE Release 2.1	Connect-Info RADIUS 属性 77 機能を使用すれば、ネットワーク アクセス サーバ（NAS）から、RADIUS クライアント（ダイヤルイン モデム）に送信される RADIUS アカウンティング「start」および「stop」レコード内で Connect-Info（属性 77）を報告できます。これらの「start」および「stop」レコードを使用すれば、送受信の接続速度、変調、および圧縮を比較することによって、接続端（ネゴシエーション後）での速度がさまざまなダイヤルイン モデム上のユーザ セッションを分析できます。 この機能は、Cisco IOS XE リリース 2.1 で、Cisco ASR 1000 シリーズ ルータに導入されました。

第 69 章

暗号化されたベンダー固有属性

暗号化されたベンダー固有属性の機能により、ユーザはRADIUSサーバでフィルタを一元的に管理することができます。また、この機能は次の種類の文字列のベンダー固有属性（VSA）をサポートしています。

- タグ付きの文字列 VSA （840 ページ）（この新しい VSA がタグ付きであることを除き、Cisco VSA Type 1（Cisco:AVPair (1)）に類似）
- 暗号化された文字列 VSA （840 ページ）（この新しい VSA が暗号化されていることを除き、Cisco VSA Type 1 に類似）
- タグ付きおよび暗号化された文字列VSA （840ページ）（この新しいVSAがタグ付きで、暗号化されていることを除き、Cisco VSA Type 1 に類似）

Cisco:AVPairs では、属性と値のペア（AVP）の文字列の形式で追加の認証情報および認可情報を指定します。Internet Engineering Task Force（IETF）の RADIUS 属性 26（Vendor-Specific）が、ベンダー ID 番号「9」およびベンダータイプ値「1」で転送された場合（Cisco AVPair であることを意味します）、Cisco AVPair の RADIUS ユーザ プロファイルは「Cisco:AVPair = "protocol:attribute=value"」というような形式になります。

暗号化されたベンダー固有属性の前提条件

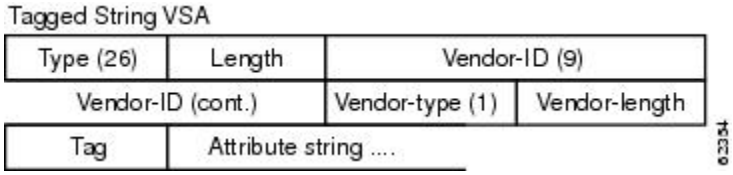
タグ付きで暗号化されたVSAをRADIUSサーバが受け付けるようにするためには、AAA認証およびAAA認可用にサーバを設定し、PPPコールを受け付けるように設定する必要があります。

暗号化されたベンダー固有属性に関する情報

タグ付きの文字列 VSA

次の図は、タグ付きの文字列 VSA のパケット形式を示します。

図 *12 :* タグ付きの文字列 *VSA* の形式

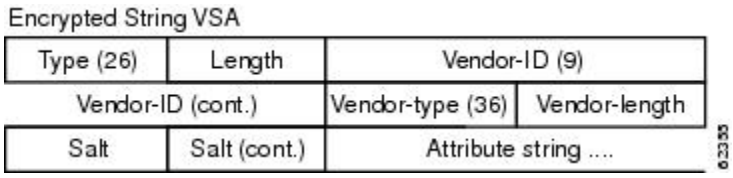


正しい値を取り出すために、Tag フィールドが正しく解析される必要があります。このフィールドの値の範囲はわずか 0x01 ～ 0x1F です。値が指定範囲内にない場合、RADIUS サーバはその値を無視し、Tag フィールドが Attribute String フィールドの一部であると見なします。

暗号化された文字列 VSA

次の図は、暗号化された文字列 VSA のパケット形式を示します。

図 *13 :* 暗号化された文字列 *VSA* の形式



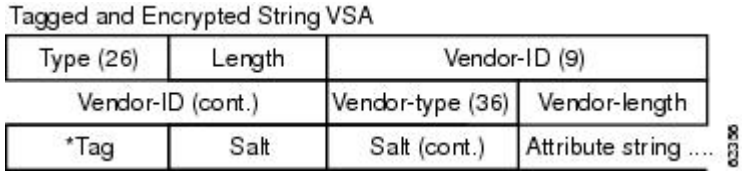
Saltフィールドは、VSAの各インスタンスの暗号化に使用される暗号キーの一意性を保証します。Salt フィールドの先頭の最上位ビットは 1 に設定する必要があります。

（注） Vendor-type (36) は、属性が暗号化された文字列 VSA であることを示しています。

タグ付きおよび暗号化された文字列 VSA

次の図は、新しくサポートされた各 VSA のパケットの形式を示しています。

図 *14 :* タグ付きおよび暗号化された文字列 *VSA* の形式



この VSA は、Tag フィールドが追加されていることを除き、暗号化された文字列 VSA とほぼ同じです。Tag フィールドは、値が有効な範囲内（0x01 ～ 0x1F）にない場合、Salt フィールドの一部と見なされます。

暗号化されたベンダー固有属性の確認方法

暗号化されたベンダー固有属性の機能では、設定は必要ありません。RADIUS のタグ付きおよび暗号化 VSA が RADIUS サーバから送信されていることを検証するために、次のコマンドを特権 EXEC モードで実行します。

コマンド	目的
`Router# debug radius`	RADIUS 関連の情報を表示します。このコマンドの出力は、タグ付きおよび暗号化 VSA が RADIUS サーバから送信されているかどうかを示しています。

暗号化されたベンダー固有属性の設定例

NAS の設定例

次の例は、タグ付きおよび暗号化 VSA を使用して、基本的な設定のネットワーク アクセス サーバ（NAS）を設定する方法を示しています（この例では、PPP コールの確立に必要な設定がすでにイネーブルになっていると想定されています）。

```
aaa new-model
aaa authentication ppp default group radius
aaa authorization network default group radius
!
radius-server host 10.2.2.2 auth-port 1645 acct-port 1646
radius-server key cisco
```

タグ付きおよび暗号化 VSA がある RADIUS ユーザ プロファイルの例

次の例は、タグ付きおよび暗号化された文字列 VSA をサポートする RADIUS サーバのユーザ プロファイルの例です。

```
mascot   Password = "password1"
```

```
Service-Type = NAS-Prompt,
Framed-Protocol = PPP,
Cisco:Cisco-Enc = "ip:route=10.0.0.0 255.0.0.0"
Cisco.attr Cisco-Enc 36 tag-encstr(*,*)
```

その他の参考資料

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『*Cisco IOS Master Commands List, All Releases*』
RADIUS 属性	『*Cisco IOS XE Security Configuration Guide: Securing User Services*, Release 2』
メディア独立型 PPP およびマルチリンク PPP	「メディア独立型 PPP およびマルチリンク PPP の設定」機能モジュール
認証	「認証の設定」機能モジュール
許可	「認可の設定」機能モジュール

標準

標準	タイトル
なし。	--

MIB

MIB	MIB のリンク
なし。	選択したプラットフォーム、Cisco ソフトウェア リリース、およびフィーチャ セットの MIB を検索してダウンロードする場合は、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

RFC

RFC	タイトル
RFC 2865	『*Remote Authentication Dial In User Service (RADIUS)*』
RFC 2868	『*RADIUS Attributes for Tunnel Protocol Support*』

シスコのテクニカル サポート

説明	リンク
シスコのサポート Web サイトでは、シスコの製品やテクノロジーに関するトラブルシューティングにお役立ていただけるように、マニュアルやツールをはじめとする豊富なオンライン リソースを提供しています。 お使いの製品のセキュリティ情報や技術情報を入手するために、Cisco Notification Service（Field Notice からアクセス）、Cisco Technical Services Newsletter、Really Simple Syndication（RSS）フィードなどの各種サービスに加入できます。 シスコのサポート Web サイトのツールにアクセスする際は、Cisco.com のユーザ ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

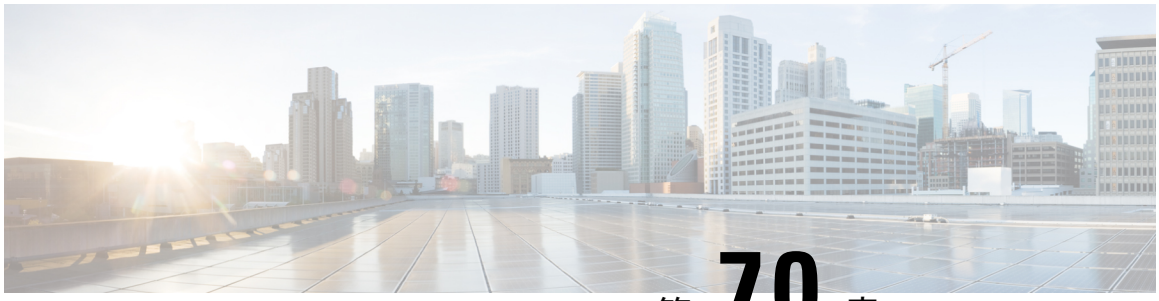
暗号化されたベンダー固有属性の機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *102*：暗号化されたベンダー固有属性の機能情報

機能名	リリース	機能情報
暗号化されたベンダー固有属性	Cisco IOS XE Release 2.3	暗号化されたベンダー固有属性の機能により、ユーザは RADIUS サーバでフィルタを一元的に管理できます。また、この機能はタグ付き、暗号化、タグ付きおよび暗号化の各文字列ベンダー固有属性（VSA）をサポートしています。 Cisco IOS XE Release 2.3 では、Cisco ASR 1000 シリーズ Aggregation Services Router にこの機能が実装されました。



第 70 章

アクセス要求内の RADIUS 属性 8 Framed-IP-Address

アクセス要求内の RADIUS 属性 8（Framed-IP-Address）機能は、ネットワーク アクセス サーバ（NAS）から RADIUS サーバに、ユーザ認証に先立って、ユーザ IP アドレスのヒントを提供できるようにします。RADIUS サーバ上で動作するアプリケーションは、このヒントを使用して、ユーザ名と アドレスのテーブル（マップ）を作成できます。マッピング情報を使用して、サービスアプリケーションは、正常なユーザ認証に使用するユーザのログイン情報の準備を開始できます。

アクセス要求内の RADIUS 属性 8 Framed-IP-Address の前提条件

RADIUS アクセス要求内で RADIUS 属性 8 を送信する場合は、NAS サーバから IP アドレスを要求するようにログイン ホストを設定しておく必要があります。また、NAS からの IP アドレスを受け入れるようにログイン ホストを設定しておく必要もあります。

NAS は、ログイン ホストをサポートしているインターフェイス上のネットワーク アドレスのプールを使用して設定する必要があります。

アクセス要求内の RADIUS 属性 8 Framed-IP-Address に関する情報

この機能の動作内容

ネットワーク デバイスが RADIUS 認証用に設定された NAS にダイヤルインすると、NAS がユーザ認証に備えて、RADIUS サーバとの通信プロセスを開始します。通常は、ユーザ認証が成功するまで、ダイヤルイン ホストの IP アドレスが RADIUS サーバに通知されません。RADIUS アクセス要求内でサーバにデバイス IP アドレスを通知すれば、他のアプリケーションがその情報を利用できるようになります。

NAS が RADIUS サーバと通信するようにセットアップされている場合は、NAS が特定のインターフェイス上で設定された IP アドレスのプールからダイヤルイン ホストに IP アドレスを割り当てます。NAS は、ダイヤルイン ホストの IP アドレスを属性 8 として RADIUS サーバに送信します。そのとき、NAS は、ユーザ名などの他のユーザ情報も RADIUS サーバに送信します。

RADIUS が NAS からユーザ情報を受信した場合は、次の 2 つの選択肢があります。

- RADIUS サーバ上のユーザ プロファイルにすでに属性 8 が含まれていた場合は、RADIUS が NAS から受け取った IP アドレスをユーザ プロファイル内で属性 8 として定義された IP アドレスに置き換えます。ユーザ プロファイル内で定義されたアドレスが NAS に返されます。
- ユーザ プロファイルに属性 8 が含まれていない場合は、RADIUS サーバが、NAS からの属性 8 を受け入れて、そのアドレスを NAS に返すことができます。

RADIUS サーバから返されたアドレスは、セッションが終わるまで、NAS 上のメモリに保存されます。NAS が RADIUS アカウンティング用に設定されている場合は、RADIUS サーバに送信されるアカウンティング開始パケットに属性 8 内のものと同じ IP アドレスが含まれています。以降のすべてのアカウンティング パケット、更新（設定されている場合）、および終了パケットにも、属性 8 で指定されたものと同じ IP アドレスが含まれています。

ただし、RADIUS 属性 8（Framed-IP-Address）は、次の 2 つの状況ではアカウンティング開始パケットに含まれません。

- ユーザがデュアルスタック（IPv4 または IPv6）サブスクライバである場合。
- IP アドレスがローカル プールからであり、RADIUS サーバからではない場合。

これらの状況では、**aaa accounting delay-start extended-time** *delay-value* コマンドを使用し、設定した遅延値でインターネットプロトコル制御プロトコルバージョン 6（IPCPv6）アドレスネゴシエーションを遅延させます。遅延している間は、IPCPv4 アドレスが使用され、フレーム化された IPv4 アドレスがアカウンティング開始パケットに追加されます。

利点

アクセス要求機能の RADIUS 属性 8（Framed-IP-Address）を使用すると、ユーザと IP アドレスのマッピング テーブルを構築する RADIUS サーバで、アプリケーションを実行することができます。この機能により、サーバは、RADIUS サーバでの正常なユーザ認証の前に、カスタマイズしたユーザ ログイン ページの準備といった他のアプリケーションで、マッピング テーブルの情報を使用することができます。

アクセス要求内の RADIUS 属性 8 Framed-IP-Address の設定方法

アクセス要求での RADIUS 属性 8 の設定

アクセス要求内で RADIUS 属性 8 を送信するには、次の手順を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **radius-server attribute 8 include-in-access-req**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**radius-server attribute 8 include-in-access-req** 例： `Router(config)# radius-server attribute 8 include-in-access-req`	access-request パケット内で RADIUS 属性 8 を送信します。

アクセス要求内の RADIUS 属性 8 の確認

RADIUS 属性 8 がアクセス要求内で送信されていることを確認するには、次の手順を実行します。属性 8 は、すべての PPP アクセス要求内に存在するはずです。

手順の概要

1. **enable**
2. **more system:running-config**
3. **debug radius**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**more system:running-config** 例： `Router# more system:running-config`	現在実行されているコンフィギュレーションファイルの内容を表示します(コマンド**more system:running-config**が **show running-config** コマンドに置き換えられていることに注意してください)。
ステップ 3	**debug radius** 例： `Router# debug radius`	RADIUS 関連の情報を表示します。このコマンドの出力は、属性 8 がアクセス要求内で送信されているかどうかを示しています。

アクセス要求内の RADIUS 属性 8 Framed-IP-Address の設定例

ダイヤルイン ホストの IP アドレスを送信する NAS の設定例

次の例は、ダイヤルイン ホストの IP アドレスを RADIUS アクセス要求内で RADIUS サーバに送信する NAS 設定を示しています。NAS は、RADIUS 認証、許可、アカウンティング（AAA）用に設定されています。IP アドレスのプール（async1-pool）が設定され、インターフェイス virtual-template1 に適用されています。

```
aaa new-model
aaa authentication login default group radius
aaa authentication ppp default group radius
aaa authorization network default group radius
aaa accounting network default start-stop group radius
```

```
!
ip address-pool local
!
interface virtual-template1
 peer default ip address pool async1-pool
!
ip local pool async1-pool 209.165.200.225 209.165.200.229
!
radius-server host 172.31.71.146 auth-port 1645 acct-port 1646
radius-server retransmit 3
radius-server attribute 8 include-in-access-req
radius-server key radhost<xxx>: Example
```

その他の参考資料

次の項で、アクセス要求内の RADIUS 属性 8（Framed-IP-Address）に関する参考資料を紹介します。

関連資料

関連項目	マニュアル タイトル
認証の設定および RADIUS の設定	『*Cisco IOS XE Security Configuration Guide: Configuring User Services*, Release 2』の「認証の設定」および「RADIUS の設定」の章。
セキュリティ コマンド	『*Cisco IOS Security Command Reference*』

標準

標準	タイトル
この機能でサポートされる新規の標準または変更された標準はありません。また、既存の標準のサポートは変更されていません。	--

MIB

MIB	MIB のリンク
この機能によってサポートされる新しい MIB または変更された MIB はありません。またこの機能による既存 MIB のサポートに変更はありません。	選択したプラットフォーム、Cisco IOS XE ソフトウェア リリース、およびフィーチャ セットの MIB の場所を検索しダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

RFC

RFC	タイトル
RFC 2138	『Remote Authentication Dial In User Service (RADIUS)』

シスコのテクニカル サポート

説明	リンク
シスコのサポート Web サイトでは、シスコの製品やテクノロジーに関するトラブルシューティングにお役立ていただけるように、マニュアルやツールをはじめとする豊富なオンライン リソースを提供しています。 お使いの製品のセキュリティ情報や技術情報を入手するために、Cisco Notification Service（Field Notice からアクセス）、Cisco Technical Services Newsletter、Really Simple Syndication（RSS）フィードなどの各種サービスに加入できます。 シスコのサポート Web サイトのツールにアクセスする際は、Cisco.com のユーザ ID およびパスワードが必要です。	http://www.cisco.com/en/US/support/index.html

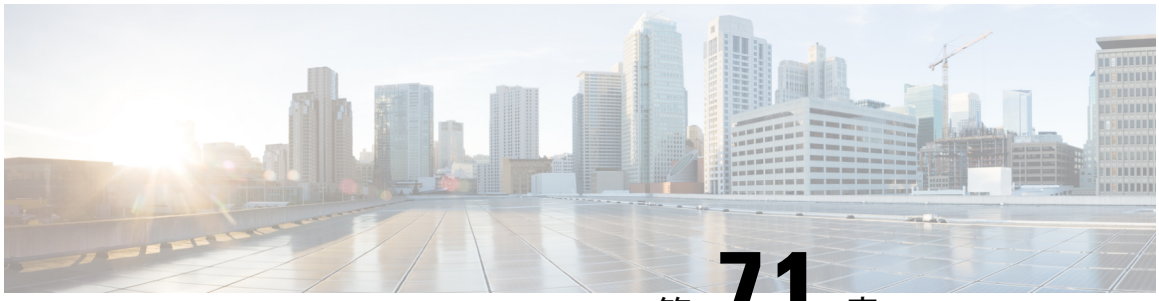
アクセス要求内の RADIUS 属性 8 Framed-IP-Address の機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *103* : アクセス要求内の *RADIUS* 属性 *8*（*Framed-IP-Address*）の機能情報

機能名	リリース	機能情報
アクセス要求内の RADIUS 属性 8（Framed-IP-Address） （スティッキーIPとも呼ばれます）	Cisco IOS XE Release 2.1	アクセス要求内の RADIUS 属性 8（Framed-IP-Address）機能は、ネットワーク アクセス サーバ（NAS）から RADIUS サーバに、ユーザ認証に先立って、ユーザ IP アドレスのヒントを提供できるようにします。 Cisco IOS XE Release 2.1 では、Cisco ASR 1000 シリーズ Aggregation Services Router にこの機能が実装されました。 次のコマンドが導入または変更されました。**radius-server attribute 8 include-in-access-req**.



第 71 章

RADIUS 属性 82 トンネル割り当て ID

RADIUS 属性 82 トンネル割り当て ID の前提条件

この機能を使用するには、VPDN をサポートするシスコプラットフォームを使用している必要があります。

RADIUS 属性 82 トンネル割り当て ID の制約事項

この機能は、VPDN ダイヤルインアプリケーション専用に設計されています。VPDN ダイヤルアウトはサポートしていません。

RADIUS 属性 82 トンネル割り当て ID に関する情報

RADIUS 属性 82：トンネル割り当て ID 機能を使用すれば、レイヤ 2 トランスポート プロトコル アクセス コンセントレータ（LAC）で複数のユーザ単位またはドメイン RADIUS プロファイルからのユーザを同じアクティブ トンネルにグループ分けすることができます。RADIUS 属性 82：トンネル割り当て ID 機能は、選択されたエンドポイント、トンネル タイプ、および Tunnel-Assignment-ID が同じ場合に、LAC で複数の RADIUS プロファイルからのユーザを同じトンネルにグループ分けできるようにする新しい avpair の Tunnel-Assignment-ID を定義します。この機能により、新しいソフトウェア機能が導入されました。この機能のために導入されたコマンドはありません。

RADIUS 属性 82 が LAC で使用されているかどうかの確認方法

RADIUS 属性 82：トンネル割り当て ID 機能に関する設定手順はありません。このタスクは、トンネル認可中に LAC で使用される RADIUS 属性 82 を確認します。

手順の概要

1. **enable**
2. **configure terminal**
3. Router# **debug radius**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	Router# **debug radius** 例： `Router# debug radius`	RADIUS 関連の情報を表示します。このコマンドの出力は、属性 82 がアクセス要求内で送信されているかどうかを示します。

RADIUS 属性 82 トンネル割り当て ID の設定例

LAC の設定例

次の例は、VPDN グループがルータで定義されている場合の LAC の設定を示しています。

```
aaa new-model
aaa authentication ppp default local
aaa authorization network default local
!
bba-group pppoe bba_group1
virtual-template 1
!
```

```
interface Loopback1
no ip address
vpdn-group VPDN_LAC1
request-dialin
protocol l2tp
local name tb162_LAC1
domain isp1.com
initiate-to ip 10.0.0.2
source-ip 10.0.0.1
l2tp tunnel receive-window 100
l2tp tunnel nosession-timeout 30
l2tp tunnel retransmit retries 5
l2tp tunnel retransmit timeout min 2
l2tp tunnel retransmit timeout max 8
l2tp tunnel hello 60
l2tp tunnel password tunnel1
!
!
interface virtual-template 1
no snmp trap link-status
no keepalive
ip unnumbered loopback1
ppp mtu adaptive
ppp authentication pap
no logging event link-status
!
```

次の例は、VPDN グループが RADIUS で定義されている場合の LAC の設定を示しています。

```
aaa authentication ppp default group radius
aaa authorization network default radius
!
bba-group pppoe bba_group1
virtual-template 1
!
interface Loopback1
no ip address
interface virtual-template 1
no snmp trap link-status
no keepalive
ip unnumbered loopback1
ppp mtu adaptive
ppp authentication pap
no logging event link-status
```

LNS の設定例

次の例は、LNS 上で VPDN を設定します。

```
hostname lns
aaa new-model
aaa authentication ppp default group radius
aaa authorization network default group radius
vpdn enable
vpdn-group VPDN_LNS1
 accept-dialin
  protocol l2tp
  virtual-template 1
 terminate-from hostname tb162_LAC1
 local name LNS1
 l2tp tunnel hello 90
```

```
 l2tp tunnel password 0 hello1
interface Loopback0
 ip address 10.1.1.3 255.255.255.0
interface Virtual-Template1
 ip unnumbered Loopback0
 no keepalive
 peer default ip address pool mypool
 ppp authentication chap
ip local pool mypool 10.1.1.10 10.1.1.50
radius-server host lns-radiusd  auth-port 1645 acct-port 1646
radius-server retransmit 3
radius-server key cisco
```

RADIUS の設定例

次の例では、トンネルのセッションをグループ化するように RADIUS サーバを設定します。

ユーザ単位の設定

```
user@router.com Password = "cisco" Service-Type = Outbound,
       Tunnel-Type = :1:L2TP,
       Tunnel-Server-Endpoint = :1:"10.14.10.54",
       Tunnel-Assignment-Id = :1:"router"
client@router.com Password = "cisco" Service-Type = Outbound,
       Tunnel-Type = :1:L2TP,
       Tunnel-Server-Endpoint = :1:"10.14.10.54",
       Tunnel-Assignment-Id = :1:"router"
```

ドメインの設定

```
eng.router.com Password = "cisco" Service-Type = Outbound,
        Tunnel-Type = :1:L2TP,
        Tunnel-Server-Endpoint = :1:"10.14.10.54",
        Tunnel-Assignment-Id = :1:"router"
sales.router.com Password = "cisco" Service-Type = Outbound,
        Tunnel-Type = :1:L2TP,
        Tunnel-Server-Endpoint = :1:"10.14.10.54",
        Tunnel-Assignment-Id = :1:"router"
```

その他の参考資料

次の項で、RADIUS トンネル属性拡張に関する参考資料を紹介します。

関連資料

関連項目	マニュアル タイトル
認証	「認証の設定」モジュール。
RADIUS 属性	「RADIUS Attributes Overview and RADIUS IETF Attributes」モジュール。
VPDN	『*Cisco IOS VPDN Configuration Guide*, Release 15.0』。

標準

標準	タイトル
なし。	--

MIB

MIB	MIB のリンク
なし。	選択したプラットフォーム、Cisco IOS リリース、およびフィーチャ セットに関する MIB を探してダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

RFC

RFC	タイトル
RFC 2868	『RADIUS Attributes for Tunnel Protocol Support』

シスコのテクニカル サポート

説明	リンク
シスコのサポート Web サイトでは、シスコの製品やテクノロジーに関するトラブルシューティングにお役立ていただけるように、マニュアルやツールをはじめとする豊富なオンライン リソースを提供しています。 お使いの製品のセキュリティ情報や技術情報を入手するために、Cisco Notification Service（Field Notice からアクセス）、Cisco Technical Services Newsletter、Really Simple Syndication（RSS）フィードなどの各種サービスに加入できます。 シスコのサポート Web サイトのツールにアクセスする際は、Cisco.com のユーザ ID およびパスワードが必要です。	http://www.cisco.com/en/US/support/index.html

RADIUS 属性 82 トンネル割り当て ID の機能情報

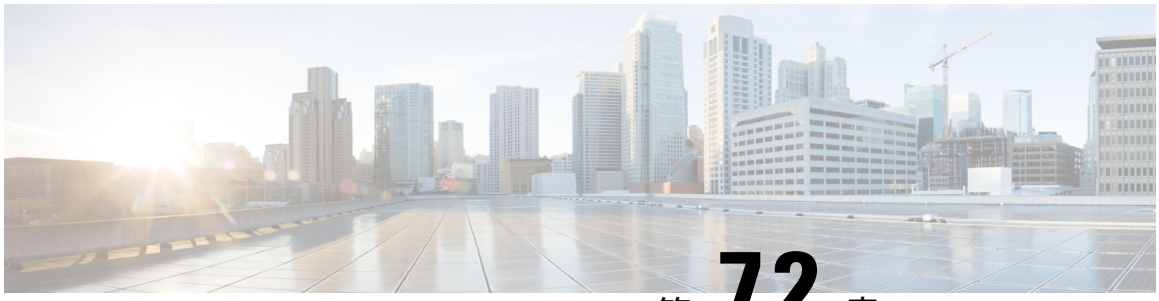
次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだ

けを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *104 : RADIUS* 属性 *82*：トンネル割り当て *ID* の機能情報

機能名	リリース	機能情報
RADIUS 属性 82：トンネル割り当て ID	Cisco IOS XE Release 2.1	RADIUS 属性 82：トンネル割り当て ID 機能を使用すれば、レイヤ 2 トランスポート プロトコル アクセス コンセントレータ（LAC）で複数のユーザ単位またはドメイン RADIUS プロファイルからのユーザを同じアクティブ トンネルにグループ分けすることができます。 Cisco IOS XE Release 2.1 では、Cisco ASR 1000 シリーズ アグリゲーション サービス ルータのサポートが追加されました。



第 72 章

RADIUS トンネル属性拡張

RADIUS トンネル属性拡張機能は、RADIUS 属性 90（Tunnel-Client-Auth-ID）と RADIUS 属性 91（Tunnel-Server-Auth-ID）を導入しています。この両方の属性は、ユーザにネットワーク アクセス サーバ（NAS）と RADIUS サーバの認証名の指定を許可することによって、バーチャル プライベート ネットワーク（VPN）での強制的トンネリングのプロビジョニングを支援します。

前提条件

RADIUS 属性の 90 と 91 を使用するには、次のタスクを完了する必要があります。

- AAA をサポートするように NAS を設定する。
- RADIUS をサポートするように NAS を設定する。
- VPN をサポートするように NAS を設定する。

機能制限

RADIUS トンネル属性の 90 と 91 を使用するには、RADIUS サーバがタグ付き属性をサポートしている必要があります。

RADIUS トンネル属性拡張に関する情報

RADIUS トンネル属性拡張の利点

RADIUS トンネル属性拡張の機能により、トンネル イニシエータとトンネル ターミネータの名前が（デフォルト以外で）指定できます。これにより、VPN トンネリングのセットアップ時に、より高度なセキュリティを確立できます。

RADIUS トンネル属性拡張の説明

NAS と RADIUS サーバ間の通信がセットアップされたら、トンネリング プロトコルを有効にできます。トンネリング プロトコルのアプリケーションの一部は自発的ですが、その他は強制的トンネリングを伴います。つまり、ユーザが何らかの処置や選択をしなくてもトンネルが作成されます。このような場合は、NAS から RADIUS サーバにトンネリング情報を伝送して認証を確立するための新しい RADIUS 属性が必要です。この新しい RADIUS 属性を次の表に示します。

（注） 強制的トンネリングでは、配備中のセキュリティ対策がトンネルエンドポイント間のトラフィックにのみ適用されます。トンネル化されたトラフィックの暗号化または完全性保護をエンドツーエンド セキュリティの代替手段と見なさないでください。

表 *105 : RADIUS* トンネル属性

番号	IETF RADIUS トンネル属性	同等の TACACS+ 属性	サポートされているプロトコル	説明
90	Tunnel-Client-Auth-ID	tunnel-id	レイヤ 2 トンネリング プロトコル（L2TP）	トンネル ターミネータを使用してトンネル セットアップを認証する際に、トンネル イニシエータ（NAS とも呼ばれます[5]）によって使用される名前を指定します。
91	Tunnel-Server-Auth-ID	gw-name	レイヤ 2 トンネリング プロトコル（L2TP）	トンネル イニシエータを使用してトンネル セットアップを認証する際に、トンネル ターミネータ（ホーム ゲートウェイとも呼ばれます[6]）によって使用される名前を指定します。

[5] L2TP が使用される場合、NAS は L2TP アクセス コンセントレータ（LAC）とも呼ばれます。
[6] L2TP が使用される場合、ホーム ゲートウェイは L2TP ネットワーク サーバ（LNS）とも呼ばれます。

RADIUS 属性 90 と RADIUS 属性 91 は次のような状況で追加されます。

- RADIUS サーバが要求を受け入れ、必要な認証名がデフォルトと異なる場合

- アカウンティング要求に値が start と stop のどちらかの Acct-Status-Type 属性が含まれ、トンネル化されたセッションが関係している場合

RADIUS トンネル属性拡張の設定方法

この機能に関連する設定作業はありません。

RADIUS 属性 90 および RADIUS 属性 91 の確認

RADIUS 属性 90 と RADIUS 属性 91 がアクセス受け入れとアカウンティング要求内で送信されていることを確認するには、EXEC モードで次のコマンドを使用します。

コマンド	目的
`Router# debug radius`	RADIUS 関連の情報を表示します。このコマンドの出力は、属性 90 と 属性 91 のどちらがアクセス受け入れとアカウンティング要求内で送信されているかを示します。

RADIUS トンネル属性拡張の設定例

L2TP ネットワーク サーバ設定の例

次の例は、RADIUS トンネリング属性の 90 と 91 を使用した基本的な L2F と L2TP の設定を含む LNS の設定方法を示しています。

```
aaa new-model
aaa authentication login default none
aaa authentication login console none
aaa authentication ppp default local group radius
aaa authorization network default group radius if-authenticated
!
username l2tp-svr-auth-id password 0 l2tp-tnl-pass
!
vpdn enable
vpdn search-order domain
!
vpdn-group 1
accept-dialin
protocol l2tp
virtual-template 1
terminate-from hostname l2tp-cli-auth-id
local name l2tp-svr-auth-id
!
interface loopback0
ip address 10.0.0.3 255.255.255.0
no ip route-cache
no ip mroute-cache
!
```

```
interface Virtual-Template1
ip unnumbered loopback0
ppp authentication pap
!
radius-server host 1.1.1.1 auth-port 1645 acct-port 1646
radius-server key <deleted>
!
```

RADIUS トンネリング属性の 90 と 91 を含む RADIUS ユーザ プロファイルの例

L2TP トンネル用の RADIUS トンネリング属性の 90 と 91 を含む RADIUS ユーザ プロファイルの例を次に示します。

```
cisco.com Password = "cisco", Service-Type = Outbound
Service-Type = Outbound,
Tunnel-Type = :1:L2TP,
Tunnel-Medium-Type = :1:IP,
Tunnel-Client-Endpoint = :1:"10.0.0.2",
Tunnel-Server-Endpoint = :1:"10.0.0.3",
Tunnel-Client-Auth-Id = :1:"l2tp-cli-auth-id",
Tunnel-Server-Auth-Id = :1:"l2tp-svr-auth-id",
Tunnel-Assignment-Id = :1:"l2tp-assignment-id",
Cisco-Avpair = "vpdn:l2tp-tunnel-password=l2tp-tnl-pass",
Tunnel-Preference = :1:1
```

その他の参考資料

次の項で、RADIUS トンネル属性拡張の機能に関する参考資料を紹介します。

関連資料

関連項目	マニュアル タイトル
認証設定	『*Cisco IOS XE Security Configuration Guide: Configuring User Services*, Release 2』の「認証の設定」
RADIUS の設定	『*Cisco IOS XE Security Configuration Guide: Configuring User Services*, Release 2』の「RADIUS の設定」
RADIUS 属性の概要	『*Cisco IOS XE Security Configuration Guide: Configuring User Services*, Release 2』の「RADIUS 属性の概要および RADIUS IETF 属性」。
セキュリティ コマンド	『*Cisco IOS* セキュリティ コマンド リファレンス』

標準

標準	タイトル
この機能でサポートされる新規の標準または変更された標準はありません。また、既存の標準のサポートは変更されていません。	--

MIB

MIB	MIB のリンク
この機能によってサポートされる新しい MIB または変更された MIB はありません。またこの機能による既存 MIB のサポートに変更はありません。	選択したプラットフォーム、Cisco IOS XE ソフトウェア リリース、およびフィーチャ セットの MIB の場所を検索しダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

RFC

RFC	タイトル
RFC 2868	『*RADIUS Attributes for Tunnel Protocol Support*』

シスコのテクニカル サポート

説明	リンク
シスコのサポート Web サイトでは、シスコの製品やテクノロジーに関するトラブルシューティングにお役立ていただけるように、マニュアルやツールをはじめとする豊富なオンライン リソースを提供しています。 お使いの製品のセキュリティ情報や技術情報を入手するために、Cisco Notification Service（Field Notice からアクセス）、Cisco Technical Services Newsletter、Really Simple Syndication（RSS）フィードなどの各種サービスに加入できます。 シスコのサポート Web サイトのツールにアクセスする際は、Cisco.com のユーザ ID およびパスワードが必要です。	http://www.cisco.com/en/US/support/index.html

RADIUS トンネル属性拡張の機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *106 : RADIUS* トンネル属性拡張の機能情報

機能名	リリース	機能情報
RADIUS トンネル属性拡張	Cisco IOS XE Release 2.1	RADIUS トンネル属性拡張機能は、RADIUS 属性 90（Tunnel-Client-Auth-ID）と RADIUS 属性 91（Tunnel-Server-Auth-ID）を導入しています。この両方の属性は、ユーザにネットワーク アクセス サーバ（NAS）と RADIUS サーバの認証名の指定を許可することによって、バーチャル プライベート ネットワーク（VPN）での強制的トンネリングのプロビジョニングを支援します。 Cisco IOS XE Release 2.1 では、Cisco ASR 1000 シリーズ Aggregation Services Router にこの機能が実装されました。

用語集

Layer 2 Tunnel Protocol (L2TP) ：ISP などのアクセスサービスで仮想トンネルを作成し、顧客のリモートサイトやリモートユーザーを企業のホームネットワークにリンクさせることが可能な Layer 2 Tunneling Protocolです。具体的には、ISP アクセス ポイント（POP）にあるネットワーク アクセス サーバ（NAS）がリモート ユーザと PPP メッセージを交換し、L2F または L2TP の要求や応答を使用して顧客のトンネル サーバと通信し、トンネルのセットアップを行います。

L2TP access concentrator (LAC) ：クライアントが直接接続し、PPP フレームが L2TP ネットワークサーバー（LNS）にトンネリングされるネットワーク アクセス サーバー（NAS）です。LAC は、L2TP が 1 つまたは複数の LNS にトラフィックを渡すために操作するメディアのみを実装します。LAC はPPP 内で伝送されるすべてのプロトコルをトンネルすることができます。また、LAC は着信コールを開始して、発信コールを受け取ります。LAC は L2F ネットワーク アクセス サーバに似ています。

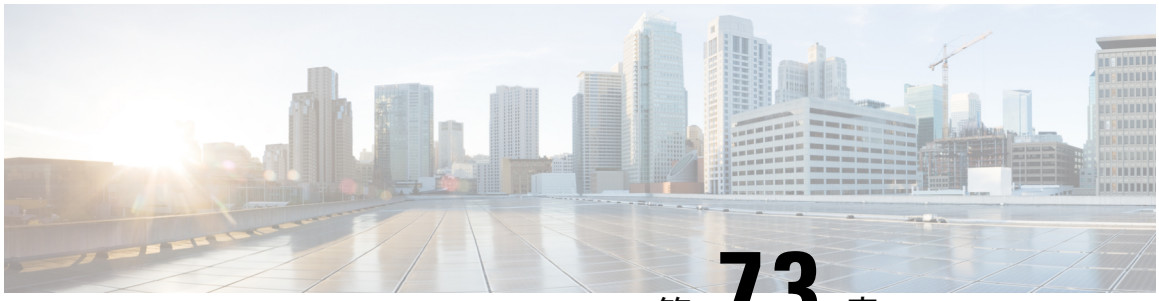
L2TP network server (LNS) ：L2TP トンネルの終端点であり、PPP フレームが処理され、上位層プロトコルに渡されるアクセスポイントです。LNS は PPP を終端させる任意のプラットフォーム上で動作できます。LNS はサーバ側の L2TP プロトコルを処理します。L2TP は、L2TP

のトンネルが到達する1つのメディアにのみ依存します。LNSは発信コールを開始して、着信コールを受け取ります。LNS は L2F テクノロジーのホーム ゲートウェイに似ています。

network access server (NAS)：パケットの世界（インターネットなど）と回線交換の世界（PSTNなど）をインターフェイスする、Cisco プラットフォームまたは AccessPath システムなどのプラットフォームの集合。

トンネル：L2TP アクセス コンセントレータ（LAC）と L2TP ネットワーク サーバ（LNS）間で複数の PPP セッションを伝送可能な仮想パイプ。

バーチャルプライベートネットワーク（VPN）：リモートでダイヤルインネットワークをホーム ネットワークに存在させ、あたかも直接接続されているかのように見せるシステム。VPN は、L2TP と L2F を使用して、L2TP アクセス コンセントレータ（LAC）の代わりに、L2TP ネットワーク サーバ（LNS）でネットワーク接続のレイヤ 2 と上位層を終端させます。



第 73 章

RADIUS 属性 66 Tunnel-Client-Endpoint 拡張

RADIUS 属性 66（Tunnel-Client-Endpoint）拡張機能を使用すれば、ネットワーク アクセス サーバ（NAS）の IP アドレスではなく、NAS のホスト名を RADIUS 属性 66（Tunnel-Client-Endpoint）に指定できます。この機能は、ユーザが数字の IP アドレスよりも覚えやすいホスト名を使用できるようにするとともに、NAS の IP アドレス の隠ぺいを支援します。

RADIUS 属性 66 Tunnel-Client-Endpoint 拡張の前提条件

VPDN をサポートするシスコプラットフォームが必要です。VPDN の詳細については、用語集（871 ページ）を参照してください。

RADIUS 属性 66 Tunnel-Client-Endpoint 拡張の制約事項

シスコ デバイスでは、バーチャル プライベート ダイヤルアップ ネットワーク（VPDN）をサポートするシスコのソフトウェア イメージを実行する必要があります。

RADIUS 属性 66 Tunnel-Client-Endpoint 拡張に関する情報

RADIUS 属性 66 Tunnel-Client-Endpoint 拡張の使用方法

バーチャルプライベートネットワーク（VPN）は、レイヤ2フォワーディング（L2F）または Layer 2 Tunnel Protocol（L2TP）トンネルを使用して、上位層プロトコルのリンク レイヤ（たとえば、PPP、非同期ハイレベルデータ リンク コントロール（HDLC）など）をトンネルします。インターネット サービス プロバイダー（ISP）は、ユーザからのコールを受信して、それを顧客のトンネル サーバに転送するよう NAS を設定します。通常、ISP はトンネル サーバ（トンネル エンドポイント）に関する情報だけを保持します。顧客では、トンネル サーバ ユーザの IP アドレス、ルーティング、その他のユーザ データベース機能が保持されます。RADIUS 属性 66 は、顧客が NAS の IP アドレスの代わりにホスト名を指定できるようにします。

（注） L2F は Cisco ASR 1000 シリーズ アグリゲーション サービス ルータではサポートされません。

RADIUS 属性 66 Tunnel-Client-Endpoint 拡張の設定方法

RADIUS 属性 66（Tunnel-Client-Endpoint）拡張のサポートに関連する設定作業はありません。

RADIUS 属性 66 Tunnel-Client-Endpoint 拡張の設定例

RADIUS 属性 66 Tunnel-Client-Endpoint 拡張用の RADIUS プロファイルの設定

次の例は、RADIUS プロファイルの RADIUS 属性 66 （Tunnel-Client-Endpoint）を使用して、ユーザが NAS のホスト名を指定できるようにするための設定方法を示しています。

```
cisco-avpair = vpdn:l2tp-cm-local-window-size=1024
cisco-avpair = vpdn:l2tp-nosession-timeout=30
cisco-avpair = vpdn:l2tp-cm-retransmit-retries=10
cisco-avpair = vpdn:l2tp-cm-min-timeout=2
cisco-avpair = vpdn:l2tp-hello-interval=60
Service-Type = outbound
Tunnel-Assignment-Id_tag1 = ISP1
Tunnel-Client-Auth-Id_tag1 = LAC1
Tunnel-Client-Endpoint_tag1 = 10.0.0.2
Tunnel-Medium-Type_tag1 = IPv4
Tunnel-Password_tag1 = tunnel1
Tunnel-Server-Auth-Id_tag1 = LNS1
Tunnel-Server-Endpoint_tag1 = 10.0.0.1
Tunnel-Type_tag1 = l2tp
```

その他の参考資料

次の項で、RADIUS 属性 66（Tunnel-Client-Endpoint）拡張の機能に関する参考資料を紹介します。

関連資料

関連項目	マニュアル タイトル
RADIUS 属性 66	『*Cisco IOS XE Security Configuration Guide: Configuring User Services*, Release 2』
セキュリティ コマンド	『*Cisco IOS* セキュリティ コマンド リファレンス』

標準

標準	タイトル
この機能でサポートされる新規の標準または変更された標準はありません。また、既存の標準のサポートは変更されていません。	--

MIB

MIB	MIB のリンク
この機能によってサポートされる新しい MIB または変更された MIB はありません。またこの機能による既存 MIB のサポートに変更はありません。	選択したプラットフォーム、Cisco IOS XE ソフトウェア リリース、およびフィーチャ セットの MIB の場所を検索しダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

RFC

RFC	タイトル
この機能によりサポートされた新規 RFC または改訂 RFC はありません。またこの機能による既存 RFC のサポートに変更はありません。	--

シスコのテクニカル サポート

説明	リンク
シスコのサポート Web サイトでは、シスコの製品やテクノロジーに関するトラブルシューティングにお役立ていただけるように、マニュアルやツールをはじめとする豊富なオンライン リソースを提供しています。 お使いの製品のセキュリティ情報や技術情報を入手するために、Cisco Notification Service（Field Notice からアクセス）、Cisco Technical Services Newsletter、Really Simple Syndication（RSS）フィードなどの各種サービスに加入できます。 シスコのサポート Web サイトのツールにアクセスする際は、Cisco.com のユーザ ID およびパスワードが必要です。	http://www.cisco.com/en/US/support/index.html

RADIUS 属性 66 Tunnel-Client-Endpoint 拡張の機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *107 : RADIUS* 属性 *66*（*Tunnel-Client-Endpoint*）拡張の機能情報

機能名	リリース	機能情報
RADIUS 属性 66（Tunnel-Client-Endpoint）拡張	Cisco IOS XE Release 2.1 Cisco IOS XE Release 2.3 Cisco IOS XE Release 3.9S	RADIUS 属性 66（Tunnel-Client-Endpoint）拡張機能を使用すれば、ネットワーク アクセス サーバ（NAS）の IP アドレスではなく、NAS のホスト名を RADIUS 属性 66（Tunnel-Client-Endpoint）に指定できます。この機能は、ユーザが数字の IP アドレスよりも覚えやすいホスト名を使用できるようにするとともに、NAS の IP アドレス の隠ぺいを支援します。 Cisco IOS XE Release 2.3 では、Cisco ASR 1000 シリーズ Aggregation Services Router にこの機能が実装されました。

用語集

L2F：レイヤ 2 フォワーディング プロトコル。インターネットでの安全なバーチャル プライベート ダイヤルアップ ネットワークの作成をサポートするプロトコルです。

L2TP：Layer 2 Tunnel Protocol。ダイヤル アクセス領域におけるバーチャル プライベート ネットワークの主要な構成要素の 1 つであり、シスコおよびその他のインターネットワーキング業界のリーダーにより支持されているプロトコルです。このプロトコルは、シスコの L2F プロトコルと Microsoft 社のポイントツーポイント トンネリング プロトコル（PPTP）のいいところを組み合わせたものです。

レイヤ 2 フォワーディング プロトコル：L2F を参照。

Layer 2 Tunnel Protocol：L2TP を参照。

ポイントツーポイント プロトコル：PPP を参照。

PPP：ポイントツーポイント プロトコル。同期回線と非同期回線上でルータ間接続とホスト/ネットワーク間接続を提供する SLIP の代替プロトコル。SLIP は IP と連動するように設計されているのに対して、PPP は IP、IPX、ARA などの複数のネットワーク層プロトコルと連動するように設計されています。PPP には、CHAP および PAP などの組み込みのセキュリティ メカニズムもあります。PPP は LCP と NCP の 2 つのプロトコルに依存します。

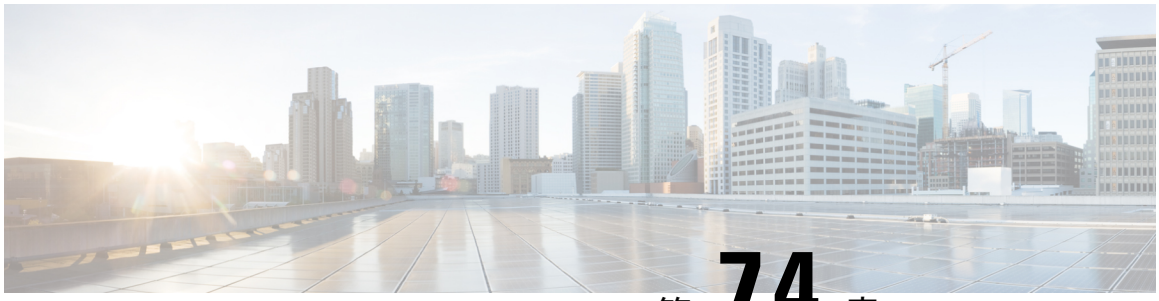
RADIUS：Remote Authentication Dial-In User Service。モデムおよび ISDN 接続の認証、および接続のトラッキングのためのデータベースです。

Remote Authentication Dial-In User Service：RADIUS を参照。

バーチャル プライベート ダイヤルアップ ネットワーク：VPDN を参照。

VPDN：バーチャルプライベートダイヤルアップネットワーク。リモートでダイヤルイン ネットワークをホーム ネットワークに存在させ、あたかも直接接続されているかのように見せるシ

ステム。VPDN は、L2TP と L2F を使用して、L2TP アクセス コンセントレータ（LAC）ではなく、L2TP ネットワーク サーバ（LNS）で、レイヤ 2 と上位のネットワーク接続部分を終端します。



第 74 章

RADIUS 属性値スクリーニング

RADIUS 属性値スクリーニング機能を使用すれば、認可やアカウンティングなどの目的で、ネットワーク アクセス サーバ（NAS）上の「許可」または「拒否」RADIUS 属性のリストを設定できます。

NAS が Access-Accept パケットで受信したすべての RADIUS 属性を受け入れて処理する場合は、不必要な属性を処理する可能性があり、顧客の認証、認可、およびアカウンティング（AAA）サーバを制御しないホールセール プロバイダーの場合に問題が発生します。たとえば、顧客が加入していないサービスを指定する属性が存在したり、他のホールセール ダイヤルユーザ向けのサービスを低下させる属性が存在したりする場合です。そのため、特定の属性の使用を制限するように NAS を設定できることが、多くのユーザの要件になります。

RADIUS 属性値スクリーニング機能を実装するには、次の方法のいずれかを使用する必要があります。

- NAS が、特定の目的で、設定された拒否リストに登録されたものを除く、すべての標準 RADIUS 属性を受け入れて、処理できるようにする
- NAS が、特定の目的で、設定された許可リストに登録されたものを除く、すべての標準 RADIUS 属性を拒否（除外）できるようにする

RADIUS 属性値スクリーニングの前提条件

RADIUS の許可リストおよび拒否リストを設定する前に、AAA を有効にする必要があります。

RADIUS 属性値スクリーニングの制約事項

NAS の要件

この機能を有効にするには、RADIUS グループを使用して認可するように NAS を設定する必要があります。

許可リストまたは拒否リストの制約事項

許可リストまたは拒否リストの設定に使用される 2 つのフィルタは相互排他的です。そのため、ユーザはサーバ グループの目的ごとに、1 つのアクセス リストか、1 つの拒否リストしか設定できません。

ベンダー固有属性

この機能は、ベンダー固有属性（VSA）スクリーニングをサポートしていません。ただし、ユーザは、すべての VSA を許可または拒否する許可リストまたは拒否リスト内で属性 26（Vendor-Specific）を指定できます。

必須属性スクリーニングの推奨事項

次の必須属性は、拒否しないことを推奨します。

- 認可用：
  - 6（Service-Type）
  - 7（Framed-Protocol）
- アカウンティング用：
  - 4（NAS-IP-Address）
  - 40（Acct-Status-Type）
  - 41（Acct-Delay-Time）
  - 44（Acct-Session-ID）

属性が必須の場合は、拒否が無視され、属性のパススルーが許可されます。

（注） 必須属性の拒否リストを設定してもエラーにはなりません。これは、リストでは目的（認可またはアカウンティング）が指定されないためです。サーバが、属性の使用目的を認識したときに、その属性が必須かどうかを判断します。

RADIUS 属性値スクリーニングに関する情報

RADIUS 属性値スクリーニング機能は、次のようなメリットを提供します。

- ユーザは、NAS 上で特定の目的の属性を選択して許可リストまたは拒否リストを設定できるため、不必要な属性が受け入れられ、処理されることがなくなります。
- 関連するアカウンティング属性だけの許可リストを設定することによって、不必要なトラフィックを削減し、アカウンティング データのカスタマイズを可能にすることができます。

RADIUS 属性のスクリーン方法

RADIUS 属性値スクリーニングの設定

RADIUS 属性の許可リストまたは拒否リストを認可またはアカウンティング用に設定するには、次のコマンドを使用します。

手順の概要

1. **enable**
2. **configure terminal**
3. Router(config)# **aaa authentication ppp default**
4. Router(config)# **aaa authorization network default group** *group-name*
5. Router(config)# **aaa group server radius** *group-name*
6. Router(config-sg-radius)# **server** *ip-address*
7. Router(config-sg-radius)# **authorization** [**accept** | **reject**] *listname*
8. Router(config-sg-radius)# **exit**
9. Router(config)# **radius-server host** {*hostname* | *ip-address*} [**key** *string*
10. Router(config)# **radius-server attribute list** *listname*
11. Router(config-sg-radius)# **attribute** *value1* [*value2* [*value3...*]]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 3	Router(config)# **aaa authentication ppp default** 例： **group** *group-name*	PPP を実行しているシリアル インターフェイス上で使用する 1 つまたは複数の AAA 認証方式を指定します。
ステップ 4	Router(config)# **aaa authorization network default group** *group-name*	ユーザのネットワーク アクセスを制限するパラメータを設定します。
ステップ 5	Router(config)# **aaa group server radius** *group-name*	複数の RADIUS サーバ ホストを別々のリストと別々の方式にグループ分けします。
ステップ 6	Router(config-sg-radius)# **server** *ip-address*	グループ サーバ用の RADIUS サーバの IP アドレスを設定します。
ステップ 7	Router(config-sg-radius)# **authorization** [**accept** | **reject**] *listname* 例： and/or 例： Router(config-sg-radius)# **accounting** [**accept** | **reject**] *listname*	RADIUS サーバから Access-Accept パケット内で返す属性用のフィルタを指定します。 および/または アカウンティング要求内で RADIUS サーバに送信すべき属性用のフィルタを指定します。 （注） **accept** キーワードは、*listname* で指定された属性を除く、すべての属性が拒否されることを意味します。**reject** キーワードは、*listname* で指定された属性とすべての標準属性を除く、すべての属性が許可されることを意味します。
ステップ 8	Router(config-sg-radius)# **exit**	server-group コンフィギュレーション モードを終了します。
ステップ 9	Router(config)# **radius-server host** {*hostname* | *ip-address*} [**key** *string*	RADIUS サーバ ホストを指定します。
ステップ 10	Router(config)# **radius-server attribute list** *listname*	**attribute** コマンドで定義された一連の属性に指定されたリスト名を定義します。 （注） *listname* はステップ 5 で定義した *listname* と同じにする必要があります。
ステップ 11	Router(config-sg-radius)# **attribute** *value1* [*value2* [*value3...*]]	設定した許可リストまたは拒否リストに属性を追加します。

	コマンドまたはアクション	目的
		（注） このコマンドは、許可リストまたは拒否リストに属性を追加するために何回も使用できます。

RADIUS 属性値スクリーニングの確認

許可リストまたは拒否リストを確認するには、特権EXECモードで次のコマンドのいずれかを使用します。

コマンド	目的
`Router# debug aaa accounting`	説明の義務があるイベントが発生したときに、その情報を表示します。
`Router# debug aaa authentication`	AAA 認証に関する情報を表示します。
`Router# show radius statistics`	アカウンティングパケットと認証パケットについてのRADIUS 統計情報を示します。

RADIUS 属性値スクリーニングの設定例

認可許可の例

次の例は、属性 6（Service-Type）と属性 7（Framed-Protocol）用の許可リストの設定方法を示しています。他のすべての属性（VSA を含む）は RADIUS 認可に対して拒否されます。

```
aaa new-model
aaa authentication ppp default group radius-sg
aaa authorization network default group radius-sg
aaa group server radius radius-sg
server 10.1.1.1
authorization accept min-author
!
radius-server host 10.1.1.1 key mykey1
radius-server attribute list min-author
attribute 6-7
```

アカウンティング拒否の例

次の例は、属性 66（Tunnel-Client-Endpoint）と属性 67（Tunnel-Server-Endpoint）用の拒否リストの設定方法を示しています。他のすべての属性（VSA を含む）は RADIUS アカウンティングに対して受け入れられます。

```
aaa new-model
aaa authentication ppp default group radius-sg
aaa authorization network default group radius-sg
aaa group server radius radius-sg
server 10.1.1.1
accounting reject tnl-x-endpoint
!
radius-server host 10.1.1.1 key mykey1
radius-server attribute list tnl-x-endpoint
attribute 66-67
```

認可拒否とアカウンティング許可の例

次の例は、RADIUS認可用の拒否リストとRADIUSアカウンティング用の許可リストの設定方法を示しています。認可またはアカウンティングのサーバグループごとに複数の許可リストまたは拒否リストを設定できませんが、サーバグループごとに認可用のリストとアカウンティング用のリストを 1 つずつ設定できます。

```
aaa new-model
aaa authentication ppp default group radius-sg
aaa authorization network default group radius-sg
aaa group server radius radius-sg
server 10.1.1.1
authorization reject bad-author
accounting accept usage-only
!
radius-server host 10.1.1.1 key mykey1
radius-server attribute list usage-only
attribute 1,40,42-43,46
!
radius-server attribute list bad-author
attribute 22,27-28,56-59
```

必須属性の拒否の例

次に、**debug aaa accounting** コマンドを使用した場合のデバッグ出力の例を示します。この例では、必須属性の 44、40、および 41 が拒否リストの「standard」に追加されています。

```
Router# debug aaa authorization
AAA/ACCT(6): Accounting method=radius-sg (radius)
RADIUS: attribute 44 cannot be rejected
RADIUS: attribute 61 rejected
RADIUS: attribute 31 rejected
RADIUS: attribute 40 cannot be rejected
RADIUS: attribute 41 cannot be rejected
```

その他の参考資料

次の項で、RADIUS 属性値スクリーニング機能に関する参考資料を紹介します。

関連資料

関連項目	マニュアル タイトル
RADIUS	「RADIUS の設定」機能モジュール。
その他のセキュリティ機能	『*Cisco IOS XE Security Configuration Guide: Securing User Services*, Release 2』
セキュリティ コマンド	『*Cisco IOS Security Command Reference*』

標準

標準	タイトル
この機能でサポートされる新規の標準または変更された標準はありません。また、既存の標準のサポートは変更されていません。	--

MIB

MIB	MIB のリンク
なし。	選択したプラットフォーム、Cisco ソフトウェア リリース、およびフィーチャ セットの MIB を検索してダウンロードする場合は、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

RFC

RFC	タイトル
この機能によりサポートされた新規 RFC または改訂 RFC はありません。またこの機能による既存 RFC のサポートに変更はありません。	--

シスコのテクニカル サポート

説明	リンク
シスコのサポート Web サイトでは、シスコの製品やテクノロジーに関するトラブルシューティングにお役立ていただけるように、マニュアルやツールをはじめとする豊富なオンライン リソースを提供しています。 お使いの製品のセキュリティ情報や技術情報を入手するために、Cisco Notification Service（Field Notice からアクセス）、Cisco Technical Services Newsletter、Really Simple Syndication（RSS）フィードなどの各種サービスに加入できます。 シスコのサポート Web サイトのツールにアクセスする際は、Cisco.com のユーザ ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

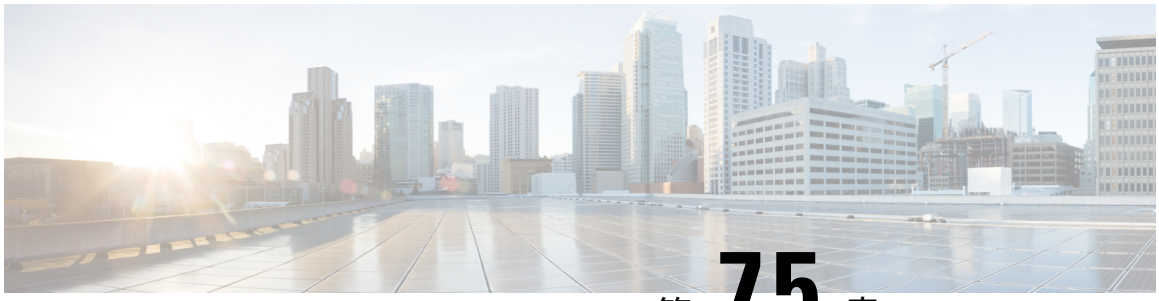
RADIUS 属性値スクリーニングの機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *108 : RADIUS* 属性値スクリーニングの機能情報

機能名	リリース	機能情報
RADIUS 属性値スクリーニング	Cisco IOS XE Release 2.1	RADIUS 属性値スクリーニング機能を使用すれば、認可やアカウンティングなどの目的で、ネットワーク アクセス サーバ（NAS）上の「許可」または「拒否」RADIUS 属性のリストを設定できます。 この機能は、Cisco IOS XE リリース 2.1 で Cisco ASR 1000 シリーズアグリゲーション サービス ルータに導入されました。 この機能により、次のコマンドが導入または変更されました。**accounting (server-group), authorization (server-group), attribute (server-group), radius-server attribute list**



第 75 章

RADIUS 属性 55 Event-Timestamp

RADIUS 属性 55 Event-Timestamp 機能により、ネットワーク アクセス サーバ（NAS）は、Network Time Protocol（NTP）同期が行われているまたは行われていない RADIUS サーバに送信されるアカウンティングおよび認証パケットに、イベント タイムスタンプ属性を挿入できます。

RADIUS 属性 55 Event-Timestamp の前提条件

アカウンティングおよび認証要求パケット内で Event-Timestamp 属性を送信するには、ネットワーク デバイスのクロックを設定する必要があります。ネットワーク デバイスのクロックの設定方法については、ネットワーク管理の設定ガイドの「基本システム管理」の章の「基本システム管理の実行」を参照してください。

ネットワークデバイスがリロードされるたびにネットワークデバイスのクロックを設定するのを避けるには、**clock calendar-valid** コマンドを有効にします。このコマンドの詳細については、ネットワーク管理の設定ガイドの「基本システム管理」の章の「時刻およびカレンダー サービスの設定」を参照してください。

RADIUS 属性 55 Event-Timestamp に関する情報

ネットワーク デバイスが RADIUS 認証用に設定されたネットワーク アクセス サーバ（NAS）にダイヤルインすると、NAS がユーザ認証に備えて、RADIUS サーバとの通信プロセスを開始します。通常、RADIUS 属性 55（Event-Timestamp）は、Network Time Protocol（NTP）の同期が正常に完了するまで、RADIUS サーバに送信されません。この機能により、NTP が同期して

いない場合でも、NAS はアカウンティングおよび認証要求パケットに Event-Timestamp 属性を挿入できます。

Event-Timestamp 属性は、NAS で発生したイベントの発生時刻を記録します。このタイムスタンプは RADIUS 属性 55 内で、1970 年 1 月 1 日 00:00 UTC 以降の秒数で送信されます。

Event-Timestamp 属性は、セッションが終わるまで NAS 上のメモリに保存されます。RADIUS アカウンティングおよび認証開始パケットと、それに続くすべてのアカウンティングおよび認証パケット、更新（設定されている場合）、停止パケットもまた、最初のパケットが送信された時刻を表す同じ RADIUS 属性 55 Event-Timestamp を含んでいます。

RADIUS 属性 55 Event-Timestamp の設定方法

RADIUS 属性 55 Event-Timestamp の設定

アカウンティングおよび認証要求内で RADIUS 属性 55 を送信するには、次の作業を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **aaa new-model**
4. **aaa authentication ppp default group radius**
5. **aaa accounting network default start-stop group radius**
6. **radius-server host** *ip-address*
7. **radius-server attribute 55 include-in-acct-req**
8. **radius-server attribute 55 access-req include**
9. **exit**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**aaa new-model** 例：	認証、許可、アカウンティング（AAA）をイネーブルにします。

	コマンドまたはアクション	目的
	`Device(config)# aaa new-model`	
ステップ 4	**aaa authentication ppp default group radius** 例： `Device(config)# aaa authentication ppp default group radius`	認証用のすべてのRADIUSサーバのリストを利用してPPPを実行するシリアルインターフェイスで使用する、1 つ以上の AAA 方式を指定します。
ステップ 5	**aaa accounting network default start-stop group radius** 例： `Device(config)# aaa accounting network default start-stop group radius`	ネットワーク アカウンティングを有効にして、RADIUS アカウンティングの方式リスト用の開始アカウンティングおよび停止アカウンティングの通知を RADIUS サーバに送信します。
ステップ 6	**radius-server host** *ip-address* 例： `Device(config)# radius-server host 192.0.2.3`	RADIUSサーバホストのIPアドレスを指定します。
ステップ 7	**radius-server attribute 55 include-in-acct-req** 例： `Device(config)# radius-server attribute 55 include-in-acct-req`	account-requestパケット内でRADIUS属性55を送信します。
ステップ 8	**radius-server attribute 55 access-req include** 例： `Device(config)# radius-server attribute 55 access-req include`	access-request パケット内で RADIUS 属性 55 を送信します。
ステップ 9	**exit** 例： `Device(config)# exit`	グローバル コンフィギュレーション モードを終了します。

RADIUS 属性 55 Event-Timestamp の確認

アカウンティングおよび認証パケット内で RADIUS 属性 55 が送信されていることを確認するには、次の作業を実行します。

手順の概要

1. **enable**
2. **show running-config**
3. **debug radius**

手順の詳細

ステップ 1 enable

特権 EXEC モードを有効にします。

- パスワードを入力します（要求された場合）。

例：

```
Device> enable
```

ステップ 2 show running-config

現在実行されているコンフィギュレーション ファイルの内容を表示します

例：

```
Device# show running-config

.
.
.
aaa group server radius sample
aaa accounting network default start-stop group radius group sample
aaa server radius dynamic-author
radius-server attribute 55 include-in-acct-req
radius-server attribute 55 access-request include
radius-server dead-criteria time 10 tries 3
radius-server host 192.0.2.3
radius-server retry method reorder
radius-server retransmit 2
radius-server deadtime 1
radius-server key rad123
radius server host
.
.
.
radius-server attribute 55 include-in-acct-req
radius-server attribute 55 access-request include
```

ステップ 3 debug radius

RADIUS 関連の情報を表示します。このコマンドの出力は、アカウンティングおよび認証要求で属性 55 が送信されているかどうかを示しています。

例：

```
Device# debug radius

AAA/BIND(0000000D): Bind i/f Virtual-Template1
AAA/AUTHEN/PPP (0000000D): Pick method list 'default'
RADIUS/ENCODE(0000000D):Orig. component type = PPPoE
RADIUS: DSL line rate attributes successfully added
RADIUS(0000000D): Config NAS IP: 0.0.0.0
RADIUS(0000000D): Config NAS IPv6: ::
RADIUS/ENCODE(0000000D): acct_session_id: 2
RADIUS(0000000D): sending
RADIUS/ENCODE: Best Local IP-Address 192.0.2.3 for Radius-Server 192.0.2.1
```

```
RADIUS(0000000D): Sending a IPv4 Radius Packet
RADIUS(0000000D): Send Access-Request to 192.0.2.1:1645 id 1645/1,len 130
RADIUS:  authenticator 66 D8 24 42 BC 45 5B 3D - 0E DC 74 D7 E9 3D 81 85
RADIUS:  Framed-Protocol     [7]   6   PPP                       [1]
RADIUS:  User-Name           [1]   6   "test"
RADIUS:  User-Password       [2]   18  *
RADIUS:  NAS-Port-Type       [61]  6   Virtual                   [5]
RADIUS:  NAS-Port            [5]   6   0
RADIUS:  NAS-Port-Id         [87]  9   "0/0/0/0"
RADIUS:  Vendor, Cisco       [26]  41
RADIUS:   Cisco AVpair       [1]   35  "client-mac-address=aabb.cc00.6500"
RADIUS:  Service-Type        [6]   6   Framed                    [2]
RADIUS:  NAS-IP-Address      [4]   6   1.1.1.2
RADIUS:  Event-Timestamp     [55]  6   1362041578
RADIUS(0000000D): Started 5 sec timeout
RADIUS: Received from id 1645/192.0.2.1:1645, Access-Accept, len 20
.
.
.
RADIUS:  authenticator 2A 2B 24 47 06 44 23 8A - CB CC 8C 96 8D 21 76 DD
RADIUS(0000000D): Received from id 1645/1
AAA/BIND(0000000D): Bind i/f Virtual-Access2.1
RADIUS/ENCODE(0000000D):Orig. component type = PPPoE
.
.
.
RADIUS(0000000D): Config NAS IP: 0.0.0.0
RADIUS(0000000D): Config NAS IPv6: ::
RADIUS(0000000D): sending
RADIUS/ENCODE: Best Local IP-Address 192.0.2.3 for Radius-Server 192.0.2.1
RADIUS(0000000D): Sending a IPv4 Radius Packet
RADIUS(0000000D): Send Accounting-Request to 192.0.2.1:1646 id 1646/1,len 182
RADIUS:  authenticator C6 81 D0 D7 EA BA 9A A9 - 19 4B 1B 90 B8 D1 66 BF
RADIUS:  Acct-Session-Id     [44]  10  "00000002"
RADIUS:  Framed-Protocol     [7]   6   PPP                       [1]
RADIUS:  User-Name           [1]   6   "test"
RADIUS:  Vendor, Cisco       [26]  32
RADIUS:   Cisco AVpair       [1]   26  "connect-progress=Call Up"
RADIUS:  Acct-Authentic      [45]  6   RADIUS                    [1]
RADIUS:  Acct-Status-Type    [40]  6   Start                     [1]
RADIUS:  NAS-Port-Type       [61]  6   Virtual                   [5]
RADIUS:  NAS-Port            [5]   6   0
RADIUS:  NAS-Port-Id         [87]  9   "0/0/0/0"
RADIUS:  Vendor, Cisco       [26]  41
RADIUS:   Cisco AVpair       [1]   35  "client-mac-address=aabb.cc00.6500"
RADIUS:  Service-Type        [6]   6   Framed                    [2]
RADIUS:  NAS-IP-Address      [4]   6   1.1.1.2
RADIUS:  home-hl-prefix      [151] 10  "163BD6D4"
RADIUS:  Event-Timestamp     [55]  6   1362041588
RADIUS:  Acct-Delay-Time     [41]  6   0
RADIUS(0000000D): Started 5 sec timeout
.
.
.
RADIUS: Received from id 1646/1 1.1.1.1:1646, Accounting-response, len 20
RADIUS:  authenticator 79 F1 6A 38 07 C3 C8 F9 - 96 66 BE EF 5C FA 91 E6
```

RADIUS 属性 55 Event-Timestamp の設定例

例：アカウンティングおよび認証パケットの RADIUS 属性 55

次の例は、アカウンティングおよび認証パケットで RADIUS 属性 55 を送信する設定を示しています。

```
Device> enable
Device# configure terminal
Device(config)# aaa new-model
Device(config)# aaa authentication ppp default group radius
Device(config)# aaa accounting network default start-stop group radius
Device(config)# radius-server host 192.0.2.3
Device(config)# radius-server attribute 55 include-in-acct-req
Device(config)# radius-server attribute 55 access-req include
Device(config)# exit
```

RADIUS 属性 55 Event-Timestamp に関するその他の参考資料

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『Cisco IOS Master Command List, All Releases』
セキュリティ コマンド	• 『Security Command Reference: Commands A to C』 • 『Security Command Reference: Commands D to L』 • 『Security Command Reference: Commands M to R』 • 『Security Command Reference: Commands S to Z』

関連項目	マニュアル タイトル
「Configuring Authentication」	『*Authentication, Authorization, and Accounting Configuration Guide*』の「認証の設定」の章
RADIUS の設定	『*RADIUS Configuration Guide*』の「RADIUS の設定」の章

標準および RFC

標準/RFC	タイトル
RFC 2138	『*Remote Authentication Dial In User Service (RADIUS)*』

シスコのテクニカル サポート

説明	リンク
右の URL にアクセスして、シスコのテクニカル サポートを最大限に活用してください。これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

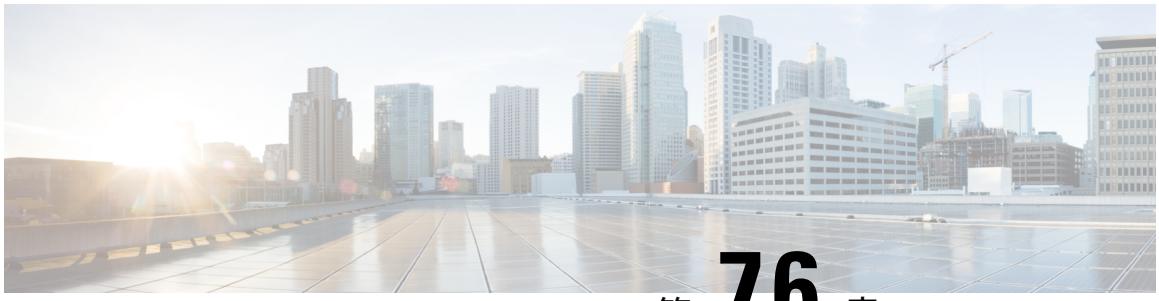
RADIUS 属性 55 Event-Timestamp の機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *109 : RADIUS* 属性 *55 Event-Timestamp* の機能情報

機能名	リリース	機能情報
RADIUS 属性 55 Event-Timestamp	Cisco IOS XE Release 3.9S	RADIUS 属性 55 Event-Timestamp 機能により、ネットワーク アクセス サーバ（NAS）は、Network Time Protocol（NTP）同期が行われているまたは行われていない RADIUS サーバに送信されるアカウンティングおよび認証パケットに、イベント タイムスタンプ属性が挿入できます。 次のコマンドが導入または変更されました。**radius-server attribute 55 access-req include** および **radius-server attribute 55 include-in-acct-req**



第 76 章

RADIUS 属性 104

RADIUS 属性 104 機能を使用すれば、RADIUS 認可プロファイル内でプライベート ルート（属性 104）を指定できます。プライベート ルートは、個々のインターフェイス上で受信されたパケットにのみ影響します。ルートはグローバル ルーティング テーブルとは別に保存され、ルーティング プロトコルに埋め込まれて再配布されることはありません。

RADIUS 属性 104 の前提条件

- シスコ RADIUS サーバを使用している必要があります。
- RADIUS の設定に精通している必要があります。
- ポリシーベース ルーティング（PBR）とプライベート ルートに精通している必要があります。
- アクセス コントロール リスト（ACL）に精通している必要があります。
- RADIUS 属性 104 機能を使用する前に、RADIUS AAA 認可と RADIUS ルート ダウンロードを設定する必要があります。
- F:\tips-migration には以下のメモリ バイトが必要です。
  - 1 つのルート マップ：50 バイト
  - 1 つの match-set 句：600 バイト
  - 1 つの拡張 ACL：366 バイト
  - 属性 104 の数 N のメモリ要件は、ユーザ当たり (600+366)*N+50 ≒1000*N です。

RADIUS 属性 104 の制約事項

- インターフェイス上ですでにPBRがローカル（静的）に設定されている状態で、属性104を指定した場合は、ローカルに設定されたPBRが無効になります。
- 疑似ネクストホップ アドレスを使用する場合は、ネクストホップ アドレスのルーティング テーブル内に、使用可能なルートが存在する必要があります。どのルートも使用できない場合は、パケットがポリシー ルーティングされません。
- ポリシー ルーティングはmatch-set句を順序付けせず、最初の一致を優先するため、一致させたい順序で属性を指定する必要があります。
- メトリック番号は属性内で使用できません。

RADIUS 属性 104 に関する情報

ポリシーベース ルーティングの背景

PBRは、定義済みのポリシーに基づいて、データ パケットを転送またはルーティングするためのメカニズムを提供します。ポリシーは、宛先アドレスではなく、サービス タイプ、送信元アドレス、優先順位、ポート番号、プロトコル タイプなどの他の要因に依存します。

ポリシーベース ルーティングは着信パケットに適用されます。ポリシーベース ルーティングが有効になっているインターフェイス上で受信されたパケットはすべて、ポリシーベース ルーティングと見なされます。ルータは、ルート マップと呼ばれる拡張パケット フィルタにそれらのパケットを通過させます。ルートマップ内で定義された基準に基づいて、パケットが適切なネクスト ホップに転送されます。

ルート マップ文のエントリごとに、match 句と set 句の組み合わせまたはコマンドが 1 つずつ含まれています。match句は、該当するパケットが特定のポリシーを満たしているかどうか（つまり、条件が満たされているかどうか）に関する基準を定義します。set 句は、一致基準を満たしたパケットをどのようにルーティングするかに関する指示を提供します。match 句は、対応する set 句を適用するためにパケットが一致しなければならないフィルタのセットを指定します。

属性 104 とポリシーベース ルート マップ

この項では、属性 104 機能と、そのポリシーベース ルート マップとの連携について説明します。

RADIUS 属性 104 の概要

RADIUS属性104機能を使用すれば、RADIUS認可プロファイル内でプライベートルートを指定できます。指定したプライベートルートは、個々のインターフェイス上で受信されたパケッ

トにのみ影響します。ルートはグローバル ルーティング テーブルとは別に保存され、ルーティング プロトコルに埋め込まれて再配布されることはありません。

許可ルート マップ

ルート マップ ステートメントは、「許可」または「拒否」にマークすることができます。ステートメントが「許可」にマークされると、一致基準を満たすパケットに set 句が適用されます。属性 104 の場合は、ルート マップの設定中に、次のようにルート マップを「許可」としてマークする必要があります。ルートマップの設定に関する情報については、関連資料 （894 ページ） を参照してください。

デフォルト プライベート ルート

ポリシー ルーティング プロセスは、一致するものが見つかるまで、ルート マップに沿って進行します。ルート マップ内で一致するものが見つからなかった場合は、グローバル ルーティング テーブルが参照されます。ユーザ プロファイル内でデフォルト ルートを指定した場合は、事実上、デフォルト ルートを越えるルートが無視されます。

ルート マップの順序

ルート マップはサーバ上で適用したい順番に指定する必要があります。

RADIUS 属性 104 の適用方法

RADIUS 属性 104 のユーザ プロファイルへの適用

次の内容を RADIUS サーバ データベースに追加することによって、RADIUS 属性 104 をユーザ プロファイルに適用できます。

手順の概要

1. RADIUS 属性 104 をユーザ プロファイルに適用します。

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	RADIUS 属性 104 をユーザ プロファイルに適用します。	`Ascend-Private-Route="dest_addr/netmask next_hop"` ルータの宛先ネットワーク アドレスは「dest_addr/netmask」で、ネクストホップ ルータのアドレスは「next_hop」です。

例

発信者に関連付けられた3つのプライベートルートを作成するユーザプロファイルのサンプルを次に示します。

```
username Password="ascend"; User-Service=Framed-User
   Framed-Protocol=PPP,
   Framed-Address=10.1.1.1,
   Framed-Netmask=255.0.0.0,
   Ascend-Private-Route="172.16.1.1/16 10.10.10.1"
   Ascend-Private-Route="192.168.1.1/32 10.10.10.2"
   Ascend-Private-Route="10.20.0.0/1 10.10.10.3"
   Ascend-Private-Route="10.0.0.0/0 10.10.10.4"
```

上のプロファイルを使用すれば、接続用のプライベートルーティングテーブルに、デフォルトルートのほかに次のルートが追加されます。

```
Destination/Mask     Gateway
172.16.1.1/16         10.10.10.1
192.168.1.1/32         10.10.10.2
10.20.20.20/1       10.10.10.3
10.0.0.0/0            10.10.10.4
```

ルート マップの確認

次の **show** コマンドを使用して、設定済みのルートマップを確認します。

手順の概要

1. **enable**
2. **show ip policy**
3. **show route-map** [*map-name* | **dynamic** [*dynamic-map-name* | **application** [*application-name*]] | **all**]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**show ip policy** 例： `Router# show ip policy`	ポリシー ルーティングに使用されるルート マップを表示します。
ステップ 3	**show route-map** [*map-name*	**dynamic** [*dynamic-map-name*	**application** [*application-name*]]	**all**]	設定済みのすべてのルートマップを表示するか、指定した 1 つのルート マップだけを表示します。

	コマンドまたはアクション	目的
	例： `Router# show route-map`	

RADIUS プロファイルのトラブルシューティング

プライベートルート設定が正常に動作しない場合は、「ポリシーベース ルーティングの背景（890 ページ）」を再度読んでみてください。このセクションは、パケットに何が発生しているかを判定するのに役立つことがあります。また、RADIUS プロファイルのトラブルシュートには、次の **debug** コマンドが使用できます。

手順の概要

1. **enable**
2. **debug radius**
3. **debug aaa per-user**
4. debug ip policy

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**debug radius** 例： `Router# debug radius`	RADIUS 関連の情報を表示します。
ステップ 3	**debug aaa per-user** 例： `Router# debug aaa per-user`	ユーザ認証として各ユーザに適用される属性を表示します。
ステップ 4	debug ip policy 例： `Router# debug ip policy`	IP ルーティング パケットのアクティビティを表示します。

RADIUS 属性 104 の設定例

属性 104 が適用された Route-Map 設定の例

次の出力は、属性 104 が適用された一般的な route-map 設定です。

```
Router# show route-map dynamic
route-map AAA-01/08/04-14:13:59.542-1-AppSpec, permit, sequence 0, identifier 1639994476

  Match clauses:
    ip address (access-lists): PBR#1 PBR#2
  Set clauses:
  Policy routing matches: 0 packets, 0 bytes
route-map AAA-01/08/04-14:13:59.542-1-AppSpec, permit, sequence 1, identifier 1640264784

  Match clauses:
    ip address (access-lists): PBR#3 PBR#4
  Set clauses:
  Policy routing matches: 0 packets, 0 bytes
route-map AAA-01/08/04-14:13:59.542-1-AppSpec, permit, sequence 2, identifier 1645563704

  Match clauses:
    ip address (access-lists): PBR#5 PBR#6
    length 10 100
  Set clauses:
    ip next-hop 10.1.1.1
    ip gateway10.1.1.1
  Policy routing matches: 0 packets, 0 bytes
 Current active dynamic routemaps = 1
```

その他の参考資料

次の項で、RADIUS NAS-IP-Address 属性設定可能性に関する参考資料を紹介します。

関連資料

関連項目	マニュアル タイトル
AAA の設定	『*Cisco IOS Security Configuration Guide: Securing User Services*』の「認証、認可、およびアカウンティング（AAA）」の項
RADIUS の設定	「Configuring RADIUS」モジュール。
RADIUS コマンド	『*Cisco IOS Security Command Reference*』

標準

標準	タイトル
なし	--

MIB

MIB	MIB のリンク
なし	選択したプラットフォーム、Cisco IOS リリース、およびフィーチャ セットに関する MIB を探してダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

RFC

RFC	タイトル
なし	--

シスコのテクニカル サポート

説明	リンク
シスコのサポート Web サイトでは、シスコの製品やテクノロジーに関するトラブルシューティングにお役立ていただけるように、マニュアルやツールをはじめとする豊富なオンライン リソースを提供しています。 お使いの製品のセキュリティ情報や技術情報を入手するために、Cisco Notification Service（Field Notice からアクセス）、Cisco Technical Services Newsletter、Really Simple Syndication（RSS）フィードなどの各種サービスに加入できます。 シスコのサポート Web サイトのツールにアクセスする際は、Cisco.com のユーザ ID およびパスワードが必要です。	http://www.cisco.com/en/US/support/index.html

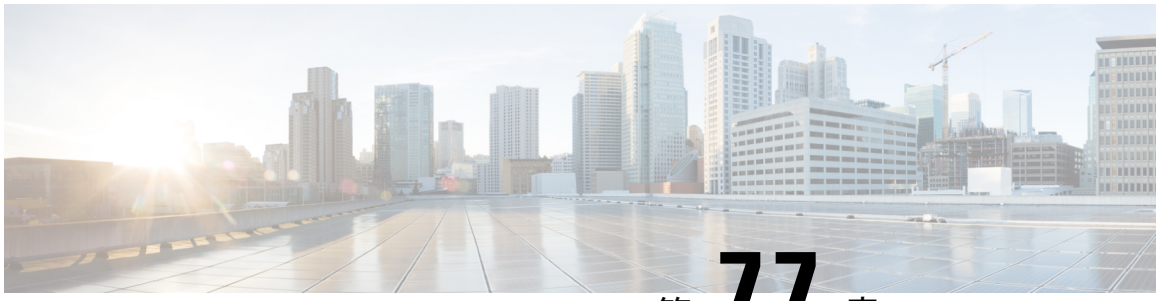
RADIUS 属性 104 の機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *110 : RADIUS* 属性 *104* の機能情報

機能名	リリース	機能情報
RADIUS 属性 104	Cisco IOS XE Release 3.9S	RADIUS 属性 104 機能を使用すれば、RADIUS 認可プロファイル内でプライベート ルート（属性 104）を指定できます。プライベート ルートは、個々のインターフェイス上で受信されたパケットにのみ影響します。ルートはグローバル ルーティング テーブルとは別に保存され、ルーティング プロトコルに埋め込まれて再配布されることはありません。 次のコマンドが導入または変更されました。\tips-migration **show ip policy**、**show route-map**。



第 77 章

RADIUS NAS-IP-Address 属性設定可能性

RADIUS NAS-IP-Address 属性設定可能性機能を使用すれば、RADIUS パケットの IP ヘッダー内の発信元 IP アドレスを変更せずに、任意の IP アドレスを設定して RADIUS 属性 4（NAS-IP-Address）として使用できます。この機能は、サービスプロバイダーが、スケーラビリティを向上させるために、小規模なネットワーク アクセス サーバ（NAS）のクラスタを使用して大規模なNASをシミュレートしている場合にも使用できます。この機能を使用すれば、NAS を RADIUS サーバから見て、単一の RADIUS クライアントとして機能させることができます。

RADIUS NAS-IP-Address 属性設定可能性の前提条件

この機能を設定する前に、次の要件を満たす必要があります。

- IP セキュリティ（IPSec）の使用経験と、RADIUS サーバと認証、許可、アカウンティング（AAA）の両方の設定経験が必要です。
- RADIUS サーバと AAA リストを設定する必要があります。

RADIUS NAS-IP-Address 属性設定可能性の制約事項

スケーラビリティを向上させるために、RADIUS クライアントのクラスタを単一の RADIUS クライアントのシミュレーションに使用している場合に、次の制約事項が適用されます。制約事項に対する解決策または次善策についても説明します。

- RADIUS 属性 44（Acct-Session-Id）は、複数の NAS からのセッション間で重複する可能性があります。

2 つの解決策があります。NAS ルータ上で **radius-server attribute 44 extend-with-addr** コマンドと **radius-server unique-ident** コマンドのどちらかを使用して、NAS ルータごとに異なる先頭の番号を指定できます。

- RADIUS サーバベースの IP アドレス プールを NAS ごとに管理する必要があります。

この解決策は、RADIUS サーバ上で NAS ごとに異なる IP アドレス プール プロファイルを設定することです。NAS ごとに異なるプール ユーザ名を使用してそれらを取得します。

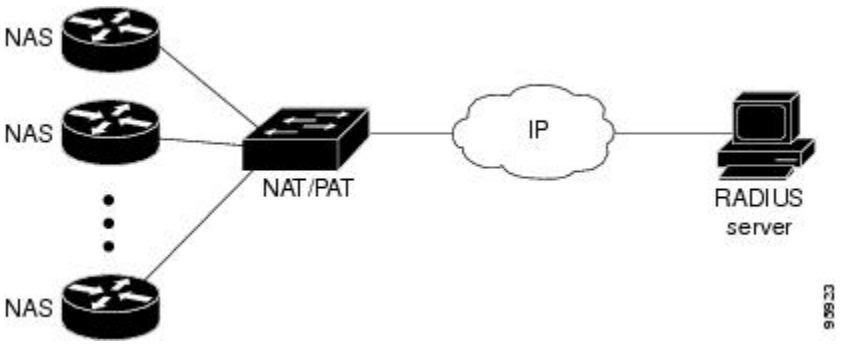
- セッション内の RADIUS 要求メッセージは NAS ごとに識別される必要があります。

この解決策の 1 つは、NAS 上で **radius-server attribute 32 include-in-access-req** コマンドを使用して、NAS ごとに異なる RADIUS 属性 32（NAS-Identifier）用の形式文字列を設定することです。

RADIUS NAS-IP-Address 属性設定可能性に関する情報

次の図に示すように、小規模な NAS RADIUS クライアントのクラスタを使用して大規模な NAS RADIUS クライアントをシミュレートする場合は、ネットワークアドレス変換（NAT）デバイスまたはポートアドレス変換（PAT）デバイスがネットワークに挿入されます。このデバイスは、NAS のクライアントと、RADIUS サーバに接続された IP クラウドの間に配置されます。複数の NAS からの RADIUS トラフィックが NAT または PAT デバイスを通過するときに、RADIUS パケットの発信元 IP アドレスが単一の IP アドレスに変換されます。ほとんどの場合、この IP アドレスは、NAT または PAT デバイスのループバック インターフェイス上の IP アドレスです。NAS ごとに異なるユーザ データグラム プロトコル（UDP）発信元プールが RADIUS パケットに割り当てられます。サーバから RADIUS 応答が返されると、NAT または PAT デバイスがそれを受信して、宛先 UDP ポートを使用して宛先 IP アドレスを NAS の IP アドレスに変換し、対応する NAS に転送します。

次の図は、複数の NAS の送信元 IP アドレスが、IP クラウドへの途中で NAT または PAT デバイスを通過するときに、どのように単一の IP アドレスに変換されるかを示しています。



通常は、RADIUS サーバが RADIUS パケットの IP ヘッダー内の発信元 IP アドレスをチェックして、RADIUS 要求の発信元を追跡し、セキュリティを確保します。NAT または PAT による

解決策は、RADIUS パケットが複数の NAS ルータから送られてきても単一の発信元 IP アドレスが使用されるため、これらの要件を満たします。

ただし、RADIUSデータベースからアカウンティング レコードを取得するときに、課金システムによっては、アカウンティング レコード内でRADIUS 属性4（NAS-IP-Address）が使用される場合があります。この属性の値は、独自の IP アドレスとして NAS ルータ上に記録されます。NAS ルータは、RADIUS サーバとの間で動作している NAT または PAT を認識しません。そのため、NAS ルータごとに異なる RADIUS 属性 4 アドレスがユーザのアカウンティング レコードに記録されます。最終的に、これらのアドレスは、複数の NAS ルータを RADIUS サーバと対応する課金システムに公開することになります。

RADIUS NAS-IP-Address 属性設定可能性機能の使用方法

RADIUS NAS-IP-Address 属性設定可能性機能を使用すれば、任意の IP アドレスを RADIUS NAS-IP-Address（RADIUS 属性 4）として設定できます。すべてのルータに対して同じ IP アドレス（ほとんどの場合、NAT または PAT デバイスのループバック インターフェイス上の IP アドレス）を手動で設定することによって、NAS ルータのクラスタを NAT または PAT デバイスの後ろに隠して、RADIUS から見えないようにすることができます。

RADIUS NAS-IP-Address 属性設定可能性の設定方法

RADIUS NAS-IP-Address 属性設定可能性の設定

RADIUS NAS-IP-Address 属性設定可能性機能を設定する前に、RADIUS サーバまたはサーバグループと AAA 方式リストを設定しておく必要があります。

RADIUS NAS-IP-Address 属性設定可能性機能を設定するには、次の手順を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **radius-server attribute 4** *ip-address*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例：	グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
	`Router# configure terminal`	
ステップ 3	**radius-server attribute 4** *ip-address* 例： `Router (config)# radius-server attribute 4 10.2.1.1`	RADIUS NAS-IP-Address（属性 4）として使用する IP アドレスを設定します。

RADIUSNAS-IP-Address属性設定可能性のモニタリングとメンテナンス

RADIUS パケット内で使用されている RADIUS 属性 4 アドレスをモニターするには、**debug radius** コマンドを使用します。

手順の概要

1. **enable**
2. **debug radius**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**debug radius** 例： `Router# debug radius`	RADIUS 関連の情報を表示します。

例

次に、**debug radius** コマンドの出力例を示します。

```
Router# debug radius
RADIUS/ENCODE(0000001C): acct_session_id: 29
RADIUS(0000001C): sending
RADIUS(0000001C): Send Access-Request to 10.0.0.10:1645 id 21645/17, len 81
RADIUS:  authenticator D0 27 34 C0 F0 C4 1C 1B - 3C 47 08 A2 7E E1 63 2F
RADIUS:  Framed-Protocol     [7]   6   PPP                       [1]
RADIUS:  User-Name           [1]   18  "shashi@pepsi.com"
RADIUS:  CHAP-Password       [3]   19  *
RADIUS:  NAS-Port-Type       [61]  6   Virtual                   [5]
RADIUS:  Service-Type        [6]   6   Framed                    [2]
RADIUS:  NAS-IP-Address      [4]   6   10.0.0.21
```

```
UDP: sent src=10.1.1.1(21645), dst=10.0.0.10(1645), length=109
UDP: rcvd src=10.0.0.10(1645), dst=10.1.1.1(21645), length=40
RADIUS: Received from id 21645/17 10.0.0.10:1645, Access-Accept, len 32
RADIUS:  authenticator C6 99 EC 1A 47 0A 5F F2 - B8 30 4A 4C FF 4B 1D F0
RADIUS:  Service-Type        [6]   6   Framed                    [2]
RADIUS:  Framed-Protocol     [7]   6   PPP                       [1]
RADIUS(0000001C): Received from id 21645/17
```

RADIUS NAS-IP-Address 属性設定可能性の設定例

RADIUS NAS-IP-Address 属性設定可能性の設定例

次の例は、IP アドレス 10.0.0.21 が RADIUS NAS-IP-Address 属性として設定されていることを示しています。

```
radius-server attribute 4 10.0.0.21
radius-server host 10.0.0.10 auth-port 1645 acct-port 1646 key cisco
```

その他の参考資料

次の項で、RADIUS NAS-IP-Address 属性設定可能性に関する参考資料を紹介します。

関連資料

関連項目	マニュアル タイトル
AAA の設定	『*Cisco IOS Security Configuration Guide: Securing User Services*』の「認証、認可、およびアカウンティング（AAA）」の項
RADIUS の設定	「Configuring RADIUS」モジュール。
RADIUS コマンド	『*Cisco IOS Security Command Reference*』

標準

標準	タイトル
この機能がサポートする新しい規格または変更された規格はありません。	--

MIB

MIB	MIB のリンク
この機能によってサポートされる新しい MIB または変更された MIB はありません。	選択したプラットフォーム、Cisco IOS リリース、およびフィーチャ セットに関する MIB を探してダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

RFC

RFC	タイトル
この機能でサポートが追加または変更された RFC はありません。	--

シスコのテクニカル サポート

説明	リンク
シスコのサポート Web サイトでは、シスコの製品やテクノロジーに関するトラブルシューティングにお役立ていただけるように、マニュアルやツールをはじめとする豊富なオンライン リソースを提供しています。 お使いの製品のセキュリティ情報や技術情報を入手するために、Cisco Notification Service（Field Notice からアクセス）、Cisco Technical Services Newsletter、Really Simple Syndication（RSS）フィードなどの各種サービスに加入できます。 シスコのサポート Web サイトのツールにアクセスする際は、Cisco.com のユーザ ID およびパスワードが必要です。	http://www.cisco.com/en/US/support/index.html

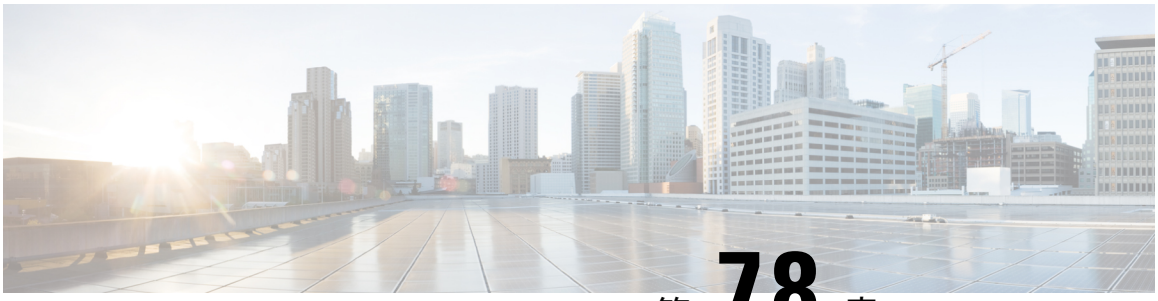
RADIUS NAS-IP-Address 属性設定可能性の機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *111 : RADIUS NAS-IP-Address* 属性設定可能性の機能情報

機能名	リリース	機能情報
RADIUS NAS-IP-Address 属性設定可能性	Cisco IOS XE Release 3.9S	この機能を使用すれば、RADIUS パケットの IP ヘッダー内の発信元 IP アドレスを変更せずに、任意の IP アドレスを設定して RADIUS 属性 4（NAS-IP-Address）として使用できます。 この機能のために **radius-server attribute 4** コマンドが導入されました。



第 78 章

サーバ単位グループ レベルで指定された RADIUS 属性 5 NAS-Port フォーマット

サーバ単位グループ レベルで指定されたRADIUS属性5（NAS-Port）フォーマット機能を使用すれば、RADIUSサーバ グループごとに設定をカスタマイズできます。この柔軟性によって、グローバルフォーマットの代わりに、カスタマイズされたネットワークアクセスサーバ（NAS）ポート フォーマットを使用できます。

サーバ単位グループ レベルで指定された RADIUS 属性 5 NAS-Port フォーマットの前提条件

- 認証、認可、およびアカウンティング（AAA）コンポーネントを含む Cisco IOS イメージを実行する必要があります。

サーバ単位グループ レベルで指定された RADIUS 属性 5 NAS-Port フォーマットに関する情報

RADIUS 属性 5 フォーマットのカスタマイズ

Cisco IOS リリース 12.3(14)T よりも前の Cisco IOS ソフトウェアでは、アクセス要求またはアカウンティング要求で送信された RADIUS 属性をグローバルにカスタマイズすることが可能でした。設定可能な各属性では、RADIUS サーバとの通信時の動作がカスタマイズできました。サーバグループの実装により、グローバル属性設定の柔軟性が制限され、ルータと相互に通信する可能性のあるさまざまな RADIUS サーバをサポートするのに必要な、種々のカスタマイズに対処できなくなりました。たとえば、**global radius-server attribute nas-port format command** オプションを設定すると、RADIUS サーバーと相互に通信するルータのすべてのサービスが同じ設定で使用されていました。

Cisco IOS リリース 12.3(14)T では、ルータを設定して、サーバ単位のグループを柔軟に上書きできるようになりました。RADIUS サーバ上のさまざまなサービス タイプに固有の名前付け方式を使用するようサービスを設定できます。サービス タイプは、独自のサービス グループを使用するように設定できます。この柔軟性により、NAS-port フォーマットをカスタマイズして、グローバル フォーマットの代わりに使用できるようになりました。

サーバ単位グループ レベルで指定された RADIUS 属性 5 NAS-Port フォーマットの設定方法

サーバ単位グループ レベルの RADIUS 属性 5 フォーマットの設定

サーバ単位グループ レベルの RADIUS 属性 5 フォーマットをサポートするようにルータを設定するには、次の手順を実行します。

（注） サーバ単位グループの機能を使用するには、名前付け方式リストをサービス内で積極的に使用する必要があります。1 つのクライアントを特定の名前付き方式を使用するように設定して、他のクライアントをデフォルト フォーマットを使用するように設定できます。

始める前に

次の手順を実行する前に、まず AAA の方式リストを設定して、お客様の状況に適用できるようにする必要があります。

手順の概要

1. **enable**
2. **configure terminal**
3. **aaa group server radius** *group-name*
4. **server** *ip-address* [**auth-port** *port-number*] [**acct-port** *port-number*]
5. **attribute nas-port format** *format-type* [*string*]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**aaa group server radius** *group-name* 例： `Router (config)# aaa group server radius radius1`	異なる RADIUS サーバ ホストを別々のリストと方式にグループ化し、server-group コンフィギュレーション モードを開始します。
ステップ 4	**server** *ip-address* [**auth-port** *port-number*] [**acct-port** *port-number*] 例： `Router (server-group)# server 172.101.159.172 auth-port 1645 acct-port 1646`	グループ サーバー用の RADIUS サーバーの IP アドレスを設定します。
ステップ 5	**attribute nas-port format** *format-type* [*string*] 例： `Router (server-group)# attribute nas-port format d`	サービスの種類ごとに固有の名前付け方式を使用するようにサービスを設定します。 • サービス タイプは、独自のサーバ グループを使用するように設定できます。

サーバ単位グループ レベルの RADIUS 属性 5 フォーマットのモニタリングとメンテナンス

サーバー単位グループレベルのRADIUS属性5フォーマットをモニターおよびメンテナンスするには、次の手順を実行します（**debug** コマンドは個別に使用される場合があります）。

手順の概要

1. **enable**
2. **debug aaa sg-server selection**
3. **debug radius**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**debug aaa sg-server selection** 例： `Router# debug aaa sg-server selection`	ルータ内の RADIUS および TACACS+ サーバ グループ システムが特定のサーバを選択している理由に関する情報を表示します。
ステップ 3	**debug radius** 例： `Router# debug radius`	サーバ グループが特定の要求に対して選択されたことを示す情報を表示します。

サーバ単位グループ レベルで指定された RADIUS 属性 5 NAS-Port フォーマットの設定例

サーバ単位グループ レベルで指定された RADIUS 属性 5 フォーマットの例

次の設定例は、デフォルトが形式 F:\tips-migration を使用する一方、RADIUS 属性 5 を送信しないよう選択された専用線 PPP クライアントを示します。

```
interface Serial2/0
 no ip address
 encapsulation ppp
 ppp accounting SerialAccounting
 ppp authentication pap
aaa accounting network default start-stop group radius
aaa accounting network SerialAccounting start-stop group group1
aaa group server radius group1
 server 10.101.159.172 auth-port 1645 acct-port 1646
 attribute nas-port none
radius-server host 10.101.159.172 auth-port 1645 acct-port 1646
radius-server attribute nas-port format d
```

その他の参考資料

ここでは、RADIUS ベンダー固有属性（VSA）および RADIUS Disconnect-Cause 属性値に関する関連資料について説明します。

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『Cisco IOS Master Commands List, All Releases』
セキュリティ コマンド	『*Cisco IOS Security Command Reference*』
セキュリティ機能	『*Cisco IOS XE Security Configuration Guide: Securing User Services*, Release 2』
セキュリティ サーバ プロトコル	『*Cisco IOS XE Security Configuration Guide: Securing User Services*, Release 2』の「セキュリティ サーバ プロトコル」の項
RADIUS Configuration	「RADIUS の設定」機能モジュール。

標準

標準	タイトル
インターネット技術特別調査委員会（IETF）インターネット ドラフト：Network Access Servers Requirements	「Network Access Servers Requirements: Extended RADIUS Practices」

MIB

MIB	MIB のリンク
なし。	選択したプラットフォーム、Cisco ソフトウェア リリース、およびフィーチャ セットの MIB を検索してダウンロードする場合は、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

RFC

RFC	タイトル
RFC 2865	『Remote Authentication Dial In User Service (RADIUS)』

シスコのテクニカル サポート

説明	リンク
シスコのサポート Web サイトでは、シスコの製品やテクノロジーに関するトラブルシューティングにお役立ていただけるように、マニュアルやツールをはじめとする豊富なオンライン リソースを提供しています。 お使いの製品のセキュリティ情報や技術情報を入手するために、Cisco Notification Service（Field Notice からアクセス）、Cisco Technical Services Newsletter、Really Simple Syndication（RSS）フィードなどの各種サービスに加入できます。 シスコのサポート Web サイトのツールにアクセスする際は、Cisco.com のユーザ ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

サーバ単位グループ レベルで指定された RADIUS 属性 5 NAS-Port フォーマットの機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

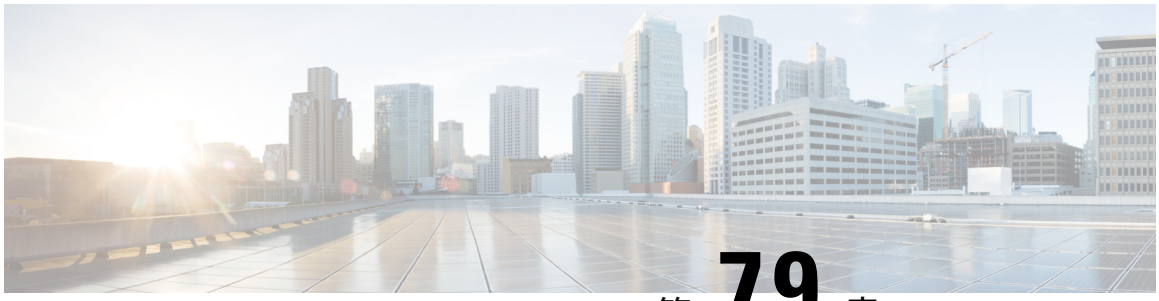
プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *112 :* サーバ単位グループ レベルで指定された *RADIUS* 属性 *5*（*NAS-Port*）フォーマットの機能情報

機能名	リリース	機能情報
サーバ単位グループ レベルで指定された RADIUS 属性 5（NAS-Port）フォーマット	Cisco IOS XE Release 3.9S	サーバ単位グループ レベルで指定された RADIUS 属性 5（NAS-Port）フォーマット機能を使用すれば、RADIUS サーバ グループごとに設定をカスタマイズできます。この柔軟性によって、グローバル フォーマットの代わりに、カスタマイズされたネットワーク アクセス サーバ（NAS）ポート フォーマットを使用できます。 次のコマンドが導入または変更されました。\tips-migration **attribute nas-port format**。

第 VI 部

TACACS



第 79 章

TACACS の設定

この章では、詳細なアカウンティング情報を提供し、認証および許可プロセスを柔軟に管理できるようにするために、TACACS+ をイネーブルにして設定する方法について説明します。TACACS+は、AAA を介して実装され、AAA コマンドを使用してのみイネーブルにできます。

TACACS に関する情報

TACACS+は、ユーザーによるルータまたはネットワーク アクセス サーバーへのアクセス試行の集中的な確認を可能にするセキュリティアプリケーションです。TACACS+ サービスは、通常 UNIX または Windows NT ワークステーション上で動作する TACACS+ デーモンのデータベースで管理されます。ネットワーク アクセス サーバーに設定した TACACS+ 機能を使用可能にするには、TACACS+ サーバーにアクセスして TACACS+ サーバーを設定しておく必要があります。

TACACS+ では、独立したモジュラ型の認証、許可、アカウンティング機能が提供されます。TACACS+ を使用すると、単一のアクセス コントロール サーバー（TACACS+ デーモン）で、各サービス（認証、許可、アカウンティング）を個別に提供できます。各サービスを固有のデータベースに結合し、デーモンの機能に応じてそのサーバーまたはネットワークで使用できる他のサービスを提供できます。

TACACS+の目的は、単一の管理サービスから複数のネットワーク アクセス ポイントを管理する方法を提供することです。アクセス サーバーおよびルーティングのシスコ ファミリおよび（ルータとアクセス サーバー両方の）Cisco IOS および Cisco IOS XE ユーザー インターフェイスは、ネットワーク アクセス サーバーにすることができます。

ネットワーク アクセス ポイントによって、従来の「低機能な」端末、端末エミュレータ、ワークステーション、パーソナル コンピュータ（PC）、およびルータと、適切なアダプタ（たとえば、モデムまたは ISDN アダプタ）を併用して、Point-to-Point Protocol（PPP）、Serial Line Internet Protocol（SLIP）、Compressed SLIP（CSLIP）、または AppleTalk Remote Access（ARA）

プロトコルを使用する通信が可能になります。つまり、ネットワーク アクセス サーバーは、単一のユーザー、ネットワークまたはサブネットワーク、および相互接続したネットワークに対して、接続を提供できます。ネットワーク アクセス サーバーを介して接続されているエンティティは、ネットワーク アクセス クライアントと呼ばれます。たとえば、音声グレードの回路で PPP を実行する PC は、ネットワーク アクセス クライアントです。AAA セキュリティ サービスを介して管理される TACACS+ は、次のサービスを提供できます。

- 認証：ログインとパスワードのダイアログ、チャレンジ/レスポンス、メッセージングのサポートを介して、認証を詳細に制御できます。

認証機能には、ユーザーに任意のダイアログを実行する機能があります（たとえば、ログインとパスワードの指定後に、自宅住所、母親の旧姓、サービス タイプ、社会保険番号などの複数の質問をユーザーに試行する機能）。さらに、TACACS+ 認証サービスは、ユーザー画面へのメッセージ送信をサポートします。たとえば、会社のパスワード有効期間ポリシーに従い、パスワードの変更の必要があることをユーザーに通知することもできます。

- 認可：autocommand、アクセス コントロール、セッション期間、プロトコル サポートの設定といった、ユーザー セッション時のユーザー機能についてきめ細かく制御します。また、TACACS+ 認可機能を使用して、ユーザーが実行できるコマンドを制限することもできます。
- アカウンティング：課金、監査、およびレポートに使用する情報を収集して TACACS+ デーモンに送信します。ネットワークの管理者は、アカウンティング機能を使用して、セキュリティ監査のためにユーザの活動状況をトラッキングしたり、ユーザ課金用の情報を提供したりできます。アカウンティング レコードには、ユーザ ID、開始時刻および終了時刻、実行されたコマンド（PPP など）、パケット数、およびバイト数が含まれます。

TACACS+ プロトコルは、ネットワーク アクセス サーバーと TACACS+ デーモンの間に認証機能を提供します。また、ネットワーク アクセス サーバーと TACACS+ デーモン間のすべてのプロトコル交換は暗号化されるため、機密性を確保できます。

TACACS+ デーモン ソフトウェアを実行するシステムで、ネットワーク アクセス サーバーで TACACS+ 機能を使用する必要があります。

独自の TACACS+ ソフトウェアを開発することに関心があるユーザー向けに、シスコでは、TACACS+ プロトコル仕様をドラフトの RFC として使用できるようにしています。

TACACS の動作

ユーザーが TACACS+ を使用してネットワーク アクセス サーバーに対して認証を受けることで、単純な ASCII ログインを試行すると、一般的に、次のプロセスが発生します。

1. 接続が確立すると、ネットワーク アクセス サーバーは TACACS+ デーモンに接続してユーザー名のプロンプトをを取得します。また、そのプロンプトはユーザーに表示されます。ユーザーがユーザー名を入力すると、ネットワーク アクセス サーバーは TACACS+ デーモンに接続し、パスワード プロンプトを取得します。ネットワーク アクセス サーバーはユーザーに対してパスワードプロンプトを表示します。ユーザーがパスワードを入力すると、パスワードは TACACS+ デーモンに送信されます。

（注） TACACS+によって、デーモンとユーザーとの間で対話できるようになり、デーモンはユーザーの認証に必要な情報を取得できるようになります。通常、この処理は、ユーザー名とパスワードの組み合わせのプロンプトを表示することで完了しますが、TACACS+デーモンの制御下で、母親の旧姓など、他のアイテムを含めることができます。

1. ネットワーク アクセス サーバーは、最終的に TACACS+ デーモンから次のいずれかの応答を得ます。
    1. ACCEPT：ユーザーは認証され、サービスを開始できます。認可を必須にするようにネットワーク アクセス サーバーが設定されている場合、この時点で認可が開始されます。
    2. REJECT：ユーザーは認証に失敗しました。ユーザーは以降のアクセスを拒否される可能性があります。または、TACACS+ デーモンに応じてログイン シーケンスを再試行するようにプロンプトが表示されます。
    3. ERROR：認証中のある時点でエラーが発生しました。エラーは、デーモン、またはデーモンとネットワーク アクセス サーバー間のネットワーク接続で発生する可能性があります。ERROR 応答を受信すると、通常、ネットワーク アクセス サーバーはユーザーを認証する代替方式を使用しようとします。
    4. CONTINUE：ユーザーは、さらに認証情報の入力を求められます。
2. PAP ログインは、ASCII ログインに似ていますが、ユーザーによる入力ではなく、PAP プロトコル パケットでユーザー名とパスワードがネットワーク アクセス サーバーに到達するため、ユーザーにはプロンプトが表示されません。PPP CHAP ログインは、原則もにています。

ネットワーク アクセス サーバーで認可をイネーブルにしている場合、認証の後に、ユーザーは追加の認可段階を実行する必要があります。ユーザーは TACACS+ 許可に進む前に、まず TACACS+ 認証を正常に完了する必要があります。

1. TACACS+ の認可が必要な場合も、TACACS+ デーモンに接続します。また、TACACS+ デーモンは、ACCEPT または REJECT 認可応答を返します。ACCEPT 応答が返される場合、この応答には、そのユーザーに関する EXEC または NETWORK セッションを指示するために使用される属性の形式のデータが含まれます。これによって、ユーザーがアクセスできるサービスを判断します。この場合のサービスは次のとおりです。
    1. Telnet、rlogin、ポイントツーポイント プロトコル（PPP）、シリアル ライン インターネット プロトコル（SLIP）、EXEC サービス
    2. 接続パラメータ（ホストまたはクライアントの IP アドレス、アクセス リスト、およびユーザ タイムアウトを含む）

TACACS の設定方法

TACACS+ をサポートするようにルータを設定するには、次のタスクを実行する必要があります。

- **aaa new-model** グローバル コンフィギュレーション コマンドを使用して、AAA をイネーブルにします。TACACS+ を使用する予定がある場合、AAA を設定する必要があります。**aaa new-model** コマンドの使用の詳細については、「AAA の概要」の章を参照してください。
- コマンドを使用して、1 つ以上の TACACS+ デーモンの IP アドレスを指定します。 コマンドを使用して、ネットワーク アクセス サーバーと TACACS+ デーモンの間のすべてのやり取りを暗号化するために使用する暗号化キーを指定します。TACACS+デーモンでも、この同じキーを設定する必要があります。
- **aaa authentication** グローバル コンフィギュレーション コマンドを使用して、認証に TACACS+ を使用する方式リストを定義します。**aaa authentication** コマンドの使用の詳細については、「認証の設定」の章を参照してください。
- line および interface コマンドを使用して、定義済みの方式リストを多様なインターフェイスに適用します。詳細については、「認証の設定」の章を参照してください。
- 必要に応じて、**aaa authorization** グローバル コマンドを使用して、ネットワーク アクセス サーバーの認可を設定します。回線またはインターフェイスごとに設定できる認証とは異なり、認可は、ネットワーク アクセス サーバー全体のグローバル設定です。**aaa authorization** コマンドの使用の詳細については、「認可の設定」の章を参照してください。
- 必要に応じて、**aaa accounting** コマンドを使用して TACACS+ 接続のアカウンティングをイネーブルにします。**aaa accounting** コマンドの使用の詳細については、「アカウンティングの設定」の章を参照してください。

TACACS サーバー ホストの指定

コマンドを使用すると、TACACS+ サーバーを保守する 1 つまたは複数の IP ホストの名前を指定できます。TACACS+ ソフトウェアは、指定した順序でホストを検索するため、この機能は、希望のデーモン リストを設定する場合に役立ちます。

TACACS+ホストを指定するには、グローバル コンフィギュレーション モードで次のコマンドを使用します。

コマンド	目的
`Router(config)# hostname [single-connection] [port integer] [timeout integer] [key string]`	TACACS+ ホストを指定します。

コマンドを使用して、次のオプションも設定できます。

- **single-connection** キーワードを使用して、単一接続を指定します。通信が必要になるたびに、ルータの接続を開き、TCP 接続を閉じるのではなく、single-connection オプションによって、ルータとデーモン間の単一のオープンな接続を保守します。この方法はデーモンが処理できる TACACS 操作数が多くなるため、効率的です。

（注） この処理を有効にするには、デーモンが single-connection モードをサポートする必要があります。サポートしていない場合、ネットワーク アクセス サーバーとデーモン間の接続が動作しなくなるか、不要なエラーを受信します。

- **port** *integer* 引数を使用して、TACACS+ デーモンに接続するときに使用される TCP ポート番号を指定します。デフォルト ポート番号は 49 です。
- **timeout** *integer* 引数を使用して、ルータがタイムアウトしてエラー宣言するまで、デーモンからの応答を待つ期間（秒）を指定します。

（注） コマンドによるタイムアウト値の指定は、このサーバーに関するコマンドで設定されたデフォルトのタイムアウト値よりも優先されます。

- **key** *string* 引数を指定して、ネットワーク アクセス サーバーと TACACS+ デーモン間のすべてのトラフィックを暗号化および復号化するための暗号キーを指定します。

（注） コマンドによる暗号キーの指定は、このサーバーに関するグローバル コンフィギュレーションの コマンドで設定されたデフォルト キーよりも優先されます。

コマンドのパラメータの一部は、 コマンドおよび コマンドによるグローバル設定よりも優先されるため、このコマンドを使用して個別の TACACS+ 接続を一意に設定することで、ネットワークのセキュリティを強化できます。

TACACS 認証キーの設定

グローバル TACACS+ 認証キーおよび暗号化キーを設定するには、グローバル コンフィギュレーション モードで次のコマンドを使用します。

コマンド	目的
`Router(config)# key`	TACACS+ デーモンで使用する、一致する暗号キーを設定します。

（注） 暗号化が成功するには、TACACS+ デーモンに同じキーを設定する必要があります。

AAA サーバー グループの設定

AAA サーバー グループを使用するようにルータを設定すると、既存のサーバー ホストをグループ化できます。これによって、設定したサーバーホストのサブセットを選択し、それを特定のサービスに使用できます。サーバー グループは、グローバル サーバー ホスト リストと併せて使用されます。サーバー グループには、選択したサーバー ホストの IP アドレスが一覧表示されます。

サーバー グループには複数のホスト エントリを含めることができます。ただし、各エントリの IP アドレスが一意である必要があります。そのサーバー グループにある異なる 2 つのホストエントリが 1 つのサービス（アカウンティングなど）に設定されている場合、設定されている 2 番めのホスト エントリは最初のホスト エントリのフェールオーバー バックアップとして動作します。この例の場合、最初のホスト エントリがアカウンティング サービスの提供に失敗すると、2 番めのホストエントリを使用してアカウンティング サービスを提供するように、ネットワーク アクセス サーバーが試行します（試行される TACACS+ ホスト エントリの順番は、設定されている順序に従います）。

サーバー グループ名を使用してサーバーホストを定義するには、グローバル コンフィギュレーション モードで次のコマンドを使用します。一覧のサーバーは、グローバル コンフィギュレーション モードに存在します。

ステップ 1 Router(config)# *name* [**single-connection**] [**port** *integer*] [**timeout** *integer*] [**key** *string*]

サーバー ホストの IP アドレスを指定および定義してから、AAA サーバー グループを設定します。 コマンドの詳細については、この章の「TACACS サーバー ホストの指定」セクションを参照してください。

ステップ 2 Router(config-if)# **aaa group server**{**radius** | **tacacs+**} *group-name*

グループ名を指定して AAA サーバー グループを定義します。グループのすべてのメンバは、タイプを同じにする必要があります。つまり、RADIUS または TACACS+ です。このコマンドでは、サーバー グループのサブコンフィギュレーション モードにルータを配置します。

ステップ 3 Router(config-sg)# **server** *ip-address* [**auth-port** *port-number*] [**acct-port** *port-number*]

特定の TACACS+ サーバーを定義済みのサーバー グループと関連付けます。**auth-port** *port-number* オプションを使用して、認証専用の UDP ポートを設定します。**acct-port** *port-number* オプションを使用して、アカウンティング専用の UDP ポートを設定します。

AAA サーバー グループの TACACS+ サーバーごとに、このステップを繰り返します。

（注） グループの各サーバーは、 コマンドを使用して事前に定義する必要があります。

DNIS に基づく AAA サーバー グループの選択の設定

Cisco IOS XE ソフトウェアを使用すると、セッションの Dialed Number Identification Service（DNIS）番号に基づき、特定の AAA サーバー グループに対してユーザーを認証できます。すべての電話回線（通常の自宅電話または商用の T1/PRI 回線）を、複数の電話番号と関連付けることができます。DNIS 番号は、ユーザー宛てに発信された番号を示します。

たとえば、複数の顧客で同じ電話番号を共有する場合に、電話を受ける前に発信元を知りたいことがあります。DNIS を使用すると、応答するときに発信元の顧客がわかるため、電話に応答する方法をカスタマイズできます。

ISDN または内部モデムと接続する Cisco ルータは、DNIS 番号を受信できます。この機能を使用すると、顧客ごとに異なる TACACS+ サーバー グループを割り当て可能です（つまり、DNIS 番号ごとに異なる TACACS+ サーバー）。さらに、サーバー グループを使用して、複数の AAA サービスに同じサーバー グループを指定できます。また、各 AAA サービスに個別のサーバー グループを指定できます。

Cisco IOS XE ソフトウェアには、認証サービスとアカウンティング サービスを複数の方法で実装できる柔軟性があります。

- グローバル：AAA サービスは、グローバル コンフィギュレーション アクセス リスト コマンドを使用して定義され、特定のネットワーク アクセス サーバー上のすべてのインターフェイスに、全般的に適用されます。
- インターフェイス別：AAA サービスは、インターフェイス コンフィギュレーション コマンドを使用して定義され、特定のネットワーク アクセス サーバーに設定されているインターフェイスにだけ適用されます。
- DNIS マッピング：DNIS を使用して、AAA サーバーが AAA サービスを提供するように指定します。

複数の AAA コンフィギュレーション方式を同時に設定できるため、シスコでは、AAA サービスを提供するサーバーまたはサーバー グループを決定するために、優先順位を設定しました。優先順位は次のとおりです。

- DNIS 別：AAA サービスを提供するサーバー グループを DNIS によって指定するようネットワーク アクセス サーバーを設定している場合、この方式がその他の AAA 選択方式よりも優先されます。
- インターフェイス別：サーバーから AAA サービスを提供する方法をアクセス リストによって決定するように、インターフェイスごとにネットワーク アクセス サーバーを設定している場合、この方式が他のグローバル コンフィギュレーション AAA アクセス リストよりも優先されます。
- グローバル：セキュリティ サーバーが AAA サービスを提供する方法を決定するために、グローバル AAA アクセス リストを使用してネットワーク アクセス サーバーを設定する場合、この方式には最も低い優先度が使用されます。

（注） DNIS に基づいて AAA サーバー グループの選択を設定する前に、各 AAA サーバー グループに関連付けられたリモートセキュリティ サーバーを設定する必要があります。「TACACS サーバー ホストの指定」および「AAA サーバー グループの設定」を参照してください。

サーバー グループの DNIS に基づいて、特定の AAA サーバー グループを選択するようにルータを設定するには、DNIS マッピングを設定します。DNIS 番号を使用して、サーバー グループをグループ名とマッピングするには、グローバル コンフィギュレーション モードで次のコマンドを使用します。

ステップ 1 Router(config)# **aaa dnis map enable**

DNIS マッピングをイネーブルにします。

ステップ 2 Router(config)# **aaa dnis map** *dnis-number* **authentication ppp group** *server-group-name*

DNIS 番号を定義済みの AAA サーバー グループにマッピングします。このサーバー グループのサーバーは、認証に使用されます。

ステップ 3 Router(config)# **aaa dnis map** *dnis-number* **accounting network** [**none** | **start-stop** | **stop-only**] **group** *server-group-name*

DNIS 番号を定義済みの AAA サーバー グループにマッピングします。このサーバー グループのサーバーは、アカウンティングに使用されます。

TACACS 認証の指定

TACACS+ デーモンを指定し、関連する TACACS+ 暗号キーを定義したら、TACACS+ 認証の方式リストを定義する必要があります。TACACS+ 認証は AAA を介して実行されるため、認証方式として TACACS+ を指定して、**aaa authentication** コマンドを発行する必要があります。詳細については、「認証の設定」の章を参照してください。

TACACS 認可の指定

AAA 許可により、ユーザによるネットワーク アクセスを制限するパラメータを設定することができます。TACACS+ を介する許可は、コマンド、ネットワーク接続、および EXEC セッションに適用できます。AAA によって TACACS+ 許可が容易になるため、認可方式として TACACS+ を指定して、**aaa authorization** コマンドを発行する必要があります。詳細については、「認可の設定」の章を参照してください。

TACACS アカウンティングの指定

AAA アカウンティングを使用すると、ユーザーがアクセスしているサービスや、ユーザーが消費しているネットワーク リソース量を追跡できます。AAA によって TACACS+ アカウンティングは容易になるため、アカウンティング方式として TACACS+ を指定して、**aaa accounting** コマンドを発行する必要があります。詳細については、「アカウンティングの設定」の章を参照してください。

TACACS の AV ペア

ネットワーク アクセス サーバーが TACACS+ 認可機能およびアカウンティング機能を実装するには、各ユーザー セッションで TACACS+ の属性と値（AV）ペアを送受信します。サポートされる TACACS+ の AV ペアのリストについては、「TACACS 属性値ペア」の章を参照してください。

TACACS の設定例

TACACS 認証の例

次に、PPP 認証に使用するセキュリティ プロトコルとして TACACS+ を設定する例を示します。

```
aaa new-model
aaa authentication ppp test group tacacs+ local
 10.1.2.3
 key goaway
interface serial 0
 ppp authentication chap pap test
```

前述の設定例の回線は、次のように定義されます。

- **aaa new-model** コマンドは、AAA セキュリティ サービスをイネーブルにします。
- **aaa authentication** コマンドにより、PPP を実行するシリアル インターフェイスに使用する方式リスト「test」を定義します。キーワード **group tacacs+** は、TACACS+ を介して認証を実行することを示します。認証中に TACACS+ から何らかのエラーが返される場合、キーワード **local** は、ネットワーク アクセス サーバ上のローカル データベースを使用して認証が試行されることを示します。
- コマンドにより、TACACS+ デーモンが 10.1.2.3 という IP アドレスを持っていると指定します。 コマンドにより、共有暗号キーを「goaway」に定義します。
- **interface** コマンドで回線を選択します。**ppp authentication** コマンドは、テスト方式リストをこの回線に適用します。

次に、PPP 認証のセキュリティ プロトコルとして TACACS+ を設定する例を示します。ただし、「test」方式リストの代わりに、「default」方式リストが使用されます。

```
aaa new-model
aaa authentication ppp default if-needed group tacacs+ local
 10.1.2.3
 key goaway
interface serial 0
 ppp authentication chap default
```

前述の設定例の回線は、次のように定義されます。

- **aaa new-model** コマンドは、AAA セキュリティ サービスをイネーブルにします。
- **aaa authentication** コマンドにより、PPP を実行するシリアル インターフェイスに使用する方式リスト「default」を定義します。キーワード **default** は、デフォルトですべてのインターフェイスに PPP 認証が適用されることを示します。**if-needed** キーワードは、ユーザが ASCII ログイン手順を介してすでに認証済みの場合には PPP 認証が不要なのでスキップできることを示します。認証が必要な場合、キーワード **group tacacs+** は、TACACS+ を介して認証が実行されることを示します。認証中に TACACS+ から何らかのエラーが返される場合、キーワード **local** は、ネットワーク アクセス サーバ上のローカル データベースを使用して認証が試行されることを示します。
- コマンドにより、TACACS+ デーモンが 10.1.2.3 という IP アドレスを持っていると指定します。 コマンドにより、共有暗号キーを「goaway」に定義します。
- **interface** コマンドで回線を選択します。**ppp authentication** コマンドは、デフォルト方式リストをこの回線に適用します。

次に、PAP に同じ認証アルゴリズムを作成し、「default」ではなく「MIS-access」の方式リストを呼び出す例を示します。

```
aaa new-model
aaa authentication pap MIS-access if-needed group tacacs+ local
 10.1.2.3
 key goaway
interface serial 0
 ppp authentication pap MIS-access
```

前述の設定例の回線は、次のように定義されます。

- **aaa new-model** コマンドは、AAA セキュリティ サービスをイネーブルにします。
- **aaa authentication** コマンドにより、PPP を実行するシリアル インターフェイスに使用する方式リスト「MIS-access」を定義します。方式リスト「MIS-access」は、PPP 認証がすべてのインターフェイスに適用されることを示します。**if-needed** キーワードは、ユーザが ASCII ログイン手順を介してすでに認証済みの場合には PPP 認証が不要なのでスキップできることを示します。認証が必要な場合、キーワード **group tacacs+** は、TACACS+ を介して認証が実行されることを示します。認証中に TACACS+ から何らかのエラーが返される場合、キーワード **local** は、ネットワーク アクセス サーバ上のローカル データベースを使用して認証が試行されることを示します。
- コマンドにより、TACACS+ デーモンが 10.1.2.3 という IP アドレスを持っていると指定します。 コマンドにより、共有暗号キーを「goaway」に定義します。

- **interface** コマンドで回線を選択します。**ppp authentication** コマンドは、デフォルト方式リストをこの回線に適用します。

次に、IP アドレスが 10.2.3.4 である TACACS+ デーモンと暗号キー「apple」の設定の例を示します。

```
aaa new-model
aaa authentication login default group tacacs+ local
 10.2.3.4
 key apple
```

前述の設定例の回線は、次のように定義されます。

- **aaa new-model** コマンドは、AAA セキュリティ サービスをイネーブルにします。
- **aaa authentication** コマンドで、デフォルトの方式リストを定義します。すべてのインターフェイスでの着信 ASCII ログイン（デフォルト）では、認証に TACACS+ を使用します。応答する TACACS+ サーバがない場合、ネットワーク アクセス サーバは、認証用のローカル ユーザ名データベースに含まれる情報を使用します。
- コマンドにより、TACACS+ デーモンが 10.2.3.4 という IP アドレスを持っていると指定します。 コマンドにより、共有暗号キーが「apple」になるように定義します。

TACACS 認可の例

次に、デフォルトの方式リストを使用して、PPP 認証用のセキュリティ プロトコルとして、TACACS+ を設定する例を示します。また、TACACS+ を介してネットワークの許可を設定する方法も示します。

```
aaa new-model
aaa authentication ppp default if-needed group tacacs+ local
aaa authorization network default group tacacs+
 10.1.2.3
 key goaway
interface serial 0
 ppp authentication chap default
```

前述の設定例の回線は、次のように定義されます。

- **aaa new-model** コマンドは、AAA セキュリティ サービスをイネーブルにします。
- **aaa authentication** コマンドにより、PPP を実行するシリアル インターフェイスに使用する方式リスト「default」を定義します。キーワード **default** は、デフォルトですべてのインターフェイスに PPP 認証が適用されることを示します。**if-needed** キーワードは、ユーザが ASCII ログイン手順を介してすでに認証済みの場合には PPP 認証が不要なのでスキップできることを示します。認証が必要な場合、キーワード **group tacacs+** は、TACACS+ を介して認証が実行されることを示します。認証中に TACACS+ から何らかのエラーが返される場合、キーワード **local** は、ネットワーク アクセス サーバ上のローカル データベースを使用して認証が試行されることを示します。

- **aaa authorization** コマンドにより、TACACS+ を介するネットワークの許可を設定します。認証リストとは異なり、この許可リストは、ネットワーク アクセス サーバに対するすべての着信ネットワーク接続に常に適用されます。
- コマンドにより、TACACS+ デーモンが 10.1.2.3 という IP アドレスを持っていると指定します。 コマンドにより、共有暗号キーを「goaway」に定義します。
- **interface** コマンドで回線を選択します。**ppp authentication** コマンドは、デフォルト方式リストをこの回線に適用します。

TACACS アカウンティングの例

次に、デフォルトの方式リストを使用して、PPP 認証用のセキュリティ プロトコルとして、TACACS+ を設定する例を示します。また、TACACS+ を介してアカウンティングを設定する方法も示します。

```
aaa new-model
aaa authentication ppp default if-needed group tacacs+ local
aaa accounting network default stop-only group tacacs+
 10.1.2.3
 key goaway
interface serial 0
 ppp authentication chap default
```

前述の設定例の回線は、次のように定義されます。

- **aaa new-model** コマンドは、AAA セキュリティ サービスをイネーブルにします。
- **aaa authentication** コマンドにより、PPP を実行するシリアル インターフェイスに使用する方式リスト「default」を定義します。キーワード **default** は、デフォルトですべてのインターフェイスに PPP 認証が適用されることを示します。**if-needed** キーワードは、ユーザが ASCII ログイン手順を介してすでに認証済みの場合には PPP 認証が不要なのでスキップできることを示します。認証が必要な場合、キーワード **group tacacs+** は、TACACS+ を介して認証が実行されることを示します。認証中に TACACS+ から何らかのエラーが返される場合、キーワード **local** は、ネットワーク アクセス サーバ上のローカル データベースを使用して認証が試行されることを示します。
- **aaa accounting** コマンドにより、TACACS+ を介するネットワーク アカウンティングを設定します。この例では、ネットワーク接続が終了するたびに、終了したセッションについて説明するアカウンティング レコードが、TACACS+ デーモンに送信されます。
- コマンドにより、TACACS+ デーモンが 10.1.2.3 という IP アドレスを持っていると指定します。 コマンドにより、共有暗号キーを「goaway」に定義します。
- **interface** コマンドで回線を選択します。**ppp authentication** コマンドは、デフォルト方式リストをこの回線に適用します。

TACACS サーバー グループの例

次に、3 つの異なる TACACS+ サーバー メンバを使用してサーバー グループを作成する例を示します。

```
aaa group server tacacs tacgroup1
server 172.16.1.1
server 172.16.1.21
server 172.16.1.31
```

DNIS に基づく AAA サーバー グループの選択の設定例

次に、特定の AAA サービスを提供するために、DNIS に基づいて TACACS+ サーバー グループを選択する例を示します。

```
! This command enables AAA.
aaa new-model
!
! The following set of commands configures the TACACS+ servers that will be associated
! with one of the defined server groups.
 172.16.0.1
 172.17.0.1
 172.18.0.1
 172.19.0.1
 172.20.0.1
 key abcdefg
! The following commands define the sg1 TACACS+ server group and associate servers
! with it.
aaa group server tacacs sg1
  server 172.16.0.1
  server 172.17.0.1
! The following commands define the sg2 TACACS+ server group and associate a server
! with it.
aaa group server tacacs sg2
  server 172.18.0.1
! The following commands define the sg3 TACACS+ server group and associate a server
! with it.
aaa group server tacacs sg3
  server 172.19.0.1
! The following commands define the default-group TACACS+ server group and associate
! a server with it.
aaa group server tacacs default-group
  server 172.20.0.1
!
! The next set of commands configures default-group tacacs server group parameters.
aaa authentication ppp default group default-group
aaa accounting network default start-stop group default-group
!
! The next set of commands enables DNIS mapping and maps DNIS numbers to the defined
! RADIUS server groups. In this configuration, all PPP connection requests using DNIS
! 7777 are sent to the sg1 server group. The accounting records for these connections
! (specifically, start-stop records) are handled by the sg2 server group. Calls with a
! DNIS of 8888 use server group sg3 for authentication and server group default-group
! for accounting. Calls with a DNIS of 9999 use server group default-group for
! authentication and server group sg3 for accounting records (stop records only). All
! other calls with DNIS other than the ones defined use the server group default-group
! for both authentication and stop-start accounting records.
aaa dnis map enable
aaa dnis map 7777 authentication ppp group sg1
```

```
aaa dnis map 7777 accounting network start-stop group sg2
aaa dnis map 8888 authentication ppp group sg3
aaa dnis map 9999 accounting network stop-only group sg3
```

TACACS デーモンの設定例

次に、TACACS+ デーモンの設定例を示します。実際に TACACS+ デーモンで使用する正確な構文は、この例の構文と異なる可能性があります。

```
user = mci_customer1 {
 chap = cleartext “some chap password”
 service = ppp protocol = ip {
inacl#1=”permit ip any any precedence immediate”
inacl#2=”deny igrp 0.0.1.2 255.255.0.0 any”
 }
```

その他の参考資料

ここでは、TACACS+ の設定機能に関する関連資料について説明します。

関連資料

関連項目	マニュアル タイトル
TACACS+ コマンド	『*Cisco IOS Security Command Reference*』

標準

標準	タイトル
この機能でサポートされる新規の標準または変更された標準はありません。また、既存の標準のサポートは変更されていません。	--

MIB

MIB	MIB のリンク
この機能によってサポートされる新しい MIB または変更された MIB はありません。またこの機能による既存 MIB のサポートに変更はありません。	選択したプラットフォーム、Cisco IOS XE ソフトウェア リリース、およびフィーチャ セットの MIB の場所を検索しダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

RFC

RFC	タイトル
この機能によりサポートされた新規 RFC または改訂 RFC はありません。またこの機能による既存 RFC のサポートに変更はありません。	--

シスコのテクニカル サポート

説明	リンク
シスコのサポート Web サイトでは、シスコの製品やテクノロジーに関するトラブルシューティングにお役立ていただけるように、マニュアルやツールをはじめとする豊富なオンライン リソースを提供しています。 お使いの製品のセキュリティ情報や技術情報を入手するために、Cisco Notification Service（Field Notice からアクセス）、Cisco Technical Services Newsletter、Really Simple Syndication（RSS）フィードなどの各種サービスに加入できます。 シスコのサポート Web サイトのツールにアクセスする際は、Cisco.com のユーザ ID およびパスワードが必要です。	http://www.cisco.com/en/US/support/index.html

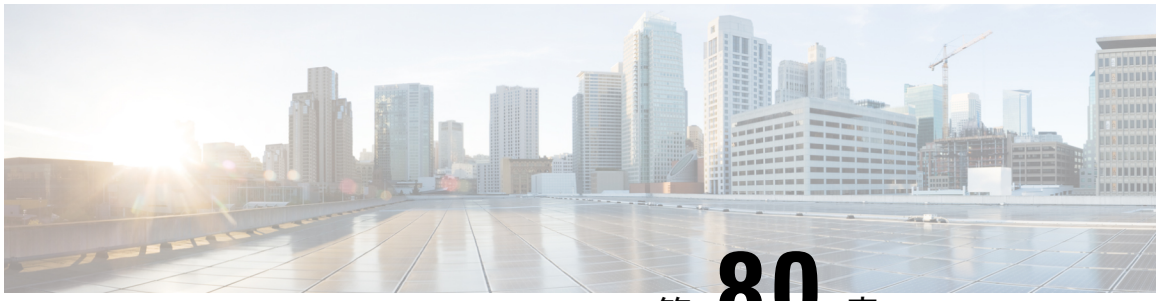
TACACS の設定に関する機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *113 : TACACS+* の設定に関する機能情報

機能名	リリース	機能情報
TACACS+		TACACS+ は、ユーザによるルータまたはネットワーク アクセス サーバへのアクセス試行の集中的な確認を可能にするセキュリティ アプリケーションです。 TACACS+ は、認証および認可プロセスについて詳細なアカウンティング情報と柔軟な管理コントロールを提供します。TACACS+ は、AAA を介して実装され、AAA コマンドを使用してのみイネーブルにできます。 次のコマンドが導入または変更されました：、、**aaa authentication**、 **aaa accounting**、**aaa group server tacacs+**。
DNIS に基づく AAA サーバー グループ		DNIS に基づく AAA サーバー グループを使用すると、セッションの着信番号識別サービス（DNIS）番号に基づき、特定の AAA サーバー グループに対してユーザーを認証できます。 次のコマンドが導入または変更されました。**aaa dnis map enable**、**aaa dnis map authentication group**、**aaa dnis map accounting**



第 80 章

TACACS サーバーの Per VRF

TACACS+ サーバーの Per VRF 機能により、TACACS+ サーバーで Per Virtual ルーティングおよび転送（Per VRF）の認証、認可、アカウンティング（AAA）を設定できます。

TACACS サーバーの Per VRF の前提条件

- TACACS+ サーバー アクセスが必要です。
- TACACS+、AAA および Per VRF AAA、およびグループ サーバー設定の経験が必要です。

TACACS サーバーの Per VRF の制限事項

- TACACS+ サーバーの Per VRF を設定する前に、ルータで VRF インスタンスをグローバルにイネーブルにする必要があります。

TACACS サーバーの Per VRF に関する情報

TACACS サーバーの Per VRF の概要

TACACS+ サーバーの Per VRF 機能を使用すると、TACACS+ サーバーで Per VRF AAA を設定できます。Cisco IOS XE リリース 2.2 よりも前のリリースでは、この機能は RADIUS サーバーでのみ使用できました。

TACACS サーバーの Per VRF の設定方法

TACACS サーバ上の Per VRF の設定

この手順の最初のステップは、AAA およびサーバ グループの設定、VRF ルーティング テーブルの作成、およびインターフェイスの設定に使用されます。ステップ 10 ～ 13 は、TACACS+ サーバ機能上での Per VRF の設定に使用されます。

手順の概要

1. **enable**
2. **configure terminal**
3. **ip vrf** *vrf-name*
4. **rd** *route-distinguisher*
5. **exit**
6. **interface** *interface-name*
7. **ip vrf forwarding** *vrf-name*
8. **ip address** *ip-address mask* [**secondary**]
9. **exit**
10. **aaa group server tacacs+** *group-name*
11. **server-private** {*ip-address* | *name*} [**nat**] [**single-connection**] [**port** *port-number*] [**timeout** *seconds*] [**key** [**0** | **7**] *string*]
12. **ip vrf forwarding** *vrf-name*
13. **ip tacacs source-interface** *subinterface-name*
14. **exit**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。

	コマンドまたはアクション	目的
ステップ 2	**configure terminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ip vrf** *vrf-name* 例： `Router (config)# ip vrf cisco`	VRFテーブルを設定し、VRF コンフィギュレーション モードを開始します。
ステップ 4	**rd** *route-distinguisher* 例： `Router (config-vrf)# rd 100:1`	VRFインスタンスに対するルーティングおよびフォワーディング テーブルを作成します。
ステップ 5	**exit** 例： `Router (config-vrf)# exit`	VRFコンフィギュレーションモードを終了します。
ステップ 6	**interface** *interface-name* 例： `Router (config)# interface Loopback0`	インターフェイスを設定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 7	**ip vrf forwarding** *vrf-name* 例： `Router (config-if)# ip vrf forwarding cisco`	インターフェイスに VRF を設定します。
ステップ 8	**ip address** *ip-address mask* [**secondary**] 例： `Router (config-if)# ip address 10.0.0.2 255.0.0.0`	インターフェイスに対するプライマリ IP アドレスまたはセカンダリ IP アドレスを設定します。
ステップ 9	**exit** 例： `Router (config-if)# exit`	インターフェイス コンフィギュレーション モードを終了します。
ステップ 10	**aaa group server tacacs+** *group-name* 例： `Router (config)# aaa group server tacacs+ tacacs1`	異なる TACACS+ サーバ ホストを別々のリストと方式にグループ化し、server-group コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 11	**server-private** {*ip-address* | *name*} [**nat**] [**single-connection**] [**port** *port-number*] [**timeout** *seconds*] [**key** [**0** | **7**] *string*] 例： `Router (config-sg-tacacs+)# server-private 10.1.1.1 port 19 key cisco`	グループ サーバに対するプライベート TACACS+ サーバの IP アドレスを設定します。
ステップ 12	**ip vrf forwarding** *vrf-name* 例： `Router (config-sg-tacacs+)# ip vrf forwarding cisco`	AAA TACACS+ サーバ グループの VRF リファレンスを設定します。
ステップ 13	**ip tacacs source-interface** *subinterface-name* 例： `Router (config-sg-tacacs+)# ip tacacs source-interface Loopback0`	すべての発信 TACACS+ パケットに対して、指定されたインターフェイスの IP アドレスを使用します。
ステップ 14	**exit** 例： `Router (config-sg-tacacs)# exit`	server-group コンフィギュレーション モードを終了します。

TACACS サーバーの Per VRF の確認

Per VRF TACACS+ 設定を確認するには、次の手順を実行します。

（注） **debug** コマンドは、任意の順番で使用できます。

注意 デバッグ CLI をイネーブルにすると、ルータのパフォーマンスが低下する可能性があります。多数のセッションに対して **debug** コマンドを使用することはお勧めしません。

手順の概要

1. **enable**
2. **debug tacacs authentication**
3. **debug tacacs authorization**
4. **debug tacacs accounting**
5. **debug tacacs packets**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**debug tacacs authentication** 例： `Router# debug tacacs authentication`	AAA/TACACS+ 認証に関する情報を表示します。
ステップ 3	**debug tacacs authorization** 例： `Router# debug tacacs authorization`	AAA/TACACS+ 認可に関する情報を表示します。
ステップ 4	**debug tacacs accounting** 例： `Router# debug tacacs accounting`	説明可能なイベントが発生したときに、その情報を表示します。
ステップ 5	**debug tacacs packets** 例： `Router# debug tacacs packets`	TACACS+ パケットに関する情報を表示します。

TACACS サーバーの Per VRF の設定例

TACACS サーバーの Per VRF の設定例

次の出力例では、Per VRF AAA サービスにグループ サーバ **tacacs1** が設定されています。

```
aaa group server tacacs+ tacacs1
    server-private 10.1.1.1 port 19 key cisco
    ip vrf forwarding cisco
    ip tacacs source-interface Loopback0
  ip vrf cisco
   rd 100:1
  interface Loopback0
   ip address 10.0.0.2 255.0.0.0
   ip vrf forwarding cisco
```

その他の参考資料

次のセクションでは、TACACS+ サーバーの Per VRF に関連する参考資料を示します。

関連資料

関連項目	マニュアル タイトル
TACACS+ の設定	「Configuring TACACS+」モジュール。
Per VRF AAA	「Per VRF AAA」モジュール。
セキュリティ コマンド	『*Cisco IOS Security Command Reference*』

標準

標準	タイトル
この機能でサポートされる新規の標準または変更された標準はありません。また、既存の標準のサポートは変更されていません。	--

MIB

MIB	MIB のリンク
この機能によってサポートされる新しい MIB または変更された MIB はありません。またこの機能による既存MIBのサポートに変更はありません。	選択したプラットフォーム、Cisco IOS リリース、およびフィーチャ セットに関する MIB を探してダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

RFC

RFC	タイトル
この機能によりサポートされた新規 RFC または改訂 RFC はありません。またこの機能による既存 RFC のサポートに変更はありません。	--

シスコのテクニカル サポート

説明	リンク
シスコのサポート Web サイトでは、シスコの製品やテクノロジーに関するトラブルシューティングにお役立ていただけるように、マニュアルやツールをはじめとする豊富なオンライン リソースを提供しています。 お使いの製品のセキュリティ情報や技術情報を入手するために、Cisco Notification Service（Field Notice からアクセス）、Cisco Technical Services Newsletter、Really Simple Syndication（RSS）フィードなどの各種サービスに加入できます。 シスコのサポート Web サイトのツールにアクセスする際は、Cisco.com のユーザ ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

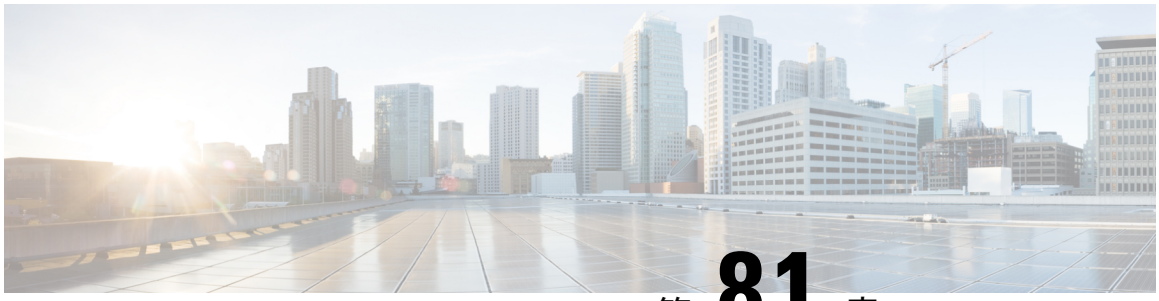
TACACS サーバーの Per VRF の機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *114 : Per VRF for TACACS+ Servers* の機能情報

機能名	リリース	機能情報
Per VRF for TACACS+ Servers	Cisco IOS XE Release 2.2	TACACS+ サーバーの Per VRF 機能により、TACACS+ サーバーで Per Virtual ルーティングおよび転送（Per VRF）の認証、認可、アカウンティング（AAA）を設定できます。 Cisco IOS XE リリース 2.2 では、Cisco ASR 1000 シリーズ アグリゲーション サービス ルータにこの機能が実装されました。 次のコマンドが導入または変更されました：**ip tacacs source-interface**、**ip vrf forwarding (server-group)**、**server-private (TACACS+)**。



第 81 章

TACACS の属性値ペア

Terminal Access Controller Access Control System Plus（TACACS+）の属性値（AV）ペアは、TACACS+ デーモンに保存されるユーザー プロファイルで特定の認証、認可、およびアカウンティング要素を定義するために使用されます。この章では、現在サポートされている TACACS+ AV ペアの一覧を示します。

TACACS の属性値ペアに関する情報

TACACS+ 認証および認可の AV ペア

次の表で、サポートされている TACACS+ 認証および認可の AV ペアの一覧と説明を示し、実装されている Cisco IOS リリースを指定しています。

表 *115*：サポートされている *TACACS+* 認証および認可の *AV* ペア

属性	説明	IOS XE 2.1
acl=x	接続アクセス リストを表す ASCII 数。service=shell の場合のみ使用されます。	あり
addr=x	ネットワーク アドレス。service=slip、service=ppp、および protocol=ip で使用されます。SLIP または PPP/IP 経由で接続する際にリモート ホストが使用する IP アドレスを含みます。たとえば、addr=10.2.3.4 となります。	あり

属性	説明	IOS XE 2.1
addr-pool=x	リモート ホスト アドレスの取得元とするローカル プールの名前を指定します。service=ppp および protocol=ip と使用されます。 **addr-pool** はローカル プーリングと連動して動作することに注意してください。ローカルプールの名前を指定します。これはネットワーク アクセス サーバで事前設定する必要があります。**ip-local pool** コマンドを使用して、ローカル プールを宣言します。次に例を示します。 ip address-pool local ip local pool boo 10.0.0.1 10.0.0.10 ip local pool moo 10.0.0.1 10.0.0.20 その後、TACACS+ を使用して addr-pool=boo または addr-pool=moo を返し、このリモート ノードのアドレスの取得元にするアドレス プールを指示することができます。	あり
autocmd=x	EXEC 起動時に実行する autocommand を指定します（たとえば autocmd=telnet example.com）。service=shell の場合のみ使用されます。	あり
callback- dialstring	コールバックの電話番号（例：callback-dialstring= 408-555-1212）を設定します。値はヌルまたはダイヤルストリングです。ヌル値は、サービスで他の手段を通じてダイヤルストリングを取得することもできることを示します。service=arap、service=slip、service=ppp、service=shell で使用されます。ISDN では無効です。	あり
callback-line	コールバックで使用する TTY 回線の数（例：callback-line=4 ）です。service=arap、service=slip、service=ppp、service=shell で使用されます。ISDN では無効です。	あり
callback-rotary	コールバックで使用するロータリー グループの数（0 ～ 100 の範囲）です（例：callback-rotary=34）。service=arap、service=slip、service=ppp、service=shell で使用されます。ISDN では無効です。	あり
cmd-arg=x	シェル（EXEC）コマンドに渡す引数です。実行されるシェル コマンドの引数を示します。cmd-arg 属性を複数指定でき、順序依存です。 （注） この TACACS+ AV ペアは、RADIUS 属性 26 で使用できません。	あり

属性	説明	IOS XE 2.1
cmd=x	シェル（EXEC）コマンドです。実行するシェル コマンドのコマンド名を示します。この属性は、サービスが「シェル」と等しい場合に指定する必要があります。ヌル値は、シェル自身が参照されることを示します。 （注） この TACACS+ AV ペアは、RADIUS 属性 26 で使用できません。	あり
data-service	service=outbound および protocol=ip で使用されます。	あり
dial-number	ダイヤルする番号を定義します。service=outbound および protocol=ip で使用されます。	あり
dns-servers=	Microsoft PPP クライアントにより、IPCP ネゴシエーション中にネットワーク アクセス サーバから要求される可能性がある DNS サーバ（プライマリまたはセカンダリ）を識別します。service=ppp および protocol=ip で使用されます。DNS サーバを特定する IP アドレスはドット付き 10 進表記で入力します。	あり
force-56	チャネルの 64 K すべてが使用可能に見える場合でも、ネットワーク アクセス サーバが 56 K の部分のみを使用するかどうかを指定します。この属性をオンにするには、「true」値（force-56=true）を使用します。他の値は、false として扱われます。service=outbound および protocol=ip で使用されます。	あり
gw-password	L2TP トンネル認証時のホーム ゲートウェイのパスワードを指定します。service=ppp および protocol=vpdn で使用されます。	あり
idletime=x	値を分単位で設定します。その時間が経過すると、アイドル セッションが終了します。ゼロ値はタイムアウトなしを示します。	あり
inacl#<n>	現在の接続期間に使用されるインターフェイスにインストールされ適用される、入力アクセス リストの ASCII アクセス リスト識別名です。service=ppp および protocol=ip、service service=ppp および protocol =ipx で使用されます。ユーザ単位のアクセス リストは、現在 ISDN インターフェイスでは使用できません。	あり
inacl=x	インターフェイス 入力アクセス リストの ASCII 識別名です。service=ppp および protocol=ip で使用されます。ユーザ単位のアクセス リストは、現在 ISDN インターフェイスでは使用できません。	あり

属性	説明	IOS XE 2.1
interface-config#<n>	仮想プロファイルを使用してユーザ固有の AAA インターフェイス設定情報を指定します。等号（=）が付いている情報は、すべての Cisco IOS インターフェイス コンフィギュレーション コマンドとして使用できます。この属性は複数インスタンスが許可されますが、各インスタンスは固有の番号を持つ必要があります。service=ppp および protocol=lcp で使用されます。 （注） 「interface-config=」属性はこの属性に置き換えられます。	あり
ip-addresses	トンネルのエンドポイントで使用できるIPアドレスの、スペースで区切ったリストです。service=ppp および protocol=vpdn で使用されます。	あり
l2tp-busy-disconnect	LNS の vpdn-group で、事前にコピーするよう設定された仮想テンプレートを使用している場合、この属性は、接続先の事前にコピーされたインターフェイスが検索されない、新しい L2TP セッションのディスポジションを制御します。属性が true（デフォルト）の場合、セッションがLNSにより切断されます。そうでない場合は、新しいインターフェイスが仮想テンプレートからコピーされます。service=ppp および protocol=vpdn で使用されます。	あり
l2tp-cm-local-window-size	L2TP 制御メッセージの最大受信ウィンドウ サイズを指定します。この値は、トンネルの確立中にピアにアドバタイズされます。service=ppp および protocol=vpdn で使用されます。	あり
l2tp-drop-out-of-order	正しくない順序で受信したデータ パケットをドロップして、シーケンス番号を順守します。これは受信した場合の処理方法であって、データパケット上でシーケンス番号が送信されるわけではありません。service=ppp および protocol=vpdn で使用されます。	あり
l2tp-hello- interval	hello キープアライブ インターバルの秒数を指定します。ここで指定した秒数、トンネルでデータが送信されないと、hello パケットが送信されます。service=ppp および protocol=vpdn で使用されます。	あり
l2tp-hidden-avp	イネーブルにすると、L2TP制御メッセージで、大文字小文字を区別するAVPにスクランブルがかけられるか、または非表示になります。service=ppp および protocol=vpdn で使用されます。	あり
l2tp-nosession-timeout	タイムアウトおよびシャットダウンまでに、セッションなしでトンネルがアクティブのままになる秒数を指定します。service=ppp および protocol=vpdn で使用されます。	あり

属性	説明	IOS XE 2.1
l2tp-tos-reflect	LNS でトンネルに入るパケットに対して、IP ToS フィールドを各ペイロード パケットの IP ヘッダーからトンネル パケットの IP ヘッダーにコピーします。service=ppp および protocol=vpdn で使用されます。	あり
l2tp-tunnel- authen	この属性を設定すると、L2TP トンネル認証が実行されます。service=ppp および protocol=vpdn で使用されます。	あり
l2tp-tunnel-password	L2TP トンネル認証および AVP 隠蔽に使用される共有秘密です。service=ppp および protocol=vpdn で使用されます。	あり
l2tp-udp- checksum	これは認可属性で、L2TP がデータ パケットに対して UDP チェックサムを実行する必要があるかどうかを定義します。有効な値は「yes」と「no」です。デフォルトは「no」です。service=ppp と protocol=vpdn で使用されます。	あり
link- compression=	PPP リンクで「stac」圧縮をオンまたはオフのどちらにするかを定義します。service=ppp で使用されます。 リンク圧縮は、次のように、数値で定義します。 • 0：なし • 1：Stac • 2：Stac-Draft-9 • 3：MS-Stac	あり
load-threshold=<n>	マルチリンク バンドルに対して他のリンクを追加または削除する発信元の負荷のしきい値を設定します。負荷がこの指定した値を超えると、追加リンクが追加されます。負荷が指定の値を下回ると、リンクが削除されます。service=ppp および protocol=multilink で使用されます。<n> の範囲は、1 から 255 です。	あり
map-class	ユーザ プロファイルに、ダイヤルアウトするネットワーク アクセス サーバ上で同じ名前のマップ クラスで設定される情報の参照を許可します。service=outbound および protocol=ip で使用されます。	あり
max-links=<n>	ユーザがマルチリンクで保持できるリンク数を制限します。service=ppp および protocol=multilink で使用されます。<n> の範囲は、1 から 255 です。	あり
min-links	MLP に対するリンクの最小数を設定します。service=ppp と protocol=multilink、protocol=vpdn で使用されます。	あり

属性	説明	IOS XE 2.1
nas-password	L2TP トンネル認証時のネットワーク アクセス サーバーのパスワードを指定します。service=ppp および protocol=vpdn で使用されます。	あり
nocallback-verify	コールバック検証が必要かを指定します。このパラメータで有効な値は 1 のみです（例：nocallback-verify=1）。service=arap、service=slip、service=ppp、service=shell で使用されます。コールバックに認証がありません。ISDN では無効です。	あり
noescape=x	ユーザがエスケープ文字を使用できないようにします。service=shell で使用されます。true または false のどちらかです（例：noescape=true）。	あり
nohangup=x	service=shell で使用されます。nohangup オプションを指定します。このオプションで EXEC シェルの終了後、ユーザに他のログイン（ユーザ名）プロンプトを表示します。true または false のどちらかです（例：nohangup=false）。	あり
old-prompts	プロバイダーが以前のシステム（TACACS および拡張 TACACS）と同じプロンプトを TACACS+ で表示できます。これにより、管理者は、TACACS または拡張 TACACS から TACACS+ に、ユーザが気づくことなくアップグレードできます。	あり
outacl#<n>	現在の状態である限りインターフェイスにインストールされ、適用されるインターフェイス出力アクセス リストの ASCII アクセス リスト識別情報です。service=ppp および protocol=ip、service service=ppp および protocol=ipx で使用されます。ユーザ単位のアクセス リストは、現在 ISDN インターフェイスでは使用できません。	あり
outacl=x	インターフェイス 出力アクセス リストの ASCII 識別名です。service=ppp および protocol=ip、service service=ppp および protocol=ipx で使用されます。SLIP または PPP/IP の IP 出力アクセス リストが含まれます（outacl=4 など）。このアクセス リスト自身はルータで事前設定する必要があります。ユーザ単位のアクセス リストは、現在 ISDN インターフェイスでは使用できません。	あり
pool-def#<n>	ネットワーク アクセス サーバで IP アドレス プールを定義します。service=ppp および protocol=ip で使用されます。	あり

属性	説明	IOS XE 2.1
pool-timeout=	pool-def とともに、ネットワーク アクセス サーバ上の IP アドレス プールを定義します。IPCP アドレス ネゴシエーション中、IP プール名がユーザに指定されている場合（addr-pool 属性を参照）、指定された名前のプールがネットワーク アクセス サーバで定義されているかチェックされます。その場合、プールに IP アドレスがあるか参照します。service=ppp および protocol=ip で使用されます。	あり
port-type	ユーザを認証するためにネットワーク アクセス サーバで使用されている物理ポートのタイプを示します。 物理ポートは、次のように数値で示されます。 • 0：非同期 • 1：同期 • 2：ISDN 同期 • 3：ISDN 非同期（V.120） • 4：ISDN-非同期（V.110） • 5：仮想 service=any および protocol=aaa で使用されます。	あり
ppp-vj-slot-compression	VJ 圧縮パケットを PPP リンク経由で送信する際に、Cisco ルータでスロット圧縮しないように指示します。	あり
priv-lvl=x	EXEC に割り当てられる権限レベルです。service=shell で使用されます。権限レベルの範囲は 0 ～ 15 で、15 が最高です。	あり
protocol=x	サービスのサブセットのプロトコルです。たとえば、任意の PPP NCP などです。現在知られている値は、**lcp**、**ip**、**ipx**、**atalk**、**vines**、**lat**、**xremote**、**tn3270**、**telnet**、**rlogin**、**pad**、**vpdn**、**osicp**、**deccp**、**ccp**、**cdp**、**bridging**、**xns**、**nbf**、**bap**、**multilink**、および **unknown** です。	あり
proxyacl#<n>	ダウンロード可能なユーザ プロファイル（ダイナミック ACL）を、認証プロキシを使用して設定でき、これにより設定されたインターフェイスのトラフィックの通過を許可するよう、認証を設定できます。service=shell および protocol=exec で使用されます。	あり

属性	説明	IOS XE 2.1
route	インターフェイスに適用されるルートを指定します。service=slip、service=ppp、および protocol=ip で使用されます。 ネットワークの許可中、route 属性はユーザ単位のスタティックルートの指定に使用でき、TACACS+ により次のようにインストールされます。 route=" *dst_address mask* [*gateway*]" これは、一時的に適用されるスタティック ルートを示します。*dst_address*、*mask*、および *gateway* は通常のドット付き 10 進表記での記述を想定されていて、よく使用されるネットワーク アクセス サーバーの **ip route** コンフィギュレーション コマンドと同じ意味を持ちます。 *gateway* を省略すると、ピアのアドレスがゲートウェイになります。ルートは接続が終了すると消去されます。	あり
route#<n>	ルート AV ペアと同様にインターフェイスに適用されるルートを指定しますが、このルートは番号が付けられて複数のルートを適用できます。service=ppp と protocol=ip、および service=ppp と protocol =ipx で使用されます。	あり
routing=x	ルーティング情報をインターフェイスに伝播し、このインターフェイスから受け入れるかどうかを指定します。service=slip、service=ppp、および protocol=ip で使用されます。機能上、SLIP および PPP コマンドの /routing フラグと同等です。true または false のいずれか（例：routing=true）です。	あり
rte-fltr-in#<n>	現在の接続中に、現在のインターフェイスのルーティングアップデートにインストールし、適用する入力アクセスリストの定義を指定します。service=ppp と protocol=ip、および service=ppp と protocol =ipx で使用されます。	あり
rte-fltr-out#<n>	現在の接続中に、現在のインターフェイスのルーティングアップデートにインストールし、適用する出力アクセスリストの定義を指定します。service=ppp と protocol=ip、および service=ppp と protocol =ipx で使用されます。	あり
sap#<n>	接続中にインストールされるスタティック サービス アドバタイジング プロトコル（SAP）エントリを指定します。service=ppp および protocol=ipx で使用されます。	あり
sap-fltr-in#<n>	現在の接続中に、現在のインターフェイスにインストールし、適用する入力 SAP フィルタ アクセス リストの定義を指定します。service=ppp および protocol=ipx で使用されます。	あり

属性	説明	IOS XE 2.1
sap-fltr-out#<n>	現在の接続中に、現在のインターフェイスにインストールし、適用する出力 SAP フィルタ アクセス リストの定義を指定します。service=ppp および protocol=ipx で使用されます。	あり
send-auth	CLID 認証に続く、username-password 認証で使用するプロトコル（PAP または CHAP）を定義します。service=any および protocol=aaa で使用されます。	あり
send-secret	NAS が発信コールの接続のリモート エンドからの chap/pap 要求に応答する際に必要なパスワードを指定します。service=ppp および protocol=ip で使用されます。	あり
service=x	プライマリ サービスです。このサービスの認証またはアカウンティングを要求していることを示すサービス属性を指定します。現在の値は、**slip**、**ppp**、**arap**、**shell**、**tty-daemon**、**connection**、および **system** です。この属性は常に含める必要があります。	あり
source-ip=x	VPDN トンネルの一部として生成されたすべての VPDN パケットの発信元 IP アドレスとして使用されます。これは、Cisco **vpdn outgoing** グローバル コンフィギュレーション コマンドと同じ意義を持ちます。	あり
spi	登録中にホーム エージェントがモバイル ノードの認証で必要とする認証情報を伝送します。この情報は、**ip mobile secure host <addr>** コンフィギュレーション コマンドと同じ構文です。基本的に、この文字列に続く残りのコンフィギュレーション コマンドはそのまま含まれます。これにはセキュリティ パラメータ インデックス（SPI）、キー、認証アルゴリズム、認証モード、およびリプレイ保護タイムスタンプ範囲が含まれています。service=mobileip および protocol=ip で使用されます。	あり
timeout=x	EXEC または ARA セッションを切断するまでの分数です（例：timeout=60）。ゼロ値はタイムアウトなしを示します。service=arap で使用されます。	あり
tunnel-id	個々のユーザ MID が生成されるトンネルの認証に使用するユーザ名を指定します。これは、**vpdn outgoing** コマンドの *remote name* と同様です。service=ppp および protocol=vpdn で使用されます。	あり
wins-servers=	IPCP ネゴシエーション中に、ネットワーク アクセス サーバから Microsoft PPP クライアントにより要求される可能性がある Windows NT サーバを特定します。service=ppp および protocol=ip で使用されます。各 Windows NT サーバを特定する IP アドレスはドット付き 10 進表記で入力します。	あり

属性	説明	IOS XE 2.1
zonelist=x	数字の zonelist の値です。service=arap で使用されます。ARA 向けの AppleTalk zonelist です（例：zonelist=5）。	あり

TACACS+ の設定の詳細については、「TACACS+ の設定」の章を参照してください。TACACS+ の認証および認可の設定について詳しくは、「認証の設定」および「認可の設定」の章を参照してください。

TACACS アカウンティング AV ペア

次の表で、サポートされている TACACS+ アカウンティングの AV ペアの一覧と説明を示し、実装されている Cisco IOS XE リリースを指定しています。

表 *116*：サポートされる *TACACS+* アカウンティング *AV* ペア

属性	説明	IOS XE 2.1
Abort-Cause	ファクス セッションが中断した場合、中断の信号を送信したシステム コンポーネントを示します。中断する可能性のあるシステム コンポーネントには、FAP（Fax Application Process）、TIFF（TIFF リーダーまたは TIFF ライター）、fax-mail クライアント、fax-mail サーバー、ESMTP クライアント、ESMTP サーバーなどがあります。	あり
bytes_in	この接続中に転送される入力バイト数です。	あり
bytes_out	この接続中に転送される出力バイト数です。	あり
Call-Type	ファクスのアクティビティのタイプを、fax receive または fax send のどちらかで記述します。	あり
cmd	ユーザが実行したコマンドです。	あり
data-rate	この AV ペアは名前が変更されました。nas-rx-speed を参照してください。	
disc-cause	接続がオフラインになった理由を特定します。Disconnect-Cause 属性は、アカウンティング終了記録で送信されます。また、この属性で、認証が実行される前に接続が切断された場合、最初に開始レコードを生成せずに終了レコードが生成されます。Disconnect-Cause 値とその意味の一覧については、次の表（接続解除原因の拡張）を参照してください。	あり
disc-cause-ext	disc-cause 属性が、接続がオフラインになったベンダー固有の理由をサポートするよう拡張します。	あり

属性	説明	IOS XE 2.1
elapsed_time	処理の経過時間（秒）です。デバイスが実時間を保持していない場合に有用です。	あり
Email-Server-Address	オンランプ fax-mail メッセージを処理する E メール サーバの IP アドレスを示します。	あり
Email-Server-Ack-Flag	オンランプ ゲートウェイが fax-mail メッセージを受け入れる E メール サーバから肯定確認応答を受信したことを示します。	あり
event	ルータの状態変化を記述した、アカウンティング パケットに含める情報です。記述されたイベントは、アカウンティング開始およびアカウンティング終了です。	あり
Fax-Account-Id-Origin	**mmoip aaa receive-id** コマンドまたは **mmoip aaa send-id** コマンドについて、アカウント ID の発信元がシステム管理者によって定義されたものとして示します。	あり
Fax-Auth-Status	このファクス セッションに対する認証が成功したかどうかを示します。このフィールドに対する有効値は、success、failed、bypassed、または unknown です。	あり
Fax-Connect-Speed	この fax-mail が最初に送信または受信された時点のモデム速度を示します。有効値は、1200、4800、9600、および 14400 です。	あり
Fax-Coverpage-Flag	カバー ページがこのファクス セッションのオフランプ ゲートウェイで生成されたかどうかを示します。true はカバー ページが生成されたことを示します。false はカバー ページが生成されなかったことを意味します。	あり
Fax-Dsn-Address	DSN の送信先のアドレスを示します。	あり
Fax-Dsn-Flag	DSN がイネーブルにされているかどうかを示します。true は DSN がイネーブルにされていることを示します。false は DSN がイネーブルにされていないことを示します。	あり
Fax-Mdn-Address	MDN の送信先のアドレスを示します。	あり
Fax-Mdn-Flag	メッセージ配信通知（MDN）がイネーブルにされているかどうかを示します。true は MDN がイネーブルにされていることを示します。false は MDN がイネーブルにされていないことを示します。	あり

属性	説明	IOS XE 2.1
Fax-Modem-Time	モデムがファクスデータを送信した時間（x）、およびファクス セッションの合計時間（y）を秒単位で示します。これには、fax-mail および PSTN 時間が x/y の形式で含まれます。たとえば、10/15 は送信時間が 10 秒で、合計ファクス セッションが 15 秒であったことを示します。	あり
Fax-Msg-Id=	Store and Forward Fax 機能によって割り当てられた一意のファクス メッセージ識別番号を示します。	あり
Fax-Pages	このファクス セッション中に送信または受信したページ数を示します。このページ数には、カバー ページも含まれます。	あり
Fax-Process-Abort-Flag	ファクス セッションが中断したこと、または正常に終了したことを示します。true はセッションが中断したことを示します。false はセッションが成功したことを示します。	あり
Fax-Recipient-Count	このファクス送信の受信者数を示します。E メール サーバがセッション モードをサポートするまで、この数字は 1 にする必要があります。	あり
Gateway-Id	ファクス セッションを処理したゲートウェイの名前を示します。この名前は、hostname.domain-name の形式で表示されます。	あり
mlp-links-max	アカウンティング レコードが生成された時点で特定のマルチリンク セッションにあるリンク数を示します。	あり
mlp-sess-id	セッションが終了した時のマルチリンク バンドルの ID 番号をレポートします。この属性は、マルチリンク バンドルの一部のセッションに適用されます。この属性は、認証応答パケットで送信されます。	あり
nas-rx-speed	接続のライフタイムでの平均ビット/秒値を指定します。この属性は、アカウンティング終了記録で送信されます。	あり
nas-tx-speed	2 つのモデムによってネゴシエートされた送信速度を報告します。	あり
paks_in	この接続中に転送される入力パケット数です。	あり
paks_out	この接続中に転送される出力パケット数です。	あり
port	ユーザがログインしたポートです。	あり
Port-Used	この fax-mail の送受信いずれかに使用される Cisco AS5300 のスロット/ポート番号を示します。	あり

属性	説明	IOS XE 2.1
pre-bytes-in	認証前の入力バイト数を記録します。この属性は、アカウンティング終了記録で送信されます。	あり
pre-bytes-out	認証前の出力バイト数を記録します。この属性は、アカウンティング終了記録で送信されます。	あり
pre-paks-in	認証前の入力パケット数を記録します。この属性は、アカウンティング終了記録で送信されます。	あり
pre-paks-out	認証前の出力パケット数を記録します。Pre-Output-Packets 属性は、アカウンティング終了記録で送信されます。	あり
pre-session-time	コールが最初に接続された時から認証が完了した時までの時間長を秒で指定します。	あり
priv_level	処理に関連付けられた権限レベルです。	あり
protocol	処理に関連付けられたプロトコルです。	あり
reason	システム変更により発生したイベントを記述した、アカウンティングパケットに含める情報です。記述されるイベントは、システムのリロード、システムのシャットダウン、またはアカウンティングが再設定（オンまたはオフ）された場合です。	あり
service	ユーザが使用するサービスです。	あり
start_time	処理を開始する時刻（エポック（1970 年 1 月 1 日 12:00 a.m.）からの秒数で指定）です。この情報を受信するよう、クロックを設定する必要があります。	あり
stop_time	処理を停止する時刻（エポックからの秒数で指定）です。この情報を受信するよう、クロックを設定する必要があります。	あり
task_id	同じ（一意の）task_id 番号を持つ同じイベントに対する開始レコードと終了レコードです。	あり
timezone	このパケットに含まれるすべてのタイムスタンプの時間帯（省略形）です。	あり
xmit-rate	この AV ペアは名前が変更されました。nas-tx-speed を参照してください。	

次の表で、Disconnect Cause Extended（disc-cause-ext）属性の原因のコードと説明の一覧を示しています。

表 *117 :* 接続解除原因の拡張

原因コード	説明	IOS XE 2.1
1000 – 理由なし	接続解除の理由はありません。	あり
1001 – 接続解除なし	イベントは接続解除されませんでした。	あり
1002 – 不明	接続解除の理由が不明です。このコードは、リモート接続が停止している場合に表示されることがあります。	あり
1003 – コール接続解除	コールが接続解除されました。	あり
1004 – CLID 認証失敗	Calling line ID（CLID）認証が失敗しました。	あり
1009 – モデム使用不可	モデムが使用できません。	あり
1010 – キャリアなし	モデムで、データ キャリア検出（DCD）が検出されませんでした。このコードは、最初のモデム接続で切断が発生した場合に表示されます。	あり
1011 – キャリアのロスト	モデムで DCD は検出されましたが、非アクティブになっています。このコードは、最初のモデム接続で切断が発生した場合に表示されます。	あり
1012 – モデム結果なし	結果コードが解析できません。このコードは、最初のモデム接続で切断が発生した場合に表示されます。	あり
1020 – TS ユーザ退出	ユーザがターミナル サーバから正常に退出しました。このコードは、ターミナル サーバ セッション中のイミディエート Telnet および raw TCP の切断に関連しています。	あり
1021 – アイドル タイムアウト	アイドル タイマーの時間切れのため、ターミナル サーバからユーザが退出しました。このコードは、ターミナル サーバ セッション中のイミディエート Telnet および raw TCP の切断に関連しています。	あり
1022 – TS Telnet 退出	ユーザが、Telnet セッションから正常に退出しました。このコードは、ターミナル サーバ セッション中のイミディエート Telnet および raw TCP の切断に関連しています。	あり

原因コード	説明	IOS XE 2.1
1023 – TS IP アドレスなし	リモートホストがIPアドレスを保持していないか、ダイナミック プールが割り当てられていないため、ユーザはシリアル ライン インターネット プロトコル（SLIP）または PPP にスイッチできませんでした。このコードは、ターミナル サーバ セッション中のイミディエート Telnet および raw TCP の切断に関連しています。	あり
1024 – TS TCP の raw 退出	ユーザが、 raw TCP セッションから正常に退出しました。このコードは、ターミナルサーバセッション中のイミディエート Telnet および raw TCP の切断に関連しています。	あり
1025 – TS パスワード不良	ユーザが 3 回、正しいパスワードの入力に失敗したため、ログイン処理が終了しました。このコードは、ターミナル サーバ セッション中のイミディエート Telnet および raw TCP の切断に関連しています。	あり
1026 – TS raw TCP なし	raw TCP オプションがイネーブルになっていません。このコードは、ターミナル サーバセッション中のイミディエート Telnet および raw TCP の切断に関連しています。	あり
1027 – TS CNTL-C	ユーザが「Ctrl C」と入力したためログイン プロセスが終了しました。このコードは、ターミナル サーバセッション中のイミディエート Telnet および raw TCP の接続解除に関連しています。	あり
1028 – TS セッション終了	ターミナル サーバ セッションが終了しました。このコードは、ターミナルサーバセッション中のイミディエート Telnet および raw TCP の切断に関連しています。	あり
1029 – TS Vconn 終了	ユーザがバーチャル コネクションを終了しました。このコードは、ターミナル サーバ セッション中のイミディエート Telnet および raw TCP の切断に関連しています。	あり
1030 – TS Vconn 終了	バーチャル コネクションが終了しました。このコードは、ターミナル サーバセッション中のイミディエート Telnet および raw TCP の切断に関連しています。	あり
1031 – TS Rlogin 退出	ユーザが Rlogin セッションから正常に退出しました。このコードは、ターミナル サーバセッション中のイミディエート Telnet および raw TCP の切断に関連しています。	あり

原因コード	説明	IOS XE 2.1
1032 – TS Rlogin オプション無効	ユーザが無効な Rlogin オプションを選択しました。このコードは、ターミナル サーバ セッション中のイミディエート Telnet および raw TCP の切断に関連しています。	あり
1033 – TS 不十分なリソース	アクセス サーバにターミナル サーバ セッションを行う十分なリソースがありません。このコードは、ターミナル サーバ セッション中のイミディエート Telnet および raw TCP の切断に関連しています。	あり
1040 – PPP LCP タイムアウト	PPP リンク コントロール プロトコル（LCP）ネゴシエーションがピアからの応答を待機している間にタイム アウトしました。このコードは、PPP 接続と関係しています。	あり
1041 – PPP LCP 失敗	PPP LCP ネゴシエーションで収束に失敗しました。このコードは、PPP 接続と関係しています。	あり
1042 – PPP Pap 失敗	PPP パスワード認証プロトコル（PAP）認証が失敗しました。このコードは、PPP 接続と関係しています。	あり
1043 – PPP CHAP 失敗	PPP チャレンジ ハンドシェーク認証プロトコル（CHAP）認証が失敗しました。このコードは、PPP 接続と関係しています。	あり
1044 – PPP リモート失敗	リモート サーバからの認証が失敗しました。このコードは、PPP セッションと関係しています。	あり
1045 – PPP 終了の受信	ピアが PPP 終了要求を送信しました。このコードは、PPP 接続と関係しています。	あり
PPP LCP 終了（1046）	LCP がオープン状態にある時に、LCP が上位層から終了要求を受信しました。このコードは、PPP 接続と関係しています。	あり
1047 – PPP NCP なし	NCP がオープンでないため、LCP が終了しました。このコードは、PPP 接続と関係しています。	あり
1048 – PPP MP エラー	ユーザに追加するマルチリンク PPP バンドルを特定できなかったため、LCPは終了しました。このコードは、PPP 接続と関係しています。	あり
1049 – PPP 最大チャネル	アクセス サーバが MP セッションにこれ以上チャネルを追加できなかったため、LCP が終了しました。このコードは、PPP 接続と関係しています。	あり

原因コード	説明	IOS XE 2.1
1050 – TS テーブルが満杯	raw TCP または Telnet 内部セッション テーブルが満杯です。このコードは、イミディエート Telnet および raw TCP の切断に関連し、この表の前のほうに記載した Telnet および TCP コードよりも詳細な情報が含まれています。	あり
1051 – TS リソースが満杯	内部リソースが満杯です。このコードは、イミディエート Telnet および raw TCP の切断に関連し、この表の前のほうに記載した Telnet および TCP コードよりも詳細な情報が含まれています。	あり
1052 – TS 無効な IP アドレス	Telnet ホストの IP アドレスが無効です。このコードは、イミディエート Telnet および raw TCP の切断に関連し、この表の前のほうに記載した Telnet および TCP コードよりも詳細な情報が含まれています。	あり
1053 – TS ホスト名不良	アクセス サーバがホスト名を解決できませんでした。このコードは、イミディエート Telnet および raw TCP の切断に関連し、この表の前のほうに記載した Telnet および TCP コードよりも詳細な情報が含まれています。	あり
1054 – TS ポート不良	アクセス サーバが不良または欠落したポート番号を検出しました。このコードは、イミディエート Telnet および raw TCP の切断に関連し、この表の前のほうに記載した Telnet および TCP コードよりも詳細な情報が含まれています。	あり
1060 – TCP リセット	ホストで TCP 接続がリセットされました。TCP スタックが、イミディエート Telnet または raw TCP セッション中に、この切断コードを返す場合があります。	あり
1061 – TCP 接続拒否	ホストで TCP 接続が拒否されました。TCP スタックが、イミディエート Telnet または raw TCP セッション中に、この切断コードを返す場合があります。	あり
1062 – TCP タイムアウト	TCP 接続がタイムアウトしました。TCP スタックが、イミディエート Telnet または raw TCP セッション中に、この切断コードを返す場合があります。	あり
1063 – TCP 外部ホストの終了	外部ホストで TCP 接続が終了しました。TCP スタックが、イミディエート Telnet または raw TCP セッション中に、この切断コードを返す場合があります。	あり

原因コード	説明	IOS XE 2.1
1064 – TCP ネット到達不能	TCP ネットワークが到達不能でした。TCP スタックが、イミディエート Telnet または raw TCP セッション中に、この切断コードを返す場合があります。	あり
1065 – TCP ホスト到達不能	TCP ホストが到達不能でした。TCP スタックが、イミディエート Telnet または raw TCP セッション中に、この切断コードを返す場合があります。	あり
1066 – TCP ネット管理到達不能	TCP ネットワークが管理的に到達不能でした。TCP スタックが、イミディエート Telnet または raw TCP セッション中に、この切断コードを返す場合があります。	あり
1067 – TCP ホスト管理到達不能	TCP ホストが管理的に到達不能でした。TCP スタックが、イミディエート Telnet または raw TCP セッション中に、この切断コードを返す場合があります。	あり
1068 – TCP ポート到達不能	TCP ポートが到達不能でした。TCP スタックが、イミディエート Telnet または raw TCP セッション中に、この切断コードを返す場合があります。	あり
1100 – セッション タイムアウト	PPP リンクでアクティビティがないため、セッションがタイムアウトしました。このコードは、すべてのセッション タイプに適用されます。	あり
1101 – セキュリティ障害	セキュリティ上の理由によりセッションが失敗しました。このコードは、すべてのセッション タイプに適用されます。	あり
1102 – コールバック	コールバックのためセッションが終了しました。このコードは、すべてのセッションタイプに適用されます。	あり
1120 – 非サポート	プロトコルがディセーブルまたは非サポートのため、片側がコールを拒否しました。このコードは、すべてのセッション タイプに適用されます。	あり
1150 – Radius 接続解除	RADIUS サーバが接続解除を要求しました。	あり
1151 – ローカル管理者接続解除	ローカル管理者が接続解除しました。	あり
1152 – SNMP 接続解除	簡易ネットワーク管理プロトコル（SNMP）が接続解除しました。	あり
1160 – V110 リトライ	V110 同期で許可されたリトライ回数を超えました。	あり
1170 – PPP 認証タイムアウト	認証がタイムアウトしました。このコードは、PPPセッションに適用されます。	あり

原因コード	説明	IOS XE 2.1
1180 – ローカル ハングアップ	ローカルがハングアップした結果、コールが接続解除しました。	あり
1185 – リモート ハングアップ	リモート エンドがハングアップしたため、コールが接続解除しました。	あり
1190 – T1 休止	伝送している T1 回線が休止したため、コールが接続解除しました。	あり
1195 – コール期間	コール期間が、アクセス サーバの Max Call Mins または Max DS0 Mins パラメータで許可された時間を越えたため、コールが接続解除しました。	あり
1600 - VPDN ユーザ接続解除	ユーザが接続解除しました。この値は、バーチャル プライベート ダイヤルアップ ネットワーク（VPDN）セッションに適用されます。	あり
1601 - VPDN 搬送波消失	搬送波消失が発生しました。このコードは、VPDN セッションに適用されます。	あり
1602 – VPDN リソースなし	リソースがありません。このコードは、VPDN セッションに適用されます。	あり
1603 – VPDN 制御パケット不良	制御パケットが無効です。このコードは、VPDN セッションに適用されます。	あり
1604 – VPDN 管理者接続解除	管理者が接続解除しました。このコードは、VPDN セッションに適用されます。	あり
1605 – VPDN トンネルダウン/確立失敗	トンネルがダウンしているか、確立に失敗しました。このコードは、VPDN セッションに適用されます。	あり
1606 – VPDN ローカル PPP 接続解除	ローカル PPP が接続解除しました。このコードは、VPDN セッションに適用されます。	あり
1607 – VPDN ソフト停止/セッション制限	VPN トンネルで新しいセッションを確立できませんでした。このコードは、VPDN セッションに適用されます。	あり
1608 – VPDN コール リダイレクト	コールがリダイレクトされました。このコードは、VPDN セッションに適用されます。	あり
1801 – Q850 未割り当て番号	番号が割り当てられていません。このコードは、ISDN または ISDN 経由のモデム コールに適用されます。	いいえ（No）

原因コード	説明	IOS XE 2.1
1802 – Q850 ルートなし	このコードを送信している機器が、認識されていない特定の中継ネットワークを使用したコールのルート要求を受信しました。このコードを送信している機器は、その中継ネットワークが存在しないか、その特定の中継ネットワークが存在していても、このコードを送信している機器で機能していないため、中継ネットワークを認識していません。このコードは、ISDN または ISDN 経由のモデム コールに適用されます。	いいえ（No）
1803 – Q850 宛先へのルートなし	コールが選択した経路で通過するネットワークが、目的の宛先で機能していないため、着信側に到達できません。このコードは、ISDN または ISDN 経由のモデム コールに適用されます。	いいえ（No）
1806 – Q850 チャネル受け入れ不能	直近で識別されたチャネルがこのコールで使用する送信エンティティに受け入れられません。このコードは、ISDN または ISDN 経由のモデム コールに適用されます。	いいえ（No）
1816 – Q850 正常な消去	このコールに関係するユーザの誰かが、コールを消去するよう要求したためコールが消去されました。このコードは、ISDN または ISDN 経由のモデム コールに適用されます。	いいえ（No）
1817 – Q850 ユーザ ビジー	ユーザビジー状態になっているため、着信側が他のコールを受けられません。このコードは、着信側のユーザまたはネットワークで生成されることがあります。ユーザにより生成された場合、ユーザの機器がこのコールに対応できます。このコードは、ISDN または ISDN 経由のモデム コールに適用されます。	いいえ（No）
1818 – Q850 ユーザ応答なし	割り当てられた所定の時間内に、着信側が、コール確立メッセージに対してアラートまたは接続表示によって応答しないときに使用されます。このコードは、ISDN または ISDN 経由のモデム コールに適用されます。	いいえ（No）
1819 – Q850 ユーザ応答なし	着信側にアラートが送信されましたが、所定の時間内に接続表示による応答がありません。このコードは、ISDN または ISDN 経由のモデム コールに適用されます。	いいえ（No）

原因コード	説明	IOS XE 2.1
1821 – Q850 コール却下	このコードを送信している機器は、ビジーまたは非対応ではないためこのコールを受けられますが、このコールを受けたくありません。このコードはネットワークにより生成されることもあり、この場合、このコールが補足サービスの制約により消去されたことを示します。診断フィールドには、補足サービスの追加情報や却下の理由が含まれている場合があります。このコードは、ISDN または ISDN 経由のモデム コールに適用されます。	いいえ（No）
1822 – Q850 番号の変更	着信側を示す番号が割り当てられていません。新しい着番号が、任意で診断フィールドに含まれている場合があります。このコードは、ISDN または ISDN 経由のモデム コールに適用されます。	いいえ（No）
1827 – Q850 宛先故障	宛先へのインターフェイスが正常に機能していないため、ユーザが指示した宛先に到達できません。「正常に機能していない」とは、シグナリング メッセージをリモート側に配信できなかったことを意味しています。このコードは、ISDN または ISDN 経由のモデム コールに適用されます。	いいえ（No）
1828 – Q850 無効な番号形式	着番号が有効な形式でないか、完全でないため、着信側に到達できません。このコードは、ISDN または ISDN 経由のモデム コールに適用されます。	いいえ（No）
1829 – Q850 ファシリティ拒否	このコードは、ユーザが要求した補足サービスがネットワークで提供されていない場合に返されます。このコードは、ISDN または ISDN 経由のモデム コールに適用されます。	いいえ（No）
1830 – Q850 状態問い合わせへの応答	このコードは、STATUS ENQUIRY メッセージよりも先に受領したために STATUS メッセージが生成された場合に、STATUS メッセージに含まれています。このコードは、ISDN または ISDN 経由のモデム コールに適用されます。	いいえ（No）
1831 – Q850 未指定の原因	他のコードが適用されない場合に適用されます。このコードは、ISDN または ISDN 経由のモデム コールに適用されます。	いいえ（No）
1834 – Q850 使用可能な回線なし	コールを処理できる回線またはチャネルがありません。このコードは、ISDN または ISDN 経由のモデム コールに適用されます。	いいえ（No）

原因コード	説明	IOS XE 2.1
1838 – Q850 ネットワーク障害	ネットワークが正常に機能しておらず、この状態が比較的長期間続く見込みです。このコードは、ISDN または ISDN 経由のモデム コールに適用されます。	いいえ（No）
1841 – Q850 一時障害	ネットワークが正常に機能していませんが、この状態は長期間続かない見込みです。このコードは、ISDN または ISDN 経由のモデム コールに適用されます。	いいえ（No）
1842 – Q850 ネットワーク輻輳	ネットワークが輻輳しています。このコードは、ISDN または ISDN 経由のモデム コールに適用されます。	いいえ（No）
1843 – Q850 アクセス情報破棄	このコードは、ネットワークがアクセス情報をリモート ユーザの要求に従って配信できなかったことを示します。このコードは、ISDN または ISDN 経由のモデム コールに適用されます。	いいえ（No）
1844 – Q850 要求チャネルが使用不可能	このコードは、要求エンティティにより指定された回線またはチャネルが、インターフェイスの片側から提供できなかった場合に返されます。このコードは、ISDN または ISDN 経由のモデム コールに適用されます。	いいえ（No）
1845 – Q850 コール プリエンプション	コールがプリエンプションされました。このコードは、ISDN または ISDN 経由のモデム コールに適用されます。	いいえ（No）
1847 – Q850 リソースが使用不可能	このコードは、リソース使用不可クラスの他のコードが適用されない場合にのみ、リソース使用不可イベントをレポートするために使用されます。このコードは、ISDN または ISDN 経由のモデム コールに適用されます。	いいえ（No）
1850 – Q850 未登録ファシリティ	登録されているファシリティではありません。このコードは、ISDN または ISDN 経由のモデム コールに適用されます。	いいえ（No）
1852 – Q850 発信コール除外	発信側が、発信非公開ユーザ グループ コールで非公開ユーザ グループのメンバーであっても、このメンバーに対して発信コールが許可されていません。このコードは、ISDN または ISDN 経由のモデム コールに適用されます。	いいえ（No）
Q850 着信コール除外（1854）	着信側が、着信非公開ユーザ グループ コールで非公開ユーザ グループのメンバーであっても、このメンバーに対して着信コールが許可されていません。このコードは、ISDN または ISDN 経由のモデム コールに適用されます。	いいえ（No）

原因コード	説明	IOS XE 2.1
1858 – Q850 ベアラー機能が使用不可	ユーザが、このコードを生成した機器に実装されているベアラー機能を要求しましたが、その時点で使用できませんでした。このコードは、ISDN または ISDN 経由のモデム コールに適用されます。	いいえ（No）
1863 – Q850 サービス使用不可	このコードは、サービスまたはオプション使用不可クラスの他のコードが適用されない場合にのみ、サービスまたはオプション使用不可イベントのレポートに使用されます。このコードは、ISDN または ISDN 経由のモデム コールに適用されます。	いいえ（No）
1865 – Q850 ベアラー機能未実装	このコードを送信した機器は、要求されたベアラ機能をサポートしていません。このコードは、ISDN または ISDN 経由のモデム コールに適用されます。	いいえ（No）
1866 – Q850 チャネル未実装	このコードを送信した機器は、要求されたチャネル タイプをサポートしていません。このコードは、ISDN または ISDN 経由のモデム コールに適用されます。	いいえ（No）
1869 – Q850 ファシリティ未実装	ユーザが要求した補足サービスがネットワークで提供できません。このコードは、ISDN または ISDN 経由のモデム コールに適用されます。	いいえ（No）
1881 – Q850 無効コール参照値	このコードを送信した機器は、ユーザネットワーク インターフェイスで現在使用されていないコール参照値が含まれたメッセージを受信しました。このコードは、ISDN または ISDN 経由のモデム コールに適用されます。	いいえ（No）
1882 – Q850 チャネルが存在しない	直近で識別されたチャネルがこのコールで使用する送信エンティティに受け入れられません。このコードは、ISDN または ISDN 経由のモデム コールに適用されます。このコードは、ISDN または ISDN 経由のモデム コールに適用されます。	いいえ（No）
1888 – Q850 互換性がない宛先	このコードを送信中の機器が、対応できない下位レイヤの互換性または他の互換性属性を持つコールを確立するよう要求されました。このコードは、ISDN または ISDN 経由のモデム コールに適用されます。	いいえ（No）
1896 – Q850 必須情報要素が喪失	このコードを送信中の機器が、メッセージが処理される前にメッセージに存在しなければならない情報要素が失われているメッセージを受信しました。このコードは、ISDN または ISDN 経由のモデム コールに適用されます。	いいえ（No）

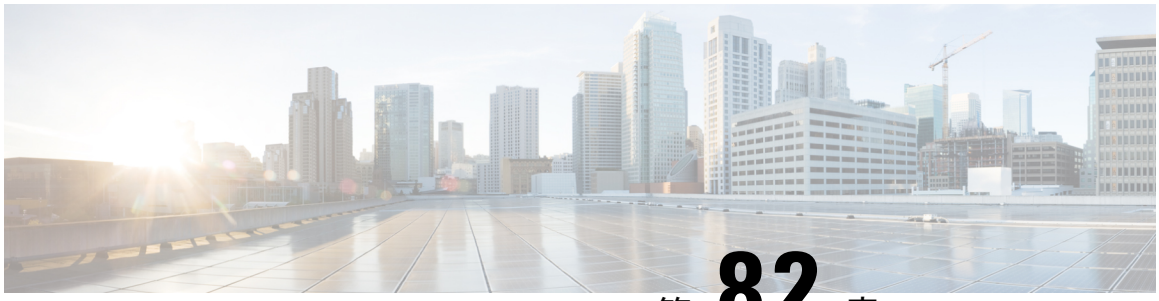
原因コード	説明	IOS XE 2.1
1897 – Q850 存在しないメッセージ タイプ	このコードを送信中の機器が、定義されていないメッセージであるか、定義されてはいるがこのコードを送信した機器で実装されていないため認識されないメッセージ タイプのメッセージを受信しました。このコードは、ISDN または ISDN 経由のモデム コールに適用されます。	いいえ（No）
1898 – Q850 無効なメッセージ	このコードは、無効なメッセージ クラスの他のコードが適用されない場合に無効なメッセージをレポートするために使用されます。このコードは、ISDN または ISDN 経由のモデム コールに適用されます。	いいえ（No）
1899 – Q850 情報要素不良	情報要素が認識されません。このコードは、ISDN または ISDN 経由のモデム コールに適用されます。	いいえ（No）
1900 – Q850 無効要素が含まれる	このコードを送信中の機器が、未実装の情報要素を受信しました。ただし、この情報要素の 1 つまたは複数のフィールドがこのコードを送信した機器で実装されていない方法で符号化されています。このコードは、ISDN または ISDN 経由のモデム コールに適用されます。	いいえ（No）
1901 – Q850 誤った状態のメッセージ	受信したメッセージは、コール ステートと互換性がありません。このコードは、ISDN または ISDN 経由のモデム コールに適用されます。	いいえ（No）
1902 – Q850 タイマーの期限切れからの回復	エラー処理手順に関連付けられたタイマーの期限切れによって、手順が初期化されました。このコードは、ISDN または ISDN 経由のモデム コールに適用されます。	いいえ（No）
1903 – Q850 情報要素エラー	このコードを送信中の機器が、情報要素識別名またはパラメータ名が定義されていないか、定義されてはいるがこのコードを送信した機器で実装されていないため、認識されない情報要素またはパラメータが含まれるメッセージを受信しました。このコードは、ISDN または ISDN 経由のモデム コールに適用されます。	いいえ（No）
1911 – Q850 プロトコル エラー	このコードは、プロトコル エラー クラスの他のコードが適用されない場合にのみ、プロトコル エラー イベントをレポートするために使用されます。このコードは、ISDN または ISDN 経由のモデム コールに適用されます。	いいえ（No）

原因コード	説明	IOS XE 2.1
1927 – Q850 未指定のインターネットワーキング イベント	行った処理に対してコードを提供しないネットワークでインターワーキングした場合にエラーになります。このコードは、ISDN またはISDN 経由のモデム コールに適用されます。	いいえ（No）

TACACS+ アカウンティングの設定の詳細については、「TACACS+ 機能の設定」モジュールを参照してください。

第 VII 部

Cisco TrustSec



第 82 章

Cisco TrustSec の概要

Cisco TrustSec は、論理グループ権限を示すためにタグを使用します。このタグは、セキュリティグループタグ（SGT）と呼ばれ、アクセスポリシーで使用されます。SGT は、シスコのスイッチ、ルータ、およびファイアウォールでトラフィックを適用するために使用されます。Cisco TrustSec は、分類、伝達、および適用の 3 つのフェーズで定義されます。

ユーザーとデバイスがネットワークに接続すると、ネットワークは、特定のセキュリティグループを割り当てます。このプロセスは「分類」と呼ばれます。分類は、認証の結果に基づいて行うことも、SGT を IP、VLAN、またはポートプロファイルに関連付けることによって行うこともできます。

ユーザートラフィックが分類されると、SGT は、分類が行われた場所から適用アクションが呼び出される場所に伝達されます。このプロセスは「伝播」と呼ばれます。Cisco TrustSec には、インラインタギングと SXP の 2 つの SGT 伝達方式があります。

インラインタタギングの場合、SGT は、イーサネットフレームに組み込まれます。イーサネットフレーム内に SGT を埋め込む機能には、特定のハードウェアサポートが必要です。そのため、ハードウェアサポートのないネットワークデバイスは、SXP（SGT 交換プロトコル）と呼ばれるプロトコルを使用します。SXP は、SGT から IP アドレスへのマッピングを共有するために使用されます。これにより、SGT 伝達がパス内の次のデバイスに対して続行されます。

最終的に、適用デバイスが、タグ情報に基づいてトラフィックを制御します。シスコのファイアウォール、ルータ、またはスイッチを TrustSec の適用ポイントとすることができます。適用デバイスは送信元 SGT を取得し、それを宛先 SGT と照合して、トラフィックを許可するか拒否するかを決定します。適用デバイスがシスコのファイアウォールである場合、そのデバイスは、単一のファイアウォールルールで同じ送信元 SGT を使用して、ステートフル ファイアウォール処理と IPS ディープ パケット インスペクションも許可します。

（注） Cisco TrustSec 機能は、Cisco 1000 シリーズ サービス統合型ルータのスイッチポートではサポートされません。

（注） CTS 適用が有効になっている場合、デバイスは、ISE からポリシーをダウンロードしようとします。これには、RADIUS サーバーが設定されている必要があります。RADIUS サーバーが設定されていないと、ポリシーをダウンロードできず、Syslog ファイルにエラーが記録されます。

分類と適用の詳細については、『Cisco TrustSec Quick Start Configuration Guide』を参照してください。

SGT インライン タギング

CTS ドメイン内の各セキュリティグループは、「スケーラブルグループタグ」（SGT）と呼ばれる一意の 16 ビットタグが割り当てられます。SGT はネットワーク全体で送信元の権限を示す単一ラベルです。これは、ネットワーク ホップ間で順番に伝搬され、任意の中間デバイス（スイッチ、ルータ）はこれによってアイデンティティ タグに基づいたポリシーを適用できます。

CTS 対応デバイスには、MAC（L2）レイヤ内に組み込まれた SGT を持つパケットを送受信できる、ハードウェア機能が組み込まれています。この機能は、「L2-SGT インポジション」と呼ばれます。これにより、デバイスのイーサネット インターフェイスで L2-SGT インポジションを有効にできるため、そのデバイスはネクスト ホップ イーサネット ネイバーに運ばれるパケット内に SGT を挿入できるようになります。SGT-over-Ethernet は、クリアテキスト（非暗号化）イーサネット パケットに組み込まれた SGT のホップバイホップの伝達方式です。インライン アイデンティティ伝達はスケーラブルで、ほぼラインレートのパフォーマンスを提供し、コントロール プレーンのオーバーヘッドを防ぎます。

SXPv4 機能を備えた Cisco TrustSec は、CTS メタ データ（CMD）ベースの L2-SGT をサポートします。パケットが CTS 対応インターフェイスに入力されると、IP-SGT マッピング データベース（SXP によって構築されたダイナミック エントリや設定コマンドによって構築されたスタティック エントリがある）が分析され、パケットの送信元 IP アドレスに対応する SGT が学習されます。この SGT はパケットに挿入され、CTS ヘッダー内でネットワーク全体に運ばれます。

このタグは、送信元のグループを表しているので、送信元グループ タグ（SGT）としても参照されます。ネットワークの出力エッジでは、パケットの宛先に割り当てられたグループが既知になります。この時点で、アクセス制御を適用できます。CTS を使用すると、セキュリティ

グループアクセスコントロールリスト（SGACL）と呼ばれるアクセスコントロールポリシーがセキュリティグループ間で定義されます。任意のパケットから見れば、これは単純にセキュリティ グループから送信され、別のセキュリティ グループに送信されています。

Protected Access Credential（PAC）

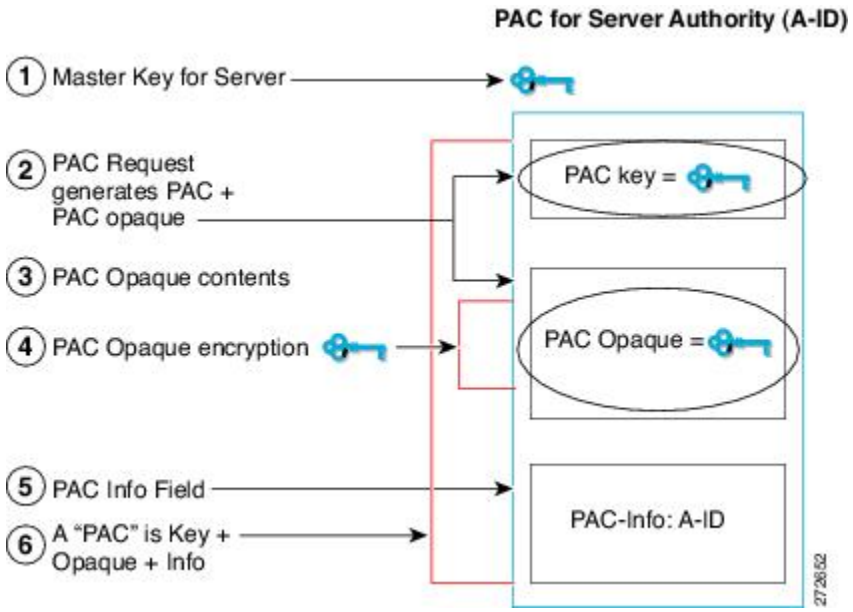
PACは、クライアントとサーバーの相互認証に使用される一意の共有ログイン情報です。これは、特定のクライアントユーザー名およびサーバー権限識別子（A-ID）に関連付けられます。PAC により、Public Key Infrastructure（PKI）およびデジタル証明書が不要になります。

PAC は次の手順で作成します。

1. サーバー A-ID は、サーバーのみが知っているローカルキー（マスターキー）を保持します。
2. クライアント（この文脈ではイニシエータ アイデンティティ（I-ID）と呼ばれる）がサーバーに PAC を要求すると、サーバーはこのクライアントに対してランダムに一意の PAC キーと PAC-Opaque フィールドを生成します。
3. PAC-Opaque フィールドには、ランダムに生成された PAC キーと、I-ID やキーの有効期間などの他の情報が含まれます。
4. PAC-Opaque フィールドの PAC キー、I-ID、およびライフタイムは、マスターキーで暗号化されます。
5. A-ID を含む PAC-Info フィールドが作成されます。
6. PAC は、クライアントに自動的に配布またはインポートされます。

（注） サーバーは PAC または PAC キーを保持しないため、EAP-FAST サーバーはステートレスになります。

次の図は、PAC の構造を示しています。PAC は、PAC-Opaque、PAC Key、および PAC-Info フィールドで構成されます。PAC-Info フィールドには A-ID が含まれます。



PAC Provisioning

Secure RADIUS では、認証中に PAC キーが各デバイスにプロビジョニングされ、共有秘密が導出されます。RADIUS ACS は各デバイスの PAC キーを保存しないため、クライアントは、PAC-Opaque フィールドを含む追加の RADIUS 属性も送信する必要があります。PAC-Opaque フィールドは可変長のフィールドであり、サーバーだけが解釈して、必要な情報を回復し、ピアのアイデンティティと認証を検証することができます。たとえば、PAC-Opaque フィールドには PAC キーと PAC のピアアイデンティティが含まれていることがあります。

PAC-Opaque フィールドの形式と内容は、発行元の PAC サーバーによって異なります。RADIUS サーバーは、PAC-Opaque フィールドから PAC キーを取得し、クライアントと同じ方法で共有秘密を導出します。Secure RADIUS は、共有秘密の導出方法のみを変更し、その使用方法は変更しません。

EAP-FAST フェーズ 0 は、PAC を使用してクライアントを自動的にプロビジョニングするために使用されます。

ハイアベイラビリティセットアップでのデバイスの展開

HA セットアップでデバイスを展開する場合は、次の手順を実行します。

1. HA セットアップに含まれるすべてのデバイスのログイン情報をクリアします。
2. スタックセットアップを起動し、デバイスロール（アクティブ、スタンバイ、およびメンバー）を確立します。
3. アクティブデバイスのログイン情報を設定します。ログイン情報を設定するには、**cts credentials id** *id* **password** *password* コマンドを使用します。

（注） 既存のスタックに新しいデバイスを追加する場合は、新しいデバイスのログイン情報をクリアしてから、既存のスタックセットアップに追加してください。

CTS ログイン情報

CTS では、ネットワーク内の各デバイスがそれ自体を一意に識別する必要があります。TrustSec ネットワーク デバイス アドミッション コントロール（NDAC）認証で使用する場合は、**cts credentials** コマンドを使用して、別の Cisco TrustSec デバイスでの認証時や、EAP-FAST を使用した PAC（Protected Access Credentials）のプロビジョニングのために、このデバイスが使用する Cisco TrustSec デバイス ID およびパスワードを指定します。CTS のクレデンシャル情報は startup-config ではなくキーストアに保存されているため、CTS のクレデンシャルの状態取得は不揮発性生成（NVGEN）プロセスでは実行されません。これらのクレデンシャルは、キーストアで保存され、running-config を保存する必要性がなくなります。CTS デバイス ID を表示するには、**show cts credentials** コマンドを使用します。保存されたパスワードは表示されません。

デバイス ID またはパスワードを変更するには、コマンドを再入力します。キーストアをクリアするには、**clear cts credentials** コマンドを使用します。

（注） CTS デバイス ID が変更された場合、Protected Access Credential（PAC）は古いデバイス ID に関連付けられており、新しいアイデンティティに対しては有効でないため、すべての PAC はキーストアから消去されます。

SGT インライン タギングの設定

手順の概要

1. **enable**
2. **configure terminal**
3. **interface** {**gigabitethernet** *port* | **vlan** *number*}
4. **cts manual**
5. **policy static sgt** *tag* [**trusted**]
6. **end**
7. **show cts interface brief**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface** {**gigabitethernet** *port* | **vlan** *number*} 例： `Device(config)# interface gigabitethernet 0`	CTS SGT の認証と転送が有効なインターフェイスを開始します。
ステップ 4	**cts manual** 例： `Device(config-if)# cts manual`	CTS SGT の承認と転送用のインターフェイスを有効化します。CTS 手動インターフェイス コンフィギュレーション モードを開始します。 （注） サブインターフェイスを使用している場合は、**config-if** モード（親インターフェイス）ではなく **config-subif** モード（サブインターフェイス）で **cts manual** コマンドを設定します。
ステップ 5	**policy static sgt** *tag* [**trusted**] 例： `Device(config-if-cts-manual)# policy static sgt 77`	インターフェイスでスタティック SGT 入力ポリシーを設定し、インターフェイスで受信する SGT の信頼性を定義します。 （注） **trusted** キーワードは、そのインターフェイスが CTS に信頼されていることを示します。このインターフェイス上のイーサネット パケット内で受信した SGT 値は信頼され、デバイスによって任意の SG 認識型ポリシーの適用または出力タギングに使用されます。
ステップ 6	**end** 例： `Device(config-if-cts-manual)# end`	CTS 手動インターフェイス コンフィギュレーション モードを終了し、特権 EXEC モードを開始します。
ステップ 7	**show cts interface brief** 例：	インターフェイスの CTS 設定の統計情報を表示します。

	コマンドまたはアクション	目的

	`Device# show cts interface brief`
	
	`Interface GigabitEthernet0/0`
	`CTS is enabled, mode: MANUAL`
	`Propagate SGT: Enabled`
	`Peer SGT assignment: Trusted`
	
	`Interface GigabitEthernet0/1`
	`CTS is enabled, mode: MANUAL`
	`Propagate SGT: Disabled`
	`Peer SGT assignment: Untrusted`
	
	`Interface GigabitEthernet0/3`
	`CTS is disabled.`	

CTS ログイン情報の設定

手順の概要

1. **enable**
2. **cts credentials id** *cts-id* **password** *cts-pwd*
3. **show cts credentials**
4. **show keystore**

手順の詳細

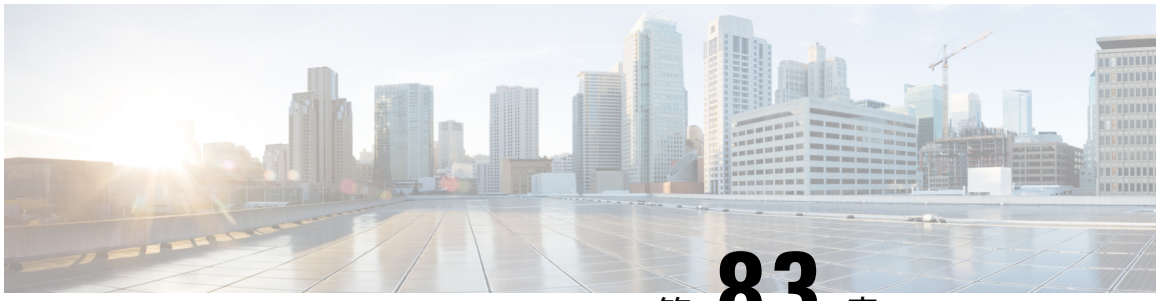
	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**cts credentials id** *cts-id* **password** *cts-pwd* 例： `Device# cts credentials id atlas password cisco123`	EAP-FAST を使用して他の Cisco TrustSec（CTS）デバイスで認証するときにこのデバイスが使用する CTS デバイス ID およびパスワードを指定します。
ステップ 3	**show cts credentials** 例： `Device# show cts credentials`	Cisco TrustSec（CTS）デバイス ID を表示します。
ステップ 4	**show keystore** 例： `**Note that the following is the sample output of the command till Cisco IOS XE Everest release`	ソフトウェアまたはハードウェア暗号化キーストアの内容を表示します。

	コマンドまたはアクション	目的
	16.5.** Device# **show keystore** Using software keystore emulation. Keystore contains the following records (S=Simple Secret, P=PAC, R=RSA): Index Type Name ----- ---- ---- 0 S CTS-password 1 P 57366898EEF9D71A6E33C3628CE7EEDE 例： ****Note that the following is the sample output of the command from Cisco IOS XE Everest release 16.6 and above. The Protected Access Credentials (PAC) information is not displayed.**** Device# **show keystore** Using software keystore emulation. Keystore contains the following records (S=Simple Secret, P=PAC, R=RSA): Index Type Name ----- ---- ---- 0 S CTS-password	

例：SGT インライン タギングの設定

この例では、デバイスのインターフェイスで L2-SGT タギングまたはインポジションを有効にして、インターフェイスが CTS に信頼されるかどうかを定義する方法を示します。

```
Device# configure terminal
Device(config)# interface gigabitethernet 0
Device(config-if)# cts manual
Device(config-if-cts-manual)# propagate sgt
Device(config-if-cts-manual)# policy static sgt 77 trusted
```



第 83 章

Cisco TrustSec SGT Exchange Protocol IPv4

Cisco TrustSec（CTS）は、信頼できるネットワーク デバイスのドメインを確立することによってセキュア ネットワークを構築します。ドメイン内の各デバイスは、そのピアによって認証されます。ドメイン内のデバイス間リンクでの通信は、暗号化、メッセージ整合性検査、データパス リプレイ防止メカニズムを組み合わせたセキュリティで保護されます。

セキュリティ グループ タグ（SGT）交換プロトコル（SXP）は、CTS をサポートする複数のプロトコルの 1 つであり、本書では CTS-SXP と呼びます。CTS-SXP は、パケットのタグ付け機能がないネットワーク デバイス全体に IP-to-SGT バインドの情報を伝播する、制御プロトコルです。CTS-SXP は、ネットワーク上のアップストリーム デバイスへの認証ポイントから SGT バインドへの IP を渡します。このプロセスにより、スイッチ、ルータ、ファイアウォールのセキュリティ サービスは、アクセス デバイスから学習したアイデンティティ情報を伝えることができます。

Cisco TrustSec SGT Exchange Protocol IPv4 の制約事項

- IOS 機能の Cisco TrustSec サポートは、第 2 世代 Cisco サービス統合型ルータ（ISR G2）のみでサポートされています。
- CTS-SXP は物理インターフェイスだけでサポートされ、論理インターフェイスでサポートされません。
- CTS-SXP 検証は、IPv6 をサポートしていません。
- ルータにデフォルトのパスワードが実装されている場合、そのルータでの接続は、デフォルト パスワードを使用するようにパスワードを設定する必要があります。デフォルトのパスワードが設定されていない場合、そのルータでの接続はパスワード設定を使用しないよ

うに設定してください。パスワードオプションの設定は導入ネットワーク全体で一貫している必要があります。

Cisco TrustSec SGT Exchange Protocol IPv4 に関する情報

セキュリティ グループ タギング

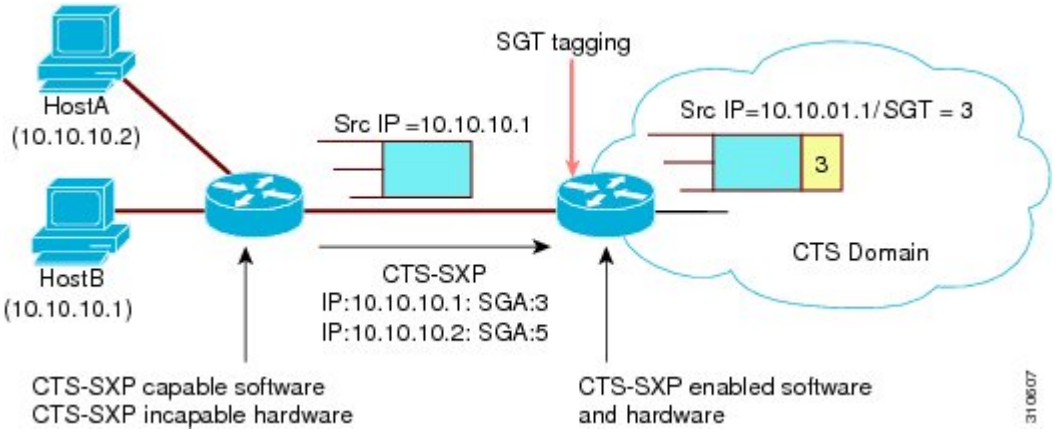
CTS-SXP は、認証時に取得したデバイスおよびユーザの識別情報を使用して、ネットワークに進入するパケットをセキュリティ グループ（SG）で分類します。このパケット分類は、CTS-SXP ネットワークへの入力時にパケットにタグ付けされることにより維持されます。タグによってパケットはデータ パス全体を通じて正しく識別され、セキュリティおよびその他のポリシー基準が適用されます。セキュリティ グループ タグ（SGT）によってエンドポイント デバイスはトラフィックをフィルタリングできるので、ネットワークへのアクセス コントロール ポリシーの適用が可能になります。

CTS-SXP によるレガシー アクセス ネットワークへの SGT の伝播

パケットへの SGT のタグ付けには、ハードウェアによるサポートが必要です。CTS 認証に参加できが、SGT でパケットをタグ付けするハードウェア機能を持たないデバイスが、ネットワーク内にある場合があります。ただし、CTS-SXP を使用する場合は、これらのデバイスが、IP と SGT のマッピングを CTS 対応ハードウェアがある CTS ピア デバイスに渡すことができます。

通常、CTS-SXP は CTS ドメイン エッジの入力アクセス レイヤ デバイスと CTS ドメイン内のディストリビューション レイヤ デバイス間で動作します。アクセス レイヤ デバイスは入力パケットの適切な SGT を判断するために、外部送信元デバイスの CTS 認証を実行します。アクセス レイヤ デバイスは IP デバイス トラッキングおよび（任意で）DHCP スヌーピングを使用して送信元デバイスの IP アドレスを学習し、その後 CTS-SXP を使用して送信元デバイスの IP アドレスおよび SGT を、ディストリビューション スイッチに渡します。CTS 対応のハードウェアを備えたディストリビューション スイッチは、この IP と SGT のマッピング情報を使用して、パケットに適切にタグを付け、セキュリティ グループ アクセス コントロール リスト（SGACL）ポリシーを強制します。次の図を参照してください。SGACL は、SGT とポリシーを関連付けます。ポリシーは、SGT タグ付けされたトラフィックが CTS ドメインから出力されると適用されます。

図 *15 : CTS-SXP* による *SGT* 情報の伝達方法



CTS ハードウェア サポート対象外のピアと CTS ハードウェア サポート対象のピア間の CTS-SXP 接続は、手動で設定する必要があります。CTS-CSXP 接続を設定する場合は、次の作業を実行する必要があります。

- CTS-SXP のデータの整合性と認証が必要な場合、同じ CTS-SXP パスワードを両方のピア デバイスで設定できます。CTS-SXP パスワードは各ピア接続に対して明示的に指定することも、デバイスに対してグローバルに設定することもできます。CTS-SXP パスワードは必須ではありませんが、推奨します。
- CTS-SXP 接続の各ピアは、CTS-SXP スピーカーまたは CTS-SXP リスナーとして設定する必要があります。スピーカー デバイスはリスナー デバイスに IP-to-SGT 情報を渡します。
- 各ピアの関係に使用する送信元 IP アドレスを指定できます。または、特定の送信元 IP アドレスが設定されていないピア接続に対して、デフォルトの送信元 IP アドレスを設定できます。送信元 IP アドレスが指定されていないと、デバイスはピアへの接続のインターフェイス IP アドレスを使用します。

CTS-SXP では複数のホップを許可します。つまり、CTS ハードウェア サポート対象外デバイスのピアが CTS ハードウェア サポートの対象外でもある場合、2 番目のピアはハードウェア対応ピアに到達するまで IP と SGT のマッピング情報の伝播を継続して、3 番目のピアへの CTS-SXP 接続を設定できます。デバイスは 1 つの CTS-SXP 接続では CTS-SXP リスナーとして、別の CTS-SXP 接続では CTS-SXP スピーカーとして設定できます。

CTS デバイスは TCP キープアライブ メカニズムを使用して、CTS-SXP ピアとの接続を維持します。ピア接続を確立または回復するために、デバイスは設定可能な再試行期間を使用して接続が成功するか、接続が設定から削除されるまで接続の確立を繰り返し試行します。

VRF-Aware CTS-SXP

仮想ルーティングおよびフォワーディング（VRF）の CTS-SXP の実装は、特定の VRF と CTS-SXP 接続をバインドします。CTS-SXP を有効化する前に、ネットワーク トポロジがレイヤ 2 またはレイヤ 3 の VPN に対して正しく設定されており、すべての VRF が設定されていることを前提としています。

CTS-SXP VRF サポートは、次のようにまとめることができます。

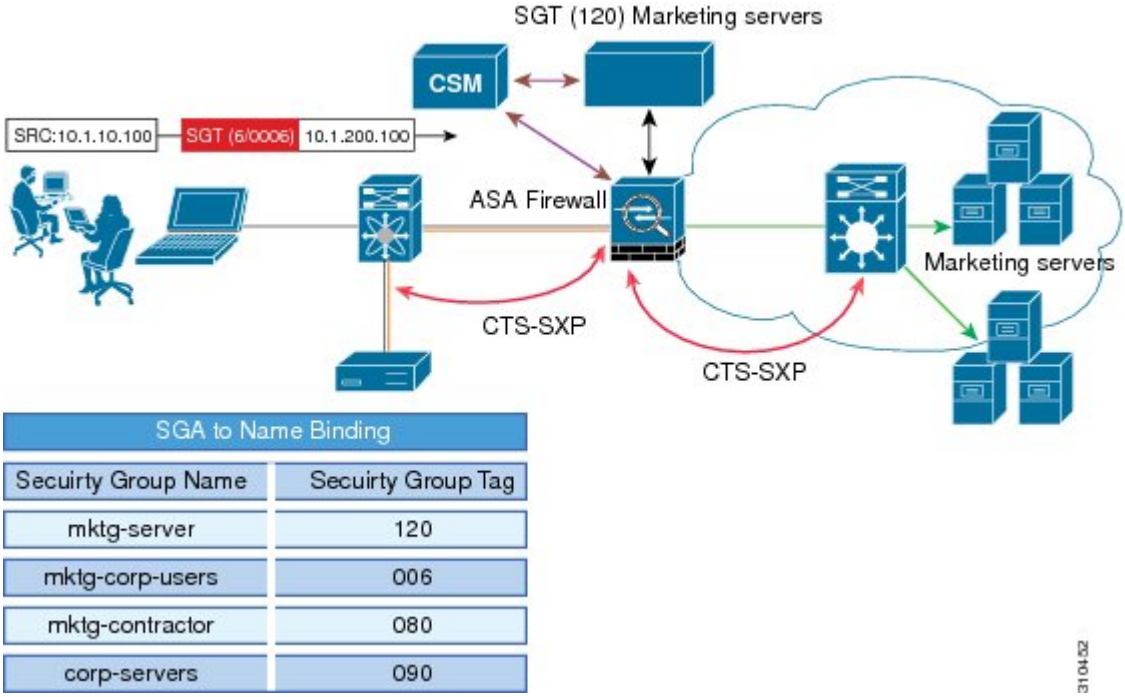
- 1 つの VRF には 1 つの CTS-SXP 接続のみをバインドできます。
- 別の VRF が重複する CTS-SXP ピアまたは送信元 IP アドレス持つ可能性があります。
- 1 つの VRF で学習（追加または削除）された IP と SGT のマッピングは、同じ VRF ドメインでのみ更新できます。CTS-SXP 接続は異なる VRF にバインドされたマッピングを更新できません。SXP 接続が VRF で終了しない場合は、その VRF の IP-SGT マッピングは SXP によって更新されません。
- CTS-SXP 検証は、送信元 IPv6 アドレスを使用した接続の確立をサポートしていません。ただし、VRF ドメイン内の 1 つの CTS-SXP 接続を IPv4 と IPv6 両方の IP と SGT のマッピングに転送できる場合は、VRF あたりで複数のアドレス ファミリがサポートされます。
- CTS-SXP には VRF あたりの接続数および IP と SGT のマッピング数に制限はありません。

セキュリティ グループ アクセスのゾーンベース ポリシー ファイアウォール

CTS-SXP は、セキュリティ グループ アクセス（SGA）ゾーンベース ポリシー ファイアウォール（ZBPF）を使用することで、ネットワーク デバイスの導入をネットワークのさらに別の場所へ拡張します。CTS-SXP は、次の図に示すとおり、ネットワーク全体に存在するプライマリ通信パスからアイデンティティ情報を学習するインラインデバイスを通じたアイデンティティ分散に使用されます。

セキュリティ グループ タグ（SGT）は、強制ポリシーを適用するため、SGA ZBPF によって使用されます。IP と SGT のマッピング情報は、CTS-SXP から学習します。パケットを受信すると、パケット内の送信元と宛先の IP アドレスは、送信元と宛先のタグを派生させるために使用されます。アイデンティティ ファイアウォールは、属性の 1 つに SGT がある、設定されたポリシーに基づいて、受信した IP パケットにポリシーを適用します。

図 *16* : ネットワーク全体の *CTS-SXP SGA ZBPF* 分散パス



Cisco TrustSec SGT Exchange Protocol IPv4 の設定方法

CTS-SXP の有効化

手順の概要

1. **enable**
2. **configure terminal**
3. **cts sxp enable**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例：	グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
	`Device# configure terminal`	
ステップ 3	**cts sxp enable** 例： `Device(config)# cts sxp enable`	設定された任意のピア接続に対して CTS-SXP 接続を有効化します。 （注） ピア接続が設定されていることを確認します。ピア接続が設定されていない場合、CTS-SXP 接続はそれらとは確立できません。

CTS-SXP ピア接続の設定

CTS-SXP ピア接続を両方のデバイスで設定する必要があります。一方のデバイスはスピーカーで、他方のデバイスはリスナーになります。パスワード保護を使用している場合は、必ず両エンドに同じパスワードを使用してください。

（注） デフォルトの CTS-SXP 送信元 IP アドレスが設定されていない場合に、接続の CTS-SXP 送信元アドレスを設定しないと、Cisco TrustSec ソフトウェアは既存のローカル IP アドレスから CTS-SXP 送信元 IP アドレスを抽出します。CTS-SXP 送信元 IP アドレスは、ルータから開始される TCP 接続ごとに異なる場合があります。

手順の概要

1. **enable**
2. **configure terminal**
3. **cts sxp connection peer** *ipv4-address* {**source** | **password**} {**default** | **none**} **mode** {**local** | **peer**} [[**listener** | **speaker**] [**vrf** *vrf-name*]]
4. **exit**
5. **show cts sxp** {**connections** | **sgt-map**} [**brief** | **vrf** *vrf-name*]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例：	グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
	`Device# configure terminal`	
ステップ 3	**cts sxp connection peer** *ipv4-address* {**source** | **password**} {**default** | **none**} **mode** {**local** | **peer**} [[**listener** | **speaker**] [**vrf** *vrf-name*]] 例： `Device(config)# cts sxp connection peer 10.20.2.2 password default mode local speaker`	CTS-SXP ピア アドレス接続を設定します。 **source** キーワードには発信元デバイスの IPv4 アドレスを指定します。接続アドレスが指定されていない場合、デフォルトの送信元アドレス（設定されている場合）、またはポートのアドレスを使用します。 **password** キーワードには、CTS-SXP で接続に使用するパスワードを指定します。次のオプションがあります。 • **default**：**cts sxp default password** コマンドを使用して設定したデフォルトの CTS-SXP パスワードを使用します。 • **none**：パスワードは使用されません。 **mode** キーワードでは、リモートピアデバイスのロールを指定します。 • **local**：指定したモードはローカルデバイスを参照します。 • **peer**：指定したモードはピアデバイスを参照します。 • **listener**：このデバイスが接続の際にリスナーになります。 • **speaker**：接続の際にこのデバイスがスピーカーになります。これはデフォルトです。 オプションの **vrf** キーワードでは、ピアに対する VRF を指定します。デフォルトはデフォルト VRF です。
ステップ 4	**exit** 例： `Device# exit`	グローバル コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。
ステップ 5	**show cts sxp** {**connections** | **sgt-map**} [**brief** | **vrf** *vrf-name*] 例： `Device# show cts sxp connections`	（オプション）CTS-SXP のステータスと接続を表示します。

デフォルトの CTS-SXP パスワードの設定

手順の概要

1. **enable**
2. **configure terminal**
3. **cts sxp default password** [**0** | **6** | **7**] *password*
4. **exit**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**cts sxp default password** [**0** | **6** | **7**] *password* 例： `Device(config)# cts sxp default password Cisco123`	CTS-SXP のデフォルト パスワードを設定します。クリアテキストパスワード（**0**を使用するかオプションなし）または暗号化パスワード（**6** または **7** オプションを使用）を入力できます。パスワードの最大長は 32 文字です。 （注） デフォルトでは、CTS-SXP は接続のセットアップ時にパスワードを使用しません。
ステップ 4	**exit** 例： `Device# exit`	グローバル コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

デフォルトの CTS-SXP 送信元 IP アドレスの設定

手順の概要

1. **enable**
2. **configure terminal**
3. **cts sxp default source-ip** *src-ip-addr*
4. **exit**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**cts sxp default source-ip** *src-ip-addr* 例： `Device(config)# cts sxp default source-ip 10.20.2.2`	CTS-SXP デフォルトの送信元 IP アドレスを設定します。これは、送信元IPアドレスが指定されていないすべての新しい TCP 接続に使用されます。 （注） デフォルトの CTS-SXP 送信元 IP アドレスが設定されている場合も、既存の TCP 接続には影響しません。
ステップ 4	**exit** 例： `Device# exit`	グローバル コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

CTS-SXP の復帰期間の設定

ピアが CTS-SXP 接続を終了すると、内部ホールドダウン タイマーが開始されます。内部ホールドダウン タイマーが終了する前にピアが再接続すると、CTS-SXP 復帰期間タイマーが開始されます。CTS-SXP 復帰期間タイマーがアクティブな間、CTS ソフトウェアは前回の接続で学習した SGT マッピング エントリを保持し、無効なエントリを削除します。デフォルト値は 120 秒（2 分）です。CTS-SXP 復帰期間を 0 秒に設定すると、タイマーがディセーブルになり、前回の接続のすべてのエントリが削除されます。

手順の概要

1. **enable**
2. **configure terminal**
3. **cts sxp reconciliation period** *seconds*
4. **exit**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**cts sxp reconciliation period** *seconds* 例： `Device(config)# cts sxp reconciliation period 150`	CTS-SXP 復帰タイマーを秒単位で設定します。範囲は 0 ～ 64000 です。デフォルトは 120 です。
ステップ 4	**exit** 例： `Device# exit`	グローバル コンフィギュレーション モードを終了し、特権 EXEC モードを開始します。

CTS-SXP 再試行期間の設定

CTS-SXP 再試行期間によって、CTS ソフトウェアが CTS-SXP 接続を再試行する頻度が決まります。CTS-SXP 接続が正常に確立されなかった場合、CTS ソフトウェアは CTS-SXP 再試行期間タイマーの終了後に、新たな接続の確立を試行します。デフォルト値は2分です。CTS-SXP 再試行期間を 0 秒に設定するとタイマーは無効になり、接続は再試行されません。

手順の概要

1. **enable**
2. **configure terminal**
3. **cts sxp retry period** *seconds*
4. **exit**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。

	コマンドまたはアクション	目的
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**cts sxp retry period** *seconds* 例： `Device(config)# cts sxp retry period 160`	CTS-SXP 再試行タイマーを秒単位で設定します。範囲は 0 ～ 64000 です。デフォルトは 120 です。
ステップ 4	**exit** 例： `Device# exit`	グローバル コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

IP と SGT のマッピング変更をキャプチャする Syslog の作成

手順の概要

1. **enable**
2. **configure terminal**
3. **cts sxp log binding-changes**
4. **exit**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**cts sxp log binding-changes** 例： `Device(config)# cts sxp log binding-changes`	IP と SGT バインド変更のロギングを有効にすると、IP と SGT バインディングの変更（追加、削除、変更）が発生するたびに CTS-SXP の syslog （sev 5 syslog）が生成されます。これらの変更は CTS-SXP 接続で学習されて伝播されます。

	コマンドまたはアクション	目的
		（注） このロギング機能は、デフォルトではディセーブルになっています。
ステップ 4	**exit** 例： `Device# exit`	グローバル コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

セキュリティ グループ アクセスのゾーンベース ポリシー ファイアウォールのクラス マップの設定

このタスクを実行して、セキュリティ グループ アクセス（SGA）ゾーンベース ポリシー ファイアウォールのネットワーク トラフィックを分類するためのクラス マップを設定します。

（注） 少なくとも 1 つの手順を実行する必要があります。

ゾーンベース ファイアウォール ポリシーは、フィルタリングにセキュリティ グループ タグの ID を使用します。ゾーンベース ファイアウォール ポリシーでは、ポリシーと一致するのは、セッションを作成した最初のパケットのみです。このフローの後続パケットは、設定されたポリシー内のフィルタと一致しませんが、セッションとは直接一致します。後続パケットに関連する統計情報は、検査アクションの一部として表示されます。

手順の概要

1. **enable**
2. **configure terminal**
3. **object-group security** *name*
4. **security-group tag-id** *sgt-id*
5. **group-object** *name*
6. **description** *text*
7. **exit**
8. **class-map type inspect** [**match-any** | **match-all**] *class-map-name*
9. **match group-object security source** *name*
10. **match group-object security destination** *name*
11. **end**
12. **show object-group** [*name*]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**object-group security** *name* 例： `Device(config)# object-group security myobject1a`	オブジェクト グループを作成して、特定のユーザまたはエンドポイントから受信するトラフィックを特定し、オブジェクトグループのアイデンティティ モードに入ります。
ステップ 4	**security-group tag-id** *sgt-id* 例： `Device(config-object-group)# security-group tag-id 120`	SGT ID 番号を使用して、セキュリティ グループのメンバーシップを指定します。この番号は 1 ～ 65535 ですこのコマンドを使用すると、複数のセキュリティ グループを指定できます。
ステップ 5	**group-object** *name* 例： `Device(config-object-group)# group-object admin`	（オプション）ネストされた参照を、ユーザ グループのタイプに指定します。このコマンドを使用すると、複数のネストされたユーザ グループを指定できます。
ステップ 6	**description** *text* 例： `Device(config-object-group)# description my sgtinfo`	（オプション）セキュリティ グループに関する情報を定義します。
ステップ 7	**exit** 例： `Device(config-object-group)# exit`	オブジェクトグループ アイデンティティ モードを終了し、グローバル コンフィギュレーション モードを開始します。
ステップ 8	**class-map type inspect** [**match-any** | **match-all**] *class-map-name* 例： `Device(config)# class-map type inspect match-any myclass1`	レイヤ 3 またはレイヤ 4 の検査タイプ クラス マップを作成し、クラスマップ コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 9	**match group-object security source** *name* 例： `Device(config-cmap)# match group-object security source myobject1`	セキュリティ グループ内のユーザからのトラフィックと一致させます。
ステップ 10	**match group-object security destination** *name* 例： `Device(config-cmap)# match group-object security destination myobject1`	セキュリティ グループ内のユーザのトラフィックと一致させます。
ステップ 11	**end** 例： `Device(config-cmap)# end`	クラスマップ コンフィギュレーション モードを終了し、特権 EXEC モードを開始します。
ステップ 12	**show object-group** [*name*] 例： `Device# show object-group admin`	（オプション）すべてのユーザ グループのコンテンツを表示します。オプションとして、*name* 引数を使用すると、単一グループの情報が表示されます。

セキュリティ グループ アクセスのゾーンベース ポリシー ファイアウォールのポリシー マップの作成

このタスクを実行して、ゾーン ペアに接続する、セキュリティ グループ アクセス（SGA）ゾーンベース ポリシー ファイアウォールのポリシー マップを作成します。また、このタスクは、セキュリティ ゾーンに属するインターフェイス上で、セキュリティ グループ タグ（SGT）交換プロトコル（SXP）またはL2タグ付きトラフィックと動作するよう、アイデンティティ ファイアウォール（IDFW）を設定します。

手順の概要

1. **enable**
2. **configure terminal**
3. **policy-map type inspect** *policy-map-name*
4. **class type inspect** *class-name*
5. **inspect**
6. **exit**
7. **zone-pair security** *zone-pair-name* **source** *source-zone* **destination** *destination-zone*
8. **service-policy type inspect** *policy-map-name*
9. **end**
10. **interface** *type number*
11. **zone-member security** *zone-name*

12. **cts manual**
13. **no propagate sgt**
14. **policy static sgt** *tag* [**trusted**]
15. **exit**
16. **show policy-map type inspect zone-pair session**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**policy-map type inspect** *policy-map-name* 例： `Device(config)# policy-map type inspect z1z2-policy`	レイヤ 3 またはレイヤ 4 の検査タイプ ポリシーマップを作成します。 • ポリシーマップ コンフィギュレーション モードを開始します。
ステップ 4	**class type inspect** *class-name* 例： `Device(config-pmap)# class type inspect cmap-1`	アクションを実行する対象のトラフィック（クラス）を指定し、ポリシー マップ クラス コンフィギュレーション モードを開始します。
ステップ 5	**inspect** 例： `Device(config-pmap-c)# inspect`	パケット インスペクションを有効化します。
ステップ 6	**exit** 例： `Device(config-pmap-c)# exit`	ポリシーマップ クラス コンフィギュレーション モードを終了し、グローバルコンフィギュレーション モードを開始します。
ステップ 7	**zone-pair security** *zone-pair-name* **source** *source-zone* **destination** *destination-zone* 例： `Device(config)# zone-pair security z1z2 source z1 destination z2`	ゾーン ペアを作成し、セキュリティ ゾーン コンフィギュレーション モードを開始します。 （注） ポリシーを適用するには、ゾーン ペアを設定する必要があります。

	コマンドまたはアクション	目的
ステップ 8	**service-policy type inspect** *policy-map-name* 例： `Device(config-sec-zone)# service-policy type inspect z1z2-policy2`	ファイアウォール ポリシー マップを宛先ゾーン ペアに付加します。 （注） ゾーンのペア間でポリシーが設定されない場合、トラフィックはデフォルトでドロップされます。
ステップ 9	**end** 例： `Device(config-sec-zone)# end`	セキュリティ ゾーン コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードを開始します。
ステップ 10	**interface** *type number* 例： `Device(config)# interface GigabitEthernet 0/1/1`	インターフェイスを設定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 11	**zone-member security** *zone-name* 例： `Device(config-if)# zone-member security Inside`	インターフェイスを指定したセキュリティ ゾーンに割り当てます。 （注） インターフェイスをセキュリティ ゾーンのメンバーにした場合、方向に関係なくインターフェイスを通過するすべてのトラフィック（ルータ宛のトラフィックまたはルータ発信のトラフィックを除く）は、デフォルトでドロップされます。トラフィックがインターフェイス通過するには、ゾーンをポリシーの適用先のゾーン ペアの一部にする必要があります。ポリシーがトラフィックを許可すると、トラフィックはそのインターフェイスを通過できます。
ステップ 12	**cts manual** 例： `Device(config-if)# cts manual`	Cisco TrustSec Security（CTS）SGT 認証と転送のインターフェイスを有効化し、CTS 手動インターフェイス コンフィギュレーション モードを開始します。
ステップ 13	**no propagate sgt** 例： `Device(config-if-cts-manual)# no propagate sgt`	CTS インターフェイスで レイヤ 2 の SGT 伝達を無効化します。

	コマンドまたはアクション	目的
ステップ 14	**policy static sgt** *tag* [**trusted**] 例： `Device(config-if-cts-manual)# policy static sgt 100 trusted`	SGT の信頼性を定義するタグ付きパケットを使用して、CTS セキュリティ グループのスタティック認証ポリシーを設定します。
ステップ 15	**exit** 例： `Device(config-if)# exit`	セキュリティ ゾーン コンフィギュレーション モードを終了し、特権 EXEC モードを開始します。
ステップ 16	**show policy-map type inspect zone-pair session** 例： `Device# show policy-map type inspect zone-pair session`	（オプション）指定されたゾーン ペアのポリシー マップアプリケーションが原因で作成された、Cisco IOS ステートフル パケット インスペクション セッションを表示します。 （注） クラスマップ フィールドの下に表示される情報は、接続開始トラフィックのみに属するトラフィックのトラフィック レート（ビット/秒）です。接続セットアップ レートが非常に高く、レートが計算される複数のインターバルにわたって高い接続セットアップ レートが持続する場合を除き、接続に関する意味のあるデータは表示されません。

例：

次の出力例は、**show policy-map type inspect zone-pair session** コマンドによって表示される、指定されたゾーンペアのポリシーマップ アプリケーションが原因で作成された、Cisco IOS ステートフル パケット インスペクション セッションに関する情報を示します。

```
Device# show policy-map type inspect zone-pair session

Zone-pair: in-out
 Service-policy inspect : test

   Class-map: test (match-any)
     Match: group-object security source sgt
     Inspect
       Established Sessions
        Session 113EF68C (192.2.2.1:8)=>(198.51.100.252:153) icmp SIS_OPEN
         Created 00:00:02, Last heard 00:00:02
         Bytes sent (initiator:responder) [360:360]


   Class-map: class-default (match-any)
```

```
Match: any
Drop (default action)
  310 packets, 37380 bytes
```

Cisco TrustSec SGT Exchange Protocol IPv4 の設定例

例：CTS-SXP ピア接続のイネーブル化と設定

次に、CTS-SXP をイネーブルにし、Device_A（スピーカー）で Device_B（リスナー）への SXP ピア接続を設定する例を示します。

```
Device# configure terminal
Device_A(config)# cts sxp enable
Device_A(config)# cts sxp default password Cisco123
Device_A(config)# cts sxp default source-ip 10.10.1.1
Device_A(config)# cts sxp connection peer 10.20.2.2 password default mode local speaker
```

次に、Device_B（リスナー）で Device_A（スピーカー）への CTS-SXP ピア接続を設定する例を示します。

```
Device# configure terminal
Device_B(config)# cts sxp enable
Device_B(config)# cts sxp default password Cisco123
Device_B(config)# cts sxp default source-ip 10.20.2.2
Device_B(config)# cts sxp connection peer 10.10.1.1 password default mode local listener
```

次に、CTS-SXP 接続を表示する **show cts sxp connections** コマンドの出力例を示します。

```
Device_B# show cts sxp connections

 SXP              : Enabled
 Default Password : Set
 Default Source IP: 10.10.1.1
Connection retry open period: 10 secs
Reconcile period: 120 secs
Retry open timer is not running
------------------------------------------------
Peer IP          : 10.20.2.2
Source IP        : 10.10.1.1
Conn status      : On
Connection mode  : SXP Listener
Connection inst# : 1
TCP conn fd      : 1
TCP conn password: default SXP password
Duration since last state change: 0:00:21:25 (dd:hr:mm:sec)
Total num of SXP Connections = 1
```

例：セキュリティ グループ アクセスのゾーンベース ポリシー ファイアウォールの設定

次の例は、SGA ゾーンベース ポリシー ファイアウォールのクラス マップとポリシー マップの設定を示します。

```
Device(config)# object-group security myobject1
Device(config-object-group)# security-group tag-id 1
Device(config-object-group)# exit
Device(config)# object-group security myobject2
Device(config-object-group)# security-group tag-id 2
Device(config-object-group)# exit
Device(config)# object-group security myobject3
Device(config-object-group)# security-group tag-id 3
Device(config-object-group)# exit
Device(config)# object-group security myobject4
Device(config-object-group)# security-group tag-id 4
Device(config-object-group)# exit

Device(config)# class-map type inspect match-any myclass1
Device(config-cmap)# match group-object security source myobject1
Device(config-cmap)# exit
Device(config)# class-map type inspect match-any myclass2
Device(config-cmap)# match group-object security source myobject2
Device(config-cmap)# exit
Device(config)# class-map type inspect match-any myclass3
Device(config-cmap)# match group-object security source myobject3
Device(config-cmap)# exit
Device(config)# class-map type inspect match-any myclass4
Device(config-cmap)# match group-object security source myobject4
Device(config-cmap)# exit

Device(config)# policy-map type inspect InsideOutside
Device(config-pmap)# class type inspect myclass1
Device(config-pmap-c)# pass
Device(config-pmap-c)# exit
Device(config-pmap)# class type inspect myclass2
Device(config-pmap-c)# drop log
Device(config-pmap-c)# exit

Device(config)# policy-map type inspect OutsideInside
Device(config-pmap)# class type inspect myclass3
Device(config-pmap-c)# pass
Device(config-pmap-c)# exit
Device(config-pmap)# class type inspect myclass4
Device(config-pmap-c)# drop
Device(config-pmap-c)# exit

Device(config)# zone-pair security Inside
Device(config-sec-zone)# description Firewall Inside Zone
Device(config-sec-zone)# exit

Device(config)# zone-pair security Outside
Device(config-sec-zone)# description Firewall Outside Zone
Device(config-sec-zone)# exit

Device(config)# zone-pair security InsideOutside source Inside destination Outside
Device(config-sec-zone)# description Firewall ZonePair Inside Outside
Device(config-sec-zone)# service-policy type inspect InsideOutside
```

```
Device(config-sec-zone)# exit

Device(config)# zone-pair security OutsideInside source Outside destination Inside
Device(config-sec-zone)# description Firewall ZonePair Outside Inside
Device(config-sec-zone)# service-policy type inspect OutsideInside
Device(config-sec-zone)# exit

Device(config)# interface Gigabit 0/1/1
Device(config-if)# zone-member security Inside
Device(config-if)# exit
```

TrustSec SGT の処理：L2 SGT のインポジションと転送に関する追加情報

関連資料

関連項目	マニュアル タイトル
セキュリティ コマンド	『Cisco IOS Security Command Reference: Commands A to C』
	『Cisco IOS Security Command Reference: Commands D to L』
	『Cisco IOS Security Command Reference: Commands M to R』
	『Cisco IOS Security Command Reference: Commands S to Z』
Cisco TrustSec スイッチ	『Cisco TrustSec スイッチ コンフィギュレーション ガイド』

MIB

MIB	MIB のリンク
CISCO-TRUSTSEC-SXP-MIB	選択したプラットフォーム、Cisco ソフトウェア リリース、およびフィーチャ セットの MIB を検索してダウンロードする場合は、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

シスコのテクニカル サポート

説明	リンク
右の URL にアクセスして、シスコのテクニカル サポートを最大限に活用してください。これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

Cisco TrustSec SGT Exchange Protocol IPv4 の機能情報

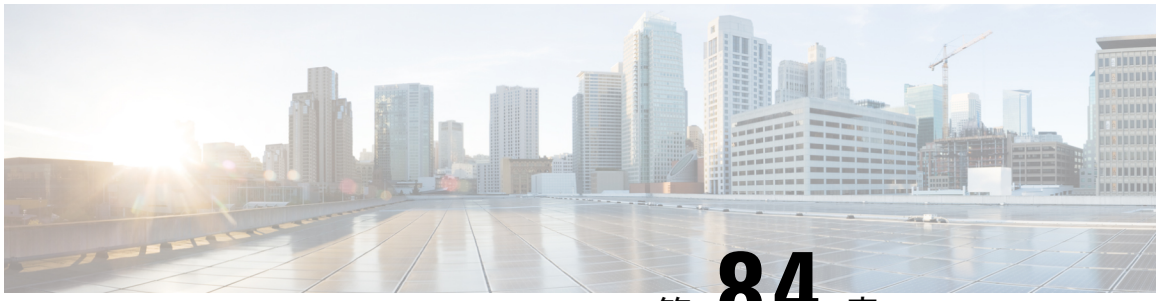
次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *118 : Cisco TrustSec SGT Exchange Protocol IPv4* の機能情報

機能名	リリース	機能情報
Cisco TrustSec SGT Exchange Protocol IPv4		セキュリティ グループ タグ（SGT）交換プロトコル（SXP）は、CTS をサポートする複数のプロトコルの 1 つであり、本書では CTS-SXP と呼びます。CTS-SXP は、パケットのタグ付け機能がないネットワーク デバイス全体に IP-to-SGT バインドの情報を伝播する、制御プロトコルです。CTS-SXP は、ネットワーク上のアップストリーム デバイスへの認証ポイントから SGT バインドへの IP を渡します。これにより、スイッチ、ルータ、ファイアウォールのセキュリティ サービスは、アクセス デバイスから学習したアイデンティティ情報を伝えることができます。 次のコマンドが導入または変更されました。**cts sxp enable, cts sxp connection peer**、**show cts sxp**、**cts sxp default source-ip, cts sxp reconciliation period, cts sxp retry period, cts sxp log binding-changes**。

機能名	リリース	機能情報
TrustSec SG Firewall Enforcement IPv4		この機能は、CTS-SXP がセキュリティ グループ アクセス（SGA）ゾーンベース ポリシー ファイアウォール（ZBPF）を通じてネットワーク デバイスを拡張するのを支援します。 次のコマンドが導入または変更されました。**group-object**、**match group-object security**、**object-group security**、**policy static sgt**、および **security-group**。



第 84 章

TrustSec SGT の処理：L2 SGT のインポジションと転送

初版：2011年7月25日

Cisco TrustSec（CTS）は、信頼できるネットワーク デバイスのドメインを確立することによってセキュア ネットワークを構築します。ドメイン内の各デバイスは、そのピアによって認証されます。ドメイン内のデバイス間リンクでの通信は、暗号化、メッセージ整合性検査、データパス リプレイ防止メカニズムを組み合わせたセキュリティで保護されます。

TrustSec SGT の処理：L2 SGT のインポジションと転送の機能により、ルータのインターフェイスは CTS を手動で有効化できるようになるため、ルータはセキュリティ グループ タグ（SGT）を、CTS ヘッダー内でネットワーク全体に運ばれるパケットに挿入できます。

TrustSec SGT の処理：L2 SGT のインポジションと転送の前提条件

TrustSec SGT の処理：L2 SGT インポジションと転送の機能を実装する前に、次の前提条件で CTS ネットワークを確立する必要があります。

- すべてのネットワーク デバイス間が接続されていること。
- Cisco Secure Access Control System（ACS）5.1 が、CTS-SXP ライセンスで動作していること。
- ディレクトリ、DHCP、DNS、認証局、およびNTPサーバーがネットワーク内で機能すること。
- 異なるルータで異なる値に **retry open timer** コマンドを設定します。

TrustSec SGT の処理：L2 SGT のインポジションと転送に関する情報

セキュリティ グループおよび SGT

セキュリティ グループは、アクセス コントロール ポリシーを共有するユーザー、エンドポイント デバイス、およびリソースのグループです。セキュリティ グループは管理者が ACS で定義します。新しいユーザーおよびデバイスが Cisco TrustSec（CTS）ドメインに追加されると、認証サーバーは、適切なセキュリティ グループにこれらの新しいエンティティを割り当てます。CTS は各セキュリティ グループに、その範囲が CTS ドメイン内でグローバルな一意のセキュリティ グループ番号（16 ビット）を割り当てます。ルータ内のセキュリティ グループの数は、認証されたネットワーク エンティティの数に制限されます。セキュリティ グループ番号は、手動で設定する必要はありません。

デバイスが認証されると、CTS はそのデバイスから発信されるすべてのパケットに、デバイスのセキュリティ グループ番号が含まれている SGT をタグ付けします。タグ付けされたパケットはネットワークを通じて CTS ヘッダーで SGT を運びます。SGT は CTS ドメイン全体で送信元の許可を特定する単一ラベルです。SGT には送信元のセキュリティ グループが含まれるため、送信元として特定されます。宛先デバイスには、宛先グループ タグ（DGT）が割り当てられます。

（注） CTS パケット タグには、宛先デバイスのセキュリティ グループ番号は含まれません。

TrustSec SGT の処理：L2 SGT のインポジションと転送の設定方法

TrustSec SGT の処理：インターフェイスでの L2 SGT のインポジションと転送の手動による有効化

次の手順を実行して、Cisco TrustSec（CTS）のデバイス上のインターフェイスを手動で有効化します。これにより、デバイスは、ネットワーク全体で伝播するパケット内のセキュリティ グループ タグ（SGT）を追加し、スタティック認証ポリシーを実装できます。

手順の概要

1. **enable**
2. **configure terminal**

3. **interface** { **GigabitEthernet** *port* | **Vlan** *number*}
4. **cts manual**
5. **policy static sgt** *tag* [trusted]
6. **end**
7. **show cts interface** [**GigabitEthernet** *port* | **Vlan** *number* | **brief** | **summary**]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface** { **GigabitEthernet** *port*	**Vlan** *number*} 例： `Device(config)# interface gigabitethernet 0`	CTS SGT の認証と転送が有効なインターフェイスを開始します。
ステップ 4	**cts manual** 例： `Device(config-if)# cts manual`	CTS SGT 認証と転送のインターフェイスを有効化し、CTS 手動インターフェイス コンフィギュレーション モードを開始します。 （注） サブインターフェイスで **cts manual** コマンドを有効にするには、Dot1Q タグの追加バイトに対応するように IP MTU サイズを増やす必要があります。これは、Cisco IOS XE リリース 3.17 より前のリリースにのみ適用されます。
ステップ 5	**policy static sgt** *tag* [trusted] 例： `Device(config-if-cts-manual)# policy static sgt 100 trusted`	SGT の信頼性を定義するタグ付きパケットを使用して、CTS セキュリティ グループのスタティック認証ポリシーを設定します。
ステップ 6	**end** 例： `Device(config-if-cts-manual)# end`	CTS 手動インターフェイス コンフィギュレーション モードを終了し、特権 EXEC モードを開始します。
ステップ 7	**show cts interface** [**GigabitEthernet** *port*	**Vlan** *number*	**brief**	**summary**] 例： `Device# show cts interface brief`	インターフェイスの CTS 設定の統計情報を表示します。

例：

次に、**show cts interface brief** コマンドの出力例を示します。

Cisco ASR 1000 Series Aggregation Services Routers and Cisco Cloud Services Router 1000V Series

```
Device# show cts interface brief

Global Dot1x feature is Disabled
 Interface GigabitEthernet0/1/0:
     CTS is enabled, mode:    MANUAL
     IFC state:               OPEN
     Interface Active for 00:00:40.386
     Authentication Status:   NOT APPLICABLE
         Peer identity:       "unknown"
         Peer's advertised capabilities: ""
     Authorization Status:    NOT APPLICABLE
     SAP Status:              NOT APPLICABLE
     Propagate SGT:           Enabled
     Cache Info:
         Cache applied to link : NONE
```

Cisco 4400 Series Integrated Services Routers

```
Device# show cts interface brief

Interface GigabitEthernet0/1/0
    CTS is enabled, mode:     MANUAL
      Propagate SGT:          Enabled
      Static Ingress SGT Policy:
        Peer SGT:             100
        Peer SGT assignment:  Trusted
```

インターフェイスでの CTS SGT 伝達の無効化

ピア デバイスが SGT を受信できない場合、次の手順を実行して、インスタンス内のインターフェイスで CTS SGT 伝達を無効化します。

手順の概要

1. **enable**
2. **configure terminal**
3. **interface** {**GigabitEthernet***port* | **Vlan** *number*}
4. **cts manual**
5. **no propagate sgt**
6. **end**
7. **show cts interface** [**GigabitEthernet***port* | **Vlan** *number* | **brief** | **summary**]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface** {**GigabitEthernet***port* | **Vlan** *number*} 例： `Device(config)# interface gigabitethernet 0`	CTS SGT の認証と転送が有効なインターフェイスを開始します。
ステップ 4	**cts manual** 例： `Device(config-if)# cts manual`	CTS SGT の承認と転送用のインターフェイスを有効化します。 CTS 手動インターフェイス コンフィギュレーション モードは、CTS パラメーターを設定できる場合に開始されます。
ステップ 5	**no propagate sgt** 例： `Device(config-if-cts-manual)# no propagate sgt`	ピア デバイスが SGT を受信できない状況では、インターフェイスの CTS SGT 伝達を無効化します。 （注） CTS SGT 伝達はデフォルトで有効化されています。ピアデバイスで CTS SGT 伝達を再度オンにする必要がある場合、**propagate sgt** コマンドを使用できます。 **no propagate sgt** コマンドが開始されると、SGT タグは L2 ヘッダーに追加できなくなります。
ステップ 6	**end** 例： `Device(config-if-cts-manual)# end`	CTS 手動インターフェイス コンフィギュレーション モードを終了し、特権 EXEC モードを開始します。

ステップ 7	**show cts interface** [**GigabitEthernet***port* | **Vlan** *number* | **brief** | **summary**]
	例：
	`Device# show cts interface brief`
	`Global Dot1x feature is Disabled`
	`Interface GigabitEthernet0:`
	`CTS is enabled, mode: MANUAL`
	`IFC state: OPEN`
	`Authentication Status: NOT APPLICABLE`
	`Peer identity: "unknown"`
	`Peer's advertised capabilities: ""`
		インターフェイスで CTS SGT 伝達が無効化されていることを確認するため、CTS 設定の統計情報を表示します。

	コマンドまたはアクション	目的
	Authorization Status: NOT APPLICABLE SAP Status: NOT APPLICABLE Propagate SGT: Disabled Cache Info: Cache applied to link : NONE	

TrustSec SGT の処理：L2 SGT のインポジションと転送に関する追加情報

関連資料

関連項目	マニュアル タイトル
セキュリティ コマンド	『Cisco IOS Security Command Reference: Commands A to C』
	『Cisco IOS Security Command Reference: Commands D to L』
	『Cisco IOS Security Command Reference: Commands M to R』
	『Cisco IOS Security Command Reference: Commands S to Z』
Cisco TrustSec スイッチ	『Cisco TrustSec スイッチ コンフィギュレーション ガイド』

MIB

MIB	MIB のリンク
CISCO-TRUSTSEC-SXP-MIB	選択したプラットフォーム、Cisco ソフトウェア リリース、およびフィーチャ セットの MIB を検索してダウンロードする場合は、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

シスコのテクニカル サポート

説明	リンク
右の URL にアクセスして、シスコのテクニカル サポートを最大限に活用してください。これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

TrustSec SGT の処理：L2 SGT のインポジションと転送の機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *119 : TrustSec SGT* の処理：*L2 SGT* のインポジションと転送の機能情報

機能名	リリース	機能情報
TrustSec SGT の処理：L2 SGT のインポジションと転送		この機能により、ルータのインターフェイスは CTS を手動で有効化できるようになるため、ルータはセキュリティ グループ タグ（SGT）を、CTS ヘッダー内でネットワーク全体に運ばれるパケットに挿入できます。 • Cisco CSR 1000V ルータ • Cisco ISR 4400 ルータ • Catalyst 3850 シリーズ スイッチ • Catalyst 3650 シリーズ スイッチ • Cisco 5700 シリーズ ワイヤレス LAN コントローラ • Cisco Catalyst 4500E Supervisor Engine 7-E • Cisco Catalyst 4500E Supervisor Engine 7L-E • Cisco Catalyst 4500-X シリーズ スイッチ • Cisco Catalyst 4500E Supervisor Engine 8-E • Cisco Catalyst 3850 シリーズ スイッチ • Cisco Catalyst 3650 シリーズ スイッチ 次のコマンドが導入または変更されました。**cts manual**、**policy static sgt**、**propagate sgt**、**show cts interface**

第 85 章

Cisco TrustSec SGT Exchange Protocol IPv4 の前提条件

SXP を実装する前に、CTS-SXP ネットワークを確立する必要があります。CTS-SXP ネットワークには次の前提条件があります。

- Cisco TrustSec の機能を既存のルータで使用するには、Cisco TrustSec のセキュリティ ライセンスを購入していること。ルータを発注済みで Cisco TrustSec の機能が必要な場合は、発送前に、このライセンスが使用するルータにプリインストールされていること。
- すべてのネットワーク デバイスで CTS-SXP ソフトウェアを実行していること。
- すべてのネットワーク デバイス間が接続されていること。
- 認証には Cisco Identity Services Engine 1.0 が必要です。認証には Secure Access Control Server（ACS）Express Appliance サーバも使用できますが、CTS ではすべての ACS 機能がサポートされていません。ACS 5.1 が CTS-SXP ライセンスで動作していること。
- 異なるルータで異なる値に **retry open timer** コマンドを設定します。

Cisco TrustSec SGT Exchange Protocol IPv4 の制約事項

- IOS 機能の Cisco TrustSec サポートは、第 2 世代 Cisco サービス統合型ルータ（ISR G2）のみでサポートされています。
- CTS-SXP は物理インターフェイスだけでサポートされ、論理インターフェイスでサポートされません。

- CTS-SXP 検証は、IPv6 をサポートしていません。
- ルータにデフォルトのパスワードが実装されている場合、そのルータでの接続は、デフォルトパスワードを使用するようにパスワードを設定する必要があります。デフォルトのパスワードが設定されていない場合、そのルータでの接続はパスワード設定を使用しないように設定してください。パスワードオプションの設定は導入ネットワーク全体で一貫している必要があります。

Cisco TrustSec SGT Exchange Protocol IPv4 に関する情報

セキュリティ グループ タギング

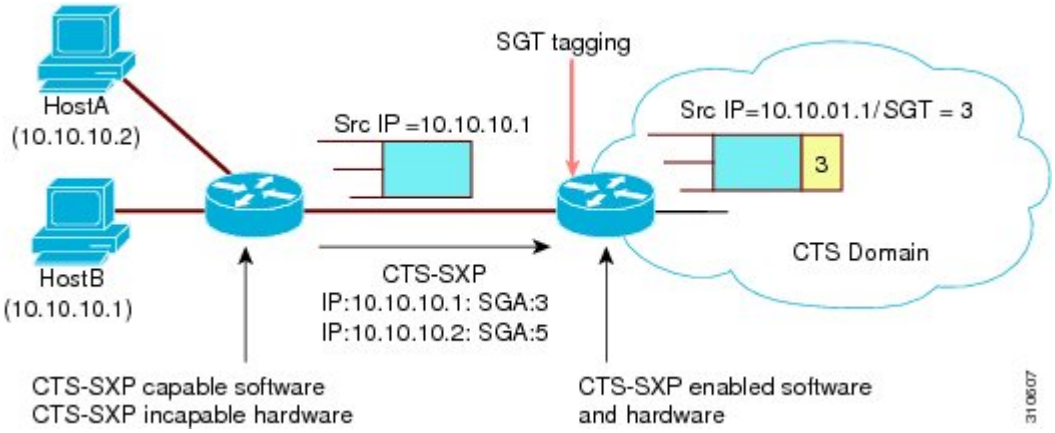
CTS-SXP は、認証時に取得したデバイスおよびユーザの識別情報を使用して、ネットワークに進入するパケットをセキュリティ グループ（SG）で分類します。このパケット分類は、CTS-SXP ネットワークへの入力時にパケットにタグ付けされることにより維持されます。タグによってパケットはデータ パス全体を通じて正しく識別され、セキュリティおよびその他のポリシー基準が適用されます。セキュリティ グループ タグ（SGT）によってエンドポイント デバイスはトラフィックをフィルタリングできるので、ネットワークへのアクセス コントロール ポリシーの適用が可能になります。

CTS-SXP によるレガシー アクセス ネットワークへの SGT の伝播

パケットへの SGT のタグ付けには、ハードウェアによるサポートが必要です。CTS 認証に参加できが、SGT でパケットをタグ付けするハードウェア機能を持たないデバイスが、ネットワーク内にある場合があります。ただし、CTS-SXP を使用する場合は、これらのデバイスが、IP と SGT のマッピングを CTS 対応ハードウェアがある CTS ピア デバイスに渡すことができます。

通常、CTS-SXP は CTS ドメイン エッジの入力アクセス レイヤ デバイスと CTS ドメイン内のディストリビューション レイヤ デバイス間で動作します。アクセス レイヤ デバイスは入力パケットの適切な SGT を判断するために、外部送信元デバイスの CTS 認証を実行します。アクセス レイヤ デバイスは IP デバイス トラッキングおよび（任意で）DHCP スヌーピングを使用して送信元デバイスの IP アドレスを学習し、その後 CTS-SXP を使用して送信元デバイスの IP アドレスおよびSGTを、ディストリビューション スイッチに渡します。CTS 対応のハードウェアを備えたディストリビューション スイッチは、この IP と SGT のマッピング情報を使用して、パケットに適切にタグを付け、セキュリティ グループ アクセス コントロール リスト（SGACL）ポリシーを強制します。次の図を参照してください。SGACL は、SGT とポリシーを関連付けます。ポリシーは、SGT タグ付けされたトラフィックが CTS ドメインから出力されると適用されます。

図 *17 : CTS-SXP* による *SGT* 情報の伝達方法



CTS ハードウェア サポート対象外のピアと CTS ハードウェア サポート対象のピア間の CTS-SXP 接続は、手動で設定する必要があります。CTS-CSXP 接続を設定する場合は、次の作業を実行する必要があります。

- CTS-SXP のデータの整合性と認証が必要な場合、同じ CTS-SXP パスワードを両方のピア デバイスで設定できます。CTS-SXP パスワードは各ピア接続に対して明示的に指定することも、デバイスに対してグローバルに設定することもできます。CTS-SXP パスワードは必須ではありませんが、推奨します。
- CTS-SXP 接続の各ピアは、CTS-SXP スピーカーまたは CTS-SXP リスナーとして設定する必要があります。スピーカー デバイスはリスナー デバイスに IP-to-SGT 情報を渡します。
- 各ピアの関係に使用する送信元 IP アドレスを指定できます。または、特定の送信元 IP アドレスが設定されていないピア接続に対して、デフォルトの送信元 IP アドレスを設定できます。送信元 IP アドレスが指定されていないと、デバイスはピアへの接続のインターフェイス IP アドレスを使用します。

CTS-SXP では複数のホップを許可します。つまり、CTS ハードウェア サポート対象外デバイスのピアが CTS ハードウェア サポートの対象外でもある場合、2 番目のピアはハードウェア対応ピアに到達するまで IP と SGT のマッピング情報の伝播を継続して、3 番目のピアへの CTS-SXP 接続を設定できます。デバイスは 1 つの CTS-SXP 接続では CTS-SXP リスナーとして、別の CTS-SXP 接続では CTS-SXP スピーカーとして設定できます。

CTS デバイスは TCP キープアライブ メカニズムを使用して、CTS-SXP ピアとの接続を維持します。ピア接続を確立または回復するために、デバイスは設定可能な再試行期間を使用して接続が成功するか、接続が設定から削除されるまで接続の確立を繰り返し試行します。

VRF-Aware CTS-SXP

仮想ルーティングおよびフォワーディング（VRF）の CTS-SXP の実装は、特定の VRF と CTS-SXP 接続をバインドします。CTS-SXP を有効化する前に、ネットワーク トポロジがレイヤ 2 またはレイヤ 3 の VPN に対して正しく設定されており、すべての VRF が設定されていることを前提としています。

CTS-SXP VRF サポートは、次のようにまとめることができます。

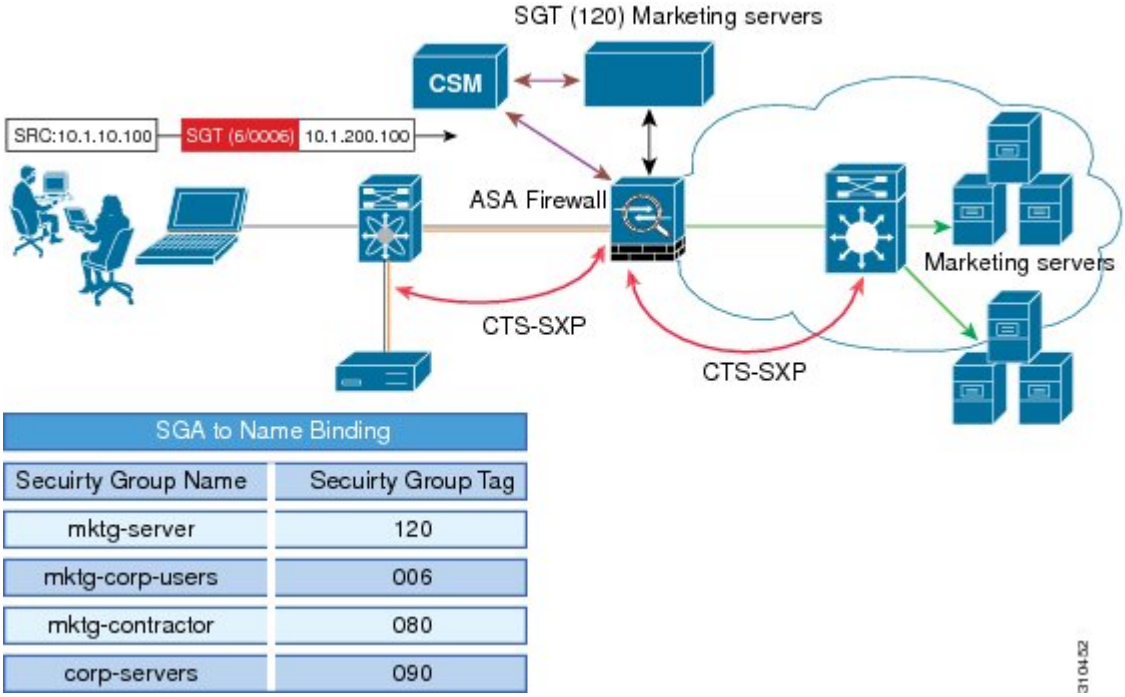
- 1 つの VRF には 1 つの CTS-SXP 接続のみをバインドできます。
- 別の VRF が重複する CTS-SXP ピアまたは送信元 IP アドレス持つ可能性があります。
- 1 つの VRF で学習（追加または削除）された IP と SGT のマッピングは、同じ VRF ドメインでのみ更新できます。CTS-SXP 接続は異なる VRF にバインドされたマッピングを更新できません。SXP 接続が VRF で終了しない場合は、その VRF の IP-SGT マッピングは SXP によって更新されません。
- CTS-SXP 検証は、送信元 IPv6 アドレスを使用した接続の確立をサポートしていません。ただし、VRF ドメイン内の 1 つの CTS-SXP 接続を IPv4 と IPv6 両方の IP と SGT のマッピングに転送できる場合は、VRF あたりで複数のアドレス ファミリがサポートされます。
- CTS-SXP には VRF あたりの接続数および IP と SGT のマッピング数に制限はありません。

セキュリティ グループ アクセスのゾーンベース ポリシー ファイアウォール

CTS-SXP は、セキュリティ グループ アクセス（SGA）ゾーンベース ポリシー ファイアウォール（ZBPF）を使用することで、ネットワーク デバイスの導入をネットワークのさらに別の場所へ拡張します。CTS-SXP は、次の図に示すとおり、ネットワーク全体に存在するプライマリ通信パスからアイデンティティ情報を学習するインラインデバイスを通じたアイデンティティ分散に使用されます。

セキュリティ グループ タグ（SGT）は、強制ポリシーを適用するため、SGA ZBPF によって使用されます。IP と SGT のマッピング情報は、CTS-SXP から学習します。パケットを受信すると、パケット内の送信元と宛先の IP アドレスは、送信元と宛先のタグを派生させるために使用されます。アイデンティティ ファイアウォールは、属性の 1 つに SGT がある、設定されたポリシーに基づいて、受信した IP パケットにポリシーを適用します。

図 *18* : ネットワーク全体の *CTS-SXP SGA ZBPF* 分散パス



Cisco TrustSec SGT Exchange Protocol IPv4 の設定方法

CTS-SXP の有効化

手順の概要

1. **enable**
2. **configure terminal**
3. **cts sxp enable**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例：	グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
	`Device# configure terminal`	
ステップ 3	**cts sxp enable** 例： `Device(config)# cts sxp enable`	設定された任意のピア接続に対して CTS-SXP 接続を有効化します。 （注） ピア接続が設定されていることを確認します。ピア接続が設定されていない場合、CTS-SXP 接続はそれらとは確立できません。

CTS-SXP ピア接続の設定

CTS-SXP ピア接続を両方のデバイスで設定する必要があります。一方のデバイスはスピーカーで、他方のデバイスはリスナーになります。パスワード保護を使用している場合は、必ず両エンドに同じパスワードを使用してください。

（注） デフォルトの CTS-SXP 送信元 IP アドレスが設定されていない場合に、接続の CTS-SXP 送信元アドレスを設定しないと、Cisco TrustSec ソフトウェアは既存のローカル IP アドレスから CTS-SXP 送信元 IP アドレスを抽出します。CTS-SXP 送信元 IP アドレスは、ルータから開始される TCP 接続ごとに異なる場合があります。

手順の概要

1. **enable**
2. **configure terminal**
3. **cts sxp connection peer** *ipv4-address* {**source** | **password**} {**default** | **none**} **mode** {**local** | **peer**} [[**listener** | **speaker**] [**vrf** *vrf-name*]]
4. **exit**
5. **show cts sxp** {**connections** | **sgt-map**} [**brief** | **vrf** *vrf-name*]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例：	グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
	`Device# configure terminal`	
ステップ 3	**cts sxp connection peer** *ipv4-address* {**source** | **password**} {**default** | **none**} **mode** {**local** | **peer**} [[**listener** | **speaker**] [**vrf** *vrf-name*]] 例： `Device(config)# cts sxp connection peer 10.20.2.2 password default mode local speaker`	CTS-SXP ピア アドレス接続を設定します。 **source** キーワードには発信元デバイスの IPv4 アドレスを指定します。接続アドレスが指定されていない場合、デフォルトの送信元アドレス（設定されている場合）、またはポートのアドレスを使用します。 **password** キーワードには、CTS-SXP で接続に使用するパスワードを指定します。次のオプションがあります。 • **default**：**cts sxp default password** コマンドを使用して設定したデフォルトの CTS-SXP パスワードを使用します。 • **none**：パスワードは使用されません。 **mode** キーワードでは、リモートピアデバイスのロールを指定します。 • **local**：指定したモードはローカルデバイスを参照します。 • **peer**：指定したモードはピアデバイスを参照します。 • **listener**：このデバイスが接続の際にリスナーになります。 • **speaker**：接続の際にこのデバイスがスピーカーになります。これはデフォルトです。 オプションの **vrf** キーワードでは、ピアに対する VRF を指定します。デフォルトはデフォルト VRF です。
ステップ 4	**exit** 例： `Device# exit`	グローバル コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。
ステップ 5	**show cts sxp** {**connections** | **sgt-map**} [**brief** | **vrf** *vrf-name*] 例： `Device# show cts sxp connections`	（オプション）CTS-SXP のステータスと接続を表示します。

デフォルトの CTS-SXP パスワードの設定

手順の概要

1. **enable**
2. **configure terminal**
3. **cts sxp default password** [**0** | **6** | **7**] *password*
4. **exit**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**cts sxp default password** [**0** | **6** | **7**] *password* 例： `Device(config)# cts sxp default password Cisco123`	CTS-SXP のデフォルト パスワードを設定します。クリアテキストパスワード（**0**を使用するかオプションなし）または暗号化パスワード（**6** または **7** オプションを使用）を入力できます。パスワードの最大長は 32 文字です。 （注） デフォルトでは、CTS-SXP は接続のセットアップ時にパスワードを使用しません。
ステップ 4	**exit** 例： `Device# exit`	グローバル コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

デフォルトの CTS-SXP 送信元 IP アドレスの設定

手順の概要

1. **enable**
2. **configure terminal**
3. **cts sxp default source-ip** *src-ip-addr*
4. **exit**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**cts sxp default source-ip** *src-ip-addr* 例： `Device(config)# cts sxp default source-ip 10.20.2.2`	CTS-SXP デフォルトの送信元 IP アドレスを設定します。これは、送信元IPアドレスが指定されていないすべての新しい TCP 接続に使用されます。 （注） デフォルトの CTS-SXP 送信元 IP アドレスが設定されている場合も、既存の TCP 接続には影響しません。
ステップ 4	**exit** 例： `Device# exit`	グローバル コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

CTS-SXP の復帰期間の設定

ピアが CTS-SXP 接続を終了すると、内部ホールドダウン タイマーが開始されます。内部ホールドダウン タイマーが終了する前にピアが再接続すると、CTS-SXP 復帰期間タイマーが開始されます。CTS-SXP 復帰期間タイマーがアクティブな間、CTS ソフトウェアは前回の接続で学習した SGT マッピング エントリを保持し、無効なエントリを削除します。デフォルト値は 120 秒（2 分）です。CTS-SXP 復帰期間を 0 秒に設定すると、タイマーがディセーブルになり、前回の接続のすべてのエントリが削除されます。

手順の概要

1. **enable**
2. **configure terminal**
3. **cts sxp reconciliation period** *seconds*
4. **exit**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**cts sxp reconciliation period** *seconds* 例： `Device(config)# cts sxp reconciliation period 150`	CTS-SXP 復帰タイマーを秒単位で設定します。範囲は 0 ～ 64000 です。デフォルトは 120 です。
ステップ 4	**exit** 例： `Device# exit`	グローバル コンフィギュレーション モードを終了し、特権 EXEC モードを開始します。

CTS-SXP 再試行期間の設定

CTS-SXP 再試行期間によって、CTS ソフトウェアが CTS-SXP 接続を再試行する頻度が決まります。CTS-SXP 接続が正常に確立されなかった場合、CTS ソフトウェアは CTS-SXP 再試行期間タイマーの終了後に、新たな接続の確立を試行します。デフォルト値は2分です。CTS-SXP 再試行期間を 0 秒に設定するとタイマーは無効になり、接続は再試行されません。

手順の概要

1. **enable**
2. **configure terminal**
3. **cts sxp retry period** *seconds*
4. **exit**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。

	コマンドまたはアクション	目的
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**cts sxp retry period** *seconds* 例： `Device(config)# cts sxp retry period 160`	CTS-SXP 再試行タイマーを秒単位で設定します。範囲は 0 ～ 64000 です。デフォルトは 120 です。
ステップ 4	**exit** 例： `Device# exit`	グローバル コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

IP と SGT のマッピング変更をキャプチャする Syslog の作成

手順の概要

1. **enable**
2. **configure terminal**
3. **cts sxp log binding-changes**
4. **exit**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**cts sxp log binding-changes** 例： `Device(config)# cts sxp log binding-changes`	IP と SGT バインド変更のロギングを有効にすると、IP と SGT バインディングの変更（追加、削除、変更）が発生するたびに CTS-SXP の syslog （sev 5 syslog）が生成されます。これらの変更は CTS-SXP 接続で学習されて伝播されます。

	コマンドまたはアクション	目的
		（注） このロギング機能は、デフォルトではディセーブルになっています。
ステップ 4	**exit** 例： `Device# exit`	グローバル コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

セキュリティ グループ アクセスのゾーンベース ポリシー ファイアウォールのクラス マップの設定

このタスクを実行して、セキュリティ グループ アクセス（SGA）ゾーンベース ポリシー ファイアウォールのネットワーク トラフィックを分類するためのクラス マップを設定します。

（注） 少なくとも 1 つの手順を実行する必要があります。

ゾーンベース ファイアウォール ポリシーは、フィルタリングにセキュリティ グループ タグの ID を使用します。ゾーンベース ファイアウォール ポリシーでは、ポリシーと一致するのは、セッションを作成した最初のパケットのみです。このフローの後続パケットは、設定されたポリシー内のフィルタと一致しませんが、セッションとは直接一致します。後続パケットに関連する統計情報は、検査アクションの一部として表示されます。

手順の概要

1. **enable**
2. **configure terminal**
3. **object-group security** *name*
4. **security-group tag-id** *sgt-id*
5. **group-object** *name*
6. **description** *text*
7. **exit**
8. **class-map type inspect** [**match-any** | **match-all**] *class-map-name*
9. **match group-object security source** *name*
10. **match group-object security destination** *name*
11. **end**
12. **show object-group** [*name*]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**object-group security** *name* 例： `Device(config)# object-group security myobject1a`	オブジェクト グループを作成して、特定のユーザまたはエンドポイントから受信するトラフィックを特定し、オブジェクトグループのアイデンティティ モードに入ります。
ステップ 4	**security-group tag-id** *sgt-id* 例： `Device(config-object-group)# security-group tag-id 120`	SGT ID 番号を使用して、セキュリティ グループのメンバーシップを指定します。この番号は 1 ～ 65535 ですこのコマンドを使用すると、複数のセキュリティ グループを指定できます。
ステップ 5	**group-object** *name* 例： `Device(config-object-group)# group-object admin`	（オプション）ネストされた参照を、ユーザ グループのタイプに指定します。このコマンドを使用すると、複数のネストされたユーザ グループを指定できます。
ステップ 6	**description** *text* 例： `Device(config-object-group)# description my sgtinfo`	（オプション）セキュリティ グループに関する情報を定義します。
ステップ 7	**exit** 例： `Device(config-object-group)# exit`	オブジェクトグループ アイデンティティ モードを終了し、グローバル コンフィギュレーション モードを開始します。
ステップ 8	**class-map type inspect** [**match-any** | **match-all**] *class-map-name* 例： `Device(config)# class-map type inspect match-any myclass1`	レイヤ 3 またはレイヤ 4 の検査タイプ クラス マップを作成し、クラスマップ コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 9	**match group-object security source** *name* 例： `Device(config-cmap)# match group-object security source myobject1`	セキュリティ グループ内のユーザからのトラフィックと一致させます。
ステップ 10	**match group-object security destination** *name* 例： `Device(config-cmap)# match group-object security destination myobject1`	セキュリティ グループ内のユーザのトラフィックと一致させます。
ステップ 11	**end** 例： `Device(config-cmap)# end`	クラスマップ コンフィギュレーション モードを終了し、特権 EXEC モードを開始します。
ステップ 12	**show object-group** [*name*] 例： `Device# show object-group admin`	（オプション）すべてのユーザ グループのコンテンツを表示します。オプションとして、*name* 引数を使用すると、単一グループの情報が表示されます。

セキュリティ グループ アクセスのゾーンベース ポリシー ファイアウォールのポリシー マップの作成

このタスクを実行して、ゾーンペアに接続する、セキュリティグループアクセス（SGA）ゾーンベース ポリシー ファイアウォールのポリシー マップを作成します。また、このタスクは、セキュリティ ゾーンに属するインターフェイス上で、セキュリティ グループ タグ（SGT）交換プロトコル（SXP）またはL2タグ付きトラフィックと動作するよう、アイデンティティファイアウォール（IDFW）を設定します。

手順の概要

1. **enable**
2. **configure terminal**
3. **policy-map type inspect** *policy-map-name*
4. **class type inspect** *class-name*
5. **inspect**
6. **exit**
7. **zone-pair security** *zone-pair-name* **source** *source-zone* **destination** *destination-zone*
8. **service-policy type inspect** *policy-map-name*
9. **end**
10. **interface** *type number*
11. **zone-member security** *zone-name*

12. **cts manual**
13. **no propagate sgt**
14. **policy static sgt** *tag* [**trusted**]
15. **exit**
16. **show policy-map type inspect zone-pair session**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**policy-map type inspect** *policy-map-name* 例： `Device(config)# policy-map type inspect z1z2-policy`	レイヤ 3 またはレイヤ 4 の検査タイプ ポリシーマップを作成します。 • ポリシーマップ コンフィギュレーション モードを開始します。
ステップ 4	**class type inspect** *class-name* 例： `Device(config-pmap)# class type inspect cmap-1`	アクションを実行する対象のトラフィック（クラス）を指定し、ポリシー マップ クラス コンフィギュレーション モードを開始します。
ステップ 5	**inspect** 例： `Device(config-pmap-c)# inspect`	パケット インスペクションを有効化します。
ステップ 6	**exit** 例： `Device(config-pmap-c)# exit`	ポリシーマップ クラス コンフィギュレーション モードを終了し、グローバルコンフィギュレーション モードを開始します。
ステップ 7	**zone-pair security** *zone-pair-name* **source** *source-zone* **destination** *destination-zone* 例： `Device(config)# zone-pair security z1z2 source z1 destination z2`	ゾーン ペアを作成し、セキュリティ ゾーン コンフィギュレーション モードを開始します。 （注） ポリシーを適用するには、ゾーン ペアを設定する必要があります。

	コマンドまたはアクション	目的
ステップ 8	**service-policy type inspect** *policy-map-name* 例： `Device(config-sec-zone)# service-policy type inspect z1z2-policy2`	ファイアウォール ポリシー マップを宛先ゾーン ペアに付加します。 （注） ゾーンのペア間でポリシーが設定されない場合、トラフィックはデフォルトでドロップされます。
ステップ 9	**end** 例： `Device(config-sec-zone)# end`	セキュリティ ゾーン コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードを開始します。
ステップ 10	**interface** *type number* 例： `Device(config)# interface GigabitEthernet 0/1/1`	インターフェイスを設定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 11	**zone-member security** *zone-name* 例： `Device(config-if)# zone-member security Inside`	インターフェイスを指定したセキュリティ ゾーンに割り当てます。 （注） インターフェイスをセキュリティ ゾーンのメンバーにした場合、方向に関係なくインターフェイスを通過するすべてのトラフィック（ルータ宛のトラフィックまたはルータ発信のトラフィックを除く）は、デフォルトでドロップされます。トラフィックがインターフェイス通過するには、ゾーンをポリシーの適用先のゾーン ペアの一部にする必要があります。ポリシーがトラフィックを許可すると、トラフィックはそのインターフェイスを通過できます。
ステップ 12	**cts manual** 例： `Device(config-if)# cts manual`	Cisco TrustSec Security（CTS）SGT 認証と転送のインターフェイスを有効化し、CTS 手動インターフェイス コンフィギュレーション モードを開始します。
ステップ 13	**no propagate sgt** 例： `Device(config-if-cts-manual)# no propagate sgt`	CTS インターフェイスで レイヤ 2 の SGT 伝達を無効化します。

	コマンドまたはアクション	目的
ステップ 14	**policy static sgt** *tag* [**trusted**] 例： `Device(config-if-cts-manual)# policy static sgt 100 trusted`	SGT の信頼性を定義するタグ付きパケットを使用して、CTS セキュリティ グループのスタティック認証ポリシーを設定します。
ステップ 15	**exit** 例： `Device(config-if)# exit`	セキュリティ ゾーン コンフィギュレーション モードを終了し、特権 EXEC モードを開始します。
ステップ 16	**show policy-map type inspect zone-pair session** 例： `Device# show policy-map type inspect zone-pair session`	（オプション）指定されたゾーン ペアのポリシーマップアプリケーションが原因で作成された、Cisco IOS ステートフル パケット インスペクション セッションを表示します。 （注） クラスマップ フィールドの下に表示される情報は、接続開始トラフィックのみに属するトラフィックのトラフィック レート（ビット/秒）です。接続セットアップ レートが非常に高く、レートが計算される複数のインターバルにわたって高い接続セットアップ レートが持続する場合を除き、接続に関する意味のあるデータは表示されません。

例：

次の出力例は、**show policy-map type inspect zone-pair session** コマンドによって表示される、指定されたゾーンペアのポリシーマップ アプリケーションが原因で作成された、Cisco IOS ステートフル パケット インスペクション セッションに関する情報を示します。

```
Device# show policy-map type inspect zone-pair session

Zone-pair: in-out
 Service-policy inspect : test

   Class-map: test (match-any)
     Match: group-object security source sgt
     Inspect
       Established Sessions
        Session 113EF68C (192.2.2.1:8)=>(198.51.100.252:153) icmp SIS_OPEN
         Created 00:00:02, Last heard 00:00:02
         Bytes sent (initiator:responder) [360:360]


   Class-map: class-default (match-any)
```

```
Match: any
Drop (default action)
  310 packets, 37380 bytes
```

Cisco TrustSec SGT Exchange Protocol IPv4 の設定例

例：CTS-SXP ピア接続のイネーブル化と設定

次に、CTS-SXP をイネーブルにし、Device_A（スピーカー）で Device_B（リスナー）への SXP ピア接続を設定する例を示します。

```
Device# configure terminal
Device_A(config)# cts sxp enable
Device_A(config)# cts sxp default password Cisco123
Device_A(config)# cts sxp default source-ip 10.10.1.1
Device_A(config)# cts sxp connection peer 10.20.2.2 password default mode local speaker
```

次に、Device_B（リスナー）で Device_A（スピーカー）への CTS-SXP ピア接続を設定する例を示します。

```
Device# configure terminal
Device_B(config)# cts sxp enable
Device_B(config)# cts sxp default password Cisco123
Device_B(config)# cts sxp default source-ip 10.20.2.2
Device_B(config)# cts sxp connection peer 10.10.1.1 password default mode local listener
```

次に、CTS-SXP 接続を表示する **show cts sxp connections** コマンドの出力例を示します。

```
Device_B# show cts sxp connections

 SXP              : Enabled
 Default Password : Set
 Default Source IP: 10.10.1.1
Connection retry open period: 10 secs
Reconcile period: 120 secs
Retry open timer is not running
----------------------------------------------
Peer IP          : 10.20.2.2
Source IP        : 10.10.1.1
Conn status      : On
Connection mode  : SXP Listener
Connection inst# : 1
TCP conn fd      : 1
TCP conn password: default SXP password
Duration since last state change: 0:00:21:25 (dd:hr:mm:sec)
Total num of SXP Connections = 1
```

例：セキュリティ グループ アクセスのゾーンベース ポリシー ファイアウォールの設定

次の例は、SGA ゾーンベース ポリシー ファイアウォールのクラス マップとポリシー マップの設定を示します。

```
Device(config)# object-group security myobject1
Device(config-object-group)# security-group tag-id 1
Device(config-object-group)# exit
Device(config)# object-group security myobject2
Device(config-object-group)# security-group tag-id 2
Device(config-object-group)# exit
Device(config)# object-group security myobject3
Device(config-object-group)# security-group tag-id 3
Device(config-object-group)# exit
Device(config)# object-group security myobject4
Device(config-object-group)# security-group tag-id 4
Device(config-object-group)# exit

Device(config)# class-map type inspect match-any myclass1
Device(config-cmap)# match group-object security source myobject1
Device(config-cmap)# exit
Device(config)# class-map type inspect match-any myclass2
Device(config-cmap)# match group-object security source myobject2
Device(config-cmap)# exit
Device(config)# class-map type inspect match-any myclass3
Device(config-cmap)# match group-object security source myobject3
Device(config-cmap)# exit
Device(config)# class-map type inspect match-any myclass4
Device(config-cmap)# match group-object security source myobject4
Device(config-cmap)# exit

Device(config)# policy-map type inspect InsideOutside
Device(config-pmap)# class type inspect myclass1
Device(config-pmap-c)# pass
Device(config-pmap-c)# exit
Device(config-pmap)# class type inspect myclass2
Device(config-pmap-c)# drop log
Device(config-pmap-c)# exit

Device(config)# policy-map type inspect OutsideInside
Device(config-pmap)# class type inspect myclass3
Device(config-pmap-c)# pass
Device(config-pmap-c)# exit
Device(config-pmap)# class type inspect myclass4
Device(config-pmap-c)# drop
Device(config-pmap-c)# exit

Device(config)# zone-pair security Inside
Device(config-sec-zone)# description Firewall Inside Zone
Device(config-sec-zone)# exit

Device(config)# zone-pair security Outside
Device(config-sec-zone)# description Firewall Outside Zone
Device(config-sec-zone)# exit

Device(config)# zone-pair security InsideOutside source Inside destination Outside
Device(config-sec-zone)# description Firewall ZonePair Inside Outside
Device(config-sec-zone)# service-policy type inspect InsideOutside
```

```
Device(config-sec-zone)# exit

Device(config)# zone-pair security OutsideInside source Outside destination Inside
Device(config-sec-zone)# description Firewall ZonePair Outside Inside
Device(config-sec-zone)# service-policy type inspect OutsideInside
Device(config-sec-zone)# exit

Device(config)# interface Gigabit 0/1/1
Device(config-if)# zone-member security Inside
Device(config-if)# exit
```

TrustSec SGT の処理：L2 SGT のインポジションと転送に関する追加情報

関連資料

関連項目	マニュアル タイトル
セキュリティ コマンド	『Cisco IOS Security Command Reference: Commands A to C』
	『Cisco IOS Security Command Reference: Commands D to L』
	『Cisco IOS Security Command Reference: Commands M to R』
	『Cisco IOS Security Command Reference: Commands S to Z』
Cisco TrustSec スイッチ	『Cisco TrustSec スイッチ コンフィギュレーション ガイド』

MIB

MIB	MIB のリンク
CISCO-TRUSTSEC-SXP-MIB	選択したプラットフォーム、Cisco ソフトウェア リリース、およびフィーチャ セットの MIB を検索してダウンロードする場合は、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

シスコのテクニカル サポート

説明	リンク
右の URL にアクセスして、シスコのテクニカル サポートを最大限に活用してください。これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

Cisco TrustSec SGT Exchange Protocol IPv4 の機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *120 : Cisco TrustSec SGT Exchange Protocol IPv4* の機能情報

機能名	リリース	機能情報
Cisco TrustSec SGT Exchange Protocol IPv4		セキュリティ グループ タグ（SGT）交換プロトコル（SXP）は、CTS をサポートする複数のプロトコルの 1 つであり、本書では CTS-SXP と呼びます。CTS-SXP は、パケットのタグ付け機能がないネットワーク デバイス全体に IP-to-SGT バインドの情報を伝播する、制御プロトコルです。CTS-SXP は、ネットワーク上のアップストリーム デバイスへの認証ポイントから SGT バインドへの IP を渡します。これにより、スイッチ、ルータ、ファイアウォールのセキュリティ サービスは、アクセス デバイスから学習したアイデンティティ情報を伝えることができます。 次のコマンドが導入または変更されました。**cts sxp enable, cts sxp connection peer**、**show cts sxp**、**cts sxp default source-ip, cts sxp reconciliation period, cts sxp retry period, cts sxp log binding-changes**。

機能名	リリース	機能情報
TrustSec SG Firewall Enforcement IPv4		この機能は、CTS-SXP がセキュリティ グループ アクセス（SGA）ゾーンベース ポリシー ファイアウォール（ZBPF）を通じてネットワーク デバイスを拡張するのを支援します。 次のコマンドが導入または変更されました。**group-object**、**match group-object security**、**object-group security**、**policy static sgt**、および **security-group**。

第 86 章

双方向 SXP サポートの有効化

双方向 SXP サポート機能は、セキュリティ グループ タグ（SGT）交換プロトコル（SXP）バインドのサポートを追加することで、SXP バージョン 4 を使用した Cisco TrustSec の機能を強化します。このバインドは、単一の接続でスピーカーとリスナーどちらの方向へも伝播できます。

双方向 SXP サポートの前提条件

- Cisco TrustSec がデバイス上に設定されていること。詳細については、『*Cisco TrustSec Configuration Guide*』の「Cisco TrustSec Support for IOS」の章を参照してください。
- Cisco TrustSec の機能を既存のデバイスで使用するには、次のセキュリティライセンスのいずれかを購入していること。
  - IP Base ライセンス
  - LAN Base ライセンス

（注） LAN Base ライセンスは、Cisco IOS XE Everest 16.5.1 から使用できます。

  - IP サービスライセンス
- すべてのネットワークデバイスに接続が存在すること。

- Cisco TrustSec ソフトウェアをすべてのネットワークデバイス上で実行すること。

双方向 SXP サポートの制約事項

- 接続のそれぞれの端のピアは、**both** キーワードを使用して双方向接続として設定する必要があります。一方の端を **both** キーワードを使用した双方向接続として設定し、他方の端をスピーカーまたはリスナーとして設定（単方向接続）するのは、誤った設定です。

双方向 SXP サポートに関する情報

双方向 SXP サポートの概要

Cisco TrustSec は、信頼できるネットワーク デバイスのドメインを確立することによってセキュア ネットワークを構築します。ドメイン内の各デバイスは、そのピアによって認証されます。データを生成するピアはスピーカーで、対応するピアはリスナーになります。

双方向セキュリティ グループ タグ（SGT）交換プロトコル（SXP）の設定をサポートすることで、ピアはスピーカーとリスナーのどちらとしても動作し、単一の接続を使用する双方向の SXP バインドを伝播できるようになります。

双方向 SXP の設定は、IP アドレスのペア 1 組と管理されます。いずれかの端で、SXP 接続を開始するのはリスナーのみであり、スピーカーは着信接続を受け入れます。

図 *19 :* 双方向 *SXP* 接続

さらに、SXP バージョン 4（SXPv4）は、引き続きループ検出メカニズムをサポートしています（ネットワークの古いバインディングを防ぐため）。

双方向 SXP サポートを有効化する方法

双方向 SXP サポートの設定

手順の概要

1. **enable**
2. **configure terminal**
3. **cts sxp enable**

4. **cts sxp default password**
5. **cts sxp default source-ip**
6. **cts sxp connection peer** *ipv4-address* {**source** | **password**} {**default** | **none**} **mode** {**local** | **peer**} **both** [**vrf** *vrf-name*]
7. **cts sxp speaker hold-time** *minimum-period*
8. **cts sxp listener hold-time** *minimum-period maximum-period*
9. **exit**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**cts sxp enable** 例： `Device(config)# cts sxp enable`	Cisco TrustSec セキュリティ グループ タグ（SGT）交換プロトコル バージョン4（SXPv4）をネットワーク デバイスで有効にします。
ステップ 4	**cts sxp default password** 例： `Device(config)# cts sxp default password Cisco123`	（オプション）Cisco TrustSec SGT SXP のデフォルト パスワードを指定します。
ステップ 5	**cts sxp default source-ip** 例： `Device(config)# cts sxp default source-ip 10.20.2.2`	（オプション）Cisco TrustSec SGT SXP 送信元 IPv4 アドレスを設定します。
ステップ 6	**cts sxp connection peer** *ipv4-address* {**source** | **password**} {**default** | **none**} **mode** {**local** | **peer**} **both** [**vrf** *vrf-name*] 例： `Device(config)# cts sxp connection peer 10.20.2.2 password default mode local both`	双方向 SXP 設定用の Cisco TrustSec SXP ピア アドレス接続を設定します。**both** キーワードは、双方向 SXP 設定を設定します。 **source** キーワードには発信元デバイスの IPv4 アドレスを指定します。接続アドレスが指定されていない場合、デフォルトの送信元アドレス（設定されている場合）、またはポートのアドレスを使用します。

	コマンドまたはアクション	目的
		password キーワードには、Cisco TrustSec SXP で接続に使用するパスワードを指定します。次のオプションがあります。 • **default**：**cts sxp default password** コマンドを使用して設定した、デフォルトの Cisco TrustSec SXP パスワードを使用します。 • **none**：パスワードは使用されません。 **mode** キーワードでは、リモートピアデバイスのロールを指定します。 • **local**：指定したモードはローカルデバイスを参照します。 • **peer**：指定したモードはピアデバイスを参照します。 • **both**：デバイスが双方向 SXP 接続のスピーカーとリスナー両方であることを指定します。 オプションの **vrf** キーワードでは、ピアに対する VRF を指定します。デフォルトはデフォルト VRF です。
ステップ 7	**cts sxp speaker hold-time** *minimum-period* 例： `Device(config)# cts sxp speaker hold-time 950`	（オプション）Cisco TrustSec SGT SXPv4 用のスピーカー ネットワーク デバイスのグローバル ホールド時間（秒単位）を設定します。有効な範囲は 1 ～ 65534 です。デフォルトは 120 です。
ステップ 8	**cts sxp listener hold-time** *minimum-period maximum-period* 例： `Device(config)# cts sxp listener hold-time 750 1500`	（オプション）Cisco TrustSec SGT SXPv4 用のリスナー ネットワーク デバイスのグローバル ホールド時間（秒単位）を設定します。有効な範囲は 1 ～ 65534 です。デフォルトは 90 ～180 です。 （注） *maximum-period* 値は、*minimum-period* 値よりも大きいか等しくする必要があります。
ステップ 9	**exit** 例： `Device(config)# exit`	グローバル コンフィギュレーション モードを終了します。

双方向 SXP サポート設定の確認

手順の概要

1. **enable**
2. **show cts sxp** {**connections** | **sgt-map**} [**brief** | **vrf** *vrf-name*]

手順の詳細

ステップ 1 enable

特権 EXEC モードを有効にします。

- パスワードを入力します（要求された場合）。

例：

```
Device> enable
```

ステップ 2 show cts sxp {connections | sgt-map} [brief | vrf vrf-name]

Cisco TrustSec 交換プロトコル（SXP）のステータスと接続を表示します。

例：

```
Device# show cts sxp connections

SXP : Enabled
Highest Version Supported: 4
Default Password : Set
Default Source IP: Not Set
Connection retry open period: 120 secs
Reconcile period: 120 secs
Retry open timer is running
------------------------------------------------
Peer IP : 2.0.0.2
Source IP : 1.0.0.2
Conn status : On (Speaker) :: On (Listener)
Conn version : 4
Local mode : Both
Connection inst# : 1
TCP conn fd : 1(Speaker) 3(Listener)
TCP conn password: default SXP password
Duration since last state change: 1:03:38:03 (dd:hr:mm:sec) :: 0:00:00:46 (dd:hr:mm:sec)


Device# show cts sxp connection brief

SXP : Enabled
Highest Version Supported: 4
Default Password : Set
Default Source IP: Not Set
Connection retry open period: 120 secs
Reconcile period: 120 secs
Retry open timer is running
------------------------------------------------------
```

```
Peer_IP Source_IP Conn Status Duration
------------------------------------------------
2.0.0.2 1.0.0.2 On(Speaker)::On(Listener) 0:00:37:17 (dd:hr:mm:sec)::0:00:37:19 (dd:hr:mm:sec)
```

次のテーブルに、接続ステータス出力のさまざまなシナリオを示します。

表 *121 :* 接続ステータスの出力シナリオ

Node1	Node2	接続ステータスについての Node1 CLI 出力	接続ステータスについての Node2 CLI 出力
両方	両方	オン（スピーカー） オン（リスナー）	オン（スピーカー） オン（リスナー）
スピーカー	リスナー	オン	点灯
リスナー	スピーカー	オン	点灯

双方向 SXP サポートの設定例

例：双方向 SXP サポートの設定

次の例は、双方向 CTS-SXP を有効化し、Device_A 上の SXP ピア接続が Device_B に接続するよう設定する方法を示します。

```
Device_A> enable
Device_A# configure terminal
Device_A(config)# cts sxp enable
Device_A(config)# cts sxp default password Cisco123
Device_A(config)# cts sxp default source-ip 10.10.1.1
Device_A(config)# cts sxp connection peer 10.20.2.2 password default mode local both
Device_A(config)# exit
```

次の例は、Device_B 上の双方向 CTS-SXP ピア接続が Device_A に接続するように設定する方法を示します。

```
Device_B> enable
Device_B# configure terminal
Device_B(config)# cts sxp enable
Device_B(config)# cts sxp default password Password123
Device_B(config)# cts sxp default source-ip 10.20.2.2
Device_B(config)# cts sxp connection peer 10.10.1.1 password default mode local both
Device_B(config)# exit
```

双方向 SXP サポートに関する追加情報

関連資料

関連項目	マニュアル タイトル
セキュリティ コマンド	• 『Cisco IOS Security Command Reference: Commands A to C』 • 『Cisco IOS Security Command Reference: Commands D to L』 • 『Cisco IOS Security Command Reference: Commands M to R』 • 『Cisco IOS Security Command Reference: Commands S to Z』
Cisco TrustSec の設定	『*Cisco TrustSec Configuration Guide*』の「Cisco TrustSec Support for IOS」の章

シスコのテクニカル サポート

説明	リンク
シスコのサポート Web サイトでは、シスコの製品やテクノロジーに関するトラブルシューティングにお役立ていただけるように、マニュアルやツールをはじめとする豊富なオンライン リソースを提供しています。 お使いの製品のセキュリティ情報や技術情報を入手するために、Cisco Notification Service（Field Notice からアクセス）、Cisco Technical Services Newsletter、Really Simple Syndication（RSS）フィードなどの各種サービスに加入できます。 シスコのサポート Web サイトのツールにアクセスする際は、Cisco.com のユーザ ID およびパスワードが必要です。	http://www.cisco.com/support

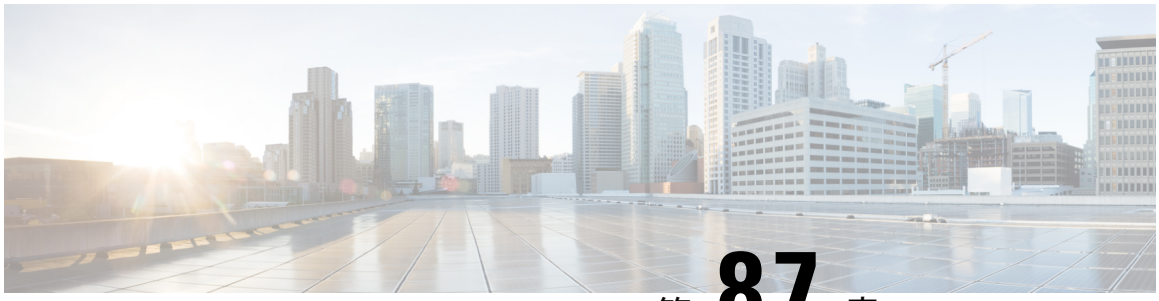
双方向 SXP サポートの機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *122 :* 双方向 *SXP* サポートの機能情報

機能名	リリース	機能情報
双方向 SXP サポート		双方向 SXP サポート機能は、セキュリティ グループ タグ（SGT）交換プロトコル（SXP）バインドのサポートを追加することで、SXP バージョン 4 を使用した Cisco TrustSec の機能を強化します。このバインドは、単一の接続でスピーカーとリスナーどちらの方向へも伝播できます。 • Cisco Catalyst 3750-X シリーズ スイッチ • Cisco Catalyst 3560-X シリーズ スイッチ • Cisco Catalyst 4500E Supervisor Engine 7-E • Cisco Catalyst 4500E Supervisor Engine 7L-E • Cisco Catalyst 4500-X シリーズ スイッチ • Cisco Catalyst 4500E Supervisor Engine 8-E • Cisco Catalyst 3850 シリーズ スイッチ • Cisco Catalyst 3650 シリーズ スイッチ 次のコマンドが導入または変更されました。**cts sxp connection peer**



第 87 章

Cisco TrustSec インターフェイスと SGT のマッピング

Cisco TrustSec インターフェイスと SGT のマッピング機能は、レイヤ 3 入力インターフェイス上のすべてのトラフィックを、セキュリティ グループ タグ（SGT）にバインドします。このマッピングを実装すると、Cisco TrustSec では、SGT を使用してさまざまな論理レイヤ 3 入力インターフェイスからトラフィックを分離できるようになります。

Cisco TrustSec インターフェイスと SGT のマッピングに関する情報

インターフェイスと SGT のマッピング

インターフェイスとセキュリティ グループ タグ（SGT）間のマッピングを使用して、基盤となる物理インターフェイスに関わらず、SGT を次の論理レイヤ 3 入力インターフェイスいずれかのトラフィックにマッピングします。

- レイヤ 3（ルーテッド）イーサネット インターフェイス
- レイヤ 3（ルーテッド）イーサネット 802.1Q サブインターフェイス
- トンネル インターフェイス

設定された SGT タグは、レイヤ 3 入力インターフェイスのすべてのトラフィックに割り当てられ、インライン タギングとポリシーの適用に使用できます。

バインディング送信元プライオリティ

Cisco TrustSec は完全優先方式で IP-SGT（IP アドレスからセキュリティ グループ タグへ）バインディング ソース間の競合を解決します。現在の優先順位の適用順序は、最小から最大まで、次のとおりです。

1. CLI：**cts role-based sgt-map sgt** コマンドを使用して設定されたバインド。
2. L3IF：一貫した L3IF-SGT（レイヤ 3 インターフェイスから SGT へ）マッピングやアイデンティティ ポート マッピングを使用する 1 つ以上のインターフェイスを通るパスを持つ FIB 転送エントリが原因で追加されたバインド。
3. SXP：SXP（SGT Exchange Protocol）ピアから学習されたバインド。
4. INTERNAL：ローカルで設定された IP アドレスとデバイス独自の SGT 間のバインド。

Cisco TrustSec インターフェイスと SGT のマッピングの設定方法

レイヤ 3 インターフェイスと SGT のマッピングの設定

手順の概要

1. **enable**
2. **configure terminal**
3. **interface** *type slot/port*
4. **cts role-based sgt-map sgt** *sgt-number*
5. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface** *type slot/port* 例： `Device(config)# interface gigabitEthernet 0/0`	インターフェイスを設定し、インターフェイス コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 4	**cts role-based sgt-map sgt** *sgt-number* 例： `Device(config-if)# cts role-based sgt-map sgt 77`	SGT は指定されたインターフェイスへの入力トラフィックに適用されます。 • *sgt-number*：セキュリティ グループ タグ（SGT）番号を指定します。有効値は 2 ～ 65519 です。
ステップ 5	**end** 例： `Device(config-if)# end`	インターフェイス コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

レイヤ 3 インターフェイスと SGT のマッピングの確認

手順の概要

1. **enable**
2. **show cts role-based sgt-map all**

手順の詳細

ステップ 1 enable

特権 EXEC モードを有効にします。

• パスワードを入力します（要求された場合）。

例：

```
Device> enable
```

ステップ 2 show cts role-based sgt-map all

レイヤ 3 インターフェイスの入力トラフィックに対するセキュリティ グループ タグ（SGT）マッピングを表示します。

例：

次は、**show cts role-based sgt-map all** コマンドからの出力例です。Cisco TrustSec インターフェイス と SGT のマッピング機能が実装されると、入力インターフェイスのトラフィックは、レイヤ 3 インターフェイス（L3IF）によって適切にタグ付けされます。この出力では、IP アドレスからセキュリティ グループ タグ（IP-SGT）バインディング ソースの優先方式を表示します（IP-SGT バインディング ソースの優先度について、詳細は「バインディング送信元プライオリティ」の項を参照）。

```
Device# show cts role-based sgt-map all

IP Address              SGT     Source
============================================
```

```
192.0.2.1               4       INTERNAL
192.0.2.5/24            3       L3IF
192.0.2.10/8            3       L3IF
192.0.2.20              5       CLI
198.51.100.1            4       INTERNAL
IP-SGT Active Bindings Summary
============================================
Total number of CLI      bindings = 1
Total number of L3IF     bindings = 2
Total number of INTERNAL bindings = 2
Total number of active   bindings = 5
```

Cisco TrustSec インターフェイスと SGT のマッピングの設定例

例：レイヤ 3 インターフェイスと SGT のマッピングの設定

次の例は、レイヤ 3 入力インターフェイスへのセキュリティ グループ タグ（SGT）のマッピング設定を示します。

```
Device> enable
Device# configure terminal
Device(config)# interface gigabitEthernet 0/0
Device(config-if)# cts role-based sgt-map sgt 77
Device(config-if)# end
```

Cisco TrustSec インターフェイスと SGT のマッピングに関する追加情報

関連資料

関連項目	マニュアル タイトル
セキュリティ コマンド	• 『Cisco IOS Security Command Reference Commands A to C』 • 『Cisco IOS Security Command Reference Commands D to L』 • 『Cisco IOS Security Command Reference Commands M to R』 • 『Cisco IOS Security Command Reference Commands S to Z』
Cisco TrustSec と SXP の設定	『Cisco TrustSec スイッチ コンフィギュレーション ガイド』

シスコのテクニカル サポート

説明	リンク
シスコのサポート Web サイトでは、シスコの製品やテクノロジーに関するトラブルシューティングにお役立ていただけるように、マニュアルやツールをはじめとする豊富なオンライン リソースを提供しています。 お使いの製品のセキュリティ情報や技術情報を入手するために、Cisco Notification Service（Field Notice からアクセス）、Cisco Technical Services Newsletter、Really Simple Syndication（RSS）フィードなどの各種サービスに加入できます。 シスコのサポート Web サイトのツールにアクセスする際は、Cisco.com のユーザ ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

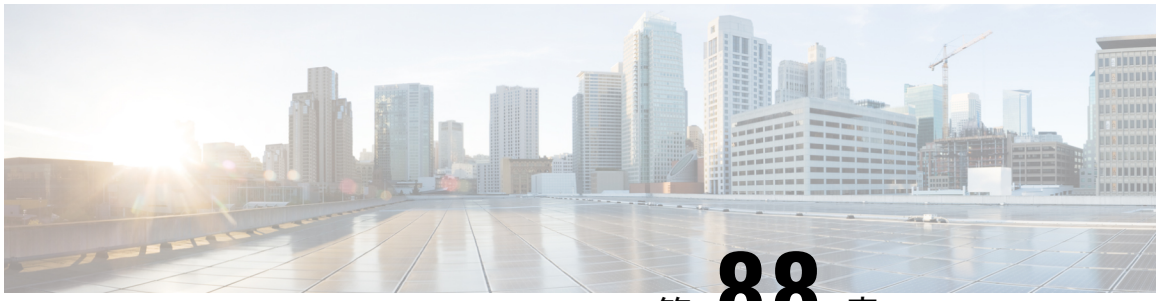
Cisco TrustSec インターフェイスと SGT のマッピングの機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *123 : Cisco TrustSec* インターフェイスと *SGT* のマッピングの機能情報

機能名	リリース	機能情報
Cisco TrustSec インターフェイスと SGT のマッピング		Cisco TrustSec インターフェイスと SGT のマッピング機能は、レイヤ3入力インターフェイス上のすべてのトラフィックを、セキュリティ グループ タグ（SGT）にバインドします。このマッピングを実装すると、Cisco TrustSec では、SGT を使用してさまざまな論理レイヤ3入力インターフェイスからトラフィックを分離できるようになります。 次のコマンドが導入または変更されました。**cts role-based sgt-map sgt**



第 88 章

Cisco TrustSec サブネットと SGT のマッピング

サブネットとセキュリティ グループ タグ（SGT）のマッピングは、指定したサブネット内のすべてのホスト アドレスに SGT をバインドします。このマッピングが実行されると、Cisco TrustSec により、指定のサブネットに属する送信元 IP アドレスを持つ任意の着信パケットに SGT が課せられます。

Cisco TrustSec サブネットと SGT のマッピングの制約事項

- /31 プレフィックスの IPv4 サブ ネットワークを拡張できません。
- サブネットホストアドレスは、**cts sxp mapping network-map** コマンドの *bindings* 引数が、指定されたサブネット内のサブネットホストの合計数より小さいか、バインド数が 0 の場合、SGT にバインドできません。
- SXP スピーカーおよびリスナーが SXPv3 以降のバージョンを実行している場合のみ、IPv6 拡張および伝播が実行されます。

Cisco TrustSec サブネットと SGT のマッピングに関する情報

IPv4 ネットワークでは、SXPv3 以降のバージョンは SXPv3 ピアからサブネットの network address/prefix ストリングを受信し、解析できます。SXP の以前のバージョンでは、SXP リス

ナー ピアにエクスポートする前に、サブネットのプレフィックスをホスト バインドのセットに変換します。

たとえば、IPv4 サブネット 198.1.1.0 /29 は次のように拡張されます（ホスト アドレスの 3 ビットのみ）。

- ホスト アドレス 198.1.1.1 から 198.1.1.7 はタグ付けされて SXP ピアに伝播します。
- ネットワーク、およびブロードキャスト アドレス 198.1.1.0 および 198.1.1.8 は、タグ付けされず、伝播しません。

（注） SXPv3 がエクスポートできるサブネットバインドの数を制限するには、**cts sxp mapping network-map** グローバル コンフィギュレーション コマンドを使用します。

サブネット バインディングは静的です。つまり、アクティブなホストは学習されません。これらは SGT インポジションおよび SGACL の適用にローカルで使用できます。サブネットと SGT のマッピングによってタグ付けされたパケットは、レイヤ 2 またはレイヤ 3 TrustSec リンクに伝播できます。

（注） IPv6 ネットワークの場合、SXPv3 は SXPv2 または SXPv1 ピアにサブネット バインディングをエクスポートできません。

Cisco TrustSec サブネットと SGT のマッピングの設定方法

サブネットと SGT のマッピングの設定

手順の概要

1. **enable**
2. **configure terminal**
3. **cts sxp mapping network-map** *bindings*
4. **cts role-based sgt-map** *ipv4-address* **sgt** *number*
5. **cts role-based sgt-map** *ipv6-address::prefix* **sgt** *number*
6. **exit**
7. **show running-config** | **include** *search-string*
8. **show cts sxp connections**
9. **show cts sxp sgt-map**
10. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**cts sxp mapping network-map** *bindings* 例： `Device(config)# cts sxp mapping network-map 10000`	サブネットと SGT のマッピングのホスト数の制限を設定します。*bindings* 引数は、SGT にバインドされ、SXP リスナーにエクスポートできる、0 ～ 65,535 のサブネット IP ホストの最大数を指定します。デフォルトは 0（実行される拡張なし）です。
ステップ 4	**cts role-based sgt-map** *ipv4-address* **sgt** *number* 例： `Device(config)# cts role-based sgt-map 10.10.10.10/29 sgt 1234`	（IPv4）CIDR 表記で IPv4 サブネットを指定します。 手順 3 で指定するバインディングの数は、サブネット上のホスト アドレスの数以上である必要があります（ネットワーク、およびブロードキャスト アドレスを除く）。**sgt** *number* キーワードペアでは、指定したサブネットの各ホストアドレスにバインドする SGT 番号を指定します。 • *ipv4-address*：ドット付き 10 進表記で IPv4 ネットワーク アドレスを指定します。 • *prefix*：（0 ～ 30）。ネットワーク アドレス内のビット数を指定します。 • **sgt** *number*：（0 ～ 65,535）。SGT 番号を指定します。
ステップ 5	**cts role-based sgt-map** *ipv6-address::prefix* **sgt** *number* 例： `Device(config)# cts role-based sgt-map 2020::/64 sgt 1234`	（IPv6）16 進数表記で IPv6 サブネットを指定します。 手順 3 で指定するバインディングの数は、サブネット上のホスト アドレスの数以上である必要があります（ネットワーク、およびブロードキャスト アドレスを除く）。**sgt** *number* キーワードペアでは、指定したサブネットの各ホストアドレスにバインドする SGT 番号を指定します。 • *ipv6-address*：ドット付き 10 進表記で IPv4 ネットワーク アドレスを指定します。

	コマンドまたはアクション	目的
		• *prefix*：（0 ～ 30）。ネットワーク アドレス内のビット数を指定します。 • **sgt** *number*：（0 ～ 65,535）。SGT 番号を指定します。
ステップ 6	**exit** 例： `Device(config)# exit`	グローバル コンフィギュレーション モードを終了します。

ステップ 7	**show running-config** | **include** *search-string*
	例：
	`Device# show running-config | include sgt 1234`
	`Device# show running-config | include network-map`
		cts role-based sgt-map コマンドと **cts sxp mapping network-map** コマンドが実行コンフィギュレーション内にあることを確認します。

ステップ 8	**show cts sxp connections** 例： `Device# show cts sxp connections`	SXP スピーカーとリスナーの接続と、動作ステータスを表示します。
ステップ 9	**show cts sxp sgt-map** 例： `Device# show cts sxp sgt-map`	SXP リスナーにエクスポートした IP と SGT のバインディングを表示します。
ステップ 10	**copy running-config startup-config** 例： `Device# copy running-config startup-config`	実行設定を、スタートアップ設定にコピーします。

Cisco TrustSec サブネットと SGT のマッピング：例

次の例は、SXPv3 を実行している 2 つのデバイス（Device 1 と Device 2）間の IPv4 サブネットと SGT のマッピングを設定する方法を示します。

Device 1（10.1.1.1）と Device 2（10.2.2.2）間の SXP スピーカー/リスナー ピアリングを設定します。

```
Device1# configure terminal
Device1(config)# cts sxp enable
Device1(config)# cts sxp default source-ip 10.1.1.1
Device1(config)# cts sxp default password 1syzygy1
Device1(config)# cts sxp connection peer 10.2.2.2 password default mode local speaker
```

Device 1 の SXP リスナーとして Device 2 を設定します。

```
Device2(config)# cts sxp enable
Device2(config)# cts sxp default source-ip 10.2.2.2
Device2(config)# cts sxp default password 1syzygy1
Device2(config)# cts sxp connection peer 10.1.1.1 password default mode local listener
```

Device 2 で、SXP 接続が動作していることを確認してください。

```
Device2# show cts sxp connections brief | include 10.1.1.1

     10.1.1.1          10.2.2.2          On                3:22:23:18 (dd:hr:mm:sec)
```

サブネットワークが Device 1 に拡張されるように設定します。

```
Device1(config)# cts sxp mapping network-map 10000
Device1(config)# cts role-based sgt-map 10.10.10.0/30 sgt 101
Device1(config)# cts role-based sgt-map 10.11.11.0/29 sgt 11111
Device1(config)# cts role-based sgt-map 172.168.1.0/28 sgt 65000
```

Device 2 で、Device 1 からのサブネットと SGT の拡張を確認します。ここには、10.10.10.0/30 サブネットワーク用の拡張が 2 個、10.11.11.0/29 サブネットワーク用の拡張が 6 個、172.168.1.0/28 サブネットワーク用の拡張が 14 個存在する必要があります。

```
Device2# show cts sxp sgt-map brief | include 101|11111|65000

IPv4,SGT: <10.10.10.1 , 101>
IPv4,SGT: <10.10.10.2 , 101>
IPv4,SGT: <10.11.11.1 , 11111>
IPv4,SGT: <10.11.11.2 , 11111>
IPv4,SGT: <10.11.11.3 , 11111>
IPv4,SGT: <10.11.11.4 , 11111>
IPv4,SGT: <10.11.11.5 , 11111>
IPv4,SGT: <10.11.11.6 , 11111>
IPv4,SGT: <172.168.1.1 , 65000>
IPv4,SGT: <172.168.1.2 , 65000>
IPv4,SGT: <172.168.1.3 , 65000>
IPv4,SGT: <172.168.1.4 , 65000>
IPv4,SGT: <172.168.1.5 , 65000>
IPv4,SGT: <172.168.1.6 , 65000>
IPv4,SGT: <172.168.1.7 , 65000>
IPv4,SGT: <172.168.1.8 , 65000>
IPv4,SGT: <172.168.1.9 , 65000>
IPv4,SGT: <172.168.1.10 , 65000>
IPv4,SGT: <172.168.1.11 , 65000>
IPv4,SGT: <172.168.1.12 , 65000>
IPv4,SGT: <172.168.1.13 , 65000>
IPv4,SGT: <172.168.1.14 , 65000>
```

Device 1 の拡張数を確認します。

```
Device1# show cts sxp sgt-map

IP-SGT Mappings expanded:22
There are no IP-SGT Mappings
```

Device 1 と Device 2 の設定を保存して、グローバル コンフィギュレーション モードを終了します。

```
Device1(config)# copy running-config startup-config
Device1(config)# exit

Device2(config)# copy running-config startup-config
Device2(config)# exit
```

その他の参考資料

関連資料

関連項目	マニュアル タイトル
セキュリティ コマンド	• 『Cisco IOS Security Command Reference Commands A to C』 • 『Cisco IOS Security Command Reference Commands D to L』 • 『Cisco IOS Security Command Reference Commands M to R』 • 『Cisco IOS Security Command Reference Commands S to Z』
Cisco TrustSec と SXP の設定	『Cisco TrustSec スイッチ コンフィギュレーション ガイド』
IPsec の設定	『Configuring Security for VPNs with IPsec』
IKEv2 の設定	『Configuring Internet Key Exchange Version 2 (IKEv2) and FlexVPN Site-to-Site』
Cisco Secure Access Control Server	『Configuration Guide for the Cisco Secure ACS』

シスコのテクニカル サポート

説明	リンク
右の URL にアクセスして、シスコのテクニカル サポートを最大限に活用してください。これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

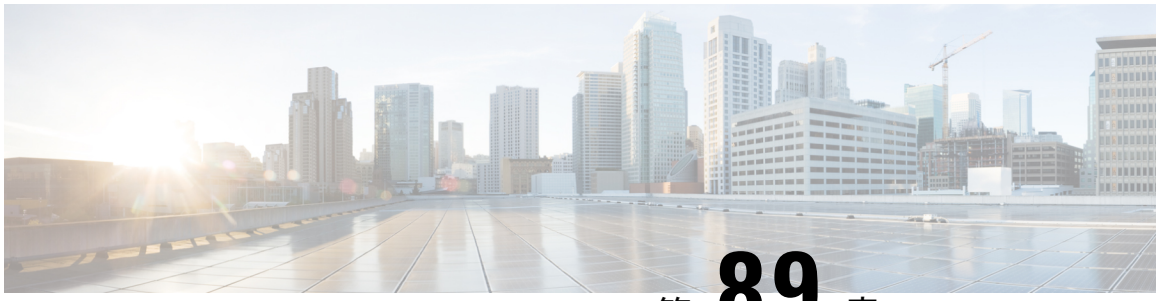
Cisco TrustSec サブネットと SGT のマッピングの機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *124 : Cisco TrustSec* サブネットと *SGT* のマッピングの機能情報

機能名	リリース	機能情報
Cisco TrustSec サブネットと SGT のマッピング		サブネットとセキュリティ グループ タグ（SGT）のマッピングは、指定したサブネット内のすべてのホスト アドレスに SGT をバインドします。このマッピングが実行されると、Cisco TrustSec により、指定のサブネットに属する送信元 IP アドレスを持つ任意の着信パケットに SGT が課せられます。 次のコマンドが導入されました：**cts sxp mapping network-map**



第 89 章

Cisco TrustSec フィールドの Flexible NetFlow エクスポート

Cisco TrustSec フィールドの Flexible NetFlow エクスポートでは、Flexible Netflow（FNF）フローレコード内の Cisco TrustSec フィールドをサポートし、Cisco TrustSec 導入の標準から外れた動作のモニタ、トラブルシューティング、および特定を支援します。

このモジュールでは、Cisco TrustSec と FNF のインタラクションについてと、NetFlow バージョン 9 フロー レコードの Cisco TrustSec フィールドを設定しエクスポートする方法を説明します。

Cisco TrustSec フィールドの Flexible NetFlow エクスポートの制約事項

- Flexible Netflow（FNF）レコードでエクスポートされるセキュリティ グループ タグ（SGT）値は、次のシナリオではゼロになります。
  - パケットは、信頼されたインターフェイスから、ゼロの SGT 値とともに受信します。
  - パケットは SGT なしで受信します。
  - IP-SGT ルックアップ中に SGT が検出されません。

Cisco TrustSec フィールドの Flexible NetFlow エクスポートに関する情報

Flexible NetFlow の Cisco TrustSec フィールド

Flexible Netflow（FNF）フローレコード内の Cisco TrustSec フィールド、送信元セキュリティグループタグ（SGT）および宛先セキュリティグループタグ（DGT）は、管理者によるフローとアイデンティティ情報の関連付けに役立ちます。ネットワーク エンジニアは、これにより、顧客のネットワーク リソースおよびアプリケーション リソースの利用について詳しく理解できます。この情報を使用して、潜在的なセキュリティやポリシーの違反を検出して解決するために、アクセスおよびアプリケーション リソースを効率的に計画して割り当てることができます。

Cisco TrustSec フィールドは入力/出力 FNF、ユニキャスト/マルチキャスト トラフィックでサポートされています。

次のテーブルに、Cisco TrustSec 用の NetFlow V9 の企業固有フィールド タイプを示します。これは、Cisco TrustSec の送信元/宛先ソース グループ タグの FNF テンプレートで使用されます。

ID	説明
CTS_SRC_GROUP_TAG	Cisco Trusted Security 送信元グループ タグ
CTS_DST_GROUP_TAG	Cisco Trusted Security 宛先グループ タグ

FNF フロー レコードで既存の一致するフィールドに加えて、Cisco TrustSec フィールドが設定されます。次の設定を使用して、Cisco TrustSec フロー オブジェクトをキー フィールドまたは非キー フィールドとして FNF フロー レコードに追加し、パケット用の送信元と宛先のセキュリティ グループ タグを設定します。

- **match flow cts {source | destination} group-tag** コマンドは、キーフィールドとして Cisco TrustSec フィールドを指定するため、フローレコード以下で設定されます。キーフィールドはフローを差別化するものです。各フローのキーフィールドには、一連の一意の値が設定されています。フロー レコードにキー フィールドが含まれていない場合は、フロー モニタで使用することができません。
- **collect flow cts {source | destination} group-tag** コマンドは、非キーフィールドとして Cisco TrustSec フィールドを指定するため、フローレコード以下で設定されます。非キーフィールドの値は、フロー内のトラフィックに関する追加情報を提供するためにフローに追加されます。

フロー レコードは、フロー モニタ下で設定され、フロー モニタはインターフェイスに適用されます。FNF データをエクスポートするには、フローエクスポータを設定し、フローモニター以下に追加する必要があります。

Cisco TrustSec フィールドの Flexible NetFlow エクスポートの設定方法

フロー レコードのキー フィールドとしての Cisco TrustSec フィールドの設定

手順の概要

1. **enable**
2. **configure terminal**
3. **flow record** *record-name*
4. **match** {**ipv4** | **ipv6**} **protocol**
5. **match** {**ipv4** | **ipv6**} **source address**
6. **match** {**ipv4** | **ipv6**} **destination address**
7. **match transport source-port**
8. **match transport destination-port**
9. **match flow direction**
10. **match flow cts source group-tag**
11. **match flow cts destination group-tag**
12. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**flow record** *record-name* 例： `Device(config)# flow record cts-record-ipv4`	Flexible Netflow（FNF）フロー レコードを作成するか、または既存の FNF フロー レコードを変更して、Flexible NetFlow フロー レコード コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 4	**match** {**ipv4** | **ipv6**} **protocol** 例： `Device(config-flow-record)# match ipv4 protocol`	（オプション）フロー レコードのキー フィールドとして IPv4 プロトコルまたは IPv6 プロトコルを設定します。
ステップ 5	**match** {**ipv4** | **ipv6**} **source address** 例： `Device(config-flow-record)# match ipv4 source address`	（オプション）IPv4 または IPv6 送信元アドレスをフロー レコードのキー フィールドとして設定します。
ステップ 6	**match** {**ipv4** | **ipv6**} **destination address** 例： `Device(config-flow-record)# match ipv4 destination address`	（オプション）IPv4 または IPv6 接続先アドレスをフロー レコードのキー フィールドとして設定します。
ステップ 7	**match transport source-port** 例： `Device(config-flow-record)# match transport source-port`	（オプション）フロー レコードのキー フィールドとして、トランスポート送信元ポートを設定します。
ステップ 8	**match transport destination-port** 例： `Device(config-flow-record)# match transport destination-port`	（オプション）フロー レコードのキー フィールドとして、トランスポート宛先ポートを設定します。
ステップ 9	**match flow direction** 例： `Device(config-flow-record)# match flow direction`	（オプション）フローがモニターされる方向をキー フィールドとして設定します。
ステップ 10	**match flow cts source group-tag** 例： `Device(config-flow-record)# match flow cts source group-tag`	FNF フロー レコード内の Cisco TrustSec 送信元セキュリティ グループ タグ（SGT）をキー フィールドとして設定します。
ステップ 11	**match flow cts destination group-tag** 例： `Device(config-flow-record)# match flow cts destination group-tag`	FNF フロー レコード内の Cisco TrustSec 宛先セキュリティ グループ タグ（DGT）をキー フィールドとして設定します。

	コマンドまたはアクション	目的
ステップ 12	**end** 例： `Device(config-flow-record)# end`	Flexible NetFlow フロー レコード コンフィギュレーション モードを終了して、特権 EXEC モードに戻ります。

フロー レコードの非キー フィールドとしての Cisco TrustSec フィールドの設定

手順の概要

1. **enable**
2. **configure terminal**
3. **flow record** *record-name*
4. **match** {**ipv4** | **ipv6**} **protocol**
5. **match** {**ipv4** | **ipv6**} **source address**
6. **match** {**ipv4** | **ipv6**} **destination address**
7. **match transport source-port**
8. **match transport destination-port**
9. **collect flow direction**
10. **collect flow cts source group-tag**
11. **collect flow cts destination group-tag**
12. **collect counter packets**
13. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**flow record** *record-name* 例： `Device(config)# flow record cts-record-ipv4`	Flexible Netflow（FNF）フロー レコードを作成するか、または既存の FNF フロー レコードを変更して、Flexible NetFlow フロー レコード コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 4	**match** {**ipv4** | **ipv6**} **protocol** 例： `Device(config-flow-record)# match ipv4 protocol`	（オプション）フロー レコードのキー フィールドとして IPv4 プロトコルまたは IPv6 プロトコルを設定します。 （注） Cisco CSR100V、ISR 4400、および ASR 1000 プラットフォームでは、Cisco TrustSec フィールドは IPv4 FNF レコードでのみサポートされます。
ステップ 5	**match** {**ipv4** | **ipv6**} **source address** 例： `Device(config-flow-record)# match ipv4 source address`	（オプション）IPv4 または IPv6 送信元アドレスをフロー レコードのキー フィールドとして設定します。 （注） Cisco CSR100V、ISR 4400、および ASR 1000 プラットフォームでは、Cisco TrustSec フィールドは IPv4 FNF レコードでのみサポートされます。
ステップ 6	**match** {**ipv4** | **ipv6**} **destination address** 例： `Device(config-flow-record)# match ipv4 destination address`	（オプション）IPv4 または IPv6 接続先アドレスをフロー レコードのキー フィールドとして設定します。 （注） Cisco CSR100V、ISR 4400、および ASR 1000 プラットフォームでは、Cisco TrustSec フィールドは IPv4 FNF レコードでのみサポートされます。
ステップ 7	**match transport source-port** 例： `Device(config-flow-record)# match transport source-port`	（オプション）フロー レコードのキー フィールドとして、トランスポート送信元ポートを設定します。
ステップ 8	**match transport destination-port** 例： `Device(config-flow-record)# match transport destination-port`	（オプション）フロー レコードのキー フィールドとして、トランスポート宛先ポートを設定します。
ステップ 9	**collect flow direction** 例： `Device(config-flow-record)# collect flow direction`	（オプション）フロー方向を非キー フィールドとして設定し、フローがモニタされた方向の収集を有効化します。

	コマンドまたはアクション	目的
ステップ 10	**collect flow cts source group-tag** 例： `Device(config-flow-record)# collect flow cts source group-tag`	FNF フロー レコード内の Cisco TrustSec 送信元セキュリティ グループ タグ（SGT）を非キー フィールドとして設定します。
ステップ 11	**collect flow cts destination group-tag** 例： `Device(config-flow-record)# collect flow cts destination group-tag`	FNF フロー レコード内の Cisco TrustSec 宛先セキュリティ グループ タグ（DGT）を非キー フィールドとして設定します。
ステップ 12	**collect counter packets** 例： `Device(config-flow-record)# collect counter packets`	（オプション）フローで確認されるパケット数を非キー フィールドとして設定し、フローから合計パケット数を収集します。
ステップ 13	**end** 例： `Device(config-flow-record)# end`	Flexible NetFlow フロー レコード コンフィギュレーション モードを終了して、特権 EXEC モードに戻ります。

フロー エクスポータの設定

フローエクスポータごとに、1 つの宛先のみがサポートされます。複数の宛先にデータをエクスポートする場合は、複数のフロー エクスポータを設定してフロー モニターに割り当てる必要があります。

始める前に

フロー レコードを作成していることを確認します。詳細については、「フロー レコードの非キー フィールドとしての Cisco TrustSec フィールドの設定」の項および「フロー レコードの非キー フィールドとしての Cisco TrustSec フィールドの設定」の項を参照してください。

手順の概要

1. **enable**
2. **configure terminal**
3. **flow exporter** *exporter-name*
4. **destination** {*ip-address* | *hostname*} [**vrf** *vrf-name*]
5. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**flow exporter** *exporter-name* 例： `Device(config)# flow exporter EXPORTER-1`	フローエクスポータを作成するか、または既存のフロー エクスポータを変更して、Flexible NetFlow フロー エクスポータ コンフィギュレーション モードを開始します。
ステップ 4	**destination** {*ip-address* | *hostname*} [**vrf** *vrf-name*] 例： `Device(config-flow-exporter)# destination 172.16.10.2`	エクスポータの宛先システムのIPアドレスまたはホスト名を指定します。
ステップ 5	**end** 例： `Device(config-flow-exporter)# end`	Flexible NetFlow フロー エクスポータ コンフィギュレーションモードを終了して、特権EXECモードに戻ります。

フロー モニタの設定

始める前に

フロー エクスポータをデータ エクスポート用のフロー モニタに追加するには、フロー エクスポータを作成していることを確認します。詳細については、「フローエクスポータの設定」の項を参照してください。

手順の概要

1. **enable**
2. **configure terminal**
3. **flow monitor** *monitor-name*
4. **record** *record-name*
5. **exporter** *exporter-name*
6. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**flow monitor** *monitor-name* 例： `Device(config)# flow monitor FLOW-MONITOR-1`	フロー モニタを作成するか、または既存のフロー モニタを変更して、Flexible NetFlow フロー モニタ コンフィギュレーション モードを開始します。
ステップ 4	**record** *record-name* 例： `Device(config-flow-monitor)# record FLOW-RECORD-1`	フロー モニターのレコードを指定します。
ステップ 5	**exporter** *exporter-name* 例： `Device(config-flow-monitor)# exporter EXPORTER-1`	フロー モニタのエクスポータを指定します。
ステップ 6	**end** 例： `Device(config-flow-monitor)# end`	Flexible NetFlow フロー モニタ コンフィギュレーション モードを終了して、特権 EXEC モードに戻ります。

インターフェイスへのフロー モニタの適用

フロー モニタをアクティベートするには、フロー モニタを 1 つ以上のインターフェイスに適用する必要があります。

始める前に

フロー モニタを作成していることを確認します。詳細については、「フロー モニタの設定」の項を参照してください。

手順の概要

1. **enable**
2. **configure terminal**

3. **interface** *type number*
4. {**ip** | **ipv6**} **flow monitor** *monitor-name* {**input** | **output**}
5. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface** *type number* 例： `Device(config)# interface ethernet 0/0`	インターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	{**ip**	**ipv6**} **flow monitor** *monitor-name* {**input**	**output**} 例： `Device (config-if)# ip flow monitor FLOW-MONITOR-1 input`	作成済みのフローモニタを、トラフィックの分析対象となるインターフェイスに割り当てることで、そのフロー モニタをアクティブにします。
ステップ 5	**end** 例： `Device(config-if)# end`	インターフェイス コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

Cisco TrustSec フィールドの Flexible NetFlow エクスポートの確認

手順の概要

1. **enable**
2. **show flow record** *record-name*
3. **show flow exporter** *exporter-name*
4. **show flow monitor** *monitor-name*
5. **show flow monitor** *monitor-name* **cache**
6. **show flow interface** *type number*

手順の詳細

ステップ 1 **enable**

特権 EXEC モードを有効にします。

- パスワードを入力します（要求された場合）。

例：

```
Device> enable
```

ステップ 2 **show flow record** *record-name*

指定した Flexible Netflow（FNF）フロー レコードの詳細を表示します。

例：

```
Device> show flow record cts-recordipv4

flow record cts-recordipv4:
  Description:        User defined
  No. of users:       1
  Total field space:  30 bytes
  Fields:
    match ipv4 protocol
    match ipv4 source address
    match ipv4 destination address
    match transport source-port
    match transport destination-port
    match interface input
    match interface output
    match flow direction
    match flow cts source group-tag
    match flow cts destination group-tag
    collect counter packets
```

ステップ 3 **show flow exporter** *exporter-name*

指定した FNF フロー エクスポータの現在のステータスを表示します。

例：

```
Device> show flow exporter EXPORTER-1

Flow Exporter EXPORTER-1:
  Description:              User defined
  Export protocol:          NetFlow Version 9
  Transport Configuration:
    Destination IP address: 100.100.100.1
    Source IP address:      3.3.3.2
```

```
    Transport Protocol:     UDP
    Destination Port:       2055
    Source Port:            65252
    DSCP:                   0x0
    TTL:                    255
    Output Features:        Used
```

ステップ 4 **show flow monitor** *monitor-name*

指定した FNF フロー モニタのステータスと統計情報を表示します。

例：

```
Device> show flow monitor FLOW-MONITOR-1

Flow Monitor FLOW-MONITOR-1:
  Description:       User defined
  Flow Record:       cts-recordipv4
  Flow Exporter:     EXPORTER-1
  Cache:
    Type:                 normal (Platform cache)
    Status:               allocated
    Size:                 200000 entries
    Inactive Timeout:     60 secs
    Active Timeout:       1800 secs
    Update Timeout:       1800 secs
    Synchronized Timeout: 600 secs
    Trans end aging:      off
```

ステップ 5 **show flow monitor** *monitor-name* **cache**

指定した FNF フロー モニタ キャッシュのコンテンツを表示します。

例：

```
Device> show flow monitor FLOW-MONITOR-1 cache

  Cache type:                               Normal
  Cache size:                               4096
  Current entries:                          2
  High Watermark:                           2

  Flows added:                              6
  Flows aged:                               4
    - Active timeout      (1800 secs)       0
    - Inactive timeout    (15 secs)         4
    - Event aged                            0
    - Watermark aged                        0
    - Emergency aged                        0

  IPV4 SOURCE ADDRESS:                      10.1.0.1
  IPV4 DESTINATION ADDRESS:                 172.16.2.0
  TRNS SOURCE PORT:                         58817
  TRNS DESTINATION PORT:                    23
  FLOW DIRECTION:                           Input
  IP PROTOCOL:                              6
```

```
SOURCE GROUP TAG:                       100
DESTINATION GROUP TAG:                  200
counter packets:                        10

IPV4 SOURCE ADDRESS:                    172.16.2.0
IPV4 DESTINATION ADDRESS:               10.1.0.1
TRNS SOURCE PORT:                       23
TRNS DESTINATION PORT:                  58817
FLOW DIRECTION:                         Output
IP PROTOCOL:                            6
SOURCE GROUP TAG:                       200
DESTINATION GROUP TAG:                  100
counter packets:                        8
```

ステップ 6 **show flow interface** *type number*

指定したインターフェイスに適用されるFNFフローモニタの詳細を表示します。フローモニタがインターフェイスに適用されない場合、出力は空になります。

例：

```
Device>  show flow interface GigabitEthernet0/0/3

Interface GigabitEthernet0/0/3
  FNF:  monitor:          FLOW-MONITOR-1
        direction:        Input
        traffic(ip):      on
  FNF:  monitor:          FLOW-MONITOR-1
        direction:        Output
        traffic(ip):      on
```

Cisco TrustSec フィールドの Flexible NetFlow エクスポートの設定例

例：フロー レコードのキー フィールドとしての Cisco TrustSec フィールドの設定

次の例は、Cisco TrustSec フロー オブジェクトを、IPv4 Flexible NetFlow フロー レコードのキー フィールドとして設定する方法を示します。

```
Device> enable
Device# configure terminal
Device(config)# flow record cts-record-ipv4
Device(config-flow-record)# match ipv4 protocol
Device(config-flow-record)# match ipv4 source address
```

```
Device(config-flow-record)# match ipv4 destination address
Device(config-flow-record)# match transport source-port
Device(config-flow-record)# match transport destination-port
Device(config-flow-record)# match flow direction
Device(config-flow-record)# match flow cts source group-tag
Device(config-flow-record)# match flow cts destination group-tag
Device(config-flow-record)# end
```

例：フローレコードの非キーフィールドとしてのCiscoTrustSecフィールドの設定

次の例は、Cisco TrustSec フロー オブジェクトを、IPv4 Flexible NetFlow フロー レコードの非キー フィールドとして設定する方法を示します。

```
Device> enable
Device# configure terminal
Device(config)# flow record cts-record-ipv4
Device(config-flow-record)# match ipv4 protocol
Device(config-flow-record)# match ipv4 source address
Device(config-flow-record)# match ipv4 destination address
Device(config-flow-record)# match transport source-port
Device(config-flow-record)# match transport destination-port
Device(config-flow-record)# collect flow direction
Device(config-flow-record)# collect flow cts source group-tag
Device(config-flow-record)# collect flow cts destination group-tag
Device(config-flow-record)# collect counter packets
Device(config-flow-record)# end
```

例：フロー エクスポータの設定

```
Device> enable
Device# configure terminal
Device(config)# flow exporter EXPORTER-1
Device(config-flow-exporter)# destination 172.16.10.2
Device(config-flow-exporter)# end
```

例：フロー モニタの設定

```
Device> enable
Device# configure terminal
Device(config)# flow monitor FLOW-MONITOR-1
Device(config-flow-monitor)# record FLOW-RECORD-1
Device(config-flow-monitor)# exporter EXPORTER-1
Device(config-flow-monitor)# end
```

例：インターフェイス上のフロー モニタの適用

次の例は、トラフィックを分析するインターフェイスにIPv4フローモニタを適用することで、このフローモニタをアクティベートする方法を示します。IPv6フローモニタをアクティベートするには、**ip** キーワードを **ipv6** キーワードと置き換えます。

```
Device> enable
Device# configure terminal
Device(config)# interface ethernet 0/0
Device(config-if)# ip flow monitor FLOW-MONITOR-1 input
Device(config-if)# end
```

Cisco TrustSec フィールドの Flexible NetFlow エクスポートに関する追加情報

関連資料

関連項目	マニュアル タイトル
セキュリティ コマンド	• 『Cisco IOS Security Command Reference: Commands A to C』 • 『Cisco IOS Security Command Reference: Commands D to L』 • 『Cisco IOS Security Command Reference: Commands M to R』 • 『Cisco IOS Security Command Reference: Commands S to Z』
Flexible NetFlow でのデータ エクスポート	『*Flexible Netflow Configuration Guide*』パブリケーションの「Flexible NetFlow Output Features on Data Export」の章
Flexible NetFlow のフロー レコードとフロー モニタ	『*Flexible Netflow Configuration Guide*』パブリケーションの「Customizing Flexible NetFlow Flow Records and Flow Monitors」の章

シスコのテクニカル サポート

説明	リンク
シスコのサポート Web サイトでは、シスコの製品やテクノロジーに関するトラブルシューティングにお役立ていただけるように、マニュアルやツールをはじめとする豊富なオンライン リソースを提供しています。 お使いの製品のセキュリティ情報や技術情報を入手するために、Cisco Notification Service（Field Notice からアクセス）、Cisco Technical Services Newsletter、Really Simple Syndication（RSS）フィードなどの各種サービスに加入できます。 シスコのサポート Web サイトのツールにアクセスする際は、Cisco.com のユーザ ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

Cisco TrustSec フィールドの Flexible NetFlow エクスポートの機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *125 : Cisco TrustSec* フィールドの *Flexible NetFlow* エクスポートの機能情報

機能名	リリース	機能情報
Cisco TrustSec フィールドの Flexible NetFlow エクスポート		Cisco TrustSec フィールドの Flexible NetFlow エクスポートでは、Flexible Netflow（FNF）フロー レコード内の Cisco TrustSec フィールドをサポートし、Cisco TrustSec 導入の標準から外れた動作のモニタ、トラブルシューティング、および特定を支援します。 この機能により、次のコマンドが導入されました。**match flow cts {source | destination} group-tag** および **collect flow cts {source | destination} group-tag**。

第 90 章

Cisco TrustSec SGT キャッシング

Cisco TrustSec SGT キャッシング 機能は、セキュリティグループタグ（SGT）の移動性を柔軟にする Cisco TrustSec の機能を強化します。この機能は、IP-SGT バインドを特定し、対応する SGT をキャッシュすることで、通常のディープ パケット インスペクションを処理するすべてのネットワーク サービスを通じて、またパケットが該当する SGT で再度タグ付けされるサービス出力ポイントにおいて、ネットワーク パケットを転送します。

Cisco TrustSec SGT キャッシング の制約事項

グローバルなセキュリティ グループ タグ（SGT）キャッシング設定と、インターフェイス固有の入力設定は相互に排他的です。次のシナリオでは、SGT キャッシングをグローバルおよびインターフェイス上の両方で構成しようとした場合に、警告メッセージが表示されます。

- **cts role-based sgt-cache ingress** コマンドをインターフェイス設定モードで使用して、インターフェイスが入力 SGT キャッシングを有効にし、**cts role-based sgt-caching** コマンドを使用してグローバル設定を試行した場合、次の例が示すような警告メッセージが表示されます。

```
Device> enable
Device# configure terminal
Device(config)# interface gigabitEthernet0/0
Device(config-if)# cts role-based sgt-cache ingress
Device(config-if)# exit
Device(config)# cts role-based sgt-caching

There is at least one interface that has ingress sgt caching configured. Please
remove all interface ingress sgt caching configuration(s) before attempting global
enable.
```

- **cts role-based sgt-caching** コマンドを使用してグローバル設定を有効化し、インターフェイス設定モードで **cts role-based sgt-cache ingress** コマンドを使用してインターフェイス設定を試行した場合、次の例が示すような警告メッセージが表示されます。

```
Device> enable
Device# configure terminal
Device(config)# cts role-based sgt-caching
Device(config)# interface gigabitEthernet0/0
Device(config-if)# cts role-based sgt-cache ingress

Note that ingress sgt caching is already active on this interface due to global
sgt-caching enable.
```

- V4 トランスポートを介した IPv6 パケットおよび V6 トランスポートを介した IPv4 パケットのトンネリングの SGT キャッシングは、サポートされていません。
- ルーティング プラットフォームでの IPv6 SGACL ポリシーのハイアベイラビリティおよび同期は、IPv6-SGT キャッシングではサポートされません。
- SGT キャッシングは、ISR4K ベースのプラットフォームにおいて ESP ヘッダーで SGT タグを伝送する IPSec パケットではサポートされません。
- SGT キャッシングは、リンクローカル IPv6 送信元アドレスに対して実行されません。

  リンクローカルアドレスとは、ホストが接続されているネットワークセグメント（リンク）またはブロードキャストドメイン内の通信にのみ有効なネットワークアドレスです。リンクローカルアドレスは、単一のネットワークセグメントを超えて一意であるとは限りません。そのため、ルータは、リンクローカルアドレスを持つパケットを転送しません。リンクローカルアドレスは一意ではないため、送信元がリンクローカル IPv6 アドレスであるパケットの SGT タグは割り当てられません。
- SGT キャッシングは、IVRF が設定された IPsec を持つトンネルインターフェイスではサポートされません。
- 仮想テンプレート インターフェイスでの SGT キャッシングの設定は、Cisco ASR 1000 プラットフォームではサポートされていません。

Cisco TrustSec SGT キャッシングの詳細

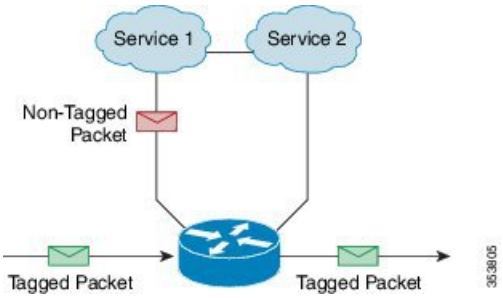
SGT キャッシングを使用した SGT の特定と再適用

Cisco TrustSec は、セキュリティ グループ タグ（SGT）キャッシングを使用して、SGT でタグ付けされたトラフィックを、SGT を認識していないサービスを通じても渡すことができるようにします。SGT を伝播できないサービスには、WAN の高速化または最適化、侵入防御システム（IPS）、およびアップストリーム ファイアウォールがあります。ワンアーム モードでは、SGT でタグ付けされたパケットはデバイス（タグがキャッシュされた場所）に入力され、サービスにリダイレクトされます。そのサービスが完了した後、パケットはデバイスに戻される

か、別のデバイスにリダイレクトされます（図を参照）。このようなシナリオでは、次のようになります。

1. Cisco TrustSec SGT キャッシング機能により、デバイスは、着信パケットからの IP-SGT バインド情報を特定し、この情報をキャッシュします。
2. デバイスは、SGT を伝播できないサービスにパケットをリダイレクトします。
3. サービスが完了した後、パケットはデバイスに返されます。
4. サービスの出力ポイントで、適切な SGT がパケットに再適用されます。
5. サービスからデバイスに返されたパケットには、ロールベースの強制が適用されます。
6. SGT のパケットは、他の Cisco TrustSec 対応デバイスのダウンストリームに転送されます。

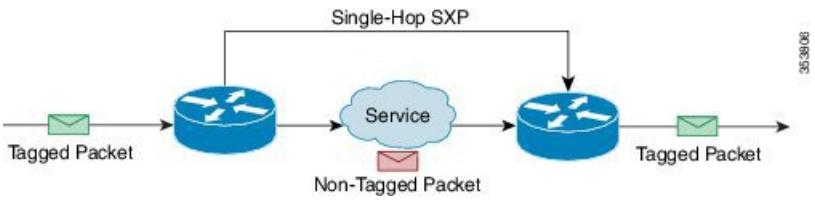
図 *20* : ワンアーム モードでの *SGT* キャッシング



特定のインスタンスでは、Bump-In-The-Wire（BITW）トポロジに導入されるサービスがあります。このようなシナリオでは、次のようになります。

1. サービスを通過するパケットはデバイスに返されません。
2. シングルホップ SGT Exchange Protocol（SXP）を使用して、IP-SGT バインドを特定し、特定されたバインドをエクスポートします。
3. ネットワーク内のアップストリームデバイスは、SXP を通じて IP-SGT バインドを特定し、適切なタグを再適用するか、それらを SGT ベース強制に使用します。出力キャッシング中、元のネットワーク アドレス移動（NAT）前の送信元 IP アドレスは、特定された IP-SGT バインド情報の一部としてキャッシュされます。
4. 300 秒間トラフィックを受信しない IP-SGT バインドは、キャッシュから削除されます。

図 *21* : *Bump-In-The-Wire*（*BITW*）トポロジでの *SGT* キャッシング



IPv6 トラフィックの SGT キャッシング

IPv6 トラフィックの SGT キャッシングに関する考慮事項は次のとおりです。

- **グローバルユニキャスト IPv6 パケット**：IPv6-SGT キャッシングは、IPv6 パケットの入力方向および出力方向で着信するトラフィックに対して実行されます。SGT タグは、パケット（イーサネットヘッダー、IPSec ヘッダー、GRE ヘッダー）にインラインで含まれます。ただし、IPSec パケットのタグの SGT キャッシングは、ISR4K ベースのプラットフォームではサポートされていません。
- **マルチキャスト IPv6 アドレス**：SGT キャッシングは、IPv6 マルチキャストトラフィックおよびリンクローカル IPv6 アドレスではサポートされません。
- **キャッシュされた IPv6-SGT バインディングの SXP を介したエクスポート**：データプレーンで学習された IPv6-SGT バインディングは、IOS の RBM（ロールベースマネージャ）データベースに通知されます。その後、これらのバインディングは、SXP を使用して他の TrustSec デバイスにエクスポートできます。

Cisco TrustSec SGT キャッシングの設定方法

SGT キャッシングのグローバル設定

手順の概要

1. **enable**
2. **configure terminal**
3. **cts role-based sgt-caching**
4. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**cts role-based sgt-caching** 例：	すべてのインターフェイスに対して、入力方向の SGT キャッシングを有効化します。

	コマンドまたはアクション	目的
	`Device(config)# cts role-based sgt-caching`	
ステップ 4	**end** 例： `Device(config)# end`	グローバル コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

インターフェイスでの SGT キャッシシングの設定

インターフェイスが Virtual Routing and Forwarding（VRF）ネットワーク上に設定された場合、そのインターフェイス上で特定された IP-SGT バインドは特定の VRF 以下に追加されます。（対応する VRF 上で特定されたバインドを表示するには、**show cts role-based sgt-map vrf** *vrf-name* **all** コマンドを使用します。）

手順の概要

1. **enable**
2. **configure terminal**
3. **interface** *type slot/port*
4. **cts role-based sgt-cache** [**ingress** | **egress**]
5. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface** *type slot/port* 例： `Device(config)# interface gigabitEthernet 0/1/0`	インターフェイスを設定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	**cts role-based sgt-cache** [**ingress**	**egress**] 例：	特定のインターフェイスでSGTキャッシングを設定します。

	コマンドまたはアクション	目的
	`Device(config-if)# cts role-based sgt-cache ingress`	• ingress：特定のインターフェイスを開始するトラフィック（インバウンドトラフィック）に対して SGT キャッシングを有効化します。 • egress：特定のインターフェイスを終了するトラフィック（アウトバウンドトラフィック）に対して SGT キャッシングを有効化します。
ステップ 5	**end** 例： `Device(config-if)# end`	インターフェイス コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

Cisco TrustSec SGT キャッシング の確認

手順の概要

1. **enable**
2. **show cts**
3. **show cts interface**
4. **show cts interface brief**
5. **show cts role-based sgt-map all ipv4**
6. **show cts role-based sgt-map vrf**

手順の詳細

ステップ 1 **enable**

特権 EXEC モードを有効にします。パスワードを入力します（要求された場合）。

例：

```
Device> enable
```

ステップ 2 **show cts**

Cisco TrustSec 接続とグローバル SGT キャッシングのステータスを表示します。

例：

```
Device# show cts

Global Dot1x feature: Disabled
CTS device identity: ""
CTS caching support: disabled
CTS sgt-caching global: Enabled
Number of CTS interfaces in DOT1X mode:  0,    MANUAL mode: 0
```

```
Number of CTS interfaces in LAYER3 TrustSec mode: 0
Number of CTS interfaces in corresponding IFC state
  INIT            state:  0
  AUTHENTICATING  state:  0
  AUTHORIZING     state:  0
  SAP_NEGOTIATING state:  0
  OPEN            state:  0
  HELD            state:  0
  DISCONNECTING   state:  0
  INVALID         state:  0
CTS events statistics:
  authentication success: 0
  authentication reject : 0
  authentication failure: 0
  authentication logoff : 0
  authentication no resp: 0
  authorization success : 0
  authorization failure : 0
  sap success           : 0
  sap failure           : 0
  port auth failure     : 0
```

ステップ 3 show cts interface

モード詳細（入力または出力）を使用した、インターフェイスと SGT キャッシング情報についての Cisco TrustSec 設定の統計情報を表示します。

例：

```
Device# show cts interface GigabitEthernet0/1

Interface GigabitEthernet0/1
    CTS sgt-caching Ingress:  Enabled
    CTS sgt-caching Egress :  Disabled
    CTS is enabled, mode:     MANUAL
      Propagate SGT:          Enabled
      Static Ingress SGT Policy:
        Peer SGT:             200
        Peer SGT assignment:  Trusted

    L2-SGT Statistics
        Pkts In                     : 16298041
        Pkts (policy SGT assigned)  : 0
        Pkts Out                    : 5
        Pkts Drop (malformed packet): 0
        Pkts Drop (invalid SGT)     : 0
```

ステップ 4 show cts interface brief

すべてのインターフェイスについて、モード詳細（入力または出力）を使用して SGT キャッシング情報を表示します。

例：

```
Device# show cts interface brief

Interface GigabitEthernet0/0
    CTS sgt-caching Ingress:  Enabled
    CTS sgt-caching Egress :  Disabled
    CTS is disabled
```

```
Interface GigabitEthernet0/1
    CTS sgt-caching Ingress:  Enabled
    CTS sgt-caching Egress :  Disabled
    CTS is enabled, mode:     MANUAL
      Propagate SGT:          Enabled
      Static Ingress SGT Policy:
        Peer SGT:             200
        Peer SGT assignment:  Trusted

Interface GigabitEthernet0/2
    CTS sgt-caching Ingress:  Enabled
    CTS sgt-caching Egress :  Disabled
    CTS is enabled, mode:     MANUAL
      Propagate SGT:          Enabled
      Static Ingress SGT Policy:
        Peer SGT:             0
        Peer SGT assignment:  Untrusted

Interface GigabitEthernet0/3
    CTS sgt-caching Ingress:  Enabled
    CTS sgt-caching Egress :  Disabled
    CTS is disabled

Interface Backplane-GigabitEthernet0/4
    CTS sgt-caching Ingress:  Enabled
    CTS sgt-caching Egress :  Disabled
    CTS is disabled

Interface RG-AR-IF-INPUT1
    CTS sgt-caching Ingress:  Enabled
    CTS sgt-caching Egress :  Disabled
    CTS is disabled
```

ステップ 5 show cts role-based sgt-map all ipv4

すべての SGT-IPv4 バインドを表示します。

例：

```
Device# show cts role-based sgt-map all ipv4

Active IPv4-SGT Bindings Information

IP Address              SGT     Source
============================================
192.0.2.1                50      CACHED
192.0.2.2                50      CACHED
192.0.2.3                50      CACHED
192.0.2.4                50      CACHED
192.0.2.5               3900    INTERNAL
192.0.2.6               3900    INTERNAL
192.0.2.7               3900    INTERNAL

IP-SGT Active Bindings Summary
============================================
Total number of CACHED   bindings = 20
Total number of INTERNAL bindings = 3
Total number of active   bindings = 23
```

ステップ 6 show cts role-based sgt-map vrf

特定の Virtual Routing and Forwarding（VRF）インターフェイスに対する SGT-IP バインドをすべて表示します。

例：

```
Device# show cts role-based sgt-map vrf

%IPv6 protocol is not enabled in VRF RED
Active IPv4-SGT Bindings Information

IP Address              SGT     Source
============================================
192.0.2.1                50      CACHED
192.0.2.2                2007    CACHED
192.0.2.3                50      CACHED
192.0.2.4                50      CACHED
```

IP と SGT のバインドの確認

データプレーンで学習された IP と SGT のバインドを表示します。

```
Device# show cts role-based sgt-map all
Active IPv4-SGT Bindings Information

IP Address              SGT     Source
============================================
10.104.33.219           300     INTERNAL

IP-SGT Active Bindings Summary
============================================
Total number of INTERNAL bindings = 1
Total number of active   bindings = 1

Active IPv6-SGT Bindings Information

IP Address                                  SGT     Source
============================================================
100::/64                                    124     CLI
200::2                                      300     INTERNAL
300::1                                      300     INTERNAL
1000::2                                     300     INTERNAL

IP-SGT Active Bindings Summary
============================================
Total number of CLI      bindings = 1
Total number of INTERNAL bindings = 3
Total number of active   bindings = 4
```

設定例 Cisco TrustSec SGT キャッシング

例：SGT キャッシングのグローバル設定

```
Device> enable
Device# configure terminal
Device(config)# cts role-based sgt-caching
Device(config)# end
```

例：インターフェイスの SGT キャッシシングの設定

```
Device> enable
Device# configure terminal
Device(config)# interface gigabitEthernet 0/1/0
Device(config-if)# cts role-based sgt-cache ingress
Device(config-if)# end
```

例：インターフェイスでの SGT キャッシシングの無効化

次の例は、キャッシングがグローバルに有効だがインターフェイスでは無効な場合に、インターフェイスで SGT キャッシングを無効化し、インターフェイスの SGT キャッシングの状態を表示する方法を示します。

```
Device> enable
Device# configure terminal
Device(config)# cts role-based sgt-caching
Device(config)# interface gigabitEthernet 0/1
Device(config-if)# no cts role-based sgt-cache ingress
Device(config-if)# end
Device# show cts interface GigabitEthernet0/1

Interface GigabitEthernet0/1
    CTS sgt-caching Ingress:  Disabled
    CTS sgt-caching Egress :  Disabled
    CTS is enabled, mode:     MANUAL
      Propagate SGT:          Enabled
      Static Ingress SGT Policy:
        Peer SGT:             200
        Peer SGT assignment:  Trusted

    L2-SGT Statistics
        Pkts In                     : 200890684
        Pkts (policy SGT assigned)  : 0
        Pkts Out                    : 14
        Pkts Drop (malformed packet): 0
```

```
Pkts Drop (invalid SGT)      : 0
```

に関する追加情報 Cisco TrustSec SGT キャッシング

関連資料

関連項目	マニュアル タイトル
Cisco IOS セキュリティ コマンド	• 『Cisco IOS Security Command Reference: Commands A to C』[英語] • 『Cisco IOS Security Command Reference: Commands D to L』[英語] • 『Cisco IOS Security Command Reference: Commands M to R』[英語] • 『Cisco IOS Security Command Reference: Commands S to Z』[英語]
Cisco TrustSec の設定	『*Cisco TrustSec Configuration Guide*』の「Cisco TrustSec Support for IOS」の章
Cisco TrustSec の概要	『Overview of TrustSec』
Cisco TrustSec ソリューション	『Cisco TrustSec Security Solution』

シスコのテクニカル サポート

説明	リンク
シスコのサポート Web サイトでは、シスコの製品やテクノロジーに関するトラブルシューティングにお役立ていただけるように、マニュアルやツールをはじめとする豊富なオンライン リソースを提供しています。 お使いの製品のセキュリティ情報や技術情報を入手するために、Cisco Notification Service（Field Notice からアクセス）、Cisco Technical Services Newsletter、Really Simple Syndication（RSS）フィードなどの各種サービスに加入できます。 シスコのサポート Web サイトのツールにアクセスする際は、Cisco.com のユーザ ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

Cisco TrustSec SGT キャッシング の機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *126 : Cisco TrustSec SGT* キャッシング の機能情報

機能名	リリース	機能情報
Cisco TrustSec SGT キャッシング		Cisco TrustSec SGT キャッシング 機能は、セキュリティ グループタグ（SGT）の移動性を柔軟にする Cisco TrustSec の機能を強化します。この機能は、IP-SGT バインドを特定し、対応する SGT をキャッシュすることで、通常のディープ パケット インスペクションを処理するすべてのネットワーク サービスを通じて、またパケットが該当する SGT で再度タグ付けされるサービス出力ポイントにおいて、ネットワーク パケットを転送します。 次のコマンドが導入または変更されました。**cts role-based sgt-caching**、**cts role-based sgt-cache** [**ingress**	**egress**]。

機能名	リリース	機能情報
IPv6の有効化：SGT キャッシング	Cisco IOS XE Fuji 16.8.1	IPv6 のサポートが導入されました。

第 91 章

CTS SGACL のサポート

CTS SGACL のサポート機能は、IP アドレスではなく、セキュリティ アソシエーションまたはセキュリティ グループ タグ値に基づいたステートレスのアクセス制御メカニズムを提供します。

CTS SGACL サポートの前提条件

CTS SGACL サポートについては、Protected Access Credential（PAC）と環境データのダウンロードが、ダイナミック SGACL のデバイスで設定されていること。

CTS SGACL サポートの制約事項

- プラットフォームあたりでサポートされている TrustSec 機能のリストおよび IOS リリースの最小要件については、次の URL の Cisco TrustSec プラットフォーム サポート マトリックス [英語] を参照してください：http://www.cisco.com/en/US/solutions/ns170/ns896/ns1051/trustsec_matrix.html
- SGACL の適用は、管理インターフェイスではサポートされていません。
- ダイナミック SGACL のダウンロード サイズは、6 KB に制限されています。
- Port-Channel インターフェイスの SGACL 適用は検証されていません。

- VRF aware SGT 設定では、Cisco IOS XE Denali 16.3 は、VRF 管理インターフェイスではありませんが、ISE 通信をサポートしています。管理インターフェイスを通じた ISE 通信はサポートされていません。
- 6 KB の拡張制限は、ダイナミック SGACL のみです。スタティック SGACL は、256*256 マトリックスのような高い拡張性をサポートできます。
- SGACL の適用は、リンクローカル IPv6 送信元/宛先アドレスを持つ IPv6 パケットについてはバイパスされます。
- IPv6 マルチキャストトラフィックの SGACL 適用はバイパスされます。
- Cisco IOS XE Bengaluru 17.4.1 以降では、VRF を認識するように自動テスターを設定できます。**automate-tester** コマンドで **vrf** キーワードを使用すると、デフォルト以外の VRF の自動テスト機能を有効化します。

（注） VRF 対応の自動テスターを機能させるには、**global config ipv4/ipv6 source interface** *interface-name* **vrf** *vrf-name* コマンドを設定する必要があります。

CTS SGACL サポートに関する情報

CTS SGACL のサポート

セキュリティ グループ アクセス コントロール リスト（SGACL）はポリシーの適用です。これによって管理者は、セキュリティグループの割り当てと宛先リソースに基づいてユーザが実行する操作を制御できます。Cisco TrustSec ドメイン内のポリシーの適用は、軸の 1 つが送信元セキュリティ グループ番号、もう 1 つの軸が宛先セキュリティ グループ番号である、アクセス許可マトリックスで表示されます。マトリックス内の各セルには、SGACL の番号付きリストが含まれます。ここでは、送信元セキュリティ グループに属し宛先セキュリティ グループに属する宛先 IP を持つ、IP から送信されるパケットに適用される必要があるアクセス権限を指定します。

SGACL は、IP アドレスではなく、セキュリティ アソシエーションまたはセキュリティ グループ タグ値に基づいたステートレスのアクセス制御メカニズムを提供し、一致クラスに基づいてトラフィックをフィルタリングします。SGACL ポリシーをプロビジョニングするには、次の 3 つの方法があります。

- スタティック ポリシー プロビジョニング：**cts role-based permission** コマンドを使用して、ユーザーが SGACL ポリシーを定義します。
- ダイナミック ポリシー プロビジョニング：SGACL ポリシーの設定は、Cisco Secure ACS または Cisco Identity Services Engine の主にポリシー管理機能によって実行する必要があります。後者については『Cisco Identity Services Engine User Guide』を参照してください。

- 認可変更（CoA）：更新されたポリシーは、SGACL ポリシーが ISE で変更され、CoA が CTS デバイスにプッシュされるとダウンロードされます。

SGACL モニター モード

Cisco TrustSec の事前導入段階で、管理者は、モニターモードを使用して、ポリシーが意図したとおりに機能することを確認するために、セキュリティポリシーを適用しない状態でテストします。セキュリティポリシーが意図したとおり機能しない場合には、モニターモードが、その問題を識別するための便利なメカニズムと、SGACL の適用を有効にする前にポリシーを修正する機会を提供します。これにより、管理者は、ポリシーを適用する前にポリシーアクションの結果をより可視的に確認でき、対象のポリシーがセキュリティ要件を満たしている（ユーザーが認証されなければリソースへのアクセスは拒否される）ことを確認できます。

モニタリング機能は、SGT-DGT ペア レベルで提供されます。SGACL モニター モード機能を有効にすると、拒否アクションがライン カード上の ACL 許可として実装されます。これにより、SGACL カウンタおよびロギングでは、接続が SGACL ポリシーによりどう処理されているかを表示できます。すべてのモニター対象トラフィックが許可されるため、SGACLモニターモードでは、SGACL によるサービスの中断はありません。

CTS SGACL サポートの設定方法

SGACL ポリシーの適用のグローバルな有効化

Cisco TrustSec 対応ルーテッドインターフェイスの SGACL ポリシーの強制を有効化するには、次のタスクを実行します。

```
enable
configure terminal
cts role-based enforcement
```

インターフェイスあたりの SGACL ポリシーの適用の有効化

cts role-based enforcement コマンドを使用すると、SGACL のグローバルな適用を有効にして、特定のインターフェイスでは無効にすることができます。また、SGACL の適用は、グローバルで有効化しなくても、特定のインターフェイスで有効化できます。

インターフェイスでの SGACL ポリシーの適用を有効化するには、次のタスクを実行します。

```
enable
configure terminal
interface GigabitEthernet 0/1/1
cts role-based enforcement
```

IPv6 SGACL アクセス制御エントリの設定

SGACL は、次のコマンドを使用して、拡張名前付き ACL と同様に定義されます。

```
Device(config)#ipv6 access-list role-based sgacl1
IPV6 Role-based Access List Configuration commands:
  default   Set a command to its defaults
  deny      Specify packets to reject
  exit      Exit from access-list configuration mode
  no        Negate a command or set its defaults
  permit    Specify packets to forward
  remark    Access list entry comment
  sequence  Sequence number for this entry
```

権限マトリックスセルへの SGACL のアタッチ

```
Device(config)#cts role-based permissions from 100 to 200
  WORD  Role-based Access-list name
  ipv4  Protocol Version - IPv4
  ipv6  Protocol Version - IPv6
```

このコマンドは、特定 <SGT, DGT> ペアの RBACL のリストを定義、置換、または削除します。このポリシーは、同じ SGT、DGT に対するダイナミックなポリシーがない場合に有効になります。デフォルトでは、IPv4 タイプの RBACL のみをアタッチできます。IPv6 SGACL を追加するには、**ipv6** を明示的に指定します。

SGACL ポリシーの手動設定

SGACL ポリシーを手動で設定するには、次のタスクを実行します。

```
enable
configure terminal
ip access-list role-based allow_webtraff
10 permit tcp dst eq 80
20 permit tcp dst eq 443
cts role-based permissions from 55 to 66 allow_webtraff
end
```

ダウンロードされた SGACL ポリシーのリフレッシュ

ダウンロードされた SGACL ポリシーを更新するには、次のタスクを実行します。

```
enable
cts refresh policy
```

または

```
enable
```

```
cts refresh policy sgt 10
```

SGACL モニター モードの設定

SGACL モニターモードを設定する前に、Cisco TrustSec が有効になっていることを確認してください。

（注） デバイスレベルのモニターモードは、いずれかの設定が適用されないかぎり、デフォルトでは有効になりません。ISE からダウンロードされた SGACL の場合、ISE からのモニターモードの状態が常に優先されます。これは、セルごとのモニターモードと、すべてのセルに適用されるグローバルモニターモードの両方に適用されます。

```
configure terminal
cts role-based monitor enable
cts role-based monitor permissions from 2 to 3 ipv4
show cts role-based permissions from 2 to 3 ipv4
show cts role-based counters ipv4
```

IPv6 SGACL ACE の設定

IPv6 SGACL のアクセス制御エントリ（ACE）を定義するには、次の CLI が使用されます。

```
Device(config)#ipv6 access-list role-based sgacl1
Device(config-ipv6rb-acl)#permit ipv6
Device(config-ipv6rb-acl)#exit
Device(config)#cts role-based permissions from 100 to 200 ipv6 sgacl1
```

（注） IPv6 ACL 設定はスタティック SGACL 用であり、ダイナミック SGACL の場合は、ACE が ISE で設定されます。

CTS SGACL サポートの設定例

例：CTS SGACL のサポート

次に、show cts role-based permissions コマンドの出力例を示します。

```
Router# show cts role-based permissions

IPv4 Role-based permissions default:
        default_sgacl-02
```

```
        Permit IP-00
IPv4 Role-based permissions from group 55:SGT_55 to group 66:SGT_66 (configured):
        allow_webtraff
RBACL Monitor All for Dynamic Policies : FALSE
RBACL Monitor All for Configured Policies : FALSE


Router#sh cts role-based permissions ipv6
IPv6 Role-based permissions from group 2103:Cisco_UC_Servers to group
2104:Exchange_Servers:
        SGACL_5-10-ipv6
RBACL Monitor All for Dynamic Policies : FALSE
RBACL Monitor All for Configured Policies : FALSE
```

次に、ダイナミック SGACL にのみ適用される show cts policy sgt コマンドの出力例を示します。

```
Router# show cts policy sgt

CTS SGT Policy
==============
RBACL Monitor All : FALSE
RBACL IP Version Supported: IPv4
SGT: 0-02:Unknown
SGT Policy Flag: 0xc1408801
RBACL Source List: Empty
RBACL Destination List: Not exist
RBACL Multicast List: Not exist
RBACL Policy Lifetime = 1800 secs
RBACL Policy Last update time = 20:58:28 IST Wed Jul 13 2016
Policy expires in 0:00:24:05 (dd:hr:mm:sec)
Policy refreshes in 0:00:24:05 (dd:hr:mm:sec)
Cache data applied = NONE

SGT: 65535-46:ANY
SGT Policy Flag: 0x41400001
RBACL Source List:
  Source SGT: 65535-46:ANY-0, Destination SGT: 65535-46:ANY-0
  rbacl_type = 80
  rbacl_index = 1
  name   = default_sgacl-02
  IP protocol version = IPV4
  refcnt = 1
  flag   = 0x40000000
  stale  = FALSE
  RBACL ACEs:
    permit icmp
    permit ip
  Source SGT: 65535-46:ANY-0, Destination SGT: 65535-46:ANY-0
  rbacl_type = 80
  rbacl_index = 2
  name   = Permit IP-00
  IP protocol version = IPV4
  refcnt = 1
  flag   = 0x40000000
  stale  = FALSE
  RBACL ACEs:
    permit ip
RBACL Destination List: Not exist
RBACL Multicast List: Not exist
RBACL Policy Lifetime = 1800 secs
```

```
RBACL Policy Last update time = 20:58:28 IST Wed Jul 13 2016
Policy expires in 0:00:24:05 (dd:hr:mm:sec)
Policy refreshes in 0:00:24:05 (dd:hr:mm:sec)
Cache data applied = NONE
```

次に、ダイナミック SGACL にのみ適用される show cts rbacl コマンドの出力例を示します。

```
Router# show cts rbacl

CTS RBACL Policy
================
RBACL IP Version Supported: IPv4 & IPv6
  name   =multple_ace-16
  IP protocol version = IPV4
  refcnt = 4
  flag = 0x40000000
  stale = FALSE
  RBACL ACEs:
      permit icmp
      deny tcp

  name   =default_sgacl-02
  IP protocol version = IPV4
  refcnt = 2
  flag = 0x40000000
  stale = FALSE
  RBACL ACEs:
      permit icmp
      permit ip

  name   =SGACL_256_ACE-71
  IP protocol version = IPV4
```

例：SGACL モニターモードの設定

次に、SGACL モニターモードの設定例を示します。

```
Device# configure terminal
Device(config)# cts role-based monitor enable
Device(config)# cts role-based permissions from 2 to 3 ipv4
Device# show cts role-based permissions from 2 to 3 ipv4

        IPv4 Role-based permissions from group 2:sgt2 to group 3:sgt3 (monitored):
        denytcpudpicmp-10
        Deny IP-00

Device# show cts role-based permissions from 2 to 3 ipv4 details

        IPv4 Role-based permissions from group 2:sgt2 to group 3:sgt3 (monitored):
        denytcpudpicmp-10
        Deny IP-00
        Details:
        Role-based IP access list denytcpudpicmp-10 (downloaded)
        10 deny tcp
```

```
        20 deny udp
        30 deny icmp
        Role-based IP access list Permit IP-00 (downloaded)
        10 permit ip
Device# show cts role-based permissions ipv6
IPv6 Role-based permissions from group 201 to group 22 (configured):
        g6
IPv6 Role-based permissions from group 100 to group 200 (configured):
        sgacl1
RBACL Monitor All for Dynamic Policies : FALSE
RBACL Monitor All for Configured Policies : FALSE

Device# show cts role-based counters ipv4
Role-based IPv4 counters
From    To      SW-Denied  HW-Denied  SW-Permitt HW-Permitt SW-Monitor HW-Monitor
100     200     0          0          0          0          0          0
101     201     0          0          0          0          0          0

Device# show cts role-based counters ipv6
Role-based IPv6 counters
From    To      SW-Denied  HW-Denied  SW-Permitt HW-Permitt SW-Monitor HW-Monitor
201     22      0          0          0          0          0          0
100     200     0          0          0          0          0          0
```

例：ダウンロードされた SGACL ポリシーのリフレッシュ

次に、ダウンロードした SGACL ポリシーをリフレッシュするための設定例を示します。このコマンドは特権 EXEC モードで実行されます。

```
Router#cts refresh policy
Router#cts refresh policy sgt
```

CTS SGACL サポートに関する追加情報

関連資料

MIB

MIB	MIB のリンク
CISCO-MIB	選択したプラットフォーム、Cisco IOS リリース、およびフィーチャ セットに関する MIB を探してダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

シスコのテクニカル サポート

説明	リンク
シスコのサポート Web サイトでは、シスコの製品やテクノロジーに関するトラブルシューティングにお役立ていただけるように、マニュアルやツールをはじめとする豊富なオンライン リソースを提供しています。 お使いの製品のセキュリティ情報や技術情報を入手するために、Cisco Notification Service（Field Notice からアクセス）、Cisco Technical Services Newsletter、Really Simple Syndication（RSS）フィードなどの各種サービスに加入できます。 シスコのサポート Web サイトのツールにアクセスする際は、Cisco.com のユーザ ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

CTS SGACL サポートの機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *127 : CTS SGACL* サポートの機能情報

機能名	リリース	機能情報
CTS SGACL のサポート	Cisco IOS Release 16.3	CTS SGACL のサポート機能は、IP アドレスではなく、セキュリティ アソシエーションまたはセキュリティ グループ タグ値に基づいたステートレスのアクセス制御メカニズムを提供します。 Cisco IOS リリース 16.3 では、この機能は、シスコ アグリゲーション サービス ルータ 1000 シリーズとサービス統合型ルータ 4000 シリーズに導入されました。 この機能により、次のコマンドが導入されました。**cts role-based enforcement, ip access-list role-based, cts role-based permissions, show cts role-based permissions, show cts rbacl**。

機能名	リリース	機能情報
TrustSec SGACL モニターモード	Cisco IOS XE Everest 16.4.1	TrustSec SGACL モニターモード機能は、ポリシーが意図したとおりに機能することを強制することなく、セキュリティポリシーをモニターします。モニターモードは、機能しないセキュリティポリシーを識別するための便利なメカニズムと、SGACL の適用を有効にする前にポリシーを修正する機会を提供します。 この機能により、次のコマンドが導入されました。**cts role-based monitor enable, cts role-based monitor permissions**。
IPv6 の有効化：SGACL の適用	Cisco IOS XE Fuji 16.8.1	IPv6 のサポートが導入されました。

第 92 章

TrustSec 動作データへの外部アクセス

Cisco TrustSec は、信頼できるネットワーク デバイスのドメインを確立することによってセキュア ネットワークを構築します。ドメイン内の各デバイスは、そのピアによって認証されます。ドメイン内のデバイス間リンクでの通信は、暗号化、メッセージ整合性検査、データパスリプレイ防止メカニズムを組み合わせたセキュリティで保護されます。

Cisco TrustSec は、グループベースのアクセス制御を使用したセキュリティも提供します。Cisco TrustSec ドメイン内のアクセスポリシーは、トポロジとは無関係であり、ネットワークアドレスではなく送信元デバイスおよび宛先デバイスのロールに基づいています。個々のパケットには、送信元のセキュリティ グループ番号のタグが付けられます。

Cisco TrustSec は、設定データと動作データの 2 種類のデータを生成します。設定データは設定プログラミングモデルから取得され、動作データは動作データモデルから取得されます。

TrustSec の運用データには、YANG を使用して構造化されたデータを処理できる外部アプリケーションからアクセスできます。Netconf および Restconf プロトコルを使用して、外部デバイスは Cisco デバイスから動作情報を抽出できます。これにより、外部インターフェイスを介したプログラマビリティが提供されます。

Cisco TrustSec 動作データへの外部アクセスの前提条件

- Cisco TrustSec、ネットワークデバイス間での SXP を使用したセキュリティタグの伝達、およびポリシーの適用について理解している必要があります。
- Cisco IOS XE Everest 16.5.1 以降、Cisco TrustSec は、IP Services または IP Base のライセンスでのみ暗号 k9 イメージをサポートします。

- CiscoデバイスでNETCONFまたはRESTCONFプロトコルを有効にする必要があります。NETCONFプロトコルを有効にするには、コンフィギュレーション モードで **netconf-yang** コマンドを使用します。

（注） LANbaseライセンスはSXPのみをサポートします。SGACLおよびIP-SGT動作データはサポートされていません。

Cisco TrustSec 動作データへの外部アクセスの制限

- SGACL ポリシーと IP-SGT および SXP 接続に限定された動作データには、外部からのみアクセスできます。
- 次の TrustSec 動作データのリストは、Cisco IOS XE Everest 16.5.1 ではサポートされていません。
  - Cisco TrustSec PAC データ、環境データ、およびリンクレベルの動作データ。
  - IPV6 ベースの SGACL ポリシー、IP-SGT マッピング、および SXP 接続動作データ。
  - VFR ベースの IP-SGT マッピングおよび SXP 接続動作データ。

Cisco TrustSec 動作データに関する情報

YTOOLなどのアプリケーションを使用すると、Ciscoデバイスに直接ログインして専用のコマンドで情報を取得することなく、外部インターフェイスから Cisco TrustSec の動作データに柔軟にアクセスできます。

外部デバイスからは、次のタイプの動作データにアクセスできます。

- 特定のデバイスのアクティブな SXP 接続。

  次に、デバイスの SXP 接続を表示する出力例を示します。

```
Device# show cts sxp connections brief
 SXP              : Enabled
 Highest Version Supported: 4
 Default Password : Not Set
 Default Source IP: Not Set
Connection retry open period: 120 secs
Reconcile period: 120 secs
Retry open timer is running
Peer-Sequence traversal limit for export: Not Set
Peer-Sequence traversal limit for import: Not Set

_____________________________________________________________________________________
---------------
Peer_IP          Source_IP        Conn Status
    Duration
```

```
---------------------------------------------------------------------------
---------------
10.10.1.1         11.11.1.1         Off
    0:00:36:24 (dd:hr:mm:sec)
10.10.1.2         11.11.1.2         Off
    0:00:36:24 (dd:hr:mm:sec)
10.10.1.3         11.11.1.3         Off
    0:00:36:23 (dd:hr:mm:sec)
10.10.1.4         11.11.1.4         Off
    0:00:36:22 (dd:hr:mm:sec)
10.10.1.5         11.11.1.5         Off
    0:00:36:22 (dd:hr:mm:sec)
10.10.1.6         11.11.1.6         Off
    0:00:36:21 (dd:hr:mm:sec)
10.10.1.7         11.11.1.7         Off
    0:00:36:21 (dd:hr:mm:sec)
10.10.1.8         11.11.1.8         Off
    0:00:36:20 (dd:hr:mm:sec)
10.10.1.9         11.11.1.9         Off
    0:00:36:15 (dd:hr:mm:sec)
10.10.1.10        11.11.1.10        Off(Speaker)::Off(Listener)
    0:00:33:40 (dd:hr:mm:sec)::0:00:33:40 (
dd:hr:mm:sec)
```

- IP-SGT マッピング情報。

  すべての送信元 IP が、対応する SGT にマッピングされ、IP-SGT バインディングが作成されます。このマッピング情報は、ロールベースマネージャ（RBM）データベースに保存されます。

  次に、IP-SGT マッピング情報を表示する出力例を示します。

```
Device# show cts role-based sgt-map all
Active IPv4-SGT Bindings Information

IP Address              SGT     Source
============================================
10.10.10.10             10      CLI
20.20.20.20             20      CLI
30.30.30.30             30      CLI
32.1.1.32               40      CLI
45.1.1.45               100     CLI
69.1.1.1                103     CLI

IP-SGT Active Bindings Summary
============================================
Total number of CLI      bindings = 6
Total number of active   bindings = 6

asr1k-cts-2006#
```

- すべてのデータパスに現在適用されているポリシーの名前。

  SGACL ポリシーは、2 つの TrustSec 対応エンドポイント間で SGT タグ付きパケットが転送されるときに適用されます。ポリシーは、スタティックまたはダイナミックのいずれかです。デバイスで CLI コマンドの **cts role-based permissons** を使用して設定されるポリシーは、スタティックポリシーです。ダイナミックポリシーは Cisco ISE（Identiy Services Engine）で設定されます。ダイナミックポリシーは、スタティックポリシーに優先します。スタティックポリシーは、ダイナミックポリシーがない場合にのみ適用されます。

  次に、SGT タグ付きトラフィックのポリシーを表示する出力例を示します。

```
Device# show cts role-based permissions
IPv4 Role-based permissions default:

        Permit IP-00
IPv4 Role-based permissions from group 10:SGT_10 to group 10:SGT_10:

        Collab1-10
IPv4 Role-based permissions from group 10:SGT_10 to group 20:SGT_20:

        SGACL_2-30
IPv4 Role-based permissions from group 11:SGT_11 to group 20:SGT_20:

        SGACL_2-30

        SGACL_3-10

        SGACL_4-90
IPv4 Role-based permissions from group 12:SGT_12 to group 20:SGT_20:

        SGACL_3-10
IPv4 Role-based permissions from group 13:SGT_13 to group 20:SGT_20:

        SGACL_4-90
IPv4 Role-based permissions from group 14:SGT_14 to group 20:SGT_20:
        SGACL_5-20
IPv4 Role-based permissions from group 15:SGT_15 to group 20:SGT_20:
        SGACL_6-30
IPv4 Role-based permissions from group 16:SGT_16 to group 20:SGT_20:
        SGACL_101-90
IPv4 Role-based permissions from group 17:SGT_17 to group 20:SGT_20:
        SGACL_2-30
IPv4 Role-based permissions from group 18:SGT_18 to group 20:SGT_20:
        SGACL_3-10
IPv4 Role-based permissions from group 19:SGT_19 to group 20:SGT_20:
        SGACL_3-10
IPv4 Role-based permissions from group 10:SGT_10 to group 30:SGT_30:
        SGACL_6-30
IPv4 Role-based permissions from group 10:SGT_10 to group 40:SGT_40:
        SGACL_2-30
IPv4 Role-based permissions from group 10:SGT_10 to group 100:SGT_100:
        SGACL_4-90
IPv4 Role-based permissions from group 102:SGT_102 to group 100:SGT_100:
        Permit IP-00
IPv4 Role-based permissions from group 102:SGT_102 to group 103:SGT_103:
        SGACL_2-30
RBACL Monitor All for Dynamic Policies : FALSE
RBACL Monitor All for Configured Policies : FALSE

asr1k-cts-2006#
```

- 各ポリシーの内容。これには、ポリシー内のACE（アクセス制御エントリ）と、ポリシーのライフタイムおよび更新時間が含まれます。

  ポリシーには、最大 256 の ACE を組み合わせて含めることができます。ライフタイムと更新時間の情報は、ダイナミックポリシーにのみ適用されます。スタティックポリシーのライフタイムと更新時間の値は 0 になります。

  次に、SGT タグ付きトラフィックのポリシーを表示する出力例を示します（出力の一部のみが表示されます）。

```
Device# show cts policy sgt
CTS SGT Policy
==============
RBACL Monitor All : FALSE
RBACL IP Version Supported: IPv4
SGT: 0-02:Unknown
SGT Policy Flag: 0x41408001
RBACL Source List: Empty
RBACL Destination List: Not exist
RBACL Multicast List: Not exist
RBACL Policy Lifetime = 1800 secs
RBACL Policy Last update time = 15:56:42 IST Mon Feb 20 2017
Policy expires in 0:00:03:04 (dd:hr:mm:sec)
Policy refreshes in 0:00:03:04 (dd:hr:mm:sec)
Cache data applied = NONE

SGT: 65535-52:ANY
SGT Policy Flag: 0x41400001
RBACL Source List:
  Source SGT: 65535-52:ANY-0, Destination SGT: 65535-52:ANY-0
  rbacl_type = 80
  rbacl_index = 1
  name   = Permit IP-00
  IP protocol version = IPV4
  refcnt = 4
  flag   = 0x41000000
  stale  = FALSE
  RBACL ACEs:
    permit ip

RBACL Destination List: Not exist
RBACL Multicast List: Not exist
RBACL Policy Lifetime = 1800 secs
RBACL Policy Last update time = 15:56:43 IST Mon Feb 20 2017
Policy expires in 0:00:03:05 (dd:hr:mm:sec)
Policy refreshes in 0:00:03:05 (dd:hr:mm:sec)
Cache data applied = NONE

SGT: 10-2770:SGT_10
SGT Policy Flag: 0x41400001
RBACL Source List:
  Source SGT: 10-2770:SGT_10-0, Destination SGT: 10-2770:SGT_10-0
  rbacl_type = 80
  rbacl_index = 1
  name   = Collab1-10
  IP protocol version = IPV4
  refcnt = 2
  flag   = 0x41000000
  stale  = FALSE
  RBACL ACEs:
    permit ip

RBACL Destination List: Not exist
RBACL Multicast List: Not exist
RBACL Policy Lifetime = 1800 secs
RBACL Policy Last update time = 15:56:43 IST Mon Feb 20 2017
Policy expires in 0:00:03:04 (dd:hr:mm:sec)
Policy refreshes in 0:00:03:04 (dd:hr:mm:sec)
Cache data applied = NONE

SGT: 20-44:SGT_20
SGT Policy Flag: 0x41400001
RBACL Source List:
```

```
Source SGT: 10-2770:SGT_10-0, Destination SGT: 20-44:SGT_20-0
rbacl_type = 80
rbacl_index = 1
name   = SGACL_2-30
IP protocol version = IPV4
refcnt = 8
flag   = 0x41000000
stale  = FALSE
RBACL ACEs:
  permit ip

Source SGT: 12-17:SGT_12-0, Destination SGT: 20-44:SGT_20-0
rbacl_type = 80
rbacl_index = 2
name   = SGACL_3-10
IP protocol version = IPV4
refcnt = 5
flag   = 0x41000000
stale  = FALSE
RBACL ACEs:
  permit ip

Source SGT: 13-14:SGT_13-0, Destination SGT: 20-44:SGT_20-0
rbacl_type = 80
rbacl_index = 3
name   = SGACL_4-90
IP protocol version = IPV4
refcnt = 5
flag   = 0x41000000
stale  = FALSE
RBACL ACEs:
  deny tcp

Source SGT: 14-14:SGT_14-0, Destination SGT: 20-44:SGT_20-0
rbacl_type = 80
rbacl_index = 4
name   = SGACL_5-20
IP protocol version = IPV4
refcnt = 2
flag   = 0x41000000
stale  = FALSE
RBACL ACEs:
  permit ip

Source SGT: 15-1410:SGT_15-0, Destination SGT: 20-44:SGT_20-0
rbacl_type = 80
rbacl_index = 5
name   = SGACL_6-30
IP protocol version = IPV4
refcnt = 4
flag   = 0x41000000
stale  = FALSE
RBACL ACEs:
  permit icmp log
  permit udp log
  permit tcp log

Source SGT: 16-14:SGT_16-0, Destination SGT: 20-44:SGT_20-0
rbacl_type = 80
rbacl_index = 6
name   = SGACL_101-90
IP protocol version = IPV4
refcnt = 2
flag   = 0x41000000
```

```
stale   = FALSE
RBACL ACEs:
  permit ip
```

外部デバイス YTOOL の設定方法

YTOOL を設定する前に、Cisco デバイスで NETCONF または RESTCONF プロトコルが有効になっていることを確認します。YTOOL が Cisco デバイスと通信するには、これらのプロトコルのいずれかが必要です。

（注） NETCONF プロトコルを有効にするには、コンフィギュレーション モードで **netconf-yang** コマンドを使用します。NETCONF を有効にしたら、CLI で **show onep session all** を実行して、NETCONF を使用するために必要な 3 つのプロセスが実行されているかどうかを確認します。NETCONF は、これらの 3 つのプロセスが実行された後にのみ使用できます。

また、デバイスとの通信に使用する IP アドレスを特定します。

（注） YTOOL は「yang-explorer」とも呼ばれます。このアプリケーションは、次の場所からダウンロードできます。

Yang Explorer：

YTOOL を Cisco デバイスに接続するには、Cisco デバイスを YTOOL に追加します。YTOOL にシスコデバイスを追加する手順は、次のとおりです。

1. YTOOL を開きます。
2. **[管理（Admin）]** を選択します。
3. **[Ytool ユーティリティ（Ytool Utilities）]** ページで、**[プロファイルの管理（Manage Profiles）]**（**[デバイスプロファイルの管理（Manage Device Profiles）]** の下）を選択します。
4. **[デバイスプロファイル名（Device Profile Name）]** ドロップダウンから **[新規デバイス（New Device）]** を選択します。
5. [デバイスプロファイルの管理（Manage Device Profile）] ページで、デバイスのすべての詳細情報（テストデバイスの IP アドレス、テストデバイスの SSH ポート番号、NETCONF ユーザー名、NETCONF パスワードなど）を入力します。

図 *22 :* デバイス プロファイルの管理

6. デバイスへの接続を確認するには、**[ビルド（Build）]** > **[デバイス設定（Device Settings）]** の順に選択します。**[プロファイル（Profile）]** からデバイスを選択し、**[Hello]** をクリックします。**[コンソール（Console）]** に応答が表示された場合は、YTOOL がデバイスと通信できることを意味します。

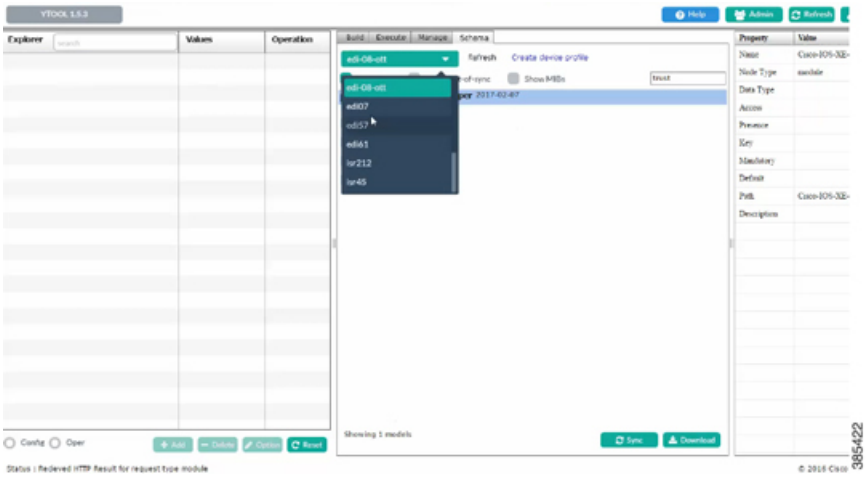
（注） Cisco デバイスと通信するために、YANG を使用して構造化されたデータを処理できる他の外部アプリケーションを選択できます。このセクションは、Cisco デバイスにアクセスするために YTOOL を選択した場合にのみ関係します。

動作データへのアクセス

開始する前に、動作データを抽出する Cisco デバイスが YTOOL で設定されていることを確認します。詳細については、「外部デバイス YTOOL の設定方法」を参照してください。

1. Cisco デバイスから Cisco TrustSec 動作情報スキーマをダウンロードします。
   1. **[スキーマ（Schema）]** を選択します。
   2. デバイスを選択します。デバイス内のスキーマのリストが表示されます。

図 *23* : デバイスの選択

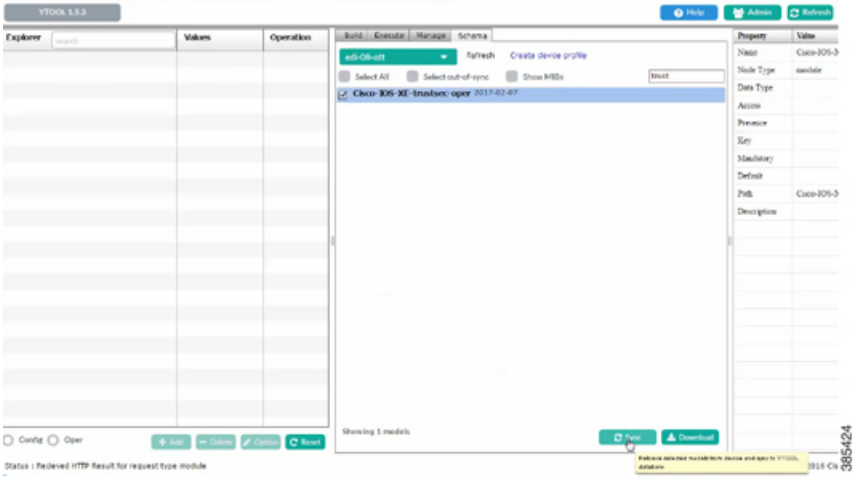


3. Cisco TrustSec 動作情報スキーマを選択します。検索ボックスを使用して、このスキーマを検索してください。

（注） 動作情報スキーマの名前は「**oper**」で終わります。

4. [同期（Sync）] をクリックします。スキーマが YTOOL にダウンロードされます。

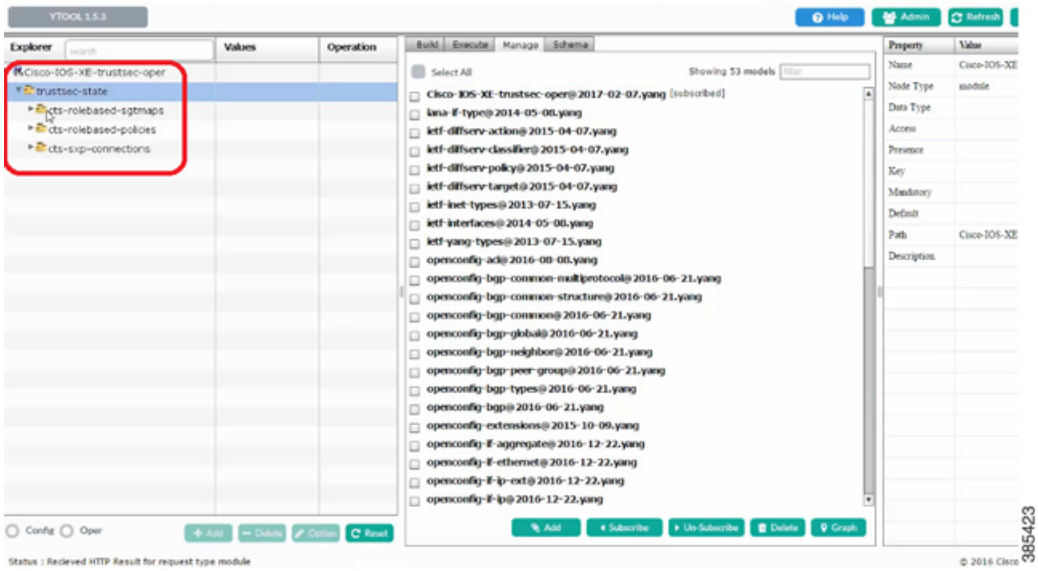
図 *24* : スキーマのダウンロード



2. YTOOL でダウンロードした動作情報スキーマに登録します。
   1. **[管理（Manage）]** を選択します。
   2. スキーマのリストから、動作情報スキーマを選択します。
   3. [Subscribe] をクリックします。

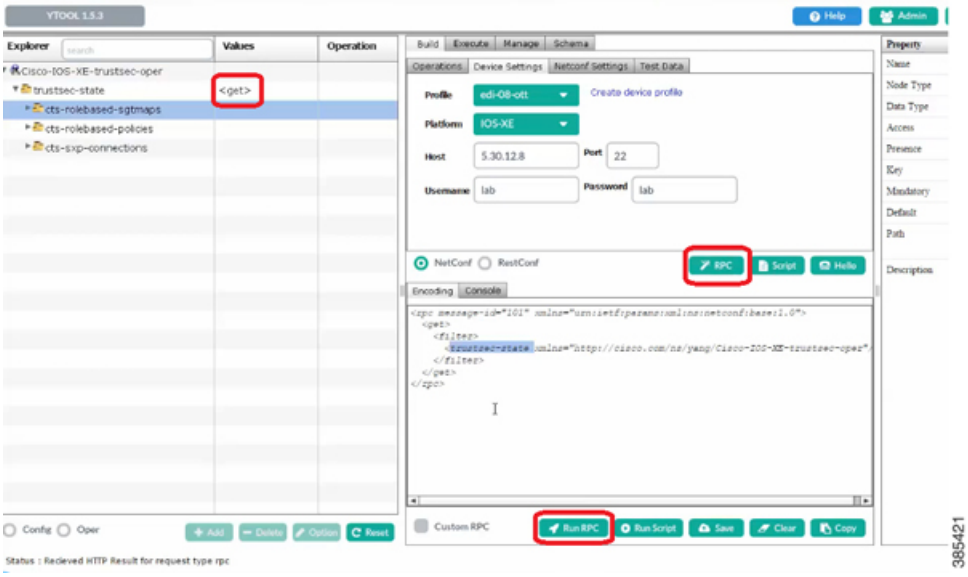
（注） 登録すると、スキーマが [エクスプローラ（Explorer）] の欄に表示されます。

図 *25* : スキーマの登録



3. スキーマを使用して、選択した動作データを取得します。
   1. 動作情報スキーマの関連情報レベルに対して、**[値（Values）]** の欄の **[取得（get）]** を選択します。
   2. **[RPC]** をクリックします。XML 生成の RPC メッセージが生成されます。
   3. **[RPC の実行（Run RPC）]** をクリックします。動作データは、RPC 生成の XML 形式で Cisco デバイスから取得されます。

図 *26* : 動作データの取得



（注） 運用データへのアクセスに使用されるコマンドについては、「Cisco TrustSec 動作データに関する情報 （1092 ページ）」の項を参照してください。

（注） Cisco デバイスと通信するために、YANG を使用して構造化されたデータを処理できる他の外部アプリケーションを選択できます。このセクションは、Cisco デバイスにアクセスするために YTOOL を選択した場合にのみ関係します。

第 VIII 部

Access Node Control Protocol

第 93 章

Access Node Control Protocol

Access Node Control Protocol（ANCP）機能は、デジタル加入者線アクセスマルチプレクサ（DSLAM）とブロードバンド リモート アクセス サーバー（BRAS）の間の通信を強化し、マルチプレクサ側とサーバー側の間でのイベント、アクション、および情報要求の交換を可能にします。その結果、どちらの側も適切なアクションを実装できます。

Access Node Control Protocol の前提条件

Transmission Control Protocol（TCP）を介して ANCP を実行するには、ブロードバンド リモート アクセス サーバー（BRAS）で IP を有効にする必要があります。RADIUS から BRAS へのインタラクションは、ANCP には必要なく、RADIUS サーバーに依存します。

リリースおよびプラットフォーム サポートの詳細については、Access Node Control Protocol に関する機能情報 （1118 ページ）を参照してください。

Access Node Control Protocol に関する制約事項

Cisco IOS XE リリース 2.4 は、ブロードバンド リモート アクセス サーバー（BRAS）からの RADIUS サーバーとのインタラクションをサポートしています。RADIUS から BRAS へのインタラクションは、ANCP には必要なく、RADIUS サーバーに依存します。

Access Node Control Protocol に関する情報

ANCPは、アプリケーションから独立したまま、複数の加入者からのトラフィックを集約し、任意のアプリケーションの情報を配信するために使用されます。ANCPは現在、デジタル加入者線（DSL）ブロードバンド環境の DSLAM とブロードバンド リモート アクセス サーバーの間のアプリケーションで使用されています。

ANCP 機能により、DSL 集約マルチプレクサ（DSLAM）とネットワークエッジデバイスの間の緊密な通信が可能になります。DSLAM と BRAS の間で ANCP を使用すると、イベント、アクション、および情報要求の交換が可能になり、DSLAM と BRAS で適切なアクションが発生します。

ANCP アーキテクチャは、ANCP の次の使用をサポートしています。

レートアダプティブモード

レートアダプティブモードは、特定の回線の回線ビットレートを最大化するのに役立ちます。そのレートは、回線で達成される信号の品質に依存します。レートアダプティブモードでは、DSLAM からブロードバンド リモート アクセス サーバーに DSL モデムの回線レートが伝えられます。

ANCP を実行している BRAS は、ANCP ネイバー（DSLAM）からの TCP 要求をリッスンします。

- TCP セッションの確立後：ANCP が、BRAS とそのネイバーの間の隣接関係を確立するためにメッセージの交換を開始します。
- 隣接関係の確立後：ANCP イベント メッセージを DSLAM から BRAS に送信できます。

レートアダプティブDSLは、信号品質を使用して回線速度を調整します。BRASは、通常、加入者インターフェイスを、サービスライセンス契約（SLA）で合意された最大帯域幅に設定します。

顧客宅内機器（CPE）が回線速度よりも低いデータレートに同期されると、DSLAM でセルまたはパケットの損失が発生します。これを防ぐために、DSLAM は、ANCP を使用して、新しく調整された回線レートを BRAS に通知できます。

顧客側のポートがアクティブ化または非アクティブ化すると、次のようになります。

- アクティブ化：DSLAM が Port Up メッセージを BRAS に送信します。ANCP によって提供される情報に従って、適切な Quality of Service（QoS）が有効になります。
- 非アクティブ化：DSLAM が Port Down メッセージを BRAS に送信します。ANCP は、DSLAMによって送信されたDSLの状態（通常、サイレントまたはアイドル）を報告します。ブロードバンドリモートアクセスサーバーが別のPort Upメッセージを受信すると、加入者セッションは、タイムアウトになるか、新しいシェーピングレートで更新されます。インターフェイスのシェーピングレートは、ルータが新しい Port Up メッセージを受信するまで変更されません。

RADIUS インタラクション

ブロードバンド リモート アクセス サーバーと RADIUS サーバーの間のインタラクションは、ルータから RADIUS へのものです。

BRAS は、次の属性および属性値ペア（AVP）を RADIUS サーバーに送信します。

ANCP 回線レート	アップストリームデータ レート	ダウンストリームデータ レート	出力ポリシー名
VSA 39	属性 197、Ascend-Data-Rate	属性 255、Ascend-Xmit-Rate	属性 77、Connect-Speed-Info
	属性タイプ 38、受信接続速度 AVP	属性タイプ 24、送信接続速度 AVP	

BRAS は、Point-to-Point Protocol（PPPoE）を使用して、認証、許可、およびアカウンティング（AAA）モジュールとやりとりします。RADIUS は、情報を処理し、適切なアクションを実行します。

ポート マッピング

ポートマッピングは、DSLAM の顧客宅内機器（CPE）クライアントを BRAS の VLAN サブインターフェイスに関連付けます。VLAN には、802.1Q または Queue-in-Queue（Q-in-Q）階層型 VLAN が含まれます。ポートマッピングは、特定の DSLAM ネイバーを持つ CPE クライアント ID をグループ化することによって、BRAS においてグローバル コンフィギュレーション モードで設定されます。

ポートは 2 つの手法でマッピングできます。1 つ目は、最初にすべての VLAN サブインターフェイスを設定してから、ANCP ネイバーマッピングを設定します。2 つ目は、インターフェイスの直下でマッピングを設定します。

たとえば、次のコマンドは、Q-in-Q VLAN サブインターフェイスのポートマッピングを設定します。

```
ancp neighbor name
dslam-name
id
dslam-id
dot1q

outer-vlanid
 second-dot1q

inner-vlanid
 [interface

type number
] client-id
 "
client-id
"
```

または

```
ancp neighbor name
dslam-name
id
 dslam-id
dot1q

outer-vlanid
 client-id
 "
client-id
"
```

client-id は、DSLAM が一意のポートごとに BRAS に送信する一意のアクセスループ回線 ID です。DSLAM は、ANCP Port Up イベントメッセージでこの ID を送信します。アクセスループ回線 ID では、次に示すように、アクセスノード識別子とデジタル加入者線（DSL）情報で構成される定義済みの形式が使用されます。

ATM/DSL

" *access-node-identifier* **atm** *slot/module/port* **.** *subinterface* **:** *vpi* **.** *vci* "

イーサネット/DSL

" *access-node-identifier* **ethernet** *slot* **/** *module* **/** *port* **.** *subinterface* [**:** *vlan-id*]"

BRAS は、DSLAM が Port Up メッセージを送信するまで、ルータのすべてのポートでデフォルト状態を Down に設定します。

非インタラクティブな運用、管理、保守

ANCP は、ブロードバンドリモートアクセスサーバーから非インタラクティブな運用、管理、保守（OAM）操作を実行するためのアウトオブバンド制御チャネルを提供します。このチャネルにより、ルータオペレータは、特定の DSLAM ポートの ANCP ポート状態を表示できます。ANCP ポートの状態の情報は、BRAS 上の ANCP ダイナミックデータベースに保存されます。

インタラクティブな OAM

インタラクティブな OAM と拡張性の改善の機能により、運用とトラブルシューティングのために、ANCP へのオンデマンド ping の機能が追加されます。

（注） この機能はデフォルトでイネーブルになり、設定は必要ありません。

General Switch Management Protocol および ANCP

ANCP は、General Switch Management Protocol（GSMP）の拡張機能です。GSMP は、プライマリネイバーがセカンダリネイバーへの接続を開始するプライマリ/セカンダリネイバー関係を

定義します。ANCP では、このプライマリ/セカンダリ関係が逆になります。つまり、BRAS（プライマリ）が DSLAM（セカンダリ）からの着信 ANCP 接続をリッスンして受け入れます。DSLAM は、イベントメッセージを使用して、トポロジ変更や Port Down または Port Up イベントなどの非同期イベントを BRAS に伝達します。

BRAS と DSLAM の間の GSMP 接続は、TCP/IP（RFC 3293）を介して行われます。DSLAM はルータへの接続を開始し、適切なインターフェイスが ANCP 対応の場合、ルータはその接続を受け入れます。

GSMP 隣接関係（アジャセンシー）プロトコルは、GSMP ネイバー関係を確立します。

1. 隣接関係の構築中は、次のことが行われます。
    1. DSLAM とルータは、それぞれの機能をネゴシエートし、2 つのエンド間の同期状態を決定します。
    2. GSMP は、転送障害が発生した場合にルータと DSLAM がローカル情報データベースの状態を保持しているかどうか、または両方のデバイスが状態の更新を必要としているかどうかを検出します。
    3. GSMP が、隣接関係を再同期する必要があると判断した場合、隣接関係同期プロセスを再開します。これには、次の場所で入手可能な ANCP 拡張のドラフトで定義されている機能ネゴシエーションが含まれます。

http://tools.ietf.org/id/draft-wadhwa-gsmp-l2control-configuration-02.txt

1. ANCP では、あるネイバー（neighbor1）にそのネイバー（neighbor2）がサポートしていない機能が含まれている場合、neighbor1 はその機能をオフにして、neighbor2 と同じ機能セットでパケットを neighbor2 に再伝達します。
2. 両方のネイバーが同じ機能セットに同意すると、隣接関係が確立されます。

Access Node Control Protocol の設定方法

ANCP を設定するには、次のグローバルまたはインターフェイス設定タスクを実行します。

イーサネット インターフェイスでの ANCP の有効化

イーサネット インターフェイス上の ANCP を有効にするには、次の作業を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **ancp adjacency timer** *interval*
4. **interface** *type number*
5. **ip address** *address mask*
6. **ancp enable**

7. **interface** *type number* **.** *subinterface*
8. **encapsulation dot1q** *vlanid* [**second-dot1q** *second-vlanid*]
9. **exit**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ancp adjacency timer** *interval* 例： `Router(config)# ancp adjacency timer 100`	ANCP 隣接タイマー間隔を設定します。これは、ANCP hello パケットを DSLAM に送信するまで待機する時間を示します。
ステップ 4	**interface** *type number* 例： `Router(config)# interface FastEthernet1/0/0`	インターフェイス コンフィギュレーション モードを開始してインターフェイスを定義します。
ステップ 5	**ip address** *address mask* 例： `Router(config-if)# ip address 10.16.1.2 255.255.0.0`	IP アドレスとサブネットマスクをインターフェイスに割り当てます。
ステップ 6	**ancp enable** 例： `Router(config-if)# ancp enable`	IP が設定されているインターフェイスで ANCP をイネーブルにします。
ステップ 7	**interface** *type number* **.** *subinterface* 例： `Router(config-if)# interface FastEthernet1/0/0.1`	サブインターフェイス コンフィギュレーション モードを開始してサブインターフェイスを定義します。
ステップ 8	**encapsulation dot1q** *vlanid* [**second-dot1q** *second-vlanid*] 例：	シングルキュー 802.1Q VLAN または Q-in-Q 階層型 VLAN のサブインターフェイスで dot1q VLAN カプセル化を有効にします。

	コマンドまたはアクション	目的
	`Router(config-subif)# encapsulation dot1q 100 second-dot1q 200`	
ステップ 9	**exit** 例： `Router(config-subif)# exit`	サブインターフェイス コンフィギュレーション モードを終了します。

ATM インターフェイスでの ANCP のイネーブル化

ancp enable コマンドは、DSLAM から ANCP メッセージを送信させる制御 VC に対してのみ設定する必要があります。ATM インターフェイス上の ANCP を有効にするには、次の作業を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **ancp adjacency timer** *interval*
4. **interface atm** *slot* / *subslot* / *port* . *subinterface*
5. **ip address** *ip-address mask*
6. **pvc** *vpi* / *vci*
7. **ancp enable**
8. **exit**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ancp adjacency timer** *interval* 例： `Router(config)# ancp adjacency timer 100`	ANCP 隣接タイマー間隔を設定します。これは、ANCP hello パケットを DSLAM に送信するまで待機する時間を示します。

	コマンドまたはアクション	目的
ステップ 4	**interface atm** *slot* / *subslot* / *port* . *subinterface* 例： `Router(config)# interface atm 2/0/1.1`	サブインターフェイス コンフィギュレーション モードを開始してサブインターフェイスを定義します。
ステップ 5	**ip address** *ip-address mask* 例： `Router(config-subif)# ip address 10.16.1.2 255.255.0.0`	IP アドレスおよびサブネットマスクをサブインターフェイスに割り当てます。
ステップ 6	**pvc** *vpi* / *vci* 例： `Router(config-subif)# pvc 2/100`	ATM PVC 上の ANCP 接続をイネーブルにするために、ATM 仮想回線コンフィギュレーション モードを開始します。
ステップ 7	**ancp enable** 例： `Router(config-if-atm-vc)# ancp enable`	IP が設定されているインターフェイスで ANCP をイネーブルにします。
ステップ 8	**exit** 例： `Router(config-if-atm-vc)# exit`	ATM 仮想回線コンフィギュレーション モードを終了します。

ブロードバンド リモート アクセス サーバー上の VLAN インターフェイスへの DSLAM ポートのマッピング

DSLAM ポートを BRAS 上の VLAN インターフェイスにマッピングするには、次の作業を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **ancp atm shaper percent-factor** *factor*
4. **interface** *type number.subinterface*
5. **encapsulation dot1q** *vlan-id*
6. **ancp neighbor name** *dslam-name* [**id** *dslam-id*] **client-id** *client-id*
7. **exit**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ancp atm shaper percent-factor** *factor* 例： `Router(config)# ancp shaper percent-factor 95`	ATM U インターフェイス接続の ANCP セル タックス アカウンティングを有効にします。
ステップ 4	**interface** *type number.subinterface* 例： `Router(config)# interface FastEthernet0/0.1`	特定のサブインターフェイスのインターフェイス コンフィギュレーション モードを開始します。
ステップ 5	**encapsulation dot1q** *vlan-id* 例： `Router(config-subif)# encapsulation dot1q 411`	指定した VLAN 上で、トラフィックの IEEE 802.1Q カプセル化を有効にします。
ステップ 6	**ancp neighbor name** *dslam-name* [**id** *dslam-id*] **client-id** *client-id* 例： `Router(config-subif)# ancp neighbor name dslam1 id 1.2.3.4 client-id "1.2.3.4. eth 0/0.1"`	VLANサブインターフェイスをマッピングするANCP アクセス DSLAM を指定します。
ステップ 7	**exit** 例： `Router(config-subif)# exit`	サブインターフェイス コンフィギュレーション モードを終了します。

ブロードバンド リモート アクセス サーバー上の PVC インターフェイスへの DSLAM ポートのマッピング

ancp neighbor name コマンドは、**pvc** および **pvc-in-range** コマンドモードで使用できます。このコマンドにより、PVC と DSLAM ポートの間の 1 対 1 マッピングが作成されます。DSLAM ポートを BRAS 上の PVC インターフェイスにマッピングするには、次の作業を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **ancp atm shaper percent-factor** *factor*
4. **interface atm** *slot* / *subslot* / *port* . *subinterface*
5. 次のいずれかを実行します。
   - **pvc** *vpi* / *vci*
   -
   - **range pvc** *start-vpi* / *start-vci* *end-vpi* / *end-vci*
6. **pvc-in-range** *vpi* / *vci*
7. **ancp neighbor name** *dslam-name* [**id** *dslam-id*] **client-id** *client-id*
8. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ancp atm shaper percent-factor** *factor* 例： `Router(config)# ancp shaper percent-factor 95`	ATM U インターフェイス接続の ANCP セル タックス アカウンティングを有効にします。
ステップ 4	**interface atm** *slot* / *subslot* / *port* . *subinterface* 例： `Router(config)# interface atm 2/0/1.1`	指定した ATM サブインターフェイスに対してインターフェイス コンフィギュレーション モードを開始します。
ステップ 5	次のいずれかを実行します。 • **pvc** *vpi* / *vci* • • **range pvc** *start-vpi* / *start-vci* *end-vpi* / *end-vci* 例： `Router(config-subif)# pvc 1/101`	PVC と DSLAM ポートの間の 1 対 1 マッピングを作成し、ATM 仮想回線コンフィギュレーション モードを開始します。 または ATM PVC の範囲を定義し、PVC 範囲コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
	例： 例： `Router(config-subif)# range pvc 9/100 9/102`	• ATM PVC の範囲が定義されている場合は、**pvc-in-range** コマンドを使用して個々の PVC を設定します。
ステップ 6	**pvc-in-range** *vpi* / *vci* 例： `Router(config-if-atm-range-pvc)# pvc-in-range 9/100`	（任意）PVC 範囲コンフィギュレーション モードで、範囲内の個々の PVC を設定します。
ステップ 7	**ancp neighbor name** *dslam-name* [**id** *dslam-id*] **client-id** *client-id* 例： `Router(config-if-atm-range-pvc)# ancp neighbor name dslam1 id 1.2.3.4 client-id "1.2.3.4. atm0/0.1"`	PVC サブインターフェイスをマッピングする ANCP アクセス DSLAM を指定します。 • このコマンドは、PVC 範囲および ATM 仮想回線コンフィギュレーション モードで使用できます。
ステップ 8	**end** 例： `Router(config-if-atm-range-pvc)# end`	PVC 範囲コンフィギュレーション モードを終了します。

Access Node Control Protocol の設定例

イーサネット インターフェイスでの Access Node Control Protocol の有効化の例

次に、イーサネット インターフェイス 2/0/1 で ANCP を有効にする方法の例を示します。

```
interface GigabitEthernet 2/0/1
 ip address 192.168.64.16 255.255.255.0
 ancp enable
!
interface GigabitEthernet 2/0/1.1
 encapsulation dot1q 100 second-dot1q 200
!
ancp adjacency timer 100
```

ATM インターフェイスでの Access Node Control Protocol のイネーブル化の例

次に、ATM インターフェイス 2/0/1.1 で ANCP を有効にする方法の例を示します。

```
interface ATM2/0/0.1 point-to-point
 description ANCP Link to one DSLAM
 no ip mroute-cache
 ip address 192.168.0.2 255.255.255.252
 pvc 254/32
   protocol ip 192.168.0.1
   ancp enable
   no snmp trap link-status
```

BRAS での DSLAM ポートと VLAN インターフェイスのマッピングの例

次に、DSLAM の CPE クライアントポートを BRAS の Q-in-Q VLAN サブインターフェイスにマッピングする例を示します。この例では、IP アドレスが 192.68.10.5 の DSLAM ネイバー（dslam1 という名前）の CPE クライアントポートが、イーサネット インターフェイス 1/0/0.2 で設定された Q-in-Q VLAN 100 および 200 にマッピングされています。また、別の CPE クライアントポートが、イーサネット インターフェイス 1/0/0.1 で設定された Q-in-Q VLAN 100 および 100 にマッピングされます。

```
interface GigabitEthernet1/0/0.1
 encapsulation dot1q 100 second-dot1q 100
 ancp neighbor name dslam1 id 192.168.10.5 client-id "192.168.10.5 ethernet1/0/0.2"
!
interface GigabitEthernet1/0/0.2
 encapsulation dot1q 100 second-dot1q 200
 ancp neighbor name dslam1 id 192.168.10.5 client-id "192.168.10.5 ethernet1/0/0.1"
!
ancp atm shaper percent-factor 95
!
```

上記の例では、ポートがサブインターフェイスレベルで直接マッピングされます。次の例に示すように、最初にすべての VLAN サブインターフェイスを設定し、次に ANCP ネイバーでマッピングを実行することもできます。

```
interface GigabitEthernet1/0/0.1
 encapsulation dot1q 100 second-dot1q 100
!
interface GigabitEthernet1/0/0.2
 encapsulation dot1q 100 second-dot1q 200
!
ancp atm shaper percent-factor 95
!
ancp neighbor name dslam1 id 192.168.10.5
 dot1q 100 second-dot1q 100 interface GigabitEthernet1/0/0.1 client-id "192.168.10.5
ethernet1/0/0.2"
!
ancp neighbor name dslam1 id 192.168.10.5
 dot1q 100 second-dot1q 200 interface GigabitEthernet1/0/0.2 client-id "192.168.10.5
ethernet1/0/0.2"
```

BRAS での DSLAM ポートと PVC インターフェイスのマッピングの例

ancp neighbor name コマンドは、DSLAM の CPE クライアントポートを BRAS 上の PVC インターフェイスにマッピングします。このコマンドは、グローバルに設定することも、PVC/PVC-in-Range モードで設定することもできます。

PVC または PVC-in-Range コンフィギュレーション モードの場合

この例では、ルータは、2つのポートまたはクライアントを持つ1つのDSLAMとインターフェイスで接続します。

```
interface ATM2/0/0.1 point-to-point
  description ANCP Link to one DSLAM
  no ip mroute-cache
  ip address 192.168.0.2 255.255.255.252
  pvc 254/32
     protocol ip 192.168.0.1 255.255.255.252
     ancp neighbor name dslam1 id 192.168.10.5 client-id "dslam-port-x-identifier"
        no snmp trap link-status
      !
interface ATM1/0/0.1 multipoint
  description TDSL clients - default TDSL 1024
  class-int speed:ubr:1184:160:10
  range pvc 10/41 10/160
    service-policy input SET-PRECEDENCE-0
    service-policy output premium-plus:l2c:25088
    pvc-in-range 10/103
      description TDSL client 16 Mbps with ANCP
      class-vc speed:ubr:17696:1184:05
      ancp neighbor name dslam1 id 192.168.10.5 client-id "dslam-port-x-identifier"
       !
  range pvc 11/41 11/160
    service-policy input SET-PRECEDENCE-0
    service-policy output premium-plus:l2c:25088
    pvc-in-range 11/108
      description TDSL client 16 Mbps with ANCP
      class-vc speed:ubr:17696:1184:05
      ancp neighbor name dslam1 id 192.168.10.5 client-id "dslam-port-y-identifier"
        !
```

グローバル コンフィギュレーション モードの場合

ancp neighbor コマンドをグローバルに設定する場合は、次の例に示すように、ATM インターフェイスの PVC 情報も指定する必要があります。

```
interface ATM1/0/0.1 multipoint
 description TDSL clients - default TDSL 1024
 class-int speed:ubr:1184:160:10
 range pvc 10/41 10/160
   service-policy input SET-PRECEDENCE-0
   service-policy output premium-plus:l2c:25088
   pvc-in-range 10/103
     description TDSL client 16 Mbps with ANCP
     class-vc speed:ubr:17696:1184:05
!
 range pvc 11/41 11/160
   service-policy input SET-PRECEDENCE-0
   service-policy output premium-plus:l2c:25088
```

```
   pvc-in-range 11/108
     description TDSL client 16 Mbps with ANCP
     class-vc speed:ubr:17696:1184:05
!
ancp neighbor name dslam1 id 192.168.10.5
 atm 10/103 interface ATM1/0/0.1 client-id "dslam-port-x-identifier"
 atm 11/108 interface ATM1/0/0.1 client-id "dslam-port-y-identifier"
```

Access Node Control Protocol に関する追加情報

関連資料

関連項目	マニュアル タイトル
ANCP コマンド	『*Cisco IOS Access Node Control Protocol Command Reference*』
IEEE 802.1q VLAN	IEEE 802.1Q カプセル化を使用する VLAN 間のルーティング設定
Queue-in-Queue VLAN タグ	IEEE 802.1Q-in-Q VLAN タグ終端

RFC

RFC	タイトル
ANCP 拡張のドラフト	『GSMP Extensions for Access Node Control Mechanism, Internet draft』
RFC 3292	『*General Switch Management Protocol (GSMP) V3*』
RFC 3293	『General Switch Management Protocol (GSMP), Packet Encapsulations for Asynchronous Transfer Mode (ATM), Ethernet and Transmission Control Protocol (TCP)』

Access Node Control Protocol に関する機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *128 : Access Node Control Protocol* に関する機能情報

機能名	リリース	機能情報
Access Node Control Protocol	Cisco IOS XE Release 2.4	この機能は、Cisco IOS XE リリース 2.4 で Cisco ASR 1000 に導入されました。 次のコマンドが導入されました。**ancp vdsl ethernet shaper**。
インタラクティブな OAM と拡張性の改善	Cisco IOS XE Release 2.4	インタラクティブな OAM と拡張性の改善の機能により、運用とトラブルシューティングのために、ANCP へのオンデマンド ping の機能が追加されます。 この機能は、Cisco IOS XE リリース 2.4 で Cisco ASR 1000 に導入されました。 次のコマンドが導入または変更されました。**ping ancp**、**show ancp neighbor port**、**show ancp port**、**show ancp session**、**show ancp session adjacency**、**show ancp session event**、および **show ancp statistics**。

第 94 章

Access-Accept メッセージでのマルチサービスアクティブ化

Access-Accept メッセージでのマルチサービスアクティブ化の機能は、Access Node Control Protocol（ANCP）の一部であり、複数のサービスを単一の RADIUS Access-Accept メッセージに含めることができます。この機能は、認可変更（CoA）メッセージでのマルチサービスアクティブ化および非アクティブ化の機能に似ていますが、この場合は、要求されたすべてのサービスアクティブ化が自動的に処理されます。つまり、サービスアクティブ化に失敗すると、それ以上のサービスアクティブ化は処理されず、Access-Accept メッセージによってすでにアクティブ化されているサービスは非アクティブ化されます。

Access-Accept メッセージでのマルチサービスアクティブ化に関する制約事項

- いずれかのサービスのアクティブ化が失敗すると、Access-Accept メッセージの未処理のサービスはすべて無視され、Access-Accept メッセージのアクティブ化されたサービスはすべて非アクティブ化されます。
- Access-Accept メッセージのサービスを介して Quality of Service（QoS）ポリシーを適用する場合、2 段階のアプリケーションプロセスが存在します。最初の段階では、ポリシーが解析され、ポリシー値がデータプレーンに送信されます。2 番目の段階では、データプレーンで QoS ポリシーが適用されます。最初の段階が正常に完了したものの、2 番目の段階が

失敗した場合、関連するサービスは、アクティブ化が成功したことを示すことができます。

Access-Accept メッセージでのマルチサービスアクティブ化に関する情報

Access-Accept メッセージでのマルチサービスアクティブ化の概要

Access-Request メッセージは、メッセージに含まれるユーザーまたはサブスクライバのプロファイルを認証するために、RADIUS クライアントから RADIUS サーバーに送信されます。ユーザーまたはサブスクライバのプロファイルの認証結果により、次のようになります。

- 受け入れ可能：RADIUS サーバーが Access-Accept メッセージを返す場合があります。
- 受け入れ不可：RADIUS サーバーが Access-Reject メッセージを返す場合があります。

マルチサービスアクティブ化を有効にするために、Access-Accept メッセージにシスコの汎用 VSA 250（SSG_ACCOUNT_INFO）エントリを複数含めることができます。各 VSA では、アクティブ化するサービス名が指定されます。

RSIM 形式

```
vsa cisco generic 250 string "Aservice-name1"
vsa cisco generic 250 string "Aservice-name2"
vsa cisco generic 250 string "Aservice-name3"
```

RADIUS 形式

```
07:06:23.234: RADIUS: Received from id 1645/36 11.12.13.2:1645, Access-Accept, len 112
07:06:23.238: RADIUS:  authenticator 92 C5 A2 F2 24 56 37 1E - 74 F4 C6 92 B0 E8 92 4C
07:06:23.238: RADIUS:  Vendor, Cisco       [26]  23
07:06:23.238: RADIUS:   ssg-account-info   [250] 17  "Aservice-name-1"
07:06:23.238: RADIUS:  Vendor, Cisco       [26]  23
07:06:23.238: RADIUS:   ssg-account-info   [250] 17  "Aservice-name-2"
07:06:23.238: RADIUS:  Vendor, Cisco       [26]  23
07:06:23.238: RADIUS:   ssg-account-info   [250] 17  "Aservice-name-3"
```

Access-Accept メッセージが受信されると、指定されたサービスが抽出され、各サービスが順番にアクティブ化されます。サービスのアクティブ化が失敗すると、Access-Accept メッセージの未処理のサービスはすべて無視され、Access-Accept メッセージのアクティブ化されたサービスはすべて非アクティブ化されます。

（注） QoS サービスの Access-Accept 複数サービス要求については、RSIM 形式は、CoA メッセージに含まれる複数サービスのアクティブ化または非アクティブ化要求には適用されません。CoA メッセージの形式は VSA 252 です。詳細については、「CoA メッセージでのマルチサービスアクティブ化および非アクティブ化」モジュールを参照してください。

VSA 250 の QoS ポリシー

セッションの確立中に、VSA 250 連結 QoS 構文を RADIUS Access-Accept メッセージとともに使用できます。構文は、VSA の連結文字列を解析し、QoS およびインテリジェント サービス ゲートウェイ（ISG）ポリシーをアクティブにします。

（注） ISG は、1 つの Access-Accept メッセージで複数の QoS サービスを管理し、メッセージを適用して静的 QoS およびパラメータ化された QoS をアクティブにします。

Access-Accept メッセージでのマルチサービスアクティブ化の設定方法

Access-Accept を使用したセッションサービスのアクティブ化

Access-Accept でセッションサービスを動的にアクティブにするには、RADIUS のサービスプロファイルで Cisco VSA 250 を設定します。RADIUS では、次の構文により、Access-Accept メッセージで VSA 250 が使用されます。

RSIM 形式

```
vsa cisco generic 250 string
"Aservice-name-1"
```

Access-Accept メッセージでのマルチサービスの設定例

VSA 250 を使用した QoS サービスのアクティブ化の例

QoS サービスをアクティブにするには、*qos:vc-qos-policy-out* 構文を RADIUS Access-Accept メッセージとともに使用します。連結文字列が解析され、QoS および ISG ポリシーがアクティブ化されます。

次に、VSA 250 の連結文字列の解析と ISG サービスおよび QoS ポリシーのアクティブ化を定義する例を示します。

qos:<qos-attribute-name>=<attribute value>[;qos:<qos-attribute-name>=<attribute value>...]

qos-attribute-name	QoS 属性名を表示します。この特殊な連結形式の QoS 属性名に使用できる属性は、次のとおりです。 vc-qos-policy-in vc-qos-policy-out vc-weight vc-watermark-min vc-watermark-max
attribute value	QoS 属性に割り当てる値を表示します。値の許容範囲はプラットフォームによって決定されます。

ターゲットセッションが ATM VC の場合、vc-weight、vc-watermark-min、および vc-watermark-max 属性が解釈されます。

次に、VSA 250 の連結 QoS 構文の例を示しています。

vsa cisco generic 250 string "Aqos:vc-qos-policy-out=IPOne_out;qos:vc-qos-policy-in=IPOne_in"

Access-Accept メッセージでのマルチサービスアクティブ化に関する追加情報

関連資料

関連項目	マニュアル タイトル
ANCP コマンド	『Cisco IOS Access Node Control Protocol Command Reference』
IEEE 802.1q VLAN	「Cisco IOS IEEE 802.1Q Support」機能モジュール
Access-Node Control Protocol	『Metro Ethernet WAN Services and Architectures』（ホワイトペーパー）、「Access Node Control Protocol」
Queue-in-Queue VLAN タグ	『IEEE 802.1Q-in-Q VLAN Tag Termination』

RFC

RFC	タイトル
ANCP 拡張のドラフト	『GSMP Extensions for Access Node Control Mechanism, Internet draft』

RFC	タイトル
RFC 3292	『*General Switch Management Protocol (GSMP) V3*』
RFC 3293	『*General Switch Management Protocol (GSMP), Packet Encapsulations for Asynchronous Transfer Mode (ATM), Ethernet and Transmission Control Protocol (TCP)*』

Access-Accept メッセージでのマルチサービスアクティブ化に関する機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *129 : Access-Accept* メッセージでのマルチサービスアクティブ化に関する機能情報

機能名	リリース	機能情報
Access-Accept メッセージでのマルチサービスアクティブ化	Cisco IOS XE Release 2.4	Access-Accept メッセージでのマルチサービスアクティブ化の機能は、RADIUS Access-Accept メッセージを使用した複数のサービスの動的なアクティブ化をサポートしています。 この機能は、Cisco IOS XE 2.4 で、Cisco ASR 1000 シリーズ ルータに導入されました。 この機能により、次のコマンドが導入または変更されました。**subscriber service multiple-accept**。

第 95 章

CoA メッセージでのマルチサービスのアクティブ化および非アクティブ化

この機能を使用すると、ポリシーサーバーから送信される単一の許可変更（CoA）メッセージによって、複数のサービスをアクティブ化または非アクティブ化できます。この機能は、Access-Accept メッセージでのマルチサービスアクティブ化の機能に似ていますが、この場合は、ユーザーセッションが事前にアクティブになっていることが前提となります。

CoA メッセージでのマルチサービスアクティブ化および非アクティブ化に関する制約事項

- マルチサービスアクティブ化または非アクティブ化メッセージに含まれるすべてのサービス名は、インテリジェント サービス ゲートウェイ（ISG）対応である必要があります。たとえば、これらは、タイプが class-map type のサービス「service1」である必要があります。
- いずれかのサービスアクティブ化または非アクティブ化メッセージが失敗した場合、ブロードバンド リモート アクセス サーバー（BRAS）は、以前に正常にアクティブ化また

は非アクティブ化されたサービスと、同じマルチサービスアクティブ化または非アクティブ化 CoA メッセージに含まれていたサービスのみをロールバックします。

- ただし、現在の ISG の実装では、以前にアクティブ化または非アクティブ化されたサービスの状態を再確立するプロセスに制限があります。たとえば、重複する可能性のある機能が同じセッションで有効になっている場合、新しい機能パラメータ、正常にアクティブ化された機能パラメータ、または非アクティブ化された機能パラメータは、そのセッションですでにアクティブ化されている同じ機能の古いパラメータを削除します。その機能の古いパラメータを再確立しようとすると失敗します。
- 有効な CLI 設定の ISG サービスが CoA を介して新しいセッションに転送され、失敗した（ISG サービスがアカウンティングリストを見つけることができない）場合は、次のようになります。
  - BRAS は、ハードウェアがプロビジョニングされるまで待機しません。
  - ACK メッセージがリレーされます。
  - ISG サービスは適用されません。
  - トレースバックが監視されます。

CoA メッセージでのマルチサービスアクティブ化および非アクティブ化に関する情報

CoA メッセージでのマルチサービスアクティブ化および非アクティブ化の概要

CoA マルチサービスアクティブ化または非アクティブ化メッセージには、サービスのリストが含まれています。それらの複数のサービスは、VSA 252 に複数行の形式でリストされます。

1 つの CoA メッセージ内でのマルチサービス非アクティブ化の場合、RADIUS サーバーは、1 つの CoA マルチサービス非アクティブ化メッセージ内で複数のサービスを非アクティブ化する要求を送信します。マルチサービス非アクティブ化メッセージにリストされているサービスごとに、BRAS がサービスを非アクティブ化します。サービスが正常に非アクティブ化されると、accounting-stop メッセージが表示されます。

サービスを正常に非アクティブ化できない場合、BRAS は、マルチサービスアクティブ化メッセージに含まれる後続のすべてのサービスの非アクティブ化を終了します。BRAS は、同じマルチサービスアクティブ化メッセージに含まれる、失敗したサービスがアクティブ化される前に正常に非アクティブ化されたすべてのサービスをアクティブ化します。

既存の VSA 252 は、1 つのマルチサービスアクティブ化または非アクティベーション CoA メッセージを形成するために使用されます。1 つのマルチサービスアクティブ化または非アクティブ化 CoA メッセージを形成するために、VSA 252 の複数の行がメッセージに含まれています。次の例は、1 つの CoA メッセージでの混合マルチサービスアクティブ化または非アクティブ化を示しています。

RADIUS 形式

```
ISG#
00:41:15: RADIUS: CoA  received from id 76 10.168.1.6:1700, CoA Request, len 67
00:41:15: CoA: 10.168.1.6 request queued
00:41:15: RADIUS:  authenticator C4 AC 5D 50 6A BE D7 00 - F9 1D FA 38 15 32 25 3A
00:41:15: RADIUS:  Vendor, Cisco       [26]  18
00:41:15: RADIUS:   ssg-account-info   [250] 12  "S151.1.1.2"
00:41:15: RADIUS:  Vendor, Cisco       [26]  17
00:41:15: RADIUS:   ssg-command-code   [252] 11
00:41:15: RADIUS:   0B 70 6F 6C 69 63 65 31           [Service-Log-On service1]
00:41:15: RADIUS:  Vendor, Cisco       [26]  17
00:41:15: RADIUS:   ssg-command-code   [252] 11
00:41:15: RADIUS:   0B 70 6F 6C 69 63 65 32           [Service-Log-On service2]
00:41:15: RADIUS:  Vendor, Cisco       [26]  17
00:41:15: RADIUS:   ssg-command-code   [252] 11
00:41:15: RADIUS:   0C 73 65 72 76 69 63 65 33       [Service-Log-Off service3]
00:41:15: RADIUS:  Vendor, Cisco       [26]  17
00:41:15: RADIUS:   ssg-command-code   [252] 11
00:41:15: RADIUS:   0B 70 6F 6C 69 63 65 34           [Service-Log-On service4]
```

VSA 252 の QoS ポリシー

RADIUS CoA メッセージでは、VSA 252 連結 Quality of Service（QoS）構文を使用できます。構文は、VSA 252 の連結文字列を解析することによって ISG サービスおよび QoS ポリシーをアクティブ化または非アクティブ化するために使用されます。

（注） ISG は、1 つの CoA メッセージで複数の QoS サービスを管理し、メッセージを適用して静的 QoS およびパラメータ化された QoS をアクティブにします。

CoA メッセージでのマルチサービスアクティブ化および非アクティブ化を設定する方法

CoA を使用したセッションサービスのアクティブ化

CoA でセッションサービスを動的にアクティブにするには、RADIUS のサービスプロファイルで Cisco VSA 252 を設定します。RADIUS では、次の構文により、CoA メッセージで VSA 252 が使用されます。

```
vsa cisco generic 252 binary 0b suffix
"qos:vc-qos-policy-out=IPOne_out;qos:vc-qos-policy-in=IPOne_in;;"
```

この例の CoA コマンドは次の処理を実行します。

- ISG サービス「qos:vc-qos-policy-out=IPOne_out;qos:vc-qos-policy-in=IPOne_in;;」を開始します。

- 仮想テンプレート IPOne_out にデフォルトの出力子ポリシーがない場合は、仮想テンプレートのデフォルトの QoS 出力子ポリシーを置き換え、IPOne_out ポリシーをインストールします。
- 仮想テンプレート IPOne_in で設定されているデフォルトの入力子ポリシーがない場合は、仮想テンプレートのデフォルトの QoS 入力子ポリシーを置き換え、IPOne_in ポリシーをインストールします。

CoA を使用したセッションサービスの非アクティブ化

仮想テンプレートで CoA およびデフォルト QoS ポリシーを使用してセッションサービスを動的にアクティブにするには、RADIUS サービスプロファイルで Cisco VSA 252 を設定します。RADIUS では、次の構文により、CoA メッセージで VSA 252 が使用されます。

```
vsa cisco generic 252 binary 0c suffix
"qos:vc-qos-policy-out=IPOne_out;qos:vc-qos-policy-in=IPOne_in;;"
```

この例の CoA コマンドは次の処理を実行します。

- ISG サービス「qos:vc-qos-policy-out=IPOne_out;qos:vc-qos-policy-in=IPOne_in」を終了します。
- QoS 出力子ポリシー IPOne_out を、適切な仮想テンプレート インターフェイスで設定されたデフォルトの子ポリシーに置き換えます。
- QoS 入力子ポリシー IPOne_in を、適切な仮想テンプレート インターフェイスで設定されたデフォルトの子ポリシーに置き換えます。

CoA メッセージでのマルチサービスアクティブ化および非アクティブ化の設定例

VSA 252 を使用した QoS サービスのアクティブ化および非アクティブ化の例

QoS サービスをアクティブにするために、RADIUS は、1 つの VSA 252 文字列で親ポリシーと子ポリシーに 1 つ以上の QoS クラスを追加し、次の構文をリレーします。

```
CoA VSA 252 0b <new service>
```

既存のサービスに加えて、新しいサービスをインストールするとともに、現在のサービスとクラスが重複しないようにする必要があります。

次の例は、QoS のアクティブ化を定義し、QoS クラスをパラメータ化された QoS サービスの RADIUS フォームに追加します。

```
VSA252 0b q-p-out=IPOne1-isg-acct_service(1)((c-d,voip)1(200000,9216,0,1,0,0)10(9));q-p-in=
 ((c-d,voip)1(200000,9216,0,1,0,0)10(9))
```

2 つ目のサービスを非アクティブ化するために、RADIUS は、サービスのアクティブ化に使用された VSA 252 文字列をリレーし、「0b」を「0c」に置き換えます。

次の例は、QoS の非アクティブ化を定義し、パラメータ化された QoS サービスの RADIUS フォームの QoS クラスを削除します。

```
VSA252 0c q-p-out=IPOne1-isg-acct_service(1)((c-d,voip)1(200000,9216,0,1,0,0)10(9));q-p-in=
 ((c-d,voip)1(200000,9216,0,1,0,0)10(9))
```

CoA メッセージでのマルチサービスアクティブ化および非アクティブ化に関する追加情報

関連資料

関連項目	マニュアル タイトル
ANCP コマンド	『*Cisco IOS Access Node Control Protocol Command Reference*』
IEEE 802.1q VLAN	IEEE 802.1Q カプセル化を使用する VLAN 間のルーティング設定
Queue-in-Queue VLAN タグ	IEEE 802.1Q-in-Q VLAN タグ終端

RFC

RFC	タイトル
ANCP 拡張のドラフト	『GSMP Extensions for Access Node Control Mechanism, Internet draft』
RFC 3292	『*General Switch Management Protocol (GSMP) V3*』
RFC 3293	『*General Switch Management Protocol (GSMP), Packet Encapsulations for Asynchronous Transfer Mode (ATM), Ethernet and Transmission Control Protocol (TCP)*』

CoA メッセージでのマルチサービスアクティブ化および非アクティブ化に関する機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだ

けを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *130 : CoA* メッセージでのマルチサービスアクティブ化および非アクティブ化に関する機能情報

機能名	リリース	機能情報
CoA メッセージでのマルチサービスのアクティブ化および非アクティブ化	Cisco IOS XE Release 2.4	CoA メッセージでのマルチサービスアクティブ化および非アクティブ化の機能は、RADIUS CoA メッセージを使用した複数のサービスの動的なアクティブ化および非アクティブ化をサポートしています。 この機能は、Cisco IOS XE 2.4 で、Cisco ASR 1000 シリーズ ルータに導入されました。

第 IX 部

ファーストホップ セキュリティ

第 96 章

IPv6 RA ガード

IPv6 RA ガード機能は、ネットワーク デバイス プラットフォームに到着した不要または不正なルータ アドバタイズメント（RA）ガード メッセージを、ネットワーク管理者がブロックまたは拒否できるようにするためのサポートを提供します。

IPv6 RA ガードの制限

- IPv6 RA ガード機能は、IPv6 トラフィックがトンネリングされる環境では保護を行いません。
- この機能は、TCAM（Ternary Content Addressable Memory）がプログラムされているハードウェアでのみサポートされています。
- この機能は、入力方向のスイッチ ポート インターフェイスで設定できます。
- この機能は、ホスト モードとルータ モードをサポートしています。
- この機能は、入力方向だけでサポートされます。出力方向ではサポートされません。
- この機能は、EtherChannel および EtherChannel ポート メンバーではサポートされません。
- この機能は、マージ モードのトランク ポートではサポートされません。
- この機能は、補助 VLAN およびプライベート VLAN（PVLAN）でサポートされています。PVLAN の場合、プライマリ VLAN の機能が継承され、ポート機能とマージされます。
- IPv6 RA ガード機能によってドロップされたパケットはスパニングできます。
- **platform ipv6 acl icmp optimize neighbor-discovery command** が設定されている場合、IPv6 RA ガード機能は設定できず、エラー メッセージが表示されます。このコマンドは、RA

ガードの ICMP エントリを上書きするデフォルトのグローバル Internet Control Message Protocol（ICMP）エントリを追加します。

IPv6 RA ガードに関する情報

IPv6 グローバル ポリシー

IPv6 グローバル ポリシーは、ストレージおよびアクセス ポリシー データベースのサービスを提供します。IPv6 ND 検査と IPv6 RA ガードは、IPv6 グローバル ポリシー機能です。ND インスペクションまたは RA ガードをグローバルに設定するたびに、ポリシーの属性が、ソフトウェア ポリシー データベースに保存されます。その後ポリシーはインターフェイスに適用され、ポリシーが適用されたこのインターフェイスを含めるためにソフトウェア ポリシー データベース エントリが更新されます。

IPv6 RA ガード

IPv6 RA ガード機能は、ネットワーク デバイス プラットフォームに到着した不要または不正な RA ガード メッセージを、ネットワーク管理者がブロックまたは拒否できるようにするためのサポートを提供します。RA は、リンクで自身をアナウンスするためにデバイスによって使用されます。IPv6 RA ガード機能は、それらの RA を分析して、承認されていないデバイスから送信された RA を除外します。ホスト モードでは、ポート上の RA とルータ リダイレクト メッセージはすべて許可されません。RA ガード機能は、レイヤ 2（L2）デバイスの設定情報を、受信した RA フレームで検出された情報と比較します。L2 デバイスは、RA フレームとルータ リダイレクト フレームの内容を設定と照らし合わせて検証した後で、RA をユニキャストまたはマルチキャストの宛先に転送します。RA フレームの内容が検証されない場合は、RA はドロップされます。

ワイヤレス展開では、ワイヤレス ポートで受信した RA はドロップされます。ルータはこれらのインターフェイスに存在できないためです。

IPv6 RA ガードの設定方法

デバイスでの IPv6 RA ガード ポリシーの設定

（注） **ipv6 nd raguard** コマンドがポートで設定されている場合、ルータ送信要求メッセージはこれらのポートに複製されません。ルータ要請メッセージを複製するには、ルータ側のすべてのポートをルータ ロールに設定する必要があります。

手順の概要

1. **enable**
2. **configure terminal**
3. **ipv6 nd raguard policy** *policy-name*
4. **device-role** {**host** | **router**}
5. **hop-limit** {**maximum** | **minimum** *limit*}
6. **managed-config-flag** {**on** | **off**}
7. **match ipv6 access-list** *ipv6-access-list-name*
8. **match ra prefix-list** *ipv6-prefix-list-name*
9. **other-config-flag** {**on** | **off**}
10. **router-preference maximum** {**high** | **low** | **medium**}
11. **trusted-port**
12. **exit**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ipv6 nd raguard policy** *policy-name* 例： `Device(config)# ipv6 nd raguard policy policy1`	RA ガード ポリシー名を定義して、RA ガード ポリシー コンフィギュレーション モードを開始します。
ステップ 4	**device-role** {**host**	**router**} 例： `Device(config-ra-guard)# device-role router`	ポートに接続されているデバイスの役割を指定します。
ステップ 5	**hop-limit** {**maximum**	**minimum** *limit*} 例： `Device(config-ra-guard)# hop-limit minimum 3`	（任意）アドバタイズされたホップ カウント制限の検証をイネーブルにします。 • 設定されていない場合、このチェックは回避されます。

	コマンドまたはアクション	目的
ステップ 6	**managed-config-flag** {**on** | **off**} 例： `Device(config-ra-guard)# managed-config-flag on`	（任意）アドバタイズされた管理アドレスの設定フラグが on であることの検証をイネーブルにします。 • 設定されていない場合、このチェックは回避されます。
ステップ 7	**match ipv6 access-list** *ipv6-access-list-name* 例： `Device(config-ra-guard)# match ipv6 access-list list1`	（任意）検査済みメッセージ内の送信者の IPv6 アドレスが設定された承認デバイス ソース アクセス リストからのものであることの検証をイネーブルにします。 • 設定されていない場合、このチェックは回避されます。
ステップ 8	**match ra prefix-list** *ipv6-prefix-list-name* 例： `Device(config-ra-guard)# match ra prefix-list listname1`	（任意）検証済みメッセージ内のアドバタイズされたプレフィックスが設定された承認プレフィックス リストからのものであることの検証をイネーブルにします。 • 設定されていない場合、このチェックは回避されます。
ステップ 9	**other-config-flag** {**on** | **off**} 例： `Device(config-ra-guard)# other-config-flag on`	（任意）アドバタイズされた [Other] 設定パラメータの検証をイネーブルにします。
ステップ 10	**router-preference maximum** {**high** | **low** | **medium**} 例： `Device(config-ra-guard)# router-preference maximum high`	（任意）アドバタイズされたデフォルト ルータの設定パラメータの値が指定された制限値以下であることの検証をイネーブルにします。
ステップ 11	**trusted-port** 例： `Device(config-ra-guard)# trusted-port`	（任意）このポリシーが信頼できるポートに適用されることを指定します。 • すべての RA ガード ポリシングが無効になります。
ステップ 12	**exit** 例： `Device(config-ra-guard)# exit`	RA ガード ポリシー コンフィギュレーション モードを終了してグローバル コンフィギュレーション モードに戻ります。

インターフェイスの IPv6 RA ガードの設定

手順の概要

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **ipv6 nd raguard attach-policy** [*policy-name* [**vlan** {**add** | **except** | **none** | **remove** | **all**} *vlan* [*vlan1, vlan2, vlan3...*]]]
5. **exit**
6. **show ipv6 nd raguard policy** [*policy-name*]
7. **debug ipv6 snooping raguard** [*filter* | *interface* | *vlanid*]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface** *type number* 例： `Device(config)# interface fastethernet 3/13`	インターフェイスのタイプと番号を指定し、デバイスをインターフェイス コンフィギュレーション モードにします。
ステップ 4	**ipv6 nd raguard attach-policy** [*policy-name* [**vlan** {**add** | **except** | **none** | **remove** | **all**} *vlan* [*vlan1, vlan2, vlan3...*]]] 例： `Device(config-if)# ipv6 nd raguard attach-policy`	指定したインターフェイスに IPv6 RA ガード機能を適用します。
ステップ 5	**exit** 例： `Device(config-if)# exit`	インターフェイス コンフィギュレーション モードを終了します。
ステップ 6	**show ipv6 nd raguard policy** [*policy-name*] 例： `Device# show ipv6 nd raguard policy raguard1`	RA ガードを使用して設定されているすべてのインターフェイスで RA ガード ポリシーを表示します。

	コマンドまたはアクション	目的
ステップ 7	**debug ipv6 snooping raguard** [*filter* | *interface* | *vlanid*] 例： `Device# debug ipv6 snooping raguard`	IPv6 RA ガード スヌーピング情報のデバッグをイネーブルにします。

IPv6 RA ガードの設定例

例：IPv6 RA ガードの設定

```
Device(config)# interface fastethernet 3/13

Device(config-if)# ipv6 nd raguard attach-policy

Device# show running-config interface fastethernet 3/13

Building configuration...
Current configuration : 129 bytes
!
interface FastEthernet3/13
 switchport
 switchport access vlan 222
 switchport mode access
 access-group mode prefer port
 ipv6 nd raguard
end
```

例：IPv6 ND インスペクションおよび RA ガードの設定

この例は、ネイバー探索インスペクションおよびRA ガード機能の両方が設定されているインターフェイスに関する情報を示しています。

```
Device# show ipv6 snooping capture-policy interface ethernet 0/0

Hardware policy registered on Ethernet 0/0
Protocol     Protocol value   Message   Value     Action    Feature
ICMP         58               RS        85        punt      RA Guard
                                                  punt      ND Inspection
ICMP         58               RA        86        drop      RA guard
                                                  punt      ND Inspection
ICMP         58               NS        87        punt      ND Inspection
ICM          58               NA        88        punt      ND Inspection
ICMP         58               REDIR     89        drop      RA Guard
                                                  punt      ND Inspection
```

その他の参考資料

関連資料

関連項目	マニュアル タイトル
IPv6 アドレッシングと接続	『*IPv6 Configuration Guide*』
Cisco IOS コマンド	『Cisco IOS Master Commands List, All Releases』
IPv6 コマンド	『*Cisco IOS IPv6 Command Reference*』
Cisco IOS IPv6 機能	『Cisco IOS IPv6 Feature Mapping』

標準および RFC

標準/RFC	タイトル
IPv6 に関する RFC	*IPv6 RFCs*

MIB

MIB	MIB のリンク
この機能によってサポートされる新しい MIB または変更された MIB はありません。またこの機能による既存MIBのサポートに変更はありません。	選択したプラットフォーム、Cisco IOS リリース、およびフィーチャ セットに関する MIB を探してダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

シスコのテクニカル サポート

説明	リンク
右の URL にアクセスして、シスコのテクニカル サポートを最大限に活用してください。これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

IPv6 RA ガードの機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *131 : IPv6 RA* ガードの機能情報

機能名	リリース	機能情報
IPv6 RA ガード	12.2(33)SXI4 12.2(50)SY 12.2(54)SG 15.0(2)SE 15.0(2)SG Cisco IOS XE Release 3.8S Cisco IOS XE Release 3.2SE Cisco IOS XE Release 3.2SG	次のコマンドが導入または変更されました。**debug ipv6 snooping raguard**、**device-role**、**hop-limit**、**ipv6 nd raguard attach-policy**、**ipv6 nd raguard policy**、**managed-config-flag**、**match ipv6 access-list**、**match ra prefix-list**、**other-config-flag**、**router-preference maximum**、**show ipv6 nd raguard policy**。

第 97 章

IPv6 スヌーピング

IPv6 スヌーピング機能は、複数のレイヤ 2 IPv6 ファーストホップ セキュリティ機能（IPv6 ネイバー探索インスペクション、IPv6 デバイス トラッキング、IPv6 アドレス収集、および IPv6 バインディング テーブルのリカバリを含む）をバンドルして、セキュリティと拡張性を提供します。IPv6 ND インスペクションは、レイヤ 2（またはレイヤ 2 とレイヤ 3 の間）で動作し、IPv6 の機能にセキュリティと拡張性を提供します。

IPv6 スヌーピングの制限

IPv6 スヌーピング機能は、EtherChannel ポートではサポートされません。

IPv6 スヌーピングに関する情報

ここでは、IPv6 スヌーピングについて説明します。

IPv6 スヌーピング

IPv6 スヌーピング機能によって、複数のレイヤ 2 IPv6 ファーストホップ セキュリティ機能（IPv6 アドレス収集と IPv6 デバイス トラッキングを含む）がバンドルされます。この機能は、レイヤ 2（またはレイヤ 2 とレイヤ 3 の間）で動作し、IPv6 の機能にセキュリティと拡張性を提供します。この機能によって、Duplicate Address Detection（DAD）、アドレス解決、デバイス検出やネイバーキャッシュに対する攻撃といった、ネイバー探索メカニズムに固有のいくつかの脆弱性が軽減されます。

IPv6 スヌーピングは、レイヤ 2 ネイバー テーブルのステートレス自動設定アドレスのバインディングを学習して保護し、信頼できるバインディング テーブルを構築するために ND メッ

セージを分析します。有効なバインディングのないIPv6NDメッセージはドロップされます。ND メッセージは、その IPv6 から MAC へのマッピングが検証可能な場合に信頼できると見なされます。

ターゲット（プラットフォームのターゲット サポートによって異なり、デバイス ポート、スイッチ ポート、レイヤ 2 インターフェイス、レイヤ 3 インターフェイス、および VLAN が含まれることがある）に IPv6 スヌーピングが設定されている場合、IPv6 トラフィックの ND プロトコルと Dynamic Host Configuration Protocol（DHCP）をルーティング デバイスのスイッチ統合セキュリティ機能（SISF）インフラストラクチャにリダイレクトするためのキャプチャ命令がハードウェアにダウンロードされます。ND トラフィックの場合、NS、NA、RS、RA、REDIRECT などのメッセージが SISF にリダイレクトされます。DHCP の場合、ポート 546 または 547 から送信された UDP メッセージがリダイレクトされます。

IPv6 スヌーピングはその「キャプチャ ルール」を分類子に登録します。分類子では、特定のターゲットにあるすべての機能のルールがすべて集約され、対応する ACL がプラットフォーム依存モジュールにインストールされます。分類子は、リダイレクトされたトラフィックを受信すると、（トラフィックを受信しているターゲットに対して）登録されているすべての機能からすべてのエントリ ポイント（IPv6 スヌーピングのエントリ ポイントを含む）を呼び出します。IPv6 スヌーピングのエントリ ポイントは最後に呼び出されるため、他の機能によって行われた決定が IPv6 スヌーピングの決定よりも優先されます。

IPv6 デバイス トラッキング

IPv6 デバイス トラッキングは、IPv6 ホストが非表示になったときにネイバー テーブルを即時に更新できるように、IPv6 ホストの活性トラッキングを提供します。

IPv6 ファーストホップ セキュリティ バインディング テーブル

IPv6 ファーストホップ セキュリティ バインディング テーブルのリカバリ メカニズム機能を使用すると、デバイスのリブート時にバインディングテーブルをリカバリできます。デバイスに接続されている IPv6 ネイバーのデータベース テーブルは、ND スヌーピングなどの情報源から作成されます。このデータベース（またはバインディング）テーブルは、スプーフィングやリダイレクト攻撃を防止するために、リンク層アドレス（LLA）、IPv4 またはIPv6アドレス、およびネイバーのプレフィックス バインディングを検証するためにさまざまな IPv6 ガード機能によって使用されます。

このメカニズムにより、デバイスのリブート時にバインディング テーブルをリカバリできます。リカバリ メカニズムは、不明な送信元、（バインディング テーブルにまだ指定されていない送信元や、ND または DHCP グリーニングを使用して学習されていない送信元）からのデータ トラフィックをブロックします。この機能は、宛先ガードで宛先アドレスの解決に失敗したときに、不足しているバインディングテーブルのエントリをリカバリします。障害が発生すると、バインディングテーブルのエントリは、設定に応じて、DHCP サーバーまたは宛先ホストにクエリを実行することでリカバリできます。

リカバリ プロトコルとプレフィックス リスト

IPv6 ファーストホップ セキュリティ バインディング テーブルのリカバリ メカニズム機能は、DHCP と NDP の両方でリカバリを試みる前に、一致するプレフィックス リストを提供する機能を導入します。

アドレスがプロトコルと関連付けられているプレフィックス リストと一致しない場合、そのプロトコルではバインディング テーブル エントリのリカバリは試行されません。プレフィックス リストは、プロトコルを使用してレイヤ2 ドメインに割り当てられているアドレスに対して有効なプレフィックスに対応している必要があります。デフォルトではプレフィックス リストは存在せず、すべてのアドレスのリカバリが試行されます。プロトコルにプレフィックス リストを関連付けるコマンドは、**protocol** {**dhcp** | **ndp**} [**prefix-list** *prefix-list-name*] です。

IPv6 デバイス トラッキング

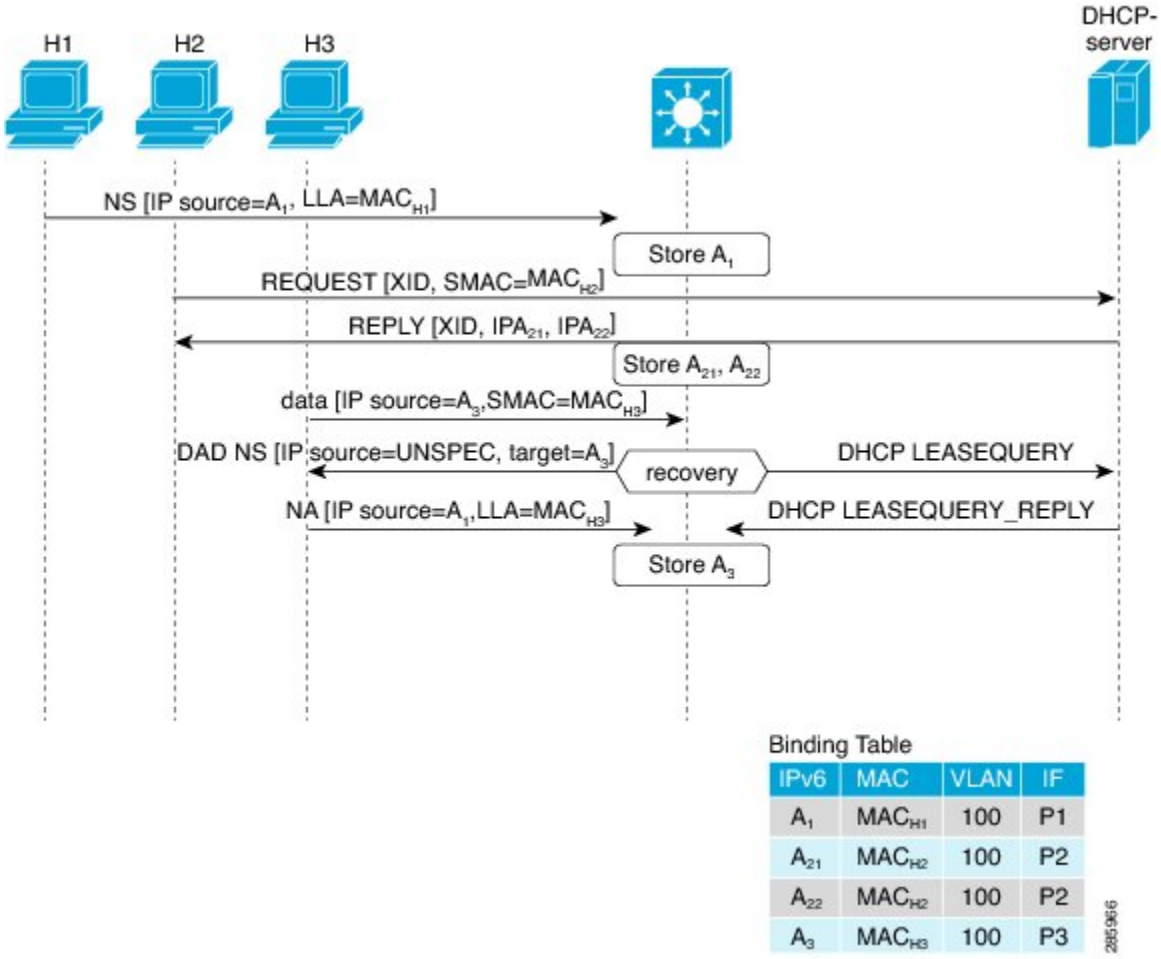
IPv6 デバイス トラッキングは、IPv6 ホストが非表示になったときにネイバー テーブルを即時に更新できるように、IPv6 ホストの活性トラッキングを提供します。

IPv6 アドレス収集

IPv6 アドレス収集は、正確なバインディング テーブルに依存するその他多くの IPv6 の機能の基盤です。この機能は、アドレス収集のためにリンク上の ND および DHCP メッセージを検査した後に、それらのアドレスをバインディング テーブルに入力します。また、この機能は、アドレスの所有権を強制し、特定のノードが要求可能なアドレスの数を制限します。

次の図は、IPv6 アドレス収集の仕組みを示しています。

図 *27 : IPv6* アドレス収集



複数の IA_NA および IA_PD のサポート

場合によっては、ネットワークデバイスが DHCP サーバーから複数の IPv6 アドレスを要求して受信することがあります。これは、レジデンシャルゲートウェイがアドレスをその LAN クライアントに配布することを要求する場合など、デバイスの複数のクライアントにアドレスを提供するために実行できます。デバイスが DHCPv6 パケットを送信すると、パケットにはデバイスに割り当てられているすべてのアドレスが含まれます。

SISF は DHCPv6 パケットを分析する際に、パケットの IA_NA（Identity Association-Nontemporary Address）および IA_PD（Identity Association-Prefix Delegation）コンポーネントを検査し、パケットに含まれる各 IPv6 アドレスを抽出します。SISF は、抽出された各アドレスをバインディングテーブルに追加します。

IPv6 スヌーピングの設定方法

インターフェイスの IPv6 スヌーピングの設定

手順の概要

1. **enable**
2. **configure terminal**
3. **ipv6 snooping policy** *snooping-policy*
4. **exit**
5. **interface** *type number*
6. **ipv6 snooping attach-policy** *snooping-policy*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ipv6 snooping policy** *snooping-policy* 例： `Device(config)# ipv6 snooping policy policy1`	IPv6 スヌーピング ポリシーを設定し、IPv6 スヌーピング コンフィギュレーション モードを開始します。
ステップ 4	**exit** 例： `Device(config-ipv6-snooping)# exit`	IPv6 スヌーピング コンフィギュレーション モードを終了します。
ステップ 5	**interface** *type number* 例： `Device(config)# interface Gigabitethernet 0/0/1`	インターフェイス コンフィギュレーション モードを開始します。
ステップ 6	**ipv6 snooping attach-policy** *snooping-policy* 例： `Device(config-if)# ipv6 snooping attach-policy policy1`	インターフェイスに IPv6 スヌーピング ポリシーを対応付けます。

IPv6 ND インスペクションの確認とトラブルシューティング

手順の概要

1. **enable**
2. **show ipv6 snooping capture-policy** [**interface** *type number*]
3. **show ipv6 snooping counter** [**interface** *type number*]
4. **show ipv6 snooping features**
5. **show ipv6 snooping policies** [**interface** *type number*]
6. **debug ipv6 snooping**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**show ipv6 snooping capture-policy** [**interface** *type number*] 例： `Device# show ipv6 snooping capture-policy interface ethernet 0/0`	スヌーピング ND メッセージキャプチャ ポリシーを表示します。
ステップ 3	**show ipv6 snooping counter** [**interface** *type number*] 例： `Device# show ipv6 snooping counter interface FastEthernet 4/12`	インターフェイス カウンタによってカウントされたパケットに関する情報を表示します。
ステップ 4	**show ipv6 snooping features** 例： `Device# show ipv6 snooping features`	デバイスに設定されているスヌーピング機能に関する情報を表示します。
ステップ 5	**show ipv6 snooping policies** [**interface** *type number*] 例： `Device# show ipv6 snooping policies`	設定されているポリシーと、ポリシーが接続されているインターフェイスに関する情報を表示します。
ステップ 6	**debug ipv6 snooping** 例： `Device# debug ipv6 snooping`	IPv6 でスヌーピング情報のデバッグをイネーブルにします。

IPv6 デバイス トラッキングの設定

IPv6 ファーストホップ セキュリティ バインディング テーブルの内容の設定

手順の概要

1. **enable**
2. **configure terminal**
3. **ipv6 neighbor binding** {*ipv6-address* | *ipv6-prefix*} **interface** *type number* [*hardware-address* | *mac-address*][**tracking** [**disable** | **enable** | **retry-interval** *value*] | **reachable-lifetime** *value*]
4. **ipv6 neighbor binding max-entries** *entries*
5. **ipv6 neighbor binding logging**
6. **exit**
7. **show ipv6 neighbor binding**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ipv6 neighbor binding** {*ipv6-address* | *ipv6-prefix*} **interface** *type number* [*hardware-address* | *mac-address*][**tracking** [**disable** | **enable** | **retry-interval** *value*] | **reachable-lifetime** *value*] 例： `Device(config)# ipv6 neighbor binding 2001:DB8:0:ABCD::1 interface GigabitEthernet 0/0/1 reachable-lifetime 100`	バインディング テーブル データベースにスタティック エントリを追加します。
ステップ 4	**ipv6 neighbor binding max-entries** *entries* 例： `Device(config)# ipv6 neighbor binding max-entries 100`	バインディング テーブル キャッシュに挿入できるエントリの最大数を指定します。
ステップ 5	**ipv6 neighbor binding logging** 例：	バインディング テーブル メイン イベントのロギングを有効にします。

	コマンドまたはアクション	目的
	`Device(config)# ipv6 neighbor binding logging`	
ステップ 6	**exit** 例： `Device(config)# exit`	グローバル コンフィギュレーション モードを終了し、特権 EXEC モードを開始します。
ステップ 7	**show ipv6 neighbor binding** 例： `Device# show ipv6 neighbor binding`	バインディング テーブルの内容を表示します。

IPv6 ファーストホップ セキュリティ バインディング テーブルのリカバリ メカニズムの設定

手順の概要

1. **enable**
2. **configure terminal**
3. **ipv6 neighbor binding** *ipv6-address* **interface** *type number*
4. **ipv6 prefix-list** *list-name* **permit** *ipv6-prefix/prefix-length* **ge** *ge-value*
5. **ipv6 snooping policy** *snooping-policy-id*
6. **destination-glean** {**recovery** | **log-only**} [**dhcp**]
7. **data-glean** {**recovery** | **log-only**} [**ndp** | **dhcp**]
8. **prefix-glean**
9. **protocol dhcp** [**prefix-list** *prefix-list-name*]
10. **exit**
11. **ipv6 destination-guard policy** *policy-name*
12. **enforcement** {**always** | **stressed**}
13. **exit**
14. **interface** *type number*
15. **ipv6 snooping attach-policy** *snooping-policy*
16. **ipv6 destination-guard attach-policy** *policy-name*
17. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。

	コマンドまたはアクション	目的
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ipv6 neighbor binding** *ipv6-address* **interface** *type number* 例： `Device(config)# ipv6 neighbor binding 2001:db8::1 interface Gigabitethernet3/0/1`	バインディング テーブル データベースにスタティック エントリを追加します。
ステップ 4	**ipv6 prefix-list** *list-name* **permit** *ipv6-prefix/prefix-length* **ge** *ge-value* 例： `Device(config)# ipv6 prefix-list abc permit 2001:DB8::/64 ge 128`	IPv6 プレフィックス リストのエントリを作成します。
ステップ 5	**ipv6 snooping policy** *snooping-policy-id* 例： `Device(config)# ipv6 snooping policy xyz`	IPv6 スヌーピング コンフィギュレーション モードを開始し、指定されたスヌーピング ポリシーの設定を変更できるようします。
ステップ 6	**destination-glean** {**recovery** | **log-only**} [**dhcp**] 例： `Device(config-ipv6-snooping)# destination-glean recovery dhcp`	宛先アドレスは DHCP からリカバリする必要があることを指定します。 （注） ロギング（リカバリなし）が必要な場合は、**destination-glean log-only** コマンドを使用します。
ステップ 7	**data-glean** {**recovery** | **log-only**} [**ndp** | **dhcp**] 例： `Device(config-ipv6-snooping)# data-glean recovery ndp`	ソース（または「データ」）アドレス グリーニングを使用して、IPv6 ファーストホップ セキュリティ バインディング テーブルのリカバリをイネーブルにします。 （注） ロギング（リカバリなし）が必要な場合は、**data-glean log-only** コマンドを使用します。
ステップ 8	**prefix-glean** 例： `Device(config-ipv6-snooping)# prefix-glean`	デバイスが IPv6 ルータ アドバタイズメント（RA）または Dynamic Host Configuration Protocol（DHCP）からプレフィックスを収集できるようにします。

	コマンドまたはアクション	目的
ステップ 9	**protocol dhcp** [**prefix-list** *prefix-list-name*] 例： `Device(config-ipv6-snooping)# protocol dhcp prefix-list abc`	（任意）アドレスを DHCP で収集し、プロトコルを特定の IPv6 プレフィックス リストと関連付ける必要があることを指定します。
ステップ 10	**exit** 例： `Device(config-ipv6-snooping)# exit`	IPv6 スヌーピング コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードに戻ります。
ステップ 11	**ipv6 destination-guard policy** *policy-name* 例： `Device(config)# ipv6 destination-guard policy xyz`	（任意）宛先ガード コンフィギュレーション モードを開始し、指定した宛先ガード ポリシーの設定を変更できるようにします。
ステップ 12	**enforcement** {**always** | **stressed**} 例： `Device(config-destguard)# enforcement stressed`	ポリシーの強制レベルを、すべての条件下で強制するか、システムに負荷がかかっている場合のみ強制するか設定します。
ステップ 13	**exit** 例： `Device(config-destguard)# exit`	宛先ガード コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードに戻ります。
ステップ 14	**interface** *type number* 例： `Device(config)# interface Gigabitethernet 0/0/1`	インターフェイス コンフィギュレーション モードを開始します。
ステップ 15	**ipv6 snooping attach-policy** *snooping-policy* 例： `Device(config-if)# ipv6 snooping attach-policy xyz`	インターフェイスに IPv6 スヌーピング ポリシーを対応付けます。
ステップ 16	**ipv6 destination-guard attach-policy** *policy-name* 例： `Device(config-if)# ipv6 destination-guard attach-policy xyz`	指定したインターフェイスに宛先ガード ポリシーを対応付けます。 （注） IPv6 宛先ガード ポリシーの設定方法の詳細については、「IPv6 宛先ガード」を参照してください。
ステップ 17	**end** 例：	インターフェイス コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

	コマンドまたはアクション	目的
	`Device(config-if)# end`	

アドレス収集の設定およびリカバリ プロトコルとプレフィックス リストの関連付け

手順の概要

1. **enable**
2. **configure terminal**
3. **ipv6 snooping policy** *snooping-policy-id*
4. **protocol** {**dhcp** | **ndp**} [**prefix-list** *prefix-list-name*]
5. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ipv6 snooping policy** *snooping-policy-id* 例： `Device(config)# ipv6 snooping policy 200`	IPv6 スヌーピング コンフィギュレーション モードを開始し、指定されたスヌーピング ポリシーの設定を変更できるようします。
ステップ 4	**protocol** {**dhcp**	**ndp**} [**prefix-list** *prefix-list-name*] 例： `Device(config-ipv6-snooping)# protocol dhcp prefix-list dhcp_prefix_list`	Dynamic Host Configuration Protocol（DHCP）で収集される必要があるアドレスを指定し、リカバリ プロトコル（DHCP）とプレフィックス リストを関連付けます。
ステップ 5	**end** 例： `Device(config-ipv6-snooping)# end`	IPv6 スヌーピング コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

IPv6 デバイス トラッキングの設定

IPv6 デバイス トラッキング機能のバインディング テーブルでエントリのライフ サイクルを細かく調整するには、次の作業を実行します。IPv6 デバイス トラッキングが機能するには、バインディング テーブルにデータを入力する必要があります。

手順の概要

1. **enable**
2. **configure terminal**
3. **ipv6 neighbor tracking** [**retry-interval** *value*]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ipv6 neighbor tracking** [**retry-interval** *value*] 例： `Device(config)# ipv6 neighbor tracking`	バインディング テーブルのエントリを追跡します。

IPv6 プレフィックス収集の設定

手順の概要

1. **enable**
2. **configure terminal**
3. **ipv6 snooping policy** *snooping-policy*
4. **prefix-glean** ［**only**］

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例：	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。

	コマンドまたはアクション	目的
	`Device> enable`	
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ipv6 snooping policy** *snooping-policy* 例： `Device(config)# ipv6 snooping policy policy1`	IPv6 スヌーピング ポリシーを設定し、IPv6 スヌーピング ポリシー コンフィギュレーション モードを開始します。
ステップ 4	**prefix-glean** ［**only**］ 例： `Device(config-ipv6-snooping)# prefix-glean`	デバイスが IPv6 RA または DHCPv6 トラフィックからプレフィックスを収集できるようにします。

IPv6 スヌーピングの設定例

例：インターフェイスの IPv6 ND インスペクションの設定

```
Device(config)# ipv6 snooping policy policy1
Device(config-ipv6-snooping)# exit
Device(config)# interface Gigabitethernet 0/0/1
Device(config-if)# ipv6 snooping attach-policy policy1
.
.
.
Device# show ipv6 snooping policies interface gigabitethernet 0/0/1
Target               Type  Policy               Feature        Target range
Gi0/0/1              PORT  my_policy            Destination Gu vlan all
Gi0/0/1              PORT  policy1              Snooping       vlan all
```

例：IPv6 バインディング テーブルの内容の設定

```
Device(config)# ipv6 neighbor binding 2001:DB8:0:ABCD::1 interface GigabitEthernet 0/0/1
 reachable-lifetime 100
Device(config)# ipv6 neighbor binding max-entries 100
Device(config)# ipv6 neighbor binding logging
Device(config)# exit
```

例：IPv6 ファーストホップ セキュリティ バインディング テーブルのリカバリの設定

```
Device> enable
Device# configure terminal
Device(config)# ipv6 neighbor binding 2001:db8::1 interface Gigabitethernet3/0/1
Device(config)# ipv6 prefix-list abc permit 2001:DB8::/64 ge 128
Device(config)# ipv6 snooping policy xyz
Device(config-ipv6-snooping)# destination-glean recovery dhcp
Device(config-ipv6-snooping)# data-glean recovery ndp
Device(config-ipv6-snooping)# prefix-glean
Device(config-ipv6-snooping)# protocol dhcp prefix-list abc
Device(config-ipv6-snooping)# exit
Device(config)# ipv6 destination-guard policy xyz
Device(config-destguard)# enforcement stressed
Device(config-destguard)# exit
Device(config)# interface Gigabitethernet 0/0/1
Device(config-if)# ipv6 snooping attach-policy xyz
Device(config-if)# ipv6 destination-guard attach-policy xyz
Device(config-if)# end
```

例：アドレス収集の設定およびリカバリプロトコルとプレフィックス リストの関連付け

次の例は、NDP がすべてのアドレスのリカバリに使用され、DHCP が dhcp_prefix_list という名前のプレフィックス リストと一致するアドレスのリカバリに使用されることを示しています。

```
Device(config-ipv6-snooping)# protocol ndp
Device(config-ipv6-snooping)# protocol dhcp prefix-list dhcp_prefix_list
```

Cisco TrustSec の概要の機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *132 : Cisco TrustSec* の概要の機能情報

機能名	リリース	機能情報
IPv6 の有効化 - インライン タギング	Cisco IOS XE Fuji 16.8.1	IPv6 のサポートが導入されました。

第 98 章

IPv6 DAD プロキシ

IPv6 Duplicate Address Detection（DAD）プロキシ機能は、クエリされたアドレスを所有するノードに代わって DAD クエリに応答します。この機能は、ノードがリンク上で直接通信できない環境で役立ちます。

IPv6 DAD プロキシの制限

- IPv6 Duplicate Address Detection（DAD）機能は、EtherChannel ポートではサポートされません。

IPv6 DAD プロキシに関する情報

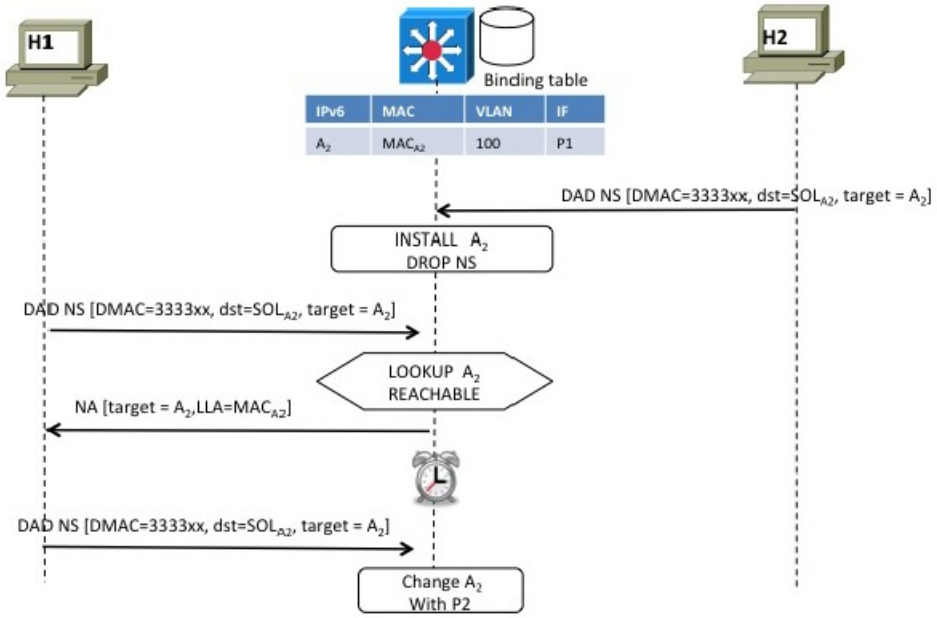
IPv6 DAD プロキシの概要

IPv6 Duplicate Address Detection（DAD）機能は、特定のセグメントに割り当てられるすべてのIPアドレスを一意なアドレスにします。このプロセスは、ホストが直接通信できず、プロキシが必要な場合に IPv6 ホスト同士が互いに直接通信するときに動作します。

ホストはそのアドレスが一意であることを確認すると、DAD手順を有効にします。ただし、2台のホストが互いに通信ができない場合、この手順では重複アドレスを検出できません。DAD手順を実行できない場合、両方のホストが同じリンクローカルアドレスを割り当てるため、どちらのホストも Dynamic Host Configuration Protocol バージョン 6（DHCPv6）サーバに接続を試みると失敗します。IPv6 DAD プロキシ機能は、アドレスが使用中の場合、そのアドレスの所有者に代わって応答します。

次の図は、IPv6 DAD プロキシ機能の概要を示しています。

図 *28 : IPv6 DAD* プロキシ



IPv6 DAD プロキシの設定方法

IPv6 DAD プロキシの設定

手順の概要

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **[no] ipv6 nd dad-proxy**
5. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface** *type number* 例： `Device(config)# interface GigabitEthernet 0/0/1`	インターフェイスのタイプおよび番号を指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	**[no] ipv6 nd dad-proxy** 例： `Device(config-if)# ipv6 nd dad-proxy`	ND 抑制を DAD プロキシ モードで動作させる必要があるかどうか指定します。 このモードでは、DAD メッセージは転送されません。メッセージは既存のエントリに応答したり、バインディング テーブルに追加されたりします。
ステップ 5	**end** 例： `Device(config-if)# end`	ルータ インターフェイス コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

IPv6 DAD プロキシの設定例

例：IPv6 DAD プロキシの設定

```
Device> enable
Device# configure terminal
Device(config)# interface Ethernet 0/0
Device(config-if)# ipv6 nd dad-proxy
Device(config-if)# end
```

IPv6 DAD プロキシのその他の参考資料

関連資料

関連項目	マニュアル タイトル
IPv6 アドレッシングと接続	『*IPv6 Configuration Guide*』
Cisco IOS コマンド	『*Cisco IOS Master Commands List, All Releases*』
IPv6 コマンド	『*Cisco IOS IPv6 Command Reference*』
Cisco IOS IPv6 機能	『*Cisco IOS IPv6 Feature Mapping*』

MIB

MIB	MIB のリンク
	選択したプラットフォーム、Cisco IOS リリース、およびフィーチャ セットに関する MIB を探してダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

シスコのテクニカル サポート

説明	リンク
右の URL にアクセスして、シスコのテクニカル サポートを最大限に活用してください。これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

IPv6 DAD プロキシの機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだ

けを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *133 : IPv6 DAD* プロキシの機能情報

機能名	リリース	機能情報
IPv6 DAD プロキシ		次のコマンドが導入または変更されました。**ipv6 nd dad-proxy**、**mode dad-proxy**、**mode md-proxy**

第 99 章

IPv6 ネイバー探索マルチキャスト抑制

IPv6 ネイバー探索（ND）マルチキャスト抑制機能は、ND マルチキャスト ネイバー送信要求（NS）メッセージをドロップする（およびターゲットに代わって送信要求に応答する）か、またはユニキャストトラフィックに変換することでメッセージを抑制します。マルチキャストトラフィックからユニキャスト トラフィックへの変換は、レイヤ 2 マルチキャスト宛先 MAC をレイヤ 2 ユニキャスト宛先 MAC で置き換えることで行われます。変換するには、リンク上のアドレスと各アドレスのレイヤ2へのバインディングを把握している必要があります。抑制されたマルチキャスト メッセージは、ネイバー送信要求（NS）メッセージです。

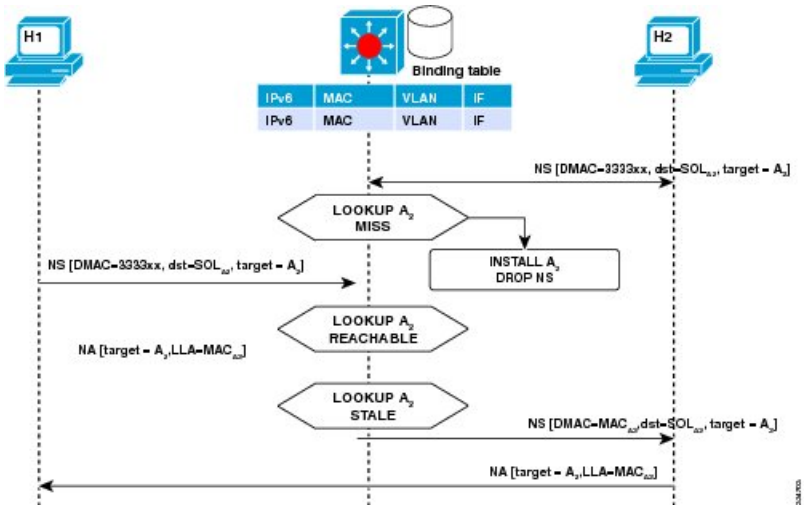
IPv6 ネイバー探索マルチキャスト抑制に関する情報

IPv6 ネイバー探索マルチキャスト抑制の概要

IPv6 ネイバー探索（ND）マルチキャスト抑制機能では、ND マルチキャスト ネイバー送信要求（NS）メッセージを、ドロップする（およびターゲットに代わって送信要求に応答する）か、またはユニキャストトラフィックに変換することで停止します。この機能は、適切なリンク運用に必要な制御トラフィックの量を削減します。

アドレスがバインディング テーブルに挿入されると、マルチキャスト アドレスに送信されたアドレス解決要求が代行受信され、デバイスはアドレスの所有者に代わって応答するか、要求をユニキャスト メッセージに変換して宛先に転送します。

次の図は、この機能の概要を示しています。



IPv6 ネイバー探索マルチキャスト抑制の設定方法

インターフェイスの IPv6 ネイバー探索マルチキャスト抑制の設定

手順の概要

1. **enable**
2. **configure terminal**
3. **ipv6 nd suppress policy** *policy-name*
4. **[no] mode mc-proxy**
5. **[no] mode full-proxy**
6. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ipv6 nd suppress policy** *policy-name* 例：	設定するネイバー探索（ND）抑制ポリシーの名前を指定します。

	コマンドまたはアクション	目的
	`Device (config)# ipv6 nd suppress policy policy1` `Device (config-nd-suppress)#`	
ステップ 4	**[no] mode mc-proxy** 例： `Device (config-nd-suppress)# mode mc-proxy`	ND 抑制ですべてのマルチキャスト ネイバー送信要求（NS）メッセージをプロキシする必要があるかどうか指定します。
ステップ 5	**[no] mode full-proxy** 例： `Device (config-nd-suppress)# mode full-proxy`	ND 抑制でユニキャストとマルチキャストの両方の NS メッセージをプロキシする必要があるかどうか指定します。
ステップ 6	**end** 例： `Device (config-nd-suppress)# end`	ND 抑制モードを終了し、特権 EXEC モードに戻ります。

IPv6 ネイバー探索マルチキャスト抑制の設定例

例：インターフェイスの IPv6 ネイバー探索抑制の設定

```
Device> enable
Device(config)# interface Ethernet 0/0
Device(config-if)# ipv6 nd suppress attach-policy policy1
```

IPv6 ネイバー探索マルチキャスト除去に関するその他の参考資料

関連資料

関連項目	マニュアル タイトル
IPv6 アドレッシングと接続	『*IPv6 Configuration Guide*』
Cisco IOS コマンド	『*Cisco IOS Master Commands List, All Releases*』
IPv6 コマンド	『*Cisco IOS IPv6 Command Reference*』

関連項目	マニュアル タイトル
Cisco IOS IPv6 機能	『*Cisco IOS IPv6 Feature Mapping*』

MIB

MIB	MIB のリンク
	選択したプラットフォーム、Cisco IOS リリース、およびフィーチャ セットに関する MIB を探してダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

シスコのテクニカル サポート

説明	リンク
右の URL にアクセスして、シスコのテクニカル サポートを最大限に活用してください。これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

Cisco TrustSec の概要の機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *134 : Cisco TrustSec* の概要の機能情報

機能名	リリース	機能情報
IPv6 の有効化 - インライン タギング	Cisco IOS XE Fuji 16.8.1	IPv6 のサポートが導入されました。

第 100 章

DHCP—DHCPv6 ガード

このモジュールでは、Dynamic Host Configuration Protocol バージョン 6（DHCPv6）ガード機能について説明します。この機能は、サーバからクライアントに DHCP パケットを転送する、承認されていない DHCP サーバとリレー エージェントから発信される DHCP 応答やアドバタイズメント メッセージをブロックします。リレー エージェントによってクライアントからサーバに送信されるクライアント メッセージはブロックされません。フィルタリングの判断は、受信側のスイッチ ポート、トランク、または VLAN に割り当てられているデバイスのロールによって決まります。また、より細かいレベルのフィルタ精度を提供するために、送信元サーバやリレー エージェントのアドレスに基づいて、または応答メッセージに記載されているプレフィックスやアドレスの範囲によってメッセージをフィルタリングできます。この機能により、トラフィック リダイレクションやサービス妨害（DoS）を防ぐことができます。

DHCPv6 ガードの制限

- DHCPv6 ガード機能は、EtherChannel ポートではサポートされません。

DHCPv6 ガードに関する情報

DHCPv6 ガードの概要

DHCPv6 ガード機能は、承認されていない DHCP サーバおよびリレー エージェントからの応答およびアドバタイズメント メッセージをブロックします。

パケットは 3 つの DHCP メッセージ タイプのいずれかに分類されます。すべてのクライアントメッセージは、デバイスのロールに関係なく、常にスイッチングされます。DHCP サーバのメッセージは、デバイスのロールがサーバに設定されている場合のみさらに処理されます。DHCP サーバのアドバタイズメント（送信元の検証とサーバの設定の場合）および DHCP サーバの応答（許可されたプレフィックスの場合）を含むサーバ メッセージはさらに処理されます。

デバイスが DHCP サーバとして設定されている場合、デバイスのロールの設定に関係なく、すべてのメッセージをスイッチングする必要があります。

DHCPv6 ガードの設定方法

DHCP—DHCPv6 ガードの設定

手順の概要

1. **enable**
2. **configure terminal**
3. **ipv6 access-list** *access-list-name*
4. **permit host** *address* **any**
5. **exit**
6. **ipv6 prefix-list** *list-name* **permit** *ipv6-prefix* **128**
7. **ipv6 dhcp guard policy** *policy-name*
8. **device-role** {**client** | **server**}
9. **match server access-list** *ipv6-access-list-name*
10. **match reply prefix-list** *ipv6-prefix-list-name*
11. **preference min** *limit*
12. **preference max** *limit*
13. **trusted-port**
14. **exit**
15. **interface** *type number*
16. **switchport**
17. **exit**
18. **exit**
19. **show ipv6 dhcp guard policy** [*policy-name*]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。

	コマンドまたはアクション	目的
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ipv6 access-list** *access-list-name* 例： `Device(config)# ipv6 access-list acl1`	IPv6 アクセス リストを定義し、IPv6 アクセス リスト コンフィギュレーション モードを開始します。
ステップ 4	**permit host** *address* **any** 例： `Device(config-ipv6-acl)# permit host FE80::A8BB:CCFF:FE01:F700 any`	名前付き IP アクセス リストに条件を設定します。
ステップ 5	**exit** 例： `Device(config-ipv6-acl)# exit`	IPv6 アクセス リスト コンフィギュレーション モードを終了して、グローバル コンフィギュレーション モードに戻ります。
ステップ 6	**ipv6 prefix-list** *list-name* **permit** *ipv6-prefix* **128** 例： `Device(config)# ipv6 prefix-list abc permit 2001:0DB8::/64 le 128`	IPv6 プレフィックス リストのエントリを作成します。
ステップ 7	**ipv6 dhcp guard policy** *policy-name* 例： `Device(config)# ipv6 dhcp guard policy pol1`	DHCPv6 ガード ポリシー名を定義して、DHCP ガード コンフィギュレーション モードを開始します。
ステップ 8	**device-role** {**client** | **server**} 例： `Device(config-dhcp-guard)# device-role server`	ターゲット（インターフェイスまたは VLAN）に接続されているデバイスのデバイス ロールを指定します。
ステップ 9	**match server access-list** *ipv6-access-list-name* 例： `Device(config-dhcp-guard)# match server access-list acl1`	（任意）検査済みメッセージ内のアドバタイズされた DHCP サーバおよびリレー アドレスが設定された承認サーバ アクセス リストからのものであることの検証をイネーブルにします。設定されていない場合、このチェックは回避されます。空のアクセス リストは、permit として処理されます。
ステップ 10	**match reply prefix-list** *ipv6-prefix-list-name* 例：	（任意）DHCP応答メッセージ内のアドバタイズされたプレフィックスが設定された承認プレフィック

	コマンドまたはアクション	目的
	`Device(config-dhcp-guard)# match reply prefix-list abc`	ス リストからのものであることの検証をイネーブルにします。設定されていない場合、このチェックは回避されます。空のプレフィクス リストは、permit として処理されます。
ステップ 11	**preference min** *limit* 例： `Device(config-dhcp-guard)# preference min 0`	（任意）アドバタイズされた設定（[preference] オプション内）が指定された制限を超過しているかどうかの検証をイネーブルにします。設定されていない場合、このチェックは回避されます。
ステップ 12	**preference max** *limit* 例： `Device(config-dhcp-guard)# preference max 255`	（任意）アドバタイズされた設定（[preference] オプション内）が指定された制限未満であるかどうかの検証をイネーブルにします。設定されていない場合、このチェックは回避されます。
ステップ 13	**trusted-port** 例： `Device(config-dhcp-guard)# trusted-port`	（任意）このポリシーが信頼できるポートに適用されることを指定します。すべての DHCP ガード ポリシングが無効になります。
ステップ 14	**exit** 例： `Device(config-dhcp-guard)# exit`	DHCP ガード コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードに戻ります。
ステップ 15	**interface** *type number* 例： `Device(config)# interface GigabitEthernet 0/2/0`	インターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 16	**switchport** 例： `Device(config-if)# switchport`	レイヤ3モードになっているインターフェイスを、レイヤ 2 設定用にレイヤ 2 モードにします。
ステップ 17	**exit** 例： `Device(config-if)# exit`	インターフェイス コンフィギュレーション モードを終了し、グローバルコンフィギュレーションモードに戻ります。
ステップ 18	**exit** 例： `Device(config)# exit`	グローバル コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

	コマンドまたはアクション	目的
ステップ 19	**show ipv6 dhcp guard policy** [*policy-name*] 例： `Device# show ipv6 dhcp policy guard pol1`	（任意）ポリシー設定と、そのポリシーが適用されるすべてのインターフェイスを表示します。

DHCPv6 ガードの設定例

例：DHCP—DHCPv6 ガードの設定

次の例は、DHCPv6 ガードの設定例を示しています。

その他の参考資料

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『Cisco IOS Master Commands List, All Releases』
DHCP コマンド：コマンド構文の詳細、コマンド モード、コマンド履歴、デフォルト、使用上の注意事項、および例	『*Cisco IOS IP Addressing Services Command Reference*』
DHCP の概念情報および設定情報	『*Cisco IOS IP Addressing Services Configuration Guide*』

標準規格/RFC

標準	タイトル
この機能でサポートが追加または変更された 標準/RFC はありません。	—

MIB

MIB	MIB のリンク
この機能によってサポートされる新しい MIB または変更された MIB はありません。	選択したプラットフォーム、Cisco IOS リリース、およびフィーチャ セットに関する MIB を探してダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

シスコのテクニカル サポート

説明	リンク
右の URL にアクセスして、シスコのテクニカル サポートを最大限に活用してください。これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

DHCP—DHCPv6 ガードの機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *135 : DHCP—DHCPv6* ガードの機能情報

機能名	リリース	機能情報
DHCP—DHCPv6 ガード		DHCP—DHCPv6 ガード機能は、サーバからクライアントに DHCP パケットを転送する、承認されていない DHCP サーバとリレー エージェントから発信される DHCP 応答やアドバタイズメント メッセージをブロックします。リレー エージェントによってクライアントからサーバに送信されるクライアント メッセージはブロックされません。 次のコマンドが導入または変更されました。**device-role** 、**ipv6 dhcp guard attach-policy (DHCPv6 Guard)**、**ipv6 dhcp guard policy**、**match reply prefix-list**、**match server access-list**、**preference (DHCPv6 Guard)**、**show ipv6 dhcp guard policy**、**trusted-port (DHCPv6 Guard)**。

第 101 章

IPv6 ソース ガードとプレフィックス ガード

IPv6 ソース ガードと IPv6 プレフィックス ガードは、IPv6 トラフィックの送信元を検証するレイヤ 2 スヌーピング機能です。IPv6 ソース ガードは、不明な送信元からのデータ トラフィックをブロックします。たとえば、バインディング テーブルにまだ入力されていないトラフィックや、ネイバー探索（ND）または Dynamic Host Configuration Protocol（DHCP）グリーニングを介して学習されていないトラフィックをブロックします。IPv6 プレフィックス ガードは、承認および委任されたトラフィック以外のホームノードが送信元のトラフィックを阻止します。

IPv6 ソース ガードとプレフィックス ガードに関する情報

IPv6 ソース ガードの概要

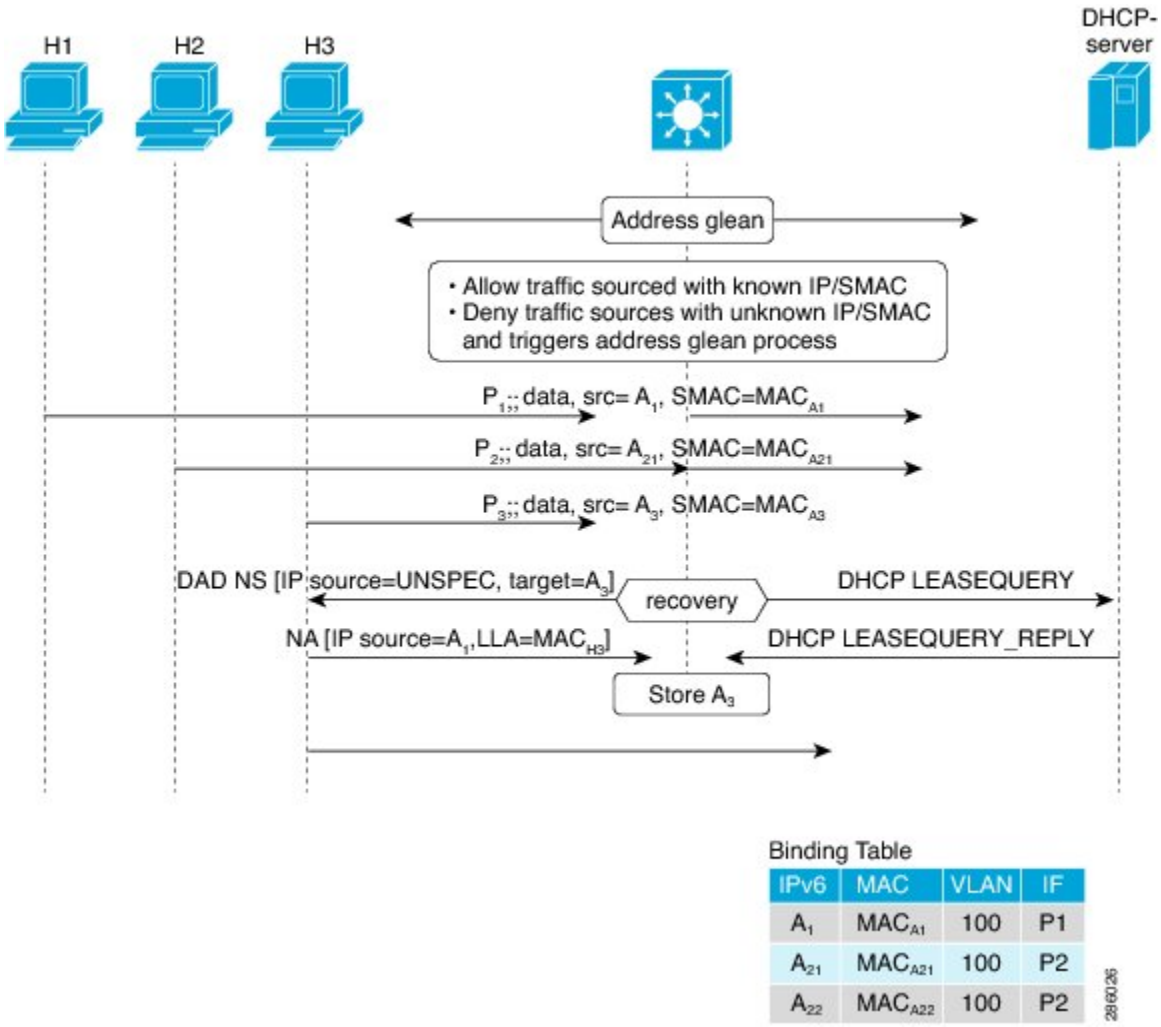
IPv6 ソース ガードは、入力されたバインディング テーブルとデータ トラフィックのフィルタリング間で動作するインターフェイス機能です。この機能により、デバイスは、バインディング テーブルに保存されていないアドレスから送信されたトラフィックを拒否できます。IPv6 ソース ガードは ND や DHCPパケットを検査せず、むしろ、IPv6 ネイバー探索（ND）インスペクションや IPv6 アドレス収集（どちらもリンク上の既存アドレスを検出して、バインディング テーブルに保存する機能）と連動して機能します。IPv6 ソース ガードは、入力されたバインディング テーブルとデータ トラフィックのフィルタリング間で動作するインターフェイスであり、IPv6 ソース ガードが機能するためには、バインディング テーブルに IPv6 プレフィックスが入力されている必要があります。

IPv6 ソース ガードは、DHCP サーバによって割り当てられていない送信元からのトラフィックなど、不明な発信元や未割り当てのアドレスからのトラフィックを拒否できます。トラフィッ

クが拒否されると、IPv6アドレス収集機能に通知されるため、DHCPサーバをクエリして、またはIPv6 NDを使用して、トラフィックのリカバリを試みることができます。データ収集機能は、有効なアドレスをバインディング テーブルに保存できず、復旧パスがなく、エンド ユーザが接続できなくなるとすぐに、デバイスとエンド ユーザがデッドロックになるのを防ぎます。

次の図は、IPv6 ソース ガードと IPv6 アドレス収集の仕組みの概要を示しています。

図 *29 : IPv6* ソース ガードとアドレス収集の概要



IPv6 プレフィックス ガードの概要

IPv6 プレフィックス ガード機能は、IPv6 ソース ガード機能内で動作し、トポロジ面で正しくないアドレスから発信されたトラフィックをデバイスが拒否できるようにします。IPv6 プレフィックス ガードは、IPv6 プレフィックスが DHCP プレフィックス委任を使用してデバイス（ホーム ゲートウェイなど）に委任される場合によく使用されています。この機能は、リンク

に割り当てられたアドレスの範囲を検出し、この範囲に入っていないアドレスを発信元とするトラフィックをブロックします。

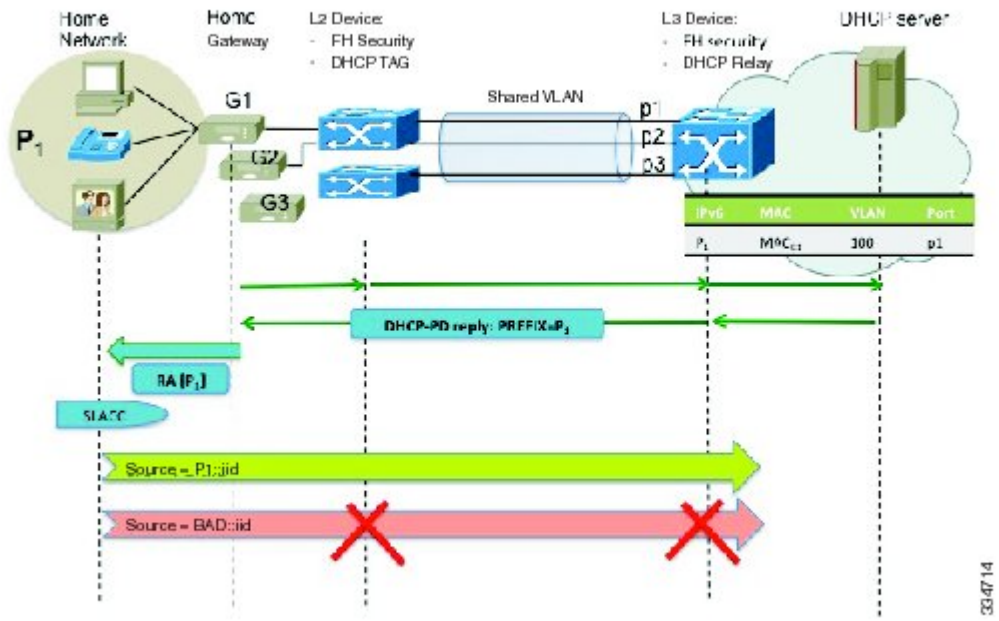
許可するプレフィックスとブロックするプレフィックスを決めるために、IPv6 プレフィックス ガードは以下の情報を使用します。

- ルータ アドバタイズメント（RA）でのプレフィックス収集
- DHCP プレフィックス委任でのプレフィックス収集
- 静的設定

IPv6 プレフィックス ガードでは、許可されるプレフィックスは常にハードウェア テーブルにダウンロードされます。ハードウェアは、パケットのスイッチングが行われるたびに、パケットの送信元をこのテーブルで照合し、一致するものがない場合そのパケットをドロップします。

次の図は、プレフィックスが DHCP-PD メッセージで収集されるサービス プロバイダー（SP）のシナリオを示しています。

図 *30* : プレフィックスが収集される *DHCP-PD* メッセージのシナリオ



IPv6 ソース ガードとプレフィックス ガードの設定方法

IPv6 ソース ガードの設定

手順の概要

1. **enable**
2. **configure terminal**
3. **ipv6 source-guard policy** *source-guard-policy*
4. **permit link-local**
5. **deny global-autoconf**
6. **trusted**
7. **exit**
8. **show ipv6 source-guard policy** ［*snooping-policy*］

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ipv6 source-guard policy** *source-guard-policy* 例： `Device(config)# ipv6 source-guard policy my_sourceguard_policy`	IPv6 ソースガードポリシー名を定義して、スイッチ統合セキュリティ機能のソースガード ポリシー コンフィギュレーション モードを開始します。
ステップ 4	**permit link-local** 例： `Device(config-sisf-sourceguard)# permit link-local`	リンクローカル アドレスから発信されるすべてのデータ トラフィックに対するハードウェア ブリッジングを許可します。
ステップ 5	**deny global-autoconf** 例： `Device(config-sisf-sourceguard)# deny global-autoconf`	自動設定されたグローバル アドレスからのデータ トラフィックを拒否します。

	コマンドまたはアクション	目的
ステップ 6	**trusted** 例： `Device(config-sisf-sourceguard)# trusted`	ポリシーが適用されるターゲットのすべてのデータトラフィックに対するハードウェアブリッジングを許可します。
ステップ 7	**exit** 例： `Device(config-sisf-sourceguard)# exit`	ソース ガード ポリシー コンフィギュレーション モードを終了して、特権 EXEC モードに戻ります。
ステップ 8	**show ipv6 source-guard policy** ［*snooping-policy*］ 例： `Device# show ipv6 source-guard policy policy1`	IPv6 ソースガード ポリシー設定を表示します。

インターフェイスの IPv6 ソース ガードの設定

手順の概要

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **ipv6 source-guard attach-policy** *source-guard-policy*
5. **exit**
6. **show ipv6 source-guard policy** *source-guard-policy*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface** *type number* 例： `Device(config)# interface fastethernet 3/13`	インターフェイスのタイプおよび番号を指定し、インターフェイス コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 4	**ipv6 source-guard attach-policy** *source-guard-policy* 例： `Device(config-if)# ipv6 source-guard attach-policy my_source_guard_policy`	インターフェイスに IPv6 ソース ガードを適用します。
ステップ 5	**exit** 例： `Device(config-if)# exit`	インターフェイス コンフィギュレーション モードを終了して、デバイスを特権 EXEC モードにします。
ステップ 6	**show ipv6 source-guard policy** *source-guard-policy* 例： `Device# show ipv6 source-guard policy policy1`	IPv6 ソース ガードが適用されているすべてのインターフェイスを表示します。

IPv6 プレフィックス ガードの設定

手順の概要

1. **enable**
2. **configure terminal**
3. **ipv6 source-guard policy** *source-guard-policy*
4. **validate address**
5. **validate prefix**
6. **exit**
7. **show ipv6 source-guard policy** ［*source-guard-policy*］

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ipv6 source-guard policy** *source-guard-policy* 例： `Device(config)# ipv6 source-guard policy my_snooping_policy`	IPv6 ソースガードポリシー名を定義して、スイッチ統合セキュリティ機能のソースガード ポリシー コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 4	**validate address** 例： `Device(config-sisf-sourceguard)# no validate address`	アドレス検証機能を無効にし、IPv6 プレフィックス ガード機能を設定できるようにします。
ステップ 5	**validate prefix** 例： `Device(config-sisf-sourceguard)# validate prefix`	IPv6 プレフィックスガード動作を実行するよう、IPv6 ソースガードを有効にします。
ステップ 6	**exit** 例： `Device(config-sisf-sourceguard)# exit`	スイッチ統合セキュリティ機能のソースガード ポリシー コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。
ステップ 7	**show ipv6 source-guard policy** ［*source-guard-policy*］ 例： `Device# show ipv6 source-guard policy policy1`	IPv6 ソースガード ポリシー設定を表示します。

IPv6 ソース ガードとプレフィックス ガードの設定例

例：IPv6 ソース ガードとプレフィックス ガードの設定

```
Device# ipv6 source-guard policy policy1

Policy guard configuration:
  validate prefix
  validate address
```

Cisco TrustSec の概要の機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *136 : Cisco TrustSec* の概要の機能情報

機能名	リリース	機能情報
IPv6 の有効化 - インライン タギング	Cisco IOS XE Fuji 16.8.1	IPv6 のサポートが導入されました。

第 102 章

IPv6 宛先ガード

IPv6 宛先ガード機能は、IPv6 ネイバー探索とともに動作して、リンク上でアクティブであると認識されているアドレスについてのみ、デバイスがアドレス解決を行うようにします。アドレス収集機能を用いてリンク上でアクティブな全ての宛先をバインディング表に追加し、バインディング表にない宛先に対するアドレス解決処理を実行前にブロックします。

IPv6 宛先ガードの前提条件

- IPv6 ネイバー探索機能についての知識が必要です。IPv6 ネイバー探索の詳細については、「IPv6 アドレッシングと基本接続の実装」を参照してください。
- IPv6 ファーストホップ セキュリティ バインディング テーブル機能についての知識が必要です。詳細については、「IPv6 ファーストホップ セキュリティ バインディング テーブル」を参照してください。

IPv6 宛先ガードに関する情報

IPv6 宛先ガードの概要

IPv6 宛先ガード機能は、IPv6 ネイバー探索とともに動作して、リンク上でアクティブであると認識されているアドレスについてのみ、デバイスがアドレス解決を行うようにします。アドレス収集機能を用いてリンク上でアクティブな全ての宛先をバインディング表に追加し、バインディング表にない宛先に対するアドレス解決処理を実行前にブロックします。

デバイスはルーティングされた着信トラフィックをフィルタリングする前に、Neighbor Discovery Protocol（NDP）メッセージおよび DHCP メッセージをスヌーピングして、リンク上のアドレスを収集します。パケットがデバイスに到達し、宛先またはネクスト ホップの隣接関係（アジャセンシー）がまだ存在していない場合、NDP はデバイス バインディング テーブルを参照して、リンク上の宛先またはネクスト ホップがすでに収集済みであるか確認します。バインディング テーブルに当該宛先が存在しない場合、そのパケットはドロップされます。存在する場合、ネイバー探索の解決が実行されます。

IPv6 宛先ガードの設定方法

IPv6 宛先ガードの設定

手順の概要

1. **enable**
2. **configure terminal**
3. **ipv6 destination-guard policy** *policy-name*
4. **enforcement** {**always** | **stressed**}
5. **exit**
6. **interface** *type number*
7. **ipv6 destination-guard attach-policy** [*policy-name*]
8. **exit**
9. **show ipv6 destination-guard policy** [*policy-name*]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ipv6 destination-guard policy** *policy-name* 例： `Device(config)# ipv6 destination-guard policy pol1`	宛先ガード ポリシー名を定義して、宛先ガード コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 4	**enforcement** {**always** | **stressed**} 例： `Device(config-destguard)# enforcement always`	ターゲット アドレスの強制レベルを設定します。
ステップ 5	**exit** 例： `Device(config-destguard)# exit`	宛先ガード コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードに戻ります。
ステップ 6	**interface** *type number* 例： `Device(config)# interface GigabitEthernet 0/0/1`	インターフェイス コンフィギュレーション モードを開始します。
ステップ 7	**ipv6 destination-guard attach-policy** [*policy-name*] 例： `Device(config-if)# ipv6 destination-guard attach-policy pol1`	インターフェイスに宛先ガードポリシーを対応付けます。
ステップ 8	**exit** 例： `Device(config-if)# exit`	インターフェイス コンフィギュレーション モードを終了し、特権EXECコンフィギュレーションモードに戻ります。
ステップ 9	**show ipv6 destination-guard policy** [*policy-name*] 例： `Device# show ipv6 destination-guard policy pol1`	（任意）ポリシー設定と、そのポリシーが適用されるすべてのインターフェイスを表示します。

IPv6 宛先ガードの設定例

例：IPv6 宛先ガード ポリシーの設定

次の例は、宛先ガード ポリシーの設定方法を示しています。

```
Router> enable
Router# configure terminal
Router(config)# interface GigabitEthernet 0/0/1
Router(config-if)# ipv6 destination-guard attach-policy destination

Router# show ipv6 destination-guard policy destination
Destination guard policy Destination:
```

```
enforcement always
      Target: Gi0/0/1
```

その他の参考資料

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『*Cisco IOS Master Command List, All Releases*』
IPv6 アドレッシングと接続	『*IPv6 Configuration Guide*』
IPv6 コマンド	『*Cisco IOS IPv6 Command Reference*』
Cisco IOS IPv6 機能	『*Cisco IOS IPv6 Feature Mapping*』

シスコのテクニカル サポート

説明	リンク
右の URL にアクセスして、シスコのテクニカル サポートを最大限に活用してください。これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

Cisco TrustSec の概要の機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *137 : Cisco TrustSec* の概要の機能情報

機能名	リリース	機能情報
IPv6 の有効化 - インライン タギング	Cisco IOS XE Fuji 16.8.1	IPv6 のサポートが導入されました。

第 103 章

IPv6 の RFC

標準および **RFC**

RFC	タイトル
RFC 1195	『*Use of OSI IS-IS for Routing in TCP/IP and Dual Environments*』
RFC 1267	『*A Border Gateway Protocol 3 (BGP-3)*』
RFC 1305	『*Network Time Protocol (Version 3) Specification, Implementation and Analysis*』
RFC 1583	『*OSPF version 2*』
RFC 1772	『*Application of the Border Gateway Protocol in the Internet*』
RFC 1886	『*DNS Extensions to Support IP version 6*』
RFC 1918	『*Address Allocation for Private Internets*』
RFC 1981	『*Path MTU Discovery for IP version 6*』
RFC 2080	『*RIPng for IPv6*』
RFC 2281	『*Cisco Hot Standby Router Protocol (HSRP)*』
RFC 2332	『*NBMA Next Hop Resolution Protocol (NHRP)*』
RFC 2373	『*IP Version 6 Addressing Architecture*』
RFC 2374	集約可能なグローバル ユニキャスト形式
RFC 2375	『*IPv6 Multicast Address Assignments*』
RFC 2401	『*Security Architecture for the Internet Protocol*』
RFC 2402	『*IP Authentication Header*』
RFC 2404	『*The Use of Hash Message Authentication Code Federal Information Processing Standard 180-1 within Encapsulating Security Payload and Authentication Header*』

RFC	タイトル
RFC 2406	『*IP Encapsulating Security Payload (ESP)*』
RFC 2407	『*The Internet Security Domain of Interpretation for ISAKMP*』
RFC 2408	『*Internet Security Association and Key Management Protocol*』
RFC 2409	『*Internet Key Exchange (IKE)*』
RFC 2427	『*Multiprotocol Interconnect over Frame Relay*』
RFC 2428	『*FTP Extensions for IPv6 and NATs*』
RFC 2460	『*Internet Protocol, Version 6 (IPv6) Specification*』
RFC 2461	『*Neighbor Discovery for IP Version 6 (IPv6)*』
RFC 2462	『*IPv6 Stateless Address Autoconfiguration*』
RFC 2463	『*Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification*』
RFC 2464	『*Transmission of IPv6 Packets over Ethernet*』
RFC 2467	『*Transmission of IPv6 Packets over FDDI*』
RFC 2472	『*IP Version 6 over PPP*』
RFC 2473	『*Generic Packet Tunneling in IPv6 Specification*』
RFC 2474	*Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers*
RFC 2475	『*An Architecture for Differentiated Services Framework*』
RFC 2492	『*IPv6 over ATM*』
RFC 2545	『*Use of BGP-4 Multiprotocol Extensions for IPv6 Inter-Domain Routing*』
RFC 2590	『*Transmission of IPv6 Packets over Frame Relay Specification*』
RFC 2597	『*Assured Forwarding PHB*』
RFC 2598	『*An Expedited Forwarding PHB*』
RFC 2640	『*Internet Protocol, Version 6 Specification*』
RFC 2684	『*Multiprotocol Encapsulation over ATM Adaptation Layer 5*』
RFC 2697	『*A Single Rate Three Color Marker*』
RFC 2698	『*A Two Rate Three Color Marker*』

RFC	タイトル
RFC 2710	『*Multicast Listener Discovery (MLD) for IPv6*』
RFC 2711	『*IPv6 Router Alert Option*』
RFC 2732	『*Format for Literal IPv6 Addresses in URLs*』
RFC 2765	『*Stateless IP/ICMP Translation Algorithm (SIIT)*』
RFC 2766	『*Network Address Translation-Protocol Translation (NAT-PT)*』
RFC 2858	『*Multiprotocol Extensions for BGP-4*』
RFC 2893	『*Transition Mechanisms for IPv6 Hosts and Routers*』
RFC 3056	『*Connection of IPv6 Domains via IPv4 Clouds*』
RFC 3068	『*An Anycast Prefix for 6to4 Relay Routers*』
RFC 3095	『*RObust Header Compression (ROHC): Framework and Four Profiles: RTP, UDP, ESP, and Uncompressed*』
RFC 3107	『*Carrying Label Information in BGP-4*』
RFC 3137	『*OSPF Stub Router Advertisement*』
RFC 3147	『*Generic Routing Encapsulation over CLNS*』
RFC 3152	*IP6.ARPA* の委任
RFC 3162	*RADIUS* および *IPv6*
RFC 3315	『*Dynamic Host Configuration Protocol for IPv6 (DHCPv6)*』
RFC 3319	『*Dynamic Host Configuration Protocol (DHCPv6) Options for Session Initiated Protocol (SIP) Servers*』
RFC 3392	『*Capabilities Advertisement with BGP-4*』
RFC 3414	『*User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3)*』
RFC 3484	『*Default Address Selection for Internet Protocol version 6 (IPv6)*』
RFC 3513	インターネット プロトコル バージョン *6*（*IPv6*）アドレス 指定アーキテクチャ
RFC 3576	『*Change of Authorization*』
RFC 3587	『*IPv6 Global Unicast Address Format*』
RFC 3590	『*Source Address Selection for the Multicast Listener Discovery (MLD) Protocol*』

RFC	タイトル
RFC 3596	『*DNS Extensions to Support IP Version 6*』
RFC 3633	『*DHCP IPv6 Prefix Delegation*』
RFC 3646	『*DNS Configuration options for Dynamic Host Configuration Protocol for IPv6 (DHCPv6)*』
RFC 3697	『*IPv6 Flow Label Specification*』
RFC 3736	『*Stateless DHCP Service for IPv6*』
RFC 3756	『*IPv6 Neighbor Discovery (ND) Trust Models and Threats*』
RFC 3759	『*RObust Header Compression (ROHC): Terminology and Channel Mapping Examples*』
RFC 3775	『*Mobility Support in IPv6*』
RFC 3810	『*Multicast Listener Discovery Version 2 (MLDv2) for IPv6*』
RFC 3846	『*Mobile IPv4 Extension for Carrying Network Access Identifiers*』
RFC 3879	『*Deprecating Site Local Addresses*』
RFC 3898	『*Network Information Service (NIS) Configuration Options for Dynamic Host Configuration Protocol for IPv6 (DHCPv6)*』
RFC 3954	『*Cisco Systems NetFlow Services Export Version 9*』
RFC 3956	『*Embedding the Rendezvous Point (RP) Address in an IPv6 Multicast Address*』
RFC 3963	『*Network Mobility (NEMO) Basic Support Protocol*』
RFC 3971	『*SEcure Neighbor Discovery (SEND)*』
RFC 3972	『*Cryptographically Generated Addresses (CGA)*』
RFC 4007	『*IPv6 Scoped Address Architecture*』
RFC 4075	『*Simple Network Time Protocol (SNTP) Configuration Option for DHCPv6*』
RFC 4087	『*IP Tunnel MIB*』
RFC 4091	『*The Alternative Network Address Types (ANAT) Semantics for the Session Description Protocol (SDP) Grouping Framework*』
RFC 4092	『*Usage of the Session Description Protocol (SDP) Alternative Network Address Types (ANAT) Semantics in the Session Initiation Protocol (SIP)*』
RFC 4109	『*Algorithms for Internet Key Exchange version 1 (IKEv1)*』
RFC 4191	『*Default Router Preferences and More-Specific Routes*』

RFC	タイトル
RFC 4193	固有ローカル *IPv6* ユニキャスト アドレス
RFC 4214	『*Intra-Site Automatic Tunnel Addressing Protocol (ISATAP)*』
RFC 4242	『*Information Refresh Time Option for Dynamic Host Configuration Protocol for IPv6 (DHCPv6)*』
RFC 4282	『*The Network Access Identifier*』
RFC 4283	『*Mobile Node Identifier Option for Mobile IPv6*』
RFC 4285	『*Authentication Protocol for Mobile IPv6*』
RFC 4291	『*IP Version 6 Addressing Architecture*』
RFC 4292	『*IP Forwarding Table MIB*』
RFC 4293	『*Management Information Base for the Internet Protocol (IP)*』
RFC 4302	『*IP Authentication Header*』
RFC 4306	『*Internet Key Exchange (IKEv2) Protocol*』
RFC 4308	『*Cryptographic Suites for IPsec*』
RFC 4364	『*BGP MPLS/IP Virtual Private Networks (VPNs)*』
RFC 4382	『*MPLS/BGP Layer 3 Virtual Private Network (VPN) Management Information Base*』
RFC 4443	『*Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification*』
RFC 4552	『*Authentication/Confidentiality for OSPFv3*』
RFC 4594	『*Configuration Guidelines for DiffServ Service Classes*』
RFC 4601	『*Protocol Independent Multicast - Sparse Mode (PIM-SM): Protocol Specification*』
RFC 4610	『*Anycast-RP Using Protocol Independent Multicast (PIM)*』
RFC 4649	『*Dynamic Host Configuration Protocol for IPv6 (DHCPv6) Relay Agent Remote-ID Option*』
RFC 4659	『*BGP-MPLS IP Virtual Private Network (VPN) Extension for IPv6 VPN*』
RFC 4724	『*Graceful Restart Mechanism for BGP*』
RFC 4798	『*Connecting IPv6 Islands over IPv4 MPLS Using IPv6 Provider Edge Routers (6PE)*』
RFC 4818	『*RADIUS Delegated-IPv6-Prefix Attribute*』

RFC	タイトル
RFC 4861	『*Neighbor Discovery for IP version 6 (IPv6)*』
RFC 4862	『*IPv6 Stateless Address Autoconfiguration*』
RFC 4884	『*Extended ICMP to Support Multi-Part Messages*』
RFC 4885	『*Network Mobility Support Terminology*』
RFC 4887	『*Network Mobility Home Network Models*』
RFC 5015	『*Bidirectional Protocol Independent Multicast (BIDIR-PIM)*』
RFC 5059	『*Bootstrap Router (BSR) Mechanism for Protocol Independent Multicast (PIM)*』
RFC 5072	『*IPv6 over PPP*』
RFC 5095	『*Deprecation of Type 0 Routing Headers in IPv6*』
RFC 5120	『*M-ISIS: Multi Topology (MT) Routing in Intermediate System to Intermediate Systems (IS-ISs)*』
RFC 5130	『*A Policy Control Mechanism in IS-IS Using Administrative Tags*』
RFC 5187	『*OSPFv3 Graceful Restart*』
RFC 5213	『*Proxy Mobile IPv6*』
RFC 5308	『*Routing IPv6 with IS-IS*』
RFC 5340	『*OSPF for IPv6*』
RFC 5460	『*DHCPv6 Bulk Leasequery*』
RFC 5643	『*Management Information Base for OSPFv3*』
RFC 5838	『*Support of Address Families in OSPFv3*』
RFC 5844	『*IPv4 Support for Proxy Mobile IPv6*』
RFC 5845	『*Generic Routing Encapsulation (GRE) Key Option for Proxy Mobile IPv6*』
RFC 5846	『*Binding Revocation for IPv6 Mobility*』
RFC 5881	『*Bidirectional Forwarding Detection (BFD) for IPv4 and IPv6 (Single Hop)*』
RFC 5905	『*Network Time Protocol Version 4: Protocol and Algorithms Specification*』
RFC 5969	『*IPv6 Rapid Deployment on IPv4 Infrastructures (6RD) -- Protocol Specification*』
RFC 6105	『*IPv6 Router Advertisement Guard*』

RFC	タイトル
RFC 6620	『*FCFS SAVI: First-Come, First-Served Source Address Validation Improvement for Locally Assigned IPv6 Addresses*』

第 X 部

MACsec と MKA

第 104 章

WAN MACSEC および MKA のサポートの機能強化

WAN MACsec および MKA 機能により、WAN 上での MACsec のサポート、および MACsec Key Agreement（MKA）プロトコルのアップリンクのサポートと事前共有キーのサポートが導入されます。

WAN MACsec および MKA

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *138 : WAN MACsec* および *MKA*

機能名	リリース	機能情報
WAN MACsec と MKA	Cisco IOS XE リリース 3.14S	WAN MACsec および MKA 機能により、WAN 上での MACsec のサポート、および MACsec Key Agreement（MKA）プロトコルのアップリンクのサポートと事前共有キーのサポートが導入されます。 次のコマンドが導入または変更されました。confidentiality-offset、eapol destination-mac、key-server、linksec policy、replay-protection window-size
WAN インターフェイス カード上の MACsec	Cisco IOS XE Release 3.16S	WAN インターフェイス カード上の MACsec 機能により、Cisco 4000 シリーズ サービス統合型ルータ（ISR）上の WAN インターフェイス カードに MACsec サポートが導入されます。
EAPoL フレームイーサネットタイプを変更する MACsec CLI オプション	Cisco IOS XE リリース 3.17S	EAPOL フレーム イーサネット タイプを変更する MACsec CLI オプションの機能により、Extensible Authentication Protocol over LAN（EAPoL）フレームイーサネットタイプをユーザーが変更できるようにするための設定オプションが提供されます。 次のコマンドが導入または変更されました。eapol eth-type
MACsec 暗号化を使用したポートチャネルの設定のサポート	Cisco IOS XE Gibraltar 17.2	この機能拡張により、MACsec 対応インターフェイスでポートチャネルを設定して、ポートチャネルトラフィックのシームレスなフローを実現できます。それにより、トラフィックが保護されます。

WAN MACsec および MKA のサポート機能強化の前提条件

- WAN MACsec には MACsec ライセンスが必要です。*Cisco ASR 1000* シリーズ イーサネット ラインカード データシート ドキュメントの表 8 を参照してください。https://www.cisco.com/c/en/us/products/collateral/application-networking-services/wide-area-application-services-waas-software/data-sheet-c78-729778.html
- Cisco ISR 4000 プラットフォームでは、MACsec を設定するために HSECK9 ライセンスが必要です。
- レイヤ 2 の透過型イーサネット サービスが存在している必要があります。
- サービス プロバイダー ネットワークが、Extensible Authentication Protocol over LAN（EAPoL）などの透過的な MACsec レイヤ 2 制御プロトコルを提供する必要があります。

WAN MACsec および MKA のサポート機能強化の制約事項

- Cisco ASR 1000 シリーズ アグリゲーション サービス ルータでは、MACsecで AAA アカウンティングがサポートされません。
- Cisco ASR 1000 シリーズ アグリゲーション サービス ルータでは、高可用性クラスタでの MKA の設定がサポートされません。
- MACsec でサポートされる最大速度は、各インターフェイスのライン レートです。ただし、転送機能はシステムの最大転送容量によって制限される場合があります。
- Cisco ASR1001-X ルータでは、MACsec は内蔵ポートでのみサポートされます。ルータに取り付けられている共有ポート アダプタ（SPA）では有効にすることはできません。
- ポートチャネルを設定するには、リンクバンドルの各インターフェイスでMACsecを設定してください。
- メイン インターフェイス上でコマンド **macsec dot1q-in-clear 1** を使用してネイティブ サブインターフェイス上に設定された MACsec はサポートされません。
- Cisco IOS XE Denali 16.3.3 リリース以降では、RP のスイッチオーバー時に、物理/サブインターフェイス コンフィギュレーション モードでの macsec コマンドの再入力は必要ありません。
- キーのラップ解除の失敗が原因で MKA セッションが切断された場合は、それぞれのインターフェイスで MACsec 設定コマンドを使用して事前共有キー ベースの MKA セッションを再設定し、MKA セッションを接続状態にします。
- イーサネット仮想回線（EVC）を使用した物理インターフェイスで設定されたMACsecはサポートされません。このような場合、EAPoL フレームはドロップされます。
- Cisco ASR 1000 シリーズ アグリゲーション サービス ルータについて、次の表に、GigabitEthernet インターフェイスと、インターフェイスごとにサポートされるピアの最大数を示します。

GigabitEthernet インターフェイス	インターフェイスごとのピア数	
1G	8	
10G	32	
40G	60	
100 G	120	

- `macsec dot1q-in-clear` が有効になっている場合、ネイティブ VLAN はサポートされません。

WAN MACsec および MKA のサポートの機能強化に関する情報

MACsec および MKA の概要

MACsec は、IEEE 802.1AE 規格ベースのレイヤ 2 ホップバイホップ暗号化であり、これにより、メディア アクセス非依存プロトコルに対してデータの機密性と完全性を確保できます。

MACsec は、暗号化キーにアウトオブバンド方式を使用して、有線ネットワーク上で MAC レイヤの暗号化を提供します。MACsec Key Agreement（MKA）プロトコルでは、必要なセッション キーを提供し、必要な暗号化キーを管理します。 ホスト側のリンク（ネットワーク アクセス デバイスと、PC や IP フォンなどのエンドポイント デバイス間のリンク）だけが MACsec を使用して保護できます。

MACsec Key Agreement（MKA）による 802.1AE 暗号化は、ルータまたはスイッチとホスト デバイス間の暗号化用に、ダウンリンク ポートでサポートされます。

MACsec は、イーサネット パケットの送信元および宛先 MAC アドレスを除くすべてのデータを暗号化します。

WAN またはメトロ イーサネット上に MACsec サービスを提供するために、サービス プロバイダーは、Ethernet over Multiprotocol Label Switching（EoMPLS）および L2TPv3 などのさまざまなトランスポート レイヤ プロトコルを使用して、E-Line や E-LAN などのレイヤ 2 透過サービスを提供しています。

EAP-over-LAN（EAPOL）プロトコルデータ ユニット（PDU）のパケット本体は、MACsec Key Agreement PDU（MKPDU）と呼ばれます。3 ハートビート（1 ハートビートは 2 秒）後に MKPDU が受信されない場合、ライブ ピアのリストからピアが削除されます。たとえば、クライアントが切断さると、最後の MKPDU が クライアントにより受信されてから 3 ハートビートが経過するまで、スイッチ上の参加者は MKA を操作し続けます。

MKA 機能のサポートにより、暗号化されていない VLAN タグ（802.1Q タグ）などのトンネリング情報を提供します。そのため、サービス プロバイダーは、複数のポイントツーポイント サービスやマルチポイント サービスが単一の物理インターフェイス上で共存でき、表示されるようになった VLAN ID に基づいて差別化できるように、サービス多重化を提供できます。

サービス多重化の他に、暗号化されていない VLAN タグもサービス プロバイダーが 802.1Q タグの一部として表示されている 802.1P（CoS）に基づいて SP ネットワーク全体にわたり Quality of Service（QoS）を提供できるようにします。

WAN MACsec および MKA のサポート機能強化の利点

- ポイントツーポイント（P2P）導入モデルのサポート。
- ポイントツーマルチポイント（P2MP）導入モデルのサポート。

- 同一の物理インターフェイス上の複数の P2P および P2MP 導入のサポート。
- 128 ビットおよび 256 ビット Advanced Encryption Standard のサポート：データ パケットの Galois Counter Mode（AES-GCM）暗号化。
- 128 ビットおよび 256 ビット Advanced Encryption Standard のサポート：制御パケットの暗号ベースのメッセージ認証コード（AEC-CMAC）暗号化。
- キャリア イーサネット サービス多重化を有効にするための、clear オプションでの VLAN タグのサポート。
- MACsec サブインターフェイスと非 MACsec サブインターフェイスの共存のサポート。
- 設定可能な Extensible Authentication Protocol over LAN 宛先アドレスのサポート。
- EAPoL イーサネット タイプを変更する設定可能オプションのサポート。
- サービス プロバイダー ネットワークでのパケット再順序付けに対応するための、設定可能なリプレイ保護ウィンドウ サイズのサポート。

WAN MACsec および MKA のサポート機能強化の実装のベスト プラクティス

- MACsec を有効にする前に、基本的なレイヤ 2 イーサネット接続が確立され、検証されていることを確認します。カスタマー エッジ デバイス間の基本的な ping が機能している必要があります。
- WAN MACsec を初めて設定する場合は、MACsec を有効にした後にセッションの確立に失敗した場合にロック アウトされないように、リモート サイトへのアウトオブバンド接続が確立されていることを確認します。
- MACsec を初めて確立するときには **access-control should-secure** コマンドを設定し、その後、移行で必要になる場合以外は、セッションの確立が成功した後にこのコマンドをデフォルトの **access-control must-secure** に変更することを推奨します。
- インターフェイス MTU を設定し、これを MACsec オーバーヘッドに合わせて調整することを推奨します（例：32 バイト）。MACsec の暗号化と復号化は物理レベルで行われ、MTU のサイズは送信元または宛先のルータには影響しませんが、中間サービス プロバイダー ルータに影響を与える可能性があります。インターフェイスで MTU 値を設定すると、MACsec オーバーヘッドを含む MTU ネゴシエーションが可能になります。

MKA ポリシーの継承

WAN ルータでは MKA ポリシーは継承され、デフォルト値も含まれます。新しいセッションが開始されると、次のルールが適用されます。

- MKA ポリシーがサブインターフェイスに設定されている場合、このポリシーは MKA セッションが開始されると適用されます。

- MKA ポリシーがサブインターフェイスに設定されていない場合、物理インターフェイスに設定されているポリシーがセッションの開始時に適用されます。
- MKA ポリシーがサブインターフェイスまたは物理インターフェイスに設定されていない場合、デフォルトのポリシーがセッションの開始時に適用されます。

キー ライフタイムおよびヒットレス キー ロールオーバー

MACsec キー チェーンには、キー ID とオプションのライフタイムが設定された複数の事前共有キー（PSK）を含めることができます。キーのライフタイムには、キーが期限切れになる時刻が指定されます。ライフタイム設定が存在しない場合は、無期限のデフォルト ライフタイムが使用されます。ライフタイムが設定されている場合、ライフタイムの期限が切れた後に、MKA はキー チェーン内の次に設定された事前共有キーにロールオーバーします。キーのタイム ゾーンは、ローカルまたはUTC を指定できます。デフォルトのタイム ゾーンはUTC です。

MACsec キー チェーンを設定するには、**key chain** *name* **macsec** を使用します。

キーチェーン内に2番目のキーを設定し、最初のキーのライフタイムを設定することで、同じキーチェーン内の次のキーにロールオーバーできます。最初のキーのライフタイムが期限切れになると、リスト内の次のキーに自動的にロールオーバーします。同一のキーがリンクの両側で同時に設定されている場合、キーのロールオーバーはヒットレスになります。つまり、キーはトラフィックを中断せずにロールオーバーされます。

（注） キーのライフタイムは、ヒットレス キー ロールオーバーを実現するためにオーバーラップする必要があります。

プロトコル パケットの暗号化アルゴリズム

MKA 制御プロトコル パケット暗号化の暗号化アルゴリズムの選択は次のように行われます。

- MKA 制御プロトコル パケットを暗号化するための暗号化アルゴリズムは、キーチェーンの一部として設定されます。1 つのキー チェーンに設定できる暗号化アルゴリズムは 1 つだけです。
- キー サーバーは、使用されるキー チェーン内に設定された MKA 暗号化アルゴリズムを使用します。
- すべての非キー サーバーは、キー サーバーと同じ暗号化アルゴリズムを使用する必要があります。

MKA 暗号化アルゴリズムが設定されていない場合、デフォルトの暗号化アルゴリズムである AES-CMAC-128（128 ビット Advanced Encryption Standard を使用した暗号ベースのメッセージ認証コード）が使用されます。

データ パケットの暗号化アルゴリズム：

```
mka policy p1
macsec-cipher-suite [gcm-aes-128 | gcm-aes-256
```

MKA 制御パケットの暗号化アルゴリズム：

```
key chain <name> macsec
key 01
key-string <Hex string>
cryptographic-algorithm [aes-256-cmac  | aes-128-cmac]
```

非キー サーバーでリストにキー サーバーと同じ暗号スイートが設定されているか、デフォルト設定になっている場合、暗号スイートのロールオーバーをシームレスにするために、キー サーバー内のデータ パケット暗号スイートを変更することが推奨されます。

スムーズな移行のためのアクセス制御オプション

MACsec がインターフェイスで有効になっている場合、デフォルトでインターフェイス トラフィック全体がセキュリティ保護されます。MACsec は、暗号化されていないパケットを同じ物理インターフェイスから送受信することを許可しません。ただし、限定されたサブインターフェイスで MACsec を有効にするために、暗号化されていないパケットを同じ物理インターフェイスから送受信できるようにする追加のシスコ独自の拡張機能が実装されています。

暗号化されていないパケットの動作を制御するには、**macsec access-control** {**must-secure** | **should-secure**} コマンドを使用します。

- キーワード **should-secure** は、物理インターフェイスまたはサブインターフェイスからの暗号化されていないパケットの送受信を許可します。
- キーワード **must-secure** は、物理インターフェイスまたはサブインターフェイスからの暗号化されていないパケットの送受信を許可しません。このようなパケットは、MKA 制御プロトコル パケットを除きすべてドロップされます。
- 限定されたサブインターフェイスでのみMACsecが有効になっている場合は、対応するインターフェイスで **should-secure** キーワード オプションを設定します。

サブインターフェイスでの MACsec のデフォルト設定は、**macsec access-control must-secure** です。このオプションは、**macsec** コマンドがインターフェイスで設定されている場合、デフォルトで有効になっています。

（注） **macsec access-control should-secure** コマンドはインターフェイス レベルでのみ設定でき、サブインターフェイス レベルでは設定できません。このコマンドを設定すると、セキュリティ保護された MACsec セッションで暗号化されていないトラフィックが許可されます。

（注） 非 MACsec サブインターフェイスの場合は、トラフィックが通過できるように **should-secure** オプションを設定する必要があります。

Extensible Authentication Protocol over LAN 宛先アドレス

MACsec セキュア セッションを確立する前に、MKA（MACsec Key Agreement）が制御プロトコルとして使用されます。MKA は、暗号化に使用する暗号スイートを選択し、必要なキーとパラメータをピア間で交換します。

MKA は、MKA メッセージを送信するためのトランスポート プロトコルとして Authentication Protocol over LAN（EAPoL）を使用します。デフォルトでは、EAPoL は宛先マルチキャスト MAC アドレスとして 01:80: c2:00:00:03 を使用して、複数の宛先へパケットをマルチキャストします。EAPoL は標準ベースのプロトコルであり、IEEE 802.1 x などの他の認証メカニズムでも同じプロトコルが使用されます。サービス プロバイダー クラウド内のデバイスは、（宛先マルチキャスト MAC アドレスに基づいて）このパケットを消費し、EAPoL パケットの処理を試み、最終的にはパケットをドロップします。これにより、MKA セッションが失敗します。

インターフェイス上でサービス プロバイダーに送信される EAPoL パケットの宛先 MAC アドレスを変更するには、**eapol destination-address** コマンドを使用します。これにより、サービス プロバイダーは、パケットを消費せずに、他のデータ パケットと同様にトンネリングできます。

（注） EAPoL宛先アドレスは、物理レベルまたはサブインターフェイスレベルで、独立して設定できます。物理インターフェイスで設定する場合、設定はサブインターフェイスによって自動的に継承されます。サブインターフェイスでの明示的な設定は、そのサブインターフェイスで継承された値またはポリシーよりも優先されます。

リプレイ保護ウィンドウ サイズ

リプレイ保護は、リプレイ攻撃に対抗するためにMACsecにより提供される機能です。暗号化された各パケットには一意のシーケンス番号が割り当てられ、シーケンスはリモートエンドで確認されます。メトロ イーサネット サービス プロバイダー ネットワークを介して送信されるフレームは、順序が変更されることが多くあります。これは、ネットワーク内で使用されている優先順位付けとロードバランシング のメカニズムによるものです。

フレームの順序が変更されるプロバイダー ネットワーク上で MACsec の使用をサポートするには、リプレイ ウィンドウが必要です。ウィンドウ内のフレームは順不同で受信できますが、リプレイ保護されません。デフォルトのウィンドウ サイズは 64 に設定されています。リプレイ ウィンドウ サイズを変更するには、**macsec replay-protection window-size** コマンドを使用します。ウィンドウ サイズの範囲は 0 ～ 4294967295 です。

リプレイ保護ウィンドウは、ゼロに設定することで、厳格な受信順序とリプレイ保護を強制できます。

（注） リプレイ保護ウィンドウは、物理インターフェイスまたはサブインターフェイスで独立して設定できます。物理インターフェイスで設定する場合、設定はサブインターフェイスによって自動的に継承されます。サブインターフェイスでの明示的な設定は、そのサブインターフェイスで継承された値またはポリシーよりも優先されます。

WAN インターフェイス カード上の MACsec

Cisco IOS XE リリース 3.16Sでは、MACsec は Cisco 4000 シリーズ サービス統合型ルータ（ISR）上の WAN インターフェイス カード（NIM-2GE-CU-SFP および NIM-2GE-CU-SFP）に導入されています。

この WAN インターフェイス カードは、2 つの 1 ギガビット イーサネット ポートを持つ次世代 WAN インターフェイス カードです。

次世代 WAN インターフェイス カードは、次のプラットフォームでサポートされます。

- Cisco ISR 4451
- Cisco ISR4431
- Cisco ISR4351
- Cisco ISR 4331
- Cisco ISR 4321

OIR サポート

WANインターフェイスカードが動作中に挿入または取り外し（OIR）されると、そのインターフェイスに関連付けられている設定が保持されます。そのため、インターフェイスがシステムに再挿入された場合、同じ設定で動作します。ただし、Cisco ISR ルータ上の Cisco IOS XE リリース 3.16s では、MACsec および MKA セッションに次の制限が適用されます。

- 一部のスケーリング シナリオでは、OIR 後に MKA/MACsec セッションが失われる可能性があります。
- MKA/MACsec セッションは、OIR 後に再確立する必要があります。

Cisco 4000 シリーズ サービス統合型ルータでの MACsec のパフォーマンス

表 *139 : Cisco ISR 4451* ルータのパフォーマンス数値

フレーム サイズ	ポートごとの**NDR**（**pps**）	ライン レート（**%**）	モジュール **CPU**（**%**）	ホスト **CPU**（**%**）
64	1,077,532	72.41	44	65
128	692,568	82	29	42
256	405,797	89.6	17	25
iMIX	296,500	90.57	13	24
512	221,615	94.32	9	14
1024	116,163	97.02	5	7
1518	79,609	97.95	3.5』	5
9000	13,808	99.64%	1	2

Cisco ASR 1000 プラットフォーム上の MACsec のパフォーマンス

次の表に、Cisco IOS XE 16.6 リリース以降の Cisco ASR 1000 ルータのパフォーマンス数値を示します。

表 *140 : Cisco ASR1001-X* ルータのパフォーマンス数値

フレーム サイズ	集約レート ビット（**bps**）	ポートあたりのライン レート（**%**）	**ESP CPU**（**%**）
64	10064767891.17	65.59	93.33
iMIX	17763891467.40	93.14	26
1418	19311044388.60	97.89	9

表 *141 : Cisco ASR1001-HX* ルータのパフォーマンス数値

フレーム サイズ	集約レート ビット（**bps**）	ポートあたりのライン レート（**%**）	**ESP CPU**（**%**）
64	28681245486.53	65.59	99
iMIX	65019905182.40	93.14	42
1418	64975057119.60	97.89	11

表 *142 : Cisco ASR1002-HX* ルータのパフォーマンス数値

フレーム サイズ	集約レート ビット（bps）	ポートあたりのライン レート（%）	ESP CPU（%）
64	51467063849.50	65.59	96
iMIX	105267526427	93.14	36
1418	100007152449	97.89	10

ASR 1000 および ISR 4400 プラットフォームの MACsec 互換性マトリックス

プラットフォーム	内蔵ポート	EPA-18x1GE	EPA-10x10GE	EPA-1x40GE / EPA-2x40GE	NIM-2GE-CU-SFP
ASR1001-X	Cisco IOS XE Release 3.13.1S	該当なし	該当なし	該当なし	該当なし
ASR1001-HX	Cisco IOS XE Everest リリース 16.4.1	該当なし	該当なし	該当なし	該当なし
ASR1002-HX	Cisco IOS XE Denali リリース 16.3.1	Cisco IOS XE Denali リリース 16.3.1	Cisco IOS XE Denali リリース 16.3.2 / 16.4.1	Cisco IOS XE Fuji リリース 16.8.1	該当なし
ASR1006-X	該当なし	Cisco IOS XE Everest リリース 16.4.1	Cisco IOS XE Denali リリース 16.3.1	Cisco IOS XE Fuji リリース 16.8.1	該当なし
ASR1009-X	該当なし	Cisco IOS XE Everest リリース 16.4.1	Cisco IOS XE Denali リリース 16.3.1	Cisco IOS XE Fuji リリース 16.8.1	該当なし
ASR1013	該当なし	Cisco IOS XE Everest リリース 16.4.1	Cisco IOS XE Denali リリース 16.3.1	Cisco IOS XE Fuji リリース 16.8.1	該当なし
ISR44XX	該当なし	該当なし	該当なし	該当なし	Cisco IOS XE Release 3.16.0S
ISR43XX	該当なし	該当なし	該当なし	該当なし	Cisco IOS XE Release 3.16.0S
ISR4462	Cisco IOS XE Fuji リリース 16.9.1	該当なし	該当なし	該当なし	Cisco IOS XE Release 3.16.0S

（注）
- GLC-100FX はサポートされていません。
- MIP-100 は、ASR1006X、ASR1009X、ASR1013 プラットフォームで EPA18x1GE、EPA-10x10GE、EPA-1x40GE、および EPA-2x40GE に対応するために必要です。
- ASR1001-X 上の MACsec には IPsec ライセンスが必要です。
- ASR1001-HX、ASR1002-HX、および EPA 上の MACsec には、ポートごとに MACsec ライセンスが必要です。
- Cisco ISR 4000 プラットフォームでは、MACsec を設定するために HSECK9 ライセンスが必要です。

（注） IOS XE 17.2 Gibraltar 以降、ポートチャネル設定は MACsec でサポートされています。この機能を設定するには、リンクバンドルの各インターフェイスでMACsecを設定してください。詳細については、「設定例」を参照してください。

WAN MACsec および MKA のサポート機能強化の設定方法

MKA の設定

MACsec Key Agreement（MKA）は、キー管理パラメータの設定と制御を可能にします。MKA を設定するには、次のタスクを実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **mka policy** *policy-name*
4. **include-icv-indicator**
5. **key-server priority** *key-server-priority*
6. **macsec-cipher-suite** {**gcm-aes-128** | **gcm-aes-256** | **gcm-aes-xpn-128** | **gcm-aes-xpn-256**}
7. **sak-rekey interval** *interval*
8. **confidentiality-offset 30**
9. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**mka policy** *policy-name* 例： `Device(config)# mka policy MKAPolicy`	MKA ポリシーを設定します。
ステップ 4	**include-icv-indicator** 例： `Device(config-mka-policy)# include-icv-indicator`	（任意）MKPDU に ICV インジケータを含めます。
ステップ 5	**key-server priority** *key-server-priority* 例： `Device(config-mka-policy)# key-server priority 200`	（任意）MKA キー サーバの優先度を設定します。
ステップ 6	**macsec-cipher-suite** {**gcm-aes-128** | **gcm-aes-256** | **gcm-aes-xpn-128** | **gcm-aes-xpn-256**} 例： `Device(config-mka-policy)# macsec-cipher-suite gcm-aes-128 gcm-aes-256`	（任意）セキュア アソシエーション キー（SAK）導出のための暗号スイートを設定します。各暗号スイートの各オプションは 1 回だけ繰り返すことができますが、任意の順序で使用できます。
ステップ 7	**sak-rekey interval** *interval* 例： `Device(config-mka-policy)# sak-rekey interval 30`	（任意）SAK キー再生成間隔を秒単位で設定します。範囲は 30 ～ 65535 で、デフォルト値は 0 です。SAK キー再生成タイマーは、デフォルトでは設定されるまで開始されません。 • SAK キー再生成タイマーを停止するには、定義された MKA ポリシーの下で **no sak-rekey interval** コマンドを使用します。
ステップ 8	**confidentiality-offset 30** 例： `Device(config-mka-policy)# confidentiality-offset 30`	（任意）MACsec 操作の機密性オフセットを設定します。

	コマンドまたはアクション	目的
ステップ 9	**end** 例： `Device(config-mka-policy)# end`	特権 EXEC モードに戻ります。 （注） MKA ポリシーは、XPN 暗号の機密性オフセットを処理しません。したがって、XPN および非 XPN 暗号の両方が機密性オフセットとともに MKA ポリシーで設定されている場合、機密性オフセットは XPN 暗号では無視されます。そのため、XPN または非XPN 暗号を使用して MKA ポリシーを設定する際は、慎重に判断してください。

例

show mka policy コマンドを使用して設定を確認できます。次に、**show** コマンドの出力例を示します。MKPDU に icv-indicator を含めないようにするには、MKA ポリシーで **no include-icv-indicator**でコマンドを使用します。

```
MKA Policy Summary...

Codes : CO - Confidentiality Offset, ICVIND - Include ICV-Indicator,
        SAKR OLPL - SAK-Rekey On-Live-Peer-Loss,
        DP - Delay Protect, KS Prio - Key Server Priority

Policy            KS   DP    CO SAKR  ICVIND Cipher          Interfaces
Name              Prio          OLPL         Suite(s)        Applied
============================================================================
*DEFAULT POLICY*  0    FALSE 0  FALSE TRUE   GCM-AES-128     N/A
                                              GCM-AES-256

confid50          0    FALSE 50 FALSE TRUE   GCM-AES-128
                                              GCM-AES-256

icv               0    FALSE 0  FALSE TRUE   GCM-AES-128     Te3/0/9
                                              GCM-AES-256

k10               0    FALSE 0  FALSE TRUE   GCM-AES-128
                                              GCM-AES-256

xpn128            0    FALSE 0  FALSE TRUE   GCM-AES-XPN-128 Fo2/1/1
```

インターフェイスでの MACsec および MKA の設定

インターフェイスで MACsec と MKA を設定するには、次のタスクを実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **interface** *type number*

4. **mka policy** *policy-name*
5. **mka pre-shared-keykey-chain***key-chain-name*
6. **macsec**
7. **macsec replay-protection window-size**
8. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface** *type number* 例： `Device(config)# interface GigabitEthernet 0/0/0`	インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	**mka policy** *policy-name* 例： `Device(config-if)# mka policy MKAPolicy`	MKA ポリシーを設定します。
ステップ 5	**mka pre-shared-keykey-chain***key-chain-name* 例： `Device(config-if)# mka pre-shared-key key-chain key-chain-name`	MKA pre-shared-key key-chain に keychain1 を設定します。 （注） MKA 事前共有キーは、物理インターフェイスまたはサブインターフェイスのいずれかで設定できますが、物理インターフェイスとサブインターフェイスの両方で設定することはできません。
ステップ 6	**macsec** 例： `Device(config-if)# macsec`	EAPOL フレーム イーサネット タイプの MACsec を設定します。
ステップ 7	**macsec replay-protection window-size** 例： `Device(config-if)# macsec replay-protection window-size 10`	リプレイ保護の MACsec ウィンドウ サイズを設定します。

	コマンドまたはアクション	目的
ステップ 8	**end** 例： `Device(config-if)# end`	特権 EXEC モードに戻ります。

MKA 事前共有キーの設定

MACsec Key Agreement（MKA）事前共有キーを設定するには、次のタスクを実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **key chain** *key-chain-name* [**macsec**]
4. **key** *hex-string*
5. **cryptographic-algorithm** {**gcm-aes-128** | **gcm-aes-256**}
6. **key-string** {[**0** | **6**] *pwd-string* | **7** | *pwd-string*}
7. **lifetime local** {{*day month year* **duration** *seconds*}
8. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**key chain** *key-chain-name* [**macsec**] 例： `Device(config)# Key chain keychain1 macsec`	キー チェーンを設定して、キー チェーン コンフィギュレーション モードを開始します。
ステップ 4	**key** *hex-string* 例：	キーを設定して、キー チェーン コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
	`Device(config-keychain)# key 9ABCD`	（注） Cisco IOS XE Everest リリース 16.6.1 以降では、接続アソシエーション キー名（CKN）は、このキーの 16 進文字列として設定されている文字列とまったく同じ文字列を使用します。この動作の変更の詳細については、このタスクの後の「MKA-PSK：CKN 動作の変更」セクションを参照してください。
ステップ 5	**cryptographic-algorithm** {**gcm-aes-128** | **gcm-aes-256**} 例： `Device(config-keychain-key)# cryptographic-algorithm gcm-aes-128`	暗号化認証アルゴリズムを設定します。
ステップ 6	**key-string** {[**0** | **6**] *pwd-string* | **7** | *pwd-string*} 例： `Device(config-keychain-key)# key-string 0 pwd`	キー文字列のパスワードを設定します。
ステップ 7	**lifetime local** {{*day month year* **duration** *seconds*} 例： `Device(config-keychain-key)# lifetime local 16:00:00 Nov 9 2014 duration 6000`	キー文字列のライフタイムを設定します。 期間に指定できる範囲は、1 ～ 864000 秒です。
ステップ 8	**end** 例： `Device(config-keychain-key)# end`	特権 EXEC モードに戻ります。

接続アソシエーション キー（CAK）再生成の例

CAK のキー再生成は、次の場合に発生します。

- キー チェーン K1 内でキー 01 からキー 02 に移動する場合。
- あるキー チェーン K1 から別のキー チェーン K2 に移動する場合。

注：CAS キー再生成が正常に行われ、キー/CA 間のシームレスな移行（トラフィック損失やセッションの再起動を伴わない）が実現するように、各キーのライフタイム間にオーバーラップがあるようにキーを設定することを推奨します。

```
Device# show key chain k1
Key-chain k1:
    MacSEC key chain
    key 01 — text "c890433a1e05ef42d723a6b58af8fdbf7a25f42b3cda6a5eeb5ae4bf3a0a679f"
        lifetime (00:00:00 UTC Oct 29 2014) - (12:10:00 UTC Oct 29 2014)
```

```
    key 02 — text "14d9167d538819405c0ff78c655141ed4b3c7242562c0fb0f7a56f780bf29e52"
        lifetime (12:00:00 UTC Oct 29 2014) - (18:05:00 UTC Oct 29 2014)
    key 03 — text "88d971cb19d9f2598ad76edc562ade2e7e91e3ed70524f5c3c4d8d9599d0670e"
        lifetime (18:00:00 UTC Oct 29 2014) - (18:10:00 UTC Oct 29 2014)
    key 04 — text "75474bce819b49ad7e5bd06236bc0c944c69892f71e942e2f9812b7d3a7b2a5f"
        lifetime (18:10:00 UTC Oct 29 2014) - (infinite)

!In this case, Key 01, 02, 03 have overlapping time, but not key 04. Here is the sequence,
 how this works:
  @00:00:00 - A new MKA session is Secured with key 01
  @12:00:00 - CAK Rekey triggers with key 02 and upon success goes to Secured state
  @18:00:00 - CAK Rekey triggers with key 03 and upon success goes to Secured state
  @18:10:00 - Key 03 dies, hence MKA sesion using this key is brought down
  @18:10:00 - Key 04 becomes active and a new MKA session is triggered with this key.
Upon success, session will be Secured and UP for infinite time.
```

MKA-PSK：CKN 動作の変更

Cisco IOS XE Everest リリース 16.6.1 以降では、MKA-PSK セッションで、固定 32 バイトの代わりに、接続アソシエーション キー名（CKN）は、このキーの 16 進文字列として設定されている文字列とまったく同じ文字列を CKN として使用します。

設定例：

```
configure terminal
key chain abc macsec
  key 11
    cryptographic-algorithm aes-128-cmac
    key-string 12345678901234567890123456789013
    lifetime local 12:21:00 Sep 9 2015 infinite

 end
```

上記の例では、 **show mka session** コマンドの **show** コマンド出力は次のようになります。

```
Device# show mka session

           Total MKA Sessions....... 1
           Secured Sessions... 1
           Pending Sessions... 0

=============================================================================================

          Interface     Local-TxSCI        Policy-Name     Inherited        Key-Server

           Port-ID        Peer-RxSCI          MACsec-Peers     Status            CKN


=============================================================================================

           Et0/0          aabb.cc00.6600/0002     icv            NO                NO

           2              aabb.cc00.6500/0002 1               Secured          11
*Note that the CKN key-string is exactly the same that has been configured for the key
as hex-string.*
```

一方で CKN 動作が変更され、もう一方で CKN 動作が変更されていない 2 つのイメージ間の相互運用性の場合、キーの 16 進数文字列は 64 文字の 16 進数文字列である必要があります。こ

の文字列は、CKN 動作が変更されたイメージを持つデバイスで動作するようにゼロ パディングされている必要があります。次の例を参照してください。

Configuration without CKN key-string behavior change:

```
config t
  key chain abc macsec
   key 11
   cryptographic-algorithm aes-128-cmac
   key-string 12345678901234567890123456789013
   lifetime local 12:21:00 Sep 9 2015 infinite
```

Configuration with CKN key-string behavior change:

```
config t
  key chain abc macsec
   key 11000000000000000000000000000000000000000000000000000000000000000000
   cryptographic-algorithm aes-128-cmac
   key-string 12345678901234567890123456789013
   lifetime local 12:21:00 Sep 9 2015 infinite
```

EAPoL イーサネット タイプを変更するオプションの設定

-

手順の概要

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **eapol** *eth-type*
5. **exit**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface** *type number* 例： `Device(config)# interface GigabitEthernet 0/0/1`	インターフェイス コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 4	**eapol** *eth-type* 例： `Device(config-if)# eapol eth-type 0xB860`	インターフェイス上の EAPoL フレームのイーサネット タイプ（16 進数）を設定します。 （注） Cisco IOS リリース XE 3.17 以降では、**macsec eth-type** コマンドは **eapol eth-type** コマンドに置き換えられました。
ステップ 5	**exit** 例： `Device(config-if)# exit`	インターフェイス コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードに戻ります。

インターフェイスおよびサブインターフェイスでの宛先 MAC アドレスの設定

インターフェイスまたはサブインターフェイスで宛先 MAC アドレスを設定するには、次のタスクを実行します。宛先 MAC は、ピアの MAC またはマルチキャスト MAC アドレスにすることができます。**eapol destination-address** コマンドがメイン インターフェイスで設定されている場合は、そのインターフェイス上のすべてのサブインターフェイスに適用されます。ただし、 **eapol destination-address** コマンドがサブインターフェイスで設定されている場合は、メイン インターフェイスのコマンドよりも優先されます。

手順の概要

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **eapol destination-address** [*MAC-Address* | [**bridge-group-address** | **broadcast-address** | **lldp-multicast-address**]
5. **eapol destination-address bridge-group-address**
6. **eapol destination-address broadcast-address**
7. **eapol destination-address lldp-multicast-address**
8. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。

	コマンドまたはアクション	目的
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface** *type number* 例： `Device(config)# interface GigabitEthernet 0/0/1`	インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	**eapol destination-address** [*MAC-Address* | [**bridge-group-address** | **broadcast-address** | **lldp-multicast-address**] 例： `Device(config-if)# eapol destination-address 0018.b967.3cd0`	インターフェイス上の Extensible Authentication Protocol over LAN（EAPoL）宛先 MAC アドレスを設定します。
ステップ 5	**eapol destination-address bridge-group-address** 例： `Device(config-if)# eapol destination-address bridge-group-address`	宛先アドレスをブリッジ グループとして設定します。
ステップ 6	**eapol destination-address broadcast-address** 例： `Device(config-if)# eapol destination-address broadcast-address`	宛先 MAC アドレスをブロードキャスト アドレスとして設定します。
ステップ 7	**eapol destination-address lldp-multicast-address** 例： `Device(config-if)# eapol destination-address lldp-multicast-address`	宛先アドレスを LLDP マルチキャスト アドレスとして設定します。
ステップ 8	**end** 例： `DeviceDevice(config-if)# end`	特権 EXEC モードに戻ります。

WAN MACsec および MKA の設定例

例：EPL サービスを使用した CE から CE へのポイントツーポイント接続

次に、ポートベースのサービスを使用して、イーサネット プライベート回線（EPL）を使用したポイントツーポイントのカスタマーエッジからカスタマーエッジへの接続の設定例を示します。

```
!Customer Edge 1
key chain k1 macsec*
  key 01
  key-string 12345678901234567890123456789012
interface GigabitEthernet0/0/4
  ip address 10.3.1.1 255.255.255.0
  mka pre-shared-key key-chain k1*
  macsec*

!Customer Edge 2
key chain k1 macsec*
  key 01
  key-string 12345678901234567890123456789012
interface GigabitEthernet0/0/4
  ip address 10.3.1.2 255.255.255.0
  mka pre-shared-key key-chain k1*
  macsec*
```

例：EVPLサービスを使用したハブとスポークのポイントツーポイント接続

次に、VLANモードのイーサネット仮想プライベート回線（EVPL）サービスを使用した、ポイントツーポイントのハブ アンド スポーク接続の設定例を示します。

```
!CE 1
key chain k1 macsec*
 key 01
 key-string 12345678901234567890123456789012
interface GigabitEthernet0/0/4
  macsec dot1q-in-clear 1*
  macsec replay-protection-window-size 100
interface GigabitEthernet0/0/4.1
  encapsulation dot1Q 10
  ip address 10.3.1.1 255.255.255.0
  mka pre-shared-key key-chain k1*
  macsec*
interface GigabitEthernet0/0/4.2
  encapsulation dot1Q 20
  ip address 10.3.2.1 255.255.255.0
  mka pre-shared-key key-chain k1*
  macsec*
```

```
!CE 2
key chain k1 macsec*
  key 01
  key-string 12345678901234567890123456789012
interface GigabitEthernet0/0/4
  macsec dot1q-in-clear 1*
  macsec replay-protection-window-size 100
interface GigabitEthernet0/0/4.1
  encapsulation dot1Q 10
   ip address 10.3.1.1 255.255.255.0
  mka pre-shared-key key-chain k1*
  macsec*

!CE 3
key chain k1 macsec*
  key 01
  key-string 12345678901234567890123456789012
interface GigabitEthernet0/0/4
  macsec dot1q-in-clear 1*
  macsec replay-protection-window-size 100
interface GigabitEthernet0/0/4.1
  encapsulation dot1Q 10
  ip address 10.3.1.1 255.255.255.0
  mka pre-shared-key key-chain k1*
  macsec*
```

（注） アスタリスク（*）付きのコマンドは、すべて必須コマンドです。

例：MACsec および非 MACsec スポークを使用したポイントツーポイントのハブ アンド スポーク接続

次に、MACsec および非 MACsec スポークを使用したポイントツーポイントのハブアンドスポーク接続の出力例を示します。

```
!CE1
key chain k1 macsec*
  key 01
  key-string 12345678901234567890123456789012
interface GigabitEthernet0/0/4
  macsec dot1q-in-clear 1*
  macsec access-control should-secure*
interface GigabitEthernet0/0/4.1
  encapsulation dot1Q 10
  ip address 10.3.1.1 255.255.255.0
  mka pre-shared-key key-chain k1*
  macsec*
interface GigabitEthernet0/0/4.2
  encapsulation dot1Q 20
  ip address 10.3.2.1 255.255.255.0
  mka pre-shared-key key-chain k1*
  macsec*
interface GigabitEthernet0/0/4.3
  encapsulation dot1Q 30
  ip address 10.3.3.1 255.255.255.0

!CE2
```

```
key chain k1 macsec*
  key 01
  key-string 12345678901234567890123456789012
interface GigabitEthernet0/0/4
  macsec dot1q-in-clear 1*
  macsec access-control should-secure*
interface GigabitEthernet0/0/4.1
  encapsulation dot1Q 10
   ip address 10.3.1.2 255.255.255.0
  mka pre-shared-key key-chain k1*
  macsec*

!CE3
key chain k1 macsec*
  key 01
  key-string 12345678901234567890123456789012
interface GigabitEthernet0/0/4
  macsec dot1q-in-clear 1*
interface GigabitEthernet0/0/4.1
  encapsulation dot1Q 20
  ip address 10.3.2.2 255.255.255.0
  mka pre-shared-key key-chain k1*
  macsec*


!CE4
interface GigabitEthernet0/0/4.1
  encapsulation dot1Q 30
  ip address 10.3.3.2 255.255.255.0
```

例：EP-LANサービスを使用したハブとスポークのマルチポイントツーマルチポイント接続

次に、ポート モードのイーサネット プライベート回線（EP-LAN）サービスを使用した、マルチポイントツーマルチポイントのハブアンドスポーク接続の設定例を示します。

```
!CE 1
key chain k1 macsec*
  key 01
  key-string 12345678901234567890123456789012
  cryptographic-algorithm aes-128-cmac
mka policy p1
  macsec-cipher-suite gcm-aes-256
interface GigabitEthernet0/0/4
  ip address 10.3.1.1 255.255.255.0
  mka pre-shared-key key-chain k1*
  mka policy p1
  macsec*

!CE 2
key chain k1 macsec*
  key 01
  key-string 12345678901234567890123456789012
  cryptographic-algorithm aes-128-cmac
mka policy p1
  macsec-cipher-suite gcm-aes-256
interface GigabitEthernet0/0/4
  ip address 10.3.1.2 255.255.255.0
```

```
  mka pre-shared-key key-chain k1*
  mka policy p1
  macsec*

!CE 3
key chain k1 macsec*
  key 01
  key-string 123456789012345678901234567890123456
  cryptographic-algorithm aes-128-cmac
mka policy p1
  macsec-cipher-suite gcm-aes-256
interface GigabitEthernet0/0/4
  ip address 10.3.1.3 255.255.255.0
  mka pre-shared-key key-chain k1*
  mka policy p1
  macsec*
```

例：EVP-LAN サービスを使用したハブとスポークのマルチポイントツーマルチポイント接続

次に、VLANモードのイーサネット仮想プライベート回線（EVP-LAN）サービスを使用した、マルチポイントツーマルチポイントのハブアンドスポーク接続の設定例を示します。

```
!CE 1
key chain k1 macsec*
  key 01
  key-string 123456789012345678901234567890123456
interface GigabitEthernet0/0/4
  macsec dot1q-in-clear 1*
  macsec replay-protection-window-size 100
  eapol destination-address broadcast
interface GigabitEthernet0/0/4.1
  encapsulation dot1Q 10
  ip address 10.3.1.1 255.255.255.0
  mka pre-shared-key key-chain k1*
  macsec*

!CE 2
key chain k1 macsec*
  key 01
  key-string 123456789012345678901234567890123456
interface GigabitEthernet0/0/4
  macsec dot1q-in-clear 1*
  macsec replay-protection-window-size 100
  eapol destination-address broadcast
interface GigabitEthernet0/0/4.1
  encapsulation dot1Q 10
  ip address 10.3.1.2 255.255.255.0
  mka pre-shared-key key-chain k1*
  macsec*

!CE 3
key chain k1 macsec*
  key 01
  key-string 123456789012345678901234567890123456
interface GigabitEthernet0/0/4
  macsec dot1q-in-clear 1*
  macsec replay-protection-window-size 100
```

```
  eapol destination-address broadcast
interface GigabitEthernet0/0/4.1
  encapsulation dot1Q 10
  ip address 10.3.1.3 255.255.255.0
  mka pre-shared-key key-chain k1*
  macsec*
```

例：トラフィックに影響を与えずにメンテナンス タスクを実行する

次に、トラフィックに影響を与えないパフォーマンス メンテナンス タスクの設定例を示します。

事前共有キーの変更（CAK ロールオーバー）

次に、事前共有キーを変更するための設定例を示します。

（注） キーは、両方のルータでライフタイムを設定することで、次のキーに自動的にロールバックされるように設定できます。

```
!From
key chain k1 macsec*
  key 01
  key-string 12345678901234567890123456789012

!To
key chain k1 macsec*
  key 01
   key-string 12345678901234567890123456789012
   lifetime local 10:30:00 Oct 30 2014 11:30:00 Oct 30 2014
  key 02
   key-string 11145678901234567890123456789012
```

キー チェーンの変更（キー チェーン ロールオーバー）

キー チェーンを変更するための設定例を次に示します：キーチェーン ロールオーバー

```
! From
key chain k1 macsec*
  key 01
  key-string 12345678901234567890123456789012
interface TenGigabitEthernet0/0/0.10
 mka pre-shared-key key-chain k1

! To
key chain k1 macsec
  key 01
   key-string 12345678901234567890123456789012
key chain k2 macsec
  key 02
   key-string abcdef0987654321abcdef0987654321
interface TenGigabitEthernet0/0/0.10
 mka pre-shared-key key-chain k2
```

（注） 任意のキーチェーンの下に定義されたキーIDは、デバイス上の一意の値にする必要があります。

ルータは、同じセッションに参加する他のピア ルータよりも低いプライオリティを設定することによって、キーサーバーになることができます。確定的にキーサーバーに選択されるように、キーサーバーのプライオリティを設定します。たとえば、ハブ アンド スポーク シナリオでは、キーサーバーの最も理想的な場所はハブ サイトのルータです。

```
!Hub Site (Key Server):
mka policy p1
key-server priority 0
!0 is the default.

interface TenGigabitEthernet0/0/0.10
 mka pre-shared-key key-chain k1
mka policy p1

!Spoke Sites (non-Key Servers):
mka policy p1
key-server priority 1

interface TenGigabitEthernet0/0/0.10
 mka pre-shared-key key-chain k1
mka policy p1
```

次に、データ トラフィックを暗号化する暗号スイートを変更するための設定例を示します。

```
mka policy p1
 macsec-cipher-suite gcm-aes-128
interface GigabitEthernet0/0/1.10
 mka policy p1

!Alternate configuration

mka policy p1
 macsec-cipher-suite gcm-aes-256
interface GigabitEthernet0/0/1.10
 mka policy p1

key chain k3 macsec
 key 01
   key-string abcdef0987654321abcdef0987654321
   cryptographic-algorithm aes-128-cmac
interface TenGigabitEthernet0/0/0.10
 mka pre-shared-key key-chain k3

!Alternate configuration:

key chain k3 macsec
 key 01
   key-string abcdef0987654321abcdef0987654321
   cryptographic-algorithm aes-256-cmac
interface TenGigabitEthernet0/0/0.10
 mka pre-shared-key key-chain k3
```

EAPOL 宛先 MAC アドレスは、物理インターフェイス コンフィギュレーション モードまたはサブインターフェイス コンフィギュレーション モードから変更できます。物理インターフェイス レベルで設定されている場合は、サブインターフェイスによって自動的に継承されます。継承された値をオーバーライドするには、サブインターフェイス モードで MAC アドレスを設定します。デフォルトの EAPOL 宛先 MAC アドレスは 01:80: c2:00:00:03 です。

```
interface TenGigabitEthernet0/0/0
eapol destination-address <H.H.H>

!Alternate configuration

interface TenGigabitEthernet0/0/0
 bridge-group-address

!Alternate configuration

interface TenGigabitEthernet0/0/0
 lldp-multicast-address>
```

```
mka policy p1
 confidentiality-offset 30
interface GigabitEthernet0/0/1.10
 mka policy p1
```

例：メンテナンス タスクの実行（トラフィックに影響する）

リプレイ保護ウィンドウ サイズの変更

リプレイ保護ウィンドウは、物理インターフェイス コンフィギュレーション モードまたはサブインターフェイス コンフィギュレーション モードから変更できます。物理インターフェイス レベルで設定されている場合は、サブインターフェイスによって自動的に継承されます。継承された値をオーバーライドするには、サブインターフェイス モードで値を設定します。デフォルトのリプレイ保護ウィンドウ サイズは 64 です。

```
interface TenGigabitEthernet0/0/0
macsec replay-protection window-size 10

interface TenGigabitEthernet0/0/0.10
macsec replay-protection window-size 5
```

clear オプションでの VLAN（dot1q）タグの有効化または無効化

macsec dot1q-in-clear コマンドは物理インターフェイス上でのみ設定できます。この設定はサブインターフェイスによって自動的に継承されます。

```
interface GigabitEthernet0/0/1
macsec dot1q-in-clear 1
```

macsec access-control [**must-secure** | **should-secure**] コマンドは物理インターフェイス上でのみ設定できます。この設定はサブインターフェイスによって自動的に継承されます。

```
interface GigabitEthernet0/0/1
macsec access-control must-secure|should-secure
```

例：MACsec を使用したポートチャネルの設定

次に、リンクバンドルの2つの個別インターフェイスでMACsecを使用してポートチャネルを設定する設定例を示します。

（注） ポートチャネルの MACsec 設定を有効にしたり削除する前に、すべてのインターフェイスがシャットダウンされていることを確認してください。

```
key chain kc1 macsec
  key 01
  key-string 12345678901234567890123456789012
  cryptographic-algorithm aes-128-cmac

key chain kc2 macsec
  key 02
  key-string 12345678901234567890123456789013
  cryptographic-algorithm aes-128-cmac

mka policy policy1
  macsec-cipher-suite gcm-aes-256

!Port-Channel Configuration

 interface Port-channel2
  mtu 9216
  ip mtu 9184
  ip address 10.3.1.3 255.255.255.0
  load-interval 30
  bfd interval 750 min_rx 750 multiplier 5
  lacp min-bundle 2
  no shut
  exit

!Member link configuration 1

 interface TenGigabitEthernet0/1/1
  no shut
  mtu 9216
  no ip address
  ip mtu 9184
  load-interval 30
  cdp enable
  no cdp tlv app
  mka policy policy1
  mka pre-shared-key key-chain kc1
  macsec
  lacp rate fast
  channel-group 2 mode active

!Member link configuration 2

  interface TenGigabitEthernet0/1/2
  no shut
  mtu 9216
  no ip address
  ip mtu 9184
  load-interval 30
```

```
cdp enable
no cdp tlv app
mka policy policy1
mka pre-shared-key key-chain kc2
macsec
lacp rate fast
channel-group 2 mode active
```

その他の参考資料

関連資料

関連項目	マニュアル タイトル
セキュリティ コマンド	• 『Security Command Reference: Commands A to C』 • 『Security Command Reference: Commands D to L』 • 『Security Command Reference: Commands M to R』 • 『Security Command Reference: Commands S to Z』

標準および RFC

標準/RFC	タイトル
IEEE 802.1AE-2006	*Media Access Control*（*MAC*）セキュリティ
IEEE 802.1X-2010	ポート ベースのネットワーク アクセス コントロール
IEEE 802.1AEbw-2013	*Media Access Control*（*MAC*）セキュリティ（IEEE 802.1AE-2006 の修正）：Extended Packet Numbering（XPN）
IEEE 802.1Xbx-2014	ポートベースのネットワーク アクセス コントロール（IEEE 802.1 x-2010 の修正）
RFC 4493	*AES-CMAC* アルゴリズム

シスコのテクニカル サポート

説明	リンク
右の URL にアクセスして、シスコのテクニカル サポートを最大限に活用してください。これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

第 105 章

MACsec スマート ライセンス

MACsec スマートライセンスの概要

この章では、MACsec スマート ライセンスの概要を説明します。Smart Licensing クライアントの機能は、Cisco ソフトウェアを簡素化し、Cisco ソフトウェアがネットワーク全体でどのように使用されるかを理解するのに役立つ標準化されたライセンス プラットフォームです。Smart Licensing は、すべての Cisco ソフトウェア ライセンスの次世代プラットフォームです。MACsec ライセンスにより、Cisco ASR 1000 プラットフォームで CSL 永久ライセンスとスマート ライセンスを有効にすることが可能になります。

MACsec スマート ライセンスの機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *143 : MACsec* スマート ライセンスの機能情報

機能名	リリース	機能情報
MACsec および DLC のサポート	Cisco IOS XE Fuji 16.9.1	Smart Licensing クライアントの機能は、Cisco ソフトウェアを簡素化し、Cisco ソフトウェアがネットワーク全体でどのように使用されるかを理解するのに役立つ標準化されたライセンス プラットフォームです。Smart Licensing は、すべての Cisco ソフトウェア ライセンスの次世代プラットフォームです。この機能によって導入または変更されたコマンドはありません。

MACsec スマート ライセンスに関する情報

Cisco IOS XE Fuji リリース 16.9.1 では、MACsec スマート ライセンス（SL）は次のプラットフォームでサポートされています。

ポート	ライセンス機能	ライセンス PID	サポートされるプラットフォーム		
			MIP-100（RP2/RP3）	ASR1001-HX	ASR1002-HX
内蔵 1 GE ポート	MACSEC1G	FLSA1-MACSEC1G	該当なし	対応	対応
内蔵 10 GE ポート	MACSEC10G	FLSA1-MACSEC10G	該当なし	対応	対応
EPA-18X1GE	MACSEC1G	FLSA1-MACSEC1G	対応	該当なし	対応
EPA-10X10GE	MACSEC10G	FLSA1-MACSEC10G	対応	該当なし	対応
EPA-1X40GE	MACSEC40G	FLSA1-MACSEC40G	対応	該当なし	対応
EPA-2X40GE	MACSEC40G	FLSA1-MACSEC40G	対応	該当なし	対応
EPA-QSFP-1X100GE	MACSEC100G	FLSA1-MACSEC100G	対応	該当なし	対応

MACsec ライセンスはポートごとに提供され、物理ポートにのみ適用されます（サブインターフェイスには追加のライセンスは必要ありません）。MACsec ポート ライセンスでは、デバイス リード変換（DLC）のサポートが提供され、ペーパー ライセンスがスマート アカウントに確実に追加されます。

デバイス リード変換により、デバイス上のライセンスについてクラシック ライセンスからスマート ライセンスへのライセンス移行が自動的に実行されます。スマート ライセンスへの変換が自動的に行われるようにするには、デバイスを Cisco Smart Software Manager（SSM）に登録する必要があります。

（注）
- 以前のリリースに従って、ASR1001 内蔵は MACsec ライセンスとして機能する IPsec ライセンスで引き続き使用できます。
- MACsec ライセンスは EPA-1X100GE および EPA-CPAK-2X40GE ではサポートされていません。
- CSL：EvalRTU ライセンスは MACsec ライセンスでは使用できません。

MACsec の設定を含むポートが閉じられていない場合、または閉じられていないポートに設定が適用されている場合は、MACsec ライセンスの 1 つのユニットが使用されます。

MACsec の設定を含むポートが閉じられた場合、または閉じられていないポートから設定が削除された場合は、MACsec ライセンスの 1 つのユニットがリリースされます。

導入と移行の例

Cisco IOS XE Fuji 16.9.1 以降では、MACsec のサポートは Cisco ソフトウェア ライセンス（CSL）モードおよびスマート ライセンス（SL）モードで提供されます。ただし、16.9.1 より後のリリースでは、MACsec はスマート ライセンスのみをサポートします。

次のシナリオでは、既存のルータを Cisco IOS XE Fuji 16.9.1 に展開、および移行する方法について説明します。

永久ライセンスがインストールされている場合の CSL モードでのアップグレード

アップグレードする前（Cisco IOS XE Fuji 16.9.1 リリースより前のリリース）に MACsec 永久ライセンスがデバイスにインストールされている場合は、アップグレード後にこれらのライセンスが使用されます。

- アップグレードの前は、次の状態であることを前提としています。
  - ルータは、Cisco IOS XE Fuji 16.9.1 より前のリリースで動作している
  - MACsec は、4つの非シャットダウン1g インターフェイスで設定されます。
  - 4 つの MACSEC1G 永久ライセンスがインストールされている
- アップグレード後、4 つの MACSEC1G ライセンスが使用されます。

永久ライセンスがインストールされていない場合の CSL モードでのアップグレード

閉じられていないポートで MACsec が設定されている場合、アップグレード後に EvalRTU ライセンスを使用するのが理想的です。EvalRTU サポートが提供されないため、ライセンス要求はスキップされ、警告メッセージが表示されます。次に例を示します。

%IOSXE_LICENSE_POLICY_MANAGER-4-INSUF_PERM_LIC: 0/0/0: Insufficient MACSEC40G permanent license, skipping license request assuming customer has honour license

- アップグレードの前は、次の状態であることを前提としています。
  - ルータは、Cisco IOS XE Fuji 16.9.1 より前のリリースで動作している
  - MACsec は、4つの非シャットダウン1g インターフェイスで設定されます。
- アップグレード後
  - 使用できる MACsec ライセンスはありません
  - 警告メッセージが表示されます
  - その後、4 つの永久ライセンスを後でインストールすると、これらのライセンスは直ちに使用されます

SL モードへの移行

コンプライアンス違反シナリオを回避するには、すべての製品アクティベーションキー（PAK）および非 PAK ライセンスをお客様の仮想 CSSM アカウントに追加する必要があります。

デバイス リード変換（DLC）機能は、ライセンスをスマート アカウントに移行します。DLC が正常に動作するには、SL モードに移行する前に、すべてのライセンスを CSL モードで有効にする必要があります。

SL モードに移行するには、次の手順を実行します。

- Cisco IOS XE 16.9.1 より前のリリースから Cisco IOS XE 16.9.1 へのアップグレード
  1. CSL モードで Cisco IOS XE Fuji 16.9.1 へアップグレードします
  2. SL モードへ移行して DLC をトリガーします
- Cisco IOS XE Fuji 16.9.1 以前のリリースから以降のリリースへのアップグレード
  1. CSL モードで Cisco IOS XE Fuji 16.9.1 へアップグレードします
  2. SL モードへ移行して DLC をトリガーします
  3. Cisco IOS XE Fuji 16.9.1 より後のリリースへアップグレードします

第 106 章

証明書ベースの MACsec 暗号化

証明書ベースの MACsec 暗号化機能は、Extensible Authentication Protocol – Transport Layer Security（EAP-TLS）による802.1X ポートベース認証を使用して、MACsec 暗号化が必要なルータ ポートの証明書を伝送します。EAP-TLS メカニズムを使用して相互認証を実行し、プライマリセッションキーを取得します。このキーから、MACsec Key Agreement（MKA）プロトコル用の接続アソシエーションキー（CAK）が導出されます。

証明書ベースの MACsec 暗号化は、リモート認証またはローカル認証のいずれかを使用して実行されます。

証明書ベース MACsec 暗号化の機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *144 :* 証明書ベース *MACsec* 暗号化の機能情報

機能名	リリース	機能情報
証明書ベースの MACsec 暗号化	Cisco IOS XE Everest リリース 16.6.1	証明書ベースの MACsec 暗号化機能は、MACsec 暗号化が必要なルータポートの証明書を伝送するために、拡張認証プロトコルを使用した 802.1 x ポートベースの認証を使用します。 Transport Layer Security (eap-tls) を使用します。EAP-TLS メカニズムを使用して相互認証を実行し、プライマリセッションキーを取得します。このキーから、MACsec Key Agreement（MKA）プロトコル用の接続アソシエーションキー（CAK）が導出されます。

証明書ベース MACsec 暗号化の前提条件

- 認証局（CA）サーバーがネットワークに設定されていることを確認します。
- CA 証明書を生成します。
- Cisco Identity Services Engine（ISE）リリース 2.0 が設定されていることを確認します。『*Cisco Identity Services Engine* リリース *2.3* 管理者ガイド』を参照してください。
- 両方の参加デバイス（CA サーバーと Cisco Identity Services Engine（ISE））が Network Time Protocol（NTP）を使用して同期されていることを確認します。時間がすべてのデバイスで同期されていないと、証明書は検証されません。
- 802.1x 認証と AAA がデバイスに設定されていることを確認します。

証明書ベース MACsec 暗号化の制約事項

- MKA は、ポート チャネルではサポートされていません。
- MKA のハイ アベイラビリティはサポートされません。
- サブインターフェイスでの証明書ベースの MACsec 暗号化はサポートされていません。

証明書ベース MACsec 暗号化に関する情報

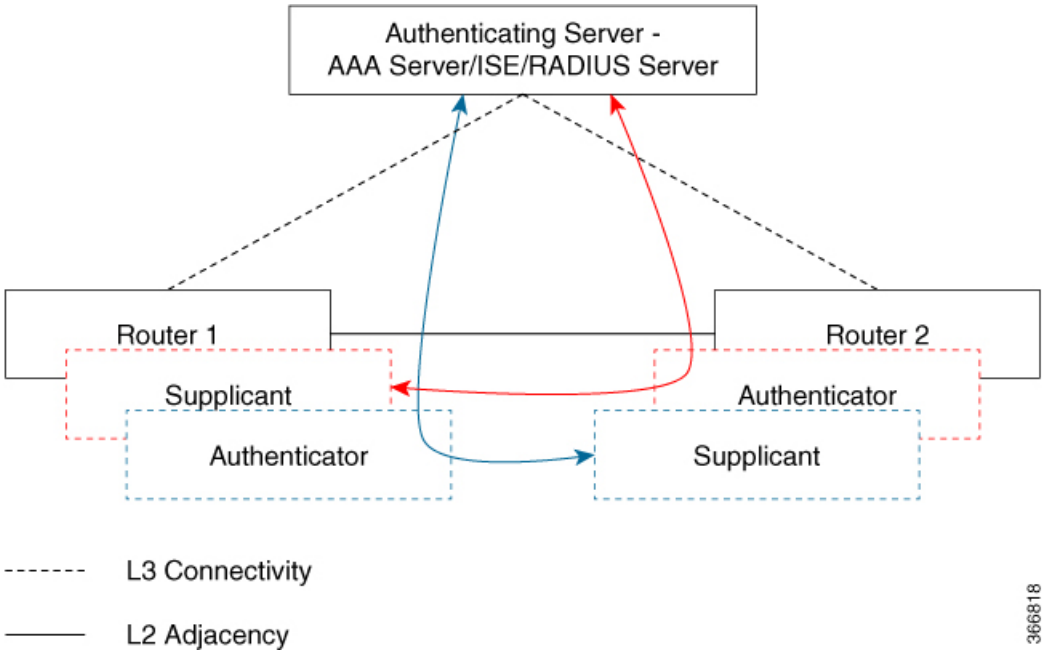
MKA MACsec は、ルータ間のリンクでサポートされています。Extensible Authentication Protocol（EAP-TLS）による IEE 802.1X ポートベース認証を使用して、デバイスのポート間の MKA MACsec を設定できます。EAP-TLS は相互認証を許可し、プライマリセッションキーを取得します。そのキーから、MKA プロトコル用の接続アソシエーションキー（CAK）が取得されます。デバイスの証明書は、AAA サーバーへの認証用に、EAP-TLS を使用して伝送されます。

リモート認証を使用した証明書ベース MACsec 暗号化のコール フロー

サプリカントは、ネットワークへアクセスしようとする未承認デバイスです。オーセンティケータは、サプリカントの認証ステータスに基づいて、ネットワークへの物理アクセスを制御するデバイスです。

次の図に示すように、デバイスは直接接続されています。ルータは、ポート上で EAP サプリカントとオーセンティケータの両方として機能します。

次の図は、ルータ上の 2 つの EAP コール フロー（個別の EAP セッション ID を持つ）を示しています。赤色のフローは、ルータ 1 をサプリカントとして、ルータ 2 をオーセンティケータとして示しています。青のフローはその逆を示しています。



インターフェイスが 802.1 x の両方のロールとして設定されている場合、ルータの認証マネージャは、サプリカントとオーセンティケータのロールを使用して 2 つの EAP セッション（個別の EAP セッション ID を持つ青色と赤色のセッション）フローを持つセッションを作成し、両方のロールがリモート認証サーバー（AAA サーバー/ISE/RADIUS）を使用した EAP-TLS 相互認証をトリガします。

相互認証後、認証サーバーとしてより大きいMACアドレスを持ち、オーセンティケータ ロールを持つルータに対応するフローの MSK が選択されて CAK を導出します。

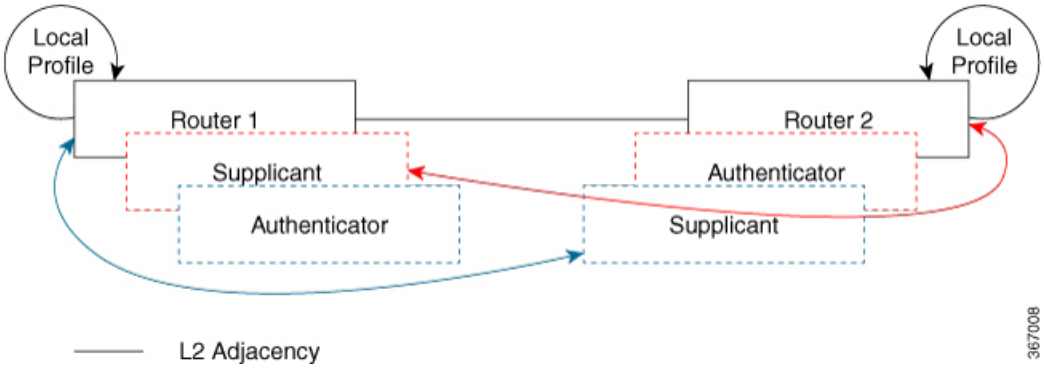
上の図では、ルータ 1 の MAC アドレスがルータ 2 より小さい場合、EAP セッション（青色のフロー）から取得したプライマリセッションキー（PSK）がMKAのEAP-PSKとして使用されます（ルータ 1 はオーセンティケータとして、ルータ 2 はサプリカントとして機能します）。これにより、ルータ1がMKA キーサーバーとして機能し、ルータ2が非キーサーバーとして機能することが保証されます。

ルータ 2 の MAC アドレスがルータ 1 の MAC アドレスよりも小さい場合は、EAP セッションから取得された PSK（赤色のフロー）が（両方のルータにより）MKA の EAP-PSK として使用され、CAK が導出されます。

ローカル認証を使用した証明書ベース MACsec 暗号化のコール フロー

次の図に示すように、デバイスは直接接続されています。ルータは、ポート上で EAP サプリカントとオーセンティケータの両方として機能します。

次の図は、ルータ上の 2 つの EAP コール フロー（個別の EAP セッション ID を持つ）を示しています。赤色のフローは、ルータ 1 をサプリカントとして、ルータ 2 をオーセンティケータとして示しています。青のフローはその逆を示しています。



インターフェイスが 802.1 x の両方のロールとして設定されている場合、ルータの認証マネージャは、サプリカントとオーセンティケータのロールを使用して 2 つの EAP セッション（個別の EAP セッション ID を持つ青色と赤色のセッション）フローを持つセッションを作成し、両方のロールがローカル認証サーバーを使用した EAP-TLS 相互認証をトリガします。

相互認証後、認証サーバーとしてより大きい MAC アドレスを持ち、オーセンティケーターロールを持つルータに対応するフローの PSK が選択されて CAK を導出します。

上の図では、ルータ 1 の MAC アドレスがルータ 2 より小さい場合、EAP セッション（青色のフロー）から取得したプライマリセッションキー（PSK）が MKA の EAP-PSK として使用されます（ルータ 1 はオーセンティケータとして、ルータ 2 はサプリカントとして機能します）。これにより、ルータ1が MKA キーサーバーとして機能し、ルータ2が非キーサーバーとして機能することが保証されます。

ルータ 2 の MAC アドレスがルータ 1 の MAC アドレスよりも小さい場合は、EAP セッションから取得された PSK（赤色のフロー）が（両方のルータにより）MKA の EAP-PSK として使用され、CAK が導出されます。

リモート認証を使用した証明書ベース MACsec 暗号化の設定

ポイントツーポイント リンクで MKA による MACsec を設定するには、次のタスクを実行します。

証明書登録の設定

キー ペアの生成

手順

	コマンドまたはアクション	目的
ステップ 1	**enable**	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**crypto key generate rsa label** *label name* **general-keys modulus** *size*	署名および暗号化用に RSA キーペアを作成します。 label キーワードを使用すると、各キーペアにラベルを割り当てることもできます。このラベルは、キーペアを使用するトラストポイントによって参照されます。ラベルを割り当てなかった場合、キーペアには <Default-RSA-Key> というラベルが自動的に付けられます。 追加のキーワードを使用しない場合、このコマンドは汎用 RSA キー ペアを 1 つ生成します。係数が指定されていない場合は、デフォルトのキー係数である 1024 が使用されます。その他の係数サイズを指定するには、modulus キーワードを使用します。
ステップ 4	**end**	特権 EXEC モードに戻ります。
ステップ 5	**show authentication session interface** *interface-id*	許可されたセッションのセキュリティ ステータスを確認します。
ステップ 6	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

SCEP による登録の設定

Simple Certificate Enrollment Protocol（SCEP）は、HTTP を使用して認証局（CA）または登録局（RA）と通信する、シスコが開発した登録プロトコルです。SCEP は、要求および証明書の送受信用に最も一般的に使用される方式です。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable**	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**crypto pki trustpoint** *server name*	トラストポイントおよび設定された名前を宣言して、CA トラストポイント コンフィギュレーション モードを開始します。
ステップ 4	**enrollment url** *url name pem*	デバイスが証明書要求を送信する CA の URL を指定します。 URL 内の IPv6 アドレスは括弧で囲む必要があります。たとえば、http:// [2001:DB8:1:1::1]:80 です。 pem キーワードは、証明書要求に Privacy Enhanced Mail（PEM）の境界を追加します。
ステップ 5	**rsakeypair** *label*	証明書に関連付けるキー ペアを指定します。 （注） **rsakeypair** 名は、信頼ポイント名と一致している必要があります。
ステップ 6	**serial-number none**	**none** キーワードは、証明書要求にシリアル番号が含まれないことを指定します。
ステップ 7	**ip-address none**	**none** キーワードは、証明書要求に IP アドレスが含まれないことを指定します。
ステップ 8	**revocation-check crl**	ピアの証明書が取り消されていないことを確認する方法として CRL を指定します。
ステップ 9	**auto-enroll** *percent* **regenerate**	自動登録をイネーブルにします。これにより、クライアントは CA から自動的にロールオーバー証明書を要求できます。

	コマンドまたはアクション	目的
		自動登録がイネーブルでない場合、証明書の失効時にクライアントを手動で PKI に再登録する必要があります。 デフォルトでは、デバイスのドメイン ネーム システム（DNS）名だけが証明書に含められます。 現行の証明書の有効期間が指定のパーセンテージに達したときに、新しい証明書が要求されるように指定するには、percent 引数を使用します。 名前付きのキーがすでに存在する場合でも、証明書の新しいキーを生成するには、regenerate キーワードを使用します。 ロールオーバー中のキー ペアがエクスポート可能な場合、新しいキーペアもエクスポート可能です。次のコメントがトラストポイントコンフィギュレーションに表示され、キー ペアがエクスポート可能かどうかが示されます。「! RSA key pair associated with trustpoint is exportable.」 新しいキー ペアは、セキュリティ上の問題に対処するために生成することを推奨します。
ステップ 10	**crypto pki authenticate** *name*	CA 証明書を取得して、認証します。
ステップ 11	**exit**	グローバル コンフィギュレーション モードを終了します。
ステップ 12	**show crypto pki certificate** *trustpoint name*	信頼ポイントの証明書に関する情報を表示します。

登録の手動設定

CA が SCEP をサポートしない場合、またはルータと CA 間のネットワーク接続が不可能な場合。手動での証明書登録を設定するには、次の作業を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable**	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal**	グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 3	**crypto pki trustpoint** *server name*	トラストポイントおよび設定された名前を宣言して、CA トラストポイント コンフィギュレーション モードを開始します。
ステップ 4	**enrollment url** *url name pem*	デバイスが証明書要求を送信する CA の URL を指定します。 URL 内の IPv6 アドレスは括弧で囲む必要があります。たとえば、http:// [2001:DB8:1:1::1]:80 です。 pem キーワードは、証明書要求に Privacy Enhanced Mail（PEM）の境界を追加します。
ステップ 5	**rsakeypair** *label*	証明書に関連付けるキー ペアを指定します。
ステップ 6	**serial-number none**	**none** キーワードは、証明書要求にシリアル番号が含まれないことを指定します。
ステップ 7	**ip-address none**	**none** キーワードは、証明書要求に IP アドレスが含まれないことを指定します。
ステップ 8	**revocation-check crl**	ピアの証明書が取り消されていないことを確認する方法として CRL を指定します。
ステップ 9	**exit**	グローバル コンフィギュレーション モードから抜けます。
ステップ 10	**crypto pki authenticate** *name*	CA 証明書を取得して、認証します。
ステップ 11	**crypto pki enroll** *name*	証明書要求を生成し、証明書サーバーにコピーおよびペーストするために要求を表示します。 プロンプトが表示されたら、登録情報を入力します。たとえば、証明書要求にデバイスの FQDN および IP アドレスを含めるかどうかを指定します。 コンソール端末に対して証明書要求を表示するかについても選択できます。 必要に応じて、Base 64 符号化証明書を PEM ヘッダーを付けて、または付けずに表示します。
ステップ 12	**crypto pki import** *name* **certificate**	許可された証明書を取得するコンソール端末で、TFTP によって証明書をインポートします。 デバイスは、拡張子が「.req」から「.crt」に変更されたことを除いて、要求の送信に使用した同じファイル名を使用して、許可された証明書を TFTP によって取得しようと試みます。用途キー証明書の場

	コマンドまたはアクション	目的
		合、拡張子「-sign.crt」および「-encr.crt」が使用されます。 デバイスは、受信したファイルを解析して証明書を検証し、証明書をスイッチの内部証明書データベースに挿入します。 （注） 一部の CA は、証明書要求の用途キー情報を無視し、汎用目的の証明書を発行します。ご使用の CA が証明書要求の用途キー情報を無視する場合は、汎用目的の証明書だけをインポートしてください。ルータは、生成される 2 つのキー ペアのいずれも使用しません。
ステップ 13	**exit**	グローバル コンフィギュレーション モードから抜けます。
ステップ 14	**show crypto pki certificate** *trustpoint name*	信頼ポイントの証明書に関する情報を表示します。
ステップ 15	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

802.1x 認証の有効化と AAA の設定

手順

	コマンドまたはアクション	目的
ステップ 1	**enable**	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**aaa new-model**	AAA をイネーブルにします。
ステップ 4	**dot1x system-auth-control**	デバイス上で 802.1X を有効にします。
ステップ 5	**radius server** *name*	RADIUS サーバの設定の名前を Protected Access Credential（PAC）のプロビジョニング用に指定し、RADIUS サーバ設定モードを開始します。
ステップ 6	**address** *ip-address* **auth-port** *port-number* **acct-port** *port-number*	RADIUSサーバーのアカウンティングおよび認証パラメータの IPv4 アドレスを設定します。

	コマンドまたはアクション	目的
ステップ 7	**automate-tester username** *username*	RADIUS サーバーの自動テスト機能を有効にします。 このようにすると、デバイスは RADIUS サーバーにテスト認証メッセージを定期的に送信し、サーバーからの RADIUS 応答を待機します。成功メッセージは必須ではありません。認証失敗であっても、サーバーが稼働していることを示しているため問題ありません。
ステップ 8	**key** *string*	デバイスと RADIUS サーバーとの間におけるすべての RADIUS 通信用の認証および暗号キーを指定します。
ステップ 9	**radius-server deadtime** *minutes*	いくつかのサーバーが使用不能になったときの RADIUS サーバーの応答時間を短くし、使用不能になったサーバーがすぐにスキップされるようにします。
ステップ 10	**exit**	グローバル コンフィギュレーション モードに戻ります。
ステップ 11	**aaa group server radius** *group-name*	異なる RADIUS サーバー ホストを別々のリストと方式にグループ化し、サーバー グループ コンフィギュレーション モードを開始します。
ステップ 12	**server** *name*	RADIUS サーバー名を割り当てます。
ステップ 13	**exit**	グローバル コンフィギュレーション モードに戻ります。
ステップ 14	**aaa authentication dot1x default group** *group-name*	IEEE 802.1x 用にデフォルトの認証サーバー グループを設定します。
ステップ 15	**aaa authorization network default group** *group-name*	ネットワーク認証のデフォルト グループを設定します。

EAP-TLS プロファイルと 802.1x クレデンシャルの設定

手順

	コマンドまたはアクション	目的
ステップ 1	**enable**	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。

	コマンドまたはアクション	目的
ステップ 2	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**eap profile** *profile-name*	EAP プロファイルを設定し、EAP プロファイル コンフィギュレーション モードを開始します。
ステップ 4	**method tls**	デバイスで EAP-TLS 方式を有効にします。
ステップ 5	**pki-trustpoint** *name*	デフォルトの PKI トラストポイントを設定します。
ステップ 6	**exit**	グローバル コンフィギュレーション モードに戻ります。
ステップ 7	**dot1x credentials** *profile-name*	802.1x クレデンシャルプロファイルを設定し、dot1x クレデンシャル コンフィギュレーション モードを開始します。
ステップ 8	**username** *username*	認証ユーザー ID を設定します。
ステップ 9	**pki-trustpoint** *name*	デフォルトの PKI トラストポイントを設定します。
ステップ 10	**end**	特権 EXEC モードに戻ります。

インターフェイスでの 802.1x MKA MACsec 設定の適用

EAP-TLS を使用して MKA MACsec をインターフェイスに適用するには、次のタスクを実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable**	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface** *interface-id*	MACsec インターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。インターフェイスは物理インターフェイスでなければなりません。
ステップ 4	**macsec**	インターフェイス上で MACsec をイネーブルにします。

	コマンドまたはアクション	目的
ステップ 5	**authentication periodic**	このポートの再認証をイネーブルにします。
ステップ 6	**authentication timer reauthenticate interval**	再認証間隔を設定します。
ステップ 7	**access-session host-mode multi-domain**	ホストにインターフェイスへのアクセスを許可します。
ステップ 8	**access-session closed**	インターフェイスへの事前認証アクセスを防止します。
ステップ 9	**access-session port-control auto**	ポートの認可状態を設定します。
ステップ 10	**dot1x pae both**	ポートを 802.1X ポート アクセス エンティティ（PAE）のサプリカントおよびオーセンティケータとして設定します。
ステップ 11	**dot1x credentials profile**	802.1x クレデンシャルプロファイルをインターフェイスに割り当てます。
ステップ 12	**dot1x supplicant eap profile** *name*	EAP-TLS プロファイルをインターフェイスに割り当てます。
ステップ 13	**service-policy type control subscriber** *control-policy name*	インターフェイスに加入者制御ポリシーを適用します。
ステップ 14	**exit**	特権 EXEC モードに戻ります。
ステップ 15	**show macsec interface**	インターフェイスの MACsec の詳細を表示します。
ステップ 16	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

ローカル認証を使用した証明書ベース MACsec 暗号化の設定

ポイントツーポイント リンクで MKA による MACsec を設定するには、次のタスクを実行します。

ローカル認証を使用した EAP クレデンシャルの設定

手順

	コマンドまたはアクション	目的
ステップ 1	**enable**	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**aaa new-model**	AAA をイネーブルにします。
ステップ 4	**aaa local authentication default authorization default**	デフォルトのローカル認証およびデフォルトのローカル認証方法を設定します。
ステップ 5	**aaa authentication dot1x default local**	IEEE 802.1x 用にデフォルトのローカル ユーザー名認証リストを設定します。
ステップ 6	**aaa authorization network default local**	ローカルユーザーの認可方式リストを設定します。
ステップ 7	**aaa authorization credential-download default local**	ローカルクレデンシャルの使用に関する認可方式リストを設定します。
ステップ 8	**exit**	特権 EXEC モードに戻ります。

ローカル EAP-TLS 認証と認証プロファイルの設定

手順

	コマンドまたはアクション	目的
ステップ 1	**enable**	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**aaa new-model**	AAA をイネーブルにします。
ステップ 4	**dot1x credentials** *profile-name*	dot1x クレデンシャルプロファイルを設定し、dot1x クレデンシャル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 5	**username** *name* **password** *password*	認証のユーザー ID およびパスワードを設定します。
ステップ 6	**exit**	グローバル コンフィギュレーション モードに戻ります。
ステップ 7	**aaa attribute list** *list-name*	（任意）AAA 属性リスト定義を設定し、属性リスト コンフィギュレーション モードを開始します。
ステップ 8	**aaa attribute type linksec-policy must-secure**	（任意）AAA 属性タイプを指定します。
ステップ 9	**exit**	グローバル コンフィギュレーション モードに戻ります。
ステップ 10	**username** *name* **aaa attribute list** *name*	（任意）ユーザー ID に AAA 属性リストを指定します。
ステップ 11	**end**	特権 EXEC モードに戻ります。

SCEP による登録の設定

Simple Certificate Enrollment Protocol（SCEP）は、HTTP を使用して認証局（CA）または登録局（RA）と通信する、シスコが開発した登録プロトコルです。SCEP は、要求および証明書の送受信用に最も一般的に使用される方式です。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable**	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**crypto pki trustpoint** *server name*	トラストポイントおよび設定された名前を宣言して、CA トラストポイント コンフィギュレーション モードを開始します。
ステップ 4	**enrollment url** *url name pem*	デバイスが証明書要求を送信する CA の URL を指定します。 URL 内の IPv6 アドレスは括弧で囲む必要があります。たとえば、http:// [2001:DB8:1:1::1]:80 です。

	コマンドまたはアクション	目的
		pem キーワードは、証明書要求に Privacy Enhanced Mail（PEM）の境界を追加します。
ステップ 5	**rsakeypair** *label*	証明書に関連付けるキー ペアを指定します。 （注） **rsakeypair** 名は、信頼ポイント名と一致している必要があります。
ステップ 6	**serial-number none**	**none** キーワードは、証明書要求にシリアル番号が含まれないことを指定します。
ステップ 7	**ip-address none**	**none** キーワードは、証明書要求に IP アドレスが含まれないことを指定します。
ステップ 8	**revocation-check crl**	ピアの証明書が取り消されていないことを確認する方法として CRL を指定します。
ステップ 9	**auto-enroll** *percent* **regenerate**	自動登録をイネーブルにします。これにより、クライアントはCAから自動的にロールオーバー証明書を要求できます。 自動登録がイネーブルでない場合、証明書の失効時にクライアントを手動で PKI に再登録する必要があります。 デフォルトでは、デバイスのドメイン ネーム システム（DNS）名だけが証明書に含められます。 現行の証明書の有効期間が指定のパーセンテージに達したときに、新しい証明書が要求されるように指定するには、percent 引数を使用します。 名前付きのキーがすでに存在する場合でも、証明書の新しいキーを生成するには、regenerate キーワードを使用します。 ロールオーバー中のキー ペアがエクスポート可能な場合、新しいキーペアもエクスポート可能です。次のコメントがトラストポイントコンフィギュレーションに表示され、キー ペアがエクスポート可能かどうかが示されます。「! RSA key pair associated with trustpoint is exportable.」 新しいキー ペアは、セキュリティ上の問題に対処するために生成することを推奨します。
ステップ 10	**crypto pki authenticate** *name*	CA 証明書を取得して、認証します。

	コマンドまたはアクション	目的
ステップ 11	**exit**	グローバル コンフィギュレーション モードを終了します。
ステップ 12	**show crypto pki certificate** *trustpoint name*	信頼ポイントの証明書に関する情報を表示します。

登録の手動設定

CA が SCEP をサポートしない場合、またはルータと CA 間のネットワーク接続が不可能な場合。手動での証明書登録を設定するには、次の作業を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable**	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**crypto pki trustpoint** *server name*	トラストポイントおよび設定された名前を宣言して、CA トラストポイント コンフィギュレーション モードを開始します。
ステップ 4	**enrollment url** *url name pem*	デバイスが証明書要求を送信する CA の URL を指定します。 URL 内の IPv6 アドレスは括弧で囲む必要があります。たとえば、http:// [2001:DB8:1:1::1]:80 です。 pem キーワードは、証明書要求に Privacy Enhanced Mail（PEM）の境界を追加します。
ステップ 5	**rsakeypair** *label*	証明書に関連付けるキー ペアを指定します。
ステップ 6	**serial-number none**	**none** キーワードは、証明書要求にシリアル番号が含まれないことを指定します。
ステップ 7	**ip-address none**	**none** キーワードは、証明書要求に IP アドレスが含まれないことを指定します。
ステップ 8	**revocation-check crl**	ピアの証明書が取り消されていないことを確認する方法として CRL を指定します。
ステップ 9	**exit**	グローバル コンフィギュレーション モードから抜けます。

	コマンドまたはアクション	目的
ステップ 10	**crypto pki authenticate** *name*	CA 証明書を取得して、認証します。
ステップ 11	**crypto pki enroll** *name*	証明書要求を生成し、証明書サーバーにコピーおよびペーストするために要求を表示します。 プロンプトが表示されたら、登録情報を入力します。たとえば、証明書要求にデバイスの FQDN および IP アドレスを含めるかどうかを指定します。 コンソール端末に対して証明書要求を表示するかについても選択できます。 必要に応じて、Base 64 符号化証明書を PEM ヘッダーを付けて、または付けずに表示します。
ステップ 12	**crypto pki import** *name* **certificate**	許可された証明書を取得するコンソール端末で、TFTP によって証明書をインポートします。 デバイスは、拡張子が「.req」から「.crt」に変更されたことを除いて、要求の送信に使用した同じファイル名を使用して、許可された証明書を TFTP によって取得しようと試みます。用途キー証明書の場合、拡張子「-sign.crt」および「-encr.crt」が使用されます。 デバイスは、受信したファイルを解析して証明書を検証し、証明書をスイッチの内部証明書データベースに挿入します。 （注） 一部の CA は、証明書要求の用途キー情報を無視し、汎用目的の証明書を発行します。ご使用の CA が証明書要求の用途キー情報を無視する場合は、汎用目的の証明書だけをインポートしてください。ルータは、生成される 2 つのキー ペアのいずれも使用しません。
ステップ 13	**exit**	グローバル コンフィギュレーション モードから抜けます。
ステップ 14	**show crypto pki certificate** *trustpoint name*	信頼ポイントの証明書に関する情報を表示します。
ステップ 15	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

EAP-TLS プロファイルと 802.1x クレデンシャルの設定

手順

	コマンドまたはアクション	目的
ステップ 1	**enable**	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**eap profile** *profile-name*	EAP プロファイルを設定し、EAP プロファイル コンフィギュレーション モードを開始します。
ステップ 4	**method tls**	デバイスで EAP-TLS 方式を有効にします。
ステップ 5	**pki-trustpoint** *name*	デフォルトの PKI トラストポイントを設定します。
ステップ 6	**exit**	グローバル コンフィギュレーション モードに戻ります。
ステップ 7	**dot1x credentials** *profile-name*	802.1x クレデンシャル プロファイルを設定し、dot1x クレデンシャル コンフィギュレーション モードを開始します。
ステップ 8	**username** *username*	認証ユーザー ID を設定します。
ステップ 9	**pki-trustpoint** *name*	デフォルトの PKI トラストポイントを設定します。
ステップ 10	**end**	特権 EXEC モードに戻ります。

インターフェイスでの 802.1x MKA MACsec 設定の適用

EAP-TLS を使用して MKA MACsec をインターフェイスに適用するには、次のタスクを実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable**	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal**	グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 3	**interface** *interface-id*	MACsecインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。インターフェイスは物理インターフェイスでなければなりません。
ステップ 4	**macsec**	インターフェイス上で MACsec をイネーブルにします。
ステップ 5	**authentication periodic**	このポートの再認証をイネーブルにします。
ステップ 6	**authentication timer reauthenticate interval**	再認証間隔を設定します。
ステップ 7	**access-session host-mode multi-domain**	ホストにインターフェイスへのアクセスを許可します。
ステップ 8	**access-session closed**	インターフェイスへの事前認証アクセスを防止します。
ステップ 9	**access-session port-control auto**	ポートの認可状態を設定します。
ステップ 10	**dot1x pae both**	ポートを 802.1X ポート アクセス エンティティ（PAE）のサプリカントおよびオーセンティケータとして設定します。
ステップ 11	**dot1x credentials profile**	802.1x クレデンシャル プロファイルをインターフェイスに割り当てます。
ステップ 12	**dot1x authenticator eap profile** *name*	EAP-TLS オーセンティケータ プロファイルをインターフェイスに割り当てます。
ステップ 13	**dot1x supplicant eap profile** *name*	EAP-TLS サプリカント プロファイルをインターフェイスに割り当てます。
ステップ 14	**service-policy type control subscriber** *control-policy name*	インターフェイスに加入者制御ポリシーを適用します。
ステップ 15	**exit**	特権 EXEC モードに戻ります。
ステップ 16	**show macsec interface**	インターフェイスの MACsec の詳細を表示します。
ステップ 17	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

証明書ベース MACsec 暗号化の確認

証明書ベースの MACsec 暗号化の設定を確認するには、次の **show** コマンドを使用します。次に、 **show** コマンドの出力例を示します。

show mka sessions コマンドは、アクティブな MACsec Key Agreement（MKA）プロトコルのセッションの概要を表示します。

```
Device# show mka sessions

  Total MKA Sessions....... 1
      Secured Sessions... 1
      Pending Sessions... 0

=============================================================================================
Interface      Local-TxSCI         Policy-Name      Inherited         Key-Server

Port-ID        Peer-RxSCI          MACsec-Peers     Status            CKN

=============================================================================================
Te0/1/3        74a2.e625.4413/0013 *DEFAULT POLICY* NO                YES

19             74a2.e625.4c22/0012 1                Secured
10000000000000000000000000000000000000000000000000000000000000000000
```

show macsec status interface *interface-id* は、指定されたインターフェイスの MACsec ステータス情報を表示します。

```
Device# show macsec status interface te0/1/2

  Capabilities:
  Ciphers Supported:        GCM-AES-128 GCM-AES-256
  Cipher:                   GCM-AES-128
  Confidentiality Offset:   0
  Replay Window:            64
  Delay Protect Enable:     FALSE
  Access Control:           must-secure

Transmit SC:
  SCI:                      74A2E6254C220012
  Transmitting:             TRUE
Transmit SA:
  Next PN:                  412
  Delay Protect AN/nextPN:  99/0

Receive SC:
  SCI:                      74A2E62544130013
  Receiving:                TRUE
Receive SA:
  Next PN:                  64
  AN:                       0
  Delay Protect AN/LPN:     0/0
```

show access-session interface *interface-id* **details** は、指定されたインターフェイスのアクセス セッションに関する詳細情報を表示します。

```
Device# show access-session interface te1/0/1 details

   Interface:  TenGigabitEthernet1/0/1
             IIF-ID:  0x17298FCD
         MAC Address:  f8a5.c592.13e4
        IPv6 Address:  Unknown
        IPv4 Address:  Unknown
           User-Name:  DOT1XCRED
              Status:  Authorized
              Domain:  DATA
      Oper host mode:  multi-host
     Oper control dir:  both
      Session timeout:  N/A
    Common Session ID:  000000000000000BB72E8AFA
      Acct Session ID:  Unknown
              Handle:  0xc3000001
       Current Policy:  MUSTS_1


Local Policies:
 Security Policy:  Must Secure
      Security Status:  Link Secured

Server Policies:


Method status list:
       Method           State
     dot1xSup           Authc Success
        dot1x           Authc Success
```

証明書ベース MACsec 暗号化の設定例

例:：証明書の登録

```
Configure Crypto PKI Trustpoint:
  crypto pki trustpoint POLESTAR-IOS-CA
   enrollment terminal
   subject-name CN=ASR1000x1@polestar.com, C=IN, ST=KA, OU=ENG,O=Polestar
   revocation-check none
   rsakeypair mkaioscarsa
   storage nvram:
  !
Manual Installation of Root CA certificate:
 crypto pki authenticate POLESTAR-IOS-CA
```

例：802.1x 認証の有効化と AAA の設定

```
aaa new-model
dot1x system-auth-control
radius server ISE
 address ipv4 <ISE ipv4 address> auth-port 1645 acct-port 1646
```

```
 automate-tester username dummy
 key dummy123
 radius-server deadtime 2
!
aaa group server radius ISEGRP
 server name ISE
!
aaa authentication dot1x default group ISEGRP
aaa authorization network default group ISEGRP
```

例：EAP-TLS プロファイルと 802.1x クレデンシャルの設定

```
eap profile EAPTLS-PROF-IOSCA
 method tls
 pki-trustpoint POLESTAR-IOS-CA
!

dot1x credentials EAPTLSCRED-IOSCA
 username asr1000@polestar.company.com
 pki-trustpoint POLESTAR-IOS-CA
!
```

例：インターフェイスでの 802.1X、PKI、および MACsec の設定の適用

```
interface TenGigabitEthernet0/1
 macsec network-link
 authentication periodic
 authentication timer reauthenticate <reauthentication interval>
 access-session host-mode multi-host
 access-session closed
 access-session port-control auto
 dot1x pae both
 dot1x credentials EAPTLSCRED-IOSCA
 dot1x supplicant eap profile EAPTLS-PROF-IOSCA
 service-policy type control subscriber DOT1X_POLICY_RADIUS
```

その他の参考資料

関連資料

関連項目	マニュアル タイトル
セキュリティ コマンド	• 『Security Command Reference: Commands A to C』 • 『Security Command Reference: Commands D to L』 • 『Security Command Reference: Commands M to R』 • 『Security Command Reference: Commands S to Z』

標準および RFC

標準/RFC	タイトル
IEEE 802.1AE-2006	*Media Access Control*（*MAC*）セキュリティ
IEEE 802.1X-2010	ポート ベースのネットワーク アクセス コントロール
IEEE 802.1AEbw-2013	*Media Access Control*（*MAC*）セキュリティ（IEEE 802.1AE-2006 の修正）：Extended Packet Numbering（XPN）
IEEE 802.1Xbx-2014	ポートベースのネットワーク アクセス コントロール（IEEE 802.1 x-2010 の修正）
RFC 4493	*AES-CMAC* アルゴリズム

シスコのテクニカル サポート

説明	リンク
右の URL にアクセスして、シスコのテクニカル サポートを最大限に活用してください。これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

第 107 章

MACsec as a Service：暗号化ソリューション

このドキュメントでは、Cisco WAN MACsec およびイーサネット仮想回線（EVC）を使用してネットワークトラフィックを保護するために、暗号化ソリューションである Cisco MACsec as a Service を展開する方法について説明します。このソリューションは、MACsec Key Agreement（MKA）プロトコルを使用した Media Access Control Security（MACsec）のイーサネット仮想回線（EVC）サポートを提供します。MKA を使用した MACsec では、EVC が検出され、EVC 基準に一致する物理インターフェイスが有効になります。この機能により、ユーザーは、WAN リンクを介して複数の企業からのレイヤ 2 トラフィックを転送し、EVC を介した MACsec によってトラフィックを個別に保護できます。

MACsec as a Service の機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *145 : MACsec as a Service* の機能情報

機能名	リリース	機能情報
MACsec as a Service：MACsec および MKA のイーサネット仮想回線サポート	Cisco IOS XE Gibraltar 16.12.1a	このドキュメントでは、MACsec Key Agreement（MKA）プロトコルによる MACsec のイーサネット仮想回線（EVC）サポートを使用して暗号化ソリューションを展開する方法について説明します。MKA を使用した MACsec では、EVC が検出され、EVC 基準に一致する物理インターフェイスが有効になります。この機能により、ユーザーは、WAN リンクを介して複数の企業からのレイヤ 2 トラフィックを転送し、EVC を介した MACsec によってトラフィックを個別に保護できます。 このリリースでは、この機能は、Cisco ASR 1000 シリーズ アグリゲーション サービス ルータでのみサポートされています。 次のコマンドが導入または変更されました： **mka pre-shared-key key-chain** *key-chain-name*、**mka policy** *policy-name*、**mka default-policy**、**macsec replay-protection window** *window size*、**eapol destination-address** *destination-address*{*bridge-group-address* | *broadcast-address* | *lldp-multicast-address* | *unicast mac-address*}、**eapol eth-type** *eth-type*。

MACsec および MKA のイーサネット仮想回線サポートの前提条件

- WAN MACsec には MACsec ライセンスが必要です。『Cisco ASR 1000 シリーズ イーサネット ラインカード データシート』の表を参照してください。
- レイヤ 2 の透過型イーサネットサービスが使用可能であることを確認します。サービス プロバイダー ネットワークが、Extensible Authentication Protocol over LAN（EAPoL）などの透過的な MACsec レイヤ 2 制御プロトコルを提供する必要があります。

MACsec および MKA のイーサネット仮想回線サポートに関する制約事項

- この機能は、Cisco 1000 シリーズ アグリゲーション サービス ルータでのみサポートされています。
- この機能は、Cisco IOS XE Gibraltar 16.12.1a 以降でサポートされています。

- MACsec を使用した EVC では、dot1q ベースのヘッダーのみがサポートされています。

  ポートあたりの MKA P2P セッションの数は、1 ギガインターフェイスで 8、10 ギガインターフェイスで 32 です。

- MACsec または MKA セッションが、物理インターフェイスまたはサブインターフェイスですでに設定されている場合、同じ物理インターフェイスのサービスインスタンスまたは EVC モードで MKA セッションを使用して MACsec を設定することはできません。その逆も同様です。

- MACsec EVC は、MKA PSK ベースのセッションでのみサポートされています。

MACsec および MKA のイーサネット仮想回線サポートに関する情報

MACsec および MKA の概要

MACsec は、IEEE 802.1AE 規格ベースのレイヤ 2 ホップバイホップ暗号化であり、これにより、メディアアクセス非依存プロトコルに対してデータの機密性と完全性を確保できます。

MACsec は、暗号化キーにアウトオブバンド方式を使用して、有線ネットワーク上で MAC レイヤの暗号化を提供します。MACsec Key Agreement（MKA）プロトコルでは、必要なセッション キーを提供し、必要な暗号化キーを管理します。ホスト側のリンク（ネットワーク アクセス デバイスと、PC や IP フォンなどのエンドポイント デバイス間のリンク）だけが MACsec を使用して保護できます。

MKA による 802.1AE 暗号化は、ルータまたはスイッチとホストデバイスの間の暗号化用に、ダウンリンクポートでサポートされます。MKA は、IEEE 規格の 802.1X で定義されている MACsec のコントロールプレーンです。MKA フレームは、EAPoL フレームの一部を形成します。MACsec は、パケット処理プロセスの最終段階であり、EAPoL フレームを除くすべてのトラフィックを暗号化します。

WAN MACsec および MKA を実装する場合は、MACsec の有効化を試みる前に、基本的なレイヤ 2 イーサネット接続が確立されていることを確認します。詳細については、「MACsec および MKA の概要」を参照してください。

シスコのイーサネット仮想回線

イーサネット仮想回線（EVC）は、レイヤ2サービスの単一インスタンスのエンドツーエンド表現です。さまざまなパラメータが統合されて、サービスが提供されます。シスコの EVC 構造では、ブリッジドメインは、サービスインスタンスと呼ばれているレイヤ2インターフェイス（1つまたは複数）で設定されます。サービス インスタンスは、あるルータ上のあるポート上で EVC をインスタンス化したものです。サービスインスタンスは、設定に基づいてブリッジドメイン（BD）に関連付けられます。

着信フレームは、次の基準に基づいてサービス インスタンスとして分類できます。

- シングル 802.1Q VLAN タグ、優先度タグ付き、または 802.1ad VLAN タグ
- 両 QinQ（内部および外部）VLAN タグ、または 802.1ad S-VLAN と C-VLAN タグの両方
- 外部 802.1p CoS ビット、内部 802.1p CoS ビット、またはその両方
- サービスインスタンスは、他のマッピング基準もサポートします。
- [Untagged]：802.1Q または 802.1ad ヘッダがないすべてのフレームにマッピングします。
- [Default]：すべてのフレームにマッピングします。

EVC アーキテクチャの詳細については、『Carrier Ethernet Configuration Guide』の「Configuring Ethernet Virtual Circuit」のセクションを参照してください。

イーサネット サービス インスタンスまたはイーサネットフローポイント

イーサネットフローポイント（EFP）は、インターフェイス上のイーサネットサービスのトランスポートに依存しない抽象化です。EFP は、ユーザー定義の基準に基づいて、同じ物理ポートからのフレームを、そのポートに関連付けられた複数のサービスインスタンスの 1 つに分類します。各 EFP に、異なる転送アクションと動作を関連付けることができます。

Extensible Authentication Protocol over LAN 宛先アドレス

MACsec セキュアセッションを確立する前に、MACsec Key Agreement（MKA）が制御プロトコルとして使用されます。MKA は、暗号化に使用する暗号スイートを選択し、必要なキーとパラメータをピア間で交換します。

MKA は、MKA メッセージを送信するためのトランスポート プロトコルとして Authentication Protocol over LAN（EAPoL）を使用します。デフォルトでは、EAPoL は宛先マルチキャスト MAC アドレスとして 01:80: c2:00:00:03 を使用して、複数の宛先へパケットをマルチキャストします。EAPoL は標準ベースのプロトコルであり、IEEE 802.1 x などの他の認証メカニズムでも同じプロトコルが使用されます。サービス プロバイダー クラウド内のデバイスは、（宛先マルチキャスト MAC アドレスに基づいて）このパケットを消費し、EAPoL パケットの処理を試み、最終的にはパケットをドロップします。これにより、MKA セッションが失敗します。

インターフェイス上でサービス プロバイダーに送信される EAPoL パケットの宛先 MAC アドレスを変更するには、**eapol destination-address** コマンドを使用します。これにより、サービス プロバイダーは、パケットを消費せずに、他のデータ パケットと同様にトンネリングできます。

（注） EAPoL宛先アドレスは、物理レベルまたはサブインターフェイスレベルで設定できます。物理インターフェイスで設定する場合、設定はサブインターフェイスによって自動的に継承されます。サブインターフェイスでの明示的な設定は、そのサブインターフェイスで継承された値またはポリシーよりも優先されます。

ブリッジドメイン（BD）は、プラットフォーム内部のブロードキャストドメインを定義し、VLAN からブロードキャストドメインを分離できます。そのため、ポートごとの VLAN シグニフィカンスが可能になります。これにより、単一のボックス単位の VLAN ID 空間に関連する拡張性の制限がなくなります。EVCが各イーサネットフローポイント（EFP）でさまざまなカプセル化を使用する機能を提供する方法の詳細については、「□ブリッジドメインインターフェイスのカプセル化」を参照してください。

イーサネット仮想回線を使用した MACsec および MKA の利点

- WAN リンクを介して複数の企業顧客からのレイヤ 2 VLAN を転送し、MACsec によってトラフィックを個別に保護します。

  MACsec を使用した WAN 経由の LAN トラフィックの選択的暗号化

WAN MACsec および MKA のサポートの利点の詳細については、「WAN MACsec および MKA のサポート機能強化の利点」の項を参照してください。

イーサネット仮想回線を使用した MACsec as a Service

次のトポロジは、ポイントツーポイントおよびポイントツーマルチポイントのシナリオでWAN MACsec を使用してイーサネット仮想回線（EVC）を EoMPLS ネットワークに展開する方法を示しています。暗号化されたトラフィックが、CVLAN を持つ CE から CE ルータに伝送され、ネットワーク内の CE ルータが、データが宛先に到達することを確認します。

図 *31 :* 単一の *SVLAN* を使用した *MKA* および *MACsec* トポロジ

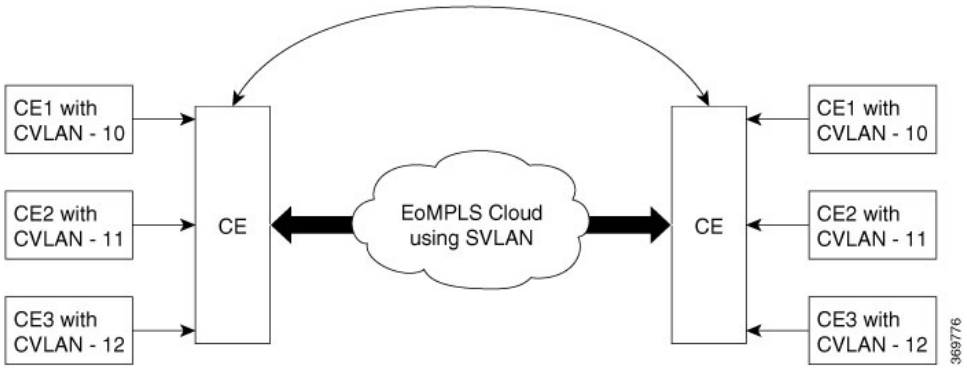
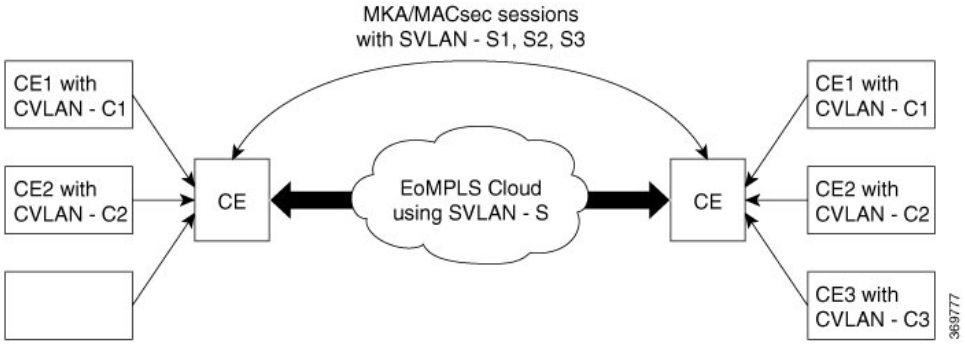


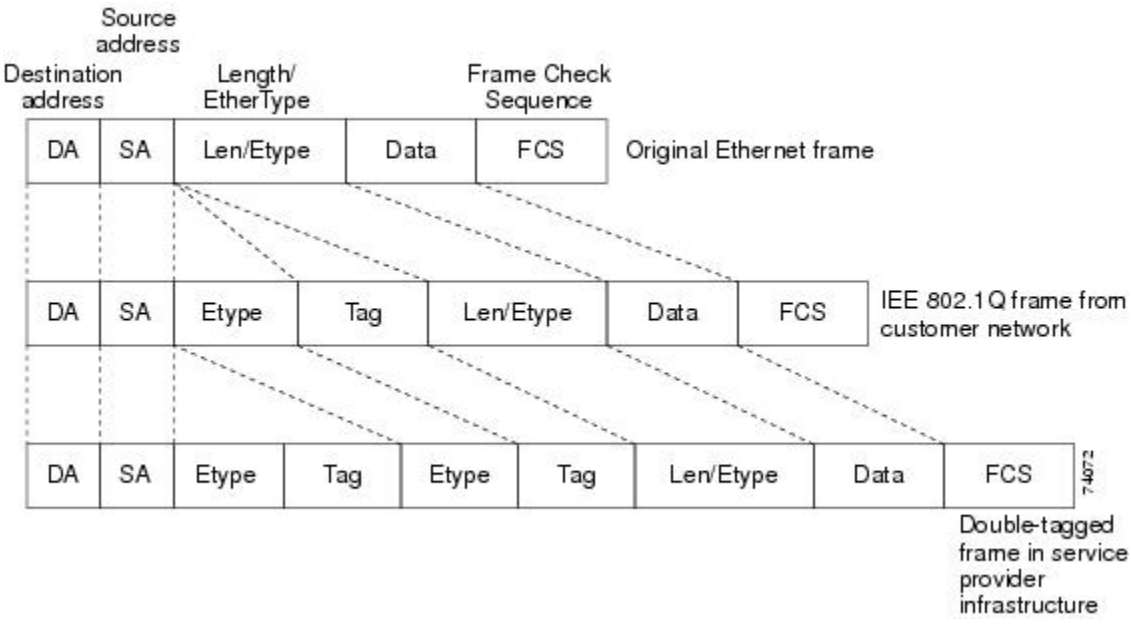
図 *32 :* 複数の *SVLAN* を使用した *MKA* および *MACsec* トポロジ



EAPoL フレームをサポートする Cisco WAN MACsec は、データを暗号化するだけでなく、さまざまなサービス プロバイダー ネットワークをシームレスに移動して、すべてのリモートサイトに安全に接続するために役立ちます。

EoMPLS ネットワークでは、異なる場所にある複数のレイヤ 2 イーサネットネットワークを接続できます。EoMPLS を介してさまざまなサービスプロバイダーに接続することを可能にするために、WAN MACsec は、暗号化されていない dot.1q タグをサポートしています。これは、サービス プロバイダー ネットワークの動作を中断することなくパブリック E-LINE または E-LAN サービスを介してリモートサイトに接続するために役立ちます。

図 *33 : 802.1Q* および二重タグ付きイーサネットパケット形式



サービスプロバイダーには、多くの場合、サポートする VLAN ID および VLAN の数に固有の要件があります。同一サービスプロバイダーネットワークのさまざまなカスタマーが必要とする VLAN 範囲は重複し、インフラストラクチャを通るカスタマーのトラフィックは混合してしまうことがあります。カスタマーごとに一意の VLAN ID 範囲を割り当てると、カスタマーの設定が制限され、802.1Q 仕様の VLAN に関する上限（4096 個）を容易に超えてしまいます。

サービス プロバイダー ネットワークを使用してネットワーク間でデータを交換する場合、MACsec を使用した EVC は、転送中のデータの暗号化に役立ちます。暗号化されていない dot.1q タグにより、複雑なネットワークを保護するための多数の設計オプションが可能になります。サービスプロバイダーはEVCを使用して、複数のカスタマーVLAN ID（C-VLAN）と、サービスプロバイダー VLAN（S-VLAN）による単一の 0x8100 Ethertype VLAN タグを持ち、サービス プロバイダー ネットワークに入るパケットをカプセル化できます。サービス プロバイダー ネットワーク内では、パケットは、S-VLANに基づいてスイッチングされます。パケットがサービス プロバイダー ネットワークからカスタマーネットワークに出ると、S-VLAN タグのカプセル化が解除され、元のカスタマーパケットが復元されます。

MACsec および MKA のイーサネット仮想回線サポートの設定方法

キーチェーンの設定

キーチェーンを設定するには、次の手順を実行します。

ステップ 1 **enable**

例：

```
Device> enable
```

特権 EXEC モードを有効にします。

ステップ 2 **configure terminal**

例：

```
Device# configure terminal
```

グローバル コンフィギュレーション モードを開始します。

ステップ 3 **key chain** *key-chain-name* **macsec**

例：

```
Device(config)# Key chain keychain1 macsec
```

キー チェーンを設定して、キー チェーン コンフィギュレーション モードを開始します。

ステップ 4 **key** *hex-string*

例：

```
Device(config-keychain)# key 01
```

キーを設定して、キー チェーン コンフィギュレーション モードを開始します。

ステップ 5 **cryptographic-algorithm** {**gcm-aes-128** | **gcm-aes-256**}

例：

```
Device(config-keychain-key)# cryptographic-algorithm aes-128-cmac
```

暗号化認証アルゴリズムを設定します。

ステップ 6 **key-string** *pwd-string*}

例：

```
Device(config-keychain-key)# key-string 12345678901234567890123456789013
```

キー文字列のパスワードを設定します。

ステップ 7 **end**

例：

```
Device(config-keychain-key)# end
```

特権 EXEC モードに戻ります。

インターフェイスでの MKA および MACsec の設定

インターフェイスで MKA および MACsec を設定するには、次の手順を実行します。

ステップ 1 **enable**

例：

```
Device> enable
```

特権 EXEC モードを有効にします。

- パスワードを入力します（要求された場合）。

ステップ 2 **configure terminal**

例：

```
Device# configure terminal
```

コンフィギュレーション モードを開始します。

ステップ 3 **mka policy** *policy-name*

例：

```
Device(config)# mka policy
```

MKA ポリシーを設定します。

ステップ 4 **mka pre-shared-key key-chain** *key-chain-name*

例：

```
Device(config)# mka pre-shared-key key-chain 10
```

MKA 事前共有キーに keychain10 を設定します。

（注） MKA事前共有キーは、物理インターフェイスまたはサブインターフェイスのいずれかで設定できますが、物理インターフェイスとサブインターフェイスの両方で設定することはできません。

ステップ5 macsec

EAPOL フレームタイプの MACsec を設定します。

ステップ6 macsec replay-protection window *window-size*

リプレイウィンドウを 10 に変更します。

ステップ7 end

特権 EXEC モードに戻ります。

カスタマーエッジ方向の入力ポートでのイーサネット仮想回線の設定

ステップ1 enable

特権 EXEC モードを有効にします。

- パスワードを入力します（要求された場合）。

ステップ2 configure terminal

グローバル コンフィギュレーション モードを開始します。

ステップ3 interface GigabitEthernet0/0/2

特権 EXEC モードを有効にします。

- パスワードを入力します（要求された場合）。

ステップ4 service instance 10 Ethernet

特権 EXEC モードを有効にします。

- パスワードを入力します（要求された場合）。

ステップ5 configure terminal

グローバル コンフィギュレーション モードを開始します。

ステップ6 interface GigabitEthernet0/0/2

特権 EXEC モードを有効にします。

- パスワードを入力します（要求された場合）。

ステップ 7 **encapsulation dot1q 10**

ステップ 8 **rewrite ingress tag push dot1q 20 symmetric**

ステップ 9 **bridge-domain** *number*

ステップ 10
```
interface GigabitEthernet0/0/2
   service instance 11 Ethernet
encapsulation dot1q 10
rewrite ingress tag push dot1q 20 symmetric
bridge-domain 21
interface GigabitEthernet0/0/2
   service instance 12 Ethernet
encapsulation dot1q 10
rewrite ingress tag push dot1q 20 symmetric
bridge-domain 22
```

サービス プロバイダー ネットワーク方向の出力ポートでの MACsec EVC の設定

ステップ 1 **enable**

ステップ 2 **configure terminal**

例：
```
interface tenGigabitEthernet0/1/1
    macsec dot1q-in-clear 1
    service instance 20 Ethernet
encapsulation dot1q 20
mka pre-shared-key key-chain kc1
macsec
bridge-domain 20
    service instance 21 Ethernet
encapsulation dot1q 21
mka pre-shared-key key-chain kc1
     macsec
     bridge-domain 21
    service instance 22 Ethernet
encapsulation dot1q 22
mka pre-shared-key key-chain kc1
macsec
bridge-domain 22
```

MACsec および MKA セッションに基づく事前共有キーの有効化の確認

手順の概要

1. **enable**

2.

手順の詳細

ステップ 1 **enable**

ステップ 2 例：

```
show running-config | sec kc1
key chain kc1 macsec
 key 01
   cryptographic-algorithm aes-128-cmac
  key-string 12345678901234567890123456789012
 mka pre-shared-key key-chain kc1
  mka pre-shared key-chain kc1
```

次に、サービスインスタンスモードでデフォルトポリシーを使用して事前共有キー（PSK）ベースの MKA/MACsec セッションを有効にするための設定例を示します。

```
Device#show running-config interface gi0/0/0
Building configuration...
 …
 …
 …
Current configuration : 142 bytes
!
interface Ethernet0/0
  no ip address
  negotiation auto
  service instance 10 ethernet
    encapsulation dot1q 10
    rewrite ingress tag pop 1 symmetric
    mka pre-shared key-chain kc1
    macsec
    bridge-domain 100
 !
end
```

MACsec および MKA のイーサネット仮想回線サポートの設定例

例：一般的なトラブルシューティング

例：一般的なトラブルシューティング

例：設定された show mka コマンド

例：設定された **show mka** コマンド

例：統計の表示

```
MACsec statistics on an EFP: To validate MACsec Statistics on an EFP instance, use
show macsec statistics interface gi0/0/3 efp 10
------------------------------------------------------------
MACsec Statistics for Gi0/0/3.EFP10
SecY Counters
  Ingress Untag Pkts:       5
  Ingress No Tag Pkts:      63440
  Ingress Bad Tag Pkts:     0
  Ingress Unknown SCI Pkts: 0
  Ingress No SCI Pkts:      0
  Ingress Overrun Pkts:     0
  Ingress Validated Octets: 0
  Ingress Decrypted Octets: 0
  Egress Untag Pkts:        0
  Egress Too Long Pkts:     0
  Egress Protected Octets:  0
  Egress Encrypted Octets:  0
Controlled Port Counters
  IF In Octets:             0
  IF In Packets:            0
  IF In Discard:            63440
  IF In Errors:             0
  IF Out Octets:            0
  IF Out Packets:           0
  IF Out Errors:            0
 Transmit SC Counters (SCI: 70708BBA4683000A)
  Out Pkts Protected:       0
  Out Pkts Encrypted:       0
Transmit SA Counters (AN 2)
  Out Pkts Protected:       0
  Out Pkts Encrypted:       0
Receive SA Counters (SCI: 70708BBA4183000A  AN 2)
  In Pkts Unchecked:        0
  In Pkts Delayed:          0
  In Pkts OK:               0
```

```
In Pkts Invalid:          0
In Pkts Not Valid:        0
In Pkts Not using SA:     0
In Pkts Unused SA:        0
In Pkts Late:             0
```

例：show efp コマンド

例：show efp コマンド

MACsec および MKA のイーサネット仮想回線サポートに関する追加情報

関連資料

標準および RFC

標準/RFC	タイトル
標準	役職

MIB

MIB	MIB のリンク
• CISCO-MIB	選択したプラットフォーム、Cisco IOS リリース、およびフィーチャ セットに関する MIB を探してダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

シスコのテクニカル サポート

説明	リンク
シスコのサポート Web サイトでは、シスコの製品やテクノロジーに関するトラブルシューティングにお役立ていただけるように、マニュアルやツールをはじめとする豊富なオンライン リソースを提供しています。 お使いの製品のセキュリティ情報や技術情報を入手するために、Cisco Notification Service（Field Notice からアクセス）、Cisco Technical Services Newsletter、Really Simple Syndication（RSS）フィードなどの各種サービスに加入できます。 シスコのサポート Web サイトのツールにアクセスする際は、Cisco.com のユーザ ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

第 XI 部

PKI

第 108 章

Cisco IOS XE PKI の概要

Cisco IOS XE 公開キー インフラストラクチャ（PKI）には、IP Security（IPSec）、セキュアシェル（SSH）、Secure Socket Layer（SSL）などのセキュリティ プロトコルをサポートする証明書管理機能があります。

このマニュアルでは、PKI を理解、計画、実装するために必要な概念を確認、説明します。

Cisco IOS XE PKI の情報

Cisco IOS XE PKI とは

PKI は以下のエンティティで構成されています。

- セキュアなネットワークで通信する複数のピア
- 証明書を発行および維持する認証局（CA）を最低 1 つ
- デジタル証明書（証明書の有効期間、ピアの ID 情報、セキュアな通信に使用する暗号キー、CA 発行のシグニチャなどで構成）
- 登録要求を処理し CA の負荷を軽減する登録局（RA）（任意）
- 証明書失効リスト（CRL）を配信するメカニズム（Lightweight Directory Access Protocol（LDAP）、HTTP など）

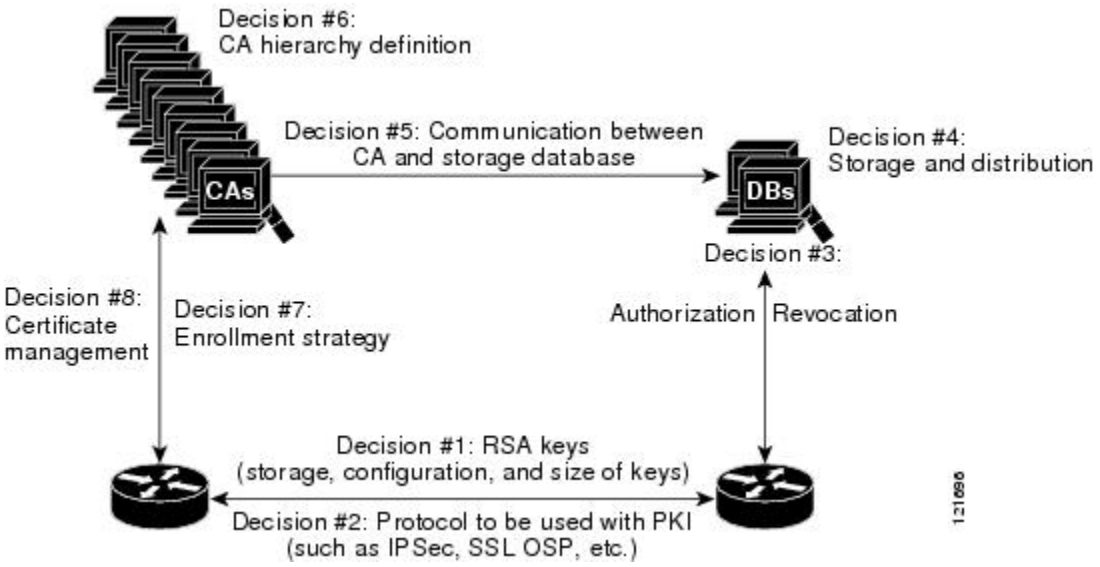
（注） Public Key Infrastructure（PKI）は、重要な拡張である **Inhibit Any Policy** をサポートしていません（内部 PKI ライブラリがこの拡張を認識しないため）。

PKI を使用すると、セキュアなデータ ネットワークで暗号化情報と ID 情報を配信、管理、失効するためのスケーラブルでセキュアなメカニズムを実現できます。セキュアな通信に関係するエンティティ（人物またはデバイス）はすべて、あるプロセスを経て PKI に登録されます。そのプロセスでは、エンティティが RSA（Rivest、Shamir、Adelman）キーのペア（秘密キーが 1 つ、公開キーが 1 つ）を生成し、信頼されているエンティティ（CA またはトラストポイントともいいます）でキーの ID を確認します。

各エンティティが PKI に登録されると、PKI のすべてのピア（エンド ホストともいいます）は、CA が発行したデジタル証明書を付与されます。セキュアな通信セッションをネゴシエーションする必要があるときは、ピアはデジタル証明書を交換します。ピアは証明書内の情報を基に他のピアの ID を確認し、証明書内の公開キーを使って、暗号化されたセッションを確立します。

PKI はさまざまな方法で計画、設定できますが、次の図に、PKI を構成する主なコンポーネントと、PKI で実行される各選択の順番を示します。図をアプローチとして推奨していますが、別の方法で PKI を設定してもかまいません。

図 *34 : PKI* の設定方法の決定



RSA キーの概要

RSA キー ペアは、公開キーと秘密キーで構成されます。PKI を設定する場合、証明書登録要求に公開キーを含める必要があります。証明書が付与された後、ピアが公開キーを使用して、ルータに送信されるデータを暗号化できるように、公開キーが証明書に組み込まれます。秘密キーはルータに保持され、ピアによって送信されたデータの復号化と、ピアとネゴシエーションするときの、トランザクションのデジタル署名に使用されます。

RSA キーペアには、キーのモジュラス値が含まれています。モジュラス値に応じて、RSA キーのサイズが決まります。モジュラス値が大きいほど、RSA キーの安全性が高まります。ただし、モジュラス値が大きくなると、キーの生成にかかる時間が長くなり、キーのサイズが大きくなると暗号化処理および復号化処理にかかる時間が長くなります。

（注） デフォルトのキーサイズは 1024 ビットです。

CA とは

CA（トラストポイントともいいます）は、証明書要求を管理し、参加ネットワーク デバイスに証明書を発行します。証明書要求の管理や証明書発行などのサービスにより、参加デバイスを一元的に管理します。またこれらのサービスによって受信者は、明示的に信頼してアイデンティティを確認し、デジタル証明書を作成できます。PKI の動作を開始する前に、CA は独自の公開キー ペアを生成し、自己署名 CA 証明書を作成します。その後、CA は、証明書要求に署名し、PKI に対してピア登録を開始できます。

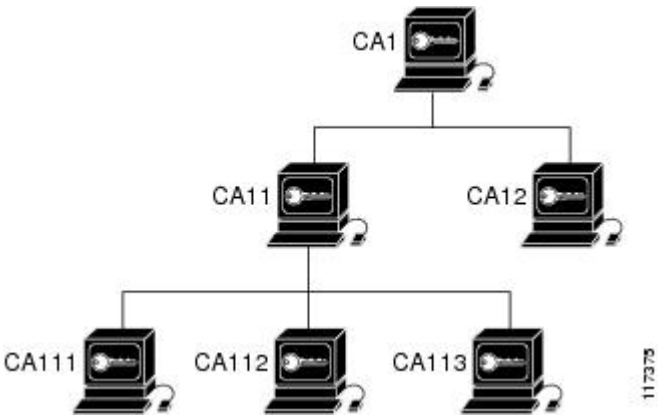
CA は、サードパーティの CA ベンダーが提供する CA を使用するか、内部の CA、つまり Cisco IOS 証明書サーバを使用します。

階層型 PKI：複数の CA

PKI は、複数の CA をサポートするために階層型フレームワーク内に設定できます。階層の最上位にはルート CA があり、自己署名証明書を保持しています。階層全体の信頼性は、ルート CA の RSA キー ペアから導出されます。階層構造内の下位 CA は、ルート CA または別の下位 CA に登録できます。どちらの方法で登録するかによって、CA の複数階層の設定方法が決まります。階層型 PKI 内では、登録されているすべてのピアが信頼できるルート CA 証明書または共通の下位 CA を共有している場合、証明書を相互に検証できます。

次の表 は、3 段の階層の CA 間の登録関係を示したものです。

図 *35 : 3* 段の *CA* 階層のサンプル トポロジ



各 CA が 1 つのトラストポイントに対応します。たとえば、CA11 および CA12 は従属 CA で、CA1 が発行した CA 証明書を保持しています。CA111、CA112、CA113 も従属 CA ですが、その CA 証明書を発行したのは CA11 です。

複数 CA を使用する場合

複数 CA を使用することにより、柔軟性および信頼性が向上します。たとえば、ルート CA を本社オフィスに配置し、下位 CA をブランチ オフィスに配置できます。また、CA ごとに異なる許可ポリシーを実行できるため、階層構造内の、ある CA では各証明書要求を手動で許可する必要があるように、別の CA では証明書要求を自動的に許可するように設定できます。

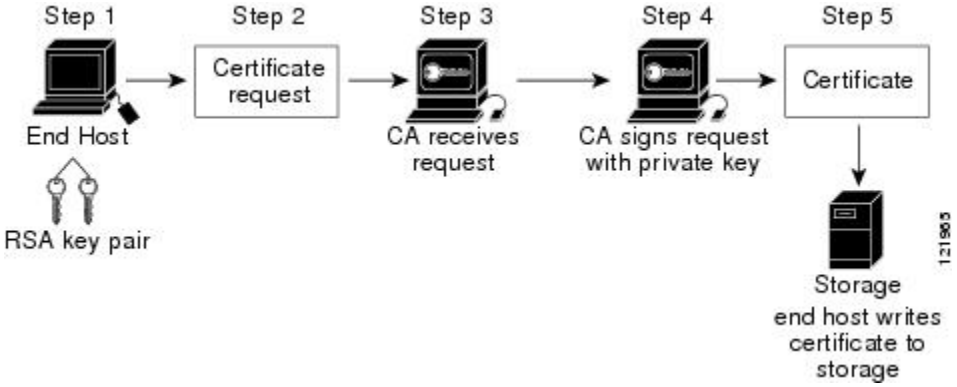
少なくとも 2 階層の CA が推奨されるシナリオは、次のとおりです。

- 多数の証明書が失効し、再発行される大規模かつ非常にアクティブなネットワーク。複数の階層を使用することにより、CA は CRL のサイズを制御しやすくなります。
- オンライン登録方式を使用するときに、ルート CA をオフラインのままにできる場合（従属 CA の証明書の発行を除く）。このシナリオでは、ルート CA のセキュリティが向上します。

証明書の登録：登録の動作

証明書の登録は、CA から証明書を取得するプロセスです。PKI に加わるエンド ホストは、それぞれ証明書を取得する必要があります。証明書の登録は、証明書を要求しているエンドホストと CA との間で行われます。次の表および手順によって、証明書の登録プロセスを説明します。

図 *36 :* 証明書の登録プロセス



1. エンド ホストが RSA キーのペアを生成します。
2. エンド ホストが証明書要求を生成し、CA（または使用可能な場合は RA）に送ります。
3. CA が証明書登録要求を受け取ります。ネットワークの設定によって、次のいずれかになります。
    1. 要求の承認に手動による操作が必要。
    2. CA に証明書を自動で要求するようにエンド ホストが設定されている。これにより、登録要求が CA サーバに送信されたときのオペレータによる手動操作は不要になります。

（注） CA に証明書を自動で要求するようにエンド ホストを設定するには、別の認証メカニズムが必要になります。

1. 要求が承認されると、CA は自分の秘密キーを使って要求に署名し、処理の終わった証明書をエンド ホストに戻します。
2. エンド ホストは、証明書を NVRAM などの保管領域に書き込みます。

Secure Device Provisioning による証明書登録

Secure Device Provisioning（SDP）は、Cisco IOS XE クライアントと Cisco IOS 証明書サーバなど、2 つのエンド デバイス間で PKI を簡単に配置できる、Web ベースの証明書登録インターフェイスです。

SDP（Trusted Transitive Introduction（TTI）とも呼ばれている）は、新しいネットワーク デバイスと VPN 間といった 2 つのエンド エンティティ間の双方向導入を実現する通信プロトコルです。SDP では次の 3 つのエンティティが関係します。

- イントロデューサ：ペティショナをレジストラに紹介する、相互に信頼できるデバイス。イントロデューサは、システム管理者などのデバイス ユーザの場合があります。
- ペティショナ：セキュアなドメインに参加した新しいデバイス。
- レジストラ：申請者を承認する証明書サーバなどのサーバ。

SDP は Web ブラウザを使い、ようこそ、紹介、完了の 3 つの段階で実装します。各段階は、Web ページを通してユーザに表示されます。

証明書の失効：失効する理由

各ピアが正常に PKI に登録されると、ピアは互いにセキュアな接続を行うためのネゴシエーションを開始できます。そのためにピアは確認に自分の証明書を提示し、失効のチェックを受けます。ピアは、通信相手のピアの証明書が、認証済みの CA によって発行された証明書であることを確認すると、CRL サーバまたは OCSP（Online Certificate Status Protocol）サーバをチェックし、証明書を発行した CA によって証明書が失効になっていないことを確認します。証明書には通常、証明書分散ポイント（CDP）が URL 形式で含まれています。Cisco IOS ソフトウェアはこの CDP を使用して、CRL の場所の特定と取得を行います。CDP サーバが応答しないと Cisco IOS ソフトウェアはエラーを生成し、ピアの証明書が拒否される場合があります。

PKI の計画

PKI の計画では、それぞれの PKI コンポーネントの要件と予定の用途を評価する必要があります。ユーザ（またはネットワーク管理者）の方で十分に PKI を計画してから、PKI の設定を始めること推奨します。

PKIの計画では検討すべきアプローチがいくつかありますが、このマニュアルでは、ピアツーピアの通信から始めます。ただし、ユーザまたはネットワーク管理者がPKIの計画を選択するときは、特定の決定がPKIの他の決定に影響することを理解しておいてください。たとえば、登録および展開をどのようにするかによって、CAの階層の計画が変わってくる場合があります。このため、PKI内の各コンポーネントがどのように機能するか、また、特定のコンポーネントのオプションが、計画プロセスで行った決定によってどのように変わるかを理解することが重要です。

次の作業

RSA キー ペアを生成したら、トラストポイントを設定する必要があります。すでにトラストポイントを設定している場合は、ルータを認証し、PKIに登録する必要があります。登録に関する情報については、「PKI の証明書登録の設定」を参照してください。

その他の参考資料

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『Cisco IOS Master Command List, All Releases』
PKI コマンド	• 『Cisco IOS Security Command Reference Commands A to C』 • 『Cisco IOS Security Command Reference Commands D to L』 • 『Cisco IOS Security Command Reference Commands M to R』 • 『Cisco IOS Security Command Reference Commands S to Z』
証明書登録：サポートされる方法、登録プロファイル、設定作業	『*Configuring Certificate Enrollment for a PKI*』
証明書の許可および失効：設定作業	『*Configuring Revocation and Authorization of Certificates in a PKI*』
Cisco IOS 証明書サーバの概要および設定作業	「*Configuring and Managing a Cisco IOS Certificate Server for PKI Deployment*」
安全なデバイス プロビジョニング：機能概要および設定作業	「*Setting Up Secure Device Provisioning (SDP) for Enrollment in a PKI*」

関連項目	マニュアル タイトル
USB eToken への RSA キーおよび証明書の保存	「*PKI* クレデンシャルの保存」

標準および RFC

標準/RFC	タイトル
RFC 2459	『*Internet X.509 Public Key Infrastructure Certificate and CRL Profile*』
RFC 2511	『*Internet X.509 Certificate Request Message Format*』
RFC 2527	『*Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework*』
RFC 2528	『*Internet X.509 Public Key Infrastructure*』
RFC 2559	『*Internet X.509 Public Key Infrastructure Operational Protocols - LDAPv2*』
RFC 2560	『*X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP*』
RFC 2585	『*Internet X.509 Public Key Infrastructure Operational Protocols: FTP and HTTP*』
RFC 2587	『*Internet X.509 Public Key Infrastructure LDAPv2 Schema*』
RFC 2875	『*Diffie-Hellman Proof-of-Possession Algorithms*』
RFC 3029	『*Internet X.509 Public Key Infrastructure Data Validation and Certification Server Protocols*』

MIB

MIB	MIB のリンク
• PKI MIB	選択したプラットフォーム、Cisco IOS ソフトウェア リリース、およびフィーチャ セットの MIB を検索してダウンロードする場合は、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

シスコのテクニカル サポート

説明	リンク
右の URL にアクセスして、シスコのテクニカル サポートを最大限に活用してください。これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

用語集

CDP：Certificate Distribution Point（証明書分散ポイント）。デジタル証明書内のフィールドで、証明書の CRL の取り出し方法を記述した情報が含まれています。最も一般的な CDP としては HTTP や LDAP の URL があります。CDP には、他の種類の URL または LDAP のディレクトリ指定が含まれている場合もあります。それぞれの CDP には、URL またはディレクトリの指定が 1 つ含まれています。

certificates：ユーザー名またはデバイス名を公開キーにバインドする電子ドキュメント。証明書は、一般的にデジタル署名を確認するために使用されます。

CRL：Certificate Revocation List（証明書失効リスト）。失効した証明書のリストが含まれる電子ドキュメントです。CRL は、証明書を発行した CA によって作成され、デジタル署名されます。CRL には、証明書の発行日と失効日が含まれています。現行の CRL が失効すると、新しい CRL が発行されます。

CA：Certification Authority（認証局）。証明書要求の管理と、関係する IPSec ネットワーク デバイスへの証明書の発行を担当しているサービス。このサービスは、参加デバイスを一元的に管理します。またこれらのサービスによって受信者は、明示的に信頼してアイデンティティを確認し、デジタル証明書を作成できます。

peer certificate：ピアが提示する証明書のことで、ピアの公開キーが含まれており、トラストポイント CA が署名します。

PKI：Public Key Infrastructure（公開キーインフラストラクチャ）。セキュアに設定された通信に使用されているネットワーク コンポーネントの暗号キーと ID 情報を管理するシステムです。

RA：Registration Authority（登録局）。CA のプロキシとして機能するサーバーで、CA がオフラインのときでも CA の機能を継続できます。RA は CA サーバー上に設定するのが通常ですが、別アプリケーションとして、稼働のための別デバイスを必要とする場合もあります。

RSA keys：公開キー暗号化システムで、Ron Rivest（ロナルド・リベスト）、Adi Shamir（アディ・シャミア）、Leonard Adleman（レオナルド・エーデルマン）の 3 人によって開発されました。ルータの証明書を取得するには、RSA キーのペア（公開キーと秘密キー）が必要です。

第 109 章

PKI 内での RSA キーの展開

この章では、公開キー インフラストラクチャ（PKI）内で Rivest、Shamir、Adelman（RSA）キーを設定および展開する方法について説明します。ルータの証明書を取得する前に、RSA キー ペア（公開キーと秘密キー）が要求されます。つまり、エンド ホストは RSA キーのペアを生成し、認証局（CA）と公開キーを交換して証明書を取得し、PKI に登録する必要があります。

（注） セキュリティに対する脅威は、脅威からの保護に役立つ暗号化技術と同様に絶え間なく変化しています。最新のシスコの暗号化に関する推奨事項については、『Next Generation Encryption』（NGE）ホワイト ペーパーを参照してください。

PKI での RSA キーの設定に関する前提条件

- PKI の RSA キーを設定および展開する前に、「Cisco IOS PKI Overview: Understanding and Planning a PKI」の内容を理解している必要があります。

RSA キーの設定に関する情報

RSA キーの概要

RSA キー ペアは、公開キーと秘密キーで構成されます。PKI を設定する場合、証明書登録要求に公開キーを含める必要があります。証明書が付与された後、ピアが公開キーを使用して、ルータに送信されるデータを暗号化できるように、公開キーが証明書に組み込まれます。秘密キーはルータに保持され、ピアによって送信されたデータの復号化と、ピアとネゴシエーションするときの、トランザクションのデジタル署名に使用されます。

RSA キーペアには、キーのモジュラス値が含まれています。モジュラス値に応じて、RSA キーのサイズが決まります。モジュラス値が大きいほど、RSA キーの安全性が高まります。ただし、モジュラス値が大きくなると、キーの生成にかかる時間が長くなり、キーのサイズが大きくなると暗号化処理および復号化処理にかかる時間が長くなります。

用途 RSA キーと汎用目的 RSA キー

RSA キー ペアには用途キーと汎用目的キーの 2 つのタイプがあり、これらは相互に排他的です。RSA キーペアを生成するとき（**crypto key generate rsa** コマンドを使用）、用途キーまたは汎用目的キーを選択するためのプロンプトが表示されます。

用途 RSA キー

用途キーは 2 組の RSA キー ペアで構成されます。このうち 1 組の RSA キー ペアは暗号化用に、もう 1 組の RSA キー ペアは署名用にそれぞれ生成され、使用されます。用途キーを使用すると、各キーは不必要に暴露されなくなります（用途キーを使用しない場合、1 つのキーが両方の認証方法に使用されるため、そのキーが暴露される危険性が高くなります）。

汎用目的 RSA キー

汎用目的キーは、1 つの RSA キー ペアだけで構成され、このキー ペアは暗号化と署名の両方に使用されます。汎用目的のキー ペアは、用途キー ペアよりも頻繁に使用されます。

RSA キー ペアとトラストポイントとの連携方法

トラストポイント（認証局（CA）としても知られる）は、証明書要求を管理し、参加ネットワーク デバイスに証明書を発行します。これらのサービスは、参加デバイスを一元的に管理します。またこれらのサービスによって受信者は、明示的に信頼してアイデンティティを確認し、デジタル証明書を作成できます。PKI の動作を開始する前に、CA は独自の公開キー ペアを生成し、自己署名 CA 証明書を作成します。その後、CA は、証明書要求に署名し、PKI に対してピア登録を開始できます。

⚠

注意 トラストポイントでは RSA キーペアを手動で生成しないでください。キーを手動で生成する場合は、キーペアを汎用キーではなく特定目的キーとして生成します。

⚠

注意 再生成オプションを使用した証明書の更新は、ゼロ（「0」）から始まるキーラベル（「0test」など）では機能しません。CLI を使用すると、トラストポイントでそのような名前を設定でき、ゼロから始まるホスト名を使用できます。トラストポイントで **rsakeypair** *name* を設定する場合は、ゼロから始まる名前を設定しないでください。キーペア名が設定されておらず、デフォルトのキーペアが使用されている場合は、ルータのホスト名がゼロから始まっていないことを確認してください。その場合は、トラストポイントで別の名前を使用して"**rsakeypair** *name* を明示的に設定してください。

ルータに複数の RSA キーを保管する理由

複数の RSA キー ペアを設定することで、Cisco IOS ソフトウェアは、対応する CA ごとに異なるキー ペアを維持できます。このようにして、このソフトウェアは、同じ CA で複数のキー ペアおよび証明書を維持できます。したがって、Cisco IOS ソフトウェアは、キーの長さ、キーのライフタイム、汎用目的キーまたは用途キーなど、他の CA で指定される要件を損なうことなく、各 CA のポリシー要件に合致します。

名前付きのキーペア（**label** *key-label* オプションを使用して指定する）を使用して、複数の RSA キーペアを用意すると、Cisco IOS ソフトウェアがアイデンティティの証明書ごとに異なるキーペアを維持できるようになります。

エクスポート可能な RSA キーのメリット

⚠

注意 エクスポート可能な RSA キーを使用すると、キーが暴露される危険性があるため、エクスポート可能な RSA キーは、使用前に慎重に評価する必要があります。既存の RSA キーはすべてエクスポート不能です。新しいキーは、デフォルトでエクスポート不能として生成されます。既存のエクスポート不能のキーは、エクスポート可能なキーに変換できません。

Cisco IOS Release 12.2(15)T では、ユーザは、ルータの秘密 RSA キー ペアをスタンバイ ルータと共有できます。したがって、ネットワーキング デバイス間でセキュリティ クレデンシャルを転送できます。キーペアを 2 台のルータ間で共有すると、一方のルータが、もう一方のルータの機能を迅速かつトランスペアレントに引き継ぐことができます。メイン ルータが故障した場合、スタンバイ ルータがネットワークに投入され、キーの再生、CA への再登録、または手動でのキーの再配布を行うことなく、メイン ルータを置き換えます。

また、セキュア シェル（SSH）を使用するすべての管理ステーションを 1 つの公開 RSA キーで設定できるように、RSA キー ペアをエクスポートおよびインポートすると、ユーザは同じ RSA キー ペアを複数のルータに配置することもできます。

PEM 形式ファイルでエクスポート可能な RSA キー

プライバシーエンハンスト メール（PEM）形式ファイルを使用した RSA キーのインポートまたはエクスポートは、Cisco IOS ソフトウェア リリース 12.3(4)T 以降を実行するお客様および、

セキュア ソケット レイヤ（SSL）またはセキュア シェル（SSH）アプリケーションを使用して、RSA キー ペアを手動で生成し、キーを PKI アプリケーションに再インポートするお客様に役立ちます。PEM形式のファイルを使用すると、新しいキーを生成しなくても、既存のRSA キー ペアを Cisco IOS ルータで直接使用できます。

RSA キーのインポートおよびエクスポート時のパスフレーズ保護

エクスポートする PKCS12 ファイルまたは PEM ファイルを暗号化するには、パスフレーズを含める必要があります。また、PKCS12 または PEM ファイルをインポートするときは、同じパスフレーズを入力して復号化する必要があります。PKCS12 または PEM ファイルをエクスポート、削除、またはインポートする際にこれらのファイルを暗号化すると、ファイルの伝送あるいは外部デバイスへの保管中に、ファイルを不正なアクセスおよび使用から保護します。

パスフレーズには、8 文字以上の任意のフレーズを指定できます。パスフレーズにはスペースおよび句読点を含めることができますが、Cisco IOS パーサに特殊な意味を持つ疑問符（?）は除きます。

エクスポート可能な RSA キー ペアをエクスポート不能な RSA キー ペアに変換する方法

パスフレーズ保護により、外部の PKCS12 または PEM ファイルが不正なアクセスおよび使用から保護されます。RSA キーペアがエクスポートされないようにするには、「nonexportable」とラベルを付ける必要があります。エクスポート可能な RSA キー ペアをエクスポート不可能なキー ペアに変換するには、キー ペアをエクスポートし、「exportable」というキーワードを指定しないで再びインポートする必要があります。

PKI 内で RSA キーを設定および展開する方法

RSA キー ペアの生成

（注） 新しく設定した PKI 証明書には、新しい RSA キーペア名を使用することをお勧めします。既存の RSA キーペア名（古い証明書に関連付けられている）を新しい PKI 証明書に再利用する場合は、次のいずれかを実行します。

- 既存の RSA キーペア名を使用して新しい RSA キーペアを再生成するのではなく、既存の RSA キーペア名を再利用します。既存の RSA キーペア名を使用して新しい RSA キーペアを再生成すると、既存の RSA キーペアに関連付けられているすべての証明書が無効になります。
- まず古い PKI 証明書設定を手動で削除してから、新しい PKI 証明書に既存の RSA キーペア名を再利用します。

.

RSA キー ペアを手動で生成するには、次の作業を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **crypto key generate rsa** [**general-keys** | **usage-keys** | **signature** | **encryption**] [**label** *key-label*] [**exportable**] [**modulus** *modulus-size*] [**storage** *devicename:*] [**on** *devicename:*]
4. **exit**
5. **show crypto key mypubkey rsa**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**crypto key generate rsa** [**general-keys**	**usage-keys**	**signature**	**encryption**] [**label** *key-label*] [**exportable**] [**modulus** *modulus-size*] [**storage** *devicename:*] [**on** *devicename:*] 例： `Router(config)# crypto key generate rsa usage-keys modulus 2048`	（任意）証明書サーバの RSA キー ペアを生成します。 • **storage** キーワードを使用すると、キーの保管場所を指定できます。 • *key-label* 引数を指定することによってラベル名を指定する場合、**crypto pki server** *cs-label* コマンドによって証明書サーバーに使用するラベルと同じ名前を使用する必要があります。*key-label* 引数を指定していない場合、ルータの完全修飾ドメイン名（FQDN）であるデフォルト値が使用されます。 **no shutdown** コマンドを発行する前に、CA 証明書が生成されるまで待ってからエクスポート可能な RSA キーペアを手動で生成する場合、**crypto ca export pkcs12** コマンドを使用して、証明書サーバー証明書および秘密キーを含む PKCS12 ファイルをエクスポートできます。 • デフォルトでは、CA キーのモジュラス サイズは 1024 ビットです。推奨される CA キーのモ

	コマンドまたはアクション	目的
		ジュラスは2048ビットです。CAキーのモジュラス サイズの範囲は360 ～ 4096ビットです。 • **on** キーワードは、指定したデバイス上でRSAキーペアが作成されることを指定します。このデバイスにはUniversal Serial Bus（USB）トークン、ローカルディスク、およびNVRAMなどがあります。装置の名前の後にはコロン（:）を付けます。 （注） USBトークン上で作成されるキーは、2048ビット以下である必要があります。 **注意** トラストポイントではRSAキーペアを手動で生成しないでください。キーを手動で生成する場合は、キーペアを汎用キーではなく特定目的キーとして生成します。
ステップ4	**exit** 例： `Router(config)# exit`	グローバル コンフィギュレーション モードを終了します。
ステップ5	**show crypto key mypubkey rsa** 例： `Router# show crypto key mypubkey rsa`	（任意）ルータのRSA公開キーを表示します。 このステップでは、RSAキーペアが正常に生成されたことを確認できます。

次の作業

正常にRSAキーペアを生成したら、この章のいずれかの追加作業に進み、RSAキーペアに対して追加のRSAキーペアを生成する、RSAキーペアのエクスポートおよびインポートを実行する、または追加のセキュリティパラメータ（秘密キーの暗号化またはロックなど）を設定します。

RSAキー ペアとトラストポイントの証明書の管理

複数のRSAキーペアを生成および保管し、トラストポイントにキーペアを関連付け、トラストポイントからルータの証明書を取得するようにルータを設定するには、次の作業を実行します。

始める前に

「RSAキー ペアの生成」の作業どおりにRSAキーペアを生成しておく必要があります。

手順の概要

1. **enable**
2. **configure terminal**
3. **crypto pki trustpoint** *name*
4. **rsakeypair** *key-label* [*key-size* [*encryption-key-size*]]
5. **enrollment selfsigned**
6. **subject-alt-name** *name*
7. **exit**
8. **cypto pki enroll** *name*
9. **exit**
10. **show crypto key mypubkey rsa**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**crypto pki trustpoint** *name* 例： `Router(config)# crypto pki trustpoint TESTCA`	トラストポイントを作成し、CA トラストポイント コンフィギュレーション モードを開始します。
ステップ 4	**rsakeypair** *key-label* [*key-size* [*encryption-key-size*]] 例： `Router(ca-trustpoint)# rsakeypair fancy-keys`	（任意）*key-label* 引数には、登録時に生成された RSA キーペアの名前を指定し（まだ存在しない場合、または **auto-enroll regenerate** コマンドが設定されている場合）、トラストポイント証明書と一緒に使用します。デフォルトでは、完全修飾ドメイン名（FQDN）キーを使用します。 • キーペア名をゼロ（「0」）から始めることはできません。詳細については、「RSA キーペアとトラストポイントとの連携方法」のセクションを参照してください。 • （任意）*key-size* 引数には、RSA キー ペアのサイズを指定します。推奨されるキー サイズは 2048 ビットです。

	コマンドまたはアクション	目的
		• （任意）*encryption-key-size* 引数には 2 番めのキーのサイズを指定します。2 番めのキーは、個別の暗号化、署名キー、および証明書を要求する場合に使用されます。
ステップ 5	**enrollment selfsigned** 例： `Router(ca-trustpoint)# enrollment selfsigned`	（任意）トラストポイントの自己署名登録を指定します。
ステップ 6	**subject-alt-name** *name* 例： `Router(ca-trustpoint)# subject-alt-name TESTCA`	（任意）*name* 引数には、トラストポイントの証明書に含まれる X.509 証明書の所有者別名（subjectAltName）フィールドのトラストポイントの名前を指定します。デフォルトでは、証明書に所有者別名フィールドは含まれていません。 （注） X.509 証明書のこのフィールドは、RFC 2511 に定義されています。 このオプションは、所有者別名（subjectAltName）フィールドにトラストポイントの名前を含むルータの自己署名トラストポイント証明書を作成する場合に使用します。所有者別名は、トラストポイントポリシーの自己署名登録に **enrollment selfsigned** コマンドが指定された場合にのみ使用できます。

ステップ 7	**exit**
	例：
	`Router`
	`(ca-trustpoint)#`
	`exit`
		CA トラストポイント コンフィギュレーション モードを終了します。

ステップ 8	**cypto pki enroll** *name*
	例：
	`Router(config)# cypto pki enroll TESTCA`
	例：
	`% Include the router serial number in the subject name? [yes/no]: no`
	例：
	`% Include an IP address in the subject name? [no]:`
		トラストポイントからのルータの証明書を要求します。
		name 引数にはトラストポイントの名前を指定します。このコマンドを入力したら、プロンプトに応答します。
		（注） **crypto pki trustpoint** コマンドで入力したものと同じトラストポイント名を使用します。

	コマンドまたはアクション	目的

	例：
	`Generate Self Signed Router Certificate? [yes/no]: yes`
	例：
	`Router Self Signed Certificate successfully created`	

ステップ 9	**exit** 例： `Router(config)# exit`	グローバル コンフィギュレーション モードを終了します。
ステップ 10	**show crypto key mypubkey rsa** 例： `Router# show crypto key mypubkey rsa`	（任意）ルータの RSA 公開キーを表示します。 このステップでは、RSA キー ペアが正常に生成されたことを確認できます。

例

次に、所有者別名（subjectAltName）フィールドにトラストポイントの名前を含むルータの自己署名トラストポイント証明書を作成する方法の例を示します。

```
Router> enable
Router# configure terminal
Router(config)#crypto pki trustpoint TESTCA
Router(ca-trustpoint)#hash sha256
Router(ca-trustpoint)#rsakeypair testca-rsa-key 2048
Router(ca-trustpoint)#exit
Router(config)#crypto pki enroll TESTCA
% Include the router serial number in the subject name? [yes/no]:no
% Include an IP address in the subject name? [no]: no
Generate Self Signed Router Certificate? [yes/no]: yes

Router Self Signed Certificate successfully created

Router(config)#
Router(config)#exit
Router#
```

次の証明書が作成されます。

```
Router#show crypto pki certificate verbose Router Self-Signed Certificate
   Status: Available
   Version: 3
   Certificate Serial Number (hex): 01
   Certificate Usage: General Purpose
   Issuer:
     hostname=Router.cisco.com
   Subject:
     Name: Router.cisco.com
```

```
    hostname=Router.cisco.com
  Validity Date:
    start date: 11:41:50 EST Aug 13 2012
    end   date: 19:00:00 EST Dec 31 2019
  Subject Key Info:
    Public Key Algorithm: rsaEncryption
    RSA Public Key: (2048 bit)
  Signature Algorithm: SHA256 with RSA Encryption
  Fingerprint MD5: CA92D937 593BF19A 5B7F8466 F554D631
  Fingerprint SHA1: 57A9D411 2DDFAC81 68260F2F C6C8D7CF 4833F3E9
  X509v3 extensions:
    X509v3 Subject Key ID: 44340F76 A6B8DC37 80724650 0672875F 741D518C
    X509v3 Basic Constraints:
        CA: TRUE
    X509v3 Authority Key ID: 44340F76 A6B8DC37 80724650 0672875F 741D518C
    Authority Info Access:
  Associated Trustpoints: TESTCA

-----BEGIN CERTIFICATE-----
MIIBszCCAV2gAwIBAgIBAjANBgkqhkiG9w0BAQQFADAuMQ8wDQYDVQQDEwZURVNU
Q0ExGzAZBgkqhkiG9w0BCQIWDHIxLmNpc2NvLmNvbTAeFw0xMDAzMjIyMDI2MjBa
Fw0yMDAxMDEwMDAwMDBaMC4xDzANBgNVBAMTBlRFU1RDQTEbMBkGCSqGSIb3DQEJ
AhYMcjEuY2lzY28uY29tMFwwDQYJKoZIhvcNAQEBBQADSwAwSAJBAI1xLjvrouLz
RNm8qYWI9Km9yX/wafXndY8A8o4+L8pexQhDlYyiaq7OoK6CYWH/ToyPidFW2DU0
t5WTGnIDcfsCAwEAAaNmMGQwDwYDVR0TAQH/BAUwAwEB/zARBgNVHREECjAIggZU
RVNUQ0EwHwYDVR0jBBgwFoAU+aSVh1+kyn1l+r44IFUY+Uxs1fMwHQYDVR0OBBYE
FPmklYdfpMp9Zfq+OCBVGPlMbNXzMA0GCSqGSIb3DQEBBAUAA0EAbZLnqKUaWu8T
WAIbeReTQTfJLZ8ao/U6cwXN0QKEQ37ghAdGVflFWVG6JUhv2OENNUQHXBYXNUWZ
4oBuU+U1dg==
-----END CERTIFICATE-----
```

RSA キーのエクスポートおよびインポート

ここでは、RSA キーのエクスポートおよびインポートに使用できる次の作業について説明します。エクスポート可能な RSA キーを使用すると、メイン ルータが故障した場合に、使用ファイルが PKCS12 ファイルか PEM ファイルかにかかわらず、新しい RSA キーを生成しなくても、Cisco IOS ルータの既存の RSA キーを使用できます。

PKCS12 ファイルの RSA キーのエクスポートおよびインポート

RSA キー ペアをエクスポートおよびインポートすることにより、ユーザは、セキュリティ クレデンシャルをデバイス間で転送できます。キーペアを2台のデバイス間で共有すると、一方のデバイスが、もう一方のデバイスの機能を迅速かつトランスペアレントに引き継ぐことができます。

始める前に

「RSA キー ペアの生成」で指定した作業のとおりに RSA キー ペアを生成して「exportable」とマークを付ける必要があります。

（注）
- システムを Cisco IOS Release 12.2(15)T 以降にアップグレードするまでは、ルータ上に存在する RSA キーをエクスポートできません。Cisco IOS ソフトウェアのアップグレード後、新しい RSA キーを生成し、このキーに「exportable」のラベルを付ける必要があります。
- サードパーティ製のアプリケーションで生成された PKCS12 ファイルをインポートする場合、PKCS12 ファイルには CA 証明書が含まれている必要があります。
- RSA キーペアをすでにエクスポートし、ターゲットルータにインポートした後で RSA キーペアを再インポートする場合、**exportable** キーワードを指定する必要があります。
- ルータがインポートできる RSA キーの最大サイズは、2048 ビットです。

手順の概要

1. **crypto pki trustpoint** *name*
2. **rsakeypair** *key-label* [*key-size* [*encryption-key-size*]]
3. **exit**
4. **crypto pki export** *trustpointname* **pkcs12** *destination-url* **password** *password-phrase*
5. **crypto pki import** *trustpointname* **pkcs12** *source-url* **password** *password-phrase*
6. **exit**
7. **show crypto key mypubkey rsa**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**crypto pki trustpoint** *name* 例： `Router(config)# crypto pki trustpoint my-ca`	RSA キーペアに関連付けるトラストポイント名を作成し、CA トラストポイント コンフィギュレーション モードを開始します。
ステップ 2	**rsakeypair** *key-label* [*key-size* [*encryption-key-size*]] 例： `Router(ca-trustpoint)# rsakeypair my-keys`	トラストポイントに使用するキー ペアを指定します。
ステップ 3	**exit** 例： `Router(ca-trustpoint)# exit`	CA トラストポイント コンフィギュレーション モードを終了します。
ステップ 4	**crypto pki export** *trustpointname* **pkcs12** *destination-url* **password** *password-phrase* 例：	トラストポイント名を使用して RSA キーをエクスポートします。 • *trustpointname* 引数は、ユーザがエクスポート予定の証明書を発行するトラストポイントの名前

	コマンドまたはアクション	目的
	`Router(config)# crypto pki export my-ca pkcs12 tftp://tftpserver/my-keys password mypassword123`	を入力します。PKCS12 ファイルをエクスポートする場合、トラストポイント名はRSA キー名です。 • *destination-url* 引数は、ユーザが RSA キー ペアをインポートする PKCS12 ファイルのファイル システム ロケーションを入力します。 • *password -phrase* 引数は、エクスポート用に PKCS12 ファイルを暗号化するのに入力する必要があります。
ステップ 5	**crypto pki import** *trustpointname* **pkcs12** *source-url* **password** *password-phrase* 例： `Router(config)# crypto pki import my-ca pkcs12 tftp://tftpserver/my-keys password mypassword123`	ターゲット ルータにRSA キーをインポートします。 • *trustpointname* 引数は、ユーザがエクスポートまたはインポート予定の証明書を発行するトラストポイントの名前を入力します。インポートすると、トラストポイントがRSA キー名になります。 • *source-url* 引数は、ユーザが RSA キー ペアをエクスポートする PKCS12 ファイルのファイル システム ロケーションを指定します。 • *password -phrase* は、RSA キーがインポートされる場合、暗号化を元に戻すために入力する必要があります。
ステップ 6	**exit** 例： `Router(config)# exit`	グローバル コンフィギュレーション モードを終了します。
ステップ 7	**show crypto key mypubkey rsa** 例： `Router# show crypto key mypubkey rsa`	（任意）ルータの RSA 公開キーを表示します。

PEM 形式ファイルの RSA キーのエクスポートおよびインポート

PEM ファイルの RSA キー ペアをエクスポートまたはインポートするには、次の作業を実行します。

始める前に

「RSA キー ペアの生成」で指定した作業のとおりに RSA キー ペアを生成して「exportable」とマークを付ける必要があります。

（注）
- システムを Cisco IOS Release 12.3 (4)T 以降のリリースにアップグレードする前に、エクスポート可能のフラグを付けずに生成された RSA キーは、エクスポートおよびインポートできません。Cisco IOS ソフトウェアをアップグレードしたら、新しい RSA キーを生成する必要があります。
- ルータがインポートできる RSA キーの最大サイズは、2048 ビットです。

（注） セキュリティに対する脅威は、脅威からの保護に役立つ暗号化技術と同様に絶え間なく変化しています。最新のシスコの暗号化に関する推奨事項については、『*Next Generation Encryption*』（NGE）ホワイト ペーパーを参照してください。

手順の概要

1. **crypto key generate rsa** {**usage-keys** | **general-keys**} **label** *key-label* [**exportable**]
2. **crypto pki export** *trustpoint* **pem** {**terminal** | **url** *destination-url*} {**3des** | **des**} **password** *password-phrase*
3. **crypto pki import** *trustpoint* **pem** [**check** | **exportable** | *usage-keys*] {**terminal** | **url** *source-url*} **password***password-phrase*
4. **exit**
5. **show crypto key mypubkey rsa**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**crypto key generate rsa** {**usage-keys** | **general-keys**} **label** *key-label* [**exportable**] 例： `Router(config)# crypto key generate rsa general-keys label mykey exportable`	RSA キー ペアを生成します。 PEM ファイルを使用するには、RSA キー ペアはエクスポート可能のラベルが付いている必要があります。
ステップ 2	**crypto pki export** *trustpoint* **pem** {**terminal** | **url** *destination-url*} {**3des** | **des**} **password** *password-phrase* 例： `Router(config)# crypto pki export mycs pem url nvram: 3des password mypassword123`	PEM形式ファイルのトラストポイントと関連付けられた証明書およびRSAキーをエクスポートします。 • エクスポートした証明書および RSA キー ペアに関連付けられた *trustpoint* 名を入力します。トラストポイント名は、**crypto pki trustpoint** コマ

	コマンドまたはアクション	目的
		ンドを使用して指定された名前と一致する必要があります。 • **terminal** キーワードを使用し、コンソール端末に PEM 形式で表示される証明書および RSA キーペアを指定します。 • **url** キーワードおよび *destination -url* 引数を使用し、ルータが証明書および RSA キーペアをエクスポートするファイルシステムの URL を指定します。 •（任意）**3des** キーワードは、Triple Data Encryption Standard（3DES）暗号化アルゴリズムを使用してトランスポイントをエクスポートします。 •（任意）**des** キーワードは、DES 暗号化アルゴリズムを使用してトランスポイントをエクスポートします。 • *password-phrase* 引数を使用し、インポート用の PEM ファイルの暗号化に使用する暗号化パスワード フレーズを指定します。 ヒント　PEM ファイルは、必ず安全な場所に保管してください。たとえば、別のバックアップ ルータに保管することもできます。
ステップ 3	**crypto pki import** *trustpoint* **pem** [**check** | **exportable** | *usage-keys*] {**terminal** | **url** *source-url*} **password***password-phrase* 例： `Router(config)# crypto pki import mycs2 pem url nvram: password mypassword123`	PEM形式ファイルからにトラストポイントに証明書および RSA キーをインポートします。 • インポートした証明書および RSA キー ペアに関連付けられた *trustpoint* 名を入力します。トラストポイント名は、**crypto pki trustpoint** コマンドを使用して指定された名前と一致する必要があります。 •（任意）**check** キーワードを使用し、古い証明書を許可しないように指定します。 •（任意）**exportable** キーワードを使用し、インポートした RSA キーペアをルータなどの別の Cisco デバイスに再びエクスポートできるように指定します。

	コマンドまたはアクション	目的
		• （オプション）*usage-keys* 引数を使用し、1 つの汎用目的キーペアの代わりに、2 つの RSA 特殊用途キー ペア（暗号化ペア 1 つとシグニチャ ペア 1 つ）がインポートされるように指定します。 • *source-url* 引数を使用し、ルータが証明書および RSA キー ペアをインポートするファイル システムの URL を指定します。 • *password-phrase* 引数を使用し、インポート用の PEM ファイルの暗号化に使用する暗号化パスワード フレーズを指定します。 （注） パスワードフレーズには、8 文字以上の任意のフレーズを指定できます。パスフレーズにはスペースおよび句読点を含めることができますが、Cisco IOS パーサに特殊な意味を持つ疑問符（?）は除きます。 （注） キーを CA からエクスポート可能にしない場合は、そのキーをエクスポート不能のキー ペアとしてエクスポートしてから、CA に再度インポートしてください。このキーは削除できなくなります。
ステップ 4	**exit** 例： `Router(config)# exit`	グローバル コンフィギュレーション モードを終了します。
ステップ 5	**show crypto key mypubkey rsa** 例： `Router# show crypto key mypubkey rsa`	（任意）ルータの RSA 公開キーを表示します。

ルータの秘密キーの暗号化およびロック

デジタル署名は、あるデバイスを別のデバイスに対して認証するために使用されます。デジタル署名を使用するには、プライベート情報（秘密キー）を、署名を提示しているデバイスに保管する必要があります。保管されたプライベート情報は、秘密キーを含むハードウェア装置を乗っ取ろうとする攻撃者に役立つことがあります。たとえば、攻撃者は、乗っ取ったルータを

使用し、ルータに保管されている RSA 秘密キーを使用して、別のサイトへのセキュアな接続を開始する可能性があります。

（注） RSA キーはパスワードの復元操作中に失われます。パスワードを喪失した場合、パスワードの復元操作を実行すると、RSA キーは削除されます（この機能により、攻撃者がパスワードの復元を実行してキーを使用するのを防止します）。

攻撃者から秘密 RSA キーを保護するために、ユーザは、パスフレーズを使用して NVRAM に保管された秘密キーを暗号化できます。侵入を試みる攻撃者によってルータが乗っ取られた場合、ユーザは、秘密キーを「ロック」することもできます。これにより、稼働中ルータからの新しい接続の試行がブロックされ、ルータ内のキーが保護されます。

NVRAM に保存された秘密キーを暗号化しロックするには、次の作業を実行します。

（注） CA の登録中は、RSA キーのロックを解除する必要があります。ルータの秘密キーは認証時に使用されないため、CA でルータを認証している間、この秘密キーをロックできます。

始める前に

秘密キーを暗号化またはロックする前に、次の作業を実行する必要があります。

- RSA キーペアを生成します（「RSA キーペアの生成」のセクションを参照）。
- 必要に応じて、各ルータを認証し、CA サーバに登録できます。

（注） **後方互換性に関する制約事項**

Cisco IOS Release 12.3(7)T よりも前のイメージは、暗号キーをサポートしません。暗号キーがルータによってすべて喪失されないように、Cisco IOS Release 12.3(7)T 以前のイメージを起動する前に、暗号化されていないキーだけが NVRAM に書き込まれていることを確認してください。

Cisco IOS Release 12.3(7)T 以前のイメージをダウンロードする必要がある場合は、ダウンロードされたイメージによって設定が上書きされないように、キーを復号化し、ただちに設定を保存してください。

アプリケーションとの相互作用

ルータの起動後、キーを手動で（**crypto key unlock rsa** コマンドを使用して）アンロックするまで、暗号キーは有効になりません。暗号化されているキー ペアによっては、この機能により、IP セキュリティ（IPsec）、SSH、SSL などのアプリケーションに悪影響が及ぶ可能性があります。つまり必要なキー ペアがアンロックされるまで、セキュア チャネル経由でのルータ管理ができない場合があります。

>

手順の概要

1. crypto key encrypt [write] rsa [name key-name] passphrase passphrase
2. **exit**
3. **show crypto key mypubkey rsa**
4. **crypto key lock rsa name** *key-name*] **passphrase** *passphrase*
5. **show crypto key mypubkey rsa**
6. **crypto key unlock rsa** [**name** *key-name*] **passphrase** *passphrase*
7. **configure terminal**
8. **crypto key decrypt** [**write**] **rsa** [**name***key-name*] **passphrase** *passphrase*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	crypto key encrypt [write] rsa [name key-name] passphrase passphrase 例： `Router(config)# crypto key encrypt write rsa name pki.example.com passphrase password`	RSA キーを暗号化します。 このコマンドが発行されると、ルータはキーを引き続き使用でき、キーはアンロックされたままになります。 （注） **write** キーワードを発行しない場合、設定を手動で NVRAM に書き込む必要があります。この作業を行わないと、次にルータをリロードするときに暗号キーが消去されます。
ステップ 2	**exit** 例： `Router(config)# exit`	グローバル コンフィギュレーション モードを終了します。
ステップ 3	**show crypto key mypubkey rsa** 例： `Router# show crypto key mypubkey rsa`	（任意）秘密キーが暗号化（保護）され、アンロックされていることを確認できます。 （注） このコマンドを使用して、キーの暗号化後、インターネット キー交換（IKE）および SSH などのアプリケーションが適切に機能していることを確認することもできます。
ステップ 4	**crypto key lock rsa name** *key-name*] **passphrase** *passphrase* 例：	（任意）暗号化された秘密キーを稼働中のルータ上でロックします。

	コマンドまたはアクション	目的
	`Router# crypto key lock rsa name pki.example.com passphrase password`	（注） キーをロックした後は、そのキーを使用してピア デバイスにルータを認証できません。この動作により、ロックされているキーを使用するIPSecまたはSSL接続はすべてディセーブルになります。ロックされたキーに基づいて作成された既存のIPSecトンネルは閉じられます。すべてのRSAキーをロックすると、SSHは自動的にディセーブルになります。
ステップ5	**show crypto key mypubkey rsa** 例： `Router# show crypto key mypubkey rsa`	（任意）秘密キーが保護され、ロックされていることを確認できます。 このコマンドの出力では、IKE、SSH、SSL などのアプリケーションによって試行された接続の失敗も表示されます。
ステップ6	**crypto key unlock rsa** [**name** *key-name*] **passphrase** *passphrase* 例： `Router# crypto key unlock rsa name pki.example.com passphrase password`	（任意）秘密キーをアンロックします。 （注） このコマンドを発行すると、IKEトンネルを引き続き確立できます。
ステップ7	**configure terminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ8	**crypto key decrypt** [**write**] **rsa** [**name***key-name*] **passphrase** *passphrase* 例： `Router(config)# crypto key decrypt write rsa name pki.example.com passphrase password`	（任意）暗号化されたキーを削除し、暗号化されていないキーだけを残します。 （注） **write** キーワードを使用すると、暗号化されていないキーはただちにNVRAMに保存されます。**write** キーワードを発行しない場合、設定を手動でNVRAMに書き込む必要があります。この作業を行わないと、次にルータをリロードしたときにキーが暗号化したままになります。

RSA キー ペア設定の削除

次のいずれかの理由により、RSA キー ペアの削除が必要になる場合があります。

- 手動での PKI 操作およびメンテナンスの間に、古い RSA キーを削除して、新しいキーと交換できます。
- 既存の CA を置き換えた場合、新しい CA では、新たにキーを生成する必要があります。たとえば、必要なキーのサイズが組織によって異なることがあるため、古い 1024 ビット キーを削除し、新しい 2048 ビット キーを生成することが必要になる場合があります。
- **T** IKEv1 および IKEv2 での署名確認の問題をデバッグできるように、ピアルータの公開キーを削除できます。デフォルトでは、キーはトラストポイントに関連付けられた証明書失効リスト（CRL）のライフタイムによってキャッシュされます。

すべての RSA キーまたはルータによって生成された指定の RSA キー ペアを削除するには、次の作業を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. crypto key zeroize rsa [key-pair-label]
4. **crypto key zeroize pubkey-chain** [*index*]
5. **exit**
6. **show crypto key mypubkey rsa**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	crypto key zeroize rsa [key-pair-label] 例： `Router(config)# crypto key zeroize rsa fancy-keys`	ルータから RSA キー ペアを削除します。 • *key-pair-label* 引数を指定していない場合、ルータによって生成された RSA キーはすべて削除されます。
ステップ 4	**crypto key zeroize pubkey-chain** [*index*] 例： `Router(config)# crypto key zeroize pubkey-chain`	キャッシュからリモート ピアの公開キーを削除します。 （任意）特定の公開キーのインデックス エントリを削除するには、*index* 引数を使用します。インデックス エントリが指定されていない場合、すべてのエン

	コマンドまたはアクション	目的
		トリが削除されます。インデックスエントリに指定できる値の範囲は 1 ～ 65535 です。
ステップ 5	**exit** 例： `Router(config)# exit`	グローバル コンフィギュレーション モードを終了します。
ステップ 6	**show crypto key mypubkey rsa** 例： `Router# show crypto key mypubkey rsa`	（任意）ルータの RSA 公開キーを表示します。 このステップでは、RSA キーペアが正常に生成されたことを確認できます。

RSA キー ペア展開での設定例

RSA キーの生成および指定例

次の例は、RSA キーペア「exampleCAkeys」を生成し、指定する方法を示すサンプルのトラストポイント設定です。

```
crypto key generate rsa general-purpose exampleCAkeys
crypto ca trustpoint exampleCAkeys
 enroll url http://exampleCAkeys/certsrv/mscep/mscep.dll
 rsakeypair exampleCAkeys 1024 1024
```

RSA キーのエクスポートおよびインポート例

PKCS12 ファイルの RSA キーのエクスポートおよびインポート例

次の例では、RSA キー ペア「mynewkp」がルータ A で生成され、トラストポイント名「mynewtp」が作成されて、この RSA キー ペアに関連付けられています。トラストポイントはルータ B にインポートできるように TFTP サーバにエクスポートされます。ユーザがルータ B にトランスポイント「mynewtp」をインポートすると、ルータ B に RSA キーペア「mynewkp」がインポートされます。

ルータ A

```
crypto key generate rsa general label mykeys exportable
! The name for the keys will be:mynewkp
Choose the size of the key modulus in the range of 360 to 2048 for your
General Purpose Keys. Choosing a key modulus greater than 512 may take
a few minutes.
How many bits in the modulus [512]: 2048
% Generating 2048 bit RSA keys ...[OK]
```

```
!
crypto pki trustpoint mynewtp
 rsakeypair mykeys
 exit
crypto pki export mytp pkcs12 flash:myexport password mypassword123
Destination filename [myexport]?
Writing pkcs12 file to tftp:/mytftpserver/myexport
CRYPTO_PKI:Exported PKCS12 file successfully.
Verifying checksum... OK (0x3307)
!
July 8 17:30:09 GMT:%CRYPTO-6-PKCS12EXPORT_SUCCESS:PKCS #12 Successfully Exported.
```

ルータ B

```
crypto pki import mynewtp pkcs12 flash:myexport password mypassword123
Source filename [myexport]?
CRYPTO_PKI:Imported PKCS12 file successfully.
!
July 8 18:07:50 GMT:%CRYPTO-6-PKCS12IMPORT_SUCCESS:PKCS #12 Successfully Imported.
```

PEM ファイルの RSA キーのエクスポートおよびインポート例

次の例では、RSA キー ペア「mytp」の生成、エクスポート、インポートを示し、そのステータスを確認します。

```
! Generate the key pair
!
Router(config)# crypto key generate rsa general-purpose label mytp exportable

The name for the keys will be: mytp
Choose the size of the key modulus in the range of 360 to 2048 for your
General Purpose Keys. Choosing a key modulus greater than 512 may take a few minutes.
How many bits in the modulus [512]: 2048
% Generating 2048 bit RSA keys ...[OK]
!
! Archive the key pair to a remote location, and use a good password.
!
Router(config)# crypto pki export mytp pem url nvram:mytp 3des password mypassword123

% Key name:mytp
Usage:General Purpose Key
Exporting public key...
Destination filename [mytp.pub]?
Writing file to nvram:mytp.pub
Exporting private key...
Destination filename [mytp.prv]?
Writing file to nvram:mytp.prv
!
! Import the key as a different name.
!
Router(config)# crypto pki import mytp2 pem url nvram:mytp2 password mypassword123

% Importing public key or certificate PEM file...
Source filename [mytp2.pub]?
Reading file from nvram:mytp2.pub
% Importing private key PEM file...
Source filename [mytp2.prv]?
Reading file from nvram:mytp2.prv% Key pair import succeeded.
!
! After the key has been imported, it is no longer exportable.
```

```
!
! Verify the status of the key.
!
Router# show crypto key mypubkey rsa

% Key pair was generated at:18:04:56 GMT Jun 6 2011
Key name:mycs
Usage:General Purpose Key
Key is exportable.
Key Data:
30819F30 0D06092A 864886F7 0D010101 05000381 8D003081 89028181 00E65253
9C30C12E 295AB73F B1DF9FAD 86F88192 7D4FA4D2 8BA7FB49 9045BAB9 373A31CB
A6B1B8F4 329F2E7E 8A50997E AADBCFAA 23C29E19 C45F4F05 DBB2FA51 4B7E9F79
A1095115 759D6BC3 5DFB5D7F BCF655BF 6317DB12 A8287795 7D8DC6A3 D31B2486
C9C96D2C 2F70B50D 3B4CDDAE F661041A 445AE11D 002EEF08 F2A627A0 5B020301 0001
% Key pair was generated at:18:17:25 GMT Jun 6 2011
Key name:mycs2
Usage:General Purpose Key
Key is not exportable.
Key Data:
30819F30 0D06092A 864886F7 0D010101 05000381 8D003081 89028181 00E65253
9C30C12E 295AB73F B1DF9FAD 86F88192 7D4FA4D2 8BA7FB49 9045BAB9 373A31CB
A6B1B8F4 329F2E7E 8A50997E AADBCFAA 23C29E19 C45F4F05 DBB2FA51 4B7E9F79
A1095115 759D6BC3 5DFB5D7F BCF655BF 6317DB12 A8287795 7D8DC6A3 D31B2486
C9C96D2C 2F70B50D 3B4CDDAE F661041A 445AE11D 002EEF08 F2A627A0 5B020301 0001
```

PEM ファイルからのルータ RSA キー ペアおよび証明書のエクスポート例

次の例では、トラストポイント「mycs」と関連付けられた PEM ファイルに RSA キー ペア「aaa」とルータの証明書を生成およびエクスポートする方法について示します。また、この例では、Base64 符号化データの前後の PEM 境界を含む PEM 形式ファイルも示します。このファイルは他の SSL と SSH アプリケーションで使用されます。

```
Router(config)# crypto key generate rsa general-keys label aaa exportable

The name for the keys will be:aaa
Choose the size of the key modulus in the range of 360 to 2048 for your General Purpose
 Keys. Choosing a key modulus greater than 512 may take a few minutes.
!
How many bits in the modulus [512]:
% Generating 512 bit RSA keys ...[OK]
!
Router(config)# crypto pki trustpoint mycs

Router(ca-trustpoint)# enrollment url http://mycs

Router(ca-trustpoint)#
rsakeypair aaa

Router(ca-trustpoint)# exit

Router(config)# crypto pki authenticate mycs

Certificate has the following attributes:
Fingerprint:C21514AC 12815946 09F635ED FBB6CF31
% Do you accept this certificate? [yes/no]: y
Trustpoint CA certificate accepted.
!
Router(config)# crypto pki enroll mycs

%
```

```
% Start certificate enrollment ..
% Create a challenge password. You will need to verbally provide this password to the
CA Administrator in order to revoke your certificate.
For security reasons your password will not be saved in the configuration.
Please make a note of it.
Password:
Re-enter password:
% The fully-qualified domain name in the certificate will be: Router
% The subject name in the certificate will be:host.example.com
% Include the router serial number in the subject name? [yes/no]: n
% Include an IP address in the subject name? [no]: n
Request certificate from CA? [yes/no]: y
% Certificate request sent to Certificate Authority
% The certificate request fingerprint will be displayed.
% The 'show crypto ca certificate' command will also show the fingerprint.
Router(config)# Fingerprint:8DA777BC 08477073 A5BE2403 812DD157
00:29:11:%CRYPTO-6-CERTRET:Certificate received from Certificate Authority
Router(config)# crypto ca export aaa pem terminal 3des password

% CA certificate:
-----BEGIN CERTIFICATE-----
MIICAzCCAa2gAwIBAgIBATANBgkqhkiG9w0BAQUFADBOMQswCQYDVQQGEwJVUzES
<snip>
waDeNOSI3WlDa0AWq5DkVBkxwgn0TqIJXJOCttjHnWHK1LMcMVGn
-----END CERTIFICATE-----
% Key name:aaa
Usage:General Purpose Key
-----BEGIN RSA PRIVATE KEY-----
Proc-Type:4,ENCRYPTED
DEK-Info:DES-EDE3-CBC,ED6B210B626BC81A
Urguv0jnjwOgowWVUQ2XR5nbzzYHI2vGLunpH/IxIsJuNjRVjbAAUpGk7VnPCT87
<snip>
kLCOtxzEv7JHc72gMku9uUlrLSnFH5slzAtoC0czfU4=
-----END RSA PRIVATE KEY-----
% Certificate:
-----BEGIN CERTIFICATE-----
MIICTjCCAfigAwIBAgICIQUwDQYJKoZIhvcNAQEFBQAwTjELMAkGA1UEBhMCVVMx
<snip>
6xlBaIsuMxnHmr89KkKkYlU6
-----END CERTIFICATE-----
```

PEM ファイルからのルータ RSA キー ペアおよび証明書のインポート例

次の例では、TFTP を使用して、PEM ファイルから RSA キー ペアと証明書をトラストポイント「ggg」にインポートする方法を示します。

```
Router(config)# crypto pki import ggg pem url tftp://10.1.1.2/username/msca password

% Importing CA certificate...
Address or name of remote host [10.1.1.2]?
Destination filename [username/msca.ca]?
Reading file from tftp://10.1.1.2/username/msca.ca
Loading username/msca.ca from 10.1.1.2 (via Ethernet0):!
[OK - 1082 bytes]
% Importing private key PEM file...
Address or name of remote host [10.1.1.2]?
Destination filename [username/msca.prv]?
Reading file from tftp://10.1.1.2/username/msca.prv
Loading username/msca.prv from 10.1.1.2 (via Ethernet0):!
[OK - 573 bytes]
% Importing certificate PEM file...
Address or name of remote host [10.1.1.2]?
```

```
Destination filename [username/msca.crt]?
Reading file from tftp://10.1.1.2/username/msca.crt
Loading username/msca.crt from 10.1.1.2 (via Ethernet0):!
[OK - 1289 bytes]
% PEM files import succeeded.
Router(config)#
```

ルータの秘密キーの暗号化およびロック例

暗号キーの設定および検証例

次の例に、RSA キー「pki-123.example.com」を暗号化する方法について示します。そのため、**show crypto key mypubkey rsa** コマンドを発行して、RSA キーが暗号化（保護）およびロック解除されているかを確認します。

```
Router(config)# crypto key encrypt rsa name pki-123.example.com passphrase password
Router(config)# exit
Router# show crypto key mypubkey rsa
```

% Key pair was generated at:00:15:32 GMT Jun 25 2003

Key name:pki-123.example.com

Usage:General Purpose Key

*** The key is protected and UNLOCKED. ***

Key is not exportable.

Key Data:

305C300D 06092A86 4886F70D 01010105 00034B00 30480241 00E0CC9A 1D23B52C

CD00910C ABD392AE BA6D0E3F FC47A0EF 8AFEE340 0EC1E62B D40E7DCC

23C4D09E

03018B98 E0C07B42 3CFD1A32 2A3A13C0 1FF919C5 8DE9565F 1F020301 0001

% Key pair was generated at:00:15:33 GMT Jun 25 2003

Key name:pki-123.example.com.server

Usage:Encryption Key

Key is exportable.

Key Data:

307C300D 06092A86 4886F70D 01010105 00036B00 30680261 00D3491E 2A21D383

854D7DA8 58AFBDAC 4E11A7DD E6C40AC6 66473A9F 0C845120 7C0C6EC8 1FFF5757

3A41CE04 FDCB40A4 B9C68B4F BC7D624B 470339A3 DE739D3E F7DDB549 91CD4DA4

DF190D26 7033958C 8A61787B D40D28B8 29BCD0ED 4E6275C0 6D020301 0001

```
Router#
```

ロックされたキーの設定および確認例

次の例に、キー「pki-123.example.com」をロックする方法について示します。そのため、**show crypto key mypubkey rsa** コマンドを発行して、キーが保護（暗号化）またはロックされているかを確認します。

```
Router# crypto key lock rsa name pki-123.example.com passphrase password
!
Router# show crypto key mypubkey rsa

% Key pair was generated at:20:29:41 GMT Jun 20 2003
Key name:pki-123.example.com
Usage:General Purpose Key
*** The key is protected and LOCKED. ***
Key is exportable.
Key Data:
305C300D 06092A86 4886F70D 01010105 00034B00 30480241 00D7808D C5FF14AC
0D2B55AC 5D199F2F 7CB4B355 C555E07B 6D0DECBE 4519B1F0 75B12D6F 902D6E9F
B6FDAD8D 654EF851 5701D5D7 EDA047ED 9A2A619D 5639DF18 EB020301 0001
```

その他の参考資料

関連資料

関連項目	マニュアル タイトル
PKI の概要（RSA キー、証明書登録、および CA を含む）	「Cisco IOS PKI Overview: Understanding and Planning a PKI」
PKI コマンド：完全なコマンドの構文、コマンドモード、デフォルト、使用上の注意事項、例	『*Cisco IOS Security Command Reference*』
推奨される暗号化アルゴリズム	『*Next Generation Encryption*』

MIB

MIB	MIB のリンク
なし	選択したプラットフォーム、Cisco IOS リリース、およびフィーチャ セットに関する MIB を探してダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

RFC

RFC	タイトル
RFC 2409	『*The Internet Key Exchange (IKE)*』

RFC	タイトル
RFC 2511	『Internet X.509 Certificate Request Message Format』

シスコのテクニカル サポート

説明	リンク
右の URL にアクセスして、シスコのテクニカル サポートを最大限に活用してください。これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

Cisco TrustSec の概要の機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *146 : Cisco TrustSec* の概要の機能情報

機能名	リリース	機能情報
IPv6 の有効化 - インライン タギング	Cisco IOS XE Fuji 16.8.1	IPv6 のサポートが導入されました。

第 110 章

PKI での証明書の許可および失効の設定

この章では、公開キーインフラストラクチャ（PKI）で証明書の許可および失効を設定する方法について説明します。証明書サーバへのハイアベイラビリティのサポートに関する情報も挙げています。

（注） セキュリティに対する脅威は、脅威からの保護に役立つ暗号化技術と同様に絶え間なく変化しています。シスコの暗号化に関する最新の推奨事項の詳細は、『Next Generation Encryption』（NGE）ホワイトペーパーを参照してください。

証明書の許可および失効に関する前提条件

PKI ストラテジの計画

ヒント 実際の証明書の展開を開始する前に、全体の PKI ストラテジを計画することを強く推奨します。

ユーザーまたはネットワーク管理者が次の作業を完了した後に、許可および失効が発生します。

- 認証局（CA）の設定。
- ピア デバイスの CA への登録。

- ピアツーピア通信に使用される（IP セキュリティ（IPsec）またはセキュア ソケット レイヤ（SSL）などの）プロトコルの確認および設定。

許可および失効に固有の情報をピアデバイス証明書に含めなければならない場合があるため、ピア デバイスを登録する前に、設定する許可および失効ストラテジを決定する必要があります。

「crypto ca」から「crypto pki」への CLI の変更

Cisco IOS Release 12.3(7)T では、「crypto ca」で始まるすべてのコマンドが、「crypto pki」から始まるように変更されました。ルータは引き続き crypto ca コマンドを受信しますが、出力はすべて crypto pki に読み替えられます。

高可用性

ハイ アベイラビリティのため、IPsec 保護された Stream Control Transmission Protocol（SCTP）はアクティブ ルータとスタンバイ ルータの両方で設定する必要があります。同期を機能させるには、SCTP を設定した後に、証明書サーバーの冗長性モードを ACTIVE/STANDBY に設定する必要があります。

証明書の許可および失効に関する制約事項

- シャーシ内での Stateful Switchover（SSO）冗長性の PKI High Availability（HA）サポートは、現在 Cisco IOS Release 12.2 S ソフトウェアを実行するすべてのスイッチ上でサポートされていません。詳細については、Cisco Bug CSCtb59872 を参照してください。
- Cisco IOS リリースに応じて、Lightweight Directory Access Protocol（LDAP）がサポートされます。

証明書の許可および失効に関する情報

PKI の許可

PKI 認証では、許可を行いません。多くの場合、一元的に管理されるソリューションが必要ですが、現在の許可用のソリューションは、設定対象のルータに固有です。

それによって証明書を特定の作業に対して許可し、その他の作業に対しては許可しない、と定義できる標準的なメカニズムはありません。アプリケーションが証明書ベースの許可情報を認識する場合、この許可情報を証明書自体に取り込めます。このソリューションでは、許可情報をリアルタイムで更新するための簡単なメカニズムを提供していないため、証明書に組み込まれた固有の許可情報を認識するように各アプリケーションに強制します。

証明書ベースの ACL メカニズムがトラストポイント認証の一部として設定される場合、該当アプリケーションは、この許可情報を判別する役割を担うことはなく、どのアプリケーション

に対して証明書を許可するのか指定できません。ルータ上の証明書ベースの ACL は、大きくなりすぎて管理できないことがあります。また、外部サーバーから証明書ベースの ACL 指示を取得する方が有利です

許可の問題にリアルタイムで対処する現在のソリューションでは、新しいプロトコルの指定や新しいサーバーの構築（それとともに管理およびデータ配布などの関連作業）が必要になります。

証明書ステータスのための PKI と AAA サーバーの統合

PKI を認証、許可、アカウンティング（AAA）サーバーと統合することにより、既存の AAA インフラストラクチャを活用する代替オンライン証明書ステータスソリューションを実現します。証明書を適切な許可レベルで AAA データベースに一覧表示できます。PKI-AAA を明示的にサポートしないコンポーネントでは、デフォルト ラベルの「all」を指定すると、AAA サーバーからの許可が可能になります。また、AAA データベースのラベルが「none」の場合、指定された証明書が有効でないことを示します（アプリケーション ラベルが欠如していることと同じですが、「none」は完全性および明確性のために含まれます）。アプリケーション コンポーネントが PKI-AAA をサポートしている場合、コンポーネントを直接指定できる場合があります。たとえば、アプリケーション コンポーネントを「ipsec」、「ssl」、または「osp」に指定できます（ipsec = IP セキュリティ、ssl = セキュア ソケット レイヤ、および osp = Open Settlement Protocol）。

（注） 現在、アプリケーション ラベルの指定をサポートするアプリケーション コンポーネントはありません。

- AAA サーバーにアクセスしたときに、時間遅延が生じる場合があります。AAA サーバーを利用できない場合、許可は失敗します。

RADIUS または TACACS+：AAA サーバー プロトコルの選択

AAA サーバーは、RADIUS または TACACS+ プロトコルと連動するように設定できます。PKI 統合用に AAA サーバーを設定する場合、許可に必要な RADIUS または TACACS 属性を設定する必要があります。

RADIUS プロトコルが使われている場合は、AAA サーバーのユーザー名に設定するパスワードを「cisco」に設定する必要があります。証明書の検証が認証を行い、AAA データベースは許可の目的だけに使用されているので、このパスワードは受け入れ可能です。TACACS プロトコルを使用する場合、TACACS では認証が不要な許可をサポートする（認証にパスワードを使用）ので、AAA サーバーのユーザー名に対して設定されるパスワードとは無関係です。

さらに、TACACS を使用する場合は、AAA サーバーに PKI サービスを追加する必要があります。カスタム属性「cert-application=all」が、PKI サービスの特定のユーザーまたはユーザー グループに追加され、特定のユーザー名が許可されます。

PKI と AAA サーバー統合用の属性値ペア

次の表 に、AAA サーバーと PKI との統合を設定する場合に使用される属性値（AV）ペアを示します（表に示す値は、可能な値であることに注意してください）。AV ペアはクライアント設定と一致する必要があります。AV ペアが一致しない場合、ピア証明書は許可されません。

（注） 場合によっては、ユーザーは、他のすべてのユーザーの AV ペアとは異なる AV ペアを持つことができます。その場合、ユーザーごとに一意のユーザー名が必要になります。（**authorization username** コマンド内に）**all** パラメータを設定すると、証明書のサブジェクト名全体を許可ユーザー名として使用するように指定できます。

表 *147*：一致する必要がある *AV* ペア

AV ペア	値
cisco-avpair=pki:cert-application=all	有効な値は、[all] および [none] です。
cisco-avpair=pki:cert-trustpoint=msca	この値は、Cisco IOS コマンドライン インターフェイス（CLI）設定のトラストポイント ラベルです。 （注） cert-trustpoint AV ペアの指定は、通常任意です。このペアが指定されている場合、Cisco IOS ルータ クエリーは、一致するラベルを持つ証明書トラストポイントから受信する必要があり、認証された証明書は、指定された証明書シリアル番号を持っている必要があります。
cisco-avpair=pki:cert-serial=16318DB7000100001671	この値は証明書のシリアル番号です。 （注） cert-serial AV ペアの指定は、通常任意です。このペアが指定されている場合、Cisco IOS ルータ クエリーは、一致するラベルを持つ証明書トラストポイントから受信する必要があり、認証された証明書は、指定された証明書シリアル番号を持っている必要があります。

AV ペア	値
cisco-avpair=pki:cert-lifetime-end=1:00 jan 1, 2003	cert-lifetime-end AV ペアは、証明書で指示された期間を越えた証明書のライフタイムを人為的に延長する場合に使用できます。cert-lifetime-end AV ペアを使用する場合は、cert-trustpoint および cert-serial AV ペアも指定する必要があります。この値は、時/分/月/日/年の形式と一致する必要があります。 （注） 月を表す最初の 3 文字（Jan、Feb、Mar、Apr、May、Jun、Jul、Aug、Sep、Oct、Nov、Dec）だけが使用されます。月を表す文字として 4 文字以上入力すると、残りの文字は無視されます（たとえば、Janxxxx）。

CRL または OCSP サーバー：証明書失効メカニズムの選択

証明書が適切に署名された証明書として有効になった後、証明書失効方法を実行して、証明書が発行元 CA によって無効にされていないことを確認します。Cisco IOS ソフトウェアは、2 つの失効メカニズムとして証明書失効リスト（CRL）と Online Certificate Status Protocol（OCSP）をサポートします。Cisco IOS ソフトウェアも、証明書のチェックために AAA 統合をサポートしますが、これには追加の許可機能が含まれます。PKI と AAA 証明書の許可とステータス確認に関する詳細については、「証明書ステータスのための PKI と AAA サーバーの統合」を参照してください。

次の項では、各失効メカニズムの機能方法について説明します。

CRL とは

CRL とは、失効した証明書のリストです。CRL は、証明書を発行した CA によって作成され、デジタル署名されます。CRL には、各証明書の発行日と失効日が含まれています。

CA は、新しい CRL を定期的に、あるいは CA が責任を負う証明書が失効したときに公開します。デフォルトでは、現在キャッシュされている CRL が失効すると、新しい CRL がダウンロードされます。管理者は、CRL がルータのメモリにキャッシュされる時間を設定したり、CRL キャッシングを完全にディセーブルにしたりできます。CRL キャッシング設定は、トラストポイントに関連付けられたすべての CRL に適用されます。

CRL が失効すると、ルータはキャッシュから CRL を削除します。証明書が検証用に表示されると、新しい CRL がダウンロードされます。ただし、検証中の証明書を記載した新しいバージョンの CRL がサーバー上にあるにもかかわらず、ルータがキャッシュ内の CRL を使用し続ける場合、ルータは証明書が失効したことを認識しません。証明書は拒否されるはずのものでも、失効チェックに合格します。

CA は、証明書を発行すると、証明書にその CRL 配布ポイント（CDP）を含めることができます。Cisco IOS クライアント デバイスは、CDP を使用して適切な CRL を見つけ、ロードします。Cisco IOS クライアントは複数の CDP をサポートしますが、Cisco IOS CA は現在 1 つの CDP しかサポートしません。ただし、サードパーティ ベンダー製の CA には、証明書ごとに複数の CDP または異なる CDP をサポートするものがあります。CDP が証明書に指定されていない場合、クライアント デバイスは、デフォルトの Simple Certificate Enrollment Protocol（SCEP）方式を使用して CRL を取得します（CDP の場所は、**cdp-url** コマンドを使用して指定できます）。

CRL を実装する際は、次の設計上の注意事項を考慮する必要があります。

- CRL ライフタイムとセキュリティ アソシエーション（SA）およびインターネット キー交換（IKE）ライフタイム
- CRL ライフタイムにより、CA が CRL の更新を発行する時間間隔が決まりますデフォルト CRL ライフタイム値は 168 時間（1 週間）です。これは、**lifetime crl** コマンドで変更できます。
- CDP のこの方式により、CRL の取得方法が決まり、この方式として、HTTP、Lightweight Directory Access Protocol（LDAP）、SCEP、または TFTP を選択できます。最も一般的に使用されている方式は、HTTP、TFTP、および LDAP です。Cisco IOS ソフトウェアでは、SCEP にデフォルト設定されていますが、CRL を使用して大容量のインストールを実行する場合、HTTP CDP を推奨します。HTTP では高いスケーラビリティを実現できるからです。
- CDP のこの場所は、CRL の取得先を決定します。たとえば、サーバーおよび CRL の取得先となるファイル パスを指定できます。

（注） 証明書失効リスト（CRL）を含む Public Key Infrastructure（PKI）が使用されている場合、PKI CRL ファイルのサイズが 200 KB（概算値）以上を超えると、CPU 占有が発生する可能性があります。

失効チェック中にすべての CDP を照会

CDP サーバが要求に返答しない場合、Cisco IOS ソフトウェアはエラーを報告し、その結果、ピアの証明書が拒否されることがあります。証明書に複数の CDP がある場合、証明書が拒否されないようにするために、Cisco IOS ソフトウェアは、証明書に表示されている順序で CDP を使用しようと試みます。ルータは、それぞれの CDP URL またはディレクトリ指定を使用して CRL を取得しようと試みます。ある CDP を使用してエラーが発生すると、次の CDP を使用して試行します。

（注） Cisco IOS Release 12.3(7)T 以前のリリースでは、証明書に 2 つ以上の CDP が含まれていても、Cisco IOS ソフトウェアは、CRL の取得を 1 回だけ試行します。

ヒント　Cisco IOS ソフトウェアは、指示された CDP のいずれかから CRL を取得するためにあらゆる試行を行いますが、CDP応答の遅延によりアプリケーションのタイムアウトを避けるために、HTTP CDP サーバを高速の冗長 HTTP サーバと併用することを推奨します。

OCSP とは

OCSP は、証明書の有効性を判別するために使用されるオンラインのメカニズムであり、失効メカニズムとして次のような柔軟性を備えています。

- OCSP では、証明書ステータスをリアルタイムでチェックできます。
- OCSP を使用すると、ネットワーク管理者は、中央 OCSP サーバーを指定でき、これにより、ネットワーク内のすべてのデバイスにサービスを提供できます。
- また、OCSP により、ネットワーク管理者は、クライアント証明書ごと、またはクライアント証明書のグループごとに複数の OCSP サーバーを柔軟に指定できます。
- OCSP サーバーの検証は通常、ルート CA 証明書または有効な下位 CA 証明書に基づいて実行されますが、外部の CA 証明書または自己署名証明書を使用できるように設定することもできます。外部の CA 証明書または自己署名証明書を使用すると、代替の PKI 階層から OCSP サーバー証明書を発行し、有効にできます。

ネットワーク管理者は、さまざまな CA サーバーから CRL を収集し、更新するように OCSP サーバーを設定できます。ネットワーク内のデバイスは、OCSP サーバーに依存して、ピアごとにCRLを取得してキャッシュすることなく証明書ステータスをチェックできます。ピアは、証明書の失効ステータスをチェックする必要がある場合、OCSP 要求に関して疑わしい証明書のシリアル番号およびオプションの固有識別情報（ナンス）を含むOCSPサーバーにクエリーを送信します。OCSP サーバーは、CRL のコピーを保持して、CA がその証明書を無効として記載しているかどうか判別します。次に、サーバーは、ナンスを含むピアに応答します。応答のナンスがOCSPサーバーからピアによって送信された元のナンスと一致しない場合、応答は無効と見なされ、証明書の検証が失敗します。OCSP サーバーとピア間の対話での帯域幅の消費量は、ほとんどの場合、CRL ダウンロードより少なくなります。

OCSP サーバーが CRL を使用する場合は、CRL 時間の制約事項が適用されます。つまり、追加の証明書失効情報を含む CRL によって新しい CRL が発行されていても、まだ有効な CRL がOCSPサーバーで使用されることがあります。CRL情報を定期的にダウンロードするデバイスが少なくなっているため、CRL ライフタイム値を小さくするか、CRL をキャッシュしないように OCSP サーバーを設定できます。詳細は、OCSP サーバーのマニュアルを参照してください。

OCSP サーバーを使用する場合

PKI に次のいずれかの特性がある場合、CRL よりも OCSP の方が適している場合があります。

- リアルタイムの証明書失効ステータスが必要。CRLが定期的にしか更新されず、必ずしも最新の CRL がクライアント デバイスでキャッシュされていない場合があります。たとえ

ば、最新の CRL がまだクライアントにキャッシュされておらず、また、新たに無効にされた証明書がチェック中の場合は、無効にされた証明書が失効チェックに合格します。

- 無効にされた大量の証明書または複数の CRL があります。大きな CRL をキャッシュすると、Cisco IOS メモリの大部分が消費されてしまい、他のプロセスに使用できるリソースが減少することがあります。
- CRL が頻繁に失効するため、CDP は大量の CRL を処理します。

（注） Cisco IOS Release 12.4(9)T 以降では、管理者は、CRL キャッシングを完全にディセーブルにするか、キャッシュされた CRL のトラストポイントごとに最大ライフタイムを設定することによって、CRL キャッシングを設定できます。

許可または失効用に証明書ベースの ACL を使用する場合

証明書には、指定された処理の実行をデバイスまたはユーザーが許可されているかどうかの判別に使用されるフィールドがいくつか含まれています。

証明書ベース ACL はデバイス上に設定されるため、大量の ACL を十分にスケーリングしません。ただし、証明書ベースの ACL では、特定のデバイスの動作を非常に細かく制御できます。また、証明書ベース ACL は追加機能で活用され、失効、許可、またはトラストポイントなどの PKI コンポーネントを使用するタイミングを判別するのを助けます。証明書ベース ACL は全般的なメカニズムを提供しており、このメカニズムによりユーザーは、許可または追加処理に対して有効になっている特定の証明書または証明書のグループを選択できます。

証明書ベース ACL では、証明書内の 1 つ以上のフィールドおよび指定された各フィールドで許可される値を指定します。証明書内でチェックする必要があるフィールドと、それらのフィールドで認められる値または認められない値を指定できます。

フィールドと値との比較には、6つの論理テスト（Equal（等しい）、Notequal（等しくない）、Contains（含む）、Less than（未満）、Does not contain（含まない）、Greater than or equal（以上））を使用できます。1 つの証明書ベース ACL で複数のフィールドを指定した場合、その ACL と一致するには、ACL 内のすべてのフィールド条件に合致しなければなりません。同じ ACL 内で、同じフィールドを複数回指定できます。複数の ACL を指定できます。一致するものが見つかるか、または ACL の処理がすべて完了するまで、各 ACL が順に処理されます。

証明書ベース ACL を使用した失効チェックの無視

証明書ベース ACL を設定して、有効なピアの失効チェックおよび失効した証明書を無視するようルータに指示できます。したがって、指定基準を満たす証明書は、証明書の有効期間にかかわらず受け入れることができます。また、証明書が指定基準を満たしている場合は失効チェックを実行する必要がなくなります。AAA サーバーとの通信が証明書で保護される場合にも、証明書ベース ACL を使用して失効チェックを無視できます。

失効リストの無視

トラストポイントが特定の証明書を除いて CRL を適用できるようにするには、**skip revocation-check** キーワードを指定して **match certificate** コマンドを入力します。このような適用は、スポークツースポークの直接接続も可能なハブアンドスポーク設定に最も便利です。純粋なハブアンドスポーク設定では、すべてのスポークはハブだけに接続するので、CRL チェックはハブ上だけで済みます。スポークが別のスポークと直接通信する場合、ネイバーピア証明書に対して、各スポーク上で CRL を要求する代わりに、**skip revocation-check** キーワードを指定して **match certificate** コマンドを使用できます。

失効した証明書の無視

失効した証明書を無視するようにルータを設定するには、**allow expired-certificate** キーワードを指定して **match certificate** コマンドを入力します。このコマンドには、次のような目的があります。

- このコマンドは、ピアの証明書が失効した場合にピアが新しい証明書を取得するまで、失効した証明書を「許可する」ために使用できます。
- ルータ クロックがまだ正しい時間に設定されていない場合、クロックが設定されるまで、ピアの証明書はまだ有効ではないものとして表示されます。このコマンドは、ルータ クロックが未設定であっても、ピアの証明書を許可する場合に使用できます。

（注） ネットワーク タイム プロトコル（NTP）が IPSec 接続だけで（通常、ハブアンドスポーク設定のハブによって）利用可能な場合は、ルータ クロックを絶対に設定できません。ハブの証明書がまだ有効でないため、ハブへのトンネルを「アップ」状態にできません。

- 「失効」とは、失効している証明書またはまだ有効ではない証明書の総称です。証明書には、開始時刻と終了時刻が指定されます。ACL を目的とした、失効証明書は、ルータの現在時刻が証明書で指定された開始および終了時刻の範囲外の証明書です。

証明書の AAA チェックのスキップ

AAA サーバーとの通信が証明書で保護され、証明書の AAA チェックをスキップする場合は、**skip authorization-check** キーワードを指定して **match certificate** コマンドを使用します。たとえば、すべての AAA トラフィックがバーチャル プライベート ネットワーク（VPN）トンネルを通過するように設定され、このトンネルが証明書で保護されている場合は、**skip authorization-check** キーワードを指定して **match certificate** コマンドを使用すると、証明書チェックをスキップしてトンネルを確立できます。

AAA サーバーとの PKI 統合が設定されると、**match certificate** コマンドと **skip authorization-check** キーワードを設定する必要があります。

（注） AAA サーバーが IPSec 接続によってのみ使用可能な場合は、IPSec 接続が確立されるまで AAA サーバーとは通信できません。AAA サーバーの証明書がまだ有効でないため、IPSec 接続を「アップ」状態にできません。

PKI 証明書チェーンの検証

証明書チェーンにより、ピア証明書からルート CA 証明書までの、一連の信頼できる証明書を確立します。階層型 PKI 内では、登録されているすべてのピアが信頼できるルート CA 証明書または共通の下位 CA を共有している場合、証明書を相互に検証できます。各 CA が 1 つのトラストポイントに対応します。

証明書チェーンをピアから受信すると、最初の信頼できる証明書またはトラストポイントに到達するまで、証明書チェーン パスのデフォルト処理が続けられます。Cisco IOS Release 12.4(6)T 以降のリリースでは、管理者は、下位 CA 証明書を含むすべての証明書における証明書チェーンの処理レベルを設定できます。

証明書チェーンの処理レベルを設定すると、信頼できる証明書の再認証、信頼できる証明書チェーンの延長、および欠落のある証明書チェーンの補完が可能になります。

信頼できる証明書の再認証

このデフォルト動作でルータは、チェーンを検証する前に、ピアによって送信された証明書チェーンから任意の信頼できる証明書を削除します。管理者は証明書チェーン パス処理を設定して、チェーン検証の前にすでに信頼されている CA 証明書をルータが削除しないようにできます。そのため、チェーン内のすべての証明書は現在のセッションに対して再度認証されます。

信頼できる証明書チェーンの延長

このデフォルト動作でルータは、ピアによって送信された証明書チェーンに欠落している証明書がある場合、その信頼できる証明書を使用して証明書チェーンを延長します。ルータが検証するのは、ピアによって送信されたチェーンの証明書だけです。管理者は証明書チェーン パス処理を設定して、ピアの証明書チェーンの証明書およびルータの信頼できる証明書を、指定したポイントに対して有効にできます。

証明書チェーンの欠落の補完

管理者は証明書チェーン処理を設定して、設定済みの Cisco IOS トラストポイント階層に欠落がある場合、ピアによって送信された証明書を使用して証明書のセットを有効にできます。

（注） 親検証を要求するようにトラストポイントが設定され、ピアが完全な証明書チェーンを提示しない場合、欠落を補完できないため証明書チェーンは拒否され、無効になります。

（注） 親検証を要求するようにトラストポイントが設定されていて、設定済みの親トラストポイントがない場合は、設定エラーです。発生する証明書チェーンの欠落を補完できず、下位 CA 証明書を有効にできません。この証明書チェーンは無効です。

PKI に対して証明書の許可および失効を設定する方法

AAA サーバーとの PKI 統合の設定

ピアによって提出された証明書から AAA ユーザー名を生成し、証明書内で AAA データベース ユーザー名の作成に使用するフィールドを指定するには、次の作業を実行します。

（注） **authorization username** コマンドでサブジェクト名として **all** キーワードを使用する際に、次の制約事項を考慮する必要があります。

- 一部のAAAサーバーでは、ユーザー名の長さが制限されます（たとえば、64文字まで）。その結果、証明書の全体のサブジェクト名は、サーバーの制約条件より長くできません。
- 一部の AAA サーバーでは、ユーザー名に使用できる文字セットが制限されます（たとえば、スペース（ ）および等号（=）を使用できない場合があります）。このような文字セットの制限がある AAA サーバーでは、**all** キーワードを使用できません。
- トラストポイント設定の **subject-name** コマンドは、必ずしも最終の AAA サブジェクト名とは限りません。証明書要求に完全修飾ドメイン名（FQDN）、シリアル番号、またはルータの IP アドレスが含まれている場合は、発行された証明書のサブジェクト名フィールドにもこれらのコンポーネントが含まれます。コンポーネントをオフにするには、**fqdn**、**serial-number**、および **ip-address** の各コマンドに **none** キーワードを使用します。
- CA サーバーが証明書を発行すると、CA サーバーは、要求したサブジェクト名フィールドを変更することがあります。たとえば、一部のベンダーの CA サーバーが要求したサブジェクト名の相対識別名（RDN）を CN、OU、O、L、ST、および C に切り替えます。ただし、別の CA サーバーは、設定した LDAP ディレクトリ ルート（O=cisco.com など）を要求したサブジェクト名の最後に追加する場合があります。
- 証明書の表示用に選択するツールによっては、サブジェクト名の RDN の印刷順序が異なることがあります。Cisco IOS ソフトウェアでは、重要度が最低の RDN を先頭に表示しますが、Open Source Secure Socket Layer（OpenSSL）などの、他のソフトウェアでは、重要度が最高の RDN を先頭に表示します。したがって、完全な識別名（DN）（サブジェクト名）を持つ AAA サーバーを対応するユーザー名として設定する場合は、Cisco IOS ソフトウェア スタイル（つまり、重要度が最低の RDN を先頭に表示）が使用されていることを確認してください。

または

radius-server host *hostname* [**key** *string*]

手順の概要

1. **enable**
2. **configure terminal**
3. **aaa new-model**
4. **aaa authorization network** *listname* [*method*]
5. **crypto pki trustpoint** *name*
6. **enrollment** [**mode**] [**retry period** *minutes*] [**retry count** *number*] **url** *url* [**pem**]
7. revocation-check method
8. **exit**
9. **authorization username subjectname** *subjectname*
10. **authorization list** *listname*

11. **tacacs-server host** hostname [**key** string]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**aaa new-model** 例： `Router(config)# aaa new-model`	AAAアクセス コントロール モデルをイネーブルにします。
ステップ 4	**aaa authorization network** *listname* [*method*] 例： `Router (config)# aaa authorization network maxaaa group tacacs+`	ネットワークへのユーザー アクセスを制限するパラメータを設定します。 • *method* ：**group radius**、**group tacacs+**、または **group group-name** を指定できます。
ステップ 5	**crypto pki trustpoint** *name* 例： `Route (config)# crypto pki trustpoint msca`	トラストポイントおよび設定された名前を宣言して、CA トラストポイント コンフィギュレーション モードを開始します。

ステップ 6	**enrollment** [**mode**] [**retry period** *minutes*] [**retry count** *number*] **url** *url* [**pem**]
	例：
	`Router (ca-trustpoint)# enrollment url http://caserver.myexample.com`
	または
	`Router (ca-trustpoint)# enrollment url http://[2001:DB8:1:1::1]:80`
		CA の次の登録パラメータを指定します。
		• （任意）CA システムが登録局（RA）を提供する場合、**mode** キーワードとして RA モードを指定します。デフォルトでは、RA モードは無効です。
		• （任意）**retry period** キーワードおよび *minutes* 引数は、CA に別の証明書要求を送信するまでルータが待機する期間を分単位で指定します。有効値は 1 ～ 60 です。デフォルトは 1 です。
		• （任意）**retry count** キーワードおよび *number* 引数は、直前の要求に対する応答をルータが受信しない場合、ルータが証明書要求を再送信する回数を指定します。有効な値は、1 ～ 100 です。デフォルトは 10 です。

	コマンドまたはアクション	目的
		• *url* 引数は、ルータが証明書要求を送信する CA の URL です。 （注） Cisco IOS リリース 15.2(1)T を導入すると、IPv6 アドレスを **http:** 登録方式に追加できます。たとえば、http://[ipv6-address]:80 です。URL 内の IPv6 アドレスは括弧で囲む必要があります。使用できるその他の登録方式に関する詳細については、コマンドリファレンスマニュアルを参照してください。 • （任意）**pem** キーワードは、証明書要求にプライバシー強化メール（PEM）の境界を追加します。
ステップ 7	revocation-check method 例： `Router (ca-trustpoint)# revocation-check crl`	（任意）証明書の失効ステータスをチェックします。
ステップ 8	**exit** 例： `Router (ca-trustpoint)# exit`	CA トラストポイント コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードに戻ります。
ステップ 9	**authorization username subjectname** *subjectname* 例： `Router (config)# authorization username subjectname serialnumber`	AAA ユーザー名の構築に使用する異なる証明書フィールドのパラメータを設定します。 *subjectname* 引数には、次のいずれかを指定できます。 • **all**：証明書の識別名（所有者名）全体。 • **commonname**：証明書の共通名。 • **country**：証明書の国。 • **email**：証明書の電子メール。 • **ipaddress**：証明書の IP アドレス。 • **locality**：証明書の地域。 • **organization**：証明書の組織。 • **organizationalunit**：証明書の組織単位。

	コマンドまたはアクション	目的
		• **postalcode**：証明書の郵便番号。 • **serialnumber**：証明書のシリアル番号。 • **state**：証明書の州フィールド。 • **streetaddress**：証明書の住所。 • **title**：証明書のタイトル。 • **unstructuredname**：証明書の非公式名。
ステップ 10	**authorization list** *listname* 例： `Route (config)# authorization list maxaaa`	AAA 認可リストを指定します。

ステップ 11	**tacacs-server host** hostname [**key** string]
	例：
	`Router(config)# tacacs-server host 192.0.2.2 key a_secret_key`
	例：
	`radius-server host hostname [key string]`
	例：
	`Router(config)# radius-server host 192.0.2.1 key another_secret_key`
		TACACS+ ホストを指定します。
		または
		RADIUS ホストを指定します。

トラブルシューティングのヒント

CA とルータ間のインタラクションのトレース（メッセージタイプ）に関するデバッグメッセージを表示するには、**debug crypto pki transactions** コマンドを使用します（サンプル出力を参照してください。ここでは、AAA サーバー交換との成功した PKI 統合、および AAA サーバー交換との失敗した PKI 統合を示します）。

成功した交換

```
Router# debug crypto pki transactions
Apr 22 23:15:03.695: CRYPTO_PKI: Found a issuer match
Apr 22 23:15:03.955: CRYPTO_PKI: cert revocation status unknown.
Apr 22 23:15:03.955: CRYPTO_PKI: Certificate validated without revocation check
```

「CRYPTO_PKI_AAA」と表示されている各行は、AAA 認可チェックの状態を示します。各 AAA AV ペアが示され、認可チェックの結果が表示されます。

```
Apr 22 23:15:04.019: CRYPTO_PKI_AAA: checking AAA authorization (ipsecca_script_aaalist,
```

```
 PKIAAA-L, <all>)
Apr 22 23:15:04.503: CRYPTO_PKI_AAA: reply attribute ("cert-application" = "all")
Apr 22 23:15:04.503: CRYPTO_PKI_AAA: reply attribute ("cert-trustpoint" = "CA1")
Apr 22 23:15:04.503: CRYPTO_PKI_AAA: reply attribute ("cert-serial" = "15DE")
Apr 22 23:15:04.503: CRYPTO_PKI_AAA: authorization passed
Apr 22 23:12:30.327: CRYPTO_PKI: Found a issuer match
```

失敗した交換

```
Router# debug crypto pki transactions
Apr 22 23:11:13.703: CRYPTO_PKI_AAA: checking AAA authorization =
Apr 22 23:11:14.203: CRYPTO_PKI_AAA: reply attribute ("cert-application" = "all")
Apr 22 23:11:14.203: CRYPTO_PKI_AAA: reply attribute ("cert-trustpoint"= "CA1")
Apr 22 23:11:14.203: CRYPTO_PKI_AAA: reply attribute ("cert-serial" = "233D")
Apr 22 23:11:14.203: CRYPTO_PKI_AAA: parsed cert-lifetime-end as: 21:30:00
Apr 22 23:11:14.203: CRYPTO_PKI_AAA: timezone specific extended
Apr 22 23:11:14.203: CRYPTO_PKI_AAA: cert-lifetime-end is expired
Apr 22 23:11:14.203: CRYPTO_PKI_AAA: cert-lifetime-end check failed.
Apr 22 23:11:14.203: CRYPTO_PKI_AAA: authorization failed
```

上記の失敗した交換では、証明書が失効しています。

PKI 証明書ステータス チェックの失効メカニズムの設定

証明書失効メカニズム（CRL またはOCSP）としてCRL を設定し、PKI の証明書のステータスをチェックするには、次の作業を実行します。

revocation-check コマンド

revocation-check コマンドを使用し、ピアの証明書が無効にされていないことを確認するための方式（OCSP、CRL、または失効チェックのスキップ）を少なくとも 1 つ指定します。複数の方式を指定する場合、方式を適用する順序は、このコマンドで指定した順序になります。

ルータに適用可能な CRL がなく、いずれの CRL も取得できない場合、あるいは OCSP サーバーがエラーを返す場合、設定に **none** キーワードを含めないかぎり、ルータはピアの証明書を拒否します。**none** キーワードを設定した場合、失効チェックは実行されず、証明書は常に受け入れられます。

（注） トラストポイントで失効チェックが「none」に変更されると、トラストポイントの CA 証明書に関連付けられている CRL キャッシュがクリアされます。

OCSP サーバーとのナンスおよびピア通信

OCSP を使用すると、OCSP サーバーとのピア通信時に、OCSP 要求に関するナンス（固有識別情報）がデフォルトで送信されます。ナンスを使用することにより、ピアと OCSP サーバー間にセキュアで信頼性の高い通信チャネルが確立されます。

OCSP サーバーがナンスをサポートしていない場合は、ナンスの送信をディセーブルにできます。詳細は、OCSP サーバのマニュアルを参照してください。

始める前に

- クライアント証明書を発行する前に、サーバーで適切な設定（CDP の設定など）を行う必要があります。
- OCSP サーバーから CA サーバーの失効ステータスを返すように設定するときは、CA サーバーが発行した OCSP 応答署名証明書を OCSP サーバーに設定する必要があります。署名証明書が正しいフォーマットであることを確認してください。署名証明書のフォーマットが正しくない場合、ルータは、OCSP 応答を受理しません。詳細については、OCSP のマニュアルを参照してください。

（注）
- OCSP は、HTTP を使用してメッセージを転送するので、OCSP サーバーにアクセスする際に遅延が発生する場合があります。
- OCSP サーバーが、失効ステータスのチェックを通常の CRL 処理に依存している場合、CRL の遅延は OCSP にも適用されます。

>

手順の概要

1. **enable**
2. **configure terminal**
3. crypto pki trustpoint *name*
4. **ocsp url** *url*
5. **revocation-check** *method1* [*method2 method3*]]
6. **ocsp disable-nonce**
7. **exit**
8. **exit**
9. **show crypto pki certificates**
10. **show crypto pki trustpoints** [**status** | *label* [**status**]]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 3	crypto pki trustpoint *name* 例： `Router(config)# crypto pki trustpoint hazel`	トラストポイントおよび設定された名前を宣言して、CA トラストポイント コンフィギュレーション モードを開始します。

ステップ 4	**ocsp url** *url*
	例：
	`Router(ca-trustpoint)# ocsp url http://ocsp-server`
	または
	`Router(ca-trustpoint)# ocsp url http://10.10.10.1:80`
	または
	`Router(ca-trustpoint)# ocsp url http://[2001DB8:1:1::2]:80`
		url 引数は、トラストポイントが証明書ステータスをチェックできるように OCSP サーバーの URL を指定します。この URL は、証明書の AIA 拡張部に指定されている OCSP サーバーの URL（存在する場合）を上書きします。設定したトラストポイントに関連するすべての証明書は、OCSP サーバーによって確認されます。使用可能な URL は、ホスト名、IPv4 アドレス、または IPv6 アドレスです。

ステップ 5	**revocation-check** *method1* [*method2 method3*]] 例： `Router(ca-trustpoint)# revocation-check ocsp none`	証明書の失効ステータスをチェックします。 • **crl**：CRL によって証明書をチェックします。これがデフォルトのオプションです。 • **none**：証明書のチェックを無視します。 • **ocsp**：OCSP サーバーによって証明書をチェックします。 2 番目と 3 番目の方法を指定した場合、各方法はその直前の方法でエラーが返された場合（サーバーがダウンしている場合など）にだけ使用されます。
ステップ 6	**ocsp disable-nonce** 例： `Router(ca-trustpoint)# ocsp disable-nonce`	（任意）OCSP サーバーとピアが通信するときに、ナンス（OCSP 要求に関する固有識別情報）が送信されないように指定します。
ステップ 7	**exit** 例： `Router(ca-trustpoint)# exit`	グローバル コンフィギュレーション モードに戻ります。
ステップ 8	**exit** 例： `Router(config)# exit`	特権 EXEC モードに戻ります。

	コマンドまたはアクション	目的
ステップ 9	**show crypto pki certificates** 例： `Router# show crypto pki certificates`	（任意）証明書に関する情報を表示します。
ステップ 10	**show crypto pki trustpoints** [**status** | *label* [**status**]] 例： `Router# show crypto pki trustpoints`	ルータに設定されているトラストポイントに関する情報を表示します。

証明書の許可および失効の設定

証明書ベース ACL の指定、失効チェックまたは失効した証明書の無視、手動によるデフォルトの CDP の場所の上書き、手動による OCSP サーバー設定の上書き、CRL キャッシングの設定、あるいは証明書シリアル番号に基づくセッションの受理/拒否の設定を行うには、必要に応じて次の作業を実行します。

失効チェックを無視するように証明書ベース ACL を設定

証明書ベース ACL を使用して、失効チェックおよび失効証明書を無視するようにルータを設定するには、次の手順を実行します。

- 既存のトラストポイントの識別またはピアの証明書の検証に使用される新しいトラストポイントを作成します。トラストポイントがまだ認証されていない場合は、認証してください。必要に応じて、ルータをこのトラストポイントに登録できます。**match certificate** コマンドと **skip revocation-check** キーワードを使用する場合は、トラストポイントにオプションの CRL を設定しないでください。
- 証明書自体の CRL をチェックする必要がない証明書の固有の特性と、許可する必要がある失効証明書の固有の特性を判別します。
- 前のステップで確認した特性と一致する証明書マップを定義します。
- 最初の手順で作成または指定したトラストポイントに、**match certificate** コマンドと **skip revocation-check** キーワード、**match certificate command**と **allow expired-certificate** キーワードを追加できます。

（注） 証明書マップは、ピアの公開キーがキャッシュされている場合でも確認されます。たとえば、ピアによって公開キーがキャッシュされており、証明書マップがトラストポイントに追加されて証明書が禁止されると、証明書マップが有効になります。これにより、過去に一度接続され、現在は禁止されている証明書を持つクライアントが再接続することを防ぎます。

証明書内の CDP の手動による上書き

ユーザーは、手動で設定した CDP で証明書内の CDP を上書きできます。証明書の CDP の手動による上書きは、特定のサーバーが長時間利用できない場合に便利です。元の CDP を含む証明書のすべてを再発行しなくても、証明書の CDP を URL またはディレクトリ指定に置き換えることができます。

手動による証明書の OCSP サーバー設定の上書き

管理者はクライアント証明書の Authority Information Access（AIA）フィールドに指定された、または **ocsp url** コマンドを発行して設定された OCSP サーバーの設定値を上書きできます。**match certificate override ocsp** コマンドを使用すると、1 つまたは複数の OCSP サーバーをクライアント証明書ごとに、またはクライアント証明書のグループごとに手動で指定できます。失効チェック時にクライアント証明書が証明書マップに正常に照合された場合、**match certificate override ocsp** コマンドを発行すると、クライアント証明書 AIA フィールドまたは **ocsp url** コマンド設定が上書きされます。

（注） 1 つのクライアント証明書には、OCSP サーバーを 1 つだけ指定できます。

CRL キャッシュ コントロールの設定

デフォルトでは、現在キャッシュされている CRL が失効すると、新しい CRL がダウンロードされます。管理者は、**crl cache delete-after** コマンドを発行して、CRL がキャッシュに保持される最大時間（分単位）を設定するか、**crl cache none** コマンドを発行して CRL キャッシュを無効にできます。**crl-cache delete-after** コマンドまたは **crl-cache none** コマンドのみを指定できます。トラストポイントに両方のコマンドを入力した場合は、後に実行されたコマンドが有効になり、メッセージが表示されます。

crl-cache none コマンドまたは **crl-cache delete-after** コマンドのいずれを実行しても現在キャッシュされている CRL に影響はありません。**crl-cache none** コマンドを設定した場合、このコマンドを発行すると、ダウンロードされたすべての CRL はキャッシュされません。**crl-cache delete-after** コマンドを設定した場合、このコマンドの発行後に設定されたライフタイムだけがダウンロードされた CRL に影響します。

この機能は、CA が失効日を指定せずに CRL を発行する場合、あるいは失効日が数日後または数週間後に迫っている場合に役立ちます。

証明書のシリアル番号セッション コントロールの設定

証明書検証要求がセッションのトラストポイントによって受け入れられる、または拒否されるように証明書シリアル番号を指定できます。証明書のシリアル番号セッション コントロールによっては、証明書がまだ有効であっても、セッションが拒否される場合があります。証明書のシリアル番号セッションコントロールは、**serial-number** フィールドを持つ証明書マップまたは AAA 属性のいずれかを使用して **cert-serial-not** コマンドで設定できます。

セッション コントロールに証明書マップを使用すると、管理者は、1 つの証明書シリアル番号を指定できます。AAA 属性を使用すると、管理者は、セッション コントロールに証明書シリアル番号を指定できます。

始める前に

- 証明書マップをトラストポイントに関連付ける前に、トラストポイントを定義し、認証する必要があります。
- CDP オーバライド機能を有効にする、または **serial-number** コマンドを発行する前に、証明書マップを設定する必要があります。
- PKI と AAA サーバーとの統合は、「証明書ステータスのための PKI と AAA サーバーの統合」の説明のとおりに AAA 属性を使用して正常に完了する必要があります。

手順の概要

1. **enable**
2. **configure terminal**
3. crypto pki certificate map label sequence-number
4. *field-name match-criteria match-value*
5. **exit**
6. **crypto pki trustpoint** *name*
7. 次のいずれかを実行します。
   - **crl-cache none**
   - **crl-cache delete-after** *time*
8. **match certificate** *certificate-map-label* [**allow expired-certificate** | **skip revocation-check** | **skip authorization-check**
9. **match certificate** *certificate-map-label* **override cdp** {**url** | **directory**} *string*
10. **match certificate** *certificate-map-label* **override ocsp** [**trustpoint** *trustpoint-label*] *sequence-number* **url** *ocsp-url*
11. **exit**
12. **aaa new-model**
13. **aaa attribute list** *list-name*
14. **attribute type** {*name*}{*value*}
15. **exit**
16. **exit**
17. **show crypto pki certificates**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例：	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。

	コマンドまたはアクション	目的
	`Router> enable`	
ステップ 2	**configure terminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	crypto pki certificate map label sequence-number 例： `Router(config)# crypto pki certificate map Group 10`	証明書において、一致する必要がある値または一致する必要がない値を定義し、CA 証明書マップ コンフィギュレーション モードを開始します。
ステップ 4	*field-name match-criteria match-value* 例： `Router(ca-certificate-map)# subject-name co MyExample`	1 つまたは複数の証明書フィールドと、これらのフィールドの一致基準および照合する値を指定します。 *field-name* には、次のいずれかの名前文字列（大文字と小文字を区別しない）または日付を指定します。 • **alt-subject-name** • **expires-on** • **issuer-name** • **name** • **serial-number** • **subject-name** • **unstructured-subject-name** • **valid-start** （注） 日付フィールドのフォーマットは、dd mm yyyy hh:mm:ss または mmm dd yyyy hh:mm:ss です。 *match-criteria* には、次の論理演算子のいずれかを指定します。 • **co**：含む（名前およびシリアル番号フィールドでのみ有効） • **eq**：等しい（名前、シリアル番号、および日付フィールドで有効） • **ge**：以上（日付フィールドでのみ有効）

	コマンドまたはアクション	目的
		• **lt**：未満（日付フィールドでのみ有効） • **nc**：含まない（名前およびシリアル番号フィールドでのみ有効） • **ne**：等しくない（名前、シリアル番号、および日付フィールドで有効） *match-value* は、match-criteria で割り当てられた論理演算子を使用してテストする名前または日付です。 （注） このコマンドは、証明書ベース ACL を設定する場合にだけ使用し、失効チェックまたは失効した証明書を無視するように証明書ベース ACL を設定する場合には使用しないでください。
ステップ 5	**exit** 例： `Router(ca-certificate-map)# exit`	グローバル コンフィギュレーション モードに戻ります。
ステップ 6	**crypto pki trustpoint** *name* 例： `Router(config)# crypto pki trustpoint Access2`	トラストポイントおよび設定された名前を宣言して、CA トラストポイント コンフィギュレーション モードを開始します。

ステップ 7	次のいずれかを実行します。
	• **crl-cache none**
	• **crl-cache delete-after** *time*
	例：
	`Router(ca-trustpoint)# crl-cache none`
	例：
	`Router(ca-trustpoint)# crl-cache delete-after 20`
		（任意）トラストポイントに関連付けられたすべての CRL の CRL キャッシングを完全にディセーブルにします。
		crl-cache none コマンドを実行しても、現在キャッシュされている CRL に影響はありません。このコマンドが設定された後にダウンロードされるすべての CRL は、キャッシュされません。
		（任意）トラストポイントに関連付けられたすべての CRL に関して、CRL がキャッシュに保持される最大時間を指定します。
		• *time*：CRL が削除されるまでの時間（分単位）。
		crl-cache delete-after コマンドを実行しても、現在キャッシュされている CRL に影響はありません。設定されたライフタイムは、このコマンドが設定さ

	コマンドまたはアクション	目的
		れた後にダウンロードされた CRL だけに影響します。
ステップ 8	**match certificate** *certificate-map-label* [**allow expired-certificate** | **skip revocation-check** | **skip authorization-check** 例： `Router(ca-trustpoint)# match certificate Group skip revocation-check`	（任意）証明書ベース ACL（**crypto pki certificate map** コマンドによって定義されている）をトラストポイントに関連付けます。 • *certificate-map-label*：**crypto pki certificate map** コマンドを使用して指定した *label* 引数と一致する必要があります。 • **allowexpired-certificate**：失効した証明書を無視します。 • **skip revocation-check**：トラストポイントが、特定の証明書を除く CRL を適用できるようにします。 • **skip authorization-check**：AAA サーバーとの PKI 統合を設定すると、証明書の AAA チェックをスキップします。
ステップ 9	**match certificate** *certificate-map-label* **override cdp** {**url** | **directory**} *string* 例： `Router(ca-trustpoint)# match certificate Group1 override cdp url http://server.cisco.com`	（任意）URL またはディレクトリが指定された証明書の、既存の CDP エントリを手動で上書きします。 • *certificate-map-label*：ユーザー指定のラベル。事前に定義された **crypto pki certificate map** コマンドに指定した *label* 引数と一致する必要があります。 • **url**：証明書の CDP が HTTP または LDAP URL で上書きされるように指定します。 • **directory**：証明書の CDP が LDAP ディレクトリ指定で上書きされるように指定します。 • *string*：URL またはディレクトリ指定。 （注） 一部のアプリケーションは、すべての CDP が試行される前にタイムアウトすることがあり、エラー メッセージで報告します。エラー メッセージはルータに影響を及ぼしません。また、Cisco IOS ソフトウェアは、すべての CDP が試行されるまで CRL の取得を続行します。

	コマンドまたはアクション	目的
ステップ 10	**match certificate** *certificate-map-label* **override ocsp** [**trustpoint** *trustpoint-label*] *sequence-number* **url** *ocsp-url* 例： `Router(ca-trustpoint)# match certificate mycertmapname override ocsp trustpoint mytp 15 url http://192.0.2.2`	（任意）OCSP サーバーをクライアント証明書ごとに、またはクライアント証明書のグループごとに指定し、複数回発行して、追加の OCSP サーバーおよびクライアント証明書の設定（代替の PKI 階層を含む）を指定できます。 • *certificate-map-label*：既存の証明書マップ名。 • **trustpoint**：OCSP サーバー証明書を検証するときに使用されるトラストポイント。 • *sequence-number*：**match certificate override ocsp** コマンドステートメントを検証対象の証明書に適用する順序。照合が最低のシーケンス番号から最高のシーケンス番号に実行されます。同じシーケンス番号で複数のコマンドを発行すると、前の OCSP サーバー オーバライド設定が上書きされます。 • **url**：OCSP サーバーの URL。 証明書が設定された証明書マップと一致すると、クライアント証明書の AIA フィールドおよび以前に発行された **ocsp url** コマンド設定値は、指定された OCSP サーバーで上書きされます。 マップベースの一致が発生しない場合、引き続き次の 2 つのケースがクライアント証明書に適用されます。 • OCSP を失効方法として指定すると、AIA フィールド値がクライアント証明書に引き続き適用されます。 • **ocsp url** 設定が存在する場合は、**ocsp url** 設定が引き続きクライアント証明書に適用されます。
ステップ 11	**exit** 例： `Router(ca-trustpoint)# exit`	グローバル コンフィギュレーション モードに戻ります。
ステップ 12	**aaa new-model** 例： `Router(config)# aaa new-model`	（任意）AAA アクセス コントロール モデルをイネーブルにします。

	コマンドまたはアクション	目的
ステップ 13	**aaa attribute list** *list-name* 例： `Router(config)# aaa attribute list crl`	（任意）ルータにローカルで AAA 属性リストを定義し、config-attr-list コンフィギュレーション モードを開始します。
ステップ 14	**attribute type** {*name*} {*value*} 例： `Router(config-attr-list)# attribute type cert-serial-not 6C4A`	（任意）ルータの AAA 属性リストにローカルに追加される AAA 属性タイプを定義します。 証明書のシリアル番号セッションコントロールを設定するために、管理者は、*value* フィールドの特定の証明書を、*name* が **cert-serial-not** に設定されているシリアル番号に基づき受け入れるか、拒否するか指定できます。証明書のシリアル番号が属性タイプ設定で指定されたシリアル番号と一致した場合、証明書は拒否されます。 使用可能な AAA 属性タイプのリストを表示するには、**show aaa attributes** コマンドを実行してください。

ステップ 15	**exit**
	例：
	`Router(ca-trustpoint)# exit`
	例：
	`Router(config-attr-list)# exit`
		グローバル コンフィギュレーション モードに戻ります。

ステップ 16	**exit** 例： `Router(config)# exit`	特権 EXEC モードに戻ります。
ステップ 17	**show crypto pki certificates** 例： `Router# show crypto pki certificates`	（任意）CA 証明書が認証されたら、ルータにインストールされた証明書のコンポーネントを表示します。

例

次に、サンプル証明書を示します。OCSP 関連の拡張子は感嘆符を使用して示されます。

```
Certificate:
        Data:
```

```
            Version: v3
            Serial Number:0x14
            Signature Algorithm:SHAwithRSA - 1.2.840.113549.1.1.4
            Issuer:CN=CA server,OU=PKI,O=Cisco Systems
            Validity:
                Not Before:Thursday, August 8, 2002 4:38:05 PM PST
                Not After:Tuesday, August 7, 2003 4:38:05 PM PST
            Subject:CN=OCSP server,OU=PKI,O=Cisco Systems
            Subject Public Key Info:
                Algorithm:RSA - 1.2.840.113549.1.1.1
                Public Key:
                    Exponent:65537
                    Public Key Modulus:(2048 bits) :
                        <snip>
            Extensions:
                Identifier:Subject Key Identifier - 2.5.29.14
                    Critical:no
                    Key Identifier:
                        <snip>
                Identifier:Authority Key Identifier - 2.5.29.35
                    Critical:no
                    Key Identifier:
                        <snip>
!                Identifier:OCSP NoCheck:- 1.3.6.1.5.5.7.48.1.5
                     Critical:no
                Identifier:Extended Key Usage:- 2.5.29.37
                     Critical:no
                     Extended Key Usage:
                     OCSPSigning
!
                Identifier:CRL Distribution Points - 2.5.29.31
                    Critical:no
                    Number of Points:1
                    Point 0
                        Distribution Point:
[URIName:ldap://CA-server/CN=CA server,OU=PKI,O=Cisco Systems]
        Signature:
            Algorithm:SHAwithRSA - 1.2.840.113549.1.1.4
            Signature:
            <snip>
```

次の例は、既存のシーケンスの先頭に **match certificate override ocsp** コマンドを追加したときの実行コンフィギュレーション出力の抜粋を示します。

```
match certificate map3 override ocsp 5 url http://192.0.2.3/
show running-configuration
.
.
.
        match certificate map3 override ocsp 5 url http://192.0.2.3/
        match certificate map1 override ocsp 10 url http://192.0.2.1/
        match certificate map2 override ocsp 15 url http://192.0.2.2/
```

次の例は、既存の **match certificate override ocsp** コマンドが置き換えられ、トラストポイントが代替のPKI階層を使用するように指定された場合の、実行コンフィギュレーション出力の抜粋を示します。

```
match certificate map4 override ocsp trustpoint tp4 10 url http://192.0.2.4/newvalue
show running-configuration
.
.
.
```

```
        match certificate map3 override ocsp trustpoint tp3 5 url http://192.0.2.3/
        match certificate map1 override ocsp trustpoint tp1 10 url http://192.0.2.1/
        match certificate map4 override ocsp trustpoint tp4 10 url
http://192.0.2.4/newvalue
        match certificate map2 override ocsp trustpoint tp2 15 url http://192.0.2.2/
```

トラブルシューティングのヒント

失効チェックまたは失効した証明書を無視した場合は、慎重に設定を確認する必要があります。証明書マップが、当該の証明書または許可する証明書、あるいはスキップするAAAチェックのいずれかと適切に一致していることを確認してください。管理された環境で、証明書マップを変更して想定どおりに機能していないものを判別します。

証明書チェーンの設定

ピア証明書の証明書チェーン パスに処理レベルを設定するには、次の作業を実行します。

始める前に

- デバイスを PKI 階層に登録する必要があります。
- 適切なキー ペアを証明書に関連付ける必要があります。

（注）
- ルート CA に関連付けられたトラストポイントは、次のレベルに対して有効になるように設定できません。

chain-validation コマンドは、ルート CA に関連付けられたトラストポイント用に **continue** キーワードを指定して設定します。エラーメッセージが表示され、チェーン検証はデフォルトの **chain-validation** コマンド設定に戻ります。

手順の概要

1. **enable**
2. **configure terminal**
3. crypto pki trustpoint *name*
4. **chain-validation** [{**stop** | **continue**} [*parent-trustpoint*]]
5. **exit**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。

	コマンドまたはアクション	目的
ステップ 2	**configure terminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	crypto pki trustpoint *name* 例： `Router(config)# crypto pki trustpoint ca-sub1`	トラストポイントおよび設定された名前を宣言して、CA トラストポイント コンフィギュレーション モードを開始します。
ステップ 4	**chain-validation** [{**stop** | **continue**} [*parent-trustpoint*]] 例： `Router(ca-trustpoint)# chain-validation continue ca-sub1`	証明書チェーンが、すべての証明書（下位 CA 証明書を含む）で処理されるレベルを設定します。 • **stop** キーワードを使用して、証明書がすでに信頼できることを明示します。これがデフォルトの設定です。 • **continue** キーワードを使用して、トラストポイントに関連付けられた下位 CA 証明書を有効にする必要があることを明示します。 • *parent-trustpoint* 引数は、証明書を照合する必要がある親トラストポイント名を指定します。
ステップ 5	**exit** 例： `Router(ca-trustpoint)# exit`	グローバル コンフィギュレーション モードに戻ります。

CRL 自動ダウンロードの設定

証明書失効リスト（CRL）の自動ダウンロードを設定するには、次の手順を実行します。

この機能を不適切に設定すると、デバイスによってすでにキャッシュされている CRL の過剰な CRL ダウンロードが発生し、CRL ダウンロードと CRL 検証を並行して実行できないために、検証が停止する可能性があります。CRL がすでにダウンロードされている場合は、追加の CRL をダウンロードせずに、ダウンロード済みの CRL を証明書の検証に使用できます。

crl-cache none コマンドを設定すると、トラストポイントの CRL を自動ダウンロードできません。CRL をダウンロードするには、**no crl cache none** コマンドを実行してトラストポイントから CRL キャッシュを削除します。同様に、CRL ダウンロードが設定されている場合は、**crl-cache none** コマンドを有効にできません。

手順の概要

1. **enable**

2. **configure terminal**
3. **crypto pki crl download url** *url* [**source-interface** *interface-name* | **vrf** *vrf-name*]
4. **crypto pki crl download trustpoint** *trustpoint-label*
5. **crypto pki crl download schedule time** *day hh*:*ss*
6. **crypto pki crl download schedule prepublish** *minutes*
7. **crypto pki crl download schedule retries** *number* **crypto pki crl download schedule retries interval** *minutes*
8. **end**
9. **crypto pki crl refresh-cache**
10. **show crypto pki crl download**
11. **show crypto pki timers**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**crypto pki crl download url** *url* [**source-interface** *interface-name* | **vrf** *vrf-name*] 例： `Device(config)# crypto pki crl download url www.abc.com source-interface GigabitEthernet 1`	CRL 自動ダウンロードで、送信元インターフェイスと VRF のいずれかまたは両方を介して CRL を取得する必要があることを指定します。
ステップ 4	**crypto pki crl download trustpoint** *trustpoint-label* 例： `Device(config)# crypto pki crl download trustpoint trp1`	CRL 自動ダウンロードで、CRL 分散ポイント（CDP）を、そのトラストポイントに関連付けられたデバイス証明書から取得する必要があることを指定します。
ステップ 5	**crypto pki crl download schedule time** *day hh*:*ss* 例： `Device(config)# crypto pki crl download schedule time Monday 00:00`	CRL 自動ダウンロードをトリガーする必要がある日時を指定します。 • *time*：CRL が見つからない場合に CRL をダウンロードする正確な日時を示します。時間と分の形式（*mm*:*ss*）で指定する必要があります。
ステップ 6	**crypto pki crl download schedule prepublish** *minutes* 例： `Device(config)# crypto pki crl download schedule prepublish 720`	CRL が期限切れになる前に CRL をダウンロードする時間間隔（分単位）。デフォルト値は 0 です。

	コマンドまたはアクション	目的
ステップ 7	**crypto pki crl download schedule retries** *number* **crypto pki crl download schedule retries interval** *minutes* 例： `Device(config)# crypto pki crl download schedule retries 15 interval 15 crypto pki crl download schedule retries 15 interval 15`	前のダウンロード試行が失敗した場合に、デバイスが CDP ロケーションからの CRL のダウンロードを再試行する時間間隔（分単位）を指定します。デフォルトの再試行回数は 5 回です。 • **interval** *minutes*：再試行の時間間隔（分単位）。デフォルトの試行間隔は 30 分です。
ステップ 8	**end** 例： `Device(config)# end`	グローバル コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。
ステップ 9	**crypto pki crl refresh-cache** 例： `Device# crypto pki crl refresh-cache`	キャッシュ内の CRL エントリを更新します。
ステップ 10	**show crypto pki crl download** 例： `Device# show crypto pki crl download`	自動ダウンロードの設定を表示します。
ステップ 11	**show crypto pki timers** 例： `Device(config)# show crypto pki timers`	公開キーインフラストラクチャについて Cisco IOS に設定されているタイマーに関する情報を表示します。

例

次に、**show crypto pki crl download** コマンドの出力例を示します。

```
Device# show crypto pki crl download

CRL Issuer Name:
    cn=ios
    LastUpdate: 10:38:23 IST Sep 18 2013
    NextUpdate: 16:38:23 IST Sep 18 2013

    Valid after expiry till: 16:58:23 IST Sep 18 2013

    CRL Downloaded at 12:38:23 IST Sep 18 2013

    Retrieved from CRL Distribution Point:
      ** CDP Not Published - Retrieved via SCEP

 CRL DER is 213 bytes
 CRL is stored in parsed CRL cache

CRL prepublish timer interval: 10

Parsed CRL cache current size is 213 bytes
Parsed CRL cache maximum size is 65536 bytes
```

- 「Valid after expiry till:」フィールドは、CRL キャッシュ拡張が設定されている場合に、有効期限が切れた後に CRL が有効である期間を示します。
- 「CRL Downloaded at」フィールドは、CRL がダウンロードされた時刻を示します。

次に、**show crypto pki timer** コマンドの出力例を示します。

```
Device# show crypto pki timers

PKI Timers
  |       13:42.564
  |       13:42.564  SESSION CLEANUP
  |       11:44.111
  |       11:44.111  CRL UPDATE cn=IOS-CA
  |       21:44.111  CRL EXPIRE cn=IOS-CA
  |    7:59:56.917  STATIC CRL DOWNLOAD
CS Timers
  |        1:44.071
  |        1:44.071  CS DB CLEANUP
  |       11:43.999  CS SHADOW CERT GENERATION
  |       21:43.883  CS CERT EXPIRE
```

「CRL UPDATE」フィールドは、事前発行時間に基づいて更新されたタイマーを示します。

証明書の許可および失効の設定例

PKI AAA 認可の設定および検証例

ここでは、PKI AAA 認可の設定例を示します。

ルータの設定例

次の **show running-config** コマンド出力は、AAA サーバー機能との PKI 統合を使用して、VPN 接続を許可するように設定されたルータの動作設定を示します。

```
Router# show running-config
Building configuration...
!
version 12.3
!
hostname router7200router7200
!
aaa new-model
!
!
aaa authentication login default group tacacs+
aaa authentication login no_tacacs enable
aaa authentication ppp default group tacacs+
aaa authorization exec ACSLab group tacacs+
aaa authorization network ACSLab group tacacs+
aaa accounting exec ACSLab start-stop group tacacs+
aaa accounting network default start-stop group ACSLab
```

```
aaa session-id common
!
ip domain name example.com
!
crypto pki trustpoint EM-CERT-SERV
 enrollment url http://192.0.2.33:80
 serial-number
 crl optional
 rsakeypair STOREVPN 2048
 auto-enroll
 authorization list ACSLab
!
crypto pki certificate chain EM-CERT-SERV
 certificate 04
  30820214 3082017D A0030201 02020104 300D0609 2A864886 F70D0101 04050030
  17311530 13060355 0403130C 454D2D43 4552542D 53455256 301E170D 30343031
  31393232 30323535 5A170D30 35303131 38323230 3235355A 3030312E 300E0603
  55040513 07314437 45424434 301C0609 2A864886 F70D0109 02160F37 3230302D
  312E6772 696C2E63 6F6D3081 9F300D06 092A8648 86F70D01 01010500 03818D00
  30818902 818100BD F3B837AA D925F391 2B64DA14 9C2EA031 5A7203C4 92F8D6A8
  7D2357A6 BCC8596F A38A9B10 47435626 D59A8F2A 123195BB BE5A1E74 B1AA5AE0
  5CA162FF 8C3ACA4F B3EE9F27 8B031642 B618AE1B 40F2E3B4 F996BEFE 382C7283
  3792A369 236F8561 8748AA3F BC41F012 B859BD9C DB4F75EE 3CEE2829 704BD68F
  FD904043 0F555702 03010001 A3573055 30250603 551D1F04 1E301C30 1AA018A0
  16861468 7474703A 2F2F3633 2E323437 2E313037 2E393330 0B060355 1D0F0404
  030205A0 301F0603 551D2304 18301680 1420FC4B CF0B1C56 F5BD4C06 0AFD4E67
  341AE612 D1300D06 092A8648 86F70D01 01040500 03818100 79E97018 FB955108
  12F42A56 2A6384BC AC8E22FE F1D6187F DA5D6737 C0E241AC AAAEC75D 3C743F59
  08DEEFF2 0E813A73 D79E0FA9 D62DC20D 8E2798CD 2C1DC3EC 3B2505A1 3897330C
  15A60D5A 8A13F06D 51043D37 E56E45DF A65F43D7 4E836093 9689784D C45FD61D
  EC1F160C 1ABC8D03 49FB11B1 DA0BED6C 463E1090 F34C59E4
  quit
 certificate ca 01
  30820207 30820170 A0030201 02020101 300D0609 2A864886 F70D0101 04050030
  17311530 13060355 0403130C 454D2D43 4552542D 53455256 301E170D 30333132
  31363231 34373432 5A170D30 36313231 35323134 3734325A 30173115 30130603
  55040313 0C454D2D 43455254 2D534552 5630819F 300D0609 2A864886 F70D0101
  01050003 818D0030 81890281 8100C14D 833641CF D784F516 DA6B50C0 7B3CB3C9
  589223AB 99A7DC14 04F74EF2 AAEEE8F5 E3BFAE97 F2F980F7 D889E6A1 2C726C69
  54A29870 7E7363FF 3CD1F991 F5A37CFF 3FFDD3D0 9E486C44 A2E34595 C2D078BB
  E9DE981E B733B868 AA8916C0 A8048607 D34B83C0 64BDC101 161FC103 13C06500
  22D6EE75 7D6CF133 7F1B515F 32830203 010001A3 63306130 0F060355 1D130101
  FF040530 030101FF 300E0603 551D0F01 01FF0404 03020186 301D0603 551D0E04
  16041420 FC4BCF0B 1C56F5BD 4C060AFD 4E67341A E612D130 1F060355 1D230418
  30168014 20FC4BCF 0B1C56F5 BD4C060A FD4E6734 1AE612D1 300D0609 2A864886
  F70D0101 04050003 81810085 D2E386F5 4107116B AD3AC990 CBE84063 5FB2A6B5
  BD572026 528E92ED 02F3A0AE 1803F2AE AA4C0ED2 0F59F18D 7B50264F 30442C41
  0AF19C4E 70BD3CB5 0ADD8DE8 8EF636BD 24410DF4 DB62DAFC 67DA6E58 3879AA3E
  12AFB1C3 2E27CB27 EC74E1FC AEE2F5CF AA80B439 615AA8D5 6D6DEDC3 7F9C2C79
  3963E363 F2989FB9 795BA8
  quit
!
!
crypto isakmp policy 10
 encr aes
 group 14
!
!
crypto ipsec transform-set ISC_TS_1 esp-aes esp-sha-hmac
!
crypto ipsec profile ISC_IPSEC_PROFILE_2
 set security-association lifetime kilobytes 530000000
 set security-association lifetime seconds 14400
 set transform-set ISC_TS_1
```

```
!
!
controller ISA 1/1
!
!
interface Tunnel0
 description MGRE Interface provisioned by ISC
 bandwidth 10000
 ip address 192.0.2.172 255.255.255.0
 no ip redirects
 ip mtu 1408
 ip nhrp map multicast dynamic
 ip nhrp network-id 101
 ip nhrp holdtime 500
 ip nhrp server-only
 no ip split-horizon eigrp 101
 tunnel source FastEthernet2/1
 tunnel mode gre multipoint
 tunnel key 101
 tunnel protection ipsec profile ISC_IPSEC_PROFILE_2
!
interface FastEthernet2/0
 ip address 192.0.2.1 255.255.255.0
 duplex auto
 speed auto
!
interface FastEthernet2/1
 ip address 192.0.2.2 255.255.255.0
 duplex auto
 speed auto
!
!
tacacs-server host 192.0.2.55 single-connection
tacacs-server directed-request
tacacs-server key company lab
!
ntp master 1
!
end
```

成功した PKI AAA 認可のデバッグ例

次の **show debugging** コマンド出力は、AAA サーバー機能との PKI 統合を使用して、成功した許可を示します。

```
Router# show debugging
General OS:
  TACACS access control debugging is on
  AAA Authentication debugging is on
  AAA Authorization debugging is on
Cryptographic Subsystem:
Crypto PKI Trans debugging is on
Router#
May 28 19:36:11.117: CRYPTO_PKI: Trust-Point EM-CERT-SERV picked up
May 28 19:36:12.789: CRYPTO_PKI: Found a issuer match
May 28 19:36:12.805: CRYPTO_PKI: cert revocation status unknown.
May 28 19:36:12.805: CRYPTO_PKI: Certificate validated without revocation check
May 28 19:36:12.813: CRYPTO_PKI_AAA: checking AAA authorization (ACSLab, POD5.example.com,
 <all>)
May 28 19:36:12.813: AAA/BIND(00000042): Bind i/f
May 28 19:36:12.813: AAA/AUTHOR (0x42): Pick method list 'ACSLab'
May 28 19:36:12.813: TPLUS: Queuing AAA Authorization request 66 for processing
```

```
May 28 19:36:12.813: TPLUS: processing authorization request id 66
May 28 19:36:12.813: TPLUS: Protocol set to None .....Skipping
May 28 19:36:12.813: TPLUS: Sending AV service=pki
May 28 19:36:12.813: TPLUS: Authorization request created for 66(POD5.example.com)
May 28 19:36:12.813: TPLUS: Using server 192.0.2.55
May 28 19:36:12.813: TPLUS(00000042)/0/NB_WAIT/203A4628: Started 5 sec timeout
May 28 19:36:12.813: TPLUS(00000042)/0/NB_WAIT: wrote entire 46 bytes request
May 28 19:36:12.813: TPLUS: Would block while reading pak header
May 28 19:36:12.817: TPLUS(00000042)/0/READ: read entire 12 header bytes (expect 27
bytes)
May 28 19:36:12.817: TPLUS(00000042)/0/READ: read entire 39 bytes response
May 28 19:36:12.817: TPLUS(00000042)/0/203A4628: Processing the reply packet
May 28 19:36:12.817: TPLUS: Processed AV cert-application=all
May 28 19:36:12.817: TPLUS: received authorization response for 66: PASS
May 28 19:36:12.817: CRYPTO_PKI_AAA: reply attribute ("cert-application" = "all")
May 28 19:36:12.817: CRYPTO_PKI_AAA: authorization passed
Router#
Router#
May 28 19:36:18.681: %DUAL-5-NBRCHANGE: IP-EIGRP(0) 101: Neighbor 192.0.2.171 (Tunnel0)
 is up: new adjacency
Router#
Router# show crypto isakmp sa
dst             src             state          conn-id slot
192.0.2.22     192.0.2.102   QM_IDLE             84    0
```

失敗した PKI AAA 認可のデバッグ例

次の **show debugging** コマンド出力は、ルータが、VPN を使用しての接続を許可されていないことを示します。このメッセージは、このような状況で表示される典型的なメッセージです。

この例においてピア ユーザ名は、Cisco Secure ACS の VPN_Router_Disabled と呼ばれる Cisco Secure ACS グループに移動することにより、許可されていないものとして設定されました。ルータ（router7200.example.com）は、任意のピアに VPN 接続を確立する前に、Cisco Secure ACS AAA サーバに確認するように設定されています。

```
Router# show debugging
General OS:
  TACACS access control debugging is on
  AAA Authentication debugging is on
  AAA Authorization debugging is on
Cryptographic Subsystem:
  Crypto PKI Trans debugging is on

Router#
May 28 19:48:29.837: CRYPTO_PKI: Trust-Point EM-CERT-SERV picked up
May 28 19:48:31.509: CRYPTO_PKI: Found a issuer match
May 28 19:48:31.525: CRYPTO_PKI: cert revocation status unknown.
May 28 19:48:31.525: CRYPTO_PKI: Certificate validated without revocation check
May 28 19:48:31.533: CRYPTO_PKI_AAA: checking AAA authorization (ACSLab, POD5.example.com,
 <all>)
May 28 19:48:31.533: AAA/BIND(00000044): Bind i/f
May 28 19:48:31.533: AAA/AUTHOR (0x44): Pick method list 'ACSLab'
May 28 19:48:31.533: TPLUS: Queuing AAA Authorization request 68 for processing
May 28 19:48:31.533: TPLUS: processing authorization request id 68
May 28 19:48:31.533: TPLUS: Protocol set to None .....Skipping
May 28 19:48:31.533: TPLUS: Sending AV service=pki
May 28 19:48:31.533: TPLUS: Authorization request created for 68(POD5.example.com)
May 28 19:48:31.533: TPLUS: Using server 192.0.2.55
May 28 19:48:31.533: TPLUS(00000044)/0/NB_WAIT/203A4C50: Started 5 sec timeout
May 28 19:48:31.533: TPLUS(00000044)/0/NB_WAIT: wrote entire 46 bytes request
May 28 19:48:31.533: TPLUS: Would block while reading pak header
```

```
May 28 19:48:31.537: TPLUS(00000044)/0/READ: read entire 12 header bytes (expect 6 bytes)
May 28 19:48:31.537: TPLUS(00000044)/0/READ: read entire 18 bytes response
May 28 19:48:31.537: TPLUS(00000044)/0/203A4C50: Processing the reply packet
May 28 19:48:31.537: TPLUS: received authorization response for 68: FAIL
May 28 19:48:31.537: CRYPTO_PKI_AAA: authorization declined by AAA, or AAA server not
found.
May 28 19:48:31.537: CRYPTO_PKI_AAA: No cert-application attribute found. Failing.
May 28 19:48:31.537: CRYPTO_PKI_AAA: authorization failed
May 28 19:48:31.537: CRYPTO_PKI: AAA authorization for list 'ACSLab', and user
'POD5.example.com' failed.
May 28 19:48:31.537: %CRYPTO-5-IKMP_INVAL_CERT: Certificate received from 192.0.2.162
is bad: certificate invalid
May 28 19:48:39.821: CRYPTO_PKI: Trust-Point EM-CERT-SERV picked up
May 28 19:48:41.481: CRYPTO_PKI: Found a issuer match
May 28 19:48:41.501: CRYPTO_PKI: cert revocation status unknown.
May 28 19:48:41.501: CRYPTO_PKI: Certificate validated without revocation check
May 28 19:48:41.505: CRYPTO_PKI_AAA: checking AAA authorization (ACSLab, POD5.example.com,
 <all>)
May 28 19:48:41.505: AAA/BIND(00000045): Bind i/f
May 28 19:48:41.505: AAA/AUTHOR (0x45): Pick method list 'ACSLab'
May 28 19:48:41.505: TPLUS: Queuing AAA Authorization request 69 for processing
May 28 19:48:41.505: TPLUS: processing authorization request id 69
May 28 19:48:41.505: TPLUS: Protocol set to None .....Skipping
May 28 19:48:41.505: TPLUS: Sending AV service=pki
May 28 19:48:41.505: TPLUS: Authorization request created for 69(POD5.example.com)
May 28 19:48:41.505: TPLUS: Using server 198.168.244.55
May 28 19:48:41.509: TPLUS(00000045)/0/IDLE/63B22834: got immediate connect on new 0
May 28 19:48:41.509: TPLUS(00000045)/0/WRITE/63B22834: Started 5 sec timeout
May 28 19:48:41.509: TPLUS(00000045)/0/WRITE: wrote entire 46 bytes request
May 28 19:48:41.509: TPLUS(00000045)/0/READ: read entire 12 header bytes (expect 6 bytes)
May 28 19:48:41.509: TPLUS(00000045)/0/READ: read entire 18 bytes response
May 28 19:48:41.509: TPLUS(00000045)/0/63B22834: Processing the reply packet
May 28 19:48:41.509: TPLUS: received authorization response for 69: FAIL
May 28 19:48:41.509: CRYPTO_PKI_AAA: authorization declined by AAA, or AAA server not
found.
May 28 19:48:41.509: CRYPTO_PKI_AAA: No cert-application attribute found. Failing.
May 28 19:48:41.509: CRYPTO_PKI_AAA: authorization failed
May 28 19:48:41.509: CRYPTO_PKI: AAA authorization for list 'ACSLab', and user
'POD5.example.com' failed.
May 28 19:48:41.509: %CRYPTO-5-IKMP_INVAL_CERT: Certificate received from 192.0.2.162
is bad: certificate invalid
Router#
Router# show crypto iskmp sa
dst             src             state          conn-id slot
192.0.2.2        192.0.2.102   MM_KEY_EXCH         95    0
```

失効メカニズムの設定例

ここでは、PKI の失効メカニズムを指定する際に使用できる設定例を示します。

OCSP サーバの設定例

次の例では、証明書の AIA 拡張部で指定された OCSP サーバーを使用するようにルータを設定する方法を示します。

```
Router(config)# crypto pki trustpoint mytp
Router(ca-trustpoint)# revocation-check ocsp
```

CRL および OCSP サーバの指定例

次の例では、CRL をCDPからダウンロードするようにルータを設定する方法を示します。CRL を利用できない場合は、証明書の AIA 拡張部で指定される OCSP サーバーが使用されます。両方のオプションが失敗した場合、証明書の検証も失敗します。

```
Router(config)# crypto pki trustpoint mytp
Router(ca-trustpoint)# revocation-check crl ocsp
```

OCSP サーバの設定例

以下に、HTTP URL 「http://myocspserver:81」にある OCSP サーバーを使用するようにルータを設定する例を示します。このサーバーがダウンしている場合は、失効チェックは行われません。

```
Router(config)# crypto pki trustpoint mytp
Router(ca-trustpoint)# ocsp url http://myocspserver:81
Router(ca-trustpoint)# revocation-check ocsp none
```

OCSP サーバとの通信でのナンスのディセーブル例

次の例は、OCSP 要求に関するナンス（固有識別情報）が、OCSP サーバーとの通信でディセーブルになっている場合の通信を示します。

```
Router(config)# crypto pki trustpoint mytp
Router(ca-trustpoint)# ocsp url http://myocspserver:81
Router(ca-trustpoint)# revocation-check ocsp none
Router(ca-trustpoint)# ocsp disable-nonce
```

セントラル サイトにあるハブ ルータを証明書失効チェック用に設定する例

次の例では、複数のブランチ オフィスにセントラル サイトへの接続を提供しているセントラル サイトにあるハブ ルータを示します。

ブランチ オフィスも追加の IPSec トンネルを使用して、ブランチ オフィス間で直接相互に通信できます。

CA は、セントラルサイトにある HTTP サーバーの CRL を公開します。セントラル サイトは、各ピアと IPSec トンネルを設定する場合、そのピアの CRL をチェックします。

次の例では、IPSec 設定を示しません。PKI 関連の設定だけを示します。

ホーム オフィスのハブ設定

```
crypto pki trustpoint VPN-GW
 enrollment url http://ca.home-office.com:80/certsrv/mscep/mscep.dll
 serial-number none
 fqdn none
 ip-address none
```

```
 subject-name o=Home Office Inc,cn=Central VPN Gateway
 revocation-check crl
```

セントラル サイトのハブ ルータ

```
Router# show crypto ca certificate
Certificate
  Status: Available
  Certificate Serial Number: 2F62BE14000000000CA0
  Certificate Usage: General Purpose
  Issuer:
    cn=Central Certificate Authority
    o=Home Office Inc
  Subject:
    Name: Central VPN Gateway
    cn=Central VPN Gateway
    o=Home Office Inc
  CRL Distribution Points:
    http://ca.home-office.com/CertEnroll/home-office.crl
  Validity Date:
    start date: 00:43:26 GMT Sep 26 2003
    end   date: 00:53:26 GMT Sep 26 2004
    renew date: 00:00:00 GMT Jan 1 1970
  Associated Trustpoints: VPN-GW
CA Certificate
  Status: Available
  Certificate Serial Number: 1244325DE0369880465F977A18F61CA8
  Certificate Usage: Signature
  Issuer:
    cn=Central Certificate Authority
    o=Home Office Inc
  Subject:
    cn=Central Certificate Authority
    o=Home Office Inc
  CRL Distribution Points:
    http://ca.home-office.com/CertEnroll/home-office.crl
  Validity Date:
    start date: 22:19:29 GMT Oct 31 2002
    end   date: 22:27:27 GMT Oct 31 2017
  Associated Trustpoints: VPN-GW
```

ブランチ オフィス ルータのトラストポイント

```
crypto pki trustpoint home-office
 enrollment url http://ca.home-office.com:80/certsrv/mscep/mscep.dll
 serial-number none
 fqdn none

ip-address none
 subject-name o=Home Office Inc,cn=Branch 1
 revocation-check crl
```

証明書マップがブランチ オフィス ルータに入力されます。

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
branch1(config)# crypto pki certificate map central-site 10
branch1(ca-certificate-map)#
```

セントラルサイトのハブルータ上で発行された**show certificate**コマンドの出力では、証明書が以下によって発行されたことを示しています。

```
cn=Central Certificate Authority
o=Home Office Inc
```

この2行は、行を区切るためのカンマ（,）を使用して1行に結合され、元の2行が最初の一致基準として追加されています。

```
Router (ca-certificate-map)# issuer-name co cn=Central Certificate Authority, ou=Home
Office Inc
!The above line wrapped but should be shown on one line with the line above it.
```

セントラル サイト ルータの証明書の所有者名についても、同じように組み合わされています（「Name:」で始まる行は、所有者名の一部ではなく、証明書マップ基準を作成する際に無視する必要があることに注意してください）。これが証明書マップで使用されるサブジェクト名です。

cn=Central VPN Gateway

o=Home Office Inc

```
Router (ca-certificate-map)# subject-name eq cn=central vpn gateway, o=home office inc
```

これで、以前に設定された証明書マップがトラストポイントに追加されます。

```
Router (ca-certificate-map)# crypto pki trustpoint home-office
Router (ca-trustpoint)# match certificate central-site skip revocation-check
Router (ca-trustpoint)# exit
Router (config)# exit
```

設定がチェックされます（大部分の設定は示されていません）。

```
Router# write term
!Many lines left out
.
.
.
crypto pki trustpoint home-office
 enrollment url http://ca.home-office.com:80/certsrv/mscep/mscep.dll
 serial-number none
 fqdn none
 ip-address none
 subject-name o=Home Office Inc,cn=Branch 1
 revocation-check crl
 match certificate central-site skip revocation-check
!
!
crypto pki certificate map central-site 10
 issuer-name co cn = Central Certificate Authority, ou = Home Office Inc
 subject-name eq cn = central vpn gateway, o = home office inc
!many lines left out
```

今後のピアの証明書との照合のために、発行者名の行とサブジェクト名の行が矛盾しないように再フォーマットされていることに注意してください。

ブランチ オフィスが AAA をチェックする場合は、トラストポイントには次のような行があります。

```
crypto pki trustpoint home-office
 auth list allow_list
 auth user subj commonname
```

証明書マップが上記のように定義されると、次のコマンドがトラストポイントに追加され、セントラル サイト ハブの AAA チェックがスキップされます。

```
match certificate central-site skip authorization-check
```

両方のケースにおいてブランチ サイト ルータは、CRL のチェックまたは AAA サーバと通信するために、セントラル サイトに IPSec トンネルを確立する必要があります。ただし、**match certificate** コマンドと **central-site skip authorization-check (argument and keyword)** を使用しないと、ブランチオフィスが CRL または AAA サーバーを確認するまで、トンネルを確立することはできません（**match certificate** コマンドと **central-site skip authorization-check** 引数およびキーワードを使用しない限り、トンネルは確立されません）。

ブランチサイトにあるデバイスの証明書が失効していて、その証明書を更新するためにセントラルサイトにトンネルを確立する必要がある場合、セントラルサイトで **match certificate** コマンドと **allow expired-certificate** キーワードを使用できます。

セントラル サイト ルータのトラストポイント

```
crypto pki trustpoint VPN-GW
 enrollment url http://ca.home-office.com:80/certsrv/mscep/mscep.dll
 serial-number none
 fqdn none
 ip-address none
 subject-name o=Home Office Inc,cn=Central VPN Gateway
 revocation-check crl
```

ブランチ 1 サイト ルータのトラストポイント

```
Router# show crypto ca certificate
Certificate
  Status: Available
  Certificate Serial Number: 2F62BE14000000000CA0
  Certificate Usage: General Purpose
  Issuer:
    cn=Central Certificate Authority
    o=Home Office Inc
  Subject:
    Name: Branch 1 Site
    cn=Branch 1 Site
    o=Home Office Inc
  CRL Distribution Points:
    http://ca.home-office.com/CertEnroll/home-office.crl
  Validity Date:
    start date: 00:43:26 GMT Sep 26 2003
    end   date: 00:53:26 GMT Oct 3 2003
    renew date: 00:00:00 GMT Jan 1 1970
  Associated Trustpoints: home-office
CA Certificate
```

```
  Status: Available
  Certificate Serial Number: 1244325DE0369880465F977A18F61CA8
  Certificate Usage: Signature
  Issuer:
    cn=Central Certificate Authority
    o=Home Office Inc
  Subject:
    cn=Central Certificate Authority
    o=Home Office Inc
  CRL Distribution Points:
    http://ca.home-office.com/CertEnroll/home-office.crl
  Validity Date:
    start date: 22:19:29 GMT Oct 31 2002
    end   date: 22:27:27 GMT Oct 31 2017
  Associated Trustpoints: home-office
```

証明書マップがセントラル サイト ルータに入力されます。

```
Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router (config)# crypto pki certificate map branch1 10
Router (ca-certificate-map)# issuer-name co cn=Central Certificate Authority, ou=Home
Office Inc
!The above line wrapped but should be part of the line above it.
Router (ca-certificate-map)# subject-name eq cn=Brahcn 1 Site,o=home office inc
```

証明書マップがトラストポイントに追加されます。

```
Router (ca-certificate-map)# crypto pki trustpoint VPN-GW
Router (ca-trustpoint)# match certificate branch1 allow expired-certificate
Router (ca-trustpoint)# exit
Router (config) #exit
```

設定がチェックされます（設定の大部分は示されていません）。

```
Router# write term
!many lines left out
crypto pki trustpoint VPN-GW
 enrollment url http://ca.home-office.com:80/certsrv/mscep/mscep.dll
 serial-number none
 fqdn none
 ip-address none
 subject-name o=Home Office Inc,cn=Central VPN Gateway
 revocation-check crl
 match certificate branch1 allow expired-certificate
!
!
crypto pki certificate map central-site 10
 issuer-name co cn = Central Certificate Authority, ou = Home Office Inc
 subject-name eq cn = central vpn gateway, o = home office inc
! many lines left out
```

match certificate コマンド、**branch1 allow expired-certificate**（引数とキーワード）および証明書マップは、ブランチルータが新しい証明書を取得した後すぐに削除する必要があります。

証明書の許可および失効の設定例

この項では、CRL キャッシュ コントロールの設定または証明書のシリアル番号セッション コントロールを指定する場合に使用する設定例を示します。

CRL キャッシュ コントロールの設定

次の例では、CA1 トラストポイントに関連付けられたすべての CRL の CRL キャッシングをディセーブルにする方法を示します。

```
crypto pki trustpoint CA1
 enrollment url http://CA1:80
 ip-address FastEthernet0/0
 crl query ldap://ldap_CA1
 revocation-check crl
 crl-cache none
```

上記の例の設定を実行した直後は、まだ現在の CRL がキャッシュされています。

Router# **show crypto pki crls**

```
CRL Issuer Name:
    cn=name Cert Manager,ou=pki,o=example.com,c=US
    LastUpdate: 18:57:42 GMT Nov 26 2005
    NextUpdate: 22:57:42 GMT Nov 26 2005
    Retrieved from CRL Distribution Point:
      ldap://ldap.example.com/CN=name Cert Manager,O=example.com
```

現在の CRL が失効すると、次の更新時に新しい CRL がルータにダウンロードされます。**crl-cache none** コマンドが有効になり、トラストポイントの CRL はすべてキャッシュされなくなります。また、キャッシュは無効になります。**show crypto pki crls** コマンドを実行して、CRL がキャッシュされていないことを確認できます。キャッシュされている CRL がないため、出力は表示されません。

次の例では、CA1 トラストポイントに関連付けられたすべての CRL に 2 分の最大ライフタイムを設定する方法を示します。

```
crypto pki trustpoint CA1
 enrollment url http://CA1:80
 ip-address FastEthernet0/0
 crl query ldap://ldap_CA1
 revocation-check crl
 crl-cache delete-after 2
```

CRL の最大ライフタイムを設定するために上記例の設定を実行した直後でも、依然現在の CRL がキャッシュされます。

Router# **show crypto pki crls**

```
CRL Issuer Name:
    cn=name Cert Manager,ou=pki,o=example.com,c=US
    LastUpdate: 18:57:42 GMT Nov 26 2005
    NextUpdate: 22:57:42 GMT Nov 26 2005
    Retrieved from CRL Distribution Point:
      ldap://ldap.example.com/CN=name Cert Manager,O=example.com
When the current CRL expires, a new CRL is downloaded to the router at the next update
and the crl-cache delete-after
command takes effect. This newly cached CRL and all subsequent CRLs will be deleted after
 a maximum lifetime of 2 minutes.
You can verify that the CRL will be cached for 2 minutes by executing the show crypto
pki crls
 command. Note that the NextUpdate time is 2 minutes after the LastUpdate time.
```

Router# **show crypto pki crls**

```
CRL Issuer Name:
    cn=name Cert Manager,ou=pki,o=example.com,c=US
    LastUpdate: 22:57:42 GMT Nov 26 2005

    NextUpdate: 22:59:42 GMT Nov 26 2005
    Retrieved from CRL Distribution Point:
```

ldap://ldap.example.com/CN=name Cert Manager,O=example.com

証明書のシリアル番号セッション コントロールの設定

次の例では、CA1 トラストポイントの証明書マップを使用した証明書のシリアル番号セッション コントロールの設定を示します。

```
crypto pki trustpoint CA1
 enrollment url http://CA1
 chain-validation stop
 crl query ldap://ldap_server
 revocation-check crl
 match certificate crl
!
crypto pki certificate map crl 10
 serial-number co 279d
```

（注） *match-criteria* 値が **co**（含む）ではなく **eq**（等しい）に設定されている場合、シリアル番号はスペースを含めて、証明書マップのシリアル番号に正確に一致する必要があります。

次の例では、AAA 属性を使用した証明書のシリアル番号セッション コントロールの設定を示します。この場合、証明書にシリアル番号「4ACA」がなければ、有効な証明書はすべて受け入れられます。

```
crypto pki trustpoint CA1
 enrollment url http://CA1
 ip-address FastEthernet0/0
 crl query ldap://ldap_CA1
 revocation-check crl
 aaa new-model
!
aaa attribute list crl
attribute-type aaa-cert-serial-not 4ACA
```

サーバー ログは、シリアル番号「4ACA」を持つ証明書が拒否されたことを示しています。証明書の拒否は、感嘆符で表示されます。

```
.
.
.
Dec 3 04:24:39.051: CRYPTO_PKI: Trust-Point CA1 picked up
Dec 3 04:24:39.051: CRYPTO_PKI: locked trustpoint CA1, refcount is 1
Dec 3 04:24:39.051: CRYPTO_PKI: unlocked trustpoint CA1, refcount is 0
Dec 3 04:24:39.051: CRYPTO_PKI: locked trustpoint CA1, refcount is 1
Dec 3 04:24:39.135: CRYPTO_PKI: validation path has 1 certs
Dec 3 04:24:39.135: CRYPTO_PKI: Found a issuer match
```

```
Dec 3 04:24:39.135: CRYPTO_PKI: Using CA1 to validate certificate
Dec 3 04:24:39.135: CRYPTO_PKI: Certificate validated without revocation check
Dec 3 04:24:39.135: CRYPTO_PKI: Selected AAA username: 'PKIAAA'
Dec 3 04:24:39.135: CRYPTO_PKI: Anticipate checking AAA list:'CRL'
Dec 3 04:24:39.135: CRYPTO_PKI_AAA: checking AAA authorization (CRL, PKIAAA-L1, <all>)
Dec 3 04:24:39.135: CRYPTO_PKI_AAA: pre-authorization chain validation status (0x4)
Dec 3 04:24:39.135: AAA/BIND(00000021): Bind i/f
Dec 3 04:24:39.135: AAA/AUTHOR (0x21): Pick method list 'CRL'
.
.
.
Dec 3 04:24:39.175: CRYPTO_PKI_AAA: reply attribute ("cert-application" = "all")
Dec 3 04:24:39.175: CRYPTO_PKI_AAA: reply attribute ("cert-trustpoint" = "CA1")
!
Dec 3 04:24:39.175: CRYPTO_PKI_AAA: reply attribute ("cert-serial-not" = "4ACA")
Dec 3 04:24:39.175: CRYPTO_PKI_AAA: cert-serial doesn't match ("4ACA" != "4ACA")
!
Dec 3 04:24:39.175: CRYPTO_PKI_AAA: post-authorization chain validation status (0x7)
!
Dec 3 04:24:39.175: CRYPTO_PKI: AAA authorization for list 'CRL', and user 'PKIAAA'
failed.
Dec 3 04:24:39.175: CRYPTO_PKI: chain cert was anchored to trustpoint CA1, and chain
validation result was: CRYPTO_PKI_CERT_NOT_AUTHORIZED
!
Dec 3 04:24:39.175: %CRYPTO-5-IKMP_INVAL_CERT: Certificate received from 192.0.2.43 is
bad: certificate invalid
Dec 3 04:24:39.175: %CRYPTO-6-IKMP_MODE_FAILURE: Processing of Main mode failed with
peer at 192.0.2.43
.
.
.
```

証明書チェーン検証の設定例

この項では、デバイス証明書の証明書チェーン処理レベルを指定する場合に使用する設定例を示します。

ピアからルート CA への証明書チェーン検証の設定

次の設定例では、ピア、SubCA11、SubCA1、および RootCA のすべての証明書が検証されます。

```
crypto pki trustpoint RootCA
 enrollment terminal
 chain-validation stop
 revocation-check none
 rsakeypair RootCA
crypto pki trustpoint SubCA1
 enrollment terminal
 chain-validation continue RootCA
 revocation-check none
 rsakeypair SubCA1
crypto pki trustpoint SubCA11
 enrollment terminal
 chain-validation continue SubCA1
 revocation-check none
 rsakeypair SubCA11
```

ピアから下位 CA への証明書チェーン検証の設定

次の設定例では、ピア証明書および SubCA1 証明書が有効にされます。

```
crypto pki trustpoint RootCA
 enrollment terminal
 chain-validation stop
 revocation-check none
 rsakeypair RootCA
crypto pki trustpoint SubCA1
 enrollment terminal
 chain-validation continue RootCA
 revocation-check none
 rsakeypair SubCA1
crypto pki trustpoint SubCA11
 enrollment terminal
 chain-validation continue SubCA1
 revocation-check none
 rsakeypair SubCA11
```

証明書チェーンの欠落確認の設定

次の設定例では、SubCA1 が、設定済みの Cisco IOS 階層にはないが、提出された証明書チェーンでピアによって提示されたと想定しています。

ピアが、提出された証明書チェーンで SubCA1 証明書を提示した場合、ピア、SubCA11、および SubCA1 の各証明書が有効になります。

ピアが、提出された証明書チェーンで SubCA1 証明書を提示しない場合、チェーンの検証は失敗します。

```
crypto pki trustpoint RootCA
 enrollment terminal
 chain-validation stop
 revocation-check none
 rsakeypair RootCA
crypto pki trustpoint SubCA11
 enrollment terminal
 chain-validation continue RootCA
 revocation-check none
 rsakeypair SubCA11
```

その他の参考資料

関連資料

関連項目	マニュアル タイトル
PKI コマンド：完全なコマンドの構文、コマンド モード、デフォルト、使用上の注意事項、例	『*Cisco IOS Security Command Reference*』

関連項目	マニュアル タイトル
PKI の概要（RSA キー、証明書登録、および CA を含む）	「Cisco IOS PKI Overview: Understanding and Planning a PKI」モジュール
RSA キーの生成および展開	「PKI 内での RSA キーの展開」モジュール
証明書登録：サポートされる方法、登録プロファイル、設定作業	「PKI の証明書登録の設定」モジュール
Cisco IOS 証明書サーバの概要および設定作業	「PKI 展開での Cisco IOS 証明書サーバの設定および管理」モジュール
推奨される暗号化アルゴリズム	『*Next Generation Encryption*』

シスコのテクニカル サポート

説明	リンク
右の URL にアクセスして、シスコのテクニカル サポートを最大限に活用してください。これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

Cisco TrustSec の概要の機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *148 : Cisco TrustSec* の概要の機能情報

機能名	リリース	機能情報
IPv6 の有効化 - インライン タギング	Cisco IOS XE Fuji 16.8.1	IPv6 のサポートが導入されました。

第 111 章

PKI の証明書登録の設定

この章では、証明書登録に利用可能なさまざまな方式および参加する PKI ピアの各セットアップ方法について説明します。証明書登録は、認証局（CA）から証明書を取得するプロセスであり、証明書を要求するエンド ホストと CA の間で発生します。公開キー インフラストラクチャ（PKI）に参加する各ピアは、CA に登録する必要があります。

（注） セキュリティに対する脅威は、脅威からの保護に役立つ暗号化技術と同様に絶え間なく変化しています。最新のシスコの暗号化に関する推奨事項については、『Next Generation Encryption』（NGE）ホワイト ペーパーを参照してください。

PKI 証明書登録の前提条件

証明書登録用にピアを設定する前に、次のものを準備、あるいは次の作業を実行することが必要です。

- 登録用に生成された Rivest、Shamir、Adelman（RSA）キー ペアおよび登録する PKI。
- 認証された CA。
- 「Cisco IOS PKI Overview: Understanding and Planning a PKI」の内容を理解していること。
- 自動登録と証明書ロールオーバーなどの PKI サービスが正しく動作するように、デバイスの NTP を有効にします。

（注） Cisco IOS Release 12.3(7)T では、「**crypto ca**」で始まるすべてのコマンドが、「**crypto pki**」から始まるように変更されました。ルータは引き続き **crypto ca** コマンドを受信しますが、出力はすべて **crypto pki** と表示されます。

PKI の証明書登録に関する情報

CA とは

CA は他の通信相手が使用できるデジタル証明書を発行するエンティティです。これが、信頼できる第三者の例です。CA は多くの PKI スキームの特性です。

CA は証明書要求を管理し、参加ネットワーク装置に証明書を発行します。これらのサービスでは、身元情報を検証してデジタル証明書を作成するために、参加装置のキーを一元的に管理します。PKI の動作を開始する前に、CA は独自の公開キー ペアを生成し、自己署名 CA 証明書を作成します。その後、CA は、証明書要求に署名し、PKI に対してピア登録を開始できます。

Cisco IOS 証明書サーバまたはサードパーティの CA ベンダーが指定する CA を使用できます。

複数の CA のためのフレームワーク

PKI は、複数の CA をサポートするために階層型フレームワーク内に設定できます。階層の最上位にはルート CA があり、自己署名証明書を保持しています。階層全体の信頼性は、ルート CA の RSA キー ペアから導出されます。階層構造内の下位 CA は、ルート CA または別の下位 CA に登録できます。CA の複数の階層が、ルート CA または別の下位 CA で設定されます。階層型 PKI 内では、登録されているすべてのピアが信頼できるルート CA 証明書または共通の下位 CA を共有している場合、証明書を相互に検証できます。

複数 CA を使用する場合

複数 CA を使用することにより、柔軟性および信頼性が向上します。たとえば、ルート CA を本社オフィスに配置し、下位 CA をブランチ オフィスに配置できます。また、CA ごとに異なる許可ポリシーを実行できるため、階層構造内の、ある CA では各証明書要求を手動で許可する必要があるように、別の CA では証明書要求を自動的に許可するように設定できます。

少なくとも 2 階層の CA が推奨されるシナリオは、次のとおりです。

- 多数の証明書が失効し、再発行される大規模かつ非常にアクティブなネットワーク。複数の階層を使用することにより、CA は証明書失効リスト（CRL）のサイズを制御しやすくなります。

- 下位の CA 証明書を発行する場合を除いて、オンラインの登録プロトコルが使用されているときは、ルート CA をオフラインにしておくことができます。このシナリオでは、ルート CA のセキュリティが向上します。

CA の認証

装置に自身の証明書が発行されて証明書登録が発生する前に、CA の証明書が認証される必要があります。CA の認証は通常、ルータで PKI サポートを初期設定するときにだけ実行されます。CA を認証するには、**crypto pki authenticate** コマンドを発行します。これにより、CA の公開キーが組み込まれた CA の自己署名証明書が取得されて CA がルータに対して認証されます。

（注） PKI は、有効期限が 2099 年を超えている証明書をサポートしていません。そのため、値が 2099 よりも小さい有効期限を選択することをお勧めします。

fingerprint コマンドによる認証

Cisco IOS リリース 12.3(12) 以降では、**fingerprint** コマンドを発行して、認証時に CA 証明書のフィンガープリントと照合するフィンガープリントを事前入力できます。

フィンガープリントがトラストポイントにあらかじめ入力されていない場合や、認証要求がインタラクティブでない場合は、CA 証明書の認証時に表示されるフィンガープリントを検証する必要があります。認証要求がインタラクティブでない場合、事前入力フィンガープリントがないと、証明書は拒否されます。

（注） 認証要求がコマンドラインインターフェイス（CLI）を使用して行われる場合、その要求はインタラクティブな要求です。認証要求が HTTP または別の管理ツールを使用して行われる場合、その要求はインタラクティブでない要求です。

サポートされる証明書の登録方式

Cisco IOS ソフトウェアは、CA から証明書を取得するために次の方式をサポートしています。

- Simple Certificate Enrollment Protocol（SCEP）：HTTP を使用して CA または登録局（RA）と通信する、シスコが開発した登録プロトコル。SCEP は、要求および証明書の送受信用に最も一般的に使用される方式です。

（注） 自動証明書およびキー ロールオーバー機能を活用するには、ロールオーバーをサポートする CA を実行する必要があります。また、クライアント登録方式として SCEP を使用する必要があります。Cisco IOS CA を実行する場合は、ロールオーバーをサポートするために Cisco IOS Release 12.4(2)T 以降のリリースを実行する必要があります。

- PKCS12：ルータは、外部のサーバから証明書を PKCS12 形式でインポートします。
- IOS ファイル システム（IFS）：ルータは、Cisco IOS ソフトウェアでサポートされるファイル システム（TFTP、FTP、フラッシュ、および NVRAM など）を使用して証明書要求を送信し、発行された証明書を受信します。ユーザの CA が SCEP をサポートしない場合、IFS 証明書登録をイネーブルにできます。

（注） Cisco IOS Release 12.3(4)T 以前のリリースでは、IFS 内で TFTP ファイル システムだけがサポートされます。

- 手動でのカットアンドペースト：ルータはコンソール端末に証明書要求を表示し、ユーザはコンソール端末で発行された証明書を入力できます。ルータと CA の間にネットワーク接続がない場合、ユーザは証明書要求および証明書を手動でカットアンドペーストできます。
- 登録プロファイル：登録プロファイルは、主に EST または端末ベースの登録に使用されます。CA サーバーが SCEP をサポートしていない場合、推奨される登録手法は EST ベースの登録または端末ベースの登録です。
- トラストポイントの自己署名証明書登録：セキュア HTTP（HTTPS）サーバは、セキュア ソケット レイヤ（SSL）ハンドシェイク時に使用される自己署名証明書を生成し、HTTPS サーバとクライアントの間にセキュアな接続を確立します。自己署名証明書は、ルータのスタートアップ コンフィギュレーション（NVRAM）に保存されます。保存された自己署名証明書は、将来の SSL ハンドシェイクに使用できます。これにより、ルータがリロードされる度に、証明書を受け入れるために必要だったユーザによる介入が不要になります。

（注） 自動登録および自動再登録を活用するには、登録方式として、TFTP または手動でのカットアンドペースト登録を使用しないでください。TFTP およびカットアンドペーストによる手動での登録方式は手動の登録プロセスでは、ユーザによる入力が必要です。

PKI の証明書登録のための Cisco IOS Suite-B サポート

Suite B の要件は、IKE および IPSec で使用するための暗号化アルゴリズムの 4 つのユーザ インターフェイス スイートで構成され、RFC 4869 に記述されています。各スイートは、暗号化アルゴリズム、デジタル署名アルゴリズム、キー合意アルゴリズム、ハッシュまたはメッセージ ダイジェスト アルゴリズムで構成されています。

Suite-B によって、PKI の証明書登録に次のサポートが追加されます。

- X.509 証明書内の署名操作で、楕円曲線デジタル署名アルゴリズム（ECDSA）（256 ビットおよび 384 ビットの曲線）が使用されます。
- ECDSA の署名を使用した X.509 証明書の確認で PKI がサポートされます。
- ECDSA の署名を使用した証明書要求の生成、および発行された証明書の IOS へのインポートで、PKI がサポートされます。

Cisco IOS での Suite-B サポートに関する詳細については、『Configuring Security for VPNs with IPsec』フィーチャ モジュールを参照してください。

登録局

Cisco IOS 証明書サーバは、RA モードで実行できるように設定できます。RA は、CA から認証および認可責任をオフロードします。RA が SCEP または手動での登録要求を受信すると、管理者はローカルポリシーごとに要求を拒否または許可できます。要求が許可された場合、その要求は発行元 CA に転送されます。また、自動的に証明書を生成して、証明書を RA に返すように CA を設定できます。クライアントは、許可された証明書を RA から後で取得できます。

自動証明書登録

証明書自動登録を使用すると、CA クライアントは、CA サーバから証明書を自動的に要求できます。この自動ルータ要求では、登録要求が CA サーバに送信された時点で、オペレータによる介入が不要になります。自動登録は、設定済みの、有効なクライアント証明書を持っていないトラストポイント CA の起動時に実行されます。証明書が失効すると、新しい証明書が自動的に要求されます。

（注） 自動登録が設定されると、クライアントは自動的にクライアント証明書を要求します。CA サーバは、独自の許可チェックを実行します。このチェックに証明書を自動的に発行するポリシーが含まれている場合は、すべてのクライアントが自動的に証明書を受信しますが、これはそれほど安全ではありません。そのため、自動証明書登録を追加の認証および許可メカニズム（既存の証明書およびワンタイム パスワードを活用した Secure Device Provisioning（SDP）など）と組み合わせる必要があります。

自動クライアント証明書およびキー ロールオーバー

デフォルトでは、自動証明書登録機能により、クライアントの現在の証明書が失効する前に、CS から新しいクライアント証明書とキーが要求されます。証明書およびキー ロールオーバーにより、新しいキーおよび証明書、ロールオーバー、証明書が利用可能になるまで、現在のキーおよび証明書を保持して証明書が失効する前に証明書更新ロールオーバー要求を行うことができます。指定された時間が経過すると、ロールオーバー証明書およびキーがアクティブに

なります。失効した証明書およびキーは、ロールオーバー時にただちに削除され、証明書チェーンおよびCRLから削除されます。

自動ロールオーバーのセットアップは2段階で行われます。まずCAクライアントが自動的に登録され、クライアントのCAが自動的に登録される必要があります。さらに**auto-rollover**コマンドがイネーブルになる必要があります。CAサーバを自動証明書ロールオーバー用に設定する場合の詳細については、『*Public Key Infrastructure Configuration Guide*』の「Configuring and Managing a Cisco IOS Certificate Server for PKI Deployment」の章にある「Automatic CA Certificate and Key Rollover」の項を参照してください。

任意のrenewal percentageパラメータを**auto-enroll**コマンドと一緒に使用すると、証明書の指定されたパーセンテージの有効期間が経過したときに、新しい証明書を要求できます。たとえば、更新パーセンテージが90に設定され、証明書の有効期間が1年の場合は、古い証明書が失効する36.5日前に新しい証明書が要求されます。自動ロールオーバーが発生するには、更新パーセンテージが100未満である必要があります。指定するパーセント値は、10以上でなくてはなりません。CA証明書の失効が差し迫っているため、有効設定期間よりも短い期間のクライアント証明書を発行する場合、その期間の残り日数に対してロールオーバー証明書が発行されます。最低でも、設定されている有効期間の10 %と、ロールオーバーが機能するのに十分な時間（絶対最小値：3分）を見込んでおく必要があります。

ヒント　CA自動登録がイネーブルになっておらず、現在のクライアント証明書の有効期間が、対応するCA証明書の有効期間と同じか、それよりも長い場合は、**crypto pki enroll**コマンドを使用して既存のクライアント上で手動でロールオーバーを開始できます。クライアントはロールオーバー プロセスを開始しますが、このプロセスは、サーバが自動ロールオーバーに設定され、利用可能なロールオーバー サーバ証明書を保持している場合にだけ発生します。

（注）　キーペアが**auto-enroll re-generate**コマンドおよびキーワードによって設定されている場合は、キーペアも送信されます。新しいキーペアは、セキュリティ上の問題に対処するために発行することを推奨します。

証明書登録プロファイル

登録プロファイルを使用すると、証明書認証、登録および再登録の各パラメータを指定するよう求められたときにユーザは、これらのパラメータを指定できます。これらのパラメータ値は、プロファイルを構成する2つのテンプレートによって参照されます。このうち、1つのテンプレートには、CAの証明書を取得するためにCAサーバに送られるHTTP要求のパラメータ（証明書認証としても知られる）が含まれ、もう1つのテンプレートには、証明書を登録するためにCAに送られるHTTP要求のパラメータが含まれます。

2つのテンプレートを設定すると、ユーザーは、証明書の認証と登録用に異なるURLまたは方法を指定できます。たとえば、認証（CAの証明書の取得）をTFTPによって（**authentication url**コマンドを使用して）実行できる一方で、（**enrollment terminal**コマンドを使用して）登録を手動で実行できます。

Cisco IOS Release 12.3(11)T 以前のリリースでは、証明書要求は PKCS10 形式でしか送信できませんでしたが、現在では、プロファイルにパラメータが追加されたことにより、証明書更新要求用に PKCS7 形式を指定できるようになりました。

（注） 1 つの登録プロファイルには、タスクごとに最大 3 つのセクション（証明書の認証、登録および再登録）を指定できます。

PKI の証明書登録を設定する方法

ここでは、次の登録の任意手順について説明します。登録または自動登録を設定する（最初の作業）場合は、手動での証明書登録を設定できません。また、TFTP またはカットアンドペーストによる手動での証明書登録を設定した場合、自動登録、自動再登録、登録プロファイルは設定できず、自動 CA 証明書ロールオーバー機能も利用できません。

証明書登録または自動登録の設定

PKI に参加しているクライアントの証明書登録を設定するには、次の作業を実行します。

始める前に

自動証明書登録要求を設定する前に、必要な登録情報がすべて設定されていることを確認する必要があります。

自動クライアント証明書およびキーロールオーバーをイネーブルにするための前提条件

自動登録を使用するときには、証明書ロールオーバーの CA クライアントサポートが自動的にイネーブルになります。自動 CA 証明書ロールオーバーを正常に実行するには、次の前提条件が適用されます。

- ネットワーク装置はシャドウ PKI をサポートしている必要があります。
- クライアントは Cisco IOS Release 12.4(2)T 以降のリリースを実行している必要があります。
- クライアントの CS は自動ロールオーバーをサポートする必要があります。CA サーバの自動ロールオーバー設定コンフィギュレーションに関する詳細については、『*Public Key Infrastructure Configuration Guide*』の「Configuring and Managing a Cisco IOS Certificate Server for PKI Deployment」の章にある「Automatic CA Certificate and Key Rollover」を参照してください。

自動登録の初期キー生成場所を指定するための前提条件

自動登録の初期キー生成場所を指定するには、Cisco IOS Release 12.4(11)T 以降のリリースを実行する必要があります。

自動登録の RSA キーペアに関する制約事項

regenerate コマンドまたは **regenerate** コマンドの **auto-enroll** キーワードを使用して新しいキーペアを生成するように設定したトラストポイントは、他のトラストポイントとキーペアを共有することはできません。各トラストポイントに独自のキーペアを付与するには、CA トラストポイント コンフィギュレーション モードで **rsakeypair** コマンドを使用します。再生トラストポイント間でのキー ペアの共有がサポートされていない場合にキー ペアを共有すると、キーと証明書が一致しなくなるため、トラストポイントの一部のサービスが失われます。

再生成オプションを使用した証明書の更新は、ゼロ（「0」）から始まるキーラベル（「0test」など）では機能しません。CLI を使用すると、トラストポイントでそのような名前を設定でき、ゼロから始まるホスト名を使用できますが、証明書の再生成は失敗します。

自動クライアント証明書およびキーロールオーバーに関する制約事項

クライアントが自動 CA 証明書ロールオーバーを正常に実行するには、次の制約事項が適用されます。

- SCEP を使用してロールオーバーをサポートする必要があります。SCEP の代わりに証明書管理プロトコルまたはメカニズム（登録プロファイル、手動での登録、または TFTP による登録など）を使用して、PKI に登録する装置では、SCEP で提供されているロールオーバー機能を利用できません。
- シャドウ証明書の生成後に、設定をスタートアップ コンフィギュレーションに保存できない場合、ロールオーバーは発生しません。
- キーペア名がゼロ（「0」）から始まる場合（「0test」など）、キー再生成を使用したロールオーバーは機能しません。トラストポイントで **rsakeypair** *name* を設定する場合は、ゼロから始まる名前を設定しないでください。キーペア名が設定されておらず、デフォルトのキーペアが使用されている場合は、ルータのホスト名がゼロから始まっていないことを確認してください。その場合は、トラストポイントで別の名前を使用して "**rsakeypair** *name* を明示的に設定してください。

（注） セキュリティに対する脅威は、脅威からの保護に役立つ暗号化技術と同様に絶え間なく変化しています。最新のシスコの暗号化に関する推奨事項については、『Next Generation Encryption』（NGE）ホワイト ペーパーを参照してください。

手順の概要

1. **enable**
2. **configure terminal**
3. **crypto pki trustpoint** *name*
4. **enrollment** [**mode** | **retry period** *minutes* | **retry count** *number*] **url** *url* [**pem**]
5. **eckeypair** *label*
6. **subject-name** [*x.500-name*]
7. **vrf** *vrf-name*
8. **ip-address** {*ip-address* | *interface* | **none**}
9. serial-number [none]

10. **auto-enroll** [*percent*] [**regenerate**]
11. **usage** *method1* [*method2* [*method3*]]
12. **password** *string*
13. **rsakeypair** *key-label key-size encryption-key-size*]]
14. **fingerprint** *ca-fingerprint*
15. **on** *devicename* **:**
16. **exit**
17. **crypto pki authenticate** *name*
18. **exit**
19. **copy system:running-config nvram:startup-config**
20. **show crypto pki certificates**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**crypto pki trustpoint** *name* 例： `Router(config)# crypto pki trustpoint mytp`	トラストポイントおよび設定された名前を宣言して、CA トラストポイント コンフィギュレーション モードを開始します。
ステップ 4	**enrollment** [**mode** | **retry period** *minutes* | **retry count** *number*] **url** *url* [**pem**] 例： `Router(ca-trustpoint)# enrollment url http://cat.example.com`	ルータが証明書要求を送信する CA の URL を指定します。 • **mode**：CA システムが RA を提供する場合は、RA モードを指定します。 • **retry period** *minutes*：証明書要求を再試行する待機期間を指定します。デフォルトの再試行間隔は 1 分です。 • **retry count** *number*：直前の要求に対する応答をルータが受信しない場合、ルータが証明書要求を再送信する回数を指定します（1 ～ 100 回の範囲で指定できます）。 • **url** *url*：ルータが証明書要求を送信するファイルシステムの URL。URL 内の IPv6 アドレス

	コマンドまたはアクション	目的
		は括弧で囲む必要があります。たとえば、http://[2001:DB8:1:1::1]:80 です。 • **pem**：証明書要求に Privacy Enhanced Mail（PEM）の境界を追加します。 （注） 自動登録をサポートするには、TFTP または手動でのカットアンドペースト以外の登録方式を設定する必要があります。
ステップ 5	**eckeypair** *label* 例： `Router(ca-trustpoint)# eckeypair Router_1_Key`	（任意）ECDSA の署名を使用して証明書要求を生成する Elliptic Curve（EC）キーを使用するように、トラストポイントを設定します。*label* 引数は、グローバル コンフィギュレーション モードで **crypto key generate rsa** または **crypto key generate ec keysize** コマンドを使用して設定される EC キーラベルを指定します。詳細については、『Configuring Internet Key Exchange for IPsec VPNs』フィーチャ モジュールを参照してください。 （注） トラストポイントの設定を使用せずに ECDSA の署名を持つ証明書をインポートする場合、ラベルにはデフォルトで FQDN の値が使用されます。
ステップ 6	**subject-name** [*x.500-name*] 例： `Router(ca-trustpoint)# subject-name cat`	（任意）証明書要求で使用される件名を指定します。 • *x.500-name*：この名前が指定されていない場合、完全修飾ドメイン名（FQDN）が使用されます。FQDN はデフォルトの件名です。
ステップ 7	**vrf** *vrf-name* 例： `Router(ca-trustpoint)# vrf myvrf`	（任意）登録、証明書失効リスト（CRL）の取得、および Online Certificate Status Protocol（OCSP）のステータに使用される公開キー インフラストラクチャ（PKI）トラストポイントで VRF インスタンスを指定します。
ステップ 8	**ip-address** {*ip-address* | *interface* | **none**} 例： `Router(ca-trustpoint)# ip address 192.168.1.66`	（任意）指定されたインターフェイスの IP アドレスを証明書要求に含めます。 • IPv4 または IPv6 アドレスのいずれかを指定するには、*ip-address* 引数を発行します。

	コマンドまたはアクション	目的
		• ルータのインターフェイスを指定するには、*interface* 引数を発行します。 • IP アドレスを含めない場合は、**none** キーワードを発行します。 （注） このコマンドがイネーブルになっている場合、このトラストポイントの登録時に IP アドレスのプロンプトは表示されません。
ステップ 9	serial-number [none] 例： `Router(ca-trustpoint)# serial-number`	（任意）**none** キーワードを発行しない場合は、証明書要求でルータのシリアル番号を指定します。 • 証明書要求にシリアル番号を含めない場合は、**none** キーワードを発行します。
ステップ 10	**auto-enroll** [*percent*] [**regenerate**] 例： `Router(ca-trustpoint)# auto-enroll regenerate`	（任意）自動登録をイネーブルにします。これにより、クライアントは CA から自動的にロールオーバー証明書を要求できます。 • 自動登録イネーブルでない場合、証明書の失効時にクライアントを手動で PKI に再登録する必要があります。 • デフォルトでは、ルータのドメイン ネーム システム（DNS）名だけが証明書に含められます。 • 現行の証明書の有効期間が指定のパーセンテージに達したときに、新しい証明書が要求されるように指定するには、*percent* 引数を使用します。 • 名前付きのキーがすでに存在する場合でも、証明書の新しいキーを生成するには、**regenerate** キーワードを使用します。 （注） ロールオーバー中のキー ペアがエクスポート可能な場合、新しいキー ペアもエクスポート可能です。次のコメントがトラストポイント コンフィギュレーションに表示され、キー ペアがエクスポート可能かどうかが示されます。「! RSA key pair associated with trustpoint is exportable.」

	コマンドまたはアクション	目的
		（注） 新しいキー ペアは、セキュリティ上の問題に対処するために生成することを推奨します。
ステップ 11	**usage** *method1* [*method2* [*method3*]] 例： `Router(ca-trustpoint)# usage ssl-client`	（任意）証明書の目的の用途を指定します。 • 使用可能なオプションは **ike**、**ssl-client**、および **ssl-server**で、デフォルトは **ike** です。
ステップ 12	**password** *string* 例： `Router(ca-trustpoint)# password string1`	（任意）証明書の失効パスワードを指定します。 • このコマンドがイネーブルになっている場合、このトラストポイントの登録時にパスワードは求められません。 （注） SCEP が使用されている場合、このパスワードを使用して証明書要求を認可できます（多くの場合、ワンタイム パスワードまたは類似のメカニズムによって行われます）。
ステップ 13	**rsakeypair** *key-label key-size encryption-key-size*]] 例： `Router(ca-trustpoint)# rsakeypair key-label 2048 2048`	（任意）証明書に関連付けるキー ペアを指定します。 • *key-label* 引数付きのキーペアがまだ存在しない、あるいは **auto-enroll regenerate** コマンドが発行された場合、登録時に key-label 引数付きのキーペアが生成されます。 • キーを生成するための *key-size* 引数を指定し、*encryption-key-size* 引数を指定して、個別の暗号化、署名キー、および証明書を要求します。key-size と encryption-key-size は同じサイズでなければなりません。2048 未満の長さを指定することは推奨されません。 （注） このコマンドがイネーブルでない場合に、FQDN キー ペアが使用されます。
ステップ 14	**fingerprint** *ca-fingerprint* 例： `Router(ca-trustpoint)# fingerprint 12EF53FA 355CD23E 12EF53FA 355CD23E`	（任意）認証時にCA 証明書のフィンガープリントと照合するフィンガープリントを指定します。 （注） フィンガープリントが指定されておらず、CA 証明書の認証がインタラクティブな場合、フィンガープリントは検証用に表示されます。

	コマンドまたはアクション	目的
ステップ 15	**on** *devicename* **:** 例： `Router(ca-trustpoint)# on usbtoken0:`	（任意）自動登録の初期キー生成時に、RSA キーが指定された装置に対して作成されるよう指定します。 • 指定可能な装置には、NVRAM、ローカルディスク、およびユニバーサル シリアル バス（USB）トークンがあります。USB トークンは、ストレージ デバイス以外に、暗号化装置として使用できます。USB トークンを暗号化装置として使用すると、トークンでキー生成、署名、認証などの RSA 操作を実行できます。
ステップ 16	**exit** 例： `Router(ca-trustpoint)# exit`	CA トラストポイント コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードに戻ります。
ステップ 17	**crypto pki authenticate** *name* 例： `Router(config)# crypto pki authenticate mytp`	CA 証明書を取得して、認証します。証明書フィンガープリントをチェックするよう求められた場合、証明書フィンガープリントをチェックします。 （注） CA 証明書がコンフィギュレーションにすでにロードされている場合、このコマンドはオプションです。
ステップ 18	**exit** 例： `Router(config)# exit`	グローバル コンフィギュレーション モードを終了します。

ステップ 19	**copy system:running-config nvram:startup-config**
	例：
	`Router#`
	`copy system:running-config nvram:startup-config`
		（任意）実行コンフィギュレーションを NVRAM スタートアップ コンフィギュレーションにコピーします。
		（注） 実行コンフィギュレーションが変更されていても NVRAM に書き込まれていない場合は、自動登録によってNVRAM が更新されません。

ステップ 20	**show crypto pki certificates** 例： `Router# show crypto pki certificates`	（任意）ロールオーバー証明書などの、証明書に関する情報を表示します。

手動での証明書登録の設定

手動での証明書登録は、TFTP または手動でのカットアンドペースト方式によって設定できます。これらの方式は両方とも、CA が SCEP をサポートしない場合またはルータと CA 間のネットワーク接続が不可能な場合に使用できます。手動での証明書登録を設定するには、次のいずれかの作業を実行します。

証明書登録要求用の PEM 形式ファイル

証明書要求用の PEM 形式ファイルは、端末またはプロファイルベースの登録を使用して CA サーバから証明書を要求する場合に役立ちます。PEM 形式ファイルを使用すると、ルータで既存の証明書を直接使用できます。

手動での証明書登録に関する制約事項

SCEP の制約事項

SCEP が使用されている場合、URL を切り替えることは推奨しません。つまり、登録 URL が「http://myca」である場合、CA 証明書を取得した後と証明書を登録する前で、登録 URL を変更しないでください。ユーザは、TFTP と手動でのカットアンドペーストを切り替えることができます。

キー再生に関する制約事項

crypto key generate コマンドを使用して、キーを手動で再生しないでください。キーの再生は、**regenerate** キーワードを指定して **crypto pki enroll** コマンドを発行します。

カットアンドペーストによる証明書登録の設定

この作業は、カットアンドペーストによる証明書登録を設定するために実行します。PKI に参加しているピアに対してカットアンドペースト方式による手動での証明書登録を設定するには、次の作業を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **crypto pki trustpoint** *name*
4. **enrollment terminal pem**
5. **fingerprint** *ca-fingerprint*
6. **exit**
7. **crypto pki authenticate** *name*
8. crypto pki enroll name
9. crypto pki import name certificate
10. **exit**
11. **show crypto pki certificates**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**crypto pki trustpoint** *name* 例： `Router(config)# crypto pki trustpoint mytp`	トラストポイントおよび設定された名前を宣言して、CA トラストポイント コンフィギュレーション モードを開始します。
ステップ 4	**enrollment terminal pem** 例： `Router(ca-trustpoint)# enrollment terminal`	カットアンドペーストによる手動での証明書登録方式を指定します。 • 証明書要求は、手動でコピー（または切り取り）できるように、コンソール端末上に表示されます。 • **pem**：PEM 形式の証明書要求をコンソール端末に対して生成するようトラストポイントを設定します。
ステップ 5	**fingerprint** *ca-fingerprint* 例： `Router(ca-trustpoint)# fingerprint 12EF53FA 355CD23E 12EF53FA 355CD23E`	（任意）認証時に CA 証明書のフィンガープリントと照合するフィンガープリントを指定します。 （注） フィンガープリントが指定されていない場合は、フィンガープリントは検証用に表示されます。
ステップ 6	**exit** 例： `Router(ca-trustpoint)# exit`	CA トラストポイント コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードに戻ります。
ステップ 7	**crypto pki authenticate** *name* 例： `Router(config)# crypto pki authenticate mytp`	CA 証明書を取得して、認証します。

	コマンドまたはアクション	目的
ステップ 8	crypto pki enroll name 例： `Router(config)# crypto pki enroll mytp`	証明書要求を生成し、証明書サーバにコピーおよびペーストするために要求を表示します。 • 証明書要求にルータの FQDN および IP アドレスを含めるかどうかなどの登録情報を求められます。コンソール端末に対して証明書要求を表示するかについても選択できます。 • 必要に応じて、Base 64 符号化証明書を PEM ヘッダーを付けて、または付けずに表示します。
ステップ 9	crypto pki import name certificate 例： `Router(config)# crypto pki import mytp certificate`	コンソール端末で証明書を手動でインポートします（貼り付けます）。 • Base 64 符号化証明書はコンソール端末から受け取られ、内部証明書データベースに挿入されます。 （注） 用途キー、署名キー、および暗号キーを使用する場合は、このコマンドを 2 度入力する必要があります。このコマンドが初めて入力されたとき、証明書の 1 つがルータにペーストされます。このコマンドが 2 回目に入力されたとき、もう 1 つの証明書がルータにペーストされます。どちらの証明書が先にペーストされても問題ありません。 （注） 一部の CA は、証明書要求の用途キー情報を無視し、汎用目的の証明書を発行します。ご使用の認証局がこれに該当する場合は、汎用目的の証明書をインポートしてください。ルータは、生成される 2 つのキー ペアのいずれも使用しません。
ステップ 10	**exit** 例： `Router(config)# exit`	グローバル コンフィギュレーション モードを終了します。
ステップ 11	**show crypto pki certificates** 例：	（任意）証明書、CA の証明書、および RA 証明書に関する情報を表示します。

	コマンドまたはアクション	目的
	`Router# show crypto pki certificates`	

TFTP による証明書登録の設定

この作業は、TFTP による証明書登録を設定するために実行します。この作業を実行すると、TFTP サーバを使用して手動で証明書登録を設定できます。

始める前に

- TFTP によって証明書登録を設定する場合は、使用する適切な URL がわかっている必要があります。
- **crypto pki enroll** コマンドを使用する場合、ルータにはファイルを TFTP サーバーに書き込む機能が必要です。
- ファイル指定と共に **enrollment** コマンドを使用する場合、ファイルには、バイナリフォーマットまたは Base 64 符号化の CA 証明書が含まれている必要があります。
- ご使用の CA が証明書要求内のキーの用途情報を無視し、汎用目的の証明書だけを発行するかどうかを知っておく必要があります。

⚠

注意 一部の TFTP サーバでは、サーバが書き込み可能になる前に、ファイルがサーバ上に存在している必要があります。ほとんどの TFTP サーバでは、ファイルを上書きできる必要があります。任意のルータまたは他の装置によって証明書要求が書き込まれたり、上書きされることがあるため、この要件によって危険が生じる可能性があります。そのため、証明書要求を許可する前に、まず登録要求フィンガープリントをチェックする必要がある CA 管理者は交換証明書要求を使用しません。

手順の概要

1. **enable**
2. **configure terminal**
3. **crypto pki trustpoint** *name*
4. **enrollment** [**mode**] [**retry period** minutes] [**retry count** number] **url** url [**pem**]
5. **fingerprint** *ca-fingerprint*
6. **exit**
7. **crypto pki authenticate** *name*
8. crypto pki enroll name
9. crypto pki import name certificate
10. **exit**
11. **show crypto pki certificates**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**crypto pki trustpoint** *name* 例： `Router(config)# crypto pki trustpoint mytp`	トラストポイントおよび設定された名前を宣言して、CA トラストポイント コンフィギュレーション モードを開始します。
ステップ 4	**enrollment** [**mode**] [**retry period** minutes] [**retry count** number] **url** url [**pem**] 例： `Router(ca-trustpoint)# enrollment url tftp://certserver/file_specification`	登録要求を送信して、CA 証明書とルータ証明書および任意のオプションのパラメータを取得するための登録方式として TFTP を指定します。 （注） TFTP 登録の場合、URL は TFTP URL（tftp://example_tftp_url）として設定する必要があります。 • TFTP URL には、任意のファイル指定ファイル名を使用できます。ファイル指定が含まれていない場合は、FQDN が使用されます。ファイル指定が含まれている場合は、ルータは指定されたファイル名に「.ca」という拡張子を付加します。
ステップ 5	**fingerprint** *ca-fingerprint* 例： `Router(ca-trustpoint)# fingerprint 12EF53FA 355CD23E 12EF53FA 355CD23E`	（任意）CA 管理者からアウトオブバンド方式によって受け取る CA 証明書のフィンガープリントを指定します。 （注） フィンガープリントが指定されていない場合は、フィンガープリントは検証用に表示されます。
ステップ 6	**exit** 例： `Router(ca-trustpoint)# exit`	CA トラストポイント コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードに戻ります。

	コマンドまたはアクション	目的
ステップ 7	**crypto pki authenticate** *name* 例： `Router(config)# crypto pki authenticate mytp`	指定された TFTP サーバから CA 証明書を取得して認証します。
ステップ 8	crypto pki enroll name 例： `Router(config)# crypto pki enroll mytp`	証明書要求を生成し、この要求を TFTP サーバに書き込みます。 • 証明書要求にルータの FQDN および IP アドレスを含めるかどうかなどの登録情報を求められます。コンソール端末に証明書要求を表示するかどうかについて尋ねられます。 • 書き込まれるファイル名には「.req」という拡張子が付加されます。用途キー、署名キー、および暗号キーの場合、2 つの要求が生成されて送信されます。用途キーの要求ファイル名には、拡張子「-sign.req」および「-encr.req」がそれぞれ付加されます。
ステップ 9	crypto pki import name certificate 例： `Router(config)# crypto pki import mytp certificate`	許可された証明書を取得するコンソール端末で、TFTP によって証明書をインポートします。 • ルータは、拡張子が「.req」から「.crt」に変更されたことを除いて、要求の送信に使用した同じファイル名を使用して、許可された証明書を TFTP によって取得しようと試みます。用途キー証明書の場合、拡張子「-sign.crt」および「-encr.crt」が使用されます。 • ルータは、受信したファイルを解析して証明書を検証し、証明書をルータの内部証明書データベースに挿入します。 （注） 一部の CA は、証明書要求の用途キー情報を無視し、汎用目的の証明書を発行します。ご使用の CA が証明書要求の用途キー情報を無視する場合は、汎用目的の証明書だけをインポートしてください。ルータは、生成される 2 つのキー ペアのいずれも使用しません。
ステップ 10	**exit** 例：	グローバル コンフィギュレーション モードを終了します。

	コマンドまたはアクション	目的
	`Router(config)# exit`	
ステップ 11	**show crypto pki certificates** 例： `Router# show crypto pki certificates`	（任意）証明書、CA の証明書、および RA 証明書に関する情報を表示します。

Trend Micro サーバとセキュアな通信を行うための URL リンクの認証

この作業は、Trend Micro サーバとセキュアに通信できるようにする URL フィルタリングで使用されるリンクを認証するために実行します。

（注） セキュリティに対する脅威は、脅威からの保護に役立つ暗号化技術と同様に絶え間なく変化しています。最新のシスコの暗号化に関する推奨事項については、『*Next Generation Encryption*』（NGE）ホワイト ペーパーを参照してください。

手順の概要

1. **enable**
2. **clock set** *hh* **:** *mm* **:** *ss date month year*
3. **configure terminal**
4. **clock timezone** *zone hours-offset* [*minutes-offset*]
5. **ip http server**
6. **hostname** *name*
7. **ip domain-name** *name*
8. **crypto key generate rsa general-keys modulus** *modulus-size*
9. **crypto pki trustpoint** *name*
10. **enrollment terminal**
11. **crypto ca authenticate** *name*
12. Base 64 符号化の CA 証明書が含まれている次のテキスト部分をコピーし、プロンプトにペーストします。
13. **yes** と入力し、この証明書を受け入れます。
14. **serial-number**
15. **revocation-check none**
16. **end**
17. **trm register**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**clock set** *hh* **:** *mm* **:** *ss date month year* 例： `Router# clock set 23:22:00 22 Dec 2009`	ルータのクロックを設定します。
ステップ 3	**configure terminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 4	**clock timezone** *zone hours-offset* [*minutes-offset*] 例： `Router(config)# clock timezone PST -08`	時間帯を設定します。 • *zone* 引数は、時間帯の名前です（通常は標準略語）。*hours-offset* 引数は、使用する時間帯が協定世界時（UTC）から異なる時間数です。*minutes-offset* 引数は、使用する時間帯が UTC から異なる分数です。 （注） **clock timezone** コマンドの *minutes-offset* 引数は、ローカル時間帯の UTC またはグリニッジ標準時（GMT）からの差が 1 時間未満の割合で異なる場合に使用できます。たとえば、アトランティック カナダの一部の地域の時間帯（大西洋標準時（AST））は UTC-3.5 です。この場合に必要なコマンドは、**clock timezone AST -3 30** です。
ステップ 5	**ip http server** 例： `Router(config)# ip http server`	HTTP サーバーを有効にします。
ステップ 6	**hostname** *name* 例： `Router(config)# hostname hostname1`	ルータのホスト名を設定します。

	コマンドまたはアクション	目的
ステップ 7	**ip domain-name** *name* 例： `Router(config)# ip domain-name example.com`	ルータのドメイン名を定義します。
ステップ 8	**crypto key generate rsa general-keys modulus** *modulus-size* 例： `Router(config)# crypto key generate rsa general-keys modulus general`	暗号キーを生成します。 • **general-keys** キーワードは、汎用のキーペアが生成されることを指定します。これがデフォルトです。 • **modulus** キーワードと *modulus-size* 引数は、キーのモジュラスの IP サイズを指定します。デフォルトでは、CA キーのモジュラス サイズは 1024 ビットです。RSA キーを生成する場合、モジュラスの長さを入力するように促されます。モジュラスの長さが長いほど安全性が高まりますが、生成と使用にかかる時間も長くなります。2048 未満の長さを指定することは推奨されません。 （注） 生成される汎用キーの名前は、手順 7 で設定したドメイン名に基づきます。たとえば、キーの名前は「example.com」になります。
ステップ 9	**crypto pki trustpoint** *name* 例： `Router(config)# crypto pki trustpoint mytp`	ルータが使用する CA を宣言し、CA トラストポイント コンフィギュレーション モードを開始します。 （注） Cisco IOS リリース 12.3(8)T では、**crypto pki trustpoint** コマンドが **crypto ca trustpoint** コマンドに置き換えられました。
ステップ 10	**enrollment terminal** 例： `Router(ca-trustpoint)# enrollment terminal`	カットアンドペーストによる手動での証明書登録方式を指定します。 • 証明書要求は、手動でコピー（または切り取り）できるように、コンソール端末上に表示されます。
ステップ 11	**crypto ca authenticate** *name* 例： `Router(ca-trustpoint)# crypto ca authenticate mytp`	CA の名前を引数として取得し、これを認証します。 • 次のコマンドの出力が表示されます。

	コマンドまたはアクション	目的
		Enter the base 64 encoded CA certificate. End with a blank line or the word "quit" on a line by itself.
ステップ 12	Base 64 符号化の CA 証明書が含まれている次のテキスト部分をコピーし、プロンプトにペーストします。	MIIDIDCCAcmgAwIBAgIENd70zzANBgkqhkiG9w0BAQUFADBOMQswCQYDVQQGEwJV UzEQMA4GA1UEChMHRXF1aWZheDEtMCsGA1UECxMkRXF1aWZheCBIZWN1cmUgQ2Vy dGlmaWNhdGUgQXV0aG9yaXR5MB4XDTk4MDgyMjE2NDE1MVoXDTE4MDgyMjE2NDE1 MVowTjELMAkGA1UEBhMCVVMxEDAOBgNVBAoTB0VxdWlmYXgxLTArBgNVBAsTJEVx dWlmYXggU2VjdXJlIENlcnRpZmljYXRlIEF1dGhvcml0eTCBnzANBgkqhkiG9w0B AQEFAAOBjQAwgYkCgYEAwV2xWGcIYu6gmi0fCG2RFGiYCh7+2gRvE4RiIcPRfM6f BeC4AfBONOziipUEZKzxa1NfBbPLZ4C/QgKO/t0BCezhABRP/PvwDN1Dulsr4R+A cJkVV5MW8Q+XarfCaCMczE1ZMKxRHjuvK9buY0V7xdlfUNLjUA86iOe/FP3gx7kC AwEAAaOCAQkwggEFMHAGA1UdHwRpMGcwZaBjoGGkXzBdMQswCQYDVQQGEwJVUzEQ MA4GA1UEChMHRXF1aWZheDEtMCsGA1UECxMkRXF1aWZheCBIZWN1cmUgQ2VydGlm aWNhdGUgQXV0aG9yaXR5MQ0wCwYDVQQDEwRDUkwxMBoGA1UdEAQTMBGBDzIwMTgw ODIyMTY0MTUxWjALBgNVHQ8EBAMCAQYwHwYDVR0jBBgwFoAUSOZo+SvSspXXR9gj IBBPM5iQn9QwHQYDVR0OBBYEFEjmaPkr0rKV10fYIyAQTzOYkJ/UMAwGA1UdEwQF MAMBAf8wGgYJKoZIhvZ9B0EABA0wCxsFVjMuMGMDAgbAMA0GCSqGSIb3DQEBBQUA A4GBAFjOKer89961zgK5F7WF0bnj4JXMJTENAKaSbn+2kmOeUJXRmm/kEd5jhW6Y 7qj/WsjTVboJmcVfewCHrPSqnI0kBBIZCe/zuf6IWUrVnZ9NA2zsmWLIodz2uFHdh 1voqZiegDfqnc1zqcPGUIWVEX/r87yloqaKHee9570+sB3c4 次のコマンドの出力が表示されます。 Certificate has the following attributes: Fingerprint MD5: 67CB9DC0 13248A82 9BB2171E D11BECD4 Fingerprint SHA1: D23209AD 23D31423 2174E40D 7F9D6213 9786633A

	コマンドまたはアクション	目的

ステップ 13	**yes** と入力し、この証明書を受け入れます。	`% Do you accept this certificate? [yes/no]: yes`
		次のコマンドの出力が表示されます。
		`Trustpoint CA certificate accepted.`
		`% Certificate successfully imported`

ステップ 14	**serial-number** 例： `hostname1(ca-trustpoint)# serial-number`	ルータのシリアル番号を証明書要求で指定します。
ステップ 15	**revocation-check none** 例： `hostname1(ca-trustpoint)# revocation-check none` 例：	証明書の確認が無視されることを指定します。
ステップ 16	**end** 例： `hostname1(ca-trustpoint)# end`	CA トラストポイントコンフィギュレーションモードを終了し、特権 EXEC モードに戻ります。
ステップ 17	**trm register** 例： `hostname1# trm register`	Trend Micro サーバ登録プロセスを手動で開始します。

登録用の永続的自己署名証明書の SSL による設定

ここでは、次のタスクについて説明します。

（注） これらの作業は任意です。これは、HTTPS サーバをイネーブルにした場合、このサーバがデフォルト値を使用して自動的に自己署名証明書を生成するからです。

永続的自己署名証明書の概要

SSL プロトコルは、HTTPS サーバとクライアント（Web ブラウザ）の間でセキュアな接続を確立するために使用されます。SSL ハンドシェイクの間、クライアントは、すでに所有している証明書を使用して SSL サーバの証明書が検証可能であると想定します。

Cisco IOS ソフトウェアが HTTP サーバで使用できる証明書を保持していない場合、サーバは、PKI アプリケーション プログラミング インターフェイス（API）を呼び出して自己署名証明書を生成します。クライアントがこの自己署名証明書を受け取ったにもかかわらず、検証できない場合、ユーザによる介入が必要です。クライアントは、証明書を受け入れるか、あとで使用するために保存するかどうかを尋ねます。証明書を受け入れると、SSL ハンドシェイクは続行されます。

それ以降、同じクライアントとサーバ間の SSL ハンドシェイクでは、同じ証明書が使用されます。ただし、ルータをリロードすると、自己署名証明書は失われます。その場合、HTTPS サーバは新しい自己署名証明書を作成する必要があります。この新しい自己署名証明書は前の証明書と一致しないため、この自己署名証明書を受け入れるかどうか再度確認されます。

ルータがリロードするたびにルータの証明書を受け入れるかどうか確認されると、この確認中に、攻撃者に不正な証明書を使用する機会を与えてしまうことがあります。永続的自己署名証明書では、ルータのスタートアップ コンフィギュレーションに証明書を保存することにより、これらの制約をすべて解消しています。

機能制限

- 1 つの永続的自己署名証明書には、トラストポイントを 1 つだけ設定できます。
- 自己署名証明書の最大ライフタイムは、2030 年 1 月 1 日 00:00:00 GMT です。

（注） 自己署名証明書の作成後は、ルータの IP ドメイン名またはホスト名を変更しないでください。いずれかの名前を変更すると、自己署名証明書の再生がトリガーされて、設定済みのトラストポイントが上書きされます。WebVPN は、SSL トラストポイント名を WebVPN ゲートウェイ設定に結合します。新しい自己署名証明書がトリガーされると、新しいトラストポイント名が WebVPN 設定と一致しなくなり、WebVPN 接続は失敗します。

トラストポイントの設定および自己署名証明書パラメータの指定

（注） セキュリティに対する脅威は、脅威からの保護に役立つ暗号化技術と同様に絶え間なく変化しています。最新のシスコの暗号化に関する推奨事項については、『*Next Generation Encryption*』（NGE）ホワイト ペーパーを参照してください。

トラストポイントを設定し、自己署名証明書パラメータを指定するには、次の作業を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **crypto pki trustpoint** name
4. **enrollment selfsigned**
5. **subject-name** [*x.500-name*]
6. **rsakeypair** *key-label* [key-size [encryption-key-size]]
7. **crypto pki enroll** name
8. **end**
9. **show crypto pki certificates** [*trustpoint-name*[**verbose**]]
10. **show crypto pki trustpoints** [**status** | *label* [**status**]]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**crypto pki trustpoint** name 例： `Router(config)# crypto pki trustpoint local`	ルータが使用する CA を宣言し、CA トラストポイント コンフィギュレーション モードを開始します。 （注） Cisco IOS リリース 12.3(8)T では、**crypto pki trustpoint** コマンドが **crypto ca trustpoint** コマンドに置き換えられました。
ステップ 4	**enrollment selfsigned** 例： `Router(ca-trustpoint)# enrollment selfsigned`	自己署名登録を指定します。
ステップ 5	**subject-name** [*x.500-name*] 例： `Router(ca-trustpoint)# subject-name`	（任意）証明書要求に使用する要求件名を指定します。 • *x-500-name* 引数を指定しない場合、デフォルト件名である FQDN が使用されます。
ステップ 6	**rsakeypair** *key-label* [key-size [encryption-key-size]] 例：	（任意）証明書に関連付けるキー ペアを指定します。

	コマンドまたはアクション	目的
	`Router(ca-trustpoint)# rsakeypair examplekey 2048`	• *key-label* 引数の値がまだ存在しない、あるいは **auto-enroll regenerate** コマンドが発行された場合は、登録時にこの引数の値が生成されます。 • キーを生成するための *key-size* 引数を指定し、*encryption-key-size* 引数を指定して、個別の暗号化、署名キー、および証明書を要求します。key-size と encryption-key-size は同じサイズでなければなりません。2048 未満の長さを指定することは推奨されません。 （注） このコマンドがイネーブルでない場合に、FQDN キー ペアが使用されます。
ステップ 7	**crypto pki enroll** name 例： `Router(config)# crypto pki enroll local`	永続的自己署名証明書を生成するようルータに指示します。
ステップ 8	**end** 例： `Router(ca-trustpoint)# end`	（任意）CA トラストポイント コンフィギュレーション モードを終了します。 • グローバル コンフィギュレーション モードを終了するため、このコマンドをもう一度入力します。
ステップ 9	**show crypto pki certificates** [*trustpoint-name*[**verbose**]] 例： `Router# show crypto pki certificates local verbose`	証明書、認証局証明書、および任意の登録認局証明書に関する情報を表示します。
ステップ 10	**show crypto pki trustpoints** [**status** | *label* [**status**]] 例： `Router# show crypto pki trustpoints status`	ルータに設定されているトラストポイントを表示します。

HTTPS サーバのイネーブル化

HTTPS サーバをイネーブルにするには、次の作業を実行します。

始める前に

パラメータを指定するには、トラストポイントを作成し、設定する必要があります。デフォルト値を使用するには、すべての既存の自己署名トラストポイントを削除します。自己署名トラ

ストポイントをすべて削除すると、HTTPS サーバがイネーブルになるとただちに、サーバはデフォルト値を使用して永続的自己署名証明書を生成します。

手順の概要

1. **enable**
2. **configure terminal**
3. **ip http secure-server**
4. **end**
5. **copy system:running-config nvram: startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ip http secure-server** 例： `Router(config)# ip http secure-server`	HTTPS Web サーバをイネーブルにします。 （注） キーペア（Modulus 1024）および自己署名証明書が自動的に生成されます。
ステップ 4	**end** 例： `Router(config)# end`	グローバル コンフィギュレーション モードを終了します。
ステップ 5	**copy system:running-config nvram: startup-config** 例： `Router# copy system:running-config nvram: startup-config`	イネーブルになっているモードで自己署名証明書および HTTPS サーバを保存します。

登録または再登録用の証明書登録プロファイルの設定

この作業は、登録または再登録用の証明書登録プロファイルを設定するために実行します。この作業は、サードパーティ ベンダー製 CA にすでに登録されている証明書またはルータを Cisco IOS CA に登録または再登録するための登録プロファイルを設定するのに役立ちます。

登録要求が自動的に許可されるように、サードパーティ ベンダー製CAに登録されているルータを Cisco IOS 証明書サーバに登録するには、このルータをイネーブルにして、その既存の証明書を使用します。この機能をイネーブルにするには、**enrollment credential** コマンドを発行する必要があります。また、手動による証明書登録は設定できません。

始める前に

次の作業は、サードパーティ ベンダー製 CA にすでに登録されているクライアント ルータの証明書登録プロファイルを設定する前に、クライアントルータで実行します。これにより、そのルータを Cisco IOS 証明書サーバに再登録できます。

- サードパーティ ベンダー製 CA をポイントするトラストポイントの定義
- サードパーティ ベンダー製 CA でのクライアント ルータの認証および登録

（注）
- 証明書プロファイルを使用するには、ネットワークに、CA への HTTP インターフェイスが設定されている必要があります。
- 登録プロファイルが指定されている場合、トラストポイント設定に登録 URL が指定されていないことがあります。両方のコマンドがサポートされていても、トラストポイントに使用できるコマンドは一度に 1 つだけです。
- 各 CA で使用される HTTP コマンドには規格がないため、ユーザは使用している CA に適したコマンドを入力する必要があります。

>

手順の概要

1. **enable**
2. **configure terminal**
3. **crypto pki trustpoint** *name*
4. enrollment profile label
5. **exit**
6. **crypto pki profile enrollment** *label*
7. 次のいずれかを実行します。
   - **authentication url** *url*
   - **authentication terminal**
8. **authentication command**
9. 次のいずれかを実行します。
   - **enrollment url** *url*
   -
   - **enrollment terminal**
10. **enrollment credential** *label*
11. **enrollment command**

12. **parameter** *number* {**value** *value* | **prompt** *string*}
13. **exit**
14. **show crypto pki certificates**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**crypto pki trustpoint** *name* 例： `Router(config)# crypto pki trustpoint Entrust`	トラストポイントおよび設定された名前を宣言して、CA トラストポイント コンフィギュレーション モードを開始します。
ステップ 4	enrollment profile label 例： `Router(ca-trustpoint)# enrollment profile E`	登録プロファイルが証明書認証および登録用に使用されるように指定します。
ステップ 5	**exit** 例： `Router(ca-trustpoint)# exit`	CA トラストポイント コンフィギュレーション モードを終了します。
ステップ 6	**crypto pki profile enrollment** *label* 例： `Router(config)# crypto pki profile enrollment E`	登録プロファイルを定義し、ca-profile-enroll コンフィギュレーション モードを開始します。 • *label*：登録プロファイルの名前。登録プロファイル名は、**enrollment profile** コマンドで指定された名前と同じである必要があります。
ステップ 7	次のいずれかを実行します。 • **authentication url** *url* • **authentication terminal** 例： `Router(ca-profile-enroll)# authentication url http://entrust:81`	証明書認証要求の送信先となる CA サーバの URL を指定します。 • *url*：ルータが認証要求を送信する CA サーバーの URL。HTTP を使用する場合、URL は「http://CA_name」という形式にする必要があります。ここで、CA_name は CA のホスト DNS 名または IP アドレスです。TFTP を使用する場

	コマンドまたはアクション	目的
	例： `Router(ca-profile-enroll)# authentication terminal`	合、この URL は「tftp://certserver/file_specification」という形式にする必要があります。（URL にファイル指定が含まれない場合、ルータの FQDN が使用されます。） カットアンドペーストによる手動での証明書認証を指定します。
ステップ 8	**authentication command** 例： `Router(ca-profile-enroll)# authentication command`	（任意）認証のために CA に送信される HTTP コマンドを指定します。

ステップ 9	次のいずれかを実行します。
	• **enrollment url** *url*
	•
	• **enrollment terminal**
	例：
	`Router(ca-profile-enroll)# enrollment url http://entrust:81/cda-cgi/clientcgi.exe`
	例：
	例：
	`Router(ca-profile-enroll)# enrollment terminal`
		証明書登録要求を HTTP または TFTP によって送信する CA サーバの URL を指定します。
		カットアンドペーストによる手動での証明書登録を指定します。

ステップ 10	**enrollment credential** *label* 例： `Router(ca-profile-enroll)# enrollment credential Entrust`	（任意）Cisco IOS CA に登録されるサードパーティベンダー製 CA トラストポイントを指定します。 （注） 手動での証明書登録が使用されている場合、このコマンドは発行できません。
ステップ 11	**enrollment command** 例： `Router(ca-profile-enroll)# enrollment command`	（任意）登録のために CA に送信される HTTP コマンドを指定します。
ステップ 12	**parameter** *number* {**value** *value* | **prompt** *string*} 例： `Router(ca-profile-enroll)# parameter 1 value aaaa-bbbb-cccc`	（任意）登録プロファイルのパラメータを指定します。 • このコマンドを繰り返して使用すると、複数の値を指定できます。

	コマンドまたはアクション	目的
ステップ 13	**exit** 例： `Router(ca-profile-enroll)# exit`	（任意）ca-profile-enroll コンフィギュレーション モードを終了します。 • グローバル コンフィギュレーション モードを終了するため、このコマンドをもう一度入力します。
ステップ 14	**show crypto pki certificates** 例： `Router# show crypto pki certificates`	（任意）証明書、CA の証明書、および RA 証明書に関する情報を表示します。

次の作業

Cisco IOS CA に再登録するようにルータを設定した場合にこの機能を活用するには、指定されたサードパーティ ベンダー製CA トラストポイントに登録されたクライアントからだけ登録要求を受け入れるように Cisco IOS 証明書サーバを設定する必要があります。詳細については、「Configuring and Managing a Cisco IOS Certificate Server for PKI Deployment」を参照してください。

2 階層 PKI 環境での証明書登録の設定

この機能により、ルート CA がオフラインのときにサブ CA がクライアントに証明書を発行できます。ルート証明書は、最初にCLIを使用してインポートできます。その後、ルート証明書を使用して、トラストポイントで設定された発行サブ CA 証明書を検証します。

（注） 次のタスクを実行する前に、環境に応じて失効チェックを有効にします。

端末を介して ROOT-CA をインポートするには、次の手順を実行します。

```
enable
!
configure terminal
!
crypto pki trustpoint ROOT-CA
revocation-check none
enrollment terminal
!
crypto pki authenticate ROOT-CA
!
exit
```

フィンガープリントを指定または受け入れずにSUB-CA を認証する場合は、次の手順を実行します。

```
enable
!
```

```
configure terminal
!
crypto pki trustpoint SUB-CA
revocation-check none
enrollment url url
chain-validation continue ROOT-CA
exit
!
crypto pki authenticate SUB-CA
exit
```

複数のトラストポイントの有効化による証明書の更新の設定

Cisco IOS XE 17.4.1 リリース以降では、登録局が証明書の初期登録および証明書の更新のために複数のトラストポイントを使用してルータのログイン情報を検証することを実現できます。この機能拡張により、SCEP 登録プロトコルを介したゼロタッチ証明書登録を維持しながら、複数のトラストポイントの自動検証が可能になります。

ルータを初めて登録すると、SCEP 要求が開始され、この要求は SUDI ログイン情報を使用して署名されます。その後、要求が登録局に送信され、登録局は、ローカルトラストポイントを介して SUDI 証明書を検証します。ローカルトラストポイントは、ルータ SCEP ログイン情報を検証します。検証が成功すると、登録局は、SUDI 証明書を使用して署名を復号し、ハッシュを検証します。ハッシュ検証も成功すると、登録局は、SCEP 要求を認証局（CA）に転送します。次に、CA は、要求に署名し、証明書を登録局に送り返します。登録局は、証明書をルータに転送します。この時点で、SCEP の登録が完了です。

証明書の更新の場合、同じプロセスに従うと、更新は失敗します。これは、ルータが現在の証明書をログイン情報として使用するため、登録局が更新要求を検証できないからです。登録局がルータのアイデンティティを検証するために使用できるトラストポイントは 1 つだけであるため、証明書の更新は失敗します。

この問題を解決するために、複数のトラストポイントを使用してルータのログイン情報を検証するように登録局を設定できるようになりました。このようにして、初期登録と更新がシームレスに機能します。

複数のトラストポイントを設定するには、**grant auto <tp-list>** コマンドを使用します。このコマンドを使用して、最大 5 つのトラストポイントを設定できます。次に例を示します。

```
grant auto tp-list <tp1 tp2>
grant auto tp-list <tp1 tp2 tp3>
grant auto tp-list <tp1 tp2 tp3 tp4>
grant auto tp-list <tp1 tp2 tp3 tp4 tp5>
```

トラストポイントを設定すると、登録局は、設定されたいずれかのトラストポイントを使用して受信した証明書を検証します。検証は最初のトラストポイントから開始されます。検証が成功すると、証明書が更新されます。それ以外の場合、登録局は、次に使用可能なトラストポイントを使用して検証します。

設定例

```
crypto pki server FANRSACA
no database archive
grant auto <tp-list> ACT2_SUDI_CA <CA_TRUSTPOINT>
```

```
hash sha256
mode ra transparent
!
crypto pki trustpoint FANRSACA
enrollment url http://10.4.1.117:8080/ejbca/publicweb/apply/scep/FANRSACA
serial-number none
fqdn none
ip-address none
subject-name serialNumber=PID:ISR4451-X/K9 SN:FOC23231CRY, CN=ISR4k-1-ra
revocation-check none
rsakeypair FANRSACA_Key 4096
!
crypto pki trustpoint ACT2_SUDI_CA
enrollment profile ACT2_SUDI_CA
revocation-check none
!
crypto pki trustpool policy
revocation-check none
```

（注） **grant auto trustpoint** と **grant auto tp-list** は、相互に排他的です。すでに grant auto trustpoint を設定している場合は、**grant auto tp-list** コマンドを実行できません。

PKI 証明書登録要求の設定例

証明書登録または自動登録の設定例

次の例では、「mytp-A」証明書サーバおよび関連付けられたトラストポイントの設定を示します。この例では、トラストポイントの初期の自動登録によって生成された RSA キーが USB トークン「usbtoken0」に保管されます。

```
crypto pki server mytp-A
   database level complete
   issuer-name CN=company, L=city, C=country
   grant auto
! Specifies that certificate requests will be granted automatically.
!
crypto pki trustpoint mytp-A
   revocation-check none
   rsakeypair myTP-A
   storage usbtoken0:
! Specifies that keys will be stored on usbtoken0:.
   on usbtoken0:
```

! Specifies that keys generated on initial auto enroll will be generated on and stored o**n !** usbtoken0:

自動登録の設定例

次の例では、自動ロールオーバーをイネーブルにして、ルータが起動時に自動的に CA に登録されるように設定する方法、および必要なすべての登録情報を設定に指定する方法を示します。

```
crypto pki trustpoint trustpt1
 enrollment url http://trustpt1.example.com//
 subject-name OU=Spiral Dept., O=example.com
 ip-address ethernet-0
 serial-number none
 usage ike
 auto-enroll regenerate
 password password1
 rsa-key trustpt1 2048
!
crypto pki certificate chain trustpt1
certificate pki 0B
30820293 3082023D A0030201 0202010B 300D0609 2A864886 F70D0101 04050030
79310B30 09060355 04061302 5553310B 30090603 55040813 02434131 15301306
0355040A 130C4369 73636F20 53797374 656D3120 301E0603 55040B13 17737562
6F726420 746F206B 6168756C 75692049 50495355 31243022 06035504 03131B79
6E692D75 31302043 65727469 66696361 7465204D 616E6167 6572301E 170D3030
30373134 32303536 32355A17 0D303130 37313430 31323834 335A3032 310E300C
06035504 0A130543 6973636F 3120301E 06092A86 4886F70D 01090216 11706B69
2D343562 2E636973 636F2E63 6F6D305C 300D0609 2A864886 F70D0101 01050003
4B003048 024100B3 0512A201 3B4243E1 378A9703 8AC5E3CE F77AF987 B5A422C4
15E947F6 70997393 70CF34D6 63A86B9C 4347A81A 0551FC02 ABA62360 01EF7DD2
6C136AEB 3C6C3902 03010001 A381F630 81F3300B 0603551D 0F040403 02052030
1C060355 1D110415 30138211 706B692D 3435622E 63697363 6F2E636F 6D301D06
03551D0E 04160414 247D9558 169B9A21 23D289CC 2DDA2A9A 4F77C616 301F0603
551D2304 18301680 14BD742C E892E819 1D551D91 683F6DB2 D8847A6C 73308185
0603551D 1F047E30 7C307AA0 3CA03AA4 38303631 0E300C06 0355040A 13054369
73636F31 24302206 03550403 131B796E 692D7531 30204365 72746966 69636174
65204D61 6E616765 72A23AA4 38303631 0E300C06 0355040A 13054369 73636F31
24302206 03550403 131B796E 692D7531 30204365 72746966 69636174 65204D61
6E616765 72300D06 092A8648 86F70D01 01040500 03410015 BC7CECF9 696697DF
E887007F 7A8DA24F 1ED5A785 C5C60452 47860061 0C18093D 08958A77 5737246B
0A25550A 25910E27 8B8B428E 32F8D948 3DD1784F 954C70
quit
```

（注） この例では、キーは再生もロールオーバーもされません。

証明書自動登録とキー再生の設定例

次の例では、ルータが起動時に「trustme1」という CA に自動的に登録され、自動ロールオーバーがイネーブルになるように設定する方法を示します。**regenerate** キーワードが発行されるため、自動ロールオーバープロセスが開始されると、新しいキーが証明書に対して生成され、再発行されます。更新パーセンテージが 90 に設定されているため、証明書の有効期間が 1 年の場合は、古い証明書が失効する 36.5 日前に新しい証明書が要求されます。実行コンフィギュレーションを変更しても、NVRAMに書き込まないかぎり自動登録によってNVRAMが更新されないため、実行コンフィギュレーションの変更はNVRAMスタートアップ コンフィギュレーションに保存されます。

```
crypto pki trustpoint trustme1
 enrollment url http://trustme1.example.com/
 subject-name OU=Spiral Dept., O=example.com
 ip-address ethernet0
 serial-number none
 auto-enroll 90 regenerate
```

```
 password password1
 rsakeypair trustme1 2048
 exit
crypto pki authenticate trustme1
copy system:running-config nvram:startup-config
```

カットアンドペーストによる証明書登録の設定例

次の例では、カットアンドペーストによる手動での登録方式を使用して、証明書登録を設定する方法を示します。

```
Router(config)#
crypto pki trustpoint TP
Router(ca-trustpoint)#
enrollment terminal
Router(ca-trustpoint)#
crypto pki authenticate TP
Enter the base 64 encoded CA certificate.
End with a blank line or the word "quit" on a line by itself
-----BEGIN CERTIFICATE-----
MIICNDCCAd6gAwIBAgIQOsCmXpVHwodKryRoqULV7jANBgkqhkiG9w0BAQUFADA5
MQswCQYDVQQGEwJVUzEWMBQGA1UEChMNQ2lzY28gU3lzdGVtczESMBAGA1UEAxMJ
bXNjYS1yb290MB4XDTAyMDIxNDAwNDYwMVoXDTA3MDIxNDAwNTQ0OFowOTELMAkG
A1UEBhMCVVMxFjAUBgNVBAoTDUNpc2NvIFN5c3RlbXMxEjAQBgNVBAMTCW1zY2Et
cm9vdDBcMA0GCSqGSIb3DQEBAQUAA0sAMEgCQQCix8nIGFg+wvy3BjFbVi25wYoG
K2N0HWWHpqxFuFhqyBnIC0OshIn9CtrdN3JvUNHr0NIKocEwNKUGYmPwWGTfAgMB
AAGjgcEwgb4wCwYDVR0PBAQDAgHGMA8GA1UdEwEB/wQFMAMBAf8wHQYDVR0OBBYE
FKIacsl6dKAfuNDVQymlSp7esf8jMG0GA1UdHwRmMGQwL6AtoCuGKWh0dHA6Ly9t
c2NhLXJvb3QvQ2VydEVucm9sbC9tc2NhLXJvb3QuY3JsMDGgL6AthitmaWxlOi8v
XFxtc2NhLXJvb3RcQ2VydEVucm9sbFxtc2NhLXJvb3QuY3JsMBAGCSsGAQQBgjcV
AQQDAgEAMA0GCSqGSIb3DQEBBQUAA0EAeuZkZMX9qkoLHfETYTpVWjZPQbBmwNRA
oJDSdYdtL3BcI/uLL5q7EmODyGfLyMGxuhQYx5r/40aSQgLCqBq+yg==
-----END CERTIFICATE-----
Certificate has the following attributes:
Fingerprint: D6C12961 CD78808A 4E02193C 0790082A
% Do you accept this certificate? [yes/no]:
y
Trustpoint CA certificate accepted.
% Certificate successfully imported
Router(config)#
crypto pki enroll TP
% Start certificate enrollment..
% The subject name in the certificate will be:
Router.example.com
% Include the router serial number in the subject name? [yes/no]:
n
% Include an IP address in the subject name? [no]:
n
Display Certificate Request to terminal? [yes/no]:
y
Signature key certificate request -
Certificate Request follows:
MIIBhTCB7wIBADAlMSMwIQYJKoZIhvcNAQkCFhRTYW5kQmFnZ2VyLmNpc2NvLmNv
bTCBnzANBgkqhkiG9w0BAQEFAAOBjQAwgYkCgYEAxdhXFDiWAn/hIZs9zfOtssKA
daoWYu0ms9Fe/Pew01dh14vXdxgacstOs2Pr5wk6jLOPxpvxOJPWyQM6ipLmyVxv
ojhyLTrVohrh6Dnqcvk+G/5ohss9o9RxvONwx042pQchFnx9EkMuZC7evwRxJEqR
mBHXBZ8GmP3jYQsjS8MCAwEAAaAhMB8GCSqGSIb3DQEJDjESMBAwDgYDVR0PAQH/
BAQDAgeAMA0GCSqGSIb3DQEBBAUAA4GBAMT6WtyFw95POY7UtF+YIYHiVRUf4SCq
hRIAGrljUePLo9iTqyPU1Pnt8JnIZ5P5BHU3MfgP8sqodaWub6mubkzaohJ1qD06
O87fnLCNid5Tov5jKogFHIki2EGGZxBosUw9lJlenQdNdDPbJc5LIWdfDvciA6jO
Nl8rOtKnt8Q+
```

```
!
!
!
Redisplay enrollment request? [yes/no]:
Encryption key certificate request -
Certificate Request follows:
MIIBhTCB7wIBADAlMSMwIQYJKoZIhvcNAQkCFhRTYW5kQmFnZ2VyLmNpc2NvLmNv
bTCBnzANBgkqhkiG9w0BAQEFAAOBjQAwgYkCgYEAwG60QojpDbzbKnyj8FyTiOcv
THkDP7XD4vLT1XaJ409z0gSIoGnIcdFtXhVlBWtpq3/O9zYFXr1tH+BMCRQi3Lts
0IpxYa3D9iFPqev7SPXpsAIsY8a6FMq7TiwLObqiQjLKL4cbuV0Frjl0Yuv5A/Z+
kqMOm7c+pWNWFdLe9lsCAwEAAaAhMB8GCSqGSIb3DQEJDjESMBAwDgYDVR0PAQH/
BAQDAgUgMA0GCSqGSIb3DQEBBAUAA4GBACF7feURj/fJMojPBlR6fa9BrlMJx+2F
H91YM/CIiz2n4mHTeWTWKhLoT8wUfa9NGOk7yi+nF/F7035twLfq6n2bSCTW4aem
8jLMMaeFxwkrV/ceQKrucmNC1uVx+fBy9rhnKx8j60XE25tnp1U08r6om/pBQABU
eNPFhozcaQ/2
!
!
!
Redisplay enrollment request? [yes/no]:
n
Router(config)#
crypto pki import TP certificate
Enter the base 64 encoded certificate.
End with a blank line or the word "quit" on a line by itself
MIIDajCCAxSgAwIBAgIKFN7C6QAAAAAMRzANBgkqhkiG9w0BAQUFADA5MQswCQYD
VQQGEwJVUzEWMBQGA1UEChMNQ2lzY28gU3lzdGVtczESMBAGA1UEAxMJbXNjYS1y
b290MB4XDTAyMDYwODAxMTY0MloXDTAzMDYwODAxMjY0MlowJTEjMCEGCSqGSIb3
DQEJAhMUU2FuZEJhZ2dlci5jaXNjby5jb20wgZ8wDQYJKoZIhvcNAQEBBQADgY0A
MIGJAoGBAMXYVxQ4lgJ/4SGbPc3zrbLCgHWqFmLtJrPRXvz3sNNXYdeL13cYGnLL
TrNj6+cJOoyzj8ab8TiT1skDOoqS5slcb6I4ci061aIa4eg56nL5Phv+aIbLPaPU
cbzjcMdONqUHIRZ8fRJDLmQu3r8EcSRKkZgR1wWfBpj942ELI0vDAgMBAAGjggHM
MIIByDALBgNVHQ8EBAMCB4AwHQYDVR0OBBYEFL8Quz8dyz4EGIeKx9A8UMNHLE4s
MHAGA1UdIwRpMGeAFKIacsl6dKAfuNDVQymlSp7esf8joT2kOzA5MQswCQYDVQQG
EwJVUzEWMBQGA1UEChMNQ2lzY28gU3lzdGVtczESMBAGA1UEAxMJbXNjYS1yb290
ghA6wKZelUfCh0qvJGipQtXuMCIGA1UdEQEB/wQYMBaCFFNhbmRCYWdnZXIuY2lz
Y28uY29tMG0GA1UdHwRmMGQwL6AtoCuGKWh0dHA6Ly9tc2NhLXJvb3QvQ2VydEVu
cm9sbC9tc2NhLXJvb3QuY3JsMDGgL6AthitmaWxlOi8vXFxtc2NhLXJvb3RcQ2Vy
dEVucm9sbFxtc2NhLXJvb3QuY3JsMIGUBggrBgEFBQcBAQSBhzCBhDA/BggrBgEF
BQcwAoYzaHR0cDovL21zY2Etcm9vdC9DZXJ0RW5yb2xsL21zY2Etcm9vdF9tc2Nh
LXJvb3QuY3J0MEEGCCsGAQUFBzAChjVmaWxlOi8vXFxtc2NhLXJvb3RcQ2VydEVu
cm9sbFxtc2NhLXJvb3RfbXNjYS1yb290LmNydDANBgkqhkiG9w0BAQUFAANBAJo2
r6sHPGBdTQX2EDoJpR/A2UHXxRYqVSHkFKZw0z31r5JzUM0oPNUETV7mnZlYNVRZ
CSEX/G8boi3WOjz9wZo=
% Router Certificate successfully imported
Router(config)#
crypto pki import TP cert
Enter the base 64 encoded certificate.
End with a blank line or the word "quit" on a line by itself
MIIDajCCAxSgAwIBAgIKFN7OBQAAAAAMSDANBgkqhkiG9w0BAQUFADA5MQswCQYD
VQQGEwJVUzEWMBQGA1UEChMNQ2lzY28gU3lzdGVtczESMBAGA1UEAxMJbXNjYS1y
b290MB4XDTAyMDYwODAxMTY0NVoXDTAzMDYwODAxMjY0NVowJTEjMCEGCSqGSIb3
DQEJAhMUU2FuZEJhZ2dlci5jaXNjby5jb20wgZ8wDQYJKoZIhvcNAQEBBQADgY0A
MIGJAoGBAMButEKI6Q282yp8o/Bck4jnL0x5Az+1w+Ly09V2ieNPc9IEiKBpyHHR
bV4VZQVraat/zvc2BV69bR/gTAkUIty7bNCKcWGtw/YhT6nr+0j16bACLGPGuhTK
u04sCzm6okIyyi+HG7ldBa45dGLr+QP2fpKjDpu3PqVjVhXS3vZbAgMBAAGjggHM
MIIByDALBgNVHQ8EBAMCBSAwHQYDVR0OBBYEFPDO29oRdlEUSgBMg6jZR+YFRWlj
MHAGA1UdIwRpMGeAFKIacsl6dKAfuNDVQymlSp7esf8joT2kOzA5MQswCQYDVQQG
EwJVUzEWMBQGA1UEChMNQ2lzY28gU3lzdGVtczESMBAGA1UEAxMJbXNjYS1yb290
ghA6wKZelUfCh0qvJGipQtXuMCIGA1UdEQEB/wQYMBaCFFNhbmRCYWdnZXIuY2lz
Y28uY29tMG0GA1UdHwRmMGQwL6AtoCuGKWh0dHA6Ly9tc2NhLXJvb3QvQ2VydEVu
cm9sbC9tc2NhLXJvb3QuY3JsMDGgL6AthitmaWxlOi8vXFxtc2NhLXJvb3RcQ2Vy
dEVucm9sbFxtc2NhLXJvb3QuY3JsMIGUBggrBgEFBQcBAQSBhzCBhDA/BggrBgEF
BQcwAoYzaHR0cDovL21zY2Etcm9vdC9DZXJ0RW5yb2xsL21zY2Etcm9vdF9tc2Nh
LXJvb3QuY3J0MEEGCCsGAQUFBzAChjVmaWxlOi8vXFxtc2NhLXJvb3RcQ2VydEVu
```

```
cm9sbFxtc2NhLXJvb3RfbXNjYS1yb290LmNydDANBgkqhkiG9w0BAQUFAANBAHaU
hyCwLirUghNxCmLzXRG7C3W1j0kSX7a4fX9OxKR/Z2SoMjdMNPPyApuh8SoT2zBP
ZKjZU2WjcZG/nZF4W5k=
% Router Certificate successfully imported
```

証明書が正常にインポートされたかどうかを確認するには、**show crypto pki certificates** コマンドを発行します。

```
Router# show crypto pki certificates
Certificate
  Status: Available
  Certificate Serial Number: 14DECE05000000000C48
  Certificate Usage: Encryption
  Issuer:
    CN = TPCA-root
     O = Company
     C = US
  Subject:
    Name: Router.example.com
    OID.1.2.840.113549.1.9.2 = Router.example.com
  CRL Distribution Point:
    http://tpca-root/CertEnroll/tpca-root.crl
  Validity Date:
    start date: 18:16:45 PDT Jun 7 2002
    end   date: 18:26:45 PDT Jun 7 2003
    renew date: 16:00:00 PST Dec 31 1969
  Associated Trustpoints: TP
Certificate
  Status: Available
  Certificate Serial Number: 14DEC2E9000000000C47
  Certificate Usage: Signature
  Issuer:
    CN = tpca-root
     O = company
     C = US
  Subject:
    Name: Router.example.com
    OID.1.2.840.113549.1.9.2 = Router.example.com
  CRL Distribution Point:
    http://tpca-root/CertEnroll/tpca-root.crl
  Validity Date:
    start date: 18:16:42 PDT Jun 7 2002
    end   date: 18:26:42 PDT Jun 7 2003
    renew date: 16:00:00 PST Dec 31 1969
  Associated Trustpoints: TP
CA Certificate
  Status: Available
  Certificate Serial Number: 3AC0A65E9547C2874AAF2468A942D5EE
  Certificate Usage: Signature
  Issuer:
    CN = tpca-root
     O = Company
     C = US
  Subject:
    CN = tpca-root
     O = company
     C = US
  CRL Distribution Point:
    http://tpca-root/CertEnroll/tpca-root.crl
  Validity Date:
    start date: 16:46:01 PST Feb 13 2002
    end   date: 16:54:48 PST Feb 13 2007
  Associated Trustpoints: TP
```

キー再生を使用した手動での証明書登録の設定例

次の例では、「trustme2」という名前の CA から手動で証明書を登録して、新しいキーを再生する方法を示します。

```
crypto pki trustpoint trustme2
 enrollment url http://trustme2.example.com/
 subject-name OU=Spiral Dept., O=example.com
 ip-address ethernet0
 serial-number none
 regenerate
 password password1
 rsakeypair trustme2 2048
 exit
crypto pki authenticate trustme2
crypto pki enroll trustme2
```

永続的自己署名の証明書の作成および検証例

次の例では、「local」という名前のトラストポイントを宣言して登録し、IPアドレスを含む自己署名証明書を生成する方法を示します。

```
crypto pki trustpoint local
 enrollment selfsigned
 end
configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
crypto pki enroll local
Nov 29 20:51:13.067: %SSH-5-ENABLED: SSH 1.99 has been enabled
Nov 29 20:51:13.267: %CRYPTO-6-AUTOGEN: Generated new 512 bit key pair
% Include the router serial number in the subject name? [yes/no]: yes
% Include an IP address in the subject name? [no]: yes
Enter Interface name or IP Address[]: ethernet 0
Generate Self Signed Router Certificate? [yes/no]: yes
Router Self Signed Certificate successfully created
```

（注） ルータに設定できる自己署名証明書は 1 つだけです。自己署名証明書がすでに存在する場合に、別の自己署名証明書用に設定されたトラストポイントを登録しようとすると、通知が表示され、自己署名証明書を置き換えるかどうか尋ねられます。置き換える場合は、新しい自己署名証明書が生成され、既存の自己署名証明書と置き換えられます。

HTTPS サーバのイネーブル化の例

次の例では、以前に HTTPS サーバが設定されていなかったため、HTTPS サーバをイネーブルにし、デフォルト トラストポイントを生成する方法を示します。

```
configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
ip http secure-server
% Generating 1024 bit RSA keys ...[OK]
*Dec 21 19:14:15.421:%PKI-4-NOAUTOSAVE:Configuration was modified.  Issue "write memory"
```

```
 to save new certificate
Router(config)#
```

（注） 自己署名証明書を保持し、次にルータをリロードしたときに HTTPS サーバをイネーブルにする場合は、コンフィギュレーションを NVRAM に保存する必要があります。

次のメッセージも表示されます。

```
*Dec 21 19:14:10.441:%SSH-5-ENABLED:SSH 1.99 has been enabled
```

（注） 自己署名証明書で使用されたキー ペアを作成すると、Secure Shell（SSH）サーバが起動します。この動作は抑制できません。ご使用のアクセスコントロールリスト（ACL）を変更して、ルータへの SSH アクセスを許可または拒否できます。**ip ssh rsa keypair-name** *unexisting-key-pair-name* コマンドを使用し、SSH サーバーをディセーブルにできます。

自己署名証明書設定の検証例

次の例では、作成した自己署名証明書に関する情報を表示します。

```
Router# show crypto pki certificates
Router Self-Signed Certificate
  Status: Available
  Certificate Serial Number: 01
  Certificate Usage: General Purpose
  Issuer:
    cn=IOS-Self-Signed-Certificate-3326000105
  Subject:
    Name: IOS-Self-Signed-Certificate-3326000105
    cn=IOS-Self-Signed-Certificate-3326000105
  Validity Date:
    start date: 19:14:14 GMT Dec 21 2004
    end   date: 00:00:00 GMT Jan 1 2020
  Associated Trustpoints: TP-self-signed-3326000105
```

（注） 上記の 3326000105 という数値はルータのシリアル番号で、これはルータの実際のシリアル番号によって異なります。

次の例では、自己署名証明書に対応するキー ペアに関する情報を表示します。

```
Router# show crypto key mypubkey rsa
% Key pair was generated at: 19:14:10 GMT Dec 21 2004
Key name: TP-self-signed-3326000105
 Usage: General Purpose Key
 Key is not exportable.
 Key Data:
  30819F30 0D06092A 864886F7 0D010101 05000381 8D003081 89028181 00B88F70
  6BC78B6D 67D6CFF3 135C1D91 8F360292 CA44A032 5AC1A8FD 095E4865 F8C95A2B
  BFD1C2B7 E64A3804 9BBD7326 207BD456 19BAB78B D075E78E 00D2560C B09289AE
```

```
  6DECB8B0 6672FB3A 5CDAEE92 9D4C4F71 F3BCB269 214F6293 4BA8FABF 9486BCFC
  2B941BCA 550999A7 2EFE12A5 6B7B669A 2D88AB77 39B38E0E AA23CB8C B7020301 0001
% Key pair was generated at: 19:14:13 GMT Dec 21 2004
Key name: TP-self-signed-3326000105.server
 Usage: Encryption Key
 Key is not exportable.
 Key Data:
  307C300D 06092A86 4886F70D 01010105 00036B00 30680261 00C5680E 89777B42
  463E5783 FE96EA9E F446DC7B 70499AF3 EA266651 56EE29F4 5B003D93 2FC9F81D
  8A46E12F 3FBAC2F3 046ED9DD C5F27C20 1BBA6B9B 08F16E45 C34D6337 F863D605
  34E30F0E B4921BC5 DAC9EBBA 50C54AA0 BF551BDD 88453F50 61020301 0001
```

（注） TP-self-signed-3326000105.server という 2 番目のキー ペアは、SSH キー ペアです。ルータに任意のキー ペアが作成されて SSH が起動すると、生成されます。

次の例では、「local」というトラストポイントに関する情報を表示します。

```
Router# show crypto pki trustpoints
Trustpoint local:
    Subject Name:
    serialNumber=C63EBBE9+ipaddress=10.3.0.18+hostname=test.example.com
          Serial Number: 01
    Persistent self-signed certificate trust point
```

HTTP による直接登録の設定例

次の例では、HTTP による CA サーバへの直接登録ための登録プロファイルを設定する方法を示します。

```
crypto pki trustpoint Entrust
 enrollment profile E
 serial
crypto pki profile enrollment E
 authentication url http://entrust:81
 authentication command GET /certs/cacert.der
 enrollment url http://entrust:81/cda-cgi/clientcgi.exe
 enrollment command POST reference_number=$P2&authcode=$P1
 &retrievedAs=rawDER&action=getServerCert&pkcs10Request=$REQ
 parameter 1 value aaaa-bbbb-cccc
 parameter 2 value 5001
```

2 階層 PKI 環境での証明書登録の設定例

端末経由で ROOT-CA をインポートする例。

```
(config)#crypto pki trustpoint ROOT-CA
(ca-trustpoint)#revocation-check none
(ca-trustpoint)#enrollment terminal


(config)#crypto pki authenticate ROOT-CA

Enter the base 64 encoded CA certificate.
End with a blank line or the word "quit" on a line by itself
```

```
-----BEGIN CERTIFICATE-----
MIIDdTCCAl2gAwIBAgIQIfTArEE1yKZPXHaAVgDk5jANBgkqhkiG9w0BAQsFADBN
MRMwEQYKCZImiZPyLGQBGRYDY29tMRgwFgYKCZImiZPyLGQBGRYIdnBuLWVhc3Qx
HDAaBgNVBAMTE3Zwbi1lYXN0LXphY2ttY2ktQ0EwHhcNMTgxMjIwMDAwNjMyWhcN
MjgxMjIwMDAxNjMyWjBNMRMwEQYKCZImiZPyLGQBGRYDY29tMRgwFgYKCZImiZPy
LGQBGRYIdnBuLWVhc3QxHDAaBgNVBAMTE3Zwbi1lYXN0LXphY2ttY2ktQ0EwggEi
MA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQC9Gdns9lU2HHc+XYhrmZKg6+Xo
5kNflu6mMgCfZ7ZiAKxZ03whJWZqNC7JRZQ+LkIJAcBUSf2mSJWRp+HVgI6k4Zf7
bMgIBq629HT8XmFLrr3lfh1lfL7WqI1Uez7/PEzjsw09y/m/WiSnrlgR3+PvyDbH
E86A6JnmtTNIs4qawUe72BlnEzwwRaFNi7VQz7GQw3CUo+RX9wtFYjABTyTUM/BA
MP47pI8CVh1jHVHqHcbqpyd97j1/8n1d/NCmcHKIg2hnKEO1Hx8oK7QIHe1rkryl
+r0ol2fS3CGgY000+FINs3qw4h8H8xfmsc5cs8lJCIbZGJhMTXq6u4Ecp+N1AgMB
AAGjUTBPMAsGA1UdDwQEAwIBhjAPBgNVHRMBAf8EBTADAQH/MB0GA1UdDgQWBBTb
zvfa7aNZspz3GwJCvKDIKO8KFTAQBgkrBgEEAYI3FQEEAwIBADANBgkqhkiG9w0B
AQsFAAOCAQEAgTIPTauHsPp7h1v/iFXkbVV1aG7O8/IaJG0sCr0f9/nsfM9HO0Jm
LP+twy5KkFa7I6u4vMlMlfNyujS60Fqnw3m8UJCy2SkYVwlGrBddN+BQbnkZ460M
sYfaynFBsvsbmmaLEqUQ3t9cmNCskXoda+FffyFTwAUBFzV66BGKpn6Y7oyIghF5
NLjjgWPVmRy7RKM4IKe9J0+oEmnugwtdfHgiFdX+d6qPovjbApj2j6N4+Cv6qHDO
/c+wUXRxz08eFNOqHNJipk70OXMrUh4UaWMnM/CYA9E1sjjSAWhBl4ii/+fiaILw
xgof+2mmIzafzFZz+eVf5kgwpV07GlZlng==
-----END CERTIFICATE-----
quit
Certificate has the following attributes:
       Fingerprint MD5: 99182E1E 96FB0595 DF86BFCE 3C781CF5
      Fingerprint SHA1: 6E55B878 9AA3B603 D689AC25 F027615E 0C88E6E4

% Do you accept this certificate? [yes/no]: yes

Authenticating SUB-CA without having to specify or accept the fingerprint.

(config)#crypto pki trustpoint SUB-CA
(ca-trustpoint)#enrollment url  http://<SUBCA_IP/FQDN>:80/certsrv/mscep/mscep.dll
(ca-trustpoint)#chain-validation continue ROOT-CA
(ca-trustpoint)#revocation-check none

(ca-trustpoint)#crypto pki authenticate SUB-CA
Certificate has the following attributes:
       Fingerprint MD5: 5C38CB0A 050AAE87 84A08A75 5F7084B8
      Fingerprint SHA1: EB829470 B8B9E26E 4457F346 7A3E957C C623C6F9
Certificate validated - Signed by existing trustpoint CA certificate.

Trustpoint CA certificate accepted.
```

その他の参考資料

関連資料

関連項目	マニュアル タイトル
USB トークンによる RSA 処理：USB トークンを使用するメリット	『Cisco IOS Security Configuration Guide: Secure Connectivity』の「Storing PKI Credentials」モジュール

関連項目	マニュアル タイトル
USB トークンによる RSA 処理：証明書サーバの設定	『Cisco IOS Security Configuration Guide: Secure Connectivity』の「Configuring and Managing a Cisco IOS Certificate Server for PKI Deployment」項 「Generating a Certificate Server RSA Key Pair」項、「Configuring a Certificate Server Trustpoint」項、および関連する例を参照してください。
PKI の概要（RSA キー、証明書登録、および CA を含む）	『Cisco IOS Security Configuration Guide: Secure Connectivity』の 「 Cisco IOS PKI Overview: Understanding and Planning a PKI 」 モジュール
安全なデバイス プロビジョニング：機能概要および設定作業	『Cisco IOS Security Configuration Guide: Secure Connectivity』の「Setting Up Secure Device Provisioning (SDP) for Enrollment in a PKI」項
RSA キーの生成および展開	『Cisco IOS Security Configuration Guide: Secure Connectivity』の「Deploying RSA Keys Within a PKI」モジュール
Cisco IOS 証明書サーバの概要および設定作業	『Cisco IOS Security Configuration Guide: Secure Connectivity』の「Configuring and Managing a Cisco IOS Certificate Server for PKI Deployment」モジュール
USB トークンの設定および使用	『Cisco IOS Security Configuration Guide: Secure Connectivity』の「Storing PKI Credentials」モジュール
Cisco IOS セキュリティ コマンド	『*Cisco IOS Security Command Reference*』
Suite-B の ESP トランスフォーム	『Configuring Security for VPNs with IPsec』フィーチャ モジュール
Suite-B SHA-2 ファミリ（HMAC バリアント）および Elliptic Curve（EC）キーペアの設定。	『Configuring Internet Key Exchange for IPsec VPNs』フィーチャ モジュール
Suite-B 整合性アルゴリズム タイプのトランスフォームの設定	『Configuring Internet Key Exchange Version 2 (IKEv2)』フィーチャ モジュール
IKEv2 用の Suite-B の Elliptic Curve Digital Signature Algorithm（ECDSA）signature（ECDSA-sig）認証方式の設定	『Configuring Internet Key Exchange Version 2 (IKEv2)』フィーチャ モジュール
IPsec SA ネゴシエーションでの Suite-B の Elliptic Curve Diffie-Hellman（ECDH）のサポート	『Configuring Internet Key Exchange for IPsec VPNs』および『Configuring Internet Key Exchange Version 2 (IKEv2)』フィーチャ モジュール

関連項目	マニュアル タイトル
推奨される暗号化アルゴリズム	『*Next Generation Encryption*』

MIB

MIB	MIB のリンク
なし。	選択したプラットフォーム、Cisco IOS リリース、およびフィーチャ セットに関する MIB を探してダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

シスコのテクニカル サポート

説明	リンク
右の URL にアクセスして、シスコのテクニカル サポートを最大限に活用してください。これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

Cisco TrustSec の概要の機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *149 : Cisco TrustSec* の概要の機能情報

機能名	リリース	機能情報
IPv6 の有効化 - インライン タギング	Cisco IOS XE Fuji 16.8.1	IPv6 のサポートが導入されました。

第 112 章

PKI への登録のための Secure Device Provisioning の設定

この章では、公開キーインフラストラクチャ（PKI）で Secure Device Provisioning（SDP）を使用する方法を説明します。SDP は、Cisco IOS クライアントと Cisco IOS 証明書サーバなど、2 つのエンド デバイス間で PKI を簡単に配置できる、Web ベースの証明書登録インターフェイスです。エンドデバイスは、配置やプロビジョニングの時点ではネットワークに直接接続されていたり、されていない場合があります。SDP は、多数のピア デバイスを導入するユーザに（証明書および設定を含む）ソリューションを提供します。

（注） セキュリティに対する脅威は、脅威からの保護に役立つ暗号化技術と同様に絶え間なく変化しています。最新のシスコの暗号化に関する推奨事項については、『Next Generation Encryption』（NGE）ホワイト ペーパーを参照してください。

PKI への登録のための Secure Device Provisioning（SDP）の設定の前提条件

PKI への登録のための SDP の設定

SDP を設定する前に、次の要件を満たす必要があります。

- ペティショナのデバイスとサーバは、互いに IP 接続されている必要があります。
- イントロデューサには、JavaScript をサポートする Web ブラウザが必要です。
- イントロデューサは、クライアントデバイスで特権をイネーブルにしておく必要があります。
- Cisco IOS リリース 12.3(8)T PKI 対応イメージまたは以降のイメージ。

USB トークンを使用した PKI への登録のための SDP の設定

USB トークンを活用してデバイスを SDP にプロビジョニングするには、ご使用の環境が次の要件を満たしている必要があります。

- ペティショナのデバイスとサーバの両方とも、互いにIP接続されている必要があります。
- イントロデューサには、JavaScript をサポートする Web ブラウザが必要です。
- イントロデューサは、クライアントデバイスで特権をイネーブルにしておく必要があります。
- イントロデューサは、ペティショナのデバイスにアクセスできなければなりません。
- イントロデューサは、設定されている場合は、USB トークンと PIN にアクセスできなければなりません。
- Cisco IOS リリース 12.4(15)T PKI 対応イメージまたは以降のイメージ。

（注） Cisco IOS リリース 12.4(15)T 以降のリリースは、USB トークンに保管されたログイン情報を移動できる柔軟性を備えています。ただし、USB トークンの設定に使用したデバイスは 任意の Cisco IOS リリース 12.3(14)T PKI 対応イメージまたは以降のイメージを実行できます。

サービス プロバイダー経由のインターネット接続に対する SDP を使用したデバイスの設定

SDP を活用してインターネットに接続されていないデバイスを設定するには、ご使用の環境が次の要件を満たしている必要があります。

- イントロデューサには、JavaScript をサポートする Web ブラウザが必要です。
- イントロデューサは、クライアントデバイスで特権をイネーブルにしておく必要があります。
- DHCP クライアントおよびPPPoE クライアントをサポートし、LAN または WAN インターフェイスが設定されている Cisco ルータ。
- Cisco IOS リリース 12.4(20)T PKI 対応イメージまたは以降のイメージ。前回の Cisco IOS リリースがいずれかのデバイスで使用されている場合、SDP 機能はデフォルトで以前の Cisco IOS バージョンになります。

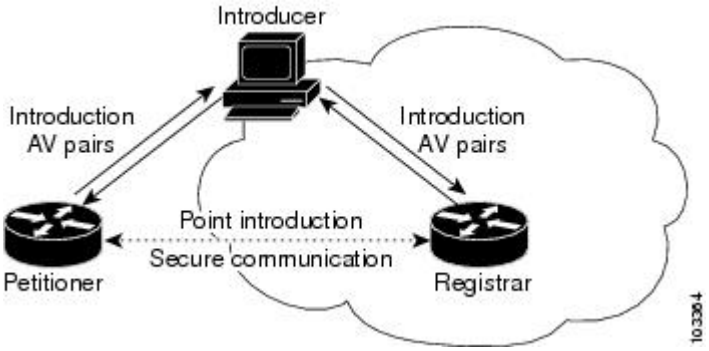
PKI への登録のための Secure Device Provisioning（SDP）の設定に関する情報

SDP の概要

SDP（「Trusted Transitive Introduction（TTI）」とも呼ばれている）は、新しいネットワークデバイスと仮想プライベートネットワーク（VPN）の間といった2つのエンドエンティティ間の双方向導入を実現する通信プロトコルです。SDP には次の3つのエンティティが必要です（次の図を参照）。

- イントロデューサ：ペティショナをレジストラに紹介する、相互に信頼できるデバイス。イントロデューサは、システム管理者などのデバイス ユーザの場合があります。
  - イントロデューサは、管理イントロデューサとして設定できます。これにより紹介を行っている管理者は、紹介中のデバイスの名前を提供できます。提供されたデバイス名は、通常の SDP メカニズムにおいてイントロデューサの名前のように使用され、SDP 設定の既存機能を保持します。管理イントロデューサの機能の詳細については、「管理イントロデューサの認証リストと認可リスト（1415 ページ）」を参照してください。
- ペティショナ：セキュアネットワークに紹介されるクライアント、あるいは新しいデバイス。
- レジストラ：ペティショナを認証するサーバー。レジストラは、証明書サーバの場合があります。

図 *37*：紹介後のセキュア通信



Cisco IOS リリース 12.4(20)T 以降のリリースの時点では、ペティショナにあらかじめインターネット接続を確立しなくても、SDP プロセスを起動できます。予備接続段階と接続段階を利用することで、サービスプロバイダー経由のインターネット接続に対してペティショナを設定できます。予備接続段階と接続段階の詳細については、SDP の機能（1404 ページ）を参照してください。

レジストラは、外部認証、許可、アカウンティング（AAA）サーバと直接通信し、ペティショナのクレデンシャルを確認し、登録を許可または拒否して、特定のペティショナ設定情報を取得します。ペティショナとレジストラは、エンドユーザであるイントロデューサへ Web ページを配信します。ペティショナは、イントロデューサの Web ブラウザを使用してリモート管理システムからブートストラップ設定を受信します。

SDP は、予備接続（任意）、接続、開始（任意）、ようこそ、紹介、および完了の可能な 6 つの段階により Web ブラウザ上に実装されます。各段階は、Web ページを通してユーザに表示されます。各段階の詳細については、SDP の機能 （1404 ページ）を参照してください。

SDP の機能

ここでは、SDP が 2 つのデバイス間で PKI を展開する方法について説明します。

- SDP 予備接続段階 （1404 ページ）
- SDP 接続段階 （1406 ページ）
- SDP スタティック段階 （1408 ページ）
- SDP ようこそ段階 （1409 ページ）
- SDP 紹介段階 （1409 ページ）
- SDP 完了段階 （1410 ページ）

SDP プロセスは、イントロデューサにより Web ブラウザにロードされている 3 つの入口ページのいずれかで起動します。3 つの入口ページは、管理者から受信した SDP 予備接続段階、レジストラからロードされた開始段階、ペティショナからロードされたようこそ段階です。

サンプル図では、ローカル デバイス（ペティショナ）をレジストラのセキュア ドメインに紹介する方法を示しています。「イントロデューサ」は、エンドユーザーとも呼ばれます。

SDP 予備接続段階

予備接続ページはオプションです。予備接続ページがない場合、ペティショナは IP 接続を確立しておく必要があります。

管理者は予備接続テンプレートを設定し、予備接続ページをイントロデューサに送信する必要があります。詳細については、デフォルトの予備接続テンプレート （1421 ページ）を参照してください。

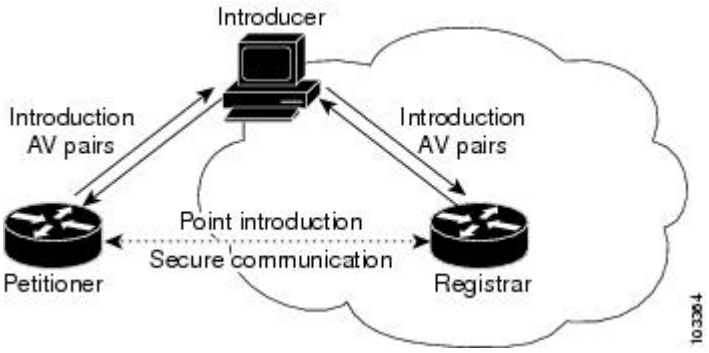
また管理者は、電話、E メール、セキュア E メール、CD、または USB トークンでセキュア ネットワークのユーザ名とパスワードを取得し、イントロデューサに連絡する必要があります。レジストラは、既存の AAA インフラストラクチャ（たとえば、既存の企業ドメインの一部である既存のユーザ名とパスワードのデータベース）を使用してイントロデューサを認証するよう設定できます。SDP 予備接続段階では、一般的な AAA インフラストラクチャで使用されているようなチャレンジパスワードメカニズムがサポートされています。詳細については、SDP による外部 AAA データベースの使用方法 （1414 ページ）を参照してください。

予備接続ページを受信後、イントロデューサはそのページを HTTP ブラウザが動作するコンピュータにロードする必要があります。イントロデューサが予備接続ページをローカルファイルとしてHTTPブラウザにロードすると、予備接続ページが表示されます（次の図を参照）。

図 *38 : SDP* 予備接続ページのサンプル

イントロデューサが [Ciscoデバイスにログオン（Log onto Cisco Device）] ボタンをクリックすると、ログインダイアログボックスが表示されます（次の図を参照）。イントロデューサは、シスコデバイスの出荷時デフォルトのユーザ名（cisco）とパスワード（cisco）を入力します。

図 *39 :* ペティショナ ログイン ダイアログボックスのサンプル



イントロデューサはペティショナを認証し、既知の URL にアクセスすることでインターネット接続をテストします。www.cisco.com（198.133.219.25）へのアクセスがデフォルトでテストされます。管理者は、デフォルト予備接続テンプレートを変更することで、URL をテスト接続用に変更できます。デフォルトテスト URL および管理者が予備接続ページに対して設定できるその他フィールドの詳細については、デフォルトの予備接続テンプレート （1421 ページ）の項を参照してください。

（注） 予備接続ページに信頼できないレジストラの IP アドレスが含まれるよう変更されたり、予備接続ページが信頼できない発信元から E メール送信される可能性を減らすため、セキュア E メールなどのセキュアな方法を使用して予備接続ページを送信してください。

インターネット接続が確立されると、管理者により定義された予備接続テンプレート設定によって、開始ページまたはようこそページのいずれかが表示されます。インターネット接続が確立されていない場合は、接続ページが表示されます。

SDP 接続段階

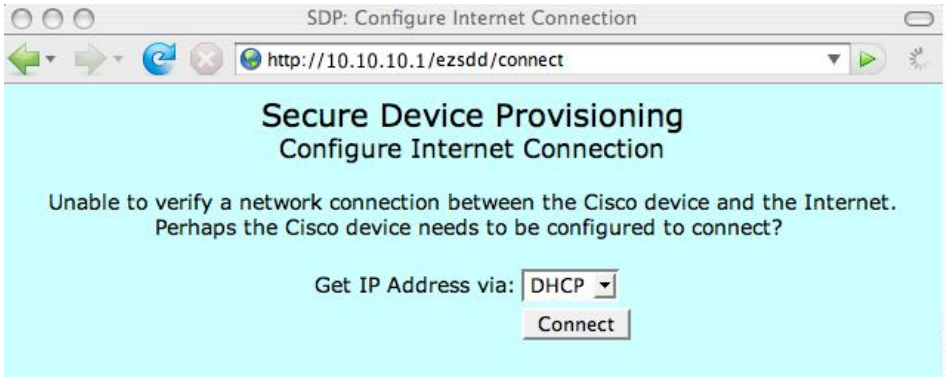
接続ページは、予備接続ページが使用され、予備接続ページの完了時にペティショナの IP 接続がない場合だけ表示されます。接続ページには、Cisco IOS プラットフォームに柔軟性をもたらすため Dynamic Host Configuration Protocol（DHCP）、Point to Point Protocol over Ethernet（PPPoE）、またはスタティック IP アドレス割り当ての 3 つの IP アドレス割り当て方法があります。

（注） インターネット接続を確立する場合、Cisco IOS 設定では SDP 機能は使用されません。SDP 機能には Cisco IOS 設定にシグニチャがあり、送信中の値が変更されないようにします。

DHCP IP アドレス割り当て方法

イントロデューサが IP アドレス割り当て方法オプションとしてデフォルト方法である DHCP を選択すると（次の図を参照）、[接続（Connect）]ボタンをクリックするとペティショナのインターネット接続が設定されます。

図 *40 : DHCP IP* アドレス割り当て方法のサンプル接続ページ



PPPoE IP アドレス割り当て方法

イントロデューサが PPPoE を選択すると、PPPoE ユーザー名およびパスワードの入力フィールドが表示されます（次の図を参照）。イントロデューサは、インターネット サービス プロバイダー（ISP）により提供されたユーザ名とパスワードを入力し、[Connect] ボタンをクリックする必要があります。これによりペティショナのインターネット接続が設定されます。

図 *41* : *PPPoE IP* アドレス割り当て方法のサンプル接続ページ

スタティック IP アドレス割り当て方法

イントロデューサがスタティックを選択すると、IP アドレス、ネットマスク、およびデフォルトゲートウェイの入力フィールドが表示されます（次の図を参照）。イントロデューサは、ISP により提供された設定値を入力し、[Connect] ボタンをクリックする必要があります。これによりペティショナのインターネット接続が設定されます。

図 *42* : スタティック *IP* アドレス割り当て方法の接続ページ

接続ページ IP アドレス設定

IP アドレス設定後、予備接続テンプレートで管理者により設定された既知の URL（デフォルトで www.cisco.com）にアクセスすることで、インターネット接続を再度テストします。これでインターネット接続が確立されると、管理者により定義された予備接続テンプレート設定によって、開始ページまたはようこそページのいずれかが表示されます。インターネット接続が確立されない場合、イントロデューサは入力された設定を確認するか、管理者に連絡します。

SDP スタティック段階

開始ページはオプションです。SDP 交換中に開始ページがない場合、ようこそページで [次へ（Next）]ボタンをクリックすると、ユーザーはレジストラの紹介ページに送信されます。ユーザはまだレジストラに接続していないので、使用可能な資格情報を使用して（レジストラを設定するたびに）レジストラにログインする必要があります。ユーザがログインデータを入力した後では、レジストラに再接続できないブラウザもあります。Cisco IOS Release 12.4(4)T の時点では、ユーザーは、開始ページからレジストラの紹介 URL に連絡することで SDP 交換を開始するようブラウザを設定できます。その後、レジストラはペティショナデバイスにあるようこそページにユーザを送信できます。SDP トランザクションは、このマニュアルに記載されているように、ようこそ段階から紹介段階を経て、完了段階へと続きます。

レジストラから SDP トランザクションを開始するには、**template http start** コマンドを使用してブラウザを設定する必要があります。それ以外の場合、SDP トランザクションはペティショナのようこそページから始まる必要があります。カスタムテンプレートの SDP での動作 （1416 ページ）を参照してください。

ようこそページが表示される前に、ユーザは自分のブラウザの開始ページが URL http://registrar/ezsdd/intro を指すように設定する必要があります。ログインダイアログボックスが表示されると、エンドユーザーは、管理者により提供されたユーザー名とパスワードを使用してレジストラにログインし、セキュアネットワークにアクセスできます（次の図を参照）。

図 *43* : レジストラ リモート ログイン ダイアログボックス

有効なユーザー名とパスワードを入力すると、開始ページが表示されます（次の図を参照）。

図 *44* : サンプル *SDP* 開始ページ

ユーザは URL http://10.10.10.1/ezsdd/welcome からペティショナにログインする必要があります。ようこそ段階は、開始ページでユーザが [Next] ボタンをクリックすると開始されます。

SDP ようこそ段階

ローカル ログイン ダイアログボックスが表示されたら（次の図を参照）、エンドユーザーは出荷時デフォルトのユーザー名（cisco）とパスワード（cisco）を使用してローカルデバイスにログインできます。ようこそページが表示されます。

図 *45*：ペティショナ ローカル ログイン ダイアログボックス

パスワードの入力に成功すると、ペティショナにより処理されるようこそ Web ページが表示されます（次の図を参照）。

図 *46*：サンプル *SDP* ようこそページ

ようこそ Web ページでレジストラの URL（例：http://192.0.2.155/ezsdd/intro）を入力し、[Next] ボタンをクリックすると、SDP紹介段階が始まり、レジストラにより処理される紹介ページが表示されます。

SDP 紹介段階

紹介ページを表示する前に、開始ページからまだログインしていない場合、エンドユーザーはレジストラにログインする必要があります（SDP スタティック段階（1408 ページ）を参照）。ここで外部 AAA データベースを利用します。

外部 AAA データベースがある場合、レジストラのイネーブル パスワードを知らなくても、イントロデューサはデータベースのアカウントを使用して紹介を行うことができます。外部AAA データベースがない場合、イントロデューサは認証のためレジストラのイネーブルパスワードを使用できます。

（注） レジストラのイネーブル パスワードを使用すると、パスワードがエンド ユーザに公開されます。したがって、イネーブル パスワードは管理テストの目的でだけ使用することを推奨します。

管理イントロデューサは、紹介ページ（または開始ページ）の HTTP 認証で識別され、AAA データベース クエリーによりユーザの管理特権が戻されます。イントロデューサに管理特権がある場合、デバイス名は管理紹介ページに入力された名前になります。イントロデューサに管理特権がない場合、デバイス名はイントロデューサ名になります。既存のデバイス証明書はペティショナの現在の証明書で、製造識別証明書（MIC）の場合があります。この証明書は存在する場合も、しない場合もあります。外部 AAA データベースの機能の詳細については、SDP による外部 AAA データベースの使用方法 （1414 ページ） を参照してください。

エンドユーザーがパスワードの入力に成功したら、紹介 Web ページが表示されます（次の図を参照）。

図 *47 : サンプル SDP* 紹介ページ

この時点で、レジストラはデバイス情報を外部管理システムに渡し、ブートストラップ設定ファイルを取得します。カスタマイズされたブートストラップ設定ファイルを識別するのに利用可能なオプションの詳細については、カスタム HTML テンプレートの展開ルール （1417 ページ）を参照してください。

紹介ページで [Next] ボタンをクリックすると、エンド ユーザは完了段階に入り、自動的に自分のデバイスに戻ります。

SDP 完了段階

エンドユーザーがペティショナをレジストラに登録したので、ペティショナは完了ページを処理します（次の図を参照）。

図 *48* : サンプル *SDP* 完了ページ

これで SDP 交換が完了しました。ペティショナはレジストラから設定情報を受信したため、まもなくレジストラから証明書を受信するはずです。

USB トークンを活用している SDP

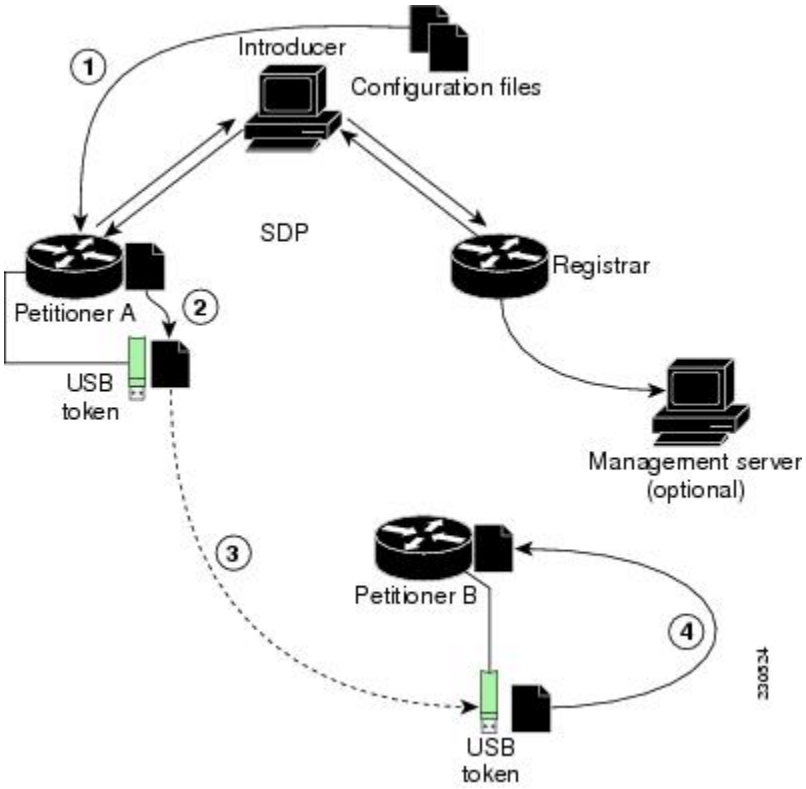
SDP により極めてスケーラブルな配置が実現され、個々のデバイスまたは複数デバイスの配置が簡略化されます。USB トークンによりセキュアな保管と設定の配信が行われます。

Cisco IOS リリース 12.4(15)T 以降の時点では、USB トークンは SDP を使用して PKI ログイン情報を転送する場合に利用でき、SDP は USB トークンの設定に使用できます。USB トークンを使用して、同じ位置にあるデバイスをプロビジョニングしたり、リモートデバイスのプロビジョニングとして使用できる別の場所に USB トークンを転送できます。

USB トークンを使用して PKI ログイン情報を転送する SDP 展開の例を次の図に示します。必要なデバイスとして、USB トークンとデバイスのプロビジョニングに必要な SDP エンティティがあります。これらの SDP エンティティは、イントロデューサ、レジストラ、ローカル位置のペティショナであるペティショナ A、リモート位置でのペティショナであるペティショナ B になります。オプションとして、管理サーバーが使用できます。

（注） オプション設定は、1 台のデバイスをレジストラおよびペティショナ両方として設定することです。これは、USB トークンがリモート位置に転送される場合に利点があります。リモート位置では、個別のペティショナ デバイスは必要ありません。

図 *49 : USB* トークンを使用したクレデンシャル転送の *SDP* 環境例



SDP を使用した USB トークンの設定

SDP 導入の開始前に、USB トークンがペティショナ デバイスに挿入されます。図の設定例では、USB トークンはペティショナ A に挿入されます。ペティショナは、USB トークンにある既存の情報を無視するように設定できます。通常の SDP 操作の場合のように、USB トークンのスケーラブル設定では、テンプレートの初期設定を作成し、適切なターゲット設定情報を備えた各 SDP デバイスに配置する必要があります。

デバイスのプロビジョニングに使用するファイルは、次の順番で移動します。

1. ペティショナの 1 つ、ペティショナ A はローカル位置にあります。ペティショナ A は SDP 交換に直接関わり、USB トークンの初期設定を行います。USB トークン、バイナリ ファイル、テンプレート ファイルの設定に使用するファイルは、レジストラから取得され、ペティショナ A に移動します。

バイナリ ファイル位置の URL は、レジストラで展開されます。バイナリ ファイルは、テンプレート展開機能では処理されません。テンプレート展開はレジストラで、発信元 URL と宛先 URL の両方に対して行われます。

デフォルトでは、バイナリ ファイルとテンプレート ファイルは NVRAM から取得され、それぞれレジストラとペティショナに保管されます。レジストラのバイナリファイル位置とペティショナ A の宛先バイナリファイル位置は、**binary file** コマンドで指定できます。レジストラの

テンプレートファイル位置とペティショナ A の宛先テンプレートファイル位置は、**template file** コマンドで指定できます。

1. Rivest、Shamir、Adelman（RSA）キーおよび証明書チェーン情報は、ペティショナ A から USB トークンに移動します。
2. USB トークンはリモート位置に転送され、ペティショナ B に挿入されます。
3. USB トークンの設定ファイルは、ローカルデバイスのプロビジョニングに使用されます。USB トークンのファイルは、**crypto key move rsa** コマンドでペティショナ B の保管位置に移動できます。

SDP 段階と USB トークン

「SDP の概要」で紹介された同じ SDP フェーズ概念が使用されます。SDP ようこそ段階、SDP 紹介段階、および SDP 完了段階には次のような違いがあります。

SDP ようこそページと USB トークン

ようこそユーザ インターフェイスに接続して紹介が開始される場合、SDP ようこそ段階は通常どおり開始します。USB トークンに既存の証明書がある場合、SDP 交換に署名する場合に使用されます。ローカルな RSA キー ペアではなく、トークンの新しい RSA キー ペアが使用されます。

（注） RSA キー ペアは、キーがトークンで生成される場合、どの場所からでも実質的に 5 分～10 分掛かります。時間の長さは、USB トークンで使用できるハードウェア キー生成により異なります。イントロデューサには、RSA キー ペアが生成されていることを示す情報 Web ページが表示されます。

ペティショナ A で生成された新しいキー ペアは、既存の RSA キー ペアを削除しなくても、USB トークンに追加されます。SDP AV ペアは、トークンが使用中であり、またトークンのセカンダリ設定情報があるかどうか両方を示します。オプションの管理サーバが使用中の場合、AV ペア情報を使用して、特殊なコンフィギュレーション コマンドが必要かどうかを判断します。

SDP 紹介段階と USB トークン

SDP 紹介段階は、レジストラに転送中の AV ペアから開始します。レジストラにより USB トークン関連の AV ペアが検出されると、レジストラがすでに設定されている場合、レジストラは USB トークン宛ての設定情報を作成できます。現在、コンフィギュレーション コマンドは特定の設定ファイルとして送信され、引き続き実行コンフィギュレーションとマージされます。

管理者は通常の SDP コンフィギュレーション コマンドを活用して、USB トークンを設定できます。設定する必要がある USB トークン情報には、証明書、ブートストラップ設定、および PIN 番号設定があります。

SDP 完了段階と USB トークン

完了段階の始めに、紹介はペティショナに転送中の AV ペアに移ります。指定のファイル システム位置には各種ファイルが保管されており、既存の設定ファイル処理が行われます。この順序により、転送された新しいファイルを設定で利用できます。

設定された USB トークンの使用

USB トークンがペティショナ A により設定されたら、その現在位置からリモート位置へと転送されます。リモート位置には、2 番目のペティショナであるペティショナ B が配置されています。USB トークンはターゲットデバイスであるペティショナ B に挿入されます。ペティショナ B では USB トークンの設定と USB トークンの暗号素材が継承されます。リモート位置のエンドユーザには、USB トークンの PIN 番号がなければなりません。PIN 番号は、出荷時デフォルトの PN 番号、または紹介段階中に管理者が設定した PIN 番号のいずれかになります。

SDP による外部 AAA データベースの使用方法

外部 AAA データベースは、SDP 交換中に 2 回アクセスされます。AAA データベースへの最初のアクセスでは、イントロデューサが認証されます。つまりレジストラで、セキュア HTTP（HTTPS）サーバー経由で紹介要求が受信されると、イントロデューサのユーザー名とパスワードに基づいて AAA 検索が行われ、要求が許可されます。AAA データベースへの 2 番目のアクセスでは、認証情報が取得され、ペティショナデバイスに発行された設定および証明書に適用されます。つまり、レジストラはペティショナが署名している証明書を使用して要求シグニチャが完全であることを確認します。証明書の題名は AAA データベースで指定でき、最大 9 つの設定テンプレート型変数を指定し、テンプレート設定にまで展開できます。

自己署名証明書と別の CA サーバにより発行された証明書の使用

デフォルトでは、SDP 交換の実施結果では、ペティショナ デバイスに証明書が 1 枚だけ発行されます。発行される証明書は 1 枚だけですが、イントロデューサでは複数デバイスを紹介し、複数の証明書を取得する際の制限はありません。発行されている証明書の題名を指定することで、イントロデューサに関連しているすべての証明書がこのように発行されていることを保証できます。PKI AAA 統合により、さらにこれらの証明書の使用を制限できます。さらに、ユーザごとに 1 つだけ認証および認可の要求を許可するよう、AAA データベースを設定できます。

ペティショナ証明書は自己署名されているため、ペティショナの公開キーを伝送するためだけに使用されます。証明書に対する確認チェックや認可チェックは行われません。したがって、認可はユーザごとに行われ、デバイス単位の情報は使用されません。

デバイス単位の認可を使用した方が好ましい場合もあります。したがって、ペティショナが SDP トランザクションのために他の認証機関（CA）サーバにより発行された証明書を使用できる場合、既存の PKI を使用でき、その証明書属性に対して認可を受けることができます。

証明書を使用して認可を受けるためにペティショナとレジストラを設定すると、展開中の特定のデバイスの認可が受けられます。以前は、イントロデューサとペティショナ間の通信は、イントロデューサとペティショナデバイス間の物理的なセキュリティだけでその安全が確保され

ていました。SDPの証明書を使用した認可では、レジストラは紹介を受け入れる前に、現在のデバイス ID を確認できる機会があります。

SDP の認証および認可リスト

SDP レジストラを設定している場合に認証リストと認可リストを指定すると、レジストラではイントロデューサのすべての要求に対して、指定のリストが使用されます。認証リストは、イントロデューサを認証する場合に使用されます（AAA サーバでユーザ名とパスワードを確認して、アカウントが有効かどうか確認されます）。認可リストは、証明書題名およびペティショナに返信される Cisco IOS コマンドライン インターフェイス（CLI）スニペットに展開されるテンプレート型変数のリストの該当認可フィールドを受信する場合に使用されます。認証リストと認可リストは通常、同じ AAA サーバ リストを指しますが、認証と認可に異なるデータベースを使用できます（異なるデータベースへのファイルの保管は推奨しません）。

ペティショナが紹介要求をする場合、複数の照会が RADIUS サーバまたは TACACS+ サーバ上の AAA リスト データベースに送信されます。照会により、次の形式のエントリが検索されます。

```
user Password <userpassword>
   cisco-avpair="ttti:subjectname=<<DN subjectname>>"
   cisco-avpair="tti:iosconfig#<<value>>"
   cisco-avpair="tti:iosconfig#<<value>>"
   cisco-avpair="tti:iosconfig#=<<value>>"
```

（注） 有効な AAA ユーザ名レコードさえあれば、認証チェックを通過できます。「cisco-avpair=tti」情報は、認可チェックの場合だけ必要です。

認可応答で題名を受信した場合、SDP レジストラによりその題名は登録データベースに保管され、「subjectname」は、ペティショナデバイスからの以降の証明書要求（PKCS10）で提供される題名より優先されます。

番号が付けられた「tti:iosconfig」値は、ペティショナに送信される SDP Cisco IOS スニペットに展開されます。設定により、あらゆる番号付き（$1 ～ $9）のテンプレート型変数が置き換えられます。デフォルト Cisco IOS スニペットテンプレートには変数 $1 ～ $9 が含まれていないため、外部 Cisco IOS スニペットテンプレートを設定しない限り、これらの変数は無視されます。外部設定を指定するには、**template config** コマンドを使用します。

（注） テンプレート設定位置には、変数「$n」が含まれている場合があります。この変数はユーザーがログインに使用した名前に展開されます。

管理イントロデューサの認証リストと認可リスト

SDP メカニズムでは、イントロデューサとデバイス間に永続的関係があることを前提としています。その結果、イントロデューサのユーザ名はデバイス名の定義に使用されます。

SDP配置シナリオの中には、イントロデューサが多数のデバイスの紹介を行う、管理者の場合があります。ただし、イントロデューサ（管理者）名を使用してデバイス名を定義すると、複数のデバイスのデバイス名が同じになり、正しく配置されなくなります。代わりに、管理イントロデューサを使用すれば、管理者は紹介中に正しいデバイス名を指定できます。

一般的に言えば、イントロデューサのユーザ名がデータベース レコード ロケータとして使用され、Cisco IOS 設定テンプレート、（AAA データベースから取り出され、テンプレートに展開される）各種テンプレート型変数、およびデバイスに発行されたPKI証明書の該当する題名など、デバイスに関する他のすべての情報が決定されます。簡単にするため、データベース レコード ロケータはユーザ名またはデバイス名と呼びます。

管理イントロデューサは、デバイス名を提供します。そのようにして、管理者は紹介を行う場合に適切なレコード ロケータを提供できます。たとえば、管理者がユーザー名「user1」のデバイスを紹介しようとしている場合、管理者はそのデバイスをPKIネットワークに紹介し、管理者自身のログイン情報を使用してレジストラにログインした後に、user1 をレコードロケータとして提供します。レコード ロケータ user1 がデバイス名になります。紹介に固有の他のすべてのテンプレートおよびPKI 証明書の題名に関する情報が、管理者のレコードではなく、user1 ユーザー名レコードにより提供されます。

レジストラ デバイスでは、ユーザ イントロデューサ名とともに、提供されたユーザ名情報が使用されます。ユーザー名により既存のメカニズムで、変更なくサポートする必要があるユーザーの認可、テンプレート、およびPKI 証明書の情報が判断できます。

カスタム テンプレートの SDP での動作

カスタム テンプレートを使用して、SDP プロセスを簡略化できます。

- カスタム テンプレートにより、Web ページに必要な開始情報を記入できるため、イントロデューサはレジストラに連絡する必要がなくなり、SDP トランザクションを即座に開始できます。
- カスタム テンプレートにより、カスタマイズされた展開情報を Web ページに表示できるため、ユーザに合せてユーザ エクスペリエンスを調整できます。

デフォルト テンプレートを変更すると、カスタム テンプレートを簡単に定義できます。カスタム テンプレートがない場合、イントロデューサは SDP トランザクションが開始できるための情報をレジストラに問い合わせる必要があります。デフォルトテンプレートのリストについては、SDP トランザクション Web ページのデフォルト テンプレート（1421 ページ）の項を参照してください。

（注） カスタムテンプレートを設定するのは、上級の SDP ユーザーだけに限定することを推奨します。テンプレートがイントロデューサのブラウザに表示される前に、テンプレートを誤って変更してしまった場合に問題が発生するおそれがあるためです。

カスタム テンプレート型変数の展開

テンプレートには、Cisco IOS SDP レジストラまたはペティショナにより置き換えられる展開変数があります。これらの変数は、次のように展開されます。

- $$：「$」
- $a：属性と値（AV）のペア
- $c：信頼できる証明書
- $d：ブラウザのダンプ AV ペア
- $h：ホスト名
- $k：キーラベルまたは「tti」
- $l：トラストポイントラベル＝「tti」
- $n：HTTP クライアントのユーザー名
- $s：TTI キーのデフォルトサイズ
- $t：トラストポイント設定
- $u：完了 URL
- $1 ～ $9：ユーザー認証中に AAA サーバーから取得された変数

カスタム テンプレート型変数の展開ルール

設定とテンプレートはSDP交換中に使用されます。使用前および配布後、これらのテンプレートは、SDP 通信段階に基づき、次のルールで展開されます。

カスタム HTML テンプレートの展開ルール

HTML テンプレートは HTTP クライアントに送信される前に、即座に展開されます。HTTP テンプレートは次のように展開されます。

- $u：SDP 完了 URL（例：http://10.10.10.1/ezsdd/completion）が入力される完了 URL。この変数は、内部「ウィザード」状態として SDP により内部的に使用されます。通常のウィザード処理のため、SDP 紹介ページには「<FORM action=\“$u\”method=\“post\”>」といったようなテキストが含まれている場合があります。
- $n：管理イントロデューサにより入力されたイントロデューサ名またはデバイス名。
- $$：$
- $h：ホスト名
- $a：指定のテンプレート文字があるないにかかわらずすべての AV ペアは、次の HTML フォーム形式に書き出されます（これらの AV ペアは「INPUT type=hidden」でないため、テンプレートまたはSDPプロセスのデバッグのためにWebページに直接表示されます）。

<INPUT type=hidden NAME="attribute string here"

value="variable string here">

すべての HTML テンプレートに以下のラインがなければなりません。

$d = dump all av pairs in: attribute = value

URL テンプレートの展開ルール

設定テンプレートの発信元、ファイル テンプレートの発信元、およびファイル宛先には URL が存在します。これらの変数は、レジストラが URL を作成するとき、つまり設定またはファイルを取得する直前に展開されます。ファイル宛先については、これらの変数は、ペティショナによりファイルがファイル宛先にコピーされる直前に展開されます。

- $$: $
- $h : ホスト名

iPhone の導入に関する URL テンプレートの展開ルール

iPhone を導入するために、次のテンプレート展開変数が導入されました。

- $o : チャレンジパスワード。このテンプレート文字は、SDP レジストラが Simple Certificate Enrollment Protocol（SCEP）サーバからチャレンジ パスワードを取得した後、開始段階で設定プロファイルが iPhone に送信される前に、SDP レジストラによって展開されます。
- $i : iPhone の固有デバイス識別子（UDID）。このテンプレート文字は、紹介段階で設定プロファイルが iPhone に送信される前に、SDP レジストラによって所有者名の CN フィールドに展開されます。
- $p : 所有者名の差別化要因。このテンプレート文字は、CLI によって設定された値を使用して SDP レジストラによって展開されます。詳細については、Apple iPhone を導入するための SDP レジストラの設定 （1439 ページ）を参照してください。この値は、SCEP サーバが iPhone に対して発行する 2 つの証明書を区別するために使用されます。1 つの証明書は完了段階で発行され、もう 1 つの証明書は VPN 確立段階で発行されます。この値を挿入する所有者名の部分またはフィールドを決定します。

詳細については、PKI で SDP が Apple iPhone を導入する方法 （1424 ページ） を参照してください。

カスタム設定およびファイルのテンプレート型変数の展開ルール

カスタム設定とファイルのテンプレート型変数は両方とも、レジストラが設定またはファイルのテンプレートを作成する場合、またペティショナが設定またはファイルのテンプレートを受信する場合に展開されます。

カスタム設定とファイルのテンプレート型変数のレジストラでの展開ルール

レジストラが設定またはファイルのテンプレートを展開する場合、Cisco IOS CA により次の変数が使用されます。これらの変数は、SDP ウィザードで送信前に展開されます。

- $$：$
- $h：ホスト名
- $t：クライアントで展開されるよう $l、$k、および $ を組み込んだ単純なトラストポイントデフォルト設定
- $1 ～ $9：ユーザー認証中に AAA サーバーから取得された変数（ファイルテンプレートには適用されない）

カスタム設定とファイルのテンプレート型変数のペティショナでの展開ルール

ペティショナが設定またはファイルのテンプレートを展開する場合、次の変数が展開されます。

- $$：$
- $h：ホスト名
- $k：キーラベル
- $l：トラストポイントラベル
- $s：キーのサイズ
- $c：証明書チェーンに展開
- $n：ユーザー名に展開（ファイルテンプレートには適用されない）

カスタム設定 HTTP テンプレート型変数の展開ルール

カスタム設定 HTTP テンプレートにより、バックエンド コモン ゲートウェイ インターフェイス（CGI）スクリプトに柔軟性が与えられ、外部管理システムと統合されます。テンプレート URL は、レジストラが外部管理システムからブートストラップ設定を受信する前に、HTTP テンプレートを展開することで実行されます。デバイス情報に基づいて特定のブートストラップ設定ファイルが見つかるようにするため、デバイス名（$n）は URL に展開され、外部管理システムへと渡されます。

（注） 表示される HTML テキストの変更だけ行う必要があります。既存の展開変数、Javascript、およびデフォルトテンプレートの形式は、テンプレートのカスタマイズ時には削除しないでください。これらのは SDP が正しく動作するために必要な情報です。

HTTP テンプレートの展開と **template config** コマンドにより、次のいずれかのファイルタイプを指定して、カスタマイズ ブートストラップ構成ファイルを取得できます。

- デバイス名を使用した構成ファイル（例：template config http://myserver/$n-config-file.conf）
- デバイス名を使用した CGI スクリプト（例：template config http://myserver/cgi-bin/mysdpcgi post）

Cisco IOS リリース 12.4(6)T の時点で、ブートストラップ設定がデバイス名だけでなく、タイプ、Cisco IOS 現行バージョン情報、および現行の設定で識別できるよう CGI サポートが拡張されました。この機能では、**post** キーワードにより **template config** コマンドが拡張されています。このキーワードはレジストラに、HTTP または HTTPS プロトコルだけを使用した CGI スクリプトによってこの追加デバイス情報を外部管理システムに送信するよう指示します。

レジストラにより、AVペア（$a）を使用してデバイス情報が外部管理システムに渡されます。AV ペア情報を使用して、管理システムは適切なブートストラップ設定ファイルを識別し、レジストラに返信します。カスタマイズ ブートストラップ構成ファイルを識別するため、拡張 CGI サポートにより送信される追加 AV ペアを次の表に示します。

表 *150 : HTTP* ポスト中に外部管理システムに送信される *AV* ペア

AV ペア	**説明**
TTIFixSubjectName	AAA_AT_TTI_SUBJECTNAME（レルム認証ユーザがレジストラでルート ユーザでない場合だけ送信）
TTIIosRunningConfig	**show running-config brief** の出力
TTIKeyHash	デバイス公開キー上で計算されるダイジェスト
TTIPrivilege	AAA_AT_TTI_PRIVILEGE：ユーザーが管理者の場合は「admin」、ユーザーが管理者でない場合は「user」が送信されます（レルム認証ユーザーが管理者で AAA サーバーから情報が利用できる場合だけ送信）
TTISignature	UserDeviceName および TTISignCert を除く AV ペアすべてで計算されるダイジェスト
TTISignCert	デバイスの現在の証明書（デバイスに現在証明書がある場合だけ送信）
TTITemplateVar	AAA_AT_TTI_IOSCONFIG（1-9）（レルム認証ユーザがレジストラでルート ユーザでない場合だけ送信）
TTIUserName	デバイス名
TTIVersion	TTI バージョンのレジストラ
UserDeviceName	管理イントロデューサにより入力されたデバイス名（レルム認証ユーザが管理者の場合だけ送信）

（注） レジストラでは Cisco IOS リリース 12.4（6）T が実行され、**template config** コマンドは **post** キーワードを指定して発行する必要があります。また、*url* 引数には HTTP または HTTPS のいずれかが含まれている必要があります。拡張CGIテンプレート機能にはその他のプロトコルはサポートされていません（例：FTP）。

SDP トランザクション Web ページのデフォルト テンプレート

SDP トランザクション Web ページにはそれぞれ、次のデフォルトテンプレートが存在します。

- デフォルトの予備接続テンプレート （1421 ページ）
- デフォルト開始ページ テンプレート （1422 ページ）
- デフォルトようこそページ テンプレート （1423 ページ）
- デフォルト紹介ページ テンプレート （1423 ページ）
- デフォルト管理紹介ページ テンプレート （1423 ページ）
- デフォルト完了ページ テンプレート （1423 ページ）

デフォルトの予備接続テンプレート

予備接続テンプレートは、ユーザの環境に応じた値を含めるよう、管理者により変更できます。予備接続ページのフォーマットも、テンプレートに含まれている設定により変更できます。

管理者がカスタマイズする必要があるレジストラの IP アドレスを除き、予備接続テンプレートは次に示すように使用できます。

```
<html><head><title>
SDP: Test Internet Connection</title></head>
<noscript><b>
If you see this message, your browser is not running JavaScript,<br>
which is required by Cisco Secure Device Provisioning.<br>
If you cannot enable JavaScript, please contact your system administrator.
<br><br></b></noscript>
<body style="background-color: rgb(204, 255, 255);">
<div style="text-align: center;"><big><big>
Secure Device Provisioning</big><br>
Test Internet Connection</big><br><br>
<form action="http://10.10.10.1/ezsdd/connect" method="post">
<input type="submit" value="Log onto Cisco Device"><br><br>
Default username/password is cisco/cisco.
<input type="hidden" name="TTIAfterConnectURL" value="http://10.10.10.1/ezsdd/welcome">
<!-- Note, that for the below, 198.133.219.25 = www.cisco.com. -->
<input type="hidden" name="TTIConnectTestURL" value="http://198.133.219.25">
<input type="hidden" name="TTIInsideAddr" value="10.10.10.1">
<input type="hidden" name="TTIlanport" value="Vlan1">
<input type="hidden" name="TTIwanport" value="FastEthernet4">
</form></div></body></html>
```

非表示 HTML 形式フィールド

非表示 HTML 形式フィールドにより、初期設定情報が管理者により設定されたとおりにブラウザに送信されますが、署名はされていません。

（注） 「非表示」という用語は、イントロデューサができるだけ混乱しないよう、これらの HTML 形式フィールドが予備接続ページに表示されないことを示します。

管理者は、次の表に示すように、予備接続テンプレートの非表示 HTML 形式フィールドを設定できます。

表 *151 :* 予備接続段階中に送信される管理者が定義した *AV* ペア

AV ペア	説明
TTIAfterConnectURL	管理者は、TTIAfterConnectURL フィールドをようこそページの URL または開始ページの URL のいずれかに設定できます。ようこそページの URL は、ペティショナの出荷時デフォルト IP アドレスに指定されています。接続後 URL は、インターネット接続確立後に SDP が使用されない場合に任意の有効な URL になることができます。
TTIConnectTestURL	管理者は、TTIConnectTestURL フィールドを、インターネット接続確立時にアクセスできるはずの有効な URL に設定できます。予備接続テンプレートのデフォルト値は、www.cisco.com（198.133.219.25）です。
TTIInsideAddr	管理者は、TTIInsideAddr フィールドをペティショナの出荷時デフォルト IP アドレスに設定できます。Cisco 871 ISR の場合は、IP アドレスは 10.10.10.1 です。
TTIlanportx	管理者は、TTIlanportx フィールドをペティショナ プラットフォームの LAN インターフェイスに設定できます。このフィールドは、Cisco IOS 接続設定の適用に使用できます。Cisco 871 の場合は、フィールド値は「Vlan1」になります。
TTIwanport	管理者は、TTIwanport フィールドをペティショナの WAN インターフェイス名に設定できます。このフィールドは、Cisco IOS 接続設定の適用に使用できます。Cisco 871 の場合は、フィールド値は「FastEthernet4」になります。

（注） 接続テンプレートはカスタマイズできません。

デフォルト開始ページ テンプレート

```
<html><head><title>EZ-Secure Device Deployment Start page on $h</title></head>
<NOSCRIPT><B>
If you see this message, your browser is not running JavaScript.<BR>
Cisco Secure Device Deployment requires JavaScript.<BR> Please contact
your system adminstrator.<BR><BR></B></NOSCRIPT>
<SCRIPT LANGUAGE="JavaScript">
function submit_to_url(form){
form.action=form.TTIWelcomeURL.value;return true;}</SCRIPT>
<B>Welcome to Cisco Secure Device Deployment Server $h</B> <FORM  action="" method="post"
 onSubmit="return submit_to_url(this)"> Your
device:<BR> <INPUT type="text" name="TTIWelcomeURL" size=80  value=\"\"><BR><BR> <INPUT
 type="submit" value="Next"><BR>
$a</FORM></html>
```

デフォルトようこそページ テンプレート

```
<html><head><title>EZ-Secure Device Deployment WELCOME to $h</title></head>
<NOSCRIPT><B>
If you see this message, your browser is not running JavaScript.<BR>
Cisco Secure Device Deployment requires JavaScript.<BR> Please contact
your system adminstrator.<BR><BR></B></NOSCRIPT>
<SCRIPT LANGUAGE=\"JavaScript\">
function submit_to_url(form){
natURL=location.href.split(\"/\");
localURL=form.TTICompletionURL.value.split(\"/\");
if(natURL[2]!=localURL[2]){
form.TTICompletionURL.value=localURL[0]+\"//\"+natURL[2]+\"/
\"+localURL[3]+
\"/\"+localURL[4];}
form.action=form.vpnserviceurl.value;
return true;}</SCRIPT>
<B>Welcome to Cisco Secure Device Deployment for $h</B> <FORM  action=\"\" method=\"post\"
 onSubmit=\"return submit_to_url (this)\">
To join a Virtual Private Network (VPN) enter the web<BR> site URL
provided by your network administrator:<BR> <INPUT type=\"text\"  name=\"vpnserviceurl\"
 size=80 value=\"\"><BR><BR><INPUT  type=\"submit\" value=\"Next>\"><BR> $a</FORM></html>
```

デフォルト紹介ページ テンプレート

```
<html><head><title>EZ-Secure Device Deployment INTRODUCTION to $h</title>
</head><B>Welcome to the VPN network gateway on $h</B> <FORM  action=\"$u\"
method=\"post\"> Your 'username' and 'password' entered
have been accepted.<BR> Your device will now be allowed to
automatically join the VPN network.<BR> <BR>Press Next to complete
automatic configuration of your VPN Device.<BR> <BR><INPUT  type=\"submit\"
value=\"Next>\"><BR> $a</P></FORM></html>
```

デフォルト管理紹介ページ テンプレート

```
<html><head><title>EZ-Secure Device Deployment ADMINISTRATIVE
INTRODUCTION to $h</title></head> <NOSCRIPT><B> If you see this
message, your browser is not running JavaScript.<BR> Cisco Secure
Device Deployment requires JavaScript.<BR> Please contact your system
adminstrator.<BR><BR></B></NOSCRIPT>
<SCRIPT LANGUAGE=\"JavaScript\">
function submit_to_url(form){
form.introadminurl.value=location.href+\"/admin\";
form.action=form.introadminurl.value;
return true;}</SCRIPT>
<B>Welcome to the VPN network gateway on $h</B> <FORM action=\"\"  method=\"post\"
onSubmit=\"return submit_to_url (this)\"> Your
administrator 'username' and 'password' entered have been
accepted.<BR> Please provide the name to be associated with this
device:<BR> <INPUT type=\"text\" name=\"userdevicename\" size=64  value=\"\"><BR><BR>
<INPUT type=\"submit\" value=\"Next>\"><BR> <INPUT  type=\"hidden\" name=\"introadminurl\"
 value=\"\"><BR>
$a</FORM></html>
```

デフォルト完了ページ テンプレート

```
<html><head><title>EZ-Secure Device Deployment COMPLETE on $h</title></head>
<B>Now enrolling $h with the VPN network...</B><BR> Full network VPN
access should be available in a moment.<BR><BR> $d<BR></html>
```

設定ファイルのデフォルト テンプレート

デフォルト設定のテンプレートを示します。このデフォルト設定ファイルは、設定テンプレートが指定されていない、または **template config** コマンドが **post** キーワードを指定せずに発行されている場合に使用されます。デフォルト設定テンプレートの使用方法の詳細については、UsingaConfigurationTemplateFile の例 （1455 ページ）を参照してください。

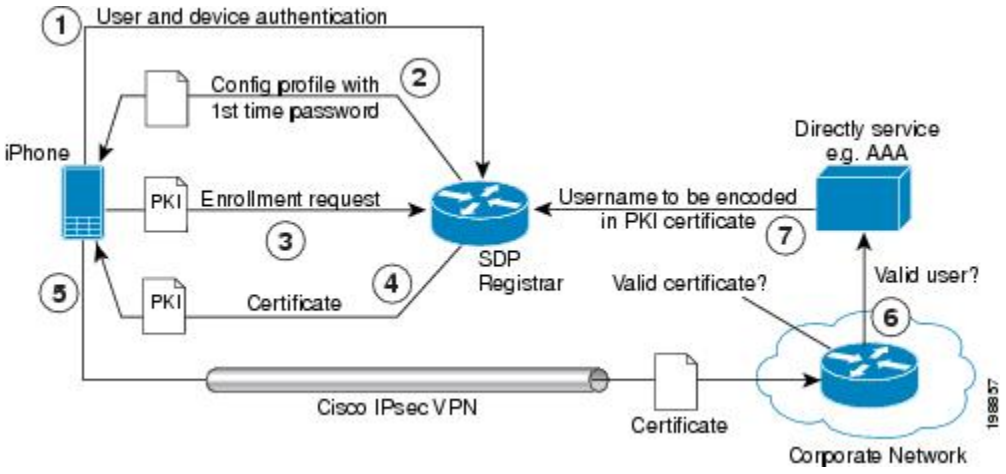
```
$t
!
$c
!
end
```

PKI で SDP が Apple iPhone を導入する方法

Cisco IOS 15.1(2)T および Apple iPhone OS 3.0 リリースが導入されたため、Cisco IOS ネットワーク デバイスで Apple iPhone がサポートされるようになりました。Cisco IOS ルータは SDP レジストラを使用して iPhone を導入し、IPSec VPN、SCEP サーバ、および PKI 証明書の導入テクノロジーを使用してネットワーク アプリケーションに安全にアクセスできるようにします。

Apple iPhone では、XML ベースの「設定プロファイル」の配布と証明書の初期導入を組み合わせて実行します。SDP はこれらの初期の証明書を使用してエンタープライズ アプリケーションへのアクセスを認証し、その後のプロファイルの配布を暗号化します。SDP は、iPhone にデジタル証明書を配布する際に、この登録ソリューションを使用します。

図 *50 : PKI* での *SDP* レジストラによる *iPhone* の導入



PKI での SDP レジストラによる Apple iPhone の導入段階

ここでは、PKI で SDP レジストラが iPhone を導入する場合の各段階について説明します。

SDP 導入開始段階

次のステップでは、SDP 導入開始段階について説明します。

（注） SDP 導入開始段階は、『Apple iPhone Enterprise Deployment Guide』（http://manuals.info.apple.com/en_US/Enterprise_Deployment_Guide.pdf）で説明する「Begin Enrollment」段階（またはフェーズ 1）と同じです。

手順の概要

1. iPhone ユーザは Safari ブラウザを開き、開始ページの HTTPS URL を入力します。たとえばこの HTTPS URL は、社内のネットワーク アドレスなどです。SDP レジストラの HTTPS ページによってプロセスが開始されます。
2. ユーザは、ユーザ名とパスワードを入力して Cisco ルータとの認証を開始します。Cisco ルータは SDP レジストラとして動作します。
3. SDP レジストラは SCEP サーバに接続し、チャレンジ パスワードを取得します。
4. SDP レジストラは、チャレンジ パスワード、SCEP サーバの URL、および iPhone 属性の要求で構成される設定プロファイルを XML 形式で作成します。SCEP サーバの URL は登録要求の送信に使用され、iPhone デバイスの属性は RSA キーを生成する際に iPhone によって使用されます。
5. iPhone ユーザは、設定ファイルを iPhone にインストールして、SDP 開始段階を終了します。

手順の詳細

ステップ 1 iPhone ユーザは Safari ブラウザを開き、開始ページの HTTPS URL を入力します。たとえばこの HTTPS URL は、社内のネットワーク アドレスなどです。SDP レジストラの HTTPS ページによってプロセスが開始されます。

ステップ 2 ユーザは、ユーザ名とパスワードを入力して Cisco ルータとの認証を開始します。Cisco ルータは SDP レジストラとして動作します。

ステップ 3 SDP レジストラは SCEP サーバに接続し、チャレンジ パスワードを取得します。

ステップ 4 SDP レジストラは、チャレンジ パスワード、SCEP サーバの URL、および iPhone 属性の要求で構成される設定プロファイルを XML 形式で作成します。SCEP サーバの URL は登録要求の送信に使用され、iPhone デバイスの属性は RSA キーを生成する際に iPhone によって使用されます。

次の例は、SDP 導入開始段階で SDP レジストラが iPhone に送信する設定プロファイルを示しています。

例：

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE plist PUBLIC "-//Apple Inc//DTD PLIST 1.0//EN" "http://
www.apple.com/DTDs/PropertyList-1.0.dtd">
<plist version="1.0">
<dict>
<key>PayloadContent</key>
<dict>
<key>URL</key>
<string>https://profileserver.example.com/iphone</string>
<key>DeviceAttributes</key>
```

```
<array>
<string>UDID</string>
<string>IMEI</string>
<string>ICCID</string>
<string>VERSION</string>
<string>PRODUCT</string>
</array>
<key>Challenge</key>
<string>optional challenge</string>
```

ステップ 5 iPhone ユーザは、設定ファイルを iPhone にインストールして、SDP 開始段階を終了します。

SDP 導入ようこそ段階

SDP 導入ようこそ段階は iPhone には適用されません。これは、イントロデューサ（Safari Web ブラウザなど）が SDP ペティショナ（iPhone）で実行されるためです。

SDP 導入紹介段階

次のステップでは、SDP 導入紹介段階について説明します。

（注） SDP 導入紹介段階は、「デバイス認証」段階に相当します。

手順の概要

1. iPhone は、要求されたデバイス属性情報とチャレンジ パスワードを含む HTTPS POST を設定プロファイルとしてトリガーします。HTTPS POST は、SDP 導入開始段階で取得した設定プロファイルに指定されている HTTPS の URL に送信されます。これは、SDP 導入紹介段階の URL である必要があります。POST データは Apple 社が発行した証明書（組み込みの ID）を使用して iPhone によって署名されます。そしてこの署名が確認され、ID が確認され、デバイス属性が確認されます。
2. iPhone によって送信された UDID は SDP レジストラによって取得され、所有者名に追加されます。その後、SDP レジストラによって取得されたデバイス属性は、これが本当に受け入れられるデバイスのタイプであるかどうかを判断するために使用されます。たとえばネットワーク管理者は、3GS の iPhone のみをネットワークで使用できるように許可します。これは、iPhone 3GS にはハードウェアに暗号化された保管場所があるためです。取得されたデバイス属性によって、SDP レジストラは 3GS の iPhone と 3G の iPhone を区別できます。
3. SDP レジストラは、SCEP サーバの HTTP URL、登録要求で送信される所有者名（UDID を含む）、キーのサイズ、キーのタイプ、キーの使用状況、およびチャレンジパスワードで構成された設定プロファイルを作成して応答します。開始段階がスキップされた場合、SDP レジストラは SCEP サーバに接続し、チャレンジパスワードを取得します。SDP レジストラが所有者名とチャレンジパスワードを取得する方法の詳細については、iPhone の導入に関する URL テンプレートの展開ルール （1418 ページ）を参照してください。

手順の詳細

ステップ 1 iPhone は、要求されたデバイス属性情報とチャレンジパスワードを含む HTTPS POST を設定プロファイルとしてトリガーします。HTTPS POST は、SDP 導入開始段階で取得した設定プロファイルに指定されている HTTPS の URL に送信されます。これは、SDP 導入紹介段階の URL である必要があります。POST データは Apple 社が発行した証明書（組み込みの ID）を使用して iPhone によって署名されます。そしてこの署名が確認され、ID が確認され、デバイス属性が確認されます。

ステップ 2 iPhone によって送信された UDID は SDP レジストラによって取得され、所有者名に追加されます。その後、SDP レジストラによって取得されたデバイス属性は、これが本当に受け入れられるデバイスのタイプであるかどうかを判断するために使用されます。たとえばネットワーク管理者は、3GS の iPhone のみをネットワークで使用できるように許可します。これは、iPhone 3GS にはハードウェアに暗号化された保管場所があるためです。取得されたデバイス属性によって、SDP レジストラは 3GS の iPhone と 3G の iPhone を区別できます。

次の例は、SDP 導入紹介段階で iPhone が送信する設定プロファイルを示しています。

例：

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN" "http://www.apple.com/
  DTDs/PropertyList-1.0.dtd">
<plist version="1.0">
<dict>
<key>UDID</key>
<string></string>
<key>VERSION</key>
<string>7A182</string>
<key>MAC_ADDRESS_EN0</key>
<string>00:00:00:00:00:00</string>
<key>CHALLENGE</key>
either:
    <string>String</string>
or:
    <data>"base64 encoded data"</data>
</dict>
</plist>
```

ステップ 3 SDP レジストラは、SCEP サーバの HTTP URL、登録要求で送信される所有者名（UDID を含む）、キーのサイズ、キーのタイプ、キーの使用状況、およびチャレンジパスワードで構成された設定プロファイルを作成して応答します。開始段階がスキップされた場合、SDP レジストラは SCEP サーバに接続し、チャレンジパスワードを取得します。SDP レジストラが所有者名とチャレンジパスワードを取得する方法の詳細については、iPhone の導入に関する URL テンプレートの展開ルール（1418 ページ）を参照してください。

（注） SDP レジストラでは RSA のキー タイプのみをサポートしています。

次の例は、SDP 導入紹介段階で SDP レジストラが送信する設定プロファイルを示しています。

例：

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE plist PUBLIC "-//Apple Inc//DTD PLIST 1.0//EN" "http://
www.apple.com/DTDs/PropertyList-1.0.dtd">
<plist version="1.0">
```

```
<dict>
<key>PayloadContent</key>
<dict>
<key>URL</key>
<string>https://iphone.vpn.apple.com/pkifoobar.exe</string>
<key>Name</key>
<string>instance_for_getcacert_call</string>
<key>Subject</key>
<array>
<array>
<array>
<string>O</string>
<string>Apple Inc.</string>
</array>
</array>
<array>
<array>
<string>CN</string>
<string>Foo</string>
</array>
</array>
</array>
<key>Challenge</key>
<string>CHALLENGE</string>
<key>Keysize</key>
<integer>1024</integer>
<key>Key Type</key>
<string>RSA</string>
<key>Key Usage</key>
<integer>5</integer>
</dict>
<key>PayloadDescription</key>
<string>Provides device encryption identity</string>
<key>PayloadUUID</key>
<string>fd8a6b9e-0fed-406f-9571-8ec98722b713</string>
<key>PayloadType</key>
<string>com.apple.security.scep</string>
<key>PayloadDisplayName</key>
<string>Encryption Identity</string>
<key>PayloadVersion</key>
<integer>1</integer>
<key>PayloadOrganization</key>
<string>Apple Inc.</string>
<key>PayloadIdentifier</key>
<string>com.apple.encrypted-profile-service</string>
</dict>
</plist>
```

SDP 導入ポスト紹介段階

次のステップでは、SDP 導入ポスト紹介段階について説明します。

（注） SDP 導入ポスト紹介段階は、『http://manuals.info.apple.com/en_US/Enterprise_Deployment_Guide.pdfApple iPhone Enterprise Deployment Guide』で説明する「Certificate Installation」段階（またはフェーズ 3）と同じです。

手順の概要

1. iPhone は、SDP 導入紹介段階で SDP レジストラから取得した SCEP 情報を含む設定プロファイルの指定をインストールします。
2. iPhone はプロファイルに指定された指示に従ってキーを生成し、HTTP URL がプロファイルに指定されている SCEP サーバに登録要求とチャレンジ パスワードを送信します。
3. SCEP サーバはチャレンジ パスワードを確認し、iPhone にデジタル証明書を発行します。
4. ユーザはこの証明書を iPhone にインストールし、Cisco IPsec VPN を使用して会社のネットワークに接続できます。

手順の詳細

ステップ 1 iPhone は、SDP 導入紹介段階で SDP レジストラから取得した SCEP 情報を含む設定プロファイルの指定をインストールします。

ステップ 2 iPhone はプロファイルに指定された指示に従ってキーを生成し、HTTP URL がプロファイルに指定されている SCEP サーバに登録要求とチャレンジ パスワードを送信します。

ステップ 3 SCEP サーバはチャレンジ パスワードを確認し、iPhone にデジタル証明書を発行します。

ステップ 4 ユーザはこの証明書を iPhone にインストールし、Cisco IPsec VPN を使用して会社のネットワークに接続できます。

（注） この証明書は、VPN の設定などの会社のその他の設定や Wi-Fi の設定のダウンロードに使用することもできます。

SDP 導入第二紹介段階

次のステップでは、SDP 導入第二紹介段階について説明します。

（注） SDP 展開第2導入段階は、『http://manuals.info.apple.com/en_US/Enterprise_Deployment_Guide.pdf Apple iPhone Enterprise Deployment guide』で説明する「Device Configuration」段階（またはフェーズ 4）と同じです。

手順の概要

1. iPhone は、次の場合を除き SDP 導入紹介段階を繰り返します。
2. SDP レジストラは、VPN の設定、Wi-Fi の設定、および電子メールの設定などの会社の一般的な設定を含む設定プロファイルを使用して応答します。また、VPN の確立に使用する別の証明書の SCEP の設定も含みます。

手順の詳細

ステップ 1 iPhone は、次の場合を除き SDP 導入紹介段階を繰り返します。

- iPhone の POST データにチャレンジ パスワードが含まれていない。
- SDP 導入ポスト紹介段階で、SCEP サーバから取得した証明書を使用して、iPhone が POST データに署名している。

ステップ 2 SDP レジストラは、VPN の設定、Wi-Fi の設定、および電子メールの設定などの会社の一般的な設定を含む設定プロファイルを使用して応答します。また、VPN の確立に使用する別の証明書の SCEP の設定も含みます。

2 回目の SDP 導入ポスト紹介段階

2 回目の SDP 導入ポスト紹介段階は、SDP 導入ポスト紹介段階と同じです。iPhone は、2 回目の SDP 導入紹介段階で SDP レジストラが提供する SCEP の設定に基づいて証明書要求を生成し、SCEP サーバに登録します。

SDP 導入完了段階

SDP 導入完了段階は iPhone には適用されません。これは、イントロデューサ（Safari Web ブラウザなど）が SDP ペティショナ（iPhone）で実行されるためです。

PKI への登録のための Secure Device Provisioning（SDP）の設定方法

ここでは、ご使用の PKI に対して SDP を設定する場合に従う次の手順について説明します。レジストラは、レジストラ設定作業のいずれかだけにしたがって設定できます。

SDP ペティショナのイネーブル化

ペティショナをイネーブルまたはディセーブルにし、トラストポイントを SDP 交換に関連付ける場合にこの作業を行います。

またこの作業で、証明書および特定のトラストポイントに関連付けられた RSA キーを使用するようペティショナを設定できます。

（注） ペティショナは、暗号イメージを含むシスコデバイスではデフォルトでイネーブルにされています。したがって、以前にペティショナをディセーブルにしたことがあったり、自動生成されたトラストポイントではなく、既存のトラストポイントを使用する場合は、**crypto provisioning petitioner** コマンドを発行するだけです。

（注） デフォルトでは、SDP ペティショナ デバイスでは既存の証明書が使用されます。複数の証明書および特定の証明書が 1 つ存在する場合は、どちらか選択するためにこの作業を行います。ただし、デフォルト動作をイネーブルにする場合にはこの作業は必要ありません。

始める前に

- **ip http server** コマンドを使用して HTTP サーバーをイネーブルにする必要があります（HTTP サーバは通常、多数の Cisco IOS 設定ではデフォルトでイネーブルにされています）。
- 証明書および RSA キーを使用するようペティショナを設定している場合、SDP ペティショナデバイスには既存の製造業者の証明書または第三者の証明書がなければなりません。

手順の概要

1. **enable**
2. **configure terminal**
3. **crypto provisioning petitioner**
4. 次のいずれかを実行します。
   - **trustpoint** *trustpoint-label*
5. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**crypto provisioning petitioner** 例： `Router(config)# crypto provisioning petitioner`	SDP ペティショナデバイスの動作を変更できるようにし、tti-petitioner コンフィギュレーション モードを開始します。 （注） Cisco IOS リリース 12.3(14)T では、**crypto provisioning petitioner** コマンドが **crypto wui tti petitioner** コマンドに置き換えられました。

	コマンドまたはアクション	目的

ステップ 4	次のいずれかを実行します。
	• **trustpoint** *trustpoint-label*
	例：
	`Router(tti-petitioner)# trustpoint mytrust`
	例：
	例：
	例：
	trustpoint signing
	trustpoint-label
	例：
	`Router(tti-petitioner)# trustpoint signing mytrust`
		（任意）ペティショナとレジストラ間でSDP交換と関連付けるトラストポイントを指定します。
		（注） このコマンドが発行されないと、*trustpoint-label* 引数には自動的に「tti」のラベルが付きます。
		（任意）SDP交換中にすべての紹介データに署名する場合に使用されるトラストポイントと関連証明書を指定します。

ステップ 5	**end** 例： `Router(tti-petitioner)# end`	（任意）tti-petitioner コンフィギュレーション モードを終了します。

トラブルシューティングのヒント

SDP交換が完了したら、「tti」という新しいトラストポイントラベルができあがります。トラストポイントは、自動的に証明書サーバ（レジストラ）に登録されます。トラストポイントが実際に存在することを確認するには、**show running-config** コマンドを使用します。

次の作業

証明書と特定のトラストポイントに関連付けられた RSA キーを使用するようペティショナを設定する場合、「証明書を使用した認可のための SDP レジストラのイネーブル化」の作業で示されている方法で、レジストラを設定する必要があります。

SDP レジストラのイネーブル化と AAA リストのサーバへの追加

レジストラをイネーブルにし、証明書サーバを SDP 交換と関連付ける場合にこの作業を行います。

また、認証リストと認可リストをRADIUSサーバまたはTACACS+サーバに追加する場合にもこの作業を行うことができます。

前提条件

レジストラを設定する前に、次の作業を実行します。

- HTTP サーバまたは HTTPS サーバをイネーブルにします。

（注） HTTPS サーバをイネーブルにする前に、標準の HTTP サーバが設定されている場合は、それをディセーブルにるす必要があります。HTTP サーバーをディセーブルにするには、**no ip http server** コマンドを使用します。HTTPS サーバーをイネーブルにするには、**ip http secure-server** コマンドの後に **ip http secure-trustpoint** コマンドを発行する必要があります。指定のトラストポイントは、レジストラとユーザーのブラウザ間の HTTPS 通信に適切なレジストラ ローカル トラストポイントです。

- **crypto pki server** コマンドを使用して、Cisco IOS 証明書サーバーを設定します。

AAA リストを設定する場合、次の作業を完了するだけでなく、レジストラに必要な前提条件を完了する必要があります。

- ユーザ情報をAAAサーバデータベースに追加します。RADIUSサーバーまたはTACACS+ AAA サーバーを設定するには、『*Cisco IOS Security Configuration Guide*』の「Configuring RADIUS」および「Configuring TACACS+」の章を参照してください。
- 新しい AAA リストを設定します。AAA リストを設定するには、『*Cisco IOS Security Configuration Guide*』の「Configuring RADIUS」、「Configuring TACACS+」、「Configuring Authentication」、および「Configuring Authorization」を参照してください。

機能制限

Cisco IOS CA デバイスの要件

SDP プロセス中、Cisco IOS CA 証明書はピア デバイスに自動的に発行されます。SDP レジストラが第三者のベンダーの CA デバイスで設定されている場合、SDP プロセスは動作しません。

template config コマンド

Cisco IOS 設定変数は 9 つあります。設定でさらに柔軟性が必要な場合、**template config** コマンドを使用して、イントロデューサに固有の設定テンプレートを参照できます。設定の柔軟性の詳細については、「カスタム設定およびファイルのテンプレート型変数の展開ルール（1418ページ）」を参照してください。

手順の概要

1. **enable**
2. **configure terminal**
3. **crypto provisioning registrar**
4. **pki-server** *label*
5. **authentication list** *list-name*
6. **authorization list** *list-name*
7. **template username** *name* **password** *password*
8. **template config** *url* [**post**]
9. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**crypto provisioning registrar** 例： `Router(config)# crypto provisioning registrar`	デバイスを SDP 交換のレジストラになるよう設定し、tti-registrar コンフィギュレーション モードを開始します。 （注） Cisco IOS リリース 12.3(14)T では、**crypto provisioning registrar** コマンドが **crypto wui tti registrar** コマンドに置き換えられました。
ステップ 4	**pki-server** *label* 例： `Router(tti-registrar)# pki-server mycs`	ペティショナとレジストラ間でSDP交換と関連付ける証明書サーバを指定します。
ステップ 5	**authentication list** *list-name* 例： `Router (tti-registrar)# authentication list authen-tac`	（任意）SDP 交換でイントロデューサを認証します。
ステップ 6	**authorization list** *list-name* 例：	（任意）証明書の題名およびペティショナに返信される Cisco IOS CLI スニペットに展開されるテンプ

	コマンドまたはアクション	目的
	`Router (tti-registrar)# authorization list author-rad`	レート型変数のリストに該当する認証フィールドを受信します。
ステップ 7	**template username** *name* **password** *password* 例： `Router(tti-registrar)# template username ftpuser password ftppwd`	（任意）ファイルシステムの設定テンプレートにアクセスするためのユーザ名およびパスワードを確立します。
ステップ 8	**template config** *url* [**post**] 例： `Router(tti-registrar)# template config http://myserver/cgi-bin/mycgi post`	（任意）Cisco IOS CLI 設定テンプレートのリモート URL を指定します。 *url* 引数は設定ファイルを参照し、デバイス名（$n）を指定してブートストラップ設定を識別できます。CGI サポートにより HTTP または HTTPS のいずれかを使用して CGI スクリプトを参照でき、デバイス名だけでなく、タイプ、Cisco IOS 現行バージョン情報、および現行の設定でブートストラップ設定を識別できます。 CGI サポートでは **post** キーワードを使用する必要があります。 （注） 拡張 CGI サポートを利用するには、レジストラは Cisco IOS リリース 12.4(6)T 以降を実行している必要があります。レジストラがそれ以前のバージョンの Cisco IOS を実行している場合は、追加デバイス ID 情報は無視されます。
ステップ 9	**end** 例： `Router(tti-registrar)# end`	（任意）tti-registrar コンフィギュレーション モードを終了します。

例

SDP トランザクションのトラブルシューティングに役立てるため、**debug crypto provisioning** コマンドを発行できます。このコマンドにより、ペティショナデバイスとレジストラデバイスからの出力が表示されます。

次に、**debug crypto provisioning** コマンドの出力を示します。次に、ペティショナ デバイスとレジストラ デバイスからの出力を示します。

```
Petitioner device
! The user starts the Welcome phase.
```

```
Nov  7 03:15:48.171: CRYPTO_PROVISIONING: received welcome get request.
! The router generates a Rivest, Shamir, and Adelman (RSA) keypair for future enrollment.
Nov  7 03:15:48.279: CRYPTO_PROVISIONING: keyhash 'A506BE3B83C6F4B4A6EFCEB3D584AACA'
! The TTI transaction is completed.
Nov  7 03:16:10.607: CRYPTO_PROVISIONING: received completion post request.
Registrar device
!. During the introduction phase, the browser prompts for login information.
06:39:18: CRYPTO_PROVISIONING: received introduction post request.
06:39:18: CRYPTO_PROVISIONING: checking AAA authentication (ipsecca_script_aaalist,
ttiuser)
! This happens if the user types in the wrong username or password.
06:39:19: CRYPTO_PROVISIONING: authentication declined by AAA, or AAA server not found
- 0x3
06:39:19: CRYPTO_PROVISIONING: aaa query fails!
! The user re-enters login information.
06:39:19: CRYPTO_PROVISIONING: received introduction post request.
06:39:19: CRYPTO_PROVISIONING: checking AAA authentication (ipsecca_script_aaalist,
ttiuser)
06:39:20: CRYPTO_PROVISIONING: checking AAA authorization (ipsecca_script_aaalist,
ttiuser)
! The login attempt succeeds and authorization information is retrieved from the AAA
database.
06:39:21: CRYPTO_PROVISIONING: aaa query ok!
! These attributes are inserted into the configuration template.
06:39:21: CRYPTO_PROVISIONING: building TTI av pairs from AAA attributes
06:39:21: CRYPTO_PROVISIONING: "subjectname" = "CN=user1, O=company, C=US"
06:39:21: CRYPTO_PROVISIONING: "$1" = "ntp server 10.3.0.1"
06:39:21: CRYPTO_PROVISIONING: "$2" = "hostname user1-vpn"
! The registrar stores this subject name and overrides the subject name in the subsequent
 enrollment request.
06:39:21: CRYPTO_PROVISIONING: subjectname=CN=user1, O=company, C=US
! The registrar stores this key information so that it may be used to automatically grant
 the subsequent enrollment request.
06:39:21: CRYPTO_PROVISIONING: key_hash=A506BE3B83C6F4B4A6EFCEB3D584AACA
```

証明書を使用した認可のための SDP レジストラのイネーブル化

SDP レジストラをイネーブルにし、指定されたトラストポイントまたは設定済みのトラストポイントを使用してペティショナ署名証明書を確認し、イントロデューサのユーザ名と証明書名フィールドを使用して認可検索を開始する場合は、この作業を実行します。

始める前に

証明書および特定のトラストポイントに関連付けられた RSA キーを使用するには、SDP ペティショナも設定する必要があります。この作業を完了するには、「SDP ペティショナのイネーブル化（1430 ページ）」の作業の項で示すように、トラストポイント署名コマンドを使用します。

（注） RADIUS では認証と認可の区別がされていないため、証明書の認可にはデフォルトパスワードの cisco を使用する必要があります。

>

手順の概要

1. **enable**
2. **configure terminal**
3. **crypto provisioning registrar**
4. **template file** *sourceURL destinationURL*
5. **binary file** *sourceURL destinationURL*
6. **authentication trustpoint** {**trustpoint-label| use-any }**
7. **authorization {login | certificate | login certificate}**
8. **authorization username subjectname** *subjectname*
9. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**crypto provisioning registrar** 例： `Router(config)# crypto provisioning registrar`	SDP レジストラになるようデバイスを設定し、tti-registrar コンフィギュレーション モードを開始します。
ステップ 4	**template file** *sourceURL destinationURL* 例： `Router(tti-registrar)# template file http://myserver/registrar_file_r1 http://myserver/petitioner_file_p1`	（任意）レジストラの発信元テンプレート ファイル位置とペティショナの宛先テンプレート ファイル位置を指定します。 （注） このコマンドは、USB トークンを使用してデバイスをプロビジョニングする場合に便利です。 テンプレート展開は、レジストラで発信元 URL とファイル コンテンツの両方について行われます。宛先 URL はペティショナで展開されます。
ステップ 5	**binary file** *sourceURL destinationURL* 例： `Router(tti-registrar)# binary file`	（任意）レジストラのバイナリ ファイル位置とペティショナの宛先バイナリ ファイル位置を指定します。

	コマンドまたはアクション	目的
	`http://myserver/registrar_file_a1` `http://myserver/petitioner_file_b1`	（注） このコマンドは、USB トークンを使用してデバイスをプロビジョニングする場合に便利です。 発信元と宛先両方の URL はレジストラで展開されます。また、宛先 URL とファイル コンテンツはペティショナで展開されます。バイナリ ファイルは、テンプレート展開機能では処理されません。
ステップ 6	**authentication trustpoint** {**trustpoint-label| use-any }** 例： `Router(tti-registrar)# authentication trustpoint mytrust`	（任意）SDP ペティショナデバイスの現在の証明書の認証に使用するトラストポイントを指定します。 • *trustpoint-label*：特定のトラストポイントを指定します。 • **use-any**：任意の設定済みトラストポイントを指定します。 （注） トラストポイントを指定するのにこのコマンドを使用しない場合、既存のペティショナ証明書は検証されません（この機能は、自己署名ペティショナ証明書と互換性があります）。
ステップ 7	**authorization {login | certificate | login certificate}** 例： `Router(tti-registrar)# authorization login certificate`	（任意）イントロデューサまたは証明書の AAA 認可をイネーブルにします。 • イントロデューサのユーザー名を使用した認可には、**login** キーワードを使用します。 • ペティショナの証明書を使用した認可には、**certificate** キーワードを使用します。 • イントロデューサのユーザー名およびペティショナの証明書を使用した認可には、**login certificate** キーワードを使用します。
ステップ 8	**authorization username subjectname** *subjectname* 例： `Router(tti-registrar)# authorization username subjectname all`	AAA ユーザー名の構築に使用する異なる証明書フィールドのパラメータを設定します。 • **all** キーワードは、証明書を認可ユーザー名として使用する場合に、所有者名全体を指定します。
ステップ 9	**end** 例：	（任意）tti-registrar コンフィギュレーション モードを終了します。

	コマンドまたはアクション	目的
	`Router(tti-registrar)# end`	

Apple iPhone を導入するための SDP レジストラの設定

会社のネットワークに Apple iPhone を導入するために HTTPS を実行するように SDP レジストラを設定する場合は、この作業を実行します。

始める前に

HTTPS を実行するために SDP レジストラがイネーブルであることを確認します。詳細については、「SDP レジストラのイネーブル化と AAA リストのサーバーへの追加」を参照してください。

手順の概要

1. **enable**
2. **configure terminal**
3. **ip http secure-server**
4. **crypto provisioning registrar**
5. **url-profile start** *profile-name*
6. **url-profile intro** *profile-name*
7. **match url** *url*
8. **match authentication trustpoint** *trustpoint-name*
9. **match certificate** *certificate-map*
10. **mime-type** *mime-type*
11. **template location** *location*
12. **template variable p** *value*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ip http secure-server** 例：	HTTPS Web サーバをイネーブルにします。

	コマンドまたはアクション	目的
	`Router(config)# ip http secure-server`	
ステップ 4	**crypto provisioning registrar** 例： `Router(config)# crypto provisioning registrar`	デバイスを SDP 交換のレジストラになるよう設定し、tti-registrar コンフィギュレーション モードを開始します。 （注） Cisco IOS リリース 12.3(14)T では、**crypto provisioning registrar** コマンドが **crypto wui tti registrar** コマンドに置き換えられました。
ステップ 5	**url-profile start** *profile-name* 例： `Router(tti-registrar)# url-profile start START`	**start** キーワードを指定して、URL プロファイルが SDP 導入開始段階と関連付けられることを示します。*profile-name* 引数には、一意の URL プロファイルの名前を指定します。 （注） SDP 導入紹介段階と SDP 導入開始段階では、いずれも異なるプロファイルを使用したり、同じ URL プロファイルを使用したりすることができます。
ステップ 6	**url-profile intro** *profile-name* 例： `Router(tti-registrar)# url-profile intro INTRO`	**intro** キーワードを指定して、URL プロファイルが SDP 導入紹介段階と関連付けられることを示します。*profile-name* 引数には、一意の URL プロファイルの名前を指定します。 （注） SDP 導入紹介段階と SDP 導入開始段階では、いずれも異なるプロファイルを使用したり、同じ URL プロファイルを使用したりすることができます。
ステップ 7	**match url** *url* 例： `Router(tti-registrar)# match url /sdp/intro`	URL プロファイルに関連付ける URL を指定します。
ステップ 8	**match authentication trustpoint** *trustpoint-name* 例： `Router(tti-registrar)# match authentication trustpoint apple-tp`	（任意）ピアの証明書の認証に使用するトラストポイントの名前を指定します。トラストポイントの名前が指定されていない場合、ピアの証明書の認証には tti-registrar コンフィギュレーション モードで **authentication trustpoint command** を使用して設定されたトラストポイントが使用されます。詳細については、「証明書を使用した認可のための SDP レジストラのイネーブル化」を参照してください。

	コマンドまたはアクション	目的
ステップ 9	**match certificate** *certificate-map* 例： `Router(tti-registrar)# match certificate cat 10`	（任意）ピアの証明書の許可に使用される証明書マップの名前を指定します。
ステップ 10	**mime-type** *mime-type* 例： `Router(tti-registrar)# mime-type application/x-apple-aspen-config`	SDP レジストラが URL プロファイルを通して受信した要求への応答に使用する多目的インターネットメール拡張（MIME）タイプを指定します。
ステップ 11	**template location** *location* 例： `Router(tti-registrar)# template location flash:intro.mobileconfig`	SDP レジストラが URL プロファイルを通して受信した要求に応答するときに使用するテンプレートの場所を指定します。
ステップ 12	**template variable p** *value* 例： `Router(tti-registrar)# template variable p iphone-vpn`	（任意）SDP レジストラによって発行されるトラストポイント証明書の所有者名の組織ユニット（OU）フィールドに入力する値を指定します。以下の「Apple CA サーバーのトラストポイント証明書の設定例」に示されている証明書のこのフィールドを参照してください。

Apple CA サーバーのトラストポイント証明書の設定

SDP レジストラは、Apple CA サーバーの証明書を信頼するために、iPhone のトラストポイント証明書から生成された署名を確認する必要があります。iPhone はトラストポイント証明書を使用してメッセージに署名します。このトラストポイント証明書は、SDP 導入紹介段階で Apple 社の CA サーバーによって発行されます。

次の例では、Apple 社の CA 証明書をカットアンドペーストして手動で登録する方式を使用して、証明書登録を設定する方法を示します。

（注） トラストポイント証明書の設定の詳細については、『Configuring Certificate Enrollment for a PKI』フィーチャモジュールの「How to Configure Certificate Enrollment for a PKI」の項も参照してください。

手順の概要

1. グローバル コンフィギュレーション モードで **crypto pki trustpoint** コマンドを入力してトラストポイントおよび設定された名前を宣言し、CA トラストポイント コンフィギュレーション モードを開始します。

2. カットアンドペーストして手動で証明書を登録するように指定するには、 **enrollment terminal** コマンドを入力します。
3. **crypto pki authenticate** コマンドを使用して、指定された TFTP サーバーから CA 証明書を取得して認証します。
4. Base 64 符号化の信頼できる Apple CA 証明書が含まれている次のテキスト部分をコピーし、プロンプトにペーストします。
5. **exit** コマンドを使用して CA トラストポイント コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードを開始します。
6. グローバル コンフィギュレーション モードで **crypto provisioning registrar** コマンドを入力し、SDP 交換用のレジストラになるルータを指定して、tti-registrar コンフィギュレーション モードを開始します。
7. tti-registrar コンフィギュレーション モードで **url-profile command with the intro** キーワードを入力し、SDP 導入紹介段階に関連付けられる一意の URL プロファイルの名前を指定します。
8. tti-registrar コンフィギュレーション モードで **match authentication trustpoint** コマンドを入力し、ピアの証明書の認証に使用するトラストポイントの名前を指定します。

手順の詳細

ステップ 1 グローバル コンフィギュレーション モードで **crypto pki trustpoint** コマンドを入力してトラストポイントおよび設定された名前を宣言し、CA トラストポイント コンフィギュレーション モードを開始します。

例：

```
Router(config)# crypto pki trustpoint apple-tp
```

ステップ 2 カットアンドペーストして手動で証明書を登録するように指定するには、 **enrollment terminal** コマンドを入力します。

例：

```
Router(ca-trustpoint)# enrollment terminal
```

ステップ 3 **crypto pki authenticate** コマンドを使用して、指定された TFTP サーバーから CA 証明書を取得して認証します。

例：

```
Router(ca-trustpoint)# crypto pki authenticate apple-tp
```

ステップ 4 Base 64 符号化の信頼できる Apple CA 証明書が含まれている次のテキスト部分をコピーし、プロンプトにペーストします。

例：

```
I Bag Attributes
    localKeyID: 7C 29 15 15 12 C9 CF F6 15 2B 5B 25 70 3D A7 9A 98 14 36 06
subject=/C=US/O=Apple Inc./OU=Apple iPhone/CN=Apple iPhone Device CA
issuer=/C=US/O=Apple Inc./OU=Apple Certification Authority/CN=Apple iPhone Certification Authority
```

```
-----BEGIN CERTIFICATE-----
MIIDaTCCAlGgAwIBAgIBATANBgkqhkiG9w0BAQUFADB5MQswCQYDVQQGEwJVUzET
MBEGA1UEChMKQXBwbGUgSW5jLjEmMCQGA1UECxMdQXBwbGUgQ2VydGlmaWNhdGlv
biBBdXRob3JpdHkxLTArBgNVBAMTJEFwcGxlIGlQaG9uZSBDZXJ0aWZpY2F0aW9u
IEF1dGhvcml0eTAeFw0wNzA0MTYyMjU0NDZaFw0xNDA0MTYyMjU0NDZaMFoxCzAJ
BgNVBAYTAlVTMRMwEQYDVQQKEwpBcHBsZSBJbmMuMRUwEwYDVQQLEwxBcHBsZSBp
UGhvbmUxHzAdBgNVBAMTFkFwcGxlIGlQaG9uZSBEZXZpY2UgQ0EwgZ8wDQYJKoZI
hvcNAQEBBQADgY0AMIGJAoGBAPGUSsnquloYYK3Lok1NTlQZaRdZB2bLl+hmmkdf
Rq5nerVKc1SxywT2vTa4DFU4ioSDMVJl+TPhl3ecK0wmsCU/6TKqewh0lOzBSzgd
Z04IUpRai1mjXNeT9KD+VYW7TEaXXm6yd0UvZ1y8Cxi/WblshvcqdXbSGXH0KWO5
JQuvAgMBAAGjgZ4wgZswDgYDVR0PAQH/BAQDAgGGMA8GA1UdEwEB/wQFMAMBAf8w
HQYDVR0OBBYEFLL+ISNEhpVqedWBJo5zENinTI50MB8GA1UdIwQYMBaAFOc0Ki4i
3jlga7SUzneDYS8xoHw1MDgGA1UdHwQxMC8wLaAroCmGJ2h0dHA6Ly93d3cuYXBw
bGUuY29tL2FwcGxlY2EvaXBob25lLmNybDANBgkqhkiG9w0BAQUFAAOCAQEAd13P
Z3pMViukVHe9WUg8Hum+0I/0kHKvjhwVd/IMwGlXyU7DhUYWdja2X/zqj7W24Aq5
7dEKm3fqqxK5XCFVGY5HI0cRsdENyTP7lxSiiTRYj2mlPedheCn+k6T5y0U4Xr40
FXwWb2nWqCF1AgIudhgvVbxlvqcxUm8Zz7yDeJ0JFovXQhyO5fLUHRLCQFssAbf8
B4i8rYYsBUhYTspVJcxVpIIltkYpdIRSIARA49HNvKK4hzjzMS/OhKQpVKw+OCEZ
xptCVeN2pjbdt9uzi175oVo/u6B2ArKAW17u6XEHIdDMOe7cb33peVI6TD15W4MI
pyQPbp8orlXe+tA8JA==
-----END CERTIFICATE-----
```

ステップ 5 **exit** コマンドを使用して CA トラストポイント コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードを開始します。

例：

```
Router(ca-trustpoint)# exit
```

ステップ 6 グローバル コンフィギュレーション モードで **crypto provisioning registrar** コマンドを入力し、SDP 交換用のレジストラになるルータを指定して、tti-registrar コンフィギュレーション モードを開始します。

例：

```
Router(config)# crypto provisioning registrar
```

ステップ 7 tti-registrar コンフィギュレーション モードで **url-profile command with the intro** キーワードを入力し、SDP 導入紹介段階に関連付けられる一意の URL プロファイルの名前を指定します。

例：

```
Router(tti-registrar)# url-profile intro INTRO
```

ステップ 8 tti-registrar コンフィギュレーション モードで **match authentication trustpoint** コマンドを入力し、ピアの証明書の認証に使用するトラストポイントの名前を指定します。

例：

```
Router(tti-registrar)# match authentication trustpoint apple-tp
```

これで、SDP レジストラは iPhone の署名を確認する際に、「apple-tp」という名前の Apple CA トラストポイント証明書を使用できます。

管理イントロデューサの設定

管理者の認証リストと認可リストを使用して、管理イントロデューサを設定するには、次の作業を行います。

始める前に

管理イントロデューサは、クライアントデバイスの特権およびサーバの管理者特権をイネーブルにしておく必要があります。

（注） RADIUS を使用する場合、管理イントロデューサにより紹介される必要があるユーザまたはデバイスのパスワードとして常に cisco を使用する必要があります。TACACS+ にはこの制限はありません。ユーザまたはデバイスはどのパスワードを使用しても、管理イントロデューサにより紹介されます。

>

手順の概要

1. **enable**
2. **configure terminal**
3. **crypto provisioning registrar**
4. **administrator authentication list** *list-name*
5. **administrator authorization list** *list-name*
6. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**crypto provisioning registrar** 例： `Router(config)# crypto provisioning registrar`	SDP レジストラになるようデバイスを設定し、tti-registrar コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 4	**administrator authentication list** *list-name* 例： `Router(tti-registrar)# administrator authentication list authen-tac`	紹介中に管理者を認証場合に使用する AAA リストを設定します。
ステップ 5	**administrator authorization list** *list-name* 例： `Router(tti-registrar)# administrator authorization list author-tac`	紹介中に管理者の認可情報を取得する場合に使用する AAA リストを設定します。取得できる情報として、証明書の題名またはペティショナに返信される Cisco IOS CLI スニペットに展開されるテンプレート型変数のリストがあります。
ステップ 6	**end** 例： `Router(tti-registrar)# end`	（任意）tti-registrar コンフィギュレーション モードを終了します。

例

show running-config コマンドの次の例では、認証リストと認可リストを使用した管理イントロデューサが作成されたことを確認できます。

```
Router# show running-config
Building configuration...
Current configuration : 2700 bytes
!
! Last configuration change at 01:22:26 GMT Fri Feb 4 2005
!
version 12.4
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname router
!
boot-start-marker
boot-end-marker
!
memory-size iomem 5
enable secret 5 $1$tpBS$PXnBDTIDXfX5pWa//1JX20
enable password lab
!
aaa new-model
!
!
!
aaa session-id common
!
resource manager
!
clock timezone GMT 0
```

```
ip subnet-zero
no ip routing
!
!
no ip dhcp use vrf connected
!
!
no ip cef
no ip domain lookup
ip domain name company.com
ip host router 10.3.0.6
ip host router.company.com 10.3.0.6
no ip ips deny-action ips-interface
!
no ftp-server write-enable
!
crypto pki server mycs
!
crypto pki trustpoint mycs
 revocation-check crl
 rsakeypair mycs
!
crypto pki trustpoint tti
 revocation-check crl
 rsakeypair tti
!
crypto pki trustpoint mic
 enrollment url http://router:80
 revocation-check crl
!
crypto pki trustpoint cat
 revocation-check crl
!
!
!
crypto pki certificate map cat 10
!
crypto pki certificate chain mycs
 certificate ca 01
crypto pki certificate chain tti
crypto pki certificate chain mic
 certificate 02
 certificate ca 01
crypto pki certificate chain cat
!
crypto provisioning registrar <---------- !SDP registrar device parameters!
 administrator authentication list authen-tac
 administrator authorization list author-tac
!
no crypto engine onboard 0
username qa privilege 15 password 0 lab
```

カスタム テンプレートの設定

カスタム テンプレートを作成および設定するには、次の作業を行います。

手順の概要

1. **enable**
2. **configure terminal**

3. **crypto provisioning registrar**
4. **template http start** *URL*
5. **template http welcome** *URL*
6. **template http introduction** *URL*
7. **template http admin-introduction** *URL*
8. **template http completion** *URL*
9. **template http error** *URL*
10. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**crypto provisioning registrar** 例： `Router(config)# crypto provisioning registrar`	SDP レジストラになるようデバイスを設定し、tti-registrar コンフィギュレーション モードを開始します。
ステップ 4	**template http start** *URL* 例： `Router(tti-registrar)# template http start tftp://registrar.company.com/start.html`	カスタム開始ページ テンプレートを使用するよう TTI レジストラに指示します。 （注） このコマンドは、開始ページ機能を使用する場合に必要です。このコマンドが発行されていない場合、ようこそページがイントロデューサとペティショナの最初の通信になります。
ステップ 5	**template http welcome** *URL* 例： `Router(tti-registrar)# template http welcome tftp://registrar.company.com/welcome.html`	（任意）デフォルト テンプレートではなく、カスタムようこそテンプレートを使用します。
ステップ 6	**template http introduction** *URL* 例： `Router(tti-registrar)#`	（任意）デフォルト テンプレートではなく、カスタム紹介テンプレートを使用します。

	コマンドまたはアクション	目的
	`template http introduction tftp://registrar.company.com/intro.html`	
ステップ 7	**template http admin-introduction** *URL* 例： `Router(tti-registrar)# template http admin-introduction tftp://registrar.company.com/admin-intro.html`	（任意）デフォルト テンプレートではなく、カスタム管理紹介テンプレートを使用します。
ステップ 8	**template http completion** *URL* 例： `Router(tti-registrar)# template http completion tftp://registrar.company.com/completion.html`	（任意）デフォルト テンプレートではなく、カスタム完了テンプレートを使用します。
ステップ 9	**template http error** *URL* 例： `Router(tti-registrar)# template http error tftp://registrar.company.com/error.html`	（任意）デフォルト テンプレートではなく、カスタム エラー テンプレートを使用します。
ステップ 10	**end** 例： `Router(tti-registrar)# end`	（任意）tti-registrar コンフィギュレーション モードを終了します。

例

次に、開始、紹介、および完了の各テンプレートを使用した例を示します。

template http start tftp://registrar.company.com/start.html

template http introduction tftp://registrar.company.com/intro.html

template http completion tftp://registrar.company.com/completion.html

PKI への登録のための Secure Device Provisioning（SDP）の設定例

SDP レジストラの確認の例

show running-config コマンドの次のサンプル出力では、証明書サーバー「cs1」が設定され、レジストラとペティショナ間の SDP 交換と関連付けられていることが確認できます。

```
Router# show running-config
Building configuration...
Current configuration : 5902 bytes
!
! Last configuration change at 09:34:44 GMT Sat Jan 31 2004
!
version 12.3
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname pki-36a
!
boot-start-marker
boot-end-marker
!
logging buffered 32768 debugging
no logging console
enable secret 5 $1$b3jz$CKquLGjFIE3AdXA2/R19./
enable password lab
!
clock timezone GMT 0
no aaa new-model
ip subnet-zero
!
!
ip cef
ip domain name company.com
ip host msca-root
ip host yni-u10
ip host pki-36a 10.23.2.131
ip host pki-36a.company.com 10.23.2.131
!
!
crypto pki server cs1
 issuer-name CN=company,L=city,C=US
 hash sha1
 lifetime crl 336
 lifetime certificate 730
!
crypto pki trustpoint pki-36a
 enrollment url http://pki-36a:80
 ip-address FastEthernet0/0
 revocation-check none
!
crypto pki trustpoint cs1
 revocation-check crl
 rsakeypair cs1 2048
```

```
!
!
crypto pki certificate chain pki-36a
 certificate 03
  308201D0 30820139 A0030201 02020103 300D0609 2A864886 F70D0101 04050030
  34310B30 09060355 04061302 55533114 30120603 55040713 0B205361 6E746120
  4372757A 310F300D 06035504 03130620 696F7363 73301E17 0D303430 31333130
  39333334 345A170D 30363031 33303039 33333434 5A303A31 38301606 092A8648
  86F70D01 09081309 31302E32 332E322E 32301E06 092A8648 86F70D01 09021611
  706B692D 3336612E 63697363 6F2E636F 6D305C30 0D06092A 864886F7 0D010101
  0500034B 00304802 4100AFFA 8F429618 112FAB9D 01F3352E 59DD3D2D AE67E31D
  370AC4DA 619735DF 9CF4EA13 64E4B563 C239C5F0 1578B773 07BED641 A18CA629
  191884B5 61B66ECF 4D110203 010001A3 30302E30 0B060355 1D0F0404 030205A0
  301F0603 551D2304 18301680 141DA8B1 71652961 3F7D69F0 02903AC3 2BADB137
  C6300D06 092A8648 86F70D01 01040500 03818100 67BAE186 327CED31 D642CB39
  AD585731 95868683 B950DF14 3BCB155A 2B63CFAD B34B579C 79128AD9 296922E9
  4DEDFCAF A7B5A412 AB1FC081 09951CE3 08BFFDD9 9FB1B9DA E9AA42C8 D1049268
  C524E58F 11C6BA7F C750320C 03DFB6D4 CBB3E739 C8C76359 CE939A97 B51B3F7F
  3FF;A9D82 9CFDB6CF E2503A14 36D0A236 A1CCFEAE
  quit
 certificate ca 01
  30820241 308201AA A0030201 02020101 300D0609 2A864886 F70D0101 04050030
  34310B30 09060355 04061302 55533114 30120603 55040713 0B205361 6E746120
  4372757A 310F300D 06035504 03130620 696F7363 73301E17 0D303430 31333130
  39333132 315A170D 30373031 33303039 33313231 5A303431 0B300906 03550406
  13025553 31143012 06035504 07130B20 53616E74 61204372 757A310F 300D0603
  55040313 0620696F 73637330 819F300D 06092A86 4886F70D 01010105 0003818D
  00308189 02818100 FC0695AF 181CE90A 1B34B348 BA957178 680C8B51 07802AC3
  BF77B9C6 CB45092E 3C22292D C7D5FFC1 899185A1 FD8F37D5 C44FC206 6D1FA581
  E2264C83 1CC7453E 548C89C6 F3CD25BC 9BFFE7C5 E6653A06 62133950 78BED51B
  49128428 AB237F80 83A530EA 6F896193 F2134B54 D181F059 348AA84B 21EE6D80
  727BF668 EB004341 02030100 01A36330 61300F06 03551D13 0101FF04 05300301
  01FF300E 0603551D 0F0101FF 04040302 0186301D 0603551D 0E041604 141DA8B1
  71652961 3F7D69F0 02903AC3 2BADB137 C6301F06 03551D23 04183016 80141DA8
  B1716529 613F7D69 F002903A C32BADB1 37C6300D 06092A86 4886F70D 01010405
  00038181 00885895 A0141169 3D754EB2 E6FEC293 5BF0A80B E424AA2F A3F59765
  3463AAD1 55E71F0F B5D1A35B 9EA79DAC DDB40721 1344C01E 015BAB73 1E148E03
  9DD01431 A5E2887B 4AEC8EF4 48ACDB66 A6F9401E 8F7CA588 8A4199BB F8A437A0
  F25064E7 112805D3 074A154F 650D09B9 8FA19347 ED359EAD 4181D9ED 0C667C10
  8A7BCFB0 FB
  quit
crypto pki certificate chain cs1
 certificate ca 01
  30820241 308201AA A0030201 02020101 300D0609 2A864886 F70D0101 04050030
  34310B30 09060355 04061302 55533114 30120603 55040713 0B205361 6E746120
  4372757A 310F300D 06035504 03130620 696F7363 73301E17 0D303430 31333130
  39333132 315A170D 30373031 33303039 33313231 5A303431 0B300906 03550406
  13025553 31143012 06035504 07130B20 53616E74 61204372 757A310F 300D0603
  55040313 0620696F 73637330 819F300D 06092A86 4886F70D 01010105 0003818D
  00308189 02818100 FC0695AF 181CE90A 1B34B348 BA957178 680C8B51 07802AC3
  BF77B9C6 CB45092E 3C22292D C7D5FFC1 899185A1 FD8F37D5 C44FC206 6D1FA581
  E2264C83 1CC7453E 548C89C6 F3CD25BC 9BFFE7C5 E6653A06 62133950 78BED51B
  49128428 AB237F80 83A530EA 6F896193 F2134B54 D181F059 348AA84B 21EE6D80
  727BF668 EB004341 02030100 01A36330 61300F06 03551D13 0101FF04 05300301
  01FF300E 0603551D 0F0101FF 04040302 0186301D 0603551D 0E041604 141DA8B1
  71652961 3F7D69F0 02903AC3 2BADB137 C6301F06 03551D23 04183016 80141DA8
  B1716529 613F7D69 F002903A C32BADB1 37C6300D 06092A86 4886F70D 01010405
  00038181 00885895 A0141169 3D754EB2 E6FEC293 5BF0A80B E424AA2F A3F59765
  3463AAD1 55E71F0F B5D1A35B 9EA79DAC DDB40721 1344C01E 015BAB73 1E148E03
  9DD01431 A5E2887B 4AEC8EF4 48ACDB66 A6F9401E 8F7CA588 8A4199BB F8A437A02;
  F25064E7 112805D3 074A154F 650D09B9 8FA19347 ED359EAD 4181D9ED 0C667C10
  8A7BCFB0 FB
  quit
!
```

```
crypto provisioning registrar
 pki-server cs1
!
!
!
crypto isakmp policy 1
 hash sha
!
!
crypto ipsec transform-set test_transformset esp-aes
!
crypto map test_cryptomap 10 ipsec-isakmp
 set peer 10.23.1.10
 set security-association lifetime seconds 1800
 set transform-set test_transformset
 match address 170
!
!
interface Loopback0
 ip address 10.23.2.131 255.255.255.255
 no ip route-cache cef
 no ip route-cache
 no ip mroute-cache
!
interface FastEthernet0/0
 ip address 10.23.2.2 255.255.255.192
 no ip route-cache cef
 no ip route-cache
 no ip mroute-cache
 duplex auto
 speed auto
 crypto map test_cryptomap
!
interface FastEthernet1/0
 no ip address
 shutdown
 duplex auto
 speed auto
!
ip default-gateway 10.23.2.62
ip http server
no ip http secure-server
ip classless
ip route 0.0.0.0 0.0.0.0 10.23.2.62
!
!
access-list 170 permit ip host 10.23.2.2 host 10.23.1.10
dialer-list 1 protocol ip permit
!
!
control-plane
!
!
line con 0
 exec-timeout 0 0
 speed 115200
line aux 0
line vty 0 4
 password lab
 login
!
!
end
```

SDP ペティショナの確認の例

SDP 交換が完了したら、ペティショナは自動的にレジストラを登録し、証明書を取得します。**show running-config** コマンドによる次のサンプル出力では、トラストポイントが実際に存在することを確認する設定が自動的に生成されているところを示しています。

```
Router# show running-config
Building configuration...
Current configuration : 4650 bytes
!
! Last configuration change at 09:34:53 GMT Sat Jan 31 2004
!
version 12.3
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname pki-36b
!
boot-start-marker
boot-end-marker
!
logging buffered 32768 debugging
no logging console
enable secret 5 $1$JYgw$060JKXgl6dERLZpU9J3gb.
enable password lab
!
clock timezone GMT 0
no aaa new-model
ip subnet-zero
!
!
ip cef
ip domain name company.com
ip host msca-root
ip host yni-u10
ip host pki-36a 10.23.2.131
ip host pki-36a.company.com 10.23.2.131
!
!
crypto pki trustpoint tti
 enrollment url http://pki-36a.company.com:80
 revocation-check crl
 rsakeypair tti 1024
 auto-enroll 70
!
!
crypto pki certificate chain tti
 certificate 02
  308201FC 30820165 A00302012;02020102 300D0609 2A864886 F70D0101 04050030
  34310B30 09060355 04061302 55533114 30120603 55040713 0B205361 6E746120
  4372757A 310F300D 06035504 03130620 696F7363 73301E17 0D303430 31333130
  39333333 385A170D 30363031 33303039 33333338 5A302231 20301E06 092A8648
  86F70D01 09021611 706B692D 3336622E 63697363 6F2E636F 6D30819F 300D0609
  2A864886 F70D0101 01050003 818D0030 81890281 8100E383 35584B6C 24751E2C
  F4088F06 C00BFECE 84CFF8EB 50D52044 03D14A2B 91E5A260 7D07ED24 DB599D27
  432065D9 0E459248 D7CDC15D 654E2AF6 BA27D79C 23850306 3E96C508 F311D333
  76FDDC9C A810F75C FCD10F1B 9A142F0C 338B6DB3 346D3F24 97A4B15D 0A9504E7
  1F6CB769 85E9F52B FE907AAF 63D54D66 1A715A20 D7DB0203 010001A3 30302E30
  0B060355 1D0F0404 030205A0 301F0603 551D2304 18301680 141DA8B1 71652961
  3F7D69F0 02903AC3 2BADB137 C6300D06 092A8648 86F70D01 01040500 03818100
```

```
  C5E2DA0E 4312BCF8 0396014F E18B3EE9 6C970BB7 B8FAFC61 EF849568 D546F73F
  67D2A73C 156202DC 7404A394 D6124DAF 6BACB8CF 96C3141D 109C5B0E 46F4F827
  022474ED 8B59D654 F04E31A2 C9AA1152 75A0C455 FD7EEEF5 A505A648 863EE9E6
  C361D9BD E12BBB36 16B729DF 823AD5CC 404CCE48 A4379CDC 67FF6362 0601B950
  quit
 certificate ca 01
  30820241 308201AA A0030201 02020101 300D0609 2A864886 F70D0101 04050030
  34310B30 09060355 04061302 55533114 30120603 55040713 0B205361 6E746120
  4372757A 310F300D 06035504 03130620 696F7363 73301E17 0D303430 31333130
  39333132 315A170D 30373031 33303039 33313231 5A303431 0B300906 03550406
  13025553 31143012 06035504 07130B20 53616E74 61204372 757A310F 300D0603
  55040313 0620696F 73637330 819F300D 06092A86 4886F70D 01010105 0003818D
  00308189 02818100 FC0695AF 181CE90A 1B34B348 BA957178 680C8B51 07802AC3
  BF77B9C6 CB45092E 3C22292D C7D5FFC1 899185A1 FD8F37D5 C44FC206 6D1FA581
  E2264C83 1CC7453E 548C89C6 F3CD25BC 9BFFE7C5 E6653A06 62133950 78BED51B
  49128428 AB237F80 83A530EA 6F896193 F2134B54 D181F059 348AA84B 21EE6D80
  727BF668 EB004341 02030100 01A36330 61300F06 03551D13 0101FF04 05300301
  01FF300E 0603551D 0F0101FF 04040302 0186301D 0603551D 0E041604 141DA8B1
  71652961 3F7D69F0 02903AC3 2BADB137 C6301F06 03551D23 04183016 80141DA8
  B1716529 613F7D69 F002903A C32BADB1 37C6300D 06092A86 4886F70D 01010405
  00038181 00885895 A0141169 3D754EB2 E6FEC293 5BF0A80B E424AA2F A3F59765
  3463AAD1 55E71F0F B5D1A35B 9EA79DAC DDB40721 1344C01E 015BAB73 1E148E03
  9DD01431 A5E2887B 4AEC8EF4 48ACDB66 A6F9401E 8F7CA588 8A4199BB F8A437A0
  F25064E7 112805D3 074A154F 650D09B9 8FA19347 ED359EAD 4181D9ED 0C667C10
  8A7BCFB0 FB
  quit
!
no crypto engine accelerator
!
!
crypto isakmp policy 1
 hash sha
!
!
crypto ipsec transform-set test_transformset esp-aes
!
crypto map test_cryptomap 10 ipsec-isakmp
 set peer 10.23.2.2
 set security-association lifetime seconds 1800
 set transform-set test_transformset
 match address 170
!
!
interface Ethernet0/0
 ip address 10.23.1.10 255.255.255.192
 no ip route-cache cef
 no ip route-cache
 no ip mroute-cache
 half-duplex
 crypto map test_cryptomap
!
interface Ethernet0/1
 no ip address
 shutdown
 half-duplex
!
interface Ethernet0/2
 no ip address
 shutdown
 half-duplex
!
interface Ethernet0/3
 no ip address
 shutdown
```

```
 half-duplex
!
interface Serial1/0
 no ip address
 shutdown
 serial restart-delay 0
!
interface Serial1/1
 no ip address
 shutdown
 serial restart-delay 0
!
interface Serial1/2
 no ip address
 shutdown
 serial restart-delay 0
!
interface Serial1/3
 no ip address
 shutdown
 serial restart-delay 0
!
ip default-gateway 10.23.1.62
ip http server
no ip http secure-server
ip classless
ip route 0.0.0.0 0.0.0.0 10.23.1.62
!
!
access-list 170 permit ip host 10.23.1.10 host 10.23.2.2
dialer-list 1 protocol ip permit
!
!
control-plane
!
!
line con 0
 exec-timeout 0 0
 speed 115200
line aux 0
line vty 0 4
 password lab
 login
!
!
end
```

AAA リストの RADIUS または TACACS+ サーバーへの追加の例

ここでは、次の設定例を示します。

TACACS+ AAA サーバーデータベースの例

次に、ユーザ情報が TACACS+ AAA データベースに追加されている例を示します。ユーザー名は「user1」です。パスワードは「cisco」です。「user1」には、iosconfig1 と iosconfig2 の 2 つの Cisco IOS 設定テンプレート変数が設定されています。変数は設定テンプレート ファイルで $1 および $2 を置き換えます。題名「CN=user1, O=company, C=US」も設定されます。この題名は、ペティショナ デバイスから受信される以降の登録要求（PKCS10）で題名フィールドを置き換えます。

```
user = user1
    password = clear "pswd"
    service=tti
        ! The certificate server inserts the following subject name to the certificate.
        set subjectname="CN=user1, O=company, C=US"
        ! Up to nine template variables may be added.
        set iosconfig1="ntp server 10.3.0.1"
        set iosconfig2="hostname user1-vpn"
```

RADIUS AAA サーバーデータベースの例

次に、ユーザ情報が RADIUS AAA サーバ データベースに追加された例を示します。ユーザー名は「user1」です。パスワードは「cisco」です。「user1」には、iosconfig1 と iosconfig2 の 2 つの Cisco IOS 設定テンプレート変数が設定されています。変数は設定テンプレート ファイルで $1 および $2 を置き換えます。題名「CN=user1, O=company, C=US」も設定されます。この題名は、ペティショナ デバイスから受信される以降の登録要求（PKCS10）で題名フィールドを置き換えます。

```
user = user1
    password = clear "pswd"
    radius=company
    reply_attributes=9,1="tti:subjectname=CN=user1, O=company, C=US"
    ! Up to nine template variables may be added.
    9,1="tti:iosconfig1=ntp server 10.3.0.5"
    9,1="tti:iosconfig2=hostname user1-vpn"
```

TACACS+ および RADIUS AAA サーバー上の AAA リストの例

次の設定例は、TACACS+ サーバで AAA 認証が、RADIUS サーバで AAA 認可が設定されていることを示しています。

（注） 通常、認証と認可は同じサーバをポイントします。

```
Router(config)# tacacs-server host 10.0.0.48 key cisco
Router(config)# aaa authentication login authen-tac group tacacs+
Router(config)# radius-server host 10.0.1.49 key cisco
Router(config)# aaa authorization network author-rad group radius
```

UsingaConfigurationTemplateFile の例

イントロデューサ名に基づいて、異なる設定テンプレート ファイルを使用できます。たとえば、異なるユーザに対する複数のテンプレートがある場合、各ファイルのファイル名にユーザ名を含め、レジストラで次のように設定します。

```
Router(config)# crypto provisioning registrar
Router (tti-registrar)# pki-server cs1
Router (tti-registrar)# template config tftp://server/config-$n.txt
```

この例では、設定ファイルのデフォルトテンプレート（1424ページ）に示されているデフォルト設定ファイルが使用されます。**template config** コマンドはCGIスクリプトを参照しないためです。

CGI スクリプトの例

次に、「mysdpcgi」というCGIスクリプトが実行される例を示します。

```
Router(config)# crypto provisioning registrar
Router (tti-registrar)# pki-server cs1
Router (tti-registrar)# template config tftp://server/cgi-bin/mysdpcgi post
```

次に、「mysdpcgi」というCGIスクリプトが上記の例の **template config** コマンドで実行される例を示します。

```
#!/usr/bin/perl -w
# for debugging use the -debug form
# use CGI (-debug);
use CGI;
# base64 decoding is being used.
use MIME::Base64;
# The following has been commented out, but left for your information.
#
# Reading everything that has been received from stdin and writing it to the debug log
to #see what has been sent from the registrar.
#
# Remember to reset the STDIN pointer so that the normal CGI processing can get the
input.
#
# print STDERR "mysdpcgi.cgi dump of stdin:\n";
# if($ENV{'REQUEST_METHOD'} eq "GET"){
#    $input_data = $ENV{'QUERY_STRING'};
# }
# else {
#    $data_length = $ENV{'CONTENT_LENGTH'};
#    $bytes_read = read(STDIN, $input_data, $data_length);
# }
# print STDERR $input_data,"\n";
# exit;

$query = new CGI;
my %av_table;
# A basic configuration file is being sent back, therefore it is being indicated as plain
 # text in the command below.
print $query->header ("text/plain");
print "\n";
# For testing, parameters can be passed in so that the test applications can
# see what has been received.
#
# print STDERR "The following are the raw AV pairs mysdpcgi.cgi received:\n";
# for each $key ($query->param) {
#    print STDERR "! $key is: \n";
#    $value = $query->param($key);
#    print STDERR "! ",$value;
#    print STDERR "! \n";
#}
# The post process AV pairs are identical to those in Cisco IOS and may be used to produce
 # AV pair specific configurations as needed.
%av_table = &postprocessavpairs($query->param);
```

```
# Decoded values may be written out.
# WARNING: Some error_logs cannot handle the amount of data and will freeze.
# print STDERR "The following are the decoded AV pairs mysdpcgi.cgi received:\n";
# now write the values out
# while ( ($a, $v) = each(%av_table) ) {
#    print STDERR "$a = $v\n";
# }
# Identifying the AV pairs and specifying them in the config.
while ( ($a, $v) = each(%av_table) ) {
    if ($a eq "TTIIosRunningConfig") {
        $search = "hostname ";
        $begin = index($v, $search) + length($search);
        $end = index($v, "\n", $begin);
        $hostname = substr($v, $begin, $end - $begin);
    }
    if ($a eq "TTIIosVersion") {
        $search = "Version ";
        $begin = index($v, $search) + length($search);
        $end = index($v, "(", $begin);
        $version = substr($v, $begin, $end - $begin);
    }
}
print <<END_CONFIG;
!
! Config auto-generated by sdp.cgi
! This is for SDP testing only and is not a real config
!
!
\$t
!
\$c
!
cry pki trust Version-$version-$hostname
! NOTE: The last line of the config must be 'end' with a blank line after the end
# statement.
END_CONFIG
;
# Emulate IOS tti_postprocessavpairs functionality
sub postprocessavpairs {
    @attributes = @_;
    # Combine any AV pairs that were split apart
    $n = 0; #element index counter
    while ($attributes[$n]) {
 # see if we are at the start of a set
 if ($attributes[$n] =~ m/_0/) {
     # determine base attribute name
     $a = (split /_0/, $attributes[$n])[0];
     # set initial (partial) value
     $v = $query->param($attributes[$n]);

     # loop and pull the rest of the matching
     # attributes's values into v (would be
     # faster if we stop at first non-match)
     $c = $n+1;
     while ($attributes[$c]) {
  if ($attributes[$c] =~ m/$a/) {
      $v = $v.$query->param($attributes[$c]);
  }
  $c++;
     }

     # store in the av hash table
     $av_table{$a} = $v;
 } else {
```

```
    # store in hash table if not part of a set
    if ($attributes[$n] !~ m/_\d/) {
 $av_table{$attributes[$n]} = $query->param($attributes[$n]);
    }
}
$n++;
   }
   # de-base64 decode all AV pairs except userdevicename
   while ( ($a, $v) = each(%av_table) ) {
       if ($a ne "userdevicename") {
           $av_table{$a} = decode_base64($av_table{$a});
       }
   }
   return %av_table;
}
```

（注） CGI スクリプトは、Cisco IOS Release 12.4(6)T 以降では、**template config** コマンド に **post** キーワードを指定せずに実行することはできません。

証明書を使用した認証のペティショナとレジストラの設定の例

次に、mytrust というトラストポイントで発行された証明書を使用する場合のペティショナの設定方法の例を示します。

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# crypto provisioning petitioner

Router(tti-petitioner)# trustpoint signing mytrust

Router(tti-petitioner)# end
```

次に、ペティショナ署名証明書を確認し、認可検索を行う場合のレジストラの設定方法の例を示します。

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# crypto provisioning registrar

Router(tti-registrar)# authentication trustpoint mytrust

Router(tti-registrar)# authorization login certificate

Router(tti-registrar)# authorization username subjectname all

Router(tti-registrar)# end
```

認証リストおよび認可リストを使用した管理イントロデューサの設定例

次に、認証リスト「authen-tac」および認可リスト「author-tac」を使用した管理イントロデューサの設定方法の例を示します。

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# crypto provisioning registrar
Router(tti-registrar)# administrator
 authentication list authen-tac
Router(tti-registrar)# administrator
 authorization list author-tac
Router(tti-registrar)# end
```

その他の参考資料

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『Cisco IOS Master Commands List, All Releases』
証明書登録	「 PKI の証明書登録の設定 」 モジュール
証明書サーバ設定	「PKI 展開での Cisco IOS 証明書サーバの設定および管理」モジュール
PKI AAA 統合の概念と設定作業	「PKI での証明書の失効および許可の設定」モジュール
PKI コマンド：完全なコマンドの構文、コマンドモード、デフォルト、使用上の注意事項、例	『*Cisco IOS Security Command Reference*』
USB トークンの設定	『*Cisco IOS Security Configuration Guide: Secure Connectivity*』の「Storing PKI Credentials」の章 SDP および USB トークンを使用した PKI クレデンシャルの導入に関するその他の 12.4T 機能については、機能情報表を参照してください。
iPhone、iPod touch、および iPad と会社のシステムとの統合	『*Apple iPhone Enterprise Deployment Guide*』
推奨される暗号化アルゴリズム	『*Next Generation Encryption*』

MIB

MIB	MIB のリンク
なし。	選択したプラットフォーム、Cisco ソフトウェア リリース、およびフィーチャ セットの MIB を検索してダウンロードする場合は、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

シスコのテクニカル サポート

説明	リンク
右の URL にアクセスして、シスコのテクニカル サポートを最大限に活用してください。これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

PKI への登録のための Secure Device Provisioning（SDP）の設定に関する機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *152 : PKI* での *SDP* の機能情報

機能名	リリース	機能情報
Secure Device Provisioning（SDP）接続テンプレート	12.4(20)T	この機能により、サービス プロバイダーを通してインターネット接続が行われるようにデバイスを設定できます。

機能名	リリース	機能情報
USB トークンと Secure Device Provisioning（SDP）の連携機能	12.4(15)T	この機能により、SDP を介して特定のネットワーク デバイスからリモート デバイスにクレデンシャルを転送するメカニズムとして USB トークンを使用することで、リモート デバイスをプロビジョニングできるようになります。 次のコマンドが導入されました。**binary file**、**crypto key move rsa**、**template file**。
SDP 拡張テンプレートの CGI サポート	12.4(6)T	この機能によりユーザーは、デバイス名だけでなく、その Cisco IOS の現行バージョンおよび現行の設定に基づいてブートストラップ設定を SDP ペティショナに送信するよう SDP レジストラを設定できます。 次のコマンドが、この機能によって変更されました。**template config.**
Secure Device Provisioning（SDP）開始ページ	12.4(4)T	この機能によりユーザーは、開始ページからレジストラの紹介 URL に連絡することで TTI トランザクションを開始するよう、ブラウザを設定できます。したがって、ユーザはペティショナのようこそページから TTI トランザクションを開始する必要はなくなります。 この機能により、次のコマンドが導入されました。**template http admin-introduction**、**template http completion**、**template http error**、**template http introduction**、**template http start**、**template http welcome.**
Administrative Secure Device Provisioning Introducer	12.3(14)T	この機能により、デバイスを PKI ネットワークに紹介し、AAA データベースのレコード ロケータのデバイス名としてユーザ名を提供する場合に、管理イントロデューサの役割を果たすことができます。 この機能により、次のコマンドが導入されました。**administrator authentication list**、**administrator authorization list.**
Easy Secure Device Deployment	12.3(8)T	この機能は、SDP をサポートできるようにします。SDP は、ネットワーク管理者が大規模ネットワークで新しいデバイスを展開できるようにする Web ベースの登録インターフェイスを実現します。 次のコマンドが導入または変更されました。**crypto wui tti petitioner**、**crypto wui tti registrar**、**pki-server**、**template config**、 **template username**、**trustpoint (tti-petitioner).**

機能名	リリース	機能情報
Easy Secure Device Deployment AAA Integration	12.3(8)T	この機能により外部 AAA データベースが統合され、ローカルなシスコ証明書サーバのイネーブル パスワードを使用しなくても、SDP イントロデューサが AAA データベースに対して認証できるようにします。 次のコマンドが導入または変更されました。**authentication list (tti-registrar)**、**authorization list (tti-registrar)**、**debug crypto wui template config**、 **template username**。
Secure Device Provisioning（SDP）証明書を使用した認可	12.3(14)T	この機能により、その他の認証局（CA）サーバで発行された証明書が SDP 導入に使用できるようになります。 この機能により、次のコマンドが導入されました。**administrator authentication list**、**administrator authorization list**
iPhone の SDP	15.1(2)T	Cisco IOS 15.1(2)T および Apple iPhone OS 3.0 リリースが導入されたため、Cisco IOS ネットワーク デバイスで Apple iPhone がサポートされるようになりました。Cisco IOS ルータは SDP レジストラを使用して iPhone を導入し、IPSec VPN、SCEP サーバ、および PKI 証明書の導入テクノロジーを使用してネットワーク アプリケーションに安全にアクセスできるようにします。 この機能により、次のコマンドが導入されました。**match authentication trustpoint, match certificate** 、 **match url, mime-type**、**template location, template variable p, url-profile.**

第 113 章

PKI クレデンシャル失効アラート

PKI クレデンシャル失効アラート機能を使用すると、CA 証明書が失効間近になるとアラート通知の形式で警告メカニズムが提供されます。

PKI クレデンシャル失効アラートの制約事項

アラートは、次の証明書には送信されません。

- 永続的または一時的な自己署名証明書。
- セキュアな固有デバイス識別子（SUDI）証明書。
- トラストプールに属する証明書。トラストプールには独自の失効アラートメカニズムがあります。
- トラストポイントのクローン。

PKI アラート通知の情報

アラート通知の概要

Cisco IOS 認証局（CA）サーバを使用すると、証明書が失効する前に証明書の自動登録が可能になり、認証中にアプリケーションの証明書が利用できるようになります。ただし、ネットワーク停止、クロック更新の問題、および CA の過負荷が証明書の更新に影響を与え、認証に有効な証明書が使用できなくなることでサブシステムがオフラインになります。PKI クレデンシャル失効アラート機能は、証明書の失効が近付くと、CA クライアントが syslog サーバに通知を送信するためのメカニズムを提供します。

通知は次の間隔で送信されます。

- 最初の通知：これは証明書が失効する 60 日前に送信されます。
- 通知の繰り返し：最初の通知の後、証明書が失効する 1 週間前まで後続の通知が毎週送信されます。最後の週には、証明書の失効日まで通知が毎日送信されます。

証明書の有効期限が 1 週間以上ある場合、通知は [warning] モードで送信されます。証明書の有効期限が 1 週間未満の場合、通知は [alert] モードで送信されます。通知には次の情報が含まれます。

- 証明書が関連付けられたトラストポイント
- 証明書タイプ
- 証明書のシリアル番号
- 証明書の発行元名
- 証明書が失効するまでの残り日数
- 証明書の自動登録が有効かどうか
- 対応する証明書のシャドウ証明書が利用可能かどうか

（注） アラート通知は syslog サーバまたは Simple Network Management Protocol（SNMP）トラップを介して送信されます。トラストポイントの自動登録が設定され、対応するシャドウまたはロールオーバー証明書が有効である場合、およびシャドウまたはロールオーバー証明書の開始時刻が証明書の終了時刻と同じまたはそれ以前の場合、通知は停止します。

この機能は無効にできず、設定作業を追加する必要はありません。**show crypto pki timers** コマンドはタイマーの有効期限情報を表示できるようになりました。次に、証明書の失効間近にタイマーを表示する **show crypto pki timers detail** コマンドの出力例を示します。このタイマーが失効すると、通知が syslog サーバに送信されます。

```
Device# show crypto pki timers detail

PKI Timers
|       14:36.150  (2019-10-30T11:33:30Z)
  |       14:36.150  (2019-10-30T11:33:30Z) SESSION CLEANUP
  |2569d23:56:19.461  (2026-11-12T11:15:13Z) SHADOW test

Expiry Alert Timers
|659d 5:56:19.599  (2021-08-19T17:15:13Z)
  |659d 5:56:19.599  (2021-08-19T17:15:13Z) ID(test)
  |2875d 4:45:18.562  (2027-09-13T16:04:12Z) CA(test)

Trustpool Timers
|3464d 9:06:48.463  (2029-04-24T20:25:42Z)
  |3464d 9:06:48.463  (2029-04-24T20:25:42Z) TRUSTPOOL
```

次に、デバイスに表示される syslog メッセージを示します。

```
Device#

Dec 16 10:24:13.533: %PKI-4-CERT_EXPIRY_WARNING: ID Certificate belonging to trustpoint
 tp will expire in 60 Days 0 hours 0 mins 0 secs.
Issuer-name cn=CA
Subject-name hostname=Router
Serial-number 02
Auto-Renewal: Not Enabled
```

PKI トラップ

PKI トラップでは、ネットワーク内のデバイスの証明書情報を取得するため、PKI 展開の監視と運用が簡単になります。ルート デバイスは、デバイスに設定されたしきい値に基づいて、ネットワーク管理システム（NMS）に SNMP トラップを定期的に送信します。トラップは次のシナリオで送信されます。

- 新しい証明書がインストールされる場合。SNMP トラップ（新しい証明書通知）は、証明書のシリアル番号、証明書の発行者名、証明書の所有者名、トラストポイント名、証明書タイプ、証明書の開始日と終了日などの情報を含む SNMP サーバーに送信されます。
- 証明書が失効間近の場合。SNMP トラップ（証明書失効通知）は、証明書の終了日の 60 日から 1 週間前まで SNMP サーバに定期的に送信されます。証明書が失効する週には、トラップが毎日送信されます。トラップには、証明書のシリアル番号、証明書の発行者名、トラストポイント名、証明書タイプ、証明書の寿命などの証明書情報が含まれます。

PKI トラップを有効にするには、**snmp-server enable traps pki** コマンドを使用します。

（注） シャドウまたはロールオーバー証明書の開始時間が証明書の終了時間よりも遅い場合、シャドウ証明書が有効でないことを示すトラップが送信されます。ただし、同じトラストポイントで利用可能なシャドウ証明書とシャドウ証明書が有効な場合には、トラップは送信されません。

PKI クレデンシャル失効アラートの追加資料

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『Cisco IOS Master Command List, All Releases』

関連項目	マニュアル タイトル
セキュリティ コマンド	• 『Cisco IOS Security Command Reference Commands A to C』 • 『Cisco IOS Security Command Reference Commands D to L』 • 『Cisco IOS Security Command Reference Commands M to R』 • 『Cisco IOS Security Command Reference Commands S to Z』

シスコのテクニカル サポート

説明	リンク
右の URL にアクセスして、シスコのテクニカル サポートを最大限に活用してください。これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

Cisco TrustSec の概要の機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *153 : Cisco TrustSec* の概要の機能情報

機能名	リリース	機能情報
IPv6 の有効化 - インライン タギング	Cisco IOS XE Fuji 16.8.1	IPv6 のサポートが導入されました。

第 114 章

PKI展開での証明書サーバの設定および管理

この章では、Cisco IOS 証明書サーバを設定および管理して、公開キー インフラストラクチャ（PKI）を展開する方法を説明します。証明書サーバは、Cisco ソフトウェアに簡単な証明書サーバを組み込んでいますが、認証局（CA）機能は限定されています。したがって、ユーザには次のようなメリットがあります。

- デフォルト動作の定義による、PKI 展開の簡素化。デフォルト動作が事前に定義されているので、ユーザ インターフェイスが簡素化されています。つまり、CA が提供する証明書の拡張子をすべて使用しなくても PKI のスケーリングのメリットを活用できます。これにより、基本的な PKI で保護されたネットワークを簡単にイネーブルにできます。
- Cisco ソフトウェアとの直接統合。

（注） セキュリティに対する脅威は、脅威からの保護に役立つ暗号化技術と同様に絶え間なく変化しています。最新のシスコの暗号化に関する推奨事項については、『*Next Generation Encryption*』（NGE）ホワイト ペーパーを参照してください。

コピー中に、running-config に CA 証明書と ID 証明書の両方が含まれている場合、CA 証明書が running-config と同じであれば、CA と ID は置き換えられません。一方、CA 証明書が異なる場合は、ID 証明書と CA 証明書の両方がクリアされ、新しい CA が再挿入されます。

証明書サーバの設定に関する前提条件

証明書サーバ設定前の PKI の計画

証明書サーバを設定する前に、PKI 内で使用する設定に対して適切な値（証明書のライフタイムおよび証明書失効リスト（CRL）ライフタイムなど）を考えて、選択することが重要です。証明書サーバに設定値が設定され、証明書が許可されたら、証明書サーバを再設定し、ピアを再登録することで、設定を変更できます。証明書サーバのデフォルト設定と推奨設定に関する詳細については、「証明書サーバのデフォルト値および推奨値」の項を参照してください。

HTTP サーバのイネーブル化

証明書サーバは、HTTP 上で Simple Certificate Enrollment Protocol（SCEP）をサポートします。証明書サーバが SCEP を使用するには、ルータで HTTP サーバをイネーブルにする必要があります（HTTP サーバーをイネーブルにするには、**ip http server** コマンドを使用します）。HTTP サーバのイネーブルとディセーブルを切り替えると、証明書サーバは SCEP サービスのイネーブルとディセーブルを自動的に切り替えます。HTTP サーバがイネーブルでない場合は、手動の PKCS10 登録だけがサポートされます。

（注） 証明書サーバのすべてのタイプで自動 CA 証明書およびキーペアのロールオーバー機能を利用するには、SCEP を登録方式として使用する必要があります。

信頼性の高い時刻サービスの設定

証明書サーバは信頼できる時刻を認識する必要があるので、時刻サービスをルータで実行する必要があります。ハードウェア クロックを利用できない場合、証明書サーバはネットワーク タイムプロトコル（NTP）などの、手動で設定したクロック設定に依存します。ハードウェア クロックがない、あるいはクロックが無効な場合、起動時に次のメッセージが表示されます。

```
% Time has not been set. Cannot start the Certificate server.
```

クロックが設定されると、証明書サーバは実行ステータスに自動的に切り替わります。

クロック設定を手動で設定する方法については、を参照してください。

証明書サーバの設定に関する制約事項

- 証明書サーバは、クライアントから受信した証明書要求を変更するメカニズムを備えていません。つまり、証明書サーバから発行される証明書は変更されていないため、その要求された証明書と一致します。名前制約などの固有の証明書ポリシーを発行する必要がある場合は、このポリシーを証明書要求に反映する必要があります。
-

- サードパーティの OpenSSL を使用して HTTP 接続を検証するために、完全な ISE 証明書チェーンがデバイスに送信されます。これらの証明書には、ISE 証明書とその発行元 CA 証明書が含まれます。環境データには、これらの証明書がリストされます。

  バージョン 2.7.0.310 以前を実行している Cisco ISE は、環境データの一部として着信証明書リストに証明書チェーンを入れます。Cisco IOS XE リリース 17.1.1 以前のリリースでは、Ciscoルータは、ISEからのマルチチェーン証明書のダウンロードをサポートしていません。そのため、デバイスは、ISE 証明書を受信せず、TLS ハンドシェイクエラーが表示されます。

証明書サーバの情報

証明書サーバの RSA キー ペアと証明書

証明書サーバは、1024 ビット Rivest、Shamir、Adelman（RSA）キー ペアを自動的に生成します。異なるキー ペア モジュラスが必要な場合は、手動で RSA キー ペアを生成する必要があります。この作業の完了に関する詳細については、「証明書サーバーの *RSA* キーペアの生成」を参照してください。

（注） 証明書サーバの RSA キー ペアで推奨されるモジュラスは、2048 ビットです。

証明書サーバは、CA キーとして通常の RSA キー ペアを使用します。このキー ペアには、証明書サーバと同じ名前を付ける必要があります。証明書サーバがルータ上に作成される前にキー ペアを生成していない場合、証明書サーバの設定時に、汎用目的キー ペアが自動的に生成されます。

CA 証明書および CA キーが証明書サーバによって一度生成されると、これらを自動的にバックアップできます。その結果、バックアップ目的のエクスポート可能な CA キーを生成する必要はなくなりました。

自動生成キー ペアの処理方法

キーペアが自動的に生成されると、キーペアにエクスポート可能のマークは付けられません。そのため、CA キーをバックアップする場合は、キー ペアをエクスポート可能なものとして手動で生成する必要があります。この作業の完了方法については、「証明書サーバーの *RSA* キーペアの生成」を参照してください。

CA 証明書および CA キーを自動的にアーカイブする方法

CA 証明書および CA キーの原本または元の設定が失われた場合に CA 証明書および CA キーを後で復元できるように、初期の証明書サーバ設定時に、CA証明書およびCAキーの自動アーカイブをイネーブルにできます。

CA 証明書および CA キーは、証明書サーバを初めて起動したときに生成されます。また、自動アーカイブがイネーブルになっている場合、CA 証明書と CA キーはサーバ データベースにエクスポート（アーカイブ）されます。アーカイブは、PKCS12 形式またはプライバシーエンハンスト メール（PEM）形式で実行できます。

（注） このCAキーのバックアップファイルは非常に重要なので、すぐに別の安全な場所に移動する必要があります。

- このアーカイブ処理は、1回しか実行されません。（1）手動で生成され、エクスポート可能のマークが付けられた CA キー、または（2）証明書サーバによって自動的に生成された CA キーだけがアーカイブされます（このキーには、エクスポート不可能のマークが付けられます）。
- 手動で CA キーを生成し、そのキーに「エクスポート不可能」のマークが付いている場合、自動アーカイブは実行されません。
- CA 証明書および CA キー アーカイブ ファイル以外にも、シリアル番号ファイル（.ser）および CRL ファイル（.crl）を定期的にバックアップする必要があります。証明書サーバを復元する必要がある場合、CA 運用においてシリアル ファイルおよび CRL ファイルは重要です。
- エクスポート不可能な RSA キーまたは手動で生成されたエクスポート不可能な RSA キーを使用するサーバを手動でバックアップできません。自動的に生成されたRSAキーには、エクスポート不可能のマークが付いていますが、このキーは一度だけ自動的にアーカイブされます。

証明書サーバ データベース

証明書サーバは専用のファイルを保管し、他のプロセスに使用するファイルを公開できます。証明書サーバによって生成された、進行中の操作に必要な重要ファイルは、専用のファイルタイプごとに1つの場所に保管されます。証明書サーバはこれらのファイルに対して読み取りおよび書き込みを行います。重要な証明書サーバ ファイルは、シリアル番号ファイル（.ser）と CRL 保管場所ファイル（.crl）です。証明書サーバによって書き込みが行われても再度読み取りが行われないファイルは場合によって公開され、他のプロセスで使用できます。公開可能なファイルの例には、発行済みの証明書ファイル（.crt）があります。

証明書サーバのパフォーマンスは、次の要因から影響を受ける場合があります。証明書サーバファイルに対して、保管オプションおよび公開オプションを選択するときには、これらの要因を考慮する必要があります。

- 選択する保管場所または公開場所が証明書サーバのパフォーマンスに影響を与えることがあります。ネットワーク ロケーションから読み取ると、ルータのローカル ストレージ デバイスから直接読み取るよりも時間がかかります。

- 特定の場所では、保管または公開するファイルの数によって証明書サーバのパフォーマンスが影響を受けることがあります。ローカルのファイルシステムは、必ずしも大量のファイルに適していません。
- 保管または公開するファイルタイプが証明書サーバのパフォーマンスに影響を与えることがあります。特定のファイル（.crlファイルなど）は非常に大きくなる可能性があります。

（注） ローカルの ファイル システムに .ser および .crl ファイルを保管し、リモート ファイル システムに.crt ファイルを公開することを推奨します。

証明書サーバ データベース ファイルの保管

証明書サーバーは、その柔軟性により、設定されたデータベースレベルに応じて、さまざまな種類の重要なファイルをさまざまな保管場所に保管できます（詳細については、**database level** コマンドを参照してください）。保管場所を選択するときは、必要なファイルセキュリティおよびサーバのパフォーマンスを考慮してください。たとえば、シリアル番号ファイルおよびアーカイブ ファイル（.p12 または .pem）では、発行された証明書ファイル（.crt）の保管場所または名前ファイル（.cnm）の保管場所よりもセキュリティ上の制約事項が多くなることがあります。

次の表に、特定の場所に保管される重要な証明書サーバファイルのタイプをファイル拡張子別に示します。

表 *154*：証明書サーバの保管場所と重要なファイル タイプ

ファイル拡張子	ファイル タイプ
.ser	メイン証明書サーバのデータベース ファイル
.crl	CRL の保管場所
.crt	発行された証明書の保管場所
.cnm	証明書名および失効ファイルの保管場所
.p12	PKCS12 形式の証明書サーバ証明書アーカイブ ファイルの保管場所
.pem	PEM 形式の証明書サーバ証明書アーカイブ ファイルの保管場所

証明書サーバ ファイルには、次の 3 つのレベルで保管場所を指定できます。

- デフォルトの場所（NVRAM）
- すべての重要ファイルに対して指定されたプライマリ保管場所
- 特定の重要ファイルに対して指定された保管場所

ファイルは、一般的な保管場所よりも、具体的に設定した保管場所に優先的に保管されます。たとえば、証明書サーバ ファイルの保管場所を指定しなかった場合、すべての証明書サーバ ファイルがNVRAMに保管されます。名前ファイルの保管場所を指定すると、名前ファイルだけがそこに保管され、その他すべてのファイルはNVRAMに保管されます。プライマリ ロケーションを指定すると、名前ファイル以外のすべてのファイルが、NVRAMの代わりに、この場所に保管されます。

（注） .p12 または .pem のいずれかを指定できますが、両方のタイプのアーカイブ ファイルは一度に指定できません。

証明書サーバ データベース ファイルの公開

公開ファイルは元のファイルのコピーで、他のプロセスまたはユーザ用に使用できます。証明書サーバがファイルの公開に失敗すると、サーバはシャットダウンします。発行された証明書ファイルおよび名前ファイルに1つの公開場所を、CRLファイルに複数の公開場所を指定できます。公開可能なファイル タイプについては、次の表を参照してください。設定されたデータベース レベルに関係なく、ファイルを公開できます。

表 *155 :* 証明書サーバの公開ファイル タイプ

ファイル拡張子	ファイル タイプ
.crl	CRL の公開場所
.crt	発行された証明書の公開場所
.cnm	証明書名および失効ファイルの公開場所

証明書サーバのトラストポイント

自動的に生成された同じ名前のトラストポイントも証明書サーバにある場合、そのトラストポイントが証明書サーバの証明書を保管します。証明書サーバの証明書を保管するためにトラストポイントが使用されていることを、ルータが検出すると、トラストポイントはロックされ変更できなくなります。

証明書サーバを設定する前に、次の操作を行います。

- このトラストポイントを手動で作成し、設定します（**crypto pki trustpoint** コマンドを使用）。これにより、代替 RSA キーペアを指定できます（ **rsakeypair** コマンドを使用）。
- **on** コマンドを使用して、設定済みの利用可能な USB トークンなどの特定のデバイス上に初期の自動登録キーペアが生成されるように指定します。

（注） 自動的に生成されたトラストポイントおよび証明書サーバ証明書は、証明書サーバデバイスのアイデンティティには使用できません。したがって、CA トラストポイントを指定して証明書を入手して接続しているクライアントの証明書を認証するために使用されるコマンドラインインターフェイス（CLI）（**ip http secure-trustpoint** コマンドなど）は、証明書サーバーデバイス上に設定された追加のトラストポイントを指定する必要があります。

サーバがルート証明書サーバの場合、このサーバは RSA キー ペアおよびその他いくつかの属性を使用して自己署名証明書を生成します。関連付けられる CA 証明書には、デジタル署名、証明書署名および CRL 署名といった拡張キー用途があります。

CA 証明書の生成後の属性変更は、証明書サーバが壊れた場合に限りできます。

（注） **auto-enroll** コマンドを使用して、証明書サーバートラストポイントを自動的に登録しないでください。証明書サーバーの初期登録は手動で開始する必要があります。また、**auto-rollover** コマンドを使用して、進行中の自動ロールオーバー機能を設定できます。

証明書失効リスト（CRL）

デフォルトでは、CRL は 168 時間（1 週間）に 1 度発行されます。CRL を発行するために、デフォルト値以外の値を指定するには、**lifetime crl** コマンドを実行します。CRL は発行されると、*ca-label*.crl として指定されたデータベースの場所に書き込まれます。この *ca-label* は、証明書サーバの名前です。

CRL は、設定済みで利用可能な場合、SCEP（デフォルト方式）または CRL 配布ポイント（CDP）を介して配布できます。CDP を設定する場合は、**cdp-url** コマンドを使用して、CDP の場所を指定します。**cdp-url** コマンドが指定されていない場合、証明書サーバーによって発行される証明書には CDP 証明書拡張子が含まれません。CDP の場所が指定されていない場合は、Cisco IOS PKI クライアントは SCEP GetCRL メッセージを使用して証明書サーバから自動的に CRL を要求します。CA は、SCEP CertRep メッセージで CRL をクライアントに返します。すべての SCEP メッセージは、エンベロープ化された署名付き PKCS#7 データであるため、証明書サーバから CRL の SCEP を取得すると、コストがかかるうえに、拡張性はあまり高くありません。非常に大規模なネットワークでは、HTTP CDP の方が拡張性が向上するため、CRL をチェックするピアデバイスが多い場合は、HTTP CDP を推奨します。たとえば、次のように簡単な HTTP URL ストリングによって CDP の場所を指定できます。

cdp-url http://my-cdp.company.com/filename.crl

証明書サーバは、CDP を 1 つだけサポートします。したがって、発行される証明書には、すべて同じ CDP が含まれます。

Cisco IOS ソフトウェアを実行せず、SCEP GetCRL 要求をサポートしない PKI クライアントがある状態で CDP を使用する場合、外部サーバを設定して CRL を配布し、このサーバをポイントするように CDP を設定できます。または、次の形式の URL で **cdp-url** コマンドを指定する

と、証明書サーバーから CRL を取得するために非 SCEP 要求を指定できます。この *cs-addr* は証明書サーバーの場所です。

cdp-url http://*cs-addr*/cgi-bin/pkiclient.exe?operation=GetCRL

（注） また、 CA が HTTP CDP サーバーとしても設定されている場合、**cdp-url** http://*cs-addr*/cgi-bin/pkiclient.exe?operation=GetCRL コマンドシンタックスを使用して CDP を指定してください。

cdp-url コマンドによって指定された場所から CRL を利用できるかどうかは、ネットワーク管理者が確認してください。

指定された場所内に埋め込まれた疑問符を保持するようパーサーに強制するには、疑問符の前に Ctrl+V キーを入力します。この処理を実行しないと、HTTP による CRL 取得でエラー メッセージが返されます。

CDP の場所は、証明書サーバーが実行されてから、**cdp-url** コマンドによって変更できます。新しい証明書には、更新された CDP の場所が含まれていますが、既存の証明書は、新たに指定された CDP 場所を含まない状態で再発行されます。新しい CRL が発行されると、証明書サーバは、キャッシュされた現在の CRL を使用して新しい CRL を生成します（証明書サーバが再起動されると、データベースから現在の CRL をリロードします）。現在の CRL が失効するまで、新しい CRL は発行できません。現在の CRL が失効すると、CLI から証明書を無効にしたときにだけ、新しい CRL が発行されます。

証明書サーバのエラー状態

証明書サーバは起動時、証明書を発行する前に現在の設定をチェックします。証明書サーバーは、**show crypto pki server** コマンドの出力で、最後に認識されたエラー状態を報告します。たとえば、エラー状態には次のものがあります。

- 保管場所にアクセスできない
- HTTP サーバを待機する
- 時間設定を待機する

証明書サーバに、CRL の公開に失敗するなどの重大な障害が発生した場合、証明書サーバは自動的に使用不可状態になります。この場合、ネットワーク管理者がエラー状態を解消できます。エラーを解消すると、証明書サーバは直前の正常な状態に戻ります。

証明書サーバを使用した証明書登録

証明書登録要求は、次のように機能します。

- 証明書サーバがエンド ユーザから登録要求を受け取ると、次の処理が発生します。

- 要求エントリが、初期状態で登録要求データベースに作成されます（証明書登録の要求状態のリストについては、次の表を参照してください）。
- 証明書サーバは、CLI 設定（パラメータが指定されていない場合は、デフォルト動作）を参照して、要求を許可するかどうか決定します。その後、登録要求の状態は登録要求データベースで更新されます。

- SCEP クエリーごとに応答するため、証明書サーバは現在の要求を調べ、次のいずれかの処理を実行します。
  - エンド ユーザに「保留」または「拒否」状態で応答します。
  - 適切な証明書を生成して署名し、証明書を登録要求データベースに保管します。

クライアントの接続が終了すると、証明書サーバは、クライアントが別の証明書を要求するまで待機します。

すべての登録要求は、次の表に定義する証明書登録状態に移行します。現在の登録要求を表示するには、**crypto pki server request pkcs10** コマンドを使用します。

表 *156 :* 証明書登録要求状態の説明

証明書登録の状態	説明
許可	証明書サーバは要求を認可しました。
拒否	証明書サーバは、ポリシー上の理由で要求を拒否しました。
付与	CA コアは、証明書要求に対して適切な証明書を生成しました。
初期	SCEP サーバによって要求が作成されました。
形式異常	証明書サーバは、暗号化上の理由により、要求が無効であると判断しました。
保留中	ネットワーク管理者が登録要求を手動で受け入れる必要があります。

SCEP 登録

すべての SCEP 要求は新しい証明書の登録要求として処理されます。SCEP 要求で前の証明書要求と重複する所有者名または公開のキー ペアが指定された場合も同様です。

CA サーバのタイプ：下位および登録局（RA）

CA サーバは、下位の証明書サーバまたは RA モード証明書サーバとして設定できるように柔軟性を備えています。

下位 CA を設定する理由とは

下位証明書サーバは、ルート証明書サーバと同じ機能を提供します。ルート RSA キーペアは、PKI 階層構造においてきわめて重要で、多くの場合、このキー ペアをオフラインにしておく

か、アーカイブしておくことが得策です。この要件をサポートするために、PKI階層に、ルート権限で署名された下位CAを組み込めます。このように、通常の動作時には、ルート権限をオフラインにして（特別なCRL更新を発行する場合を除く）、下位CAを使用できます。

RA モード証明書サーバを設定する理由とは

証明書サーバは、RAモードで実行できるように設定できます。RAは、CAから認証および認可責任をオフロードします。RAがSCEPまたは手動での登録要求を受信すると、管理者はローカルポリシーごとに要求を拒否または許可できます。要求が許可されると、その要求は発行元CAに転送され、CAは自動的に証明書を生成してRAに返します。クライアントは、許可された証明書をRAから後で取得できます。

RAとは、CAが証明書を発行するために必要なデータの一部またはすべてを記録あるいは検証する役割を担う機関です。多くの場合、CAはRAの機能自体をすべて請け負いますが、CAが広範囲の地理的エリアで運用されている、あるいはCAがネットワーク アクセスに直接さらされるというセキュリティ上の懸念がある場合、管理上好ましいのは、作業の一部をRAに委任して、CAが基本作業である証明書およびCRLの署名に集中できるようにすることです。

CA サーバの互換性

CAサーバの互換性によって、RAモードのIOS CAサーバは複数のタイプのCAサーバと相互運用できます。詳細については、「証明書サーバを *RA* モードで実行するように設定」を参照してください。

自動 CA 証明書およびキー ロールオーバー

CA（ルートCA、下位CA、およびRAモードCA）は、クライアントと同様、有効期限付きの証明書とキー ペアを持っており、これらの証明書とキー ペアは、現在の証明書とキー ペアが失効するときに再発行する必要があります。ルートCAの証明書とキー ペアが失効すると、CAは自己署名付きロールオーバー証明書とキー ペアを生成する必要があります。下位CAまたはRAモードCAの証明書およびキー ペアが失効すると、CAは、その上位CAからロールオーバー証明書とキーペアを要求すると同時に上位CAの新しい自己署名付きロールオーバー証明書を取得します。CAは、そのすべてのピアに新しいCAロールオーバー証明書とキーを配布する必要があります。CAおよびそのクライアントが失効するCA証明書とキー ペアから新しいCA証明書とキーペアに切り替えている間に、ロールオーバーと呼ばれるプロセスにより、ネットワークは中断せずに動作します。

ロールオーバーは、PKIインフラストラクチャの信頼関係の要件および同期化されたクロックに依存します。PKIの信頼関係により、（1）新しいCA証明書の認証が可能になり、（2）セキュリティが損なわれることなく、ロールオーバーを自動的に実行できます。同期化されたクロックにより、ロールオーバーをネットワーク全体で調整できます。

自動 CA 証明書ロールオーバーの動作原理

CAサーバには、ロールオーバーが設定されている必要があります。すべてのレベルのCAを自動的に登録し、**auto-rollover**をイネーブルにする必要があります。CAクライアントは、自動的に登録されると、自動的にロールオーバーをサポートします。クライアントおよび自動ロー

ルオーバーの詳細については、「PKI の証明書登録の設定」の章にある「自動証明書登録」を参照してください。

CA がロールオーバーをイネーブルにして、そのクライアントが自動的に登録された後に、3 段階の自動 CA 証明書ロールオーバー プロセスがあります。

1 段階：アクティブな CA 証明書およびキー ペアのみ

1 段階には、アクティブな CA 証明書およびキー ペアだけがあります。

2 段階：CA 証明書のロールオーバーおよびキー ペアの生成と配布

2 段階では、ロールオーバー CA 証明書およびキー ペアが生成され、配布されます。上位 CA はロールオーバー証明書とキー ペアを生成します。CA が正常にアクティブな設定を保存すると、CA はロールオーバー証明書およびキー ペアのクライアント要求に応答する準備が完了です。上位CAがクライアントから新しいCA証明書とキーペアに対する要求を受信すると、CA は、新しいロールオーバー CA 証明書とキー ペアを要求元クライアントに送信して応答します。クライアントは、ロールオーバー CA 証明書とキー ペアを保管します。

（注） CA は、ロールオーバー証明書とキー ペアを生成したときに、そのアクティブな設定を保存できる必要があります。現在の設定が変更された場合、ロールオーバー証明書とキー ペアは自動的には保存されません。この場合、管理者は手動で設定を保存する必要があります。保存しない場合、ロールオーバー情報は失われます。

3 段階：ロールオーバー CA 証明書とキー ペアがアクティブな CA 証明書とキー ペアになる

3 段階では、ロールオーバー CA 証明書とキー ペアがアクティブな CA 証明書とキー ペアになります。有効なロールオーバー CA 証明書を保管しているすべてのデバイスは、ロールオーバー証明書をアクティブな証明書の名前に変更し、それまでアクティブだった証明書とキーペアは削除されます。

CA 証明書のロールオーバー後、通常の証明書のライフタイムおよび更新時間との間に次のような時間の違いがあることがわかる場合があります。

- ロールオーバー中に発行された証明書のライフタイムは、あらかじめ設定された値よりも低くなります。
- 特定の条件下では、更新時間が実際のライフタイムの設定割合よりも低くなる場合があります。証明書のライフタイムが 1 時間未満の場合に確認される違いは、20% までになることがあります。

このような違いがあるのは通常の状態であり、証明書サーバー上のアルゴリズムで発生する **jitter**（ランダムな時間の変動）によるものです。この作業は、PKI に参加するホストが自分の登録タイマーと同期しないようにするために実行します。同期すると、証明書サーバで輻輳が発生する場合があります。

（注） 発生するライフタイムの変動は、常にライフタイムが短くなるように発生し、証明書に対して設定された最大ライフタイム内に収まるため、PKIの適切な動作に悪影響を与えることはありません。

暗号化ハッシュ関数を指定するためのサポート

セキュア ハッシュ アルゴリズム（SHA）を使用すると、ユーザーはCisco IOSCisco IOS XE 証明書サーバーおよびクライアントの暗号化ハッシュ関数を指定できます。指定できる暗号化ハッシュ関数は、メッセージ ダイジェスト アルゴリズム 5（MD5）、SHA-1、SHA-256、SHA-384、またはSHA-512 です。

（注） シスコはMD5 の使用を推奨しません。その代わりにSHA-256 を使用する必要があります。シスコの最新の暗号化に関する推奨事項については、『*Next Generation Encryption*（NGE）』ホワイト ペーパーを参照してください。

この機能の実装に使用される **hash** (ca-trustpoint) および **hash** (cs-server) コマンドの指定に関する詳細については、「下位証明書サーバーの設定」の作業を参照してください。

証明書サーバの設定および展開方法

証明書サーバの RSA キー ペアの生成

証明書サーバの RSA キー ペアを手動で生成するには、次の作業を実行します。証明書サーバの RSA キー ペアを手動で生成すると、生成しようとするキー ペアのタイプの指定、バックアップ目的のエクスポート可能なキー ペアの作成、キー ペアの保管場所の指定、またはキー生成場所の指定ができます。

（注） バックアップまたはアーカイブ目的でエクスポート可能な証明書サーバ キー ペアを作成するとします。この作業を実行しない場合、証明書サーバは自動的にキーペアを生成し、このキーペアにはエクスポート可能のマークが付けられます。

デバイスでUSB トークンを設定し、それが利用可能な場合、USB トークンは、ストレージデバイスとしてだけでなく、暗号化デバイスとしても使用できます。USB トークンを暗号化装置として使用すると、USB トークンでクレデンシャルのキー生成、署名、認証などの RSA 操作を実行できます。秘密キーは決してUSB トークンから出ないようになっており、エクスポートできません。公開キーはエクスポート可能です。USB トークンの設定および暗号装置として

の使用に関する具体的なマニュアルのタイトルについては、「関連資料」を参照してください。

（注） 秘密キーを安全な場所に保管し、定期的に証明書サーバデータベースをアーカイブすることを推奨します。

（注） セキュリティに対する脅威は、脅威からの保護に役立つ暗号化技術と同様に絶え間なく変化しています。最新のシスコの暗号化に関する推奨事項については、『*Next Generation Encryption*』（NGE）ホワイト ペーパーを参照してください。

手順の概要

1. **enable**
2. **configure terminal**
3. **crypto key generate rsa** [**general-keys** | **usage-keys** | **signature** | **encryption**] [**label** *key-label*] [**exportable**] [**modulus** *modulus-size*] [**storage** *devicename:*] [**on** *devicename:*]
4. **crypto key export rsa** *key-label* **pem** {**terminal** | **url** *url*} {**3des** | **des**} *passphrase*
5. **crypto key import rsa** *key-label* **pem** [**usage-keys** | **signature** | **encryption**] {**terminal** | **url** *url*} [**exportable**] [**on** *devicename:*] *passphrase*
6. **exit**
7. **show crypto key mypubkey rsa**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**crypto key generate rsa** [**general-keys**	**usage-keys**	**signature**	**encryption**] [**label** *key-label*] [**exportable**] [**modulus** *modulus-size*] [**storage** *devicename:*] [**on** *devicename:*] 例： `Device(config)# crypto key generate rsa label mycs exportable modulus 2048`	証明書サーバの RSA キー ペアを生成します。 • **storage** キーワードを使用すると、キーの保管場所を指定できます。 • *key-label* 引数を指定することによってラベル名を指定する場合、**crypto pki server** *cs-label* コマンドによって証明書サーバーに使用するラベルと同じ名前を使用する必要があります。*key-label* 引数を指定していない場合、ルータの完全修飾

	コマンドまたはアクション	目的
		ドメイン名（FQDN）であるデフォルト値が使用されます。 **no shutdown** コマンドを発行する前に、CA 証明書が生成されるまで待ってからエクスポート可能な RSA キーペアを手動で生成する場合、**crypto ca export pkcs12** コマンドを使用して、証明書サーバー証明書および秘密キーを含む PKCS12 ファイルをエクスポートできます。 • デフォルトでは、CA RSA キーのモジュラス サイズは 1024 ビットです。推奨される CA RSA キーのモジュラスは 2048 ビットです。CA RSA キーのモジュラス サイズの範囲は 350 ～ 4096 ビットです。 • **on** キーワードは、指定したデバイス上で RSA キーペアが作成されることを指定します。このデバイスには Universal Serial Bus（USB）トークン、ローカルディスク、および NVRAM などがあります。装置の名前の後にはコロン（:）を付けます。 （注） USB トークン上で作成されるキーは、2048 ビット以下である必要があります。
ステップ 4	**crypto key export rsa** *key-label* **pem** {**terminal** | **url** *url*} {**3des** | **des**} *passphrase* 例： `Device(config)# crypto key export rsa mycs pem url nvram: 3des PASSWORD`	（任意）生成された RSA キー ペアをエクスポートします。 生成されたキーをエクスポートできます。
ステップ 5	**crypto key import rsa** *key-label* **pem** [**usage-keys** | **signature** | **encryption**] {**terminal** | **url** *url*} [**exportable**] [**on** *devicename:*] *passphrase* 例： `Device(config)# crypto key import rsa mycs2 pem url nvram:mycs PASSWORD`	（任意）RSA キー ペアをインポートします。 USB トークンにインポートするキーを作成するには、**on** キーワードを使用して、適切なデバイスの場所を指定します。 **exportable** キーワードを使用して RSA キーをエクスポートし、RSA キーペアをエクスポート不可に変更する場合は、**exportable** キーワードを使用せずに証明書サーバーにキーを再度インポートします。キーを再度エクスポートできません。
ステップ 6	**exit** 例：	グローバル コンフィギュレーションを終了します。

	コマンドまたはアクション	目的
	`Device(config)# exit`	
ステップ 7	**show crypto key mypubkey rsa** 例： `Device# show crypto key mypubkey rsa`	ルータの RSA 公開キーを表示します。

例

次の例では、「ms2」というラベルの USB トークンに汎用 1024 ビット RSA キー ペアを生成し、それとともに表示される暗号エンジンのデバッギング メッセージを示します。

```
Device(config)# crypto key generate rsa on usbtoken0 label ms2 modulus 2048
The name for the keys will be: ms2
% The key modulus size is 2048 bits
% Generating 2048 bit RSA keys, keys will be on-token, non-exportable...
Jan 7 02:41:40.895: crypto_engine: Generate public/private keypair [OK]
Jan 7 02:44:09.623: crypto_engine: Create signature
Jan 7 02:44:10.467: crypto_engine: Verify signature
Jan 7 02:44:10.467: CryptoEngine0: CRYPTO_ISA_RSA_CREATE_PUBKEY(hw)(ipsec)
Jan 7 02:44:10.467: CryptoEngine0: CRYPTO_ISA_RSA_PUB_DECRYPT(hw)(ipsec)
```

これで、「ms2」というラベルが付けられた、トークン上のキーを登録に使用できます。

次の例では、設定済みの利用可能なUSBトークンに正常にインポートされた暗号キーを示します。

```
Device# configure terminal

Enter configuration commands, one per line. End with CNTL/Z.

Device(config)# crypto key import rsa encryption on usbtoken0 url nvram:e password

% Importing public Encryption key or certificate PEM file...
filename [e-encr.pub]?
Reading file from nvram:e-encr.pub
% Importing private Encryption key PEM file...
Source filename [e-encr.prv]?
Reading file from nvram:e-encr.prv
% Key pair import succeeded.
```

証明書サーバの設定

自動 CA 証明書ロールオーバーに関する前提条件

証明書サーバを設定する場合、自動 CA 証明書ロールオーバーが正常に実行するために、CA サーバに次の前提条件が適用されます。

- CA サーバは、イネーブルにされ、信頼できる時刻、利用可能なキー ペア、キー ペアに関連付けられた自己署名付きの有効なCA証明書、CRL、アクセス可能なストレージデバイ

ス、およびアクティブな HTTP/SCEP サーバとともに完全に設定されている必要があります。

- CA クライアントでは、自動登録が正常に完了しており、同じ証明書サーバへの自動登録がイネーブルになっている必要があります。

自動 CA 証明書ロールオーバーに関する制約事項

証明書サーバを設定する場合、自動 CA 証明書ロールオーバーを正常に実行するために、次の制約事項が適用されます。

- SCEP を使用してロールオーバーをサポートする必要があります。SCEP の代わりに証明書管理プロトコルまたはメカニズム（登録プロファイル、手動での登録、または TFTP による登録など）を使用して、PKI に登録する装置では、SCEP で提供されているロールオーバー機能を利用できません。
- ネットワークに自動アーカイブを設定していてもアーカイブが失敗する場合、証明書サーバがロールオーバー状態にならず、ロールオーバー証明書およびキーペアが自動的に保存されないため、ロールオーバーは発生しません。

証明書サーバの設定

証明書サーバを設定し、自動ロールオーバーをイネーブルにするには、次の作業を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **ip http server**
4. **crypto pki server** *cs-label*
5. **no shutdown**
6. **auto-rollover** [*time-period*]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 3	**ip http server** 例： `Device(config)# ip http server`	ご使用のシステムの HTTP サーバをイネーブルにします。
ステップ 4	**crypto pki server** *cs-label* 例： `Device(config)# crypto pki server server-pki`	証明書サーバのラベルを定義し、証明書サーバ コンフィギュレーション モードを開始します。 （注） 手動で RSA キー ペアを生成した場合、*cs-label* 引数はキー ペアの名前と一致する必要があります。
ステップ 5	**no shutdown** 例： `Device(cs-server)# no shutdown`	（任意）証明書サーバをイネーブルにします。 （注） デフォルト機能を使用する場合は、この時点ではこのコマンドだけを使用します。つまり、デフォルト設定のいずれかを「証明書サーバ機能の設定」の作業に従って変更する場合、まだこのコマンドを発行しないでください。
ステップ 6	**auto-rollover** [*time-period*] 例： `Device(cs-server)# auto-rollover 90`	（任意）自動CA証明書ロールオーバー機能をイネーブルにします。 • *time-period*：デフォルトは 30 日です。

例

次の例では、証明書サーバ「ms2」を設定する方法について示します。ms2 は 2048 ビット RSA キー ペアのラベルです。

```
Device(config)# crypto pki server ms2
Device(cs-server)# no shutdown

% Once you start the server, you can no longer change some of
% the configuration.
Are you sure you want to do this? [yes/no]:
yes
% Certificate Server enabled.
Device(cs-server)# end
!
Device# show crypto pki server ms2
Certificate Server ms2:
    Status: enabled, configured
    CA cert fingerprint: 5A856122 4051347F 55E8C246 866D0AC3
    Granting mode is: manual
    Last certificate issued serial number: 0x1
    CA certificate expiration timer: 19:44:57 GMT Oct 14 2006

CRL NextUpdate timer: 19:45:25 GMT Oct 22 2003
```

```
    Current storage dir: nvram:
    Database Level: Complete - all issued certs written as <serialnum>.cer
```

次の例では、**auto-rollover** コマンドを使用して、サーバー ms2 の自動 CA 証明書ロールオーバーをイネーブルにする方法を示します。**show crypto pki server** コマンドを実行すると、自動ロールオーバーが 25 日のオーバラップ期間でサーバー mycs に設定されたことが示されます。

```
Device(config)# crypto pki server ms2
Device(cs-server)# auto-rollover 25
Device(cs-server)# no shutdown
%Some server settings cannot be changed after CA certificate generation.
% Exporting Certificate Server signing certificate and keys...
% Certificate Server enabled.
Device(cs-server)#
Device# show crypto pki server ms2
Certificate Server ms2:
    Status:enabled
    Server's configuration is locked  (enter "shut" to unlock it)
    Issuer name:CN=mycs
    CA cert fingerprint:70AFECA9 211CDDCC 6AA9D7FF 3ADB03AE
    Granting mode is:manual
    Last certificate issued serial number:0x1
    CA certificate expiration timer:00:49:26 PDT Jun 20 2008
    CRL NextUpdate timer:00:49:29 PDT Jun 28 2005
    Current storage dir:nvram:
    Database Level:Minimum - no cert data written to storage
    Auto-Rollover configured, overlap period 25 days
    Autorollover timer:00:49:26 PDT May 26 2008
```

下位証明書サーバの設定

すべて、または特定の SCEP 証明書要求あるいは手動の証明書要求を許可するために下位証明書サーバを設定し、自動ロールオーバーをイネーブルにするには、次の作業を実行します。

（注） セキュリティに対する脅威は、脅威からの保護に役立つ暗号化技術と同様に絶え間なく変化しています。最新のシスコの暗号化に関する推奨事項については、『*Next Generation Encryption*』（NGE）ホワイト ペーパーを参照してください。

始める前に

- ルート証明書サーバーは、Cisco IOS XE 証明書サーバーである必要があります。
- 下位の認証局（CA）の場合、ルート CA またはアップストリーム CA への登録は SCEP を介してのみ有効です。アップストリーム CA は、アップストリーム CA への登録が完了するまでオンラインである必要があります。ルート CA またはアップストリーム CA に下位 CA を手動で登録することはできません。

手順の概要

1. **enable**
2. **configure terminal**

3. **crypto pki trustpoint** *name*
4. **enrollment** [**mode**] [**retry period** *minutes*] [**retry count** *number*] **url** *url* [**pem**]
5. **hash** {**md5** | **sha1** | **sha256** | **sha384** | **sha512**}
6. **exit**
7. **crypto pki server** *cs-label*
8. **issuer name** *DN-string*
9. **mode sub-cs**
10. **auto-rollover** [*time-period*]
11. **grant auto rollover** {**ca-cert** | **ra-cert**}
12. **hash** {**md5** | **sha1** | **sha256** | **sha384** | **sha512**}
13. **no shutdown**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**crypto pki trustpoint** *name* 例： `Device(config)# crypto pki trustpoint sub`	下位の証明書サーバが使用するトラストポイントを宣言し、CA トラストポイント コンフィギュレーション モードを開始します。

ステップ 4	**enrollment** [**mode**] [**retry period** *minutes*] [**retry count** *number*] **url** *url* [**pem**]
	例：
	`Device(ca-trustpoint)# enrollment url http://caserver.myexample.com`
	または
	`Device(ca-trustpoint)# enrollment url http://[2001:DB8:1:1::1]:80`
		CA の次の登録パラメータを指定します。
		• （任意）CA システムが登録局（RA）を提供する場合、**mode** キーワードとして RA モードを指定します。デフォルトでは、RA モードは無効です。
		• （任意）**retry period** キーワードおよび *minutes* 引数は、CA に別の証明書要求を送信するまでルータが待機する期間を分単位で指定します。有効値は 1 ～ 60 です。デフォルトは 1 です。
		• （任意）**retry count** キーワードおよび *number* 引数は、直前の要求に対する応答をルータが受信しない場合、ルータが証明書要求を再送信する回数を指定します。有効な値は、1 ～ 100 です。デフォルトは 10 です。
		• *url* 引数は、ルータが証明書要求を送信する CA の URL です。

	コマンドまたはアクション	目的
		（注） IPv6 アドレスは **http:** 登録方式に追加できます。たとえば、http://[ipv6-address]:80 です。URL 内の IPv6 アドレスは括弧で囲む必要があります。使用できるその他の登録方式に関する詳細については、*enrollment url (ca-trustpoint)* コマンド ページを参照してください。 • （任意）**pem** キーワードは、証明書要求にプライバシー強化メール（PEM）の境界を追加します。
ステップ 5	**hash** {**md5** | **sha1** | **sha256** | **sha384** | **sha512**} 例： `Device(ca-trustpoint)# hash sha384`	（任意）Cisco IOS XE クライアントが自己署名証明書の署名に使用する署名のハッシュ関数を指定します。デフォルトでは、Cisco IOS XE クライアントは MD5 暗号化ハッシュ関数を自己署名証明書に使用します。 トラストポイントのデフォルト値を上書きするように、次のコマンド アルゴリズム キーワード オプションのいずれかを指定できます。その後、この設定が、自己署名証明書のデフォルトの暗号化ハッシュ アルゴリズム関数になります。 • **md5**：デフォルトのハッシュ関数 MD5 が使用されるように指定します（非推奨）。 • **sha1**：SHA-1 ハッシュ関数が RSA キーのデフォルトのハッシュアルゴリズムとして使用されるように指定します（非推奨）。 • **sha256**：SHA-256 ハッシュ関数が Elliptic Curve（EC）256 ビットキーのハッシュアルゴリズムとして使用されるように指定します。 • **sha384**：SHA-384 ハッシュ関数が EC 384 ビットキーのハッシュアルゴリズムとして使用されるように指定します。 • **sha512**：SHA-512 ハッシュ関数が EC 512 ビットキーのハッシュアルゴリズムとして使用されるように指定します。

	コマンドまたはアクション	目的
ステップ 6	**exit** 例： `Device(ca-trustpoint)# exit`	CA トラストポイントコンフィギュレーションモードを終了します。
ステップ 7	**crypto pki server** *cs-label* 例： `Device(config)# crypto pki server sub`	Cisco IOS XE 証明書サーバーをイネーブルにし、CS サーバーコンフィギュレーションモードを開始します。 （注） 下位のサーバには、上記ステップ 3 で作成されたトラストポイントと同じ名前を付ける必要があります。
ステップ 8	**issuer name** *DN-string* 例： `Device(cs-server)# issuer-name CN=sub CA, O=Cisco, C=us`	（任意）証明書サーバの CA 発行者名として DN を指定します。
ステップ 9	**mode sub-cs** 例： `Device(cs-server)# mode sub-cs`	PKI サーバをサブ証明書サーバ モードにします。 • 下位 CA と CA との関係は、ネットワーク上のすべてのデバイスが Cisco IOS XE デバイスタイプに含まれる場合のみサポートされます。そのため、Cisco IOS XE の下位 CA は、サードパーティの CA サーバーに登録することはできません。
ステップ 10	**auto-rollover** [*time-period*] 例： `Device(cs-server)# auto-rollover 90`	（任意）自動 CA 証明書ロールオーバー機能をイネーブルにします。 • *time-period*：デフォルトは 30 日です。
ステップ 11	**grant auto rollover** {**ca-cert** | **ra-cert**} 例： `Device(cs-server)# grant auto rollover ca-cert`	（任意）オペレータが介入せずに、下位の CA および RA モード CA の再登録要求を自動的に許可します。 • **ca-cert**：下位の CA ロールオーバー証明書が自動的に付与されるように指定します。 • **ra-cert**：RA モード CA ロールオーバー証明書が自動的に付与されるように指定します。 （注） これが、初めて下位の証明書サーバをイネーブルにし、登録するときであれば、証明書要求を手動で許可する必要があります。

	コマンドまたはアクション	目的
ステップ 12	**hash** {**md5** | **sha1** | **sha256** | **sha384** | **sha512**} 例： `Device(cs-server)# hash sha384`	（任意）Cisco IOS XE 認証局（CA）はサーバーから発行されたすべての証明書の署名に使用する署名のハッシュ関数を設定します。 • **md5**：デフォルトのハッシュ関数 MD5 が使用されるように指定します（非推奨）。 • **sha1**：SHA-1 ハッシュ関数が使用されるように指定します（非推奨）。 • **sha256**：SHA-256 ハッシュ関数が使用されるように指定します。 • **sha384**：SHA-384 ハッシュ関数が使用されるように指定します。 • **sha512**：SHA-512 ハッシュ関数が使用されるように指定します。
ステップ 13	**no shutdown** 例： `Device(cs-server)# no shutdown`	証明書サーバをイネーブルまたは再イネーブル化します。 これが下位の証明書サーバを初めてイネーブルにするときであれば、証明書サーバはキーを生成し、ルート証明書サーバから署名付き証明書を取得します。

例

証明書サーバーがイネーブルにならない、あるいは証明書サーバーが設定された要求を処理する際にトラブルが発生した場合は、**debug crypto pki server** コマンドを使用すると、次に示すように（「クロックが未設定」および「トラストポイントが未設定」）設定をトラブルシューティングできます。ここでは、「ms2」は 2048 ビットの RSA キー ペアのラベルを示します。

```
Router# debug crypto pki server
```

Clock Not Set

```
Router(config)# crypto pki server ms2
Router(cs-server)# mode sub-cs
Router(cs-server)# no shutdown
%Some server settings cannot be changed after CA certificate generation.
% Please enter a passphrase to protect the private key % or type Return to exit
Password:
*Jan  6 20:57:37.667: CRYPTO_CS: enter FSM: input state initial, input signal no shut
Re-enter password:
*Jan  6 20:57:45.303: CRYPTO_CS: starting enabling checks
*Jan  6 20:57:45.303: CRYPTO_CS: key 'sub' does not exist; generated automatically[OK]
% Time has not been set. Cannot start the Certificate server
```

Trustpoint Not Configured

```
Router(config)# crypto pki server ms2
Router(cs-server)# mode sub-cs
Router(cs-server)# no shutdown
%Some server settings cannot be changed after CA certificate generation.
% Please enter a passphrase to protect the private key or type Return to exit
Password:
Jan  6 21:00:15.961: CRYPTO_CS: enter FSM: input state initial, input signal no shut.
Jan  6 21:03:34.309: CRYPTO_CS: enter FSM: input state initial, input signal time set.
Jan  6 21:03:34.313: CRYPTO_CS: exit FSM: new state initial.
Jan  6 21:03:34.313: CRYPTO_CS: cs config has been unlocked
Re-enter password:
Jan  6 21:03:44.413: CRYPTO_CS: starting enabling checks
Jan  6 21:03:44.413: CRYPTO_CS: associated trust point 'sub' does not exist; generated
automatically
Jan  6 21:03:44.417: CRYPTO_CS: key 'sub' does not exist; generated automatically[OK]
Jan  6 21:04:03.993: CRYPTO_CS: nvram filesystem
Jan  6 21:04:04.077: CRYPTO_CS: serial number 0x1 written.
You must specify an enrollment URL for this CA before you can authenticate it.
% Failed to authenticate the Certificate Authority
```

証明書サーバーが署名証明書をルート証明書サーバーから取得できない場合は、次の例に示すように、**debug crypto pki transactions** コマンドを使用して設定をトラブルシューティングできます。

```
Router# debug crypto pki transactions
Jan  6 21:07:00.311: CRYPTO_CS: enter FSM: input state initial, input signal time set
Jan  6 21:07:00.311: CRYPTO_CS: exit FSM: new state initial
Jan  6 21:07:00.311: CRYPTO_CS: cs config has been unlocked no sh
%Some server settings cannot be changed after CA certificate generation.
% Please enter a passphrase to protect the private key % or type Return to exit
Password:
Jan  6 21:07:03.535: CRYPTO_CS: enter FSM: input state initial, input signal no shut
Re-enter password:
Jan  6 21:07:10.619: CRYPTO_CS: starting enabling checks
Jan  6 21:07:10.619: CRYPTO_CS: key 'sub' does not exist; generated automatically[OK]
Jan  6 21:07:20.535: %SSH-5-ENABLED: SSH 1.99 has been enabled
Jan  6 21:07:25.883: CRYPTO_CS: nvram filesystem
Jan  6 21:07:25.991: CRYPTO_CS: serial number 0x1 written.
Jan  6 21:07:27.863: CRYPTO_CS: created a new serial file.
Jan  6 21:07:27.863: CRYPTO_CS: authenticating the CA 'sub'
Jan  6 21:07:27.867: CRYPTO_PKI: Sending CA Certificate Request:
GET /cgi-bin/pkiclient.exe?operation=GetCACert&message=sub HTTP/1.0
User-Agent: Mozilla/4.0 (compatible; MSIE 5.0; Cisco PKI)
Jan 6 21:07:27.867: CRYPTO_PKI: can not resolve server name/IP address
Jan 6 21:07:27.871: CRYPTO_PKI: Using unresolved IP Address 192.0.2.6 Certificate has
the following attributes:
     Fingerprint MD5: 328ACC02 52B25DB8 22F8F104 B6055B5B
     Fingerprint SHA1: 02FD799D DD40C7A8 61DC53AB 1E89A3EA 2A729EE2
% Do you accept this certificate? [yes/no]:
Jan  6 21:07:30.879: CRYPTO_PKI: http connection opened
Jan 6 21:07:30.903: CRYPTO_PKI: HTTP response header:
  HTTP/1.1 200 OK
Date: Thu, 06 Jan 2005 21:07:30 GMT
Server: server-IOS
Content-Type: application/x-x509-ca-cert
Expires: Thu, 06 Jan 2005 21:07:30 GMT
Last-Modified: Thu, 06 Jan 2005 21:07:30 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Accept-Ranges: none
```

```
Content-Type indicates we have received a CA certificate.
Jan  6 21:07:30.903: Received 507 bytes from server as CA certificate:
Jan  6 21:07:30.907: CRYPTO_PKI: transaction GetCACert completed
Jan  6 21:07:30.907: CRYPTO_PKI: CA certificate received.
Jan  6 21:07:30.907: CRYPTO_PKI: CA certificate received.
Jan  6 21:07:30.927: CRYPTO_PKI: crypto_pki_authenticate_tp_cert()
Jan  6 21:07:30.927: CRYPTO_PKI: trustpoint sub authentication status = 0 y Trustpoint
CA certificate accepted.%
% Certificate request sent to Certificate Authority
% Enrollment in progress...
Router (cs-server)#
Jan 6 21:07:51.772: CRYPTO_CA: certificate not found
Jan 6 21:07:51.772: CRYPTO_CA: certificate not found
Jan 6 21:07:52.460: CRYPTO_CS: Publishing 213 bytes to crl file nvram:sub.crl
Jan 6 21:07:54.348: CRYPTO_CS: enrolling the server's trustpoint 'sub'
Jan 6 21:07:54.352: CRYPTO_CS: exit FSM: new state check failed
Jan 6 21:07:54.352: CRYPTO_CS: cs config has been locked
Jan 6 21:07:54.356: CRYPTO_PKI: transaction PKCSReq completed
Jan 6 21:07:54.356: CRYPTO_PKI: status:
Jan 6 21:07:55.016: CRYPTO_PKI:  Certificate Request Fingerprint MD5: 1BA027DB 1C7860C7
 EC188F65 64356C80
Jan 6 21:07:55.016: CRYPTO_PKI:  Certificate Request Fingerprint SHA1: 840DB52C E17614CB
 0C7BE187 0DFC884D D32CAA75
Jan 6 21:07:56.508: CRYPTO_PKI: can not resolve server name/IP address
Jan 6 21:07:56.508: CRYPTO_PKI: Using unresolved IP Address 192.0.2.6
Jan 6 21:07:56.516: CRYPTO_PKI: http connection opened
Jan 6 21:07:59.136: CRYPTO_PKI: received msg of 776 bytes
Jan 6 21:07:59.136: CRYPTO_PKI: HTTP response header:
  HTTP/1.1 200 OK
  Date: Thu, 06 Jan 2005 21:07:57 GMT
  Server: server-IOS
  Content-Type: application/x-pki-message
  Expires: Thu, 06 Jan 2005 21:07:57 GMT
  Last-Modified: Thu, 06 Jan 2005 21:07:57 GMT
  Cache-Control: no-store, no-cache, must-revalidate
  Pragma: no-cache
  Accept-Ranges: none
Jan 6 21:07:59.324: The PKCS #7 message has 1 verified signers.
Jan 6 21:07:59.324: signing cert: issuer=cn=root1
Jan 6 21:07:59.324: Signed Attributes:
Jan 6 21:07:59.328: CRYPTO_PKI: status = 102: certificate request pending
Jan 6 21:08:00.788: CRYPTO_PKI: can not resolve server name/IP address
Jan 6 21:08:00.788: CRYPTO_PKI: Using unresolved IP Address 192.0.2.6
Jan 6 21:08:00.796: CRYPTO_PKI: http connection opened
Jan 6 21:08:11.804: CRYPTO_PKI: received msg of 776 bytes
Jan 6 21:08:11.804: CRYPTO_PKI: HTTP response header: HTTP/1.1 200 OK
  Date: Thu, 06 Jan 2005 21:08:01 GMT
  Server: server-IOS
  Content-Type: application/x-pki-message
  Expires: Thu, 06 Jan 2005 21:08:01 GMT
  Last-Modified: Thu, 06 Jan 2005 21:08:01 GMT
  Cache-Control: no-store, no-cache, must-revalidate
  Pragma: no-cache
  Accept-Ranges: none
Jan  6 21:08:11.992: The PKCS #7 message has 1 verified signers.
Jan  6 21:08:11.992: signing cert: issuer=cn=root1
Jan  6 21:08:11.996: Signed Attributes:
Jan  6 21:08:11.996: CRYPTO_PKI: status = 102: certificate request pending
Jan  6 21:08:21.996: CRYPTO_PKI: All sockets are closed for trustpoint sub.
Jan  6 21:08:31.996: CRYPTO_PKI: All sockets are closed for trustpoint sub.
Jan  6 21:08:41.996: CRYPTO_PKI: All sockets are closed for trustpoint sub.
Jan  6 21:08:51.996: CRYPTO_PKI: All sockets are closed for trustpoint sub.
Jan  6 21:09:01.996: CRYPTO_PKI: All sockets are closed for trustpoint sub.
Jan  6 21:09:11.996: CRYPTO_PKI: resend GetCertInitial, 1
```

```
Jan  6 21:09:11.996: CRYPTO_PKI: All sockets are closed for trustpoint sub.
Jan  6 21:09:11.996: CRYPTO_PKI: resend GetCertInitial for session: 0
Jan  6 21:09:11.996: CRYPTO_PKI: can not resolve server name/IP address
Jan  6 21:09:11.996: CRYPTO_PKI: Using unresolved IP Address 192.0.2.6
Jan  6 21:09:12.024: CRYPTO_PKI: http connection opened% Exporting Certificate Server
signing certificate and keys...
Jan  6 21:09:14.784: CRYPTO_PKI: received msg of 1611 bytes
Jan  6 21:09:14.784: CRYPTO_PKI: HTTP response header:
  HTTP/1.1 200 OK
  Date: Thu, 06 Jan 2005 21:09:13 GMT
  Server: server-IOS
  Content-Type: application/x-pki-message
  Expires: Thu, 06 Jan 2005 21:09:13 GMT
  Last-Modified: Thu, 06 Jan 2005 21:09:13 GMT
  Cache-Control: no-store, no-cache, must-revalidate
  Pragma: no-cache
  Accept-Ranges: none
Jan  6 21:09:14.972: The PKCS #7 message has 1 verified signers.
Jan  6 21:09:14.972: signing cert: issuer=cn=root1
Jan  6 21:09:14.972: Signed Attributes:
Jan  6 21:09:14.976: CRYPTO_PKI: status = 100: certificate is granted
Jan  6 21:09:15.668: The PKCS #7 message contains 1 certs and 0 crls.
Jan  6 21:09:15.688: Newly-issued Router Cert: issuer=cn=root serial=2
Jan  6 21:09:15.688: start date: 21:08:03 GMT Jan 6 2005
Jan  6 21:09:15.688: end date: 21:08:03 GMT Jan 6 2006
Jan  6 21:09:15.688: Router date: 21:09:15 GMT Jan 6 2005
Jan  6 21:09:15.692: Received router cert from CA
Jan  6 21:09:15.740: CRYPTO_CA: certificate not found
Jan  6 21:09:15.744: CRYPTO_PKI: All enrollment requests completed for trustpoint sub.
Jan  6 21:09:15.744: %PKI-6-CERTRET: Certificate received from Certificate Authority
Jan  6 21:09:15.744: CRYPTO_PKI: All enrollment requests completed for trustpoint sub.
Jan  6 21:09:15.744: CRYPTO_PKI: All enrollment requests completed for trustpoint sub.
Jan  6 21:09:15.748: CRYPTO_CS: enter FSM: input state check failed, input signal cert
configured
Jan  6 21:09:15.748: CRYPTO_CS: starting enabling checks
Jan  6 21:09:15.748: CRYPTO_CS: nvram filesystem
Jan  6 21:09:15.796: CRYPTO_CS: found existing serial file.
Jan  6 21:09:15.820: CRYPTO_CS: old router cert flag 0x4
Jan  6 21:09:15.820: CRYPTO_CS: new router cert flag 0x44
Jan  6 21:09:18.432: CRYPTO_CS: DB version 1
Jan  6 21:09:18.432: CRYPTO_CS: last issued serial number is 0x1
Jan  6 21:09:18.480: CRYPTO_CS: CRL file sub.crl exists.
Jan  6 21:09:18.480: CRYPTO_CS: Read 213 bytes from crl file sub.crl.
Jan  6 21:09:18.532: CRYPTO_CS: SCEP server started
Jan  6 21:09:18.532: CRYPTO_CS: exit FSM: new state enabled
Jan  6 21:09:18.536: CRYPTO_CS: cs config has been locked
Jan  6 21:09:18.536: CRYPTO_PKI: All enrollment requests completed for trustpoint sub.
```

証明書サーバーがイネーブルにならない、あるいは証明書サーバーが設定された要求を処理する際に問題が発生した場合は、**debug crypto pki server** コマンドを使用して、登録の進行状況をトラブルシューティングできます。このコマンドは、ルート CA をデバッグする場合にも使用できます（このコマンドは、ルート CA でオンにしてください）。

証明書サーバを RA モードで実行するように設定

証明書サーバは、 CA または別のサードパーティの CA の RA として機能することができます。サードパーティの CA を使用する場合は、**transparent** キーワードオプションに関する手順 8 の詳細を確認してください。

手順の概要

1. **enable**
2. **configure terminal**
3. **crypto pki trustpoint** *name*
4. **enrollment url** *url*
5. **subject-name** *x.500-name*
6. **exit**
7. **crypto pki server** *cs-label*
8. **mode ra** [**transparent**]
9. **auto-rollover** [*time-period*]
10. **grant auto rollover** {**ca-cert** | **ra-cert**}
11. **no shutdown**
12. **no shutdown**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**crypto pki trustpoint** *name* 例： `Device(config)# crypto pki trustpoint ra-server`	RA モード証明書サーバが使用するトラストポイントを宣言し、CA トラストポイント コンフィギュレーション モードを開始します。
ステップ 4	**enrollment url** *url* 例： `Device(ca-trustpoint)# enrollment url http://ca-server.company.com`	発行元 CA 証明書サーバ（ルート証明書サーバ）の登録 URL を指定します。
ステップ 5	**subject-name** *x.500-name* 例： `Device(ca-trustpoint)# subject-name cn=ioscs RA`	RA が使用する所有者名を指定します。 （注） 発行元 CA 証明書サーバが RA を認識できるように、所有者名に「cn=ioscs RA」または「ou=ioscs RA」を含めます（ステップ 7 を参照）。
ステップ 6	**exit** 例： `Device(ca-trustpoint)# exit`	CA トラストポイント コンフィギュレーション モードを終了します。

	コマンドまたはアクション	目的
ステップ 7	**crypto pki server** *cs-label* 例： `Device(config)# crypto pki server ra-server`	証明書サーバをイネーブルにし、CS サーバ コンフィギュレーション モードを開始します。 （注） 証明書サーバには、上記ステップ 3 で作成されたトラストポイントと同じ名前を付ける必要があります。
ステップ 8	**mode ra** [**transparent**] 例： `Device(cs-server)# mode ra`	PKI サーバを RA 証明書サーバ モードにします。 RA モードの CA サーバーが複数のタイプの CA サーバーと相互運用できるようにするには、**transparent** キーワードを使用します。**transparent** キーワードを使用すると、元の PKCS#10 登録メッセージは再署名されず、変更せずに転送されます。この登録メッセージによって、IOS RA 証明書サーバは Microsoft CA サーバなどの CA サーバと連携します。
ステップ 9	**auto-rollover** [*time-period*] 例： `Device(cs-server)# auto-rollover 90`	（任意）自動 CA 証明書ロールオーバー機能をイネーブルにします。 • *time-period*：デフォルトは 30 日です。
ステップ 10	**grant auto rollover** {**ca-cert** | **ra-cert**} 例： `Device(cs-server)# grant auto rollover ra-cert`	（任意）オペレータが介入せずに、下位の CA および RA モード CA の再登録要求を自動的に許可します。 • **ca-cert**：下位の CA ロールオーバー証明書が自動的に付与されるように指定します。 • **ra-cert**：RA モード CA ロールオーバー証明書が自動的に付与されるように指定します。 これが、初めて下位の証明書サーバをイネーブルにし、登録するときであれば、証明書要求を手動で許可する必要があります。
ステップ 11	**no shutdown** 例： `Device(cs-server)# no shutdown`	証明書サーバをイネーブルにします。 （注） このコマンドが発行されると、RA はルート証明書サーバに自動的に登録されます。RA 証明書が正常に受信されたら、 **no shutdown** コマンドを再度発行する必要があります。これにより、証明書サーバーが再イネーブル化されます。

	コマンドまたはアクション	目的
ステップ 12	**no shutdown** 例： `Device(cs-server)# no shutdown`	証明書サーバを再イネーブル化します。

RA モード証明書サーバに登録作業を委任するためのルート証明書サーバの設定

発行元証明書サーバを実行しているルータで、次のステップを実行します。具体的には、登録作業を RA モード証明書サーバに委任するルート証明書サーバを設定します。

（注） RA の登録要求を許可することは、本質的にクライアントデバイスの登録要求を許可するプロセスと同じですが、RA の登録要求が **crypto pki server info-requests** コマンドのコマンド出力の「RA certificate requests」セクションに表示されるという点が異なります。

手順の概要

1. **enable**
2. **crypto pki server** *cs-label* **info requests**
3. **crypto pki server** *cs-label* **grant** *req-id*
4. **configure terminal**
5. **crypto pki server** *cs-label*
6. **grant ra-auto**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**crypto pki server** *cs-label* **info requests** 例： `Device# crypto pki server root-server info requests`	未処理の RA 証明書要求を表示します。 （注） このコマンドは、発行元証明書サーバを実行しているルータ上で発行されます。
ステップ 3	**crypto pki server** *cs-label* **grant** *req-id* 例： `Device# crypto pki server root-server grant 9`	保留の RA 証明書要求を許可します。 （注） 発行元証明書サーバが RA に登録要求の検証作業を委任するので、RA 証明書要求を許可する前に、RA 証明書要求に十分注意を払ってください。

	コマンドまたはアクション	目的
ステップ 4	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 5	**crypto pki server** *cs-label* 例： `Device(config)# crypto pki server root-server`	証明書サーバをイネーブルにし、CS サーバ コンフィギュレーション モードを開始します。
ステップ 6	**grant ra-auto** 例： `Device(cs-server)# grant ra-auto`	（任意）RA からのすべての登録要求が自動的に許可されるように指定します。 （注） **grant ra-auto** コマンドを機能させるには、RA 証明書の所有者名に「cn=ioscs RA」または「ou=ioscs RA」を含める必要があります（上記のステップ 2 を参照）。

次の作業

証明書サーバを設定したら、デフォルト値を使用するか、証明書サーバの機能用の CLI を使用して値を指定できます。デフォルト値以外の値を指定する場合は、「証明書サーバー機能の設定」の項を参照してください。

証明書サーバ機能の設定

証明書サーバをイネーブルにし、証明書サーバ コンフィギュレーション モードになったら、次の作業のいずれかのステップを使用して、基本証明書サーバ機能の値（デフォルト値以外）を設定します。

証明書サーバのデフォルト値および推奨値

証明書サーバのデフォルト値は、比較的小規模のネットワーク（10 台程度のデバイス）に対処することを意図しています。たとえば、データベース設定値が最小に設定されている場合（**database level minimal** コマンドによって）、証明書サーバーは SCEP を使用してすべての CRL 要求を処理します。大規模なネットワークでは、考えられる監査および失効目的のためにデータベース設定「names」または「complete」（ **database level** コマンドで示されるように）を使用することを推奨します。さらに大規模なネットワークでは、CRL 確認ポリシーに応じて、外部 CDP を使用する必要があります。

証明書サーバ ファイルの保管および公開場所

ファイル タイプをさまざまな保管場所に保管し、さまざまな公開場所で公開できる柔軟性が備わっています。

手順の概要

1. **database url** *root-url*
2. **database url** {**cnm** | **crl** | **crt** | **p12** | **pem** | **ser**} *root-url*
3. **database url** {**cnm** | **crl** | **crt**} **publish** *root-url*
4. **database level** {**minimal** | **names** | **complete**}
5. **database username** *username* [**password** [*encr-type*] *password*]
6. **database archive** {**pkcs12** | **pem**}[**password** *encr-type*] *password*]
7. **issuer-name** *DN-string*
8. **lifetime** {**ca-certificate** | **certificate**} *time*
9. **lifetime crl** *time*
10. **lifetime enrollment-request** *time*
11. **cdp-url** *url*
12. **no shutdown**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**database url** *root-url* 例： `Device(cs-server)# database url tftp://cert-svr-db.company.com`	証明書サーバのデータベース エントリが書き出されるプライマリ ロケーションを指定します。 このコマンドが指定されていない場合、すべてのデータベース エントリは NVRAM に書き込まれます。
ステップ 2	**database url** {**cnm** | **crl** | **crt** | **p12** | **pem** | **ser**} *root-url* 例： `Device(cs-server)# database url ser nvram:`	証明書サーバの重要なファイルの保管場所をファイル タイプ別に指定します。 （注） このコマンドが指定されていないと、すべての重要ファイルは、（指定されている場合）プライマリ ロケーションに保管されます。プライマリ ロケーションが指定されてない場合は、すべての重要ファイルが NVRAM に保管されます。
ステップ 3	**database url** {**cnm** | **crl** | **crt**} **publish** *root-url* 例： `Device(cs-server)# database url crl publish tftp://csdb_specific_crl_files.company.com`	証明書サーバの公開場所をファイル タイプ別に指定します。 （注） このコマンドが指定されていないと、すべての公開ファイルは、（指定されている場合）プライマリ ロケーションに保管されます。プライマリ ロケーションが指定されてない場合は、すべての公開ファイルが NVRAM に保管されます。

	コマンドまたはアクション	目的
ステップ 4	**database level** {**minimal** | **names** | **complete**} 例： `Device(cs-server)# database level complete`	証明書登録データベースに保管されるデータのタイプを制御します。 • **minimal**：新しい証明書を、継続して問題なく発行できる程度の情報が保管されます。これがデフォルト値です。 • **names**：minimal レベルで提供される情報以外に、各証明書のシリアル番号および所有者名を保存します。 • **complete**：minimal レベルおよび names レベルで提供される情報以外に、発行済みの各証明書がデータベースに書き込まれます。 （注） **complete** キーワードを指定すると、大量の情報が生成されます。このキーワードを発行する場合、**database url** コマンドを使用して、データを保管する外部 TFTP サーバーも指定する必要があります。
ステップ 5	**database username** *username* [**password** [*encr-type*] *password*] 例： `Device(cs-server)# database username user password PASSWORD`	（任意）プライマリ証明書登録データベースの保管場所にアクセスする必要がある場合、ユーザ名とパスワードを設定します。
ステップ 6	**database archive** {**pkcs12** | **pem**}[**password** *encr-type*] *password*] 例： `Device(cs-server)# database archive pem`	（任意）ファイルを暗号化するための CA キーと CA 証明書のアーカイブ形式およびパスワードを設定します。 デフォルト値は **pkcs12** です。したがって、このサブコマンドが設定されていなくても、自動アーカイブが引き続き実行され、PKCS12 形式が使用されます。 • パスワードの設定は任意です。パスワードが設定されていない場合、サーバを初めて起動したときに、パスワードの入力を求めるプロンプトが表示されます。 （注） アーカイブが完了したら、設定からパスワードを削除することを推奨します。

	コマンドまたはアクション	目的
ステップ 7	**issuer-name** *DN-string* 例： `Device(cs-server)# issuer-name my-server`	（任意）指定した識別名（*DN-string*）にCA発行者名を設定します。デフォルト値は **issuer-name cn**={*cs-label* } です。
ステップ 8	**lifetime** {**ca-certificate** | **certificate**} *time* 例： `Device(cs-server)# lifetime certificate 888`	（任意）CA 証明書または証明書のライフタイム（日数）を指定します。 有効な値の範囲は、1 ～ 1825 日です。CA 証明書のデフォルトのライフタイムは3年、証明書のデフォルトのライフタイムは1年です。証明書の最大のライフタイムは、CA 証明書のライフタイムより 1 カ月短い日数です。
ステップ 9	**lifetime crl** *time* 例： `Device(cs-server)# lifetime crl 333`	（任意）証明書サーバが使用する CRL のライフタイム（時間単位）を定義します。 最大ライフタイム値は336時間（2週間）です。デフォルト値は 168 時間（1 週間）です。
ステップ 10	**lifetime enrollment-request** *time* 例： `Device(cs-server)# lifetime enrollment-request 888`	（任意）登録要求が削除されるまで、登録データベースに保管される期間を指定します。 最大ライフタイムは 1000 時間です。
ステップ 11	**cdp-url** *url* 例： `Device(cs-server)# cdp-url http://my-cdp.company.com`	（任意）証明書サーバが発行した証明書で使用される CDP の場所を定義します。 • URL は、HTTP URL を使用する必要があります。 Cisco IOS ソフトウェアを実行せず、また SCEP GetCRL 要求をサポートしない PKI クライアントの場合は、次の URL 形式を使用します。 http://server.company.com/certEnroll/filename.crl また、Cisco IOS 証明書サーバが CDP としても設定されている場合は、次の URL 形式を使用します。 http://cs-addr/cgi-bin/pkiclient.exe?operation=GetCRL この *cs-addr* は証明書サーバの場所です。 指定された場所内に埋め込まれた疑問符を保持するようパーサーに強制するには、疑問符の前にCtrl+Vキーを入力します。この処理を実行しないと、HTTP による CRL 取得でエラー メッセージが返されます。

	コマンドまたはアクション	目的
		（注） このコマンドは任意ですが、すべての展開シナリオで使用することをぜひ推奨します。
ステップ 12	**no shutdown** 例： `Device(cs-server)# no shutdown`	証明書サーバをイネーブルにします。 このコマンドは、証明書サーバの設定が完了した後で発行する必要があります。

例

次の例では、PKI クライアントが SCEP GetCRL 要求をサポートしない CDP の場所を設定する方法を示します。

```
Device(config)# crypto pki server aaa
Device(cs-server)# database level minimum
Device(cs-server)# database url tftp://10.1.1.1/username1/
Device(cs-server)# issuer-name CN=aaa
Device(cs-server)# cdp-url http://server.company.com/certEnroll/aaa.crl
```

証明書サーバーがルータ上でイネーブルになってから、 **show crypto pki server** コマンドを実行すると、次の出力が表示されます。

```
Device# show crypto pki server

    Certificate Server status:enabled, configured
    Granting mode is:manual
    Last certificate issued serial number:0x1
    CA certificate expiration timer:19:31:15 PST Nov 17 2006
    CRL NextUpdate timer:19:31:15 PST Nov 25 2003
    Current storage dir:nvram:
    Database Level:Minimum - no cert data written to storage
```

自動 CA 証明書ロールオーバーでの作業

自動 CA 証明書ロールオーバーをただちに開始する

ルート CA サーバ上で自動 CA 証明書ロールオーバー プロセスをただちに開始するには、次の作業を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **crypto pki server** *cs-label* **rollover** [**cancel**]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**crypto pki server** *cs-label* **rollover** [**cancel**] 例： `Device(config)# crypto pki server mycs rollover`	シャドウ CA 証明書を生成して、CA 証明書ロールオーバー プロセスをただちに開始します。 CA 証明書ロールオーバー証明書およびキーを削除するには、**cancel** キーワードを使用します。

証明書サーバ クライアントのロールオーバー証明書の要求

証明書サーバクライアントのロールオーバー証明書を要求するには、次の作業を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **crypto pki server** *cs-label* **rollover request pkcs10 terminal**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**crypto pki server** *cs-label* **rollover request pkcs10 terminal** 例： `Device(config)# crypto pki server mycs rollover request pkcs10 terminal`	サーバからクライアント ロールオーバー証明書を要求します。

例

次は、サーバに入力されるロールオーバー証明書要求の例です。

```
Device# crypto pki server mycs rollover request pkcs10 terminal

% Enter Base64 encoded or PEM formatted PKCS10 enrollment request.
% End with a blank line or "quit" on a line by itself.
-----BEGIN CERTIFICATE REQUEST-----
MIIBUTCBuwIBADASMRAwDgYDVQQDEwdOZXdSb290MIGfMA0GCSqGSIb3DQEBAQUA
A4GNADCBiQKBgQDMHeev1ERSs320zbLQQk+3lhV/R2HpYQ/iM6uT1jkJf5iy0UPR
wF/X16yUNmG+ObiGiW9fsASF0nxZw+fO7d2X2yh1PakfvF2wbP27C/sgJNOw9uPf
sBxEc40Xe0d5FMh0YKOSAShfZYKOflnyQR2Drmm2x/33QGol5QyRvjkeWQIDAQAB
oAAwDQYJKoZIhvcNAQEEBQADgYEALM90r4d79X6vxhD0qjuYJXfBCOvv4FNyFsjr
aBS/y6CnNVYySF8UBUohXYIGTWf4I4+sj6i8gYfoFUW1/L82djS18TLrUr6wpCOs
RqfAfps7HW1e4cizOfjAUU+C7lNcobCAhwF1o6q2nIEjpQ/2yfK9O7sb3SCJZBfe
eW3tyCo=
-----END CERTIFICATE REQUEST-----
```

CA ロールオーバー証明書のエクスポート

CA ロールオーバー証明書をエクスポートするには、次の作業を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **crypto pki export** *trustpoint* **pem** {**terminal** | **url** *url*} [**rollover**]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**crypto pki export** *trustpoint* **pem** {**terminal** | **url** *url*} [**rollover**] 例： `Device(config)# crypto pki export mycs pem terminal rollover`	CA シャドウ証明書をエクスポートします。

証明書サーバ、証明書、CAの保守、検証、およびトラブルシューティング

登録要求データベースの管理

SCEP は、2 つのクライアント認証メカニズム（手動による登録と事前共有キーを使用する登録）をサポートします。手動による登録では、管理者は、CA サーバで具体的に登録要求を認可する必要があります。事前共有キーを使用する登録では、管理者は、ワンタイムパスワード（OTP）を生成することにより、登録要求を事前に許可できます。

次の作業のうち、いずれかのステップを使用して、SCEP で使用される登録処理パラメータの指定、および実行時動作または証明書サーバの制御などの機能を実行すると、登録要求データベースが管理しやすくなります。

手順の概要

1. **enable**
2. **crypto pki server** *cs-label* **grant** {**all** | *req-id*}
3. **crypto pki server** *cs-label* **reject** {**all** | *req-id*}
4. **crypto pki server** *cs-label* **password generate** *minutes*
5. **crypto pki server** *cs-label* **revoke** *certificate-serial-number*
6. **crypto pki server** *cs-label* **request pkcs10** {*url* | **terminal**} [**base64**| **pem**
7. **show crypto pki server** *cs-label* **crl**
8. **show crypto pki server** *cs-label* **requests**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**crypto pki server** *cs-label* **grant** {**all**	*req-id*} 例： `Device# crypto pki server mycs grant all`	すべての SCEP 要求または特定の SCEP 要求を許可します。
ステップ 3	**crypto pki server** *cs-label* **reject** {**all**	*req-id*} 例： `Device# crypto pki server mycs reject all`	すべての SCEP 要求または特定の SCEP 要求を拒否します。
ステップ 4	**crypto pki server** *cs-label* **password generate** *minutes* 例： `Device# crypto pki server mycs password generate 75`	SCEP 要求に対して OTP を生成します。 • *minutes*：パスワードの有効時間（分）。有効な値の範囲は、1 ～ 1440 分です。デフォルトは 60 分です。

	コマンドまたはアクション	目的
		（注） 有効になる OTP は、一度に 1 つだけです。別の OTP が生成されると、1 番目の OTP は無効になります。
ステップ 5	**crypto pki server** *cs-label* **revoke** *certificate-serial-number* 例： `Device# crypto pki server mycs revoke 3`	証明書を証明書のシリアル番号に基づいて無効にします。 • *certificate-serial-number*：次のオプションのいずれかを指定します。 • 0x で始まるストリング。これは 16 進値として処理されます • 0 と no x で始まるストリング。これは 8 進値として処理されます • その他すべてのストリング。これらは 10 進値として処理されます
ステップ 6	**crypto pki server** *cs-label* **request pkcs10** {*url* | **terminal**} [**base64**| **pem** 例： `Device# crypto pki server mycs request pkcs10 terminal pem`	Base 64 符号化形式または PEM 形式の PKCS10 証明書登録要求を要求データベースに手動で追加します。 証明書が付与されると、証明書は Base 64 符号化を使用してコンソール端末に表示されます。 • **pem**：要求に PEM ヘッダーが使用されたかどうかにかかわらず、証明書を付与された後、PEM ヘッダーを自動的に追加した証明書を返すように指定します。 • **base64**：要求に PEM ヘッダーが使用されたかどうかにかかわらず、証明書をプライバシー強化メール（PEM）ヘッダーなしで返すように指定します。
ステップ 7	**show crypto pki server** *cs-label* **crl** 例： `Device# show crypto pki server mycs crl`	現在の CRL のステータスに関する情報を表示します。
ステップ 8	**show crypto pki server** *cs-label* **requests** 例： `Device# show crypto pki server mycs requests`	未処理の証明書登録要求をすべて表示します。

登録要求データベースからの要求の削除

証明書サーバは、登録要求を受け取ると、要求を保留状態のままにする、拒否するか、あるいは許可できます。要求は、クライアントが要求の結果を求めて証明書サーバをポーリングするまで、登録要求データベースに1週間保存されます。クライアントが終了し、証明書サーバを絶対にポーリングしない場合は、個々の要求またはすべての要求をデータベースから削除できます。

次の作業を実行して、データベースから要求を削除し、キーおよびトランザクション ID に関してサーバをクリーンな状態に戻せます。また、この作業を実行して、適切に動作しないSCEPクライアントのトラブルシューティングができます。

手順の概要

1. **enable**
2. **crypto pki server** *cs-label* **remove** {**all** | *req-id*}

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**crypto pki server** *cs-label* **remove** {**all**	*req-id*} 例： `Device# crypto pki server mycs remove 15`	登録要求を登録要求データベースから削除します。

証明書サーバの削除

証明書サーバをPKI設定に残したくない場合、証明書サーバをPKI設定から削除できます。通常、下位の証明書サーバまたは RA は削除されます。ただし、保存された RSA キーを使用してルート証明書サーバを別のデバイスに移動した場合は、ルート証明書サーバを削除できます。

PKI 設定から証明書サーバを削除するには、次の作業を実行します。

（注） 証明書サーバを削除すると、関連付けられているトラストポイントおよびキーも削除されます。

手順の概要

1. **enable**
2. **configure terminal**
3. **no crypto pki server** *cs-label*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**no crypto pki server** *cs-label* 例： `Device(config)# no crypto pki server mycs`	証明書サーバおよび関連付けられたトラストポイントとキーを削除します。

証明書サーバと CA ステータスの検証およびトラブルシューティング

証明書サーバまたは CA のステータスを検証するには、次の手順のいずれかを使用します。

手順の概要

1. **enable**
2. **debug crypto pki server**
3. **dir** *filesystem* :

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**debug crypto pki server** 例： `Device# debug crypto pki server`	暗号 PKI 証明書サーバのデバッグをイネーブルにします。 • 証明書サーバが応答しない場合、あるいは証明書サーバが設定された要求を処理する際に問題が発生した場合は、このコマンドを使用して登録の進行状況のモニタリングおよびトラブルシューティングができます。
ステップ 3	**dir** *filesystem* : 例： `Device# dir slot0:`	ファイル システムのファイル リストを表示します。 • ローカルファイルシステムをポイントするために **database url** コマンドを入力した場合は、このコマンドを使用して、証明書サーバー自動

	コマンドまたはアクション	目的
		アーカイブファイルを検証できます。少なくともデータベース内の「*cs-label* .ser」および「*cs-label* .crl」ファイルを参照できる必要があります。

CA 証明書情報の検証

CA 証明書に関連する情報（証明書サーバ ロールオーバー プロセス、ロールオーバー証明書、およびタイマーなど）を入手するには、次のコマンドのいずれかを使用します。

（注） これらのコマンドは、シャドウ証明書情報に対して排他的ではありません。シャドウ証明書が存在しない場合、次のコマンドを実行すると、アクティブな証明書情報だけが表示されます。

手順の概要

1. **crypto pki certificate chain**
2. **crypto pki server info requests**
3. **show crypto pki certificates**
4. **show crypto pki server**
5. **show crypto pki trustpoints**

手順の詳細

ステップ 1 **crypto pki certificate chain**

例：

```
Device(config)# crypto pki certificate chain mica

certificate 06
certificate ca 01
! This is the peer's shadow PKI certificate.
certificate rollover 0B
! This is the CA shadow PKI certificate
certificate rollover ca 0A
```

証明書チェーンの詳細を表示し、現在のアクティブな証明書と証明書チェーンのロールオーバー証明書を区別します。次の例では、アクティブな CA 証明書を持つ証明書チェーンおよびシャドウ証明書、またはロールオーバー証明書を示します。

ステップ 2 **crypto pki server info requests**

例：

```
Device# crypto pki server myca info requests

Enrollment Request Database:
RA certificate requests:
```

```
  ReqID  State      Fingerprint                      SubjectName
--------------------------------------------------------------
RA rollover certificate requests:
  ReqID  State      Fingerprint                      SubjectName
  --------------------------------------------------------------
Router certificates requests:
  ReqID  State      Fingerprint                      SubjectName
--------------------------------------------------------------
1      pending    A426AF07FE3A4BB69062E0E47198E5BF hostname=client
  Router rollover certificates requests:
  ReqID  State      Fingerprint                      SubjectName
  --------------------------------------------------------------
  2      pending    B69062E0E47198E5BFA426AF07FE3A4B hostname=client
```

未処理の証明書登録要求をすべて表示します。次に、シャドウ PKI 証明書情報要求の出力例を示します。

ステップ 3 show crypto pki certificates

例：

```
Device# show crypto pki certificates

Certificate
  Subject Name
    Name: myrouter.example.com
    IP Address: 192.0.2.1
    Serial Number: 04806682
  Status: Pending
  Key Usage: General Purpose
    Fingerprint: 428125BD A3419600 3F6C7831 6CD8FA95 00000000
CA Certificate
  Status: Available
  Certificate Serial Number: 3051DF7123BEE31B8341DFE4B3A338E5F
  Key Usage: Not Set
```

証明書、認証局証明書、シャドウ証明書、および任意の登録認局証明書に関する情報を表示します。次の例では、ルータの証明書および CA の証明書を表示します。利用可能なシャドウ証明書はありません。単一の汎用目的 RSA キー ペアが以前に生成されていましたが、このキー ペアについては、証明書が要求されているものの、受信されていません。ルータの証明書のステータスが「Pending」であることに注意してください。ルータが CA からその証明書を受信すると、**show** 出力の [Status] フィールドが「Available」に変わります。

ステップ 4 show crypto pki server

例：

```
Device# show crypto pki server

Certificate Server routercs:
   Status: enabled, configured
   Issuer name: CN=walnutcs
   CA cert fingerprint: 800F5944 74337E5B C2DF6C52 9A7B1BDB
   Granting mode is: auto
   Last certificate issued serial number: 0x7
   CA certificate expiration timer: 22:10:29 GMT Jan 29 2007
   CRL NextUpdate timer: 21:50:56 GMT Mar 5 2004
   Current storage dir: nvram:
   Database Level: Minimum - no cert data written to storage
Rollover status: available for rollover
    Rollover CA cert fingerprint: 6AAF5944 74227A5B 23DF3E52 9A7F1FEF
    Rollover CA certificate expiration timer: 22:10:29 GMT Jan 29 2017
```

証明書サーバの現在の状態および設定を表示します。次の例では、証明書サーバ「routercs」にロールオーバーが設定されていることを示します。CA 自動ロールオーバー時間が発生し、ロールオーバーまたはシャドウ証明書、PKI 証明書が利用可能です。ステータスには、ロールオーバー証明書フィンガープリントおよびロールオーバー CA 証明書の失効タイマー情報が示されています。

ステップ 5 show crypto pki trustpoints

例：

```
Device# show crypto pki trustpoints

Trustpoint vpn:
   Subject Name:
   cn=Cisco SSL CA
   o=Cisco Systems
   Serial Number: 0FFEBBDC1B6F6D9D0EA7875875E4C695
   Certificate configured.
   Rollover certificate configured.
   Enrollment Protocol:
   SCEPv1, PKI Rollover
```

デバイスに設定されているトラストポイントを表示します。次の出力は、シャドウ CA 証明書が使用可能であることを示し、最後の登録操作中に報告された SCEP 機能を示します。

証明書サーバを使用するための設定例

例：特定の保管および公開場所の設定

次の例では、証明書サーバが迅速に証明書要求に応答できるように、最低限のローカル ファイル システムの設定を示します。.ser および .crl ファイルは、素早くアクセスできるようにローカルの システムの上に保管され、長時間のロギングでは、.crt ファイルのすべてのコピーがリモートの場所に公開されます。

```
crypto pki server myserver
     !Pick your database level.
     database level minimum
     !Specify a location for the .crt files that is different than the default local
   !Cisco IOS file system.
     database url crt publish http://url username user1 password secret
```

（注） .crl ファイルが非常に大きくなる場合に備えて、ローカル ファイル システムの空き容量をモニタリングする必要があります。

次の例では、重要ファイルのプライマリ保管場所、重要ファイルのシリアル番号ファイル固有の保管場所、メイン証明書サーバのデータベース ファイル、および CRL ファイルのパスワード保護されたファイル公開場所の設定を示します。

```
Device(config)# crypto pki server mycs
Device(cs-server)# database url ftp://cs-db.company.com

!
% Server database url was changed. You need to move the
% existing database to the new location.
!
Device(cs-server)# database url ser nvram:
Device(cs-server)# database url crl publish ftp://crl.company.com username myname password
 mypassword
Device(cs-server)# end
```

次の出力は、指定されたプライマリ保管場所および指定された重要ファイルの保管場所を示します。

```
Device# show

Sep  3 20:19:34.216: %SYS-5-CONFIG_I: Configured from console by user on console
Device# show crypto pki server

Certificate Server mycs:
     Status: disabled
     Server's configuration is unlocked  (enter "no shut" to lock it)
     Issuer name: CN=mycs
     CA cert fingerprint: -Not found-
     Granting mode is: manual
     Last certificate issued serial number: 0x0
     CA certificate expiration timer: 00:00:00 GMT Jan 1 1970
     CRL not present.
     Current primary storage dir: ftp://cs-db.company.com
     Current storage dir for .ser files: nvram:
     Database Level: Minimum - no cert data written to storage The following output
displays all storage and publication locations. The serial number file (.ser) is stored
 in NVRAM. The CRL file will be published to ftp://crl.company.com with a username and
password. All other critical files will be stored to the primary location,
ftp://cs-db.company.com.

Device# show running-config

   section crypto pki server
   crypto pki server mycs shutdown database url ftp://cs-db.company.com
   database url crl publish ftp://crl.company.com username myname password 7
12141C0713181F13253920
   database url ser nvram:
Device#
```

例：登録要求データベースからの登録要求の削除

次の例では、現在登録要求データベース内にある両方の登録要求と、これらの登録要求のうち 1 つがデータベースから削除された結果を示します。

例：現在登録要求データベース内にある登録要求

次の例では、現在登録要求データベース内にある登録要求を表示するために、**crypto pki server info requests** コマンドが使用されたことを示します。

```
Device# crypto pki server myserver info requests
```

```
Enrollment Request Database:
RA certificate requests:
ReqID    State      Fingerprint                                SubjectName
--------------------------------------------------------------------------
Router certificates requests:
ReqID    State      Fingerprint                                SubjectName
--------------------------------------------------------------------------
2        pending    1B07F3021DAAB0F19F35DA25D01D8567      hostname=host1.company.com
1        denied     5322459D2DC70B3F8EF3D03A795CF636      hostname=host2.company.com
```

例：crypto pki server remove コマンドを使用して 1 つの登録要求を削除する

次の例では、**crypto pki server remove** コマンドを使用して、登録要求 1 が削除されたことを示します。

```
Device# crypto pki server myserver remove 1
```

例：登録要求を 1 つ削除した後の登録要求データベース

次の例では、登録要求データベースから登録要求 1 を削除した結果を示します。

```
Device# crypto pki server mycs info requests

Enrollment Request Database:
RA certificate requests:
ReqID    State     Fingerprint                        SubjectName
--------------------------------------------------------------------
Router certificates requests:
ReqID    State     Fingerprint                        SubjectName
--------------------------------------------------------------------
2        pending   1B07F3021DAAB0F19F35DA25D01D8567   hostname=host1.company.com
```

例：証明書サーバのルート キーの自動アーカイブ化

次の出力設定および例では、**database archive** コマンドを設定していない（つまりデフォルト値を使用して設定した）場合、パスワードを設定せずに **database archive** コマンドを設定して CA 証明書および CA キーアーカイブ形式を PEM にする場合、およびパスワードを設定して **database archive** コマンドを設定し、CA 証明書および CA キーアーカイブ形式を PKCS12 にする場合の表示内容を示します。最後の例は、PEM 形式のアーカイブ ファイルのサンプル内容です。次の例の「ms2」は 2048 ビット キー ペアのラベルを示します。

例：database archive コマンド未設定

（注） デフォルトは PKCS12 です。**no shutdown** コマンドを発行すると、パスワードの入力を求めるプロンプトが表示されます。

```
Device(config)# crypto pki server ms2
Device(cs-server)# no shutdown

% Ready to generate the CA certificate.
%Some server settings cannot be changed after CA certificate generation.
```

```
Are you sure you want to do this? [yes/no]: y
% Exporting Certificate Server signing certificate and keys...
! Note the next two lines, which are asking for a password.
% Please enter a passphrase to protect the private key.
Password:
% Certificate Server enabled.
Device(cs-server)# end
Device# dir nvram:

Directory of nvram:/
  125  -rw-        1693              <no date>  startup-config
  126  ----           5              <no date>  private-config
    1  -rw-          32              <no date>  myserver.ser
    2  -rw-         214              <no date>  myserver.crl
! Note the next line, which indicates PKCS12 format.
    3  -rw-        1499              <no date>  myserver.p12
```

例：database archive コマンドおよび pem キーワードを設定

（注） **no shutdown** コマンドを発行すると、パスワードの入力を求めるプロンプトが表示されます。

```
Device(config)# crypto pki server ms2
Device(cs-server)# database archive pem
Device(cs-server)# no shutdown

% Ready to generate the CA certificate.
%Some server settings cannot be changed after CA certificate generation.
Are you sure you want to do this? [yes/no]: y
% Exporting Certificate Server signing certificate and keys...
!Note the next two lines, which are asking for a password.
% Please enter a passphrase to protect the private key.
Password:
% Certificate Server enabled.
Device(cs-server)# end
Device# dir nvram

Directory of nvram:/
  125  -rw-        1693            <no date>  startup-config
  126  ----           5            <no date>  private-config
    1  -rw-          32            <no date>  myserver.ser
    2  -rw-         214            <no date>  myserver.crl
! Note the next line showing that the format is PEM.
    3  -rw-        1705            <no date>  myserver.pem
```

例：database archive コマンドおよび pkcs12 キーワード（およびパスワード）を設定

（注） パスワードは、入力されると暗号化されます。ただし、アーカイブが完了したら、設定からパスワードを削除することを推奨します。

```
Device(config)# crypto pki server ms2
Device(cs-server)# database archive pkcs12 password cisco123
Device(cs-server)# no shutdown
```

```
% Ready to generate the CA certificate.
% Some server settings cannot be changed after CA certificate generation.
Are you sure you want to do this? [yes/no]: y
% Exporting Certificate Server signing certificate and keys...
! Note that you are not being prompted for a password.
% Certificate Server enabled.
Device(cs-server)# end
Device# dir nvram:

Directory of nvram:/
   125   -rw-         1693            <no date>   startup-config
   126   ----            5            <no date>   private-config
     1   -rw-           32            <no date>   myserver.ser
     2   -rw-          214            <no date>   myserver.crl
! Note that the next line indicates that the format is PKCS12.
     3   -rw-         1499            <no date>   myserver.p12
```

例：PEM フォーマットのアーカイブ

次のサンプル出力は、自動アーカイブがPEMファイル形式で設定されたことを示します。アーカイブは、CA 証明書と CA 秘密キーから成ります。バックアップを使用して証明書サーバを復元するには、PEM 形式の CA 証明書と CA キーを別々にインポートする必要があります。

（注） CA 証明書および CA キー アーカイブ ファイル以外にも、シリアル番号ファイル（.ser）および CRL ファイル（.crl）を定期的にバックアップする必要があります。証明書サーバを復元する必要がある場合、CA 運用においてシリアル ファイルおよび CRL ファイルは重要です。

```
Device# more nvram:mycs.pem

-----BEGIN CERTIFICATE-----
MIIB9zCCAWCgAwIBAgIBATANBgkqhkiG9w0BAQQFADAPMQ0wCwYDVQQDEwRteWNz
MB4XDTA0MDgyNzAyMzI0NloXDTA3MDgyNzAyMzI0NlowDzENMAsGA1UEAxMEbXlj
czCBnzANBgkqhkiG9w0BAQEFAAOBjQAwgYkCgYEA1lZpKP4nGDJHgPkpYSkix7lD
nr23aMlZ9Kz5oo/qTBxeZ8mujpjYcZ0T8AZvoOiCuDnYMl796ZwpkMgjz1aZZbL+
BtuVvllsEOfhC+u/Ol/vxfGG5xpshoz/F5J3xdg5ZZuWWuIDAUYu9+QbI5feuG04
Z/BiPIb4AmGTP4B2MM0CAwEAAaNjMGEwDwYDVR0TAQH/BAUwAwEB/zAOBgNVHQ8B
Af8EBAMCAYYwHwYDVR0jBBgwFoAUKi/cuK6wkz+ZswVtb06vUJboEeEwHQYDVR0O
BBYEFCov3LiusJM/mbMFbW9Or1CW6BHhMA0GCSqGSIb3DQEBBAUAA4GBAKLOmoE2
4+NeOKEXMCXG1jcohK7O2HrkFfl/vpK0+q92PTnMUFhxLOqI8pWIq5CCgC7heace
OrTv2zcUAoH4rzx3Rc2USIxkDokWWQMLujsMm/SLIeHit0G5uj//GCcbgK20MAW6
ymf7+TmblSFljWzstoUXC2hLnsJIMq/KffaD
-----END CERTIFICATE-----

!The private key is protected by the password that is
configured in “database archive pem password pwd” or that
is entered when you are prompted for the password.
-----BEGIN RSA PRIVATE KEY-----
Proc-Type: 4,ENCRYPTED
DEK-Info: DES-EDE3-CBC,106CE91FFD0A075E

zyiFC8rKv8Cs+IKsQG2QpsVpvDBHqZqBSM4D528bvZv7jzr6WuHj8E6zO+6G8R/A
zjsfTALo+e+ZDg7KMzbryHARvjskbqFdOMLlVIYBhCeSElKsskWB6chOuyPHJInW
JwC5YzZdZwOqcyLBP/xOYXcvjzzNfPAXZzN12VR8vWDNq/kHT+3Lplc8hY++ABMI
M+C9FB3dpNZzu5O1BZCJg46bqbkulaCCmScIDaVt0zDFZwWTSufiemmNxZBG4xS8
t5t+FEhmSfv8DAmwg4f/KVRFTm10phUArcLxQO38Al0W5YHHORdACnuzVUvHgco7
VT4XUTjO7qMhmJgFNWy1pu49fbdS2NnOn5IoiyAq5lk1KUPrz/WABWiCvLMylGnZ
kyMCWoaMtgS/vdx74BBCj09yRZJnLMlIi6SDofjCNTDHfmFEVg4LsSWCd4lP9OP8
```

```
0MqhP1D5VIx6PbMNwkWW12lpBbCCdesFRGHjZD2dOu96kHD7ItErx34CC8W04aG4
b7DLktUu6WNV6M8g3CAqJiC0V8ATlp+kvdHZVkXovgND5IU0OJpsj0HhGzKAGpOY
KTGTUekUboISjVVkI6efp1vO6temVL3Txg3KGhzWMJGrq1snghE0KnV8tkddv/9N
d/t1l+we9mrccTq50WNDnkEi/cwHI/0PKXg+NDNH3k3QGpAprsqGQmMPdqc5ut0P
86i4cF9078QwWg4Tpay3uqNH1Zz6UN0tcarVVNmDupFESUxYw10qJrrEYVRadu74
rKAU4Ey4xkAftB2kuqvr21Av/L+jne4kkGIoZYdB+p/M98pQRgkYyg==
-----END RSA PRIVATE KEY-----
```

例：証明書サーバ バックアップ ファイルからの証明書サーバの復元

次の例は、PKCS12アーカイブから復元され、データベースURLがNVRAM（デフォルト）であることを示します。

```
Device# copy tftp://192.0.2.71/backup.ser nvram:mycs.ser

Destination filename [mycs.ser]?
32 bytes copied in 1.320 secs (24 bytes/sec)

Device# copy tftp://192.0.2.71/backup.crl nvram:mycs.crl

Destination filename [mycs.crl]?
214 bytes copied in 1.324 secs (162 bytes/sec)

Device# configure terminal
Device(config)# crypto pki import mycs pkcs12 tftp://192.0.2.71/backup.p12 cisco123

Source filename [backup.p12]?
CRYPTO_PKI: Imported PKCS12 file successfully.

Device(config)# crypto pki server mycs
! fill in any certificate server configuration here

Device(cs-server)# no shutdown
% Certificate Server enabled.

Device(cs-server)# end
Device# show crypto pki server

Certificate Server mycs:
    Status: enabled
    Server's current state: enabled
    Issuer name: CN=mycs
    CA cert fingerprint: 34885330 B13EAD45 196DA461 B43E813F
    Granting mode is: manual
    Last certificate issued serial number: 0x1
    CA certificate expiration timer: 01:49:13 GMT Aug 28 2007
    CRL NextUpdate timer: 01:49:16 GMT Sep 4 2004
    Current storage dir: nvram:
    Database Level: Minimum - no cert data written to storage
```

次の例は、PEMアーカイブから復元され、データベースURLがflashであることを示します。

```
Device# copy tftp://192.0.2.71/backup.ser flash:mycs.ser

Destination filename [mycs.ser]?
32 bytes copied in 1.320 secs (24 bytes/sec)
Router# copy tftp://192.0.2.71/backup.crl flash:mycs.crl
Destination filename [mycs.crl]?
214 bytes copied in 1.324 secs (162 bytes/sec)
Device# configure terminal
```

```
! Because CA cert has Digital Signature usage, you need to import using the "usage-keys"
 keyword

Device(config)# crypto ca import mycs pem usage-keys terminal cisco123
% Enter PEM-formatted CA certificate.
% End with a blank line or "quit" on a line by itself.
! Paste the CA cert from .pem archive.
-----BEGIN CERTIFICATE-----
MIIB9zCCAWCgAwIBAgIBATANBgkqhkiG9w0BAQQFADAPMQ0wCwYDVQQDEwRteWNz
MB4XDTA0MDkwMjIxMDI1NloXDTA3MDkwMjIxMDI1NlowDzENMAsGA1UEAxMEbXlj
czCBnzANBgkqhkiG9w0BAQEFAAOBjQAwgYkCgYEAuGnnDXJbpDDQwCuKGs5Zg2rc
K7ZJauSUotTmWYQvNx+ZmWrUs5/j9Ee5FV2YonirGBQ9mc6u163kNlrIPFck062L
GpahBhNmKDgod1o2PHTnRlZpEZNDIqU2D3hACgByxPjrY4vUnccV36ewLnQnYpp8
szEu7PYTJr5dU5ltAekCAwEAAaNjMGEwDwYDVR0TAQH/BAUwAwEB/zAOBgNVHQ8B
Af8EBAMCAYYwHwYDVR0jBBgwFoAUaEEQwYKCQ1dm9+wLYBKRTlzxaDIwHQYDVR0O
BBYEFGhBEMGCgkNXZvfsC2ASkU5c8WgyMA0GCSqGSIb3DQEBBAUAA4GBAHyhiv2C
mH+vswkBjRA1Fzzk8ttu9s5kwqG0dXp25QRUWsGlr9nsKPNdVKt3P7p0A/KochHe
eNiygiv+hDQ3FVnzsNv983le6O5jvAPxc17RO1BbfNhqvEWMsXdnjHOcUy7XerCo
+bdPcUf/eCiZueH/BEy/SZhD7yovzn2cdzBN
-----END CERTIFICATE-----
% Enter PEM-formatted encrypted private SIGNATURE key.
% End with "quit" on a line by itself.
! Paste the CA private key from .pem archive.
-----BEGIN RSA PRIVATE KEY-----
Proc-Type: 4,ENCRYPTED
DEK-Info: DES-EDE3-CBC,5053DC842B04612A

1CnlF5Pqvd0zp2NLZ7iosxzTy6nDeXPpNyJpxB5q+V29IuY8Apb6TlJCU7YrsEB/
nBTK7K76DCeGPlLpcuyEI171QmkQJ2gA0QhC0LrRo09WrINVH+b4So/y7nffZkVb
p2yDpZwqoJ8cmRH94Tie0YmzBtEh6ayOud11z53qbrsCnfSEwszt1xrW1MKrFZrk
/fTy6loHzGFzl3BDj4r5gBecExwcPp74ldHO+Ld4Nc9egG8BYkeBCsZZOQNVhXLN
I0tODOs6hP915zb6OrZFYv0NK6grTBO9D8hjNZ3U79jJzsSP7UNzIYHNTzRJiAyu
i56Oy/iHvkCSNUIK6zeIJQnW4bSoM1BqrbVPwHU6QaXUqlNzZ8SDtw7ZRZ/rHuiD
RTJMPbKquAzeuBss1132OaAUJRStjPXgyZTUbc+cWb6zATNws2yijPDTR6sRHoQL
47wHMr2Yj80VZGgkCSLAkL88ACz9TfUiVFhtfl6xMC2yuFl+WRk1XfF5VtWe5Zer
3Fn1DcBmlF7O86XUkiSHP4EV0cI6n5ZMzVLx0XAUtdAl1gD94y1V+6p9PcQHLyQA
pGRmj5IlSFw90aLafgCTbRbmC0ChIqHy91UFa1ub0130+yu7LsLGRlPmJ9NE61JR
bjRhlUXItRYWY7C4M3m/0wz6fmVQNSumJM08RHq6lUB3olzIgGIZlZkoaESrLG0p
qq2AENFemCPF0uhyVS2humMHjWuRr+jedfc/IMl7sLEgAdqCVCfV3RZVEaNXBud1
4QjkuTrwaTcRXVFbtrVioT/puyVUlpA7+k7w+F5TZwUV08mwvUEqDw==
-----END RSA PRIVATE KEY-----
quit
% Enter PEM-formatted SIGNATURE certificate.
% End with a blank line or "quit" on a line by itself.
! Paste the CA cert from .pem archive again.
-----BEGIN CERTIFICATE-----
MIIB9zCCAWCgAwIBAgIBATANBgkqhkiG9w0BAQQFADAPMQ0wCwYDVQQDEwRteWNz
MB4XDTA0MDkwMjIxMDI1NloXDTA3MDkwMjIxMDI1NlowDzENMAsGA1UEAxMEbXlj
czCBnzANBgkqhkiG9w0BAQEFAAOBjQAwgYkCgYEAuGnnDXJbpDDQwCuKGs5Zg2rc
K7ZJauSUotTmWYQvNx+ZmWrUs5/j9Ee5FV2YonirGBQ9mc6u163kNlrIPFck062L
GpahBhNmKDgod1o2PHTnRlZpEZNDIqU2D3hACgByxPjrY4vUnccV36ewLnQnYpp8
szEu7PYTJr5dU5ltAekCAwEAAaNjMGEwDwYDVR0TAQH/BAUwAwEB/zAOBgNVHQ8B
Af8EBAMCAYYwHwYDVR0jBBgwFoAUaEEQwYKCQ1dm9+wLYBKRTlzxaDIwHQYDVR0O
BBYEFGhBEMGCgkNXZvfsC2ASkU5c8WgyMA0GCSqGSIb3DQEBBAUAA4GBAHyhiv2C
mH+vswkBjRA1Fzzk8ttu9s5kwqG0dXp25QRUWsGlr9nsKPNdVKt3P7p0A/KochHe
eNiygiv+hDQ3FVnzsNv983le6O5jvAPxc17RO1BbfNhqvEWMsXdnjHOcUy7XerCo
+bdPcUf/eCiZueH/BEy/SZhD7yovzn2cdzBN
-----END CERTIFICATE-----

% Enter PEM-formatted encrypted private ENCRYPTION key.
% End with "quit" on a line by itself.
! Because the CA cert only has Digital Signature usage, skip the encryption part.
quit
```

```
% PEM files import succeeded.
Device(config)# crypto pki server mycs
Device(cs-server)# database url flash:

! Fill in any certificate server configuration here.
Device(cs-server)# no shutdown

% Certificate Server enabled.
Device(cs-server)# end
Device# show crypto pki server

Certificate Server mycs:
    Status: enabled
    Server's current state: enabled
    Issuer name: CN=mycs
    CA cert fingerprint: F04C2B75 E0243FBC 19806219 B1D77412
    Granting mode is: manual
    Last certificate issued serial number: 0x2
    CA certificate expiration timer: 21:02:55 GMT Sep 2 2007
    CRL NextUpdate timer: 21:02:58 GMT Sep 9 2004
    Current storage dir: flash:
    Database Level: Minimum - no cert data written to storage
```

例：下位証明書サーバ

次の設定および出力は、下位の証明書サーバを設定した後で、通常表示されるものです。「ms2」は前述の手順で生成した 2048 ビット RSA キーを表します。

```
Device(config)# crypto pki trustpoint sub
Device(ca-trustpoint)# enrollment url http://192.0.2.6
Device(ca-trustpoint)# rsa keypair ms2 2048
Device(ca-trustpoint)# exit
Device(config)# crypto pki server sub
Device(cs-server)# mode sub-cs
Device(ca-server)# no shutdown

%Some server settings cannot be changed after CA certificate generation.
% Please enter a passphrase to protect the private key
% or type Return to exit
Password:
Jan  6 22:32:22.698: CRYPTO_CS: enter FSM: input state initial, input signal no shut
Re-enter password:
Jan  6 22:32:30.302: CRYPTO_CS: starting enabling checks
Jan  6 22:32:30.306: CRYPTO_CS: key 'sub' does not exist; generated automatically [OK]
Jan  6 22:32:39.810: %SSH-5-ENABLED: SSH 1.99 has been enabled
Certificate has the following attributes:
     Fingerprint MD5: 328ACC02 52B25DB8 22F8F104 B6055B5B
     Fingerprint SHA1: 02FD799D DD40C7A8 61DC53AB 1E89A3EA 2A729EE2
% Do you accept this certificate? [yes/no]:
Jan  6 22:32:44.830: CRYPTO_CS: nvram filesystem
Jan  6 22:32:44.922: CRYPTO_CS: serial number 0x1 written.
Jan  6 22:32:46.798: CRYPTO_CS: created a new serial file.
Jan  6 22:32:46.798: CRYPTO_CS: authenticating the CA 'sub'y
Trustpoint CA certificate accepted.%
% Certificate request sent to Certificate Authority
% Enrollment in progress...
Router (cs-server)#
Jan  6 22:33:30.562: CRYPTO_CS: Publishing 213 bytes to crl file nvram:sub.crl
Jan  6 22:33:32.450: CRYPTO_CS: enrolling the server's trustpoint 'sub'
Jan  6 22:33:32.454: CRYPTO_CS: exit FSM: new state check failed
Jan  6 22:33:32.454: CRYPTO_CS: cs config has been locked
```

```
Jan  6 22:33:33.118: CRYPTO_PKI:  Certificate Request Fingerprint MD5: CED89E5F 53B9C60E

> AA123413 CDDAD964
Jan  6 22:33:33.118: CRYPTO_PKI:  Certificate Request Fingerprint SHA1: 70787C76 ACD7E67F
 7D2C8B23 98CB10E7 718E84B1
% Exporting Certificate Server signing certificate and keys...
Jan  6 22:34:53.839: %PKI-6-CERTRET: Certificate received from Certificate Authority
Jan  6 22:34:53.843: CRYPTO_CS: enter FSM: input state check failed, input signal cert
configured
Jan  6 22:34:53.843: CRYPTO_CS: starting enabling checks
Jan  6 22:34:53.843: CRYPTO_CS: nvram filesystem
Jan  6 22:34:53.883: CRYPTO_CS: found existing serial file.
Jan  6 22:34:53.907: CRYPTO_CS: old router cert flag 0x4
Jan  6 22:34:53.907: CRYPTO_CS: new router cert flag 0x44
Jan  6 22:34:56.511: CRYPTO_CS: DB version
Jan  6 22:34:56.511: CRYPTO_CS: last issued serial number is 0x1
Jan  6 22:34:56.551: CRYPTO_CS: CRL file sub.crl exists.
Jan  6 22:34:56.551: CRYPTO_CS: Read 213 bytes from crl file sub.crl.
Jan  6 22:34:56.603: CRYPTO_CS: SCEP server started
Jan  6 22:34:56.603: CRYPTO_CS: exit FSM: new state enabled
Jan  6 22:34:56.603: CRYPTO_CS: cs config has been locked
Jan  6 22:35:02.359: CRYPTO_CS: enter FSM: input state enabled, input signal time set
Jan  6 22:35:02.359: CRYPTO_CS: exit FSM: new state enabled
Jan  6 22:35:02.359: CRYPTO_CS: cs config has been locked
```

例：ルート証明書サーバの区別

証明書を発行するとき、ルート証明書サーバ（親の下位証明書サーバ）は、次のサンプル出力に示すように、証明書要求を「Sub CA」、「RA」およびピアの各要求に区別します。

```
Device# crypto pki server server1 info req

Enrollment Request Database:
RA certificate requests:
ReqID     State        Fingerprint                                SubjectName
--------------------------------------------------------------------------------
Subordinate CS certificate requests:
ReqID     State        Fingerprint                                SubjectName
--------------------------------------------------------------------------------
1     pending        CB9977AD8A73B146D3221749999B0F66 hostname=host-subcs.company.com
RA certificate requests:
ReqID     State        Fingerprint                                 SubjectName
--------------------------------------------------------------------------------
Router certificate requests:
ReqID     State        Fingerprint                                 SubjectName
--------------------------------------------------------------------------------
```

例：下位証明書サーバの出力表示

次の **show crypto pki server command** 出力は、下位の証明書サーバーが設定されたことを示しています。

```
Device# show crypto pki server

Certificate Server sub:
  Status: enabled
  Server's configuration is locked  (enter "shut" to unlock it)
  Issuer name: CN=sub
  CA cert fingerprint: 11B586EE 3B354F33 14A25DDD 7BD39187
  Server configured in subordinate server mode
  Upper CA cert fingerprint: 328ACC02 52B25DB8 22F8F104 B6055B5B
```

```
  Granting mode is: manual
  Last certificate issued serial number: 0x1
  CA certificate expiration timer: 22:33:44 GMT Jan 6 2006
  CRL NextUpdate timer: 22:33:29 GMT Jan 13 2005
  Current storage dir: nvram:
  Database Level: Minimum - no cert data written to storage
```

例：RA モード証明書サーバ

次の出力は、RA モード証明書サーバの設定後に、通常表示される内容です。

```
Device-ra(config)# crypto pki trustpoint myra
Device-ra(ca-trustpoint)# enrollment url http://192.0.2.17
! Include "cn=ioscs RA" or "ou=ioscs RA" in the subject-name.
Device-ra(ca-trustpoint)# subject-name cn=myra, ou=ioscs RA, o=company, c=us
Device-ra(ca-trustpoint)# exit
Device-ra(config)# crypto pki server myra
Device-ra(cs-server)# mode ra
Device-ra(cs-server)# no shutdown

% Generating 1024 bit RSA keys ...[OK]
Certificate has the following attributes:
Fingerprint MD5: 32661452 0DDA3CE5 8723B469 09AB9E85
Fingerprint SHA1: 9785BBCD 6C67D27C C950E8D0 718C7A14 C0FE9C38
% Do you accept this certificate? [yes/no]: yes
Trustpoint CA certificate accepted.
% Ready to request the CA certificate.
%Some server settings cannot be changed after the CA certificate has been requested.
Are you sure you want to do this? [yes/no]: yes
%
% Start certificate enrollment ..
% Create a challenge password. You will need to verbally provide this
   password to the CA administrator in order to revoke your certificate.
   For security reasons your password will not be saved in the configuration.
   Please make a note of it.
Password:
Re-enter password:
% The subject name in the certificate will include: cn=myra, ou=ioscs RA, o=company,
c=us
% The subject name in the certificate will include: Router-ra.company.com
% Include the router serial number in the subject name? [yes/no]: no
% Include an IP address in the subject name? [no]: no
Request certificate from CA? [yes/no]: yes
% Certificate request sent to Certificate Authority
% The certificate request fingerprint will be displayed.
% The 'show crypto pki certificate' command will also show the fingerprint.
% Enrollment in progress...
Device-ra (cs-server)#

Sep 15 22:32:40.197: CRYPTO_PKI:  Certificate Request Fingerprint MD5: 82B41A76 AF4EC87D
 AAF093CD 07747D3A
Sep 15 22:32:40.201: CRYPTO_PKI:  Certificate Request Fingerprint SHA1: 897CDF40 C6563EAA
 0FED05F7 0115FD3A 4FFC5231
Sep 15 22:34:00.366: %PKI-6-CERTRET: Certificate received from Certificate Authority

Device-ra(cs-server)# end
Device-ra# show crypto pki server

Certificate Server myra:
    Status: enabled
    Issuer name: CN=myra
```

```
    CA cert fingerprint: 32661452 0DDA3CE5 8723B469 09AB9E85
    ! Note that the certificate server is running in RA mode
    Server configured in RA mode
    RA cert fingerprint: C65F5724 0E63B3CC BE7AE016 BE0D34FE
    Granting mode is: manual
    Current storage dir: nvram:
    Database Level: Minimum - no cert data written to storage
```

次の出力は、RA がイネーブルになった後の、発行元証明書サーバの登録要求データベースを示します。

（注） 所有者名に「ou=ioscs RA」が表示されていることから、RA 証明書要求は発行元証明書サーバによって認識されています。

```
Device-ca# crypto pki server mycs info request

Enrollment Request Database:
Subordinate CA certificate requests:
ReqID  State      Fingerprint                      SubjectName
--------------------------------------------------------------
! The request is identified as RA certificate request.
RA certificate requests:
ReqID  State      Fingerprint                      SubjectName
--------------------------------------------------------------
12     pending    88F547A407FA0C90F97CDE8900A30CB0
hostname=Router-ra.company.com,cn=myra,ou=ioscs RA,o=company,c=us
Router certificates requests:
ReqID   State     Fingerprint                      SubjectName
--------------------------------------------------------------
! Issue the RA certificate.
Device-ca# crypto pki server mycs grant 12
```

次の出力は、要求が RA から出された場合に、発行元証明書サーバが自動的に証明書を発行するように設定されていることを示します。

```
Device-ca(config)# crypto pki server mycs
Device-ca(cs-server)# grant ra-auto

% This will cause all certificate requests already authorized by known RAs to be
automatically granted.
Are you sure you want to do this? [yes/no]: yes
Router-ca (cs-server)# end
Device-ca# show crypto pki server

Certificate Server mycs:
    Status: enabled
    Server's current state: enabled
    Issuer name: CN=mycs
    CA cert fingerprint: 32661452 0DDA3CE5 8723B469 09AB9E85
    ! Note that the certificate server will issue certificate for requests from the RA.
    Granting mode is: auto for RA-authorized requests, manual otherwise
    Last certificate issued serial number: 0x2
    CA certificate expiration timer: 22:29:37 GMT Sep 15 2007
    CRL NextUpdate timer: 22:29:39 GMT Sep 22 2004
    Current storage dir: nvram:
    Database Level: Minimum - no cert data written to storage
```

次の例は、「myra」の設定（RA サーバ）が自動ロールオーバーを「myca」（CA）からサポートするように設定されていることを示します。RA サーバが設定されると、証明書再登録要求の自動許可がイネーブルになります。

```
crypto pki trustpoint myra
 enrollment url
http://myca
 subject-name ou=iosca RA
 rsakeypair myra
crypto pki server myra
 mode ra
 auto-rollover
crypto pki server mycs
 grant auto rollover ra-cert
 auto-rollover 25
```

例：CA 証明書ロールオーバーを有効にしてただちに開始する

次の例では、**crypto pki server** コマンドを使用して、サーバー mycs の自動 CA 証明書ロールオーバーをイネーブルにする方法を示します。**show crypto pki server** コマンドを実行すると、mycs サーバーの現在の状態と、ロールオーバー証明書が現在ロールオーバーに使用可能であることが示されます。

```
Device(config)# crypto pki server mycs rollover

Jun 20 23:51:21.211:%PKI-4-NOSHADOWAUTOSAVE:Configuration was
modified.  Issue "write memory" to save new IOS CA certificate
! The config has not been automatically saved because the config has been changed.
Device# show crypto pki server

Certificate Server mycs:
    Status:enabled
    Server's configuration is locked  (enter "shut" to unlock it)
    Issuer name:CN=mycs
    CA cert fingerprint:E7A5FABA 5D7AA26C F2A9F7B3 03CE229A
    Granting mode is:manual
    Last certificate issued serial number:0x2
    CA certificate expiration timer:00:49:26 PDT Jun 20 2008
    CRL NextUpdate timer:00:49:29 PDT Jun 28 2005
    Current storage dir:nvram:
    Database Level:Minimum - no cert data written to storage
    Rollover status:available for rollover
    ! Rollover certificate is available for rollover.
    Rollover CA certificate fingerprint:9BD7A443 00A6DD74 E4D9ED5F B7931BE0
    Rollover CA certificate expiration time:00:49:26 PDT Jun 20 2011
    Auto-Rollover configured, overlap period 25 days
```

次の作業

証明書サーバが正常に実行されたら、登録元クライアントを手動のメカニズムによって（「*PKI* の証明書登録の設定」の説明に従って）開始する、または Web ベースの登録インターフェイスである SDP の設定を（「*Setting Up Secure Device Provisioning (SDP) for Enrollment in a PKI*」の説明に従って）開始できます。

PKI 展開での 証明書サーバの設定および管理に関する追加資料

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『Cisco IOS Master Commands List, All Releases』
PKI およびセキュリティ コマンド	• 『Cisco IOS Security Command Reference: Commands A to C』 • 『Cisco IOS Security Command Reference Commands D to L』 • 『Cisco IOS Security Command Reference Commands M to R』 • 『Cisco IOS Security Command Reference Commands S to Z』
USB トークンによる RSA 処理：初期の自動登録用の USB トークンにおける RSA キーの使用	「*PKI* の証明書登録の設定」
USB トークンによる RSA 処理：USB トークンを使用するメリット	「*PKI* クレデンシャルの保存」
証明書サーバ クライアント証明書の登録、自動登録、および自動ロールオーバー	「*PKI* の証明書登録の設定」
USB トークンの設定およびUSB トークンへのロギング	「*PKI* クレデンシャルの保存」
Web を使用した証明書登録	「*Setting Up Secure Device Provisioning (SDP) for Enrollment in a PKI*」
PEM 形式ファイル内の RSA キー	「*PKI* 内での *RSA* キーの展開」
証明書失効メカニズムの選択	「*PKI* での証明書の許可および失効の設定」
推奨される暗号化アルゴリズム	『Next Generation Encryption』

シスコのテクニカル サポート

説明	リンク
右の URL にアクセスして、シスコのテクニカル サポートを最大限に活用してください。これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

PKI 展開での 証明書サーバの設定および管理に関する機能情報

第 115 章

PKI クレデンシャルの保存

Rivest、Shamir、Adelman（RSA）キーと証明書などの公開キー インフラストラクチャ（PKI）は、NVRAM やフラッシュ メモリなどのルータまたは USB eTtoken 64 KB スマート カード上の特定の場所に保存できます。USB トークンを使用すると、セキュアな設定配布や、トークン上のキー生成、署名、認証などの RSA 処理、配置のためのバーチャル プライベート ネットワーク（VPN）クレデンシャルを USB トークンのストレージが提供されます。

PKI クレデンシャルを保存するための前提条件

ローカル証明書の保管場所を指定するための前提条件

ローカル証明書の保管場所を指定するためには、ご使用のシステムが次の要件を満たしている必要があります。

- Cisco IOS Release 12.4(2)T PKI 対応イメージまたはそれ以降のイメージ
- PKI クレデンシャルを個別のファイルとして保存できるプラットフォームであること。
- 設定内に証明書が少なくとも 1 つ含まれていること。
- アクセス可能なローカル ファイル システムがあること。

PKI クレデンシャルの保管場所として USB トークンを指定するための前提条件

USB トークンを使用するためには、ご使用のシステムが次の要件を満たしている必要があります。

- Cisco 871 ルータ、Cisco 1800 シリーズ ルータ、Cisco 2800 シリーズ ルータ、Cisco 3800 シリーズ ルータ、または Cisco 7200VXR NPE-G2 プラットフォームを使用していること。
- サポートされているいずれかのプラットフォーム上で、少なくとも Cisco IOS Release 12.3(14)T イメージが稼働していること。
- シスコのサポート対象 USB トークン（Safenet/Aladdin eToken PRO 32 KB または 64 KB）
- k9 イメージを使用していること。

PKI クレデンシャルの保存に関する制約事項

ローカル証明書の保管場所を指定する場合の制約事項

証明書をローカルな保管場所に保存する場合には、次のような制約事項があります。

- 使用できるのはローカル ファイル システムだけです。リモート ファイル システムを選択すると、エラー メッセージが表示され、コマンドは無効になります。
- ローカルファイルシステムでサポートされていれば、サブディレクトリを指定できます。NVRAM では、サブディレクトリはサポートされていません。

保管場所として USB トークンを指定する場合の制約事項

USB トークンを使用して PKI データを保存する場合には、次のような制約事項があります。

- USB トークンがサポートされるためには、ファイルをセキュアに保存できる 3DES（k9）Cisco IOS ソフトウェア イメージが必要です。
- イメージは USB トークンからは起動できません（ただし、設定は USB トークンからでも起動できます）。
- USBハブは現在、サポートされていません。そのため、サポートされるデバイスの数は、多くても使用できる USB ポートの数までです。

PKI クレデンシャルの保存について

ローカルな保管場所への証明書の保存

デフォルトでは、証明書はNVRAMに格納されます。ただし、ルータによっては、証明書を正常に保存するために必要なサイズの NVRAM が搭載されていないことがあります。

シスコのプラットフォームはすべて、NVRAMおよびフラッシュ ローカル ストレージをサポートしています。ご使用のプラットフォームによっては、ブートフラッシュ、スロット、ディス

ク、USB フラッシュ、USB トークンなど、サポートされているその他のローカル ストレージを使用できます。

実行時には、証明書を保存するアクティブなローカル ストレージ デバイスを指定できます。

PKI クレデンシャルと USB トークン

ご使用のルータ上でセキュアな USB トークンを使用するためには、次に説明する事柄について十分な知識が必要です。

USB トークンの動作のしくみ

スマートカードはプラスティック製の小型カードで、データの保存や処理を行うためのマイクロプロセッサやメモリが搭載されています。USB インターフェイスを備えたスマート カードが USB トークンです。USB トークンでは、記憶域の容量（32KB）内であれば、どのようなタイプのファイルでもセキュアに保存できます。USB トークンに保存されたコンフィギュレーション ファイルに対する暗号化およびアクセスは、ユーザ PIN を介してだけ行えます。デバイスにコンフィギュレーションファイルをロードするには、デバイスのコンフィギュレーション ファイルをセキュアに配布できるよう適切な PIN が設定されている必要があります。

USB トークンをデバイスに装着したら、その USB トークンにログインする必要があります。ログイン後は、ユーザ PIN（デフォルトは 1234567890）や、ログインが拒否されるようになるまで許容されるログイン試行の失敗回数（デフォルトは 15 回）など、さまざまなデフォルト設定を変更できます。USB トークンのアクセス方法および設定方法については、「USB トークンへのログインと USB トークンの設定」を参照してください。

USB トークンへ正常にログインした場合は、**copy** コマンドを使用して、デバイスから USB トークンへファイルをコピーできます。USB トークンの RSA キーおよび関連する IPsec トンネルは、デバイスがリロードされるまで使用できます。キーが削除され IPsec トンネルが切断されるまでの時間を指定する場合は、**crypto pki token removal timeout** コマンドを発行します。デフォルト タイムアウトはゼロのため、eToken がデバイスから削除されると RSA キーが自動的に削除されるようになります。デフォルト値は、実行中のコンフィギュレーションで次のように表示されます。

```
crypto pki token default removal timeout 0
```

次の表に、USB トークンの機能を示します。

表 *157 : USB* トークンの主な機能性

機能	USB トークン
アクセシビリティ	デジタル証明書、事前共有キー、およびデバイス設定を USB トークンからデバイスへセキュアに保存したり転送したりするためのものです。
ストレージのサイズ	32 KB または 64 KB

機能	USB トークン
ファイル タイプ	• 通常、IPsec VPN 用のデジタル証明書、事前共有キー、およびデバイス設定を保存する場合には、ファイル タイプを指定します。 • USB トークンには、Cisco IOS イメージは保存できません。
セキュリティ	• ファイルに対する暗号化およびアクセスは、ユーザ PIN を介してだけ行えます。 • ファイルは、ノンセキュアなフォーマットでも保存できます。
ブート設定	• デバイスではブート時に、USB トークンに保存されている設定を使用できます。 • デバイスではブート時に、USB トークンに保存されているセカンダリ設定を使用できます（セカンダリ設定を使用すると、ユーザは各自の IPsec 設定をロードできます）。

USB トークンの応用上の利点

Cisco ルータ上で USB トークンがサポートされていることにより、応用上次のような利点が生まれます。

移動可能な証明書：配置する VPN クレデンシャルを外部デバイスに保存できます。

USB トークンでは、スマート カード テクノロジーにより、IPsec VPN の導入に必要なデジタル証明書や設定を保存できます。これにより、ルータにおいて RSA 公開キーを生成し、少なくとも 1 つの IPsec トンネルを認証できるようになりました（ルータでは複数の IPsec トンネルを開始できるため、USB トークンには、必要に応じて複数の証明書を保存できるようになっています）。

VPN クレデンシャルを外部デバイスに保存すると、機密データが漏洩する危険性は低くなります。

ファイルをセキュアに配置するための PIN 設定

USB トークンには、ユーザが設定した PIN を介してルータにおける暗号化をイネーブルにする際に使用できるコンフィギュレーション ファイルを保存できます（つまり、デジタル証明書、事前共有キー、および VPN は使用されません）。

軽減されるまたは不要になる手動での設定作業

USB トークンを使用すると、リモート ソフトウェアの設定やプロビジョニングの際、手動で行う作業がほとんど（あるいは完全に）必要なくなります。設定は自動プロセスとして構成されます。具体的には、ルータに装着した USB トークンにブートストラップ設定を保存しておくと、そのブートストラップ設定によりルータが起動します。さらにこのルータは、ブートス

トラップ設定によって TFTP サーバへ接続され、その TFTP サーバに保存されている設定に基づいて、すべてのルータ設定が行われます。

RSA 処理

USB トークンは、ストレージ デバイス以外に、暗号化装置として使用できます。USB トークンを暗号化装置として使用すると、トークンでキー生成、署名、認証などの RSA 操作を実行できます。

ご使用のトークン ストレージ デバイス上に配置されているクレデンシャルからは、モジュラスが 2048 ビット以下の汎用 RSA キー ペア、特殊 RSA キー ペア、暗号化 RSA キー ペア、またはシグニチャ RSA キーペアを生成できます。秘密キーは、デフォルトでは配布されず、トークン上に保存されたままです。ただし、秘密キーの保管場所を設定することは可能です。

USB トークン上に常駐するキーは、生成された段階でトークンの永続的な保管場所に保存されます。キーの削除操作を行うと、トークンに保存されているキーは、永続的な保管場所からただちに削除されます（トークン上に常駐していないキーは、**write memory** またはそれに類するコマンドが発行されると、トークン以外の保管場所で保存や削除が行われます）。

セキュア デバイス プロビジョニング（SDP）環境におけるリモート デバイスの設定およびプロビジョニング

SDP は USB トークンの設定に使用される場合があります。設定された USB トークンを送付すれば、リモート ロケーションにあるデバイスをプロビジョニングできます。つまり、あるネットワーク デバイスから別のリモート ネットワーク デバイスへ暗号化された情報を送る際に USB トークンを使用することで、USB トークンを段階的に配置できます。

SDP で USB トークンを使用する方法については、「その他の関連資料」に記載されている参照先を参照してください。

PKI データの保管場所の設定方法

証明書のローカル ストレージ場所の指定

手順の概要

1. **enable**
2. **configure terminal**
3. **crypto pki certificate storage** *location-name*
4. **exit**
5. **copy** *source-url destination-url*
6. **show crypto pki certificates storage**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**crypto pki certificate storage** *location-name* 例： `Device(config)# crypto pki certificate storage flash:/certs`	証明書のローカルな保管場所を指定します。
ステップ 4	**exit** 例： `Device(config)# exit`	グローバル コンフィギュレーション モードを終了します。
ステップ 5	**copy** *source-url destination-url* 例： `Device# copy system:running-config nvram:startup-config`	（任意）実行コンフィギュレーションをスタートアップ コンフィギュレーションに保存します。 （注） 設定は、実行コンフィギュレーションがスタートアップ コンフィギュレーションに保存された場合にだけ有効になります。
ステップ 6	**show crypto pki certificates storage** 例： `Device# show crypto pki certificates storage`	（任意）PKI 証明書の保管場所に関する現在の設定を表示します。

例

次に、**show crypto pki certificates storage** コマンドの出力例を示します。ここでは、証明書が disk0 の certs サブディレクトリに保存されています。

```
Device# show crypto pki certificates storage
Certificates will be stored in disk0:/certs/
```

Cisco デバイスにおける USB トークンの設定と使用

USB トークンによる設定の保存

手順の概要

1. **enable**
2. **configure terminal**
3. **boot config** *usbtoken[0-9]:filename*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**boot config** *usbtoken[0-9]:filename* 例： `Device(config)# boot config usbtoken0:file`	スタートアップ コンフィギュレーション ファイルがセキュアなUSBトークンに保存されるよう指定します。

USB トークンへのログインと USB トークンの設定

RSA キーと USB トークンの併用方法

- RSA キーは、USB トークンがルータへ正常にログインした後にロードされます。
- デフォルトの場合、新規に生成された RSA キーは、最後に装着された USB トークンに保存されます。再生成されたキーは、元の RSA キーが生成されたのと同じ場所に保存する必要があります。

手動ログイン用のデバイスの設定

自動ログインとは異なり、手動ログインを使用する場合は、ユーザが実際のUSBトークンPINを把握している必要があります。

（注） 手動ログインまたは自動ログインのいずれかを使用する必要があります。

手動ログインは、PINをデバイス上に保存するのが適していない場合に使用できます。また、初期導入時やハードウェア交換時に、デバイスを現地の業者から調達したり、リモートサイトへ直送したりする場合にも、手動ログインが適しています。手動ログインは、権限の有無にかかわらず実行できます。また、手動ログインを実行すると、USBトークン上のファイルおよびRSAキーが、Cisco IOSソフトウェアで使用可能になります。セカンダリ コンフィギュレーション ファイルを設定する場合は、ログインを実行するユーザの権限がある場合にだけ手動ログインを実行できます。そのため、何らかの目的で、手動ログインを実行し、USBトークン上にセカンダリ コンフィギュレーション ファイルを設定する場合は、権限をイネーブルにする必要があります。

手動ログインは、失われたデバイス設定のリカバリを行う場合にも使用できます。通常VPNを使用してコア ネットワークへ接続しているリモート サイトが存在する状況では、設定およびRSAキーが失われた場合、USBトークンが備えているアウトオブバンド サービスが必要となります。USBトークンには、ブート設定、セカンダリ設定、および接続を認証するためのRSAキーを保存できます。

手順の概要

1. **enable**
2. **crypto pki token** *token-name* [**admin**] **login** [*pin*]
3. **show usbtoken** *0-9*:*filename*

手順の詳細

	コマンドまたはアクション	目的
ステップ1	**enable** 例： `Device> enable`	特権EXECモードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ2	**crypto pki token** *token-name* [**admin**] **login** [*pin*] 例： `Device# crypto pki token usbtoken0 admin login 5678`	USBトークンに手動でログインします。 **admin**キーワードを最初に指定していない場合は、このキーワードオプションで**crypto pki token**コマンドを再び入力できます。
ステップ3	**show usbtoken** *0-9*:*filename* 例： `Device# show usbtoken0:usbfile`	（任意）USBトークンがデバイスにログインしているかどうかを確認します。

次の作業

USBトークンへのログインが完了すると、次のような作業が行えます。

- USBトークンを詳細に設定する。「USBトークンの設定」の項を参照してください。

- ユーザ PIN の変更、ルータから USB トークンに設定されたキーの保管場所へのファイルのコピー、USB トークンの変更など、USB トークンの管理作業を行う。「USB トークンにおける管理機能の設定」の項を参照してください。

USB トークンの設定

USB トークンに対しては、自動ログインの設定後、さらに次のような設定を行えます。

PIN およびパスフレーズ

自動ログインにおける PIN のセキュリティをさらに強化するため、NVRAM に保存されている PIN を暗号化し、USB トークンにパスフレーズを設定できます。パスフレーズを設定すると、他のユーザには PIN そのものではなく、そのパスフレーズを周知すればよいため、PIN の安全性を維持できます。

このパスフレーズは、USB トークンをデバイスに装着した後、PIN を復号化する際に必要となります。PIN が復号化されると、デバイスはその PIN を使用して USB トークンにログインします。

（注） ユーザがログインするには特権レベル 1 が必要です。

USB トークンのロック/ロック解除

USB トークン自体をロック（暗号化）またはロック解除（復号化）できます。

USB トークンは、ロック解除すると使用できるようになります。ロック解除した場合、Cisco IOS ソフトウェアでは、その USB トークンは自動ログインされたものと見なされ、その USB トークン上にあるいずれかのキーがロードされます。また、セカンダリ コンフィギュレーション ファイルがトークン上に存在する場合は、ログインしたユーザの権限レベルとは独立したフル ユーザ権限（権限レベル 15）を使用して、そのセカンダリ コンフィギュレーション ファイルが実行されます。

トークンをロックした場合は、トークンからログアウトする場合とは異なり、トークンからロードされた RSA キーがすべて削除され、セカンダリ アンコンフィギュレーション ファイルが（もし設定されていれば）実行されます。

セカンダリ コンフィギュレーション ファイルとセカンダリ アンコンフィギュレーション ファイル

USB トークン上に存在するコンフィギュレーション ファイルは、セカンダリ コンフィギュレーション ファイルと呼ばれます。セカンダリ コンフィギュレーション ファイルを作成および設定する場合、セカンダリ コンフィギュレーション ファイルの有無は、NVRAM に保存された Cisco IOS 設定内のセカンダリ コンフィギュレーション ファイル オプションの存在によって決定されます。ユーザがトークンを取り外した後またはトークンからログアウトした後に、無効タイマーで設定された期間が経過すると、別途用意されているセカンダリ アンコンフィギュレーション ファイルが実行され、セカンダリ コンフィギュレーションのすべての要素が、実行コンフィギュレーションから削除されます。セカンダリ コンフィギュレーション ファイル

およびセカンダリ アンコンフィギュレーション ファイルは、ログインしたユーザの権限レベルとは関係なく、権限レベル 15 で実行されます。

手順の概要

1. **enable**
2. **crypto pki token** *token-name* **unlock** [*pin*]
3. **configure terminal**
4. **crypto pki token** *token-name* **encrypted-user-pin** [**write**]
5. **crypto pki token** *token-name* **secondary unconfig** *file*
6. **exit**
7. **crypto pki token** *token-name* **lock** [*pin*]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**crypto pki token** *token-name* **unlock** [*pin*] 例： `Device# crypto pki token mytoken unlock mypin`	（任意）ロックされているUSB トークンを使用できるようにします。 ロック解除した場合、Cisco IOS ソフトウェアでは、そのUSB トークンは自動ログインされたものと見なされ、そのUSB トークン上にあるいずれかのキーがロードされます。また、セカンダリ コンフィギュレーション ファイルが存在する場合、このファイルは実行されます。
ステップ 3	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 4	**crypto pki token** *token-name* **encrypted-user-pin** [**write**] 例： `Device(config)# crypto pki token mytoken encrypted-user-pin write`	（任意）NVRAM に保存されている PIN を暗号化します。
ステップ 5	**crypto pki token** *token-name* **secondary unconfig** *file* 例：	（任意）セカンダリ コンフィギュレーション ファイルとその保管場所を指定します。

	コマンドまたはアクション	目的
	`Device(config)# crypto pki token mytoken secondary unconfig configs/myunconfigfile.cfg`	
ステップ 6	**exit** 例： `Device(config)# exit`	特権 EXEC モードを開始します。
ステップ 7	**crypto pki token** *token-name* **lock** [*pin*] 例： `Device# crypto pki token mytoken lock mypin`	（任意）トークンからロードされたRSAキーをすべて削除し、セカンダリ アンコンフィギュレーション ファイルが存在する場合は、それを実行します。

例

次の例は、ユーザ PIN の設定、ユーザ PIN の暗号化、デバイスのリロード、およびユーザ PIN のロック解除の各プロセスを順に示したものです。

```
! Configuring the user PIN

Enter configuration commands, one per line. End with CNTL/Z.

Device(config)# crypto pki token usbtoken0: userpin

Enter password: mypassword

! Encrypt the user PIN

Device(config)# crypto pki token usbtoken0: encrypted-user-pin

Enter passphrase: mypassphrase

Device(config)# exit

Device#

Sep 20 21:51:38.076: %SYS-5-CONFIG_I: Configured from console by console

Device# show running config

crypto pki token usbtoken0 user-pin *encrypted*

! Reloading the router.

Device> enable

Password:

! Decrypting the user pin.

Device# crypto pki token usbtoken0: unlock

Token eToken is usbtoken0

Enter passphrase: mypassphrase
```

```
Token login to usbtoken0(eToken) successful

Device#

Sep 20 22:31:13.128: %CRYPTO-6-TOKENLOGIN: Cryptographic Token eToken

Login Successful
```

次に示すのは、実行コンフィギュレーションからセカンダリ コンフィギュレーションの要素を削除する際に使用されるセカンダリ アンコンフィギュレーション ファイルの設定例です。セカンダリ コンフィギュレーション ファイルを使用してPKIトラストポイントが設定されている場合を例にとると、それに対応するアンコンフィギュレーション ファイル mysecondaryunconfigfile.cfg には、次のようなコマンド ラインが設定されます。

```
no crypto pki trustpoint token-tp
```

トークンが取り外された後で、次のコマンドが実行されると、デバイスの実行コンフィギュレーションから、トラストポイントおよびそれに関連付けられた証明書が削除されます。

```
 Device# configure terminal
Device(config)# no crypto pki token mytoken secondary unconfig mysecondaryunconfigfile.cfg
```

次の作業

USB トークンへのログインおよびUSB トークンの設定が完了すると、次のような作業が行えます。ユーザ PIN の変更、ルータから USB トークンに設定されたキーの保管場所へのファイルのコピー、USB トークンの変更など、USB トークンの管理作業を行う。「USB トークンにおける管理機能の設定」の項を参照してください。

USB トークンにおける管理機能の設定

ここでは、ユーザPIN、USBトークンに対するログイン試行の失敗回数の上限、クレデンシャルの保管場所など、さまざまなデフォルト設定を変更する手順について説明します。

手順の概要

1. **enable**
2. **crypto pki token** *token-name* **admin**] **change-pin** [*pin*]
3. **crypto pki token** *token-name device-name***: label** *token-label*
4. **configure terminal**
5. **crypto key storage** *device-name***:**
6. **crypto key generate rsa** [**general-keys** | **usage-keys** | **signature** | **encryption**] [**label** *key-label*] [**exportable**] [**modulus** *modulus-size*] [**storage** *device-name***:**] [**redundancy**] [**on** *device-name*]**:**
7. **crypto key move rsa** *keylabel* [**non-exportable** | [**on** | **storage**]] *location*
8. **crypto pki token** {*token-name* | **default**} **removal timeout** [*seconds*]
9. **crypto pki token** {*token-name* | **default**} **max-retries** [*number*]
10. **exit**
11. **copy usbflash**[*0-9*]**:***filename destination-url*
12. **show usbtoken**[*0-9*]**:***filename*

13. **crypto pki token** *token-name* **logout**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**crypto pki token** *token-name* **admin**] **change-pin** [*pin*] 例： `Device# crypto pki token usbtoken0 admin change-pin`	（任意）USB トークン上のユーザ PIN 番号を変更します。 • PIN が変更されない場合は、デフォルトの PIN（1234567890）が使用されます。 （注） PIN の変更後は、ログインの失敗回数を 0 にリセットする必要があります（**crypto pki token max-retries** コマンドを使用）。許容されるログインの失敗回数の上限は、15（デフォルト）に設定されています。
ステップ 3	**crypto pki token** *token-name device-name*: **label** *token-label* 例： `Device# crypto pki token mytoken usb0: label newlabel`	（任意）USB トークンの名前を設定または変更します。 • *token-label* 引数には、英数字（ダッシュおよびアンダースコアを含む）からなる 31 文字以下の文字列を指定できます。 ヒント このコマンドは、自動ログインやセカンダリ コンフィギュレーション ファイルなどのトークン固有の設定用として複数の USB トークンを設定する場合に有用です。
ステップ 4	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 5	**crypto key storage** *device-name*: 例： `Device(config)# crypto key storage usbtoken0:`	（任意）新規作成した RSA キーに対するデフォルトの保管場所を設定します。 （注） 設定の内容にかかわらず、既存のキーは、ロード元のデバイスに保存されます。

	コマンドまたはアクション	目的
ステップ 6	**crypto key generate rsa** [**general-keys** | **usage-keys** | **signature** | **encryption**] [**label** *key-label*] [**exportable**] [**modulus** *modulus-size*] [**storage** *device-name***:**] [**redundancy**] [**on** *device-name*]**:** 例： `Device(config)# crypto key generate rsa label tokenkey1 storage usbtoken0:`	（任意）証明書サーバの RSA キー ペアを生成します。 • **storage** キーワードを使用すると、キーの保管場所を指定できます。 • *key-label* 引数を指定することによってラベル名を指定する場合、**crypto pki server** *cs-label* コマンドによって証明書サーバーに使用するラベルと同じ名前を使用する必要があります。*key-label* 引数を指定していない場合、デバイスの完全修飾ドメイン名（FQDN）であるデフォルト値が使用されます。 **no shutdown** コマンドを発行する前に、CA 証明書が生成されるまで待ってからエクスポート可能な RSA キーペアを手動で生成する場合、**crypto ca export pkcs12** コマンドを使用して、証明書サーバー証明書および秘密キーを含む PKCS12 ファイルをエクスポートできます。 • デフォルトでは、CA キーのモジュラス サイズは 1024 ビットです。推奨される CA キーのモジュラスは 2048 ビットです。CA キーのモジュラス サイズの範囲は 350 ～ 4096 ビットです。 • **on** キーワードは、指定したデバイス上で RSA キーペアが作成されることを指定します。このデバイスには Universal Serial Bus（USB）トークン、ローカルディスク、および NVRAM などがあります。装置の名前の後にはコロン（:）を付けます。 （注） USB トークン上で作成されるキーは、2048 ビット以下である必要があります。
ステップ 7	**crypto key move rsa** *keylabel* [**non-exportable** | [**on** | **storage**]] *location* 例： `Device(config)# crypto key move rsa keypairname non-exportable on token`	（任意）既存の Cisco IOS クレデンシャルを、現在の保管場所から指定した保管場所へ移動します。 デフォルトの場合、RSA キー ペアは現在のデバイス上に保存されたままになります。 デバイス上でキーを生成しそれをトークンに移動するまでの所要時間は 1 分未満です。トークン上でキーを生成する際に **on** キーワードを使用すると、

	コマンドまたはアクション	目的
		USB トークン上で使用可能なハードウェアキー生成ルーチンに応じて、5 ～ 10 分程度の時間がかかります。 Cisco IOS で生成された既存の RSA キー ペアが USB トークンに保存され、登録に使用される場合は、それら既存の RSA キー ペアを代替場所に移動して永続的に保存する必要があります。 このコマンドは、USB トークンと SDP を使用してクレデンシャルを配置する場合に有用です。
ステップ 8	**crypto pki token** {*token-name* | **default**} **removal timeout** [*seconds*] 例： `Device(config)# crypto pki token usbtoken0 removal timeout 60`	（任意）USB トークンがデバイスから取り外されてから、USB トークンに保存されている RSA キーが削除されるまで、デバイスが待機する時間を秒単位で設定します。 （注） このコマンドが発行されない場合は、USB トークンがデバイスから取り外された直後に、すべての RSA キーが削除されるほか、USB トークンに関連付けられている IPsec トンネルもすべて切断されます。
ステップ 9	**crypto pki token** {*token-name* | **default**} **max-retries** [*number*] 例： `Device(config)# crypto pki token usbtoken0 max-retries 20`	（任意）USB トークンへのアクセスが拒否されるまでに許容されるログイン試行の連続失敗回数の上限を設定します。 • デフォルト値は 15 です。
ステップ 10	**exit** 例： `Device(config)# exit`	グローバル コンフィギュレーション モードを終了します。
ステップ 11	**copy usbflash**[*0-9*]**:***filename destination-url* 例： `Device# copy usbflash0:file1 nvram:`	USB トークンからデバイスへファイルをコピーします。 • *destination-url*：サポートされているオプションのリストについては、**copy** コマンドに関するセクションを参照してください。
ステップ 12	**show usbtoken**[*0-9*]**:***filename* 例： `Device# show usbtoken:usbfile`	（任意）USB トークンに関する情報を表示します。このコマンドを使用すると、USB トークンがデバイスにログインしているかどうかを確認できます。

	コマンドまたはアクション	目的
ステップ 13	**crypto pki token** *token-name* **logout** 例： `Device# crypto pki token usbtoken0 logout`	USB トークンからデバイスをログアウトします。 （注） USD トークンに何らかのデータを保存する場合は、再度トークンにログインする必要があります。

USB トークンに関するトラブルシューティング

ここでは、次の各 Cisco IOS コマンドについて説明します。これらのコマンドは、USB トークンの使用中に発生しうる問題についてのトラブルシューティングに使用できます。

USB ポート接続のトラブルシューティング

show file systems コマンドを使用すると、USB モジュールが USB ポートに差し込まれていることをルータが認識しているかどうかを判定できます。差し込まれている USB モジュールは、ファイルシステムのリスト上に表示されます。これらのモジュールがリスト上に表示されない場合は、次のいずれかの問題が発生している可能性があります。

- USB モジュールとの接続に問題がある。
- ルータ上で稼働している Cisco IOS イメージによりサポートされていない USB モジュールがある。
- USB モジュールそのものにハードウェア上の問題がある。

次に示すのは、 **show file systems** コマンドによる出力例です。この中には USB トークンも表示されています。USB モジュールが現れるのはリストの最下行です。

```
Device# show file systems
File Systems:
     Size(b)     Free(b)      Type  Flags  Prefixes
           -           -    opaque     rw   archive:
           -           -    opaque     rw   system:
           -           -    opaque     rw   null:
           -           -   network     rw   tftp:
*  129880064    69414912      disk     rw   flash:#
      491512      486395     nvram     rw   nvram:
           -           -    opaque     wo   syslog:
           -           -    opaque     rw   xmodem:
           -           -    opaque     rw   ymodem:
           -           -   network     rw   rcp:
           -           -   network     rw   pram:
           -           -   network     rw   ftp:
           -           -   network     rw   http:
           -           -   network     rw   scp:
           -           -   network     rw   https:
           -           -    opaque     ro   cns:
    63158272    33037312  usbflash     rw   usbflash0:
       32768         858  usbtoken     rw   usbtoken1:
```

シスコによりサポートされている USB トークンの特定

show usb device コマンドを使用すると、USB トークンがシスコによりサポートされているかどうかを判定できます。このコマンドの次の出力例では、太字で記されているのが、モジュールがサポートされているかどうかを示す箇所です。

```
Router# show usb device
Host Controller:1
Address:0x11
Device Configured:YES
Device Supported:YES
Description:eToken Pro 4254
Manufacturer:AKS
Version:1.0
Serial Number:
Device Handle:0x1010000
USB Version Compliance:1.0
Class Code:0xFF
Subclass Code:0x0
Protocol:0x0
Vendor ID:0x529
Product ID:0x514
Max. Packet Size of Endpoint Zero:8
Number of Configurations:1
Speed:Low
Selected Configuration:1
Selected Interface:0
Configuration:
    Number:1
    Number of Interfaces:1
    Description:
    Attributes:None
    Max Power:60 mA
    Interface:
        Number:0
        Description:
        Class Code:255
        Subclass:0
        Protocol:0
        Number of Endpoints:0
```

USB トークンのデバイス問題の特定

show usb controllers コマンドを使用すると、USB フラッシュモジュールにハードウェア上の問題があるかどうかを判別できます。**show usb controllers** コマンドの出力結果にエラーが表示された場合は、USB モジュールにハードウェア上の問題があると考えられます。

USB フラッシュモジュールに対するコピー操作が正常に行われていることを確認する場合にも、この **show usb controllers** コマンドを使用できます。ファイルのコピーを実行した後で、**show usb controllers** コマンドを発行すると、データ転送が正常に行われたことを示す内容が表示されます。

次に示すのは、使用中の USB フラッシュモジュールの **show usb controllers** コマンドによる出力例です。

```
Router# show usb controllers
Name:1362HCD
```

```
Controller ID:1
Controller Specific Information:
    Revision:0x11
    Control:0x80
    Command Status:0x0
    Hardware Interrupt Status:0x24
    Hardware Interrupt Enable:0x80000040
    Hardware Interrupt Disable:0x80000040
    Frame Interval:0x27782EDF
    Frame Remaining:0x13C1
    Frame Number:0xDA4C
    LSThreshold:0x628
    RhDescriptorA:0x19000202
    RhDescriptorB:0x0
    RhStatus:0x0
    RhPort1Status:0x100103
    RhPort2Status:0x100303
    Hardware Configuration:0x3029
    DMA Configuration:0x0
    Transfer Counter:0x1
    Interrupt:0x9
    Interrupt Enable:0x196
    Chip ID:0x3630
    Buffer Status:0x0
    Direct Address Length:0x80A00
    ATL Buffer Size:0x600
    ATL Buffer Port:0x0
    ATL Block Size:0x100
    ATL PTD Skip Map:0xFFFFFFFF
    ATL PTD Last:0x20
    ATL Current Active PTD:0x0
    ATL Threshold Count:0x1
    ATL Threshold Timeout:0xFF
Int Level:1
Transfer Completion Codes:
         Success              :920             CRC              :0
         Bit Stuff            :0               Stall            :0
         No Response          :0               Overrun          :0
         Underrun             :0               Other            :0
         Buffer Overrun       :0               Buffer Underrun :0
Transfer Errors:
         Canceled Transfers   :2               Control Timeout :0
Transfer Failures:
         Interrupt Transfer   :0               Bulk Transfer   :0
         Isochronous Transfer :0               Control Transfer:0
Transfer Successes:
         Interrupt Transfer   :0               Bulk Transfer   :26
         Isochronous Transfer :0               Control Transfer:894
USBD Failures:
         Enumeration Failures :0               No Class Driver Found:0
         Power Budget Exceeded:0
USB MSCD SCSI Class Driver Counters:
         Good Status Failures :3               Command Fail    :0
         Good Status Timed out:0               Device not Found:0
         Device Never Opened  :0               Drive Init Fail :0
         Illegal App Handle   :0               Bad API Command :0
         Invalid Unit Number  :0               Invalid Argument:0
         Application Overflow :0               Device in use   :0
         Control Pipe Stall   :0               Malloc Error    :0
         Device Stalled       :0               Bad Command Code:0
         Device Detached      :0               Unknown Error   :0
         Invalid Logic Unit Num:0
USB Aladdin Token Driver Counters:
         Token Inserted       :1               Token Removed   :0
```

```
        Send Insert Msg Fail :0                 Response Txns   :434
        Dev Entry Add Fail   :0                 Request Txns    :434
        Dev Entry Remove Fail:0                 Request Txn Fail:0
        Response Txn Fail    :0                 Command Txn Fail:0
        Txn Invalid Dev Handle:0
USB Flash File System Counters:
        Flash Disconnected   :0                 Flash Connected :1
        Flash Device Fail    :0                 Flash Ok        :1
        Flash startstop Fail :0                 Flash FS Fail   :0
USB Secure Token File System Counters:
        Token Inserted       :1                 Token Detached  :0
        Token FS success     :1                 Token FS Fail   :0
        Token Max Inserted   :0                 Create Talker Failures:0
        Token Event          :0                 Destroy Talker Failures:0
        Watched Boolean Create Failures:0
```

USB トークン情報の表示

dir コマンドと **filesystem** キーワードオプション **usbtoken***0-9***:** を使用すると、USB トークン上にあるすべてのファイル、ディレクトリ、およびそれらの権限文字列を表示できます。

次の出力例は、USB トークンに関する情報を表示したものです。

```
Device# dir usbtoken1:
Directory of usbtoken1:/
    2  d---           64  Dec 22 2032 05:23:40 +00:00  1000
    5  d---         4096  Dec 22 2032 05:23:40 +00:00  1001
    8  d---            0  Dec 22 2032 05:23:40 +00:00  1002
   10  d---          512  Dec 22 2032 05:23:42 +00:00  1003
   12  d---            0  Dec 22 2032 05:23:42 +00:00  5000
   13  d---            0  Dec 22 2032 05:23:42 +00:00  6000
   14  d---            0  Dec 22 2032 05:23:42 +00:00  7000
   15  ----          940  Jun 27 1992 12:50:42 +00:00  mystartup-config
   16  ----         1423  Jun 27 1992 12:51:14 +00:00  myrunning-config
32768 bytes total (858 bytes free)
```

次の出力例では、デバイスが認識しているすべてのデバイスのディレクトリ情報を表示します。

```
Device# dir all-filesystems
Directory of archive:/
No files in directory
No space information available
Directory of system:/
    2  drwx           0                    <no date>  its
  115  dr-x           0                    <no date>  lib
  144  dr-x           0                    <no date>  memory
    1  -rw-        1906                    <no date>  running-config
  114  dr-x           0                    <no date>  vfiles
No space information available
Directory of flash:/
    1  -rw-    30125020  Dec 22 2032 03:06:04 +00:00  c3825-entservicesk9-mz.123-14.T
129880064 bytes total (99753984 bytes free)
Directory of nvram:/
  476  -rw-        1947                    <no date>  startup-config
  477  ----          46                    <no date>  private-config
  478  -rw-        1947                    <no date>  underlying-config
    1  -rw-           0                    <no date>  ifIndex-table
    2  ----           4                    <no date>  rf_cold_starts
    3  ----          14                    <no date>  persistent-data
491512 bytes total (486395 bytes free)
```

```
Directory of usbflash0:/
    1  -rw-    30125020  Dec 22 2032 05:31:32 +00:00  c3825-entservicesk9-mz.123-14.T
63158272 bytes total (33033216 bytes free)
Directory of usbtoken1:/
    2  d---          64  Dec 22 2032 05:23:40 +00:00  1000
    5  d---        4096  Dec 22 2032 05:23:40 +00:00  1001
    8  d---           0  Dec 22 2032 05:23:40 +00:00  1002
   10  d---         512  Dec 22 2032 05:23:42 +00:00  1003
   12  d---           0  Dec 22 2032 05:23:42 +00:00  5000
   13  d---           0  Dec 22 2032 05:23:42 +00:00  6000
   14  d---           0  Dec 22 2032 05:23:42 +00:00  7000
   15  ----         940  Jun 27 1992 12:50:42 +00:00  mystartup-config
   16  ----        1423  Jun 27 1992 12:51:14 +00:00  myrunning-config
32768 bytes total (858 bytes free)
```

PKI データの保存に関する設定例

例：特定のローカルな保管場所への証明書の保存

次に示すのは、certsサブディレクトリに証明書を保存する場合の設定例です。ここでは、certsサブディレクトリは存在しないため、自動的に作成されています。

```
Router# dir nvram:
 114  -rw-        4687                    <no date>  startup-config
 115  ----        5545                    <no date>  private-config
 116  -rw-        4687                    <no date>  underlying-config
   1  ----          34                    <no date>  persistent-data
   3  -rw-         707                    <no date>  ioscaroot#7401CA.cer
   9  -rw-         863                    <no date>  msca-root#826E.cer
  10  -rw-         759                    <no date>  msca-root#1BA8CA.cer
  11  -rw-         863                    <no date>  msca-root#75B8.cer
  24  -rw-        1149                    <no date>  storagename#6500CA.cer
  26  -rw-         863                    <no date>  msca-root#83EE.cer
129016 bytes total (92108 bytes free)
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# crypto pki certificate storage disk0:/certs
Requested directory does not exist -- created
Certificates will be stored in disk0:/certs/
Router(config)# end
Router# write
*May 27 02:09:00:%SYS-5-CONFIG_I:Configured from console by consolemem
Building configuration...
[OK]
Router# directory disk0:/certs
Directory of disk0:/certs/
  14  -rw-         707  May 27 2005 02:09:02 +00:00  ioscaroot#7401CA.cer
  15  -rw-         863  May 27 2005 02:09:02 +00:00  msca-root#826E.cer
  16  -rw-         759  May 27 2005 02:09:02 +00:00  msca-root#1BA8CA.cer
  17  -rw-         863  May 27 2005 02:09:02 +00:00  msca-root#75B8.cer
  18  -rw-        1149  May 27 2005 02:09:02 +00:00  storagename#6500CA.cer
  19  -rw-         863  May 27 2005 02:09:02 +00:00  msca-root#83EE.cer
47894528 bytes total (20934656 bytes free)
! The certificate files are now on disk0/certs:
```

例：USB トークンへのログインと USB トークンへの RSA キーの保存

次に示すのは、USB トークンにログインして RSA キーを生成し、その RSA キーを USB トークンに保存する場合の設定例です。

```
! Configure the router to automatically log into the eToken
configure terminal
 crypto pki token default user-pin 0 1234567890
! Generate RSA keys and enroll certificates with the CA.
crypto pki trustpoint IOSCA
 enrollment url http://10.23.2.2
 exit
crypto ca authenticate IOSCA
Certificate has the following attributes:
       Fingerprint MD5:23272BD4 37E3D9A4 236F7E1A F534444E
      Fingerprint SHA1:D1B4D9F8 D603249A 793B3CAF 8342E1FE 3934EB7A
% Do you accept this certificate? [yes/no]:yes
Trustpoint CA certificate accepted.
crypto pki enroll
crypto pki enroll IOSCA
%
% Start certificate enrollment ..
% Create a challenge password. You will need to verbally provide this
   password to the CA Administrator in order to revoke your certificate.
   For security reasons your password will not be saved in the configuration.
   Please make a note of it.
Password:
Re-enter password:
% The subject name in the certificate will include:c2851-27.cisco.com
% Include the router serial number in the subject name? [yes/no]:no
% Include an IP address in the subject name? [no]:no
Request certificate from CA? [yes/no]:yes
% Certificate request sent to Certificate Authority
% The 'show crypto ca certificate IOSCA verbose' command will show the fingerprint.
*Jan 13 06:47:19.413:CRYPTO_PKI: Certificate Request Fingerprint MD5:E6DDAB1B
 0E30EFE6 54529D8A DA787DBA
*Jan 13 06:47:19.413:CRYPTO_PKI: Certificate Request Fingerprint SHA1:3B0F33B
7 57C02A10 3935042B C4B6CD3D 61039251
*Jan 13 06:47:21.021:%PKI-6-CERTRET:Certificate received from Certificate Authority
! Issue the write memory command, which will automatically save the RSA keys to the
eToken ! instead of private NVRAM.
Router# write memory
Building configuration...
[OK]
*Jan 13 06:47:29.481:%CRYPTO-6-TOKENSTOREKEY:Key c2851-27.cisco.com stored on
Cryptographic Token eToken Successfully
```

次に示すのは、USB トークンから正常にロードされた保存済みログイン情報の **show crypto key mypubkey rsa** コマンドによる出力例です。USB トークン上に保存されているクレデンシャルは、保護領域内に存在します。USB トークン上にクレデンシャルを保存する場合、それらのファイルは /keystore というディレクトリに保存されます。ただし、キー ファイルは、コマンドライン インターフェイス（CLI）では表示されません。

```
Router#
show crypto key mypubkey rsa
% Key pair was generated at:06:37:26 UTC Jan 13 2005
Key name:c2851-27.cisco.com
 Usage:General Purpose Key
 Key is not exportable.
```

```
 Key Data:
  305C300D 06092A86 4886F70D 01010105 00034B00 30480241 00E3C644 43AA7DDD
  732E0F4E 3CA0CDAB 387ABF05 EB8F22F2 2431F1AE 5D51FEE3 FCDEA934 7FBD3603
  7C977854 B8E999BF 7FC93021 7F46ABF8 A4BA2ED6 172D3D09 B5020301 0001
% Key pair was generated at:06:37:27 UTC Jan 13 2005
Key name:c2851-27.cisco.com.server
 Usage:Encryption Key
 Key is not exportable.
 Key Data:
  307C300D 06092A86 4886F70D 01010105 00036B00 30680261 00DD96AE 4BF912EB
  2C261922 4784EF98 2E70E837 774B3778 7F7AEB2D 87F5669B BF5DDFBC F0D521A5
  56AB8FDC 9911968E DE347FB0 A514A856 B30EAFF4 D1F453E1 003CFE65 0CCC6DC7
  21FBE3AC 2F8DEA16 126754BC 1433DEF9 53266D33 E7338C95 BB020301 0001
```

その他の参考資料

関連資料

関連項目	マニュアル タイトル
ルータへの USB モジュールの接続	『*Cisco Access Router USB Flash Module and USB eToken Hardware Installation Guide*』
eToken および USB フラッシュのデータ シート	『*USB eToken and USB Flash Features Support*』
RSA キー	PKI 内での RSA キーの展開
ファイル管理（ファイルのロード、コピー、および再起動）	『*Cisco Configuration Fundamentals Configuration Guide*』（Cisco.com）
USB トークンによる RSA 処理：証明書サーバの設定	「PKI 展開での Cisco IOS 証明書サーバの設定および管理」の機能に関する資料。 「Generating a Certificate Server RSA Key Pair」項、「Configuring a Certificate Server Trustpoint」項、および関連する例を参照してください。
USB トークンの RSA 処理：初期自動登録時における USB トークンを使用した RSA 処理	『Configuring Certificate Enrollment for a PKI』の「Configuring Certificate Enrollment or Autoenrollment」項を参照してください。
SDP のセットアップ、設定、および USB トークンとの使用	PKI クレデンシャルの展開での SDP と USB トークンの使用方法については、「Setting Up Secure Device Provisioning (SDP) for Enrollment in a PKI」にある機能名の機能情報の項を参照してください。

シスコのテクニカル サポート

説明	リンク
右の URL にアクセスして、シスコのテクニカル サポートを最大限に活用してください。これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

PKI クレデンシャルの保存に関する機能情報

表 *158 : PKI* クレデンシャルの保存に関する機能情報

機能名	リリース	機能情報
証明書：保管場所の指定		この機能を使用すると、証明書を個別のファイルとして保存する機能をサポートしているプラットフォームにおいて、ローカル証明書の保管場所を指定できます。シスコのプラットフォームはすべて、デフォルトの保管場所として使用する NVRAM、およびフラッシュ ローカル ストレージをサポートしています。ご使用のプラットフォームによっては、ブートフラッシュ、スロット、ディスク、USB フラッシュ、USB トークンなど、サポートされているその他のローカル ストレージを使用できます。 この機能により、次のコマンドが導入されました。**crypto pki certificate storage**、**show crypto pki certificates storage**。
ソフトウェア暗号エンジンサポートでの RSA 4096 ビット キー生成	15.1(1)T	**crypto key generate rsa** コマンドの **modulus** キーワードの値の範囲は、360 ～ 2048 ビットから 360 ～ 4096 ビットに拡張されました。

第 116 章

CA における発信トラフィックの送信元インターフェイス選択機能

認証局（CA）における発信トラフィックの送信元インターフェイス選択機能により、指定のトラストポイントが設定されたときに、インターフェイスのアドレスをそのトラストポイントと関連付けられたすべての TCP 接続の送信元アドレスとして使用するよう設定できます。

CAにおける発信トラフィックの送信元インターフェイス選択機能の詳細

エンティティを識別する証明書

証明書を使用して、エンティティを識別できます。認証局（CA）とも呼ばれるトラステッドサーバにより、エンティティの ID を決定した後にエンティティに証明書が発行されます。Cisco IOS XE ソフトウェアを実行しているルータは、CA にネットワーク接続することでその証明書を取得します。Simple Certificate Enrollment Protocol（SCEP）を使用して、ルータはその証明書要求を CA に送信し、許可された証明書を受信します。ルータは、SCEP を使用した場合と同様に CA の証明書を取得します。リモートデバイスからの証明書を検証する場合、ルータは再度 CA または Lightweight Directory Access Protocol（LDAP）サーバあるいは HTTP サーバに連絡して、リモートデバイスの証明書が失効しているかどうか判断できます（このプロセスは、証明書失効リスト（CRL）のチェックとも呼ばれています）。

（注） Cisco IOS リリースに応じて、LDAP がサポートされます。

設定によっては、有効またはルーティング可能な IP アドレスを持たないインターフェイスを使用して発信 TCP 接続を実行できる場合があります。ユーザは、異なるインターフェイスのアドレスを発信接続の送信元 IP アドレスとして使用するよう指定する必要があります。この要件の具体例としてケーブル モデムがあります。発信ケーブル インターフェイス（RF インターフェイス）には通常、ルーティング可能なアドレスがないためです。ただし、ユーザインターフェイス（通常は FastEthernet）には有効な IP アドレスはありません。

トラストポイントに関連付けられた発信 TCP 接続の送信元インターフェイス

トラストポイントを指定するには、**crypto pki trustpoint** コマンドを使用します。インターフェイスのアドレスを、そのトラストポイントに関連付けられたすべての発信 TCP 接続の送信元アドレスとして指定する場合は、**source interface** コマンドも **crypto pki trustpoint** コマンドとともに使用します。

（注） インターフェイスアドレスが **source interface** コマンドを使用して指定されていない場合は、発信インターフェイスのアドレスが使用されます。

CAにおける発信トラフィックの送信元インターフェイス選択機能の設定方法

トラストポイントに関連付けられたすべての発信 TCP 接続のインターフェイスの設定

トラストポイントに関連付けられたすべての発信 TCP 接続の送信元アドレスとして使用するインターフェイスを設定するには、次の作業を行います。

手順の概要

1. **enable**
2. **configure terminal**
3. **crypto pki trustpoint** *name*
4. **enrollment url** *url*
5. **source interface** *interface-address*
6. **interface** *type slot / port*

7. **description** *string*
8. **ip address** *ip-address mask*
9. **interface** *type slot / port*
10. **description** *string*
11. **ip address** *ip-address mask*
12. **crypto map** *map-name*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**crypto pki trustpoint** *name* 例： `Router (config)# crypto pki trustpoint ms-ca`	ルータが使用する認証局（CA）を宣言し、CA トラストポイント コンフィギュレーション モードを開始します。
ステップ 4	**enrollment url** *url* 例： `Router (ca-trustpoint)# enrollment url http://yourname:80/certsrv/mscep/mscep.dll`	CA の登録パラメータを指定します。
ステップ 5	**source interface** *interface-address* 例： `Router (ca-trustpoint)# interface fastethernet1/0`	そのトラストポイントに関連付けられたすべての発信 TCP 接続の送信元アドレスとして使用するインターフェイス。
ステップ 6	**interface** *type slot / port* 例： `Router (ca-trustpoint)# interface fastethernet1/0`	インターフェイス タイプを設定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 7	**description** *string* 例： `Router (config-if)# description inside interface`	インターフェイスの設定に説明を加えます。

	コマンドまたはアクション	目的
ステップ 8	**ip address** *ip-address mask* 例： `Router (config-if)# ip address 10.1.1.1 255.255.255.0`	インターフェイスに対するプライマリ IP アドレスまたはセカンダリ IP アドレスを設定します。
ステップ 9	**interface** *type slot / port* 例： `Router (config-if)# interface fastethernet1/0`	インターフェイス タイプを設定します。
ステップ 10	**description** *string* 例： `Router (config-if)# description outside interface 10.1.1.205 255.255.255.0`	インターフェイスの設定に説明を加えます。
ステップ 11	**ip address** *ip-address mask* 例： `Router (config-if)# ip address 10.2.2.205 255.255.255.0`	インターフェイスに対するプライマリ IP アドレスまたはセカンダリ IP アドレスを設定します。
ステップ 12	**crypto map** *map-name* 例： `Router (config-if)# crypto map mymap`	インターフェイスに対して以前に定義されたクリプト マップ セットを適用します。

トラブルシューティングのヒント

コマンドで指定されたインターフェイスのアドレスが有効であることを確認します。指定されたインターフェイスのアドレスを使用して別のデバイス（可能性としては CRL を処理している HTTP または LDAP サーバ）からルータに ping を実行します。外部デバイスからルータへのトレースルートを使用しても同じことができます。

Cisco IOS XE コマンドライン インターフェイス（CLI）を使用して、ルータと CA または LDAP サーバ間の接続をテストすることもできます。**ping ip** コマンドを入力し、プロンプトに回答します。「Extended commands [n]:」プロンプトに「はい」と回答すると、送信元アドレスまたはインターフェイスが指定できるようになります。

また、Cisco IOS XE CLI を使用して traceroute コマンドを入力できます。**traceroute ip** コマンド（EXEC モード）を入力すると、宛先および送信元アドレスを求めるプロンプトが表示されます。CA または LDAP サーバを、宛先および送信元アドレスの「送信元インターフェイス」として指定されたインターフェイスのアドレスとして指定する必要があります。

CAにおける発信トラフィックの送信元インターフェイス選択機能の設定例

CA における発信トラフィックの送信元インターフェイス選択の例

次に、ルータが支社にある例を示します。ルータは IP セキュリティ（IPSec）を使用して本社と通信します。FastEthernet 1 は、ISP（インターネット サービス プロバイダー）に接続する「外部」インターフェイスです。FastEthernet 0 は、支社の LAN に接続されたインターフェイスです。本社にある CA サーバにアクセスするには、ルータは IPSec トンネルを使用してその IP データグラムを外部インターフェイスである FastEthernet 1（アドレス 10.2.2.205）に送信する必要があります。アドレス 10.2.2.205 は ISP により割り当てられています。アドレス 10.2.2.205 は支社または本社の一部ではありません。

CA は、ファイアウォールがあるため、社外のアドレスにはアクセスできません。CA は 10.2.2.205 から発信されたメッセージを確認しますが、応答はできません（つまり、CA は、ルータが支社の到達可能なアドレス 10.1.1.1 にあることを認識していません）。

source interface コマンドを追加すると、ルータはアドレス 10.1.1.1 を CA に送信される IP データグラムの送信元アドレスとして使用するよう指示されます。CA は 10.1.1.1 に応答できます。

このシナリオは、上記の **source interface** コマンドとインターフェイスアドレスを使用して設定されています。

```
crypto pki trustpoint ms-ca
 enrollment url http://ms-ca:80/certsrv/mscep/mscep.dll
 source interface fastethernet0
!
interface fastethernet 0
 description inside interface
 ip address 10.1.1.1 255.255.255.0
!
interface fastethernet 1
 description outside interface
 ip address 10.2.2.205 255.255.255.0
 crypto map main-office
```

その他の参考資料

次に、CA における発信トラフィックの送信元インターフェイスの機能に関する資料を示します。

関連資料

関連項目	マニュアル タイトル
IPsec と認証局の設定	「Security for VPNs with IPsec」

関連項目	マニュアル タイトル
IPsec と認証局に関するコマンド	『*Cisco IOS Security Command Reference*』

標準

標準	タイトル
この機能がサポートする新しい規格または変更された規格はありません。	-

MIB

MIB	MIB のリンク
この機能によってサポートされる新しい MIB または変更された MIB はありません。	選択したプラットフォーム、Cisco IOS XE ソフトウェア リリース、およびフィーチャ セットの MIB の場所を検索しダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

RFC

RFC	タイトル
この機能でサポートが追加または変更された RFC はありません。	-

シスコのテクニカル サポート

説明	リンク
シスコのサポート Web サイトでは、シスコの製品やテクノロジーに関するトラブルシューティングにお役立ていただけるように、マニュアルやツールをはじめとする豊富なオンライン リソースを提供しています。 お使いの製品のセキュリティ情報や技術情報を入手するために、Cisco Notification Service（Field Notice からアクセス）、Cisco Technical Services Newsletter、Really Simple Syndication（RSS）フィードなどの各種サービスに加入できます。 シスコのサポート Web サイトのツールにアクセスする際は、Cisco.com のユーザ ID およびパスワードが必要です。	http://www.cisco.com/techsupport

CAにおける発信トラフィックの送信元インターフェイス選択の機能情報

表 *159 : CA* における発信トラフィックの送信元インターフェイス選択の機能情報

機能名	リリース	機能情報
CA における発信トラフィックの送信元インターフェイス選択機能	Cisco IOS XE Release 2.1	この機能により、指定のトラストポイントが設定されたときに、インターフェイスのアドレスをそのトラストポイントと関連付けられたすべての TCP 接続の送信元アドレスとして使用するよう設定できます。 次のコマンドが導入されました。**source interface**

用語集

認証：IDの証明書およびIDがもたらす秘密を使用してエンティティのIDを証明すること（通常は、秘密キーは証明書の公開キーに対応します）。

CA：認証局。CAはデジタル証明書を発行するエンティティ（特にX.509証明書）で、証明書のデータ項目間のバインディングを保証します。

CA authentication：ユーザーはルート CA からの証明書を手動で承認します。通常は、証明書のフィンガープリントがユーザに提示され、ユーザはフィンガープリントに基づく証明書を承認するよう求められます。ルート CA の証明書は、通常の証明書確認プロセスで自動的に認証できないよう、自ら署名（自己署名）されます。

CRL：証明書失効リスト。CRL は、発行者により無効にされたデジタル証明書をそれらの期限満了予定までに列挙するデータ構造です。

enrollment：ルータは登録プロセス経由でその証明書を受信します。ルータは、（PKCS#10 と呼ばれる）特定の形式で証明書の要求を生成します。その要求は CA に転送され、CA は要求を許可し、要求と同じ形式に符号化された証明書を生成します。ルータは許可された証明書を受信し、通常操作中に使用するため、内部データベースに保管します。

certificate：エンティティ（マシンまたはユーザー）をそのエンティティの公開キーと関連付けるため国際標準化機構（ISO）規格 X.509 で定義されたデータ構造。証明書には、エンティティの名前など特定のフィールドが含まれています。証明書は通常は、エンティティに代わって CA により発行されます。この場合は、ルータが CA としての役割を果たします。証明書内の共通フィールドには、エンティティの認定者名（DN）、証明書を発行している認証局の DN、およびエンティティの公開キーがあります。

LDAP：Lightweight Directory Access Protocol。LDAP は、X.500 ディレクトリに読み書きインタラクティブ アクセスできる、管理アプリケーションおよびブラウザ アプリケーションにアクセスできるプロトコルです。

第 117 章

PKI トラストプール管理

PKI トラストプール管理機能を使用すると、認証局（CA）と呼ばれる一般的に認識された信頼できるエージェントを使用して、デバイス間で発生する HTTPS などのセッションを認証できます。

Trustpool 証明書は、信頼を確立できる既知の CA 証明書です。IOS PKI には両方の CA が組み込まれており、trustpool バンドルをダウンロードするオプションもあります。組み込み CA 証明書は、ダウンロードされた trustpool バンドルの PKCS7 署名を検証するために使用されます。署名の検証に失敗した場合は、trustpool バンドルをダウンロードできます。組み込み trustpool 証明書は削除できます。trustpool 証明書は、SSLVPN、PnP、スマートライセンス、MacSec などのアプリケーションで使用されます。

デフォルトで有効に設定されているこの機能を使用すると、セッションのセキュリティ保護のためにブラウザが提供するサービスと同じ方法で、既知の CA の証明書のプールのプロビジョニング、保管、管理を行うスキーマを作成できます。

（注） 新しいルート証明書は、シスコのプラグ アンド プレイ アプリケーションの組み込み証明書に含まれています。

（注） Cisco IOS XE Denali 16.3 から、PKI トラストプールが管理される方法が変更されました。このリリースへのアップグレードを計画している場合は、「*PKI* トラストプールの拡張」項に含まれる次の機能に対する変更を確認してください。

PKI トラストプール管理の前提条件

証明書を使用するには、暗号化サブシステムが Cisco IOS ソフトウェア イメージに含まれている必要があります。

PKI トラストプール管理の制約事項

CA 証明書を使用するデバイス証明書は PKI トラストプールに登録できません。

トラストプール URL を介してダウンロードできるのは、シスコの署名済み PKCS7 証明書のみです。

PKI トラストプール管理の情報

PKI トラストプール内の CA 証明書の保管場所

ルータは、PKI トラストプールと呼ばれる特別な証明書ストアに格納された内蔵型 CA 証明書バンドルを使用します。これはシスコから自動的に更新されます。この PKI トラストプールは、シスコおよび他のベンダーにも知られています。CA 証明書バンドルは次の形式で提供されます。

- 公開キー暗号化メッセージ構文標準 7（pkcs7）内にエンベロープ化された、Distinguished Encoding Rules（DER）バイナリ形式の X.509 証明書。PKI でメッセージの署名と暗号化に使用します。X.509 証明書は、PKI と権限管理インフラストラクチャ（PMI）の標準で、特に、公開キー証明書の標準形式、証明書失効リスト、属性証明書、および認証パス検証アルゴリズムを指定します。
- PEM ヘッダー付きプライバシー強化メール（PEM）形式の連結型 X.509 証明書を含むファイル。

（注） また、NVRAM の代わりに、バンドルの保管場所としてフラッシュも使用できます。

PKI トラストプールの更新

PKI トラストプールは、次の条件が発生した場合に更新する必要のある単一エンティティとして処理されます。

- PKI トラストプールの証明書が期限切れまたは再発行されている。

- 公開された CA 証明書のバンドルに、特定のアプリケーションで必要な追加の信頼できる証明書が含まれている。
- 設定が破損している。

（注） PKI トラストプールに組み込まれた証明書は物理的に置き換えることができません。ただし、組み込まれた証明書の X.509 所有者名属性が CA 証明書バンドル内の証明書と一致する場合、組み込まれた証明書は無効と表示されます。

PKI トラストプールは自動または手動で更新できます。PKI トラストプールを使用するアプリケーションによっては、PKI トラストプールが証明書検証で使用される場合があります。詳細については「PKI トラストプール内の証明書の手動更新」と「PKI トラストプール ポリシー パラメータの設定」の項を参照してください。

（注） 自動更新が有効になっていると、インポート方法に関係なく、ダウンロードされている既存のすべてのトラストプール証明書（組み込まれたトラストプール証明書を除く）が削除されます。

PKI トラストプール タイマーは、最初に失効する CA 証明書と一致します。タイマーが作動しても、バンドルのロケーションが設定されておらず、明示的に無効になっていない場合、syslog 警告が発効され、PKI トラストプール ポリシー オプションが設定されていないことが管理者に警告されます。

PKI トラストプールの自動更新では設定済み URL を使用します。

PKI トラストプールが失効すると、ポリシーが読み込まれ、バンドルがロードされ、PKI トラストプールが置き換えられます。PKI トラストプールの自動更新の開始時に問題が発生した場合は、ダウンロードが成功するまで、次のスケジュールで更新が開始されます。20 日、15 日、10 日、5 日、4 日、3 日、2 日、1 日、最後に 1 時間ごとです。

PKI トラストプールとトラストポイントの両方での CA 処理

PKI トラストプールとトラストポイントの両方に CA が格納されている場合があります。たとえば、トラストポイントで CA を使用し、CA バンドルが同じ CA 内で後からダウンロードされたりします。このシナリオでは、PKI トラストプール管理機能がルータに実装されても、現在の動作が変更されないようにするため、トラストポイント内の CA とこのトラストポイントのポリシーが、PKI トラストプールまたは PKI トラストプール ポリシーの CA よりも優先されます。

PKI トラストプールの拡張機能

Cisco IOS XE Denali 16.3 より前のリリースでは、トラストプールは、すべてのシスコ ボックスで展開された内蔵型証明書と、公開されたバンドルからダウンロードした CA 証明書で構成さ

れています。ダウンロードした証明書は、デフォルトでは NVRAM に保存されます。ダウンロードしたトラストプールバンドルの証明書は抽出され、非効率的で多くの領域を使用する実行コンフィギュレーションに保存されていました。

Cisco IOS XE Denali 16.3 以降、PKI トラストプールの拡張機能では、これまでのリリースのような個別の証明書の代わりに、保管場所（デフォルトではNVRAM）にあるファイルと同じダウンロードしたバンドル形式でバンドルが保存されます。このため、ファイルが圧縮形式の場合は、ストレージメモリが節約されます。また、証明書は実行コンフィギュレーションでは個別に表示されません。再起動するたびに、バンドルは保存場所から読み取られ、個別の証明書がデータベースにインストールされます。

この機能は、実行コンフィギュレーションから現在のダウンロードした証明書を削除します。これらの証明書は古いNVRAMおよび新しいイメージと互換性がないため、**crypto pki certificate pool** には DER 形式の証明書を指定できません。アップグレード中、DER 形式のトラストプール証明書が失われたら、バンドルを保管場所に再インストールする必要があります。古い NVRAM ファイルの場合、これは再起動時に syslog に記されます。**show crypto pki trustpool** コマンドは、設定が削除されたことを示します。アップグレード前に、**show crypto pki trustpool** コマンドを使用し、証明書が利用可能かどうかを確認します。

Cisco IOS XE Denali 16.3 へのアップグレード前に、次の手順を実行する必要があります。

- **crypto pki trustpool clean** コマンドを使用して、ダウンロードしたトラストプール証明書を削除します
- **write memory** コマンドを使用します。
- デバイスを再起動します。
- **crypto pki trustpool import url** コマンドを使用して、トラストプールバンドルをダウンロードします。

SSHへのログインにトラストプールを使用している場合、追加の手順を実行して、特定の証明書をバンドルからトラストポイントに転送する必要があります。詳細については、「例：アップグレード中の *SSH* 接続に *PKI* トラストプールを使用」を参照してください。

（注） Cisco IOS XE Gibraltar 16.10 リリース以降では、トラストポイントで **match crlsign** コマンドを設定すると、検証中に crlsign がクロスチェックされます。

PKI トラストプール管理の設定方法

PKI トラストプールの証明書の手動更新

PKI トラストプール管理機能はデフォルトで有効で、PKI トラストプールに組み込まれた CA 証明書バンドルを使用し、シスコから自動更新を受信します。PKI トラストプール内の証明書

が最新のものではない、破損している、または特定の証明書を更新する必要がある場合は、次の作業を実行して手動で更新します。

手順の概要

1. **enable**
2. **configure terminal**
3. **crypto pki trustpool import clean** [**terminal** | **url** *url*]
4. **crypto pki trustpool import** {**terminal**} {**url** *url* | **ca-bundle**} {**vrf** *vrf-name* | **source interface** *interface-name*}
5. **exit**
6. **show crypto pki trustpool**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**crypto pki trustpool import clean** [**terminal**	**url** *url*] 例： `Device(config)# crypto pki trustpool import clean`	（任意）ダウンロードしたすべての PKI CA 証明書を手動で削除します。 • **clean** キーワードは、新しい証明書のダウンロードの前に、ダウンロード済みの PKI トラストプール証明書の削除を指定します。 • **terminal** キーワードは、既存の CA 証明書バンドル端末設定を削除します。 • **url** キーワードおよび *url* 引数は、既存の URL ファイル システム設定を削除します。
ステップ 4	**crypto pki trustpool import** {**terminal**} {**url** *url*	**ca-bundle**} {**vrf** *vrf-name*	**source interface** *interface-name*} 例： `Device(config)# crypto pki trustpool import url http://www.cisco.com/security/pki/trs/ios.p7b`	CA 証明書バンドルを PKI トラストプールに手動でインポート（ダウンロード）したり、既存の CA 証明書バンドルを交換したりします。 • **terminal** キーワードを指定すると、端末（カットアンドペースト）を介して CA 証明書バンドルが PEM 形式でインポートされます。

	コマンドまたはアクション	目的
		• **url** キーワードと *url* 引数を指定すると、URL を介して CA 証明書バンドルがインポートされます。この URL は、HTTP などのさまざまな URL ファイル システムを経由できます。詳細については、「*PKI* トラストプールの更新」の項を参照してください。CA バンドルで、**crypto pki trustpool import** コマンドを使用すると、グローバル VRF を介してトラフィックを転送できます。また、VRF と送信元インターフェイスを指定する **crypto pki trustpool policy** コマンドを設定すると、トラフィックが VRF を介して転送されることはありません。
ステップ 5	**exit** 例： `Device(config)# exit`	グローバル コンフィギュレーション モードを終了します。
ステップ 6	**show crypto pki trustpool** 例： `Device(config)# show crypto pki trustpool`	冗長形式でルータの PKI トラストプール証明書を表示します。

オプション PKI トラストプール ポリシー パラメータの設定

手順の概要

1. **enable**
2. **configure terminal**
3. **crypto pki trustpool policy**
4. **cabundle url** {*url* | **none**}
5. **chain-validation**
6. **crl** {**cache** {**delete-after** {*minutes* | **none**} | **query** *url*}
7. **default** *command-name*
8. **match certificate** *certificate-map-name* [**allow expired-certificate** | **override** {**cdp directory** *ldap-location* | **ocsp** {*number* **url** *url* | **trustpool** *name number* **url** *url*} | **sia** *number url*} | **skip** [**revocation-check** | **authorization-check**]]
9. **ocsp** {**disable-nonce** | **url** *url*}
10. **revocation-check** *method1* [*method2* [*method3*]]
11. **source interface** *name number*
12. **storage** *location*
13. **vrf** *vrf-name*
14. **show**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。

ステップ 3	**crypto pki trustpool policy**
	例：
	`Device(config)# crypto pki trustpool policy`
	`Device(ca-trustpool)#`
		CA PKI トラストプール ポリシー パラメータを設定するコマンドにアクセスできる、ca-trustpool コンフィギュレーション モードを入力します。トラストプール ポリシーは crl 検索プロセスにのみ影響し、トラストプール インポート プロセスには影響しません。

ステップ 4	**cabundle url** {*url* | **none**}
	例：
	`Device(ca-trustpool)# cabundle url`
	`http://www.cisco.com/security/pki/crl/crca2048.crl`
		PKI トラストプール認証局の CA 証明書バンドルのダウンロード元となる URL を指定します。
		• *url* 引数は CA 証明書バンドルの URL です。
		• **none** キーワードを指定すると、PKI トラストプール CA の自動更新が許可されません。

ステップ 5	**chain-validation** 例： `Device(ca-trustpool)# chain-validation`	ピアの証明書から PKI トラストプールのルート CA 証明書までチェーン検証を有効にします。デフォルトの検証はピア証明書の発行者で停止します。

ステップ 6	**crl** {**cache** {**delete-after** {*minutes* | **none**} | **query** *url*}
	例：
	`Device(ca-trustpool)# crl query`
	`http://www.cisco.com/security/pki/crl/crca2048.crl`
		PKI トラストプールの証明書失効リスト（CRL）クエリおよび CRL キャッシュ オプションを指定します。
		• **cache** キーワードは CRL キャッシュオプションを指定します。
		• **delete-after** キーワードは、タイムアウト後にキャッシュから CRL を削除します。
		• *minutes* 引数は、キャッシュから CRL が削除されるまで待機する分数（1 ～ 43,200）です。
		• **none** キーワードを指定すると、CRL がキャッシュ化されません。

	コマンドまたはアクション	目的
		• *url* 引数の **query** キーワードは、CRL を照会するために CA サーバーによって公開される URL を指定します。
ステップ 7	**default** *command-name* 例： `Device(ca-trustpool)# default crl query http://www.cisco.com/security/pki/crl/crca2048.crl`	ca-trustpool コンフィギュレーション サブコマンドの値をデフォルト値にリセットします。 • *command-name* 引数は、その適用可能なキーワードを設定した ca-trustpool コンフィギュレーション モード コマンドです。
ステップ 8	**match certificate** *certificate-map-name* [**allow expired-certificate** | **override** {**cdp directory** *ldap-location* | **ocsp** {*number* **url** *url* | **trustpool** *name number* **url** *url*} | **sia** *number url*} | **skip** [**revocation-check** | **authorization-check**]] 例： `match certificate mycert override ocsp 1 url http://ocspts.identrust.com`	PKI トラストプールの証明書マップを使用できるようにします。 • *certifcate-map-name* 引数は証明書マップ名と一致します。 • オプションの **allow expired-certificate** キーワードは、失効した証明書を無視します。 （注） このキーワードを設定しないと、ルータは失効した証明書を無視しません。 • **override** キーワードは、PKI トラストプール内にある証明書の Online Certificate Status Protocol（OCSP）または SubjectInfoAccess（SIA）属性フィールドを上書きします。 • **cdp** キーワードは、証明書の証明書分散ポイント（CDP）を上書きします。 • **directory** キーワードおよび *ldap-location* は、証明書内で上書きする http: または ldap: URL の CDP、あるいは LDAP ディレクトリを指定します。 • **ocsp** キーワードと *number* 引数および **url** キーワードと *url* 引数は、証明書内で上書きする OCSP シーケンス番号（0～10000）および URL を指定します。 • **trustpool** キーワードと *name* や *number* 引数および **url** キーワードと *url* 引数は、PKI トラストプール名、シーケンス番号、URL を指定することで、OCSP 証明書を確認するための PKI トラストプールを上書きします。

	コマンドまたはアクション	目的
		• **sia** キーワードと *number* や *url* 引数は、SIA シーケンス番号と URL を指定することで、証明書内の SIA URL を上書きします。 • オプションの **skip revocation-check** キーワードを組み合わせると、PKI トラストプールが特定の証明書を除いた証明書失効リスト（CRL）を適用できます。 （注） このキーワードの組み合わせを設定しないと、PKI トラストプールはすべての証明書に CRL を適用します。 • オプションの **skip authorization-check** キーワードを組み合わせると、公開キーインフラストラクチャ（PKI）と AAA サーバーとの統合を設定した場合に、証明書の認証、許可、アカウンティング（AAA）の確認をスキップします。 （注） このキーワードの組み合わせを設定せずに、PKI と AAA サーバとの統合を設定すると、証明書の AAA の確認が行われます。
ステップ 9	**ocsp** {**disable-nonce** | **url** *url*} 例： `Device(ca-trustpool)# ocsp url http://ocspts.identrust.com`	PKI トラストプールの OCSP 設定を指定します。 • **disable-nonce** キーワードは OCSP ナンス拡張部を無効にします。 • **url** キーワードと *url* 引数は、証明書の Authority Info Access（AIA）拡張部で上書きする（存在する場合）OCSP サーバーの URL を指定します。設定した PKI トラストプールに関連するすべての証明書は、指定した HTTP URL の OCSP サーバによって確認されます。使用可能な URL は、ホスト名、IPv4 アドレス、または IPv6 アドレスです。
ステップ 10	**revocation-check** *method1* [*method2* [*method3*]] 例：	PKI トラストプール ポリシー使用時の失効確認を無効にします。*method* 引数は、ルータが証明書の失効ステータスを確認するために使用されます。使用可能なキーワードは次のとおりです。

	コマンドまたはアクション	目的
	`Device(ca-trustpool)# revocation-check ocsp crl none`	• **crl** キーワードは、証明書失効リスト（CRL）で証明書の確認を行います。これはデフォルトの動作です。 • **none** キーワードでは、証明書の確認が必要ありません。 • **ocsp** キーワードは、Online Certificate Status Protocol（OCSP）サーバによって証明書の確認を行います。 2 番目と 3 番目の方法を指定した場合、各方法はその直前の方法でエラーが返された場合（サーバがダウンしている場合など）にだけ使用されます。
ステップ 11	**source interface** *name number* 例： `Device(ca-trustpool)# source interface tunnel 1`	CRL の取得、OCSP ステータス、または PKI トラストプールの CA 証明書バンドルのダウンロードに使用する送信元インターフェイスを指定します。 • *name* および *number* 引数は、PKI トラストプールの送信元アドレスとして使用されるインターフェイスのタイプと数値です。
ステップ 12	**storage** *location* 例： `Device(ca-trustpool)# storage storage disk0:crca2048.crl`	PKI トラストプール証明書がルータ上で保存される場合のファイル システム ロケーションを指定します。 • *location* は、PKI トラストプール証明書が保存されるファイル システム ロケーションです。ファイルシステム ロケーションのタイプには、**disk0:**、**disk1:**、**nvram:**、**unix:**、または名前付きファイル システムがあります。
ステップ 13	**vrf** *vrf-name* 例： `Device(ca-trustpool)# vrf myvrf`	登録、CRL の取得、および OCSP ステータスに使用される VPN ルーティングおよび転送（VRF）インスタンスを指定します。

ステップ 14	**show**
	例：
	`Device(ca-trustpool)# show`
	`Chain validation will stop at the first CA certificate in the pool`
	`  Trustpool CA certificates will expire 12:58:31 PST Apr 5 2012`
	`  Trustpool policy revocation order:  crl`
	`  Certficate matching is disabled`
	`  Policy Overrides:`
		ルータの PKI トラストプール ポリシーを表示します。

PKI トラストプール管理の設定例

例：PKI トラストプール管理の設定

次の **show crypto pki trustpool** コマンド出力は、PKI トラストプールの証明書を表示します。

（注） この例のコマンド出力は、デバッグのためなので省略されています。

```
Device# show crypto pki trustpool

CA Certificate
  Status: Available
  Version: 3
  Certificate Serial Number (hex): 00D01E474000000111C38A964400000002
  Certificate Usage: Signature
  Issuer:
    cn=DST Root CA X3
    o=Digital Signature Trust Co.
  Subject:
    cn=Cisco SSCA
    o=Cisco Systems
  CRL Distribution Points:
    http://crl.identrust.com/DSTROOTCAX3.crl
  Validity Date:
    start date: 12:58:31 PST Apr 5 2007
    end   date: 12:58:31 PST Apr 5 2012

CA Certificate
  Status: Available
  Version: 3
  Certificate Serial Number (hex): 6A6967B3000000000003
  Certificate Usage: Signature
  Issuer:
    cn=Cisco Root CA 2048
    o=Cisco Systems
  Subject:
    cn=Cisco Manufacturing CA
    o=Cisco Systems
  CRL Distribution Points:
    http://www.cisco.com/security/pki/crl/crca2048.crl
  Validity Date:
    start date: 14:16:01 PST Jun 10 2005
    end   date: 12:25:42 PST May 14 2029
```

次の **show crypto pki trustpool verbose** コマンド出力は、PKI トラストプールの証明書を表示します。

```
Device# show crypto pki trustpool verbose
```

```
CA Certificate
  Status: Available
  Version: 3
  Certificate Serial Number (hex): 01
  Certificate Usage: Signature
  Issuer:
    cn=Licensing Root - DEV
    o=Cisco
  Subject:
    cn=Licensing Root - DEV
    o=Cisco
  Validity Date:
    start date: 03:25:43 IST Apr 25 2013
    end   date: 03:25:43 IST Apr 25 2033
  Subject Key Info:
    Public Key Algorithm: rsaEncryption
    RSA Public Key: (2048 bit)
  Signature Algorithm: SHA256 with RSA Encryption
  Fingerprint MD5: 432CBFA0 32D2983A 8A56A319 FD28C6F9
  Fingerprint SHA1: 6341FCAF 19CE9FEE 961D92A5 D47390B5 2DD6D94D
  X509v3 extensions:
    X509v3 Key Usage: 6000000
      Key Cert Sign
      CRL Signature
    X509v3 Subject Key ID: 43214521 B5FB217A 1A4D1BB7 0236E664 CBEC8B65
    X509v3 Basic Constraints:
        CA: TRUE
    Authority Info Access:
  Associated Trustpoints: Trustpool
  Trustpool: Built-In
```

例：アップグレード中の SSH 接続に PKI トラストプールを使用

Cisco IOS XE Denali 16.3 へアップグレードの前に、トラストプールから新しいトラストポイントに証明書をコピーします。

```
Device # show run | sec pool
crypto pki trustpool policy
 revocation-check none
 source interface GigabitEthernet0/0/0
crypto pki certificate pool
 certificate ca 01
  308204FA 308202E2 A0030201 02020101 300D0609 2A864886 F70D0101 0C050030
  0E310C30 0A060355 04031303 61626330 1E170D31 36303730 35303435 3935335A
  170D3136 30373035 30353535 35335A30 0E310C30 0A060355 04031303 61626330
  82022230 0D06092A 864886F7 0D010101 05000382 020F0030 82020A02 82020100
  C78AA144 8EC1D18A 4EECC3E8 81450CC7 A85A4C57 AF59E584 5C1EA888 6EF70DA8
  33327D93 E1F6CED7 32BB4FCF 693F60E0 37000225 40F6F9C5 0462C4AD 899E5BDD
  ED779180 D6C75E1B FBE97D42 E2A7B35D DDC18C4D 4CCDE401 68F67A6D E40FD744
  904EE49F 40820640 C6E0B072 510BC40E A0883F6C E8DF5128 EFF3B5F4 B31E5C16
  217652FF AFC30EBF 593CB19C 56C0E793 2814D504 0E079E0C 8E9E856A BCADB19C
  F2376994 A0A040C1 7BC1E88F CF80F218 9C48B4D9 F84ED5C0 79827BD1 32448478
  8F1F82F2 C91A9479 692B6456 C53CF937 777D0C31 1B8A1F5E 24B33553 047C2448
  855CF974 DFA21665 8AD8A0E5 81ED8068 81688997 FF05118C 93A59CA0 7FD594F6
  B7B1898C 272E089A 3392A2C4 22A22625 2BC1E16F 95B2FC15 207CCA49 378AD3A6
  0C574197 C5E94D8C E6736271 CE0BA9AB ACB380E3 A8084243 4E038DD1 8E86E206
  E2269290 F1AFB29A D28CFB3A 5ABADE4A 21A59728 7174E7A3 2FF59C90 E6100C6E
  E2E8CB4C 91BD574D 57B5E18A 78F9CE75 624C4A2E 1A6EFCC3 7D1BB20B 1CC79024
```

```
CD2FBC4D 46BE1B7A 6EFD8F05 6FD84E91 51215E9B E5E952A4 6E2D1388 10075706
7D6FAF9B 3F7F8994 F39B9B5D 0C7CD5BC 40738877 5D9985AC 5AB6363D 811BA440
41A1639F 352F4F01 1994300A A4B85B75 01486CA0 4C4B3175 82038B26 BEFE1D2A
4AC0D577 7784FACF A6877D68 5D73DD04 DC8D942B DE3FC9FE 4C1FF715 A2E7A5AB
02030100 01A36330 61300F06 03551D13 0101FF04 05300301 01FF300E 0603551D
0F0101FF 04040302 0186301F 0603551D 23041830 168014CA 195EDBF1 51753A92
71342CA8 36DDABA9 63A93130 1D060355 1D0E0416 0414CA19 5EDBF151 753A9271
342CA836 DDABA963 A931300D 06092A86 4886F70D 01010C05 00038202 0100553B
FB77A348 C4447C40 BEB2DDFD 63C82441 3CBDC198 B5D5B1AB DF17C4E2 98AEAF2F
CD570939 BCC116E0 33CFF471 E91EE308 8B29B5BD 11DFACF9 A3AC3135 8BE81B22
ED205587 5DE04654 A051CC14 CA8D2A6E 81F924DA 001BB1C4 7F85F177 4E75D8EA
797CCAEF 1502492D 17627CD1 E39E295B 44C55884 8E6DFF68 2129B222 18E3187D
AB97B4A7 6F838E75 A8908566 AD9E6687 35B150DE 0C8C1B37 6F17FDAC 7A7C53A4
434F5CF3 6EB71957 E65EC5D2 7685B05B A9D8C0D3 2DB8F97E E6B37E11 C9E26F4F
BFB97745 83E1A214 461B0E49 0FFDEF21 A7CA5364 44416002 03A01F0C 2BC098D3
B50A4071 AC4D2234 4E55C5D4 0FD9C308 63F2A8D4 24D34613 B73EAA1B B407D56F
90EEF5C7 AE61C0D8 13FB493D 0E1C8F9B 1D2D6DEA 458CDE18 8753FF14 F8C75213
35557FCC 50405056 D9790AF0 EAC21646 2D9AF88D 59C05434 45F21248 0BB72191
74D951DD 9D23997E 1134611E 837137E6 C40C694E 7AB4A05F E8470E87 E0F6D924
A69A98A8 5AA2B9B3 B7446883 94A7230D EE3C6EDA 4A348351 FC40C16D 6FDC91EC
CEFF580B F7826DD1 1D1D07DB 17CA3298 8C510826 D2712E04 EB669909 3D8106EB
5391A5BA 80B7E981 B41AAEB9 CE4A5236 20E30AE7 01D5FDB3 604C5505 0F8C96DC
8F5CF569 5D90C1FB F5679221 B7B922C0 5F11C379 9EBA283C 45A209F7 132B8DA2
EAF4751B 290A1CAC C3E7978B 760FB05A 185991FE 4884FA1A D3EEDD7C 63
3B
      quit
```

新しいトラストポイントを作成し、設定モードで証明書を貼り付けます。

```
Device(config)#cry pki trust abc
Device(ca-trustpoint)#cry pki cert chain abc
Device(config-cert-chain)#certificate ca 01
```

16 進数で証明書を入力します

```
Device(config-pki-hexmode)#  308204FA 308202E2 A0030201 02020101 300D0609 2A864886
F70D0101 0C050030
Device(config-pki-hexmode)#  0E310C30 0A060355 04031303 61626330 1E170D31 36303730
35303435 3935335A
Device(config-pki-hexmode)#  170D3136 30373035 30353535 35335A30 0E310C30 0A060355
04031303 61626330
Device(config-pki-hexmode)#  82022230 0D06092A 864886F7 0D010101 05000382 020F0030
82020A02 82020100
Device(config-pki-hexmode)#  C78AA144 8EC1D18A 4EECC3E8 81450CC7 A85A4C57 AF59E584
5C1EA888 6EF70DA8
Device(config-pki-hexmode)#  33327D93 E1F6CED7 32BB4FCF 693F60E0 37000225 40F6F9C5
0462C4AD 899E5BDD
Device(config-pki-hexmode)#  ED779180 D6C75E1B FBE97D42 E2A7B35D DDC18C4D 4CCDE401
68F67A6D E40FD744
Device(config-pki-hexmode)#  904EE49F 40820640 C6E0B072 510BC40E A0883F6C E8DF5128
EFF3B5F4 B31E5C16
Device(config-pki-hexmode)#  217652FF AFC30EBF 593CB19C 56C0E793 2814D504 0E079E0C
8E9E856A BCADB19C
Device(config-pki-hexmode)#  F2376994 A0A040C1 7BC1E88F CF80F218 9C48B4D9 F84ED5C0
79827BD1 32448478
Device(config-pki-hexmode)#  8F1F82F2 C91A9479 692B6456 C53CF937 777D0C31 1B8A1F5E
24B33553 047C2448
Device(config-pki-hexmode)#  855CF974 DFA21665 8AD8A0E5 81ED8068 81688997 FF05118C
93A59CA0 7FD594F6
```

```
Device(config-pki-hexmode)#  B7B1898C 272E089A 3392A2C4 22A22625 2BC1E16F 95B2FC15
207CCA49 378AD3A6
Device(config-pki-hexmode)#  0C574197 C5E94D8C E6736271 CE0BA9AB ACB380E3 A8084243
4E038DD1 8E86E206
Device(config-pki-hexmode)#  E2269290 F1AFB29A D28CFB3A 5ABADE4A 21A59728 7174E7A3
2FF59C90 E6100C6E
Device(config-pki-hexmode)#  E2E8CB4C 91BD574D 57B5E18A 78F9CE75 624C4A2E 1A6EFCC3
7D1BB20B 1CC79024
Device(config-pki-hexmode)#  CD2FBC4D 46BE1B7A 6EFD8F05 6FD84E91 51215E9B E5E952A4
6E2D1388 10075706
Device(config-pki-hexmode)#  7D6FAF9B 3F7F8994 F39B9B5D 0C7CD5BC 40738877 5D9985AC
5AB6363D 811BA440
Device(config-pki-hexmode)#  41A1639F 352F4F01 1994300A A4B85B75 01486CA0 4C4B3175
82038B26 BEFE1D2A
Device(config-pki-hexmode)#  4AC0D577 7784FACF A6877D68 5D73DD04 DC8D942B DE3FC9FE
4C1FF715 A2E7A5AB
Device(config-pki-hexmode)#  02030100 01A36330 61300F06 03551D13 0101FF04 05300301
01FF300E 0603551D
Device(config-pki-hexmode)#  0F0101FF 04040302 0186301F 0603551D 23041830 168014CA
195EDBF1 51753A92
Device(config-pki-hexmode)#  71342CA8 36DDABA9 63A93130 1D060355 1D0E0416 0414CA19
5EDBF151 753A9271
Device(config-pki-hexmode)#  342CA836 DDABA963 A931300D 06092A86 4886F70D 01010C05
00038202 0100553B
Device(config-pki-hexmode)#  FB77A348 C4447C40 BEB2DDFD 63C82441 3CBDC198 B5D5B1AB
DF17C4E2 98AEAF2F
Device(config-pki-hexmode)#  CD570939 BCC116E0 33CFF471 E91EE308 8B29B5BD 11DFACF9
A3AC3135 8BE81B22
Device(config-pki-hexmode)#  ED205587 5DE04654 A051CC14 CA8D2A6E 81F924DA 001BB1C4
7F85F177 4E75D8EA
Device(config-pki-hexmode)#  797CCAEF 1502492D 17627CD1 E39E295B 44C55884 8E6DFF68
2129B222 18E3187D
Device(config-pki-hexmode)#  AB97B4A7 6F838E75 A8908566 AD9E6687 35B150DE 0C8C1B37
6F17FDAC 7A7C53A4
Device(config-pki-hexmode)#  434F5CF3 6EB71957 E65EC5D2 7685B05B A9D8C0D3 2DB8F97E
E6B37E11 C9E26F4F
Device(config-pki-hexmode)#  BFB97745 83E1A214 461B0E49 0FFDEF21 A7CA5364 44416002
03A01F0C 2BC098D3
Device(config-pki-hexmode)#  B50A4071 AC4D2234 4E55C5D4 0FD9C308 63F2A8D4 24D34613
B73EAA1B B407D56F
Device(config-pki-hexmode)#  90EEF5C7 AE61C0D8 13FB493D 0E1C8F9B 1D2D6DEA 458CDE18
8753FF14 F8C75213
Device(config-pki-hexmode)#  35557FCC 50405056 D9790AF0 EAC21646 2D9AF88D 59C05434
45F21248 0BB72191
Device(config-pki-hexmode)#  74D951DD 9D23997E 1134611E 837137E6 C40C694E 7AB4A05F
E8470E87 E0F6D924
Device(config-pki-hexmode)#  A69A98A8 5AA2B9B3 B7446883 94A7230D EE3C6EDA 4A348351
FC40C16D 6FDC91EC
Device(config-pki-hexmode)#  CEFF580B F7826DD1 1D1D07DB 17CA3298 8C510826 D2712E04
EB669909 3D8106EB
Device(config-pki-hexmode)#  5391A5BA 80B7E981 B41AAEB9 CE4A5236 20E30AE7 01D5FDB3
604C5505 0F8C96DC
Device(config-pki-hexmode)#  8F5CF569 5D90C1FB F5679221 B7B922C0 5F11C379 9EBA283C
45A209F7 132B8DA2
Device(config-pki-hexmode)#  EAF4751B 290A1CAC C3E7978B 760FB05A 185991FE 4884FA1A
D3EEDD7C 63
Device(config-pki-hexmode)#  3B
Device(config-pki-hexmode)#       quit
```

これで Cisco IOS XE Denali 16.3 にアップグレードできるようになりました。トラストプールの証明書は消えていますが、トラストポイントにはまだ保管されています。アップグレード後にトラストプールに証明書をインストールします。

PKI トラストプール管理の追加資料

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『Cisco IOS Master Command List, All Releases』
セキュリティ コマンド	• 『Cisco IOS Security Command Reference: Commands A to C』 • 『Cisco IOS Security Command Reference: Commands D to L』 • 『Cisco IOS Security Command Reference: Commands M to R』 • 『Cisco IOS Security Command Reference: Commands S to Z』[英語]

シスコのテクニカル サポート

説明	リンク
右の URL にアクセスして、シスコのテクニカル サポートを最大限に活用してください。これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

PKI トラストプール管理の機能情報

表 *160 : PKI* トラストプール管理の機能情報

機能名	リリース	機能情報
PKI トラストプール管理		次のコマンドが導入または変更されました。**cabundle url**、**chain-validation (ca-trustpool)**、**crypto pki trustpool import**、**crypto pki trustpool policy**、**crl**、**default (ca-trustpool)**、**match certificate (ca-trustpool)**、**ocsp**、**show (ca-trustpool)**、**show crypto pki trustpool**、**source interface (ca-trustpool)**、**storage**、**vrf (ca-trustpool)**、**show crypto pki trustpool built-in**、**crypto pki trustpool import clean ca-bundle**。

第 118 章

トラストポイントの PKI 分割 VRF

トラストポイントの PKI 分割 VRF 機能を使用すると、証明書登録と失効で VPN ルーティングおよび転送（VRF）を設定できます。

トラストポイントの PKI 分割 VRF に関する情報

トラストポイントの PKI 分割 VRF の概要

トラストポイントの PKI 分割 VRF 機能を使用すると、証明書登録と証明書失効リスト（CRL）の確認で VPN ルーティングおよび転送（VRF）を設定できます。VRF は、**crypto pki profile enrollment** コマンドの後に **enrollment url** コマンドを使用して登録プロファイルに設定し、この登録プロファイルをトラストポイントに添付します。登録および CRL に同じ VRF を設定したり、異なる VRF を設定したりできます。設定（登録または失効）に基づいて、対応する VRF が選択され、Simple Certificate Enrollment Protocol（SCEP）要求が各 VRF を介して送信されます。

さまざまなルーティングパスを介して登録および CRL を設定するには、**crypto pki profile enrollment** コマンドを使用して登録 url コマンドを設定する必要があります。ここで設定した VRF は登録 VRF として動作し、登録要求はこの VRF を介して送信されます。ただし、CRL はトラストポイントで設定したグローバル VRF を使用します。

enrollment url コマンドで設定した VRF がない場合は、登録が **crypto pki trustpoint** コマンドで設定されるグローバル登録に変わります。

トラストポイントの PKI 分割 VRF の設定方法

分割 VRF の設定

手順の概要

1. **enable**
2. **configure terminal**
3. **crypto pki profile enrollment** *label*
4. **enrollment url** *url* [**vrf** *vrf-name*]
5. **exit**
6. **show crypto pki profile**
7. **show crypto pki trustpoint**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**crypto pki profile enrollment** *label* 例： `Device(config)# crypto pki profile enrollment pki_profile`	登録プロファイルを定義し、ca-profile-enroll コンフィギュレーション モードを開始します。 • *label*：登録プロファイルの名前。登録プロファイル名は、**enrollment profile** コマンドで指定された名前と同じである必要があります。
ステップ 4	**enrollment url** *url* [**vrf** *vrf-name*] 例： `Device(ca-profile-enroll)# enrollment url http://entrust:81/cda-cgi/clientcgi.exe vrf vrf1`	証明書登録要求を HTTP または TFTP によって送信する CA サーバの URL および VPN ルーティングおよび転送（VRF）を指定します。
ステップ 5	**exit** 例： `Device(ca-profile-enroll)# exit`	ca-profile-enroll コンフィギュレーション モードを終了します。 • グローバル コンフィギュレーション モードを終了するため、このコマンドをもう一度入力します。

	コマンドまたはアクション	目的
ステップ 6	**show crypto pki profile** 例： `Device# show crypto pki profile`	（任意）PKI プロファイルの情報を表示します。
ステップ 7	**show crypto pki trustpoint** 例： `Device# show crypto pki trustpoint`	（任意）PKI トラストポイントの情報を表示します。

トラストポイントの PKI 分割 VRF の設定例

例：トラストポイントの PKI 分割 VRF の設定

同一 VRF を介した登録と証明書失効リスト

次の例では、同一VRFを介した登録と証明書失効リスト（CRL）の設定方法について示します。

```
crypto pki trustpoint trustpoint1
 enrollment url http://10.10.10.10:80
 vrf vrf1
 revocation-check crl
```

異なる VRF を介した登録と証明書失効リスト

次の例では、異なるVRFを介した登録と証明書失効リスト（CRL）の設定方法について示します。

```
crypto pki profile enrollment pki_profile
 enrollment url http://10.10.10.10:80 vrf vrf2

crypto pki trustpoint trustpoint1
 enrollment profile pki_profile
 vrf vrf1
 revocation-check crl
```

トラストポイントの PKI 分割 VRF の追加資料

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『Cisco IOS Master Command List, All Releases』

関連項目	マニュアル タイトル
セキュリティ コマンド	• 『Cisco IOS Security Command Reference Commands A to C』 • 『Cisco IOS Security Command Reference Commands D to L』 • 『Cisco IOS Security Command Reference Commands M to R』 • 『Cisco IOS Security Command Reference Commands S to Z』
推奨される暗号化アルゴリズム	『Next Generation Encryption』

シスコのテクニカル サポート

説明	リンク
右の URL にアクセスして、シスコのテクニカル サポートを最大限に活用してください。これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

Cisco TrustSec の概要の機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *161 : Cisco TrustSec* の概要の機能情報

機能名	リリース	機能情報
IPv6 の有効化 - インライン タギング	Cisco IOS XE Fuji 16.8.1	IPv6 のサポートが導入されました。

第 119 章

EST クライアント サポート

EST クライアント サポート機能を使用すると、SSL または TLS を使用して転送の安全性を保護しながら、すべてのトラストポイントの EST（Enrollment Over Secure Transport）を有効にできます。

Cisco TrustSec の概要の機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *162 : Cisco TrustSec* の概要の機能情報

機能名	リリース	機能情報
IPv6 の有効化 - インライン タギング	Cisco IOS XE Fuji 16.8.1	IPv6 のサポートが導入されました。

EST クライアント サポートの情報

EST クライアント サポートの概要

EST クライアント サポート機能を使用すると、証明書をプロビジョニングするための証明書管理プロトコルとして Enrollment over Secure Transport（EST）を使用できます。PKI コンポーネント内に統合された既存の SCEP 登録では、EST を追加すると、転送を保護する SSL または TLS を使用する新しいコンポーネントが導入されます。PKI にはすべての証明書が格納されます。

EST サポートを有効にするには、EST クライアントが、TLS 接続の確立中にサーバを認証する必要があります。この認証では、TLS サーバがクライアントのクレデンシャルを要求する場合があります。

EST クライアント サポートの前提条件

- **ip http authentication fore-close** コマンドを有効にします。

EST クライアント サポートの制約事項

- EST クライアントは TLS 1.2 のみをサポートしています。
- 証明書属性要求はサポートされていません。
- CA 証明書のロールオーバーはサポートされていません。
- 証明書のない TLS 認証はサポートされていません。
- HTTP ベースのクライアント認証はサポートされていません。

EST クライアント サポートの設定方法

EST を使用するためのトラストポイントの設定

ユーザが登録プロファイルを使用できるようにすることで、EST（Enrolment Over Secure Transport）を使用するトラストポイントを設定するには、この作業を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **crypto pki profile enrollment**ラベル

4. **method-est**
5. **enrollment url***url*［**vrf** *vrf name*］
6. **enrollment credential** *label*
7. **exit**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**crypto pki profile enrollment**ラベル 例： `Device(config)# crypto pki profile enrollment pki_profile`	登録プロファイルを定義し、ca-profile-enroll コンフィギュレーション モードを開始します。 • *label*：登録プロファイルの名前。登録プロファイル名は、**enrollment profile** コマンドで指定された名前と同じである必要があります。
ステップ 4	**method-est** 例： `Device(ca-profile-enroll)# method-est`	登録プロファイルでESTの使用を選択できるようにします。
ステップ 5	**enrollment url***url*［**vrf** *vrf name*］ 例： `Device(ca-profile-enroll)# enrollment url http://entrust:81/cda-cgi/clientcgi.exe vrf vrf1`	証明書登録に登録プロファイルを使用するように指定します。 （注） 認証 URL が指定されていない場合は、登録 URL が認証に使用されます。
ステップ 6	**enrollment credential** *label* 例： `Device(ca-profile-enroll)# enrollment credential test_label`	TLS クライアント認証にプロファイルで現在利用可能なトラストポイントログイン情報を提供します。
ステップ 7	**exit** 例： `Device(ca-profile-enroll)# exit`	ca-profile-enroll コンフィギュレーション モードを終了します。

EST クライアントサポートの設定の確認

次の show コマンドを使用すると、EST クライアントサポートの設定を確認できます。

- **show crypto pki profile**
- **show crypto pki trustpoints estclient status**

EST クライアント サポートの設定例

EST を使用するためのトラストポイントの設定

次の例では、Enrollment over Secure Transport（EST）を使用するためにトラストポイントを設定する方法について示します。

```
crypto pki profile enrollment pki_profile
 method-est
 enrollment url http://www.example.com/BigCA/est/simpleenroll.dll
 enrollment credential test_label
```

EST クライアントサポートの確認

次に、EST クライアントサポートの設定を確認する **show crypto pki trustpoints estclient status** コマンドの出力例を示します。

```
Router# show crypto pki trustpoints estclient status
Trustpoint estclient:
  Issuing CA certificate configured:
    Subject Name:
     cn=estExampleCA
    Fingerprint MD5: B9D0403C 7D33F1AA F9957796 CA6E86AA
    Fingerprint SHA1: F3698C9C DCB2B5F2 A38EBCB4 1DBA6A90 9F877A5B
  Router Signature certificate configured:
    Subject Name:
     cn=estclientrouter
    Fingerprint MD5: B740849B 37016DB7 A6797CE4 D6140D27
    Fingerprint SHA1: F032B015 50BB5742 2619EFC6 F1F0B8B1 31D9906D
  State:
    Keys generated ..... Yes (Signature, non-exportable)
    Issuing CA authenticated ..... Yes
    Certificate request(s) ..... Yes
```

次に、再登録前と再登録後のステータスを示す **show crypto pki certificate estclient** コマンドの出力例を示します。

```
BEFORE REENROLLMENT

Router# show crypto pki certificate estclient


Certificate
  Status: Available
  Certificate Serial Number (hex): 2603
  Certificate Usage: Signature
  Issuer:
    cn=estExampleCA
```

```
  Subject:
    Name: estclientrouter
    cn=estclientrouter
  CRL Distribution Points:
    http://example.com/crl.pem
  Validity Date:
    start date: 19:31:24 GMT Feb 8 2019
    end   date: 19:31:24 GMT Feb 8 2020
    renew date: 19:35:50 GMT Feb 8 2019
  Associated Trustpoints: estclient

CA Certificate
  Status: Available
  Certificate Serial Number (hex): 00ACFCD09D3182CBEB
  Certificate Usage: General Purpose
  Issuer:
    cn=estExampleCA
  Subject:
    cn=estExampleCA
  Validity Date:
    start date: 09:40:47 GMT Mar 28 2018
    end   date: 09:40:47 GMT Mar 28 2019
  Associated Trustpoints: estclient ROOT


AFTER REENROLLMENT

show crypto pki certificates estclient
Certificate
  Status: Available
  Certificate Serial Number (hex): 4B
  Certificate Usage: Signature
  Issuer:
    cn=estExampleCA
  Subject:
    Name: estclientrouter
    cn=estclientrouter
  CRL Distribution Points:
    http://example.com/crl.pem
  Validity Date:
    start date: 07:34:05 GMT Feb 9 2019
    end   date: 07:34:05 GMT Feb 9 2020
    renew date: 19:38:35 GMT Feb 8 2019
  Associated Trustpoints: estclient

CA Certificate
  Status: Available
  Certificate Serial Number (hex): 00E5EEC53E0FBD597D
  Certificate Usage: General Purpose
  Issuer:
    cn=estExampleCA
  Subject:
    cn=estExampleCA
  Validity Date:
    start date: 04:59:30 GMT Dec 20 2018
    end   date: 04:59:30 GMT Dec 20 2019
  Associated Trustpoints: estclient ROOT_SEC
```

EST クライアント サポートの追加資料

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『Cisco IOS Master Command List, All Releases』
セキュリティ コマンド	• 『Cisco IOS Security Command Reference Commands A to C』 • 『Cisco IOS Security Command Reference Commands D to L』 • 『Cisco IOS Security Command Reference Commands M to R』 • 『Cisco IOS Security Command Reference Commands S to Z』

標準および RFC

標準/RFC	タイトル
RFC 7030	『*Enrollment over Secure Transport*』
RFC 2818	『*HTTP Over TLS*』
RFC 6125	『*Representation and Verification of Domain-Based Application Service Identity within Internet Public Key Infrastructure Using X.509 (PKIX) Certificates in the Context of Transport Layer Security (TLS)*』
RFC 2510	『*Internet X.509 Public Key Infrastructure Certificate Management Protocols*』
RFC 4210	『*Internet X.509 Public Key Infrastructure Certificate Management Protocol (CMP)*』

シスコのテクニカル サポート

説明	リンク
右の URL にアクセスして、シスコのテクニカル サポートを最大限に活用してください。これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

第 120 章

OCSP 応答ステープリング

OCSP 応答ステープリング機能では、Online Certificate Status Protocol（OCSP）を使用してデジタル証明書に含まれるピアのユーザまたはデバイス クレデンシャルの有効期間を確認できます。

OCSP 応答ステープリングの情報

OCSP 応答ステープリングの概要

ピアが失効情報を取得し、この情報を検証して証明書失効のステータスを確認する場合、Online Certificate Status Protocol（OCSP）は証明書失効を確認するための方式になります。この方式では、証明書失効のステータスは、クラウドを介してOCSP応答者に到達するピアの能力、または証明書失効情報を検索する際の証明書送信者の能力によって制限されます。

OCSP 応答ステープリングは、デバイスの独自の証明書で OCSP 応答を取得する新しい方式をサポートします。この機能を使用すると、OCSP サーバに接続し、この結果とその証明書をピアに直接送信して、その独自の証明書失効情報を入手できます。その結果、ピアがOCSP応答者に接続する必要はありません。

OCSP 応答ステープリングの設定方法

EKU 属性を要求するための PKI クライアントの設定

次の作業を実行し、OCSP（Online Certificate Status Protocol）応答ステープリングを設定します。

手順の概要

1. **enable**
2. **configure terminal**
3. **crypto pki trustpoint** *name*
4. **ocsp url** *url*
5. **eku request** *attribute*
6. **match eku** *attribute*
7. **revocation-check** *method1* ［*method2* ［*method3*］］
8. **exit**
9. **exit**
10. **show cry pki counters**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 1. パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**crypto pki trustpoint** *name* 例： `Device(config)# crypto pki trustpoint msca`	トラストポイントおよび設定された名前を宣言して、CA トラストポイント コンフィギュレーション モードを開始します。

ステップ 4	**ocsp url** *url*
	例：
	`Device(ca-trustpoint)# ocsp url http://ocsp-server`
	例：
	`Device(ca-trustpoint)# ocsp url http://10.10.10.1:80`
	例：
	`Device(ca-trustpoint)# ocsp url http://[2001DB8:1:1::2]:80`
		url 引数は、トラストポイントが証明書ステータスをチェックできるように OCSP サーバーの URL を指定します。この URL は、証明書の AIA 拡張部に指定されている OCSP サーバーの URL（存在する場合）を上書きします。設定したトラストポイントに関連するすべての証明書は、OCSP サーバーによって確認されます。使用可能な URL は、ホスト名、IPv4 アドレス、または IPv6 アドレスです。
		（注） OCSP 要求 URL が HTTP プロキシサーバーではなく **ocsp url** *url* コマンドで設定されていることを確認してください。

	コマンドまたはアクション	目的
ステップ 5	**eku request** *attribute* 例： `Device(ca-trustpoint)# eku request ssh-client`	証明書に指定した eku *attribute* を含めるように要求します。この要求は、PKI クライアントで設定した場合、登録時に CA サーバに送信されます。 *attribute* 引数には次のいずれかを指定できます。 • client-auth • code-signing • email-protection • ipsec-end-system • ipsec-tunnel • ipsec-user • ocsp-signing • server-auth • time-stamping • ssh-server • ssh-client
ステップ 6	**match eku** *attribute* 例： `Device(ca-trustpoint)# match eku client-auth`	指定した属性が証明書内に存在し、他の検証が失敗した場合のみ、PKI はピア証明書を検証できます。 *attribute* 引数には次のいずれかを指定できます。 • client-auth • code-signing • email-protection • ipsec-end-system • ipsec-tunnel • ipsec-user • ocsp-signing • server-auth • time-stamping • ssh-server • ssh-client

	コマンドまたはアクション	目的
ステップ 7	**revocation-check** *method1* ［*method2* ［*method3*］］ 例： `Device(ca-trustpoint)# revocation-check ocsp none`	（任意）証明書の失効ステータスをチェックします。 • crl：CRL によって証明書をチェックします。これがデフォルトのオプションです。 • none：証明書のチェックを無視します。 • ocsp：OCSP サーバによって証明書をチェックします。 2 番目と 3 番目の方法を指定した場合、各方法はその直前の方法でエラーが返された場合（サーバがダウンしている場合など）にだけ使用されます。
ステップ 8	**exit** 例： `Device(ca-trustpoint)# exit`	CA トラストポイント コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードに戻ります。
ステップ 9	**exit** 例： `Device(config)# exit`	特権 EXEC モードに戻ります。
ステップ 10	**show cry pki counters** 例： `Device# show cry pki counters`	（任意）デバイスの PKI カウンタを表示します。

EKU 属性を追加するための PKI サーバの設定

次の作業を実行し、OCSP（Online Certificate Status Protocol）応答ステープリングを設定します。

手順の概要

1. **enable**
2. **configure terminal**
3. **ip http server**
4. **crypto pki server** *cs-label*
5. **eku request** *attribute*
6. **exit**
7. **exit**
8. **show crypto pki counters**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 1. パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ip http server** 例： `Device(config)# ip http server`	ご使用のシステムの HTTP サーバをイネーブルにします。
ステップ 4	**crypto pki server** *cs-label* 例： `Device(config)# crypto pki server server-pki`	証明書サーバのラベルを定義し、証明書サーバ コンフィギュレーション モードを開始します。 （注） 手動で RSA キー ペアを生成した場合、*cs-label* 引数はキー ペアの名前と一致する必要があります。
ステップ 5	**eku request** *attribute* 例： `Device(cs-server)# eku request ssh-server`	証明書に指定した eku *attribute* を含めるように要求します。 *attribute* 引数には次のいずれかを指定できます。 • client-auth • code-signing • email-protection • ipsec-end-system • ipsec-tunnel • ipsec-user • ocsp-signing • server-auth • time-stamping • ssh-server • ssh-client

	コマンドまたはアクション	目的
ステップ 6	**exit** 例： `Device(cs-server)# exit`	cs-server コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードに戻ります。
ステップ 7	**exit** 例： `Device(config)# exit`	特権 EXEC モードに戻ります。
ステップ 8	**show crypto pki counters** 例： `Device# show crypto pki counters`	（任意）デバイスの PKI カウンタを表示します。

例

次に、**show crypto pki counters** の出力例を示します。

```
Device# show crypto pki counters

PKI Sessions Started: 0
PKI Sessions Ended: 0
PKI Sessions Active: 0
Successful Validations: 0
Failed Validations: 0
Bypassed Validations: 0
Pending Validations: 0
CRLs checked: 0
CRL - fetch attempts: 0
CRL - failed attempts: 0
CRL - rejected busy fetching: 0
OCSP - fetch requests: 0
OCSP - received responses: 0
OCSP - failed attempts: 0
OCSP - staple requests: 0
AAA authorizations: 0
```

OCSP 応答ステープリングの追加資料

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『Master Command List, All Releases』

関連項目	マニュアル タイトル
セキュリティ コマンド	• 『Cisco IOS Security Command Reference Commands A to C』 • 『Cisco IOS Security Command Reference Commands D to L』 • 『Cisco IOS Security Command Reference Commands M to R』 • 『Cisco IOS Security Command Reference Commands S to Z』

標準および RFC

標準/RFC	タイトル
RFC 2560	『*X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP*』
RFC 4806	『*Online Certificate Status Protocol (OCSP) Extensions to IKEv2*』
RFC 5280	『*Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile*』
RFC 6187	『*X.509v3 Certificates for Secure Shell Authentication*』
RFC 6066	『*Transport Layer Security (TLS) Extensions: Extension Definitions*』

MIB

MIB	MIB のリンク
	選択したプラットフォーム、Cisco IOS リリース、およびフィーチャ セットに関する MIB を探してダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

シスコのテクニカル サポート

説明	リンク
シスコのサポート Web サイトでは、シスコの製品やテクノロジーに関するトラブルシューティングにお役立ていただけるように、マニュアルやツールをはじめとする豊富なオンライン リソースを提供しています。 お使いの製品のセキュリティ情報や技術情報を入手するために、Cisco Notification Service（Field Notice からアクセス）、Cisco Technical Services Newsletter、Really Simple Syndication（RSS）フィードなどの各種サービスに加入できます。 シスコのサポート Web サイトのツールにアクセスする際は、Cisco.com のユーザ ID およびパスワードが必要です。	http://www.cisco.com/support

Cisco TrustSec の概要の機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *163 : Cisco TrustSec* の概要の機能情報

機能名	リリース	機能情報
IPv6 の有効化 - インライン タギング	Cisco IOS XE Fuji 16.8.1	IPv6 のサポートが導入されました。

第 121 章

PKI の Route Processor Redundancy の設定

Route Processor Redundancy は、ハイ システム アベイラビリティ機能の代替機能です。HSA によって、システムはアクティブ ルート スイッチ プロセッサ（RSP）が停止したときに、スタンバイ RSP をリセットして使用できます。RPR を使用すると、アクティブ RSP に重大エラーが発生したとき、RPR がアクティブ RSP とスタンバイ RSP の間で瞬時に切り替えを実現するため、計画外のダウンタイムを削減できます。

Route Processor Redundancy 機能は、現時点では、デュアル RP をサポートする Cisco ASR プラットフォーム（ASR 1006、ASR 1009、ASR 1013 など）で使用できます。

（注） Route Processor Redundancy は、トラストプールのインポートをサポートしています。

Route Processor Redundancy の設定の前提条件

- フェールオーバー時にはセカンダリ RSP がプライマリ RSP をサポートできる必要があるため、両方の RSP で同じメモリを使用する必要があります。

Route Processor Redundancy の設定に関する制約事項

- Route Processor Redundancy 機能は、デュアル RP をサポートするプラットフォームのみをサポートします。
- Route Processor Redundancy は、デュアル RSP をサポートするルータ上でのみサポートされます。

• RA（登録局）は検証されていないため、設定することは推奨されません。

Route Processor Redundancy の設定方法

Route Processor Redundancy SSO モードの設定

```
configure terminal
redundancy
 mode sso
 main-cpu
  standby console enable
exit
```

Route Processor Redundancy の確認

```
show redundancy states
show crypto pki server
show crypto pki certificates tname
```

Route Processor Redundancy SSO モードの設定例

サーバー側の設定例：

```
asr1k(config)#ip http server

asr1k(config)#crypto pki trustpoint ROOTCA

asr1k(ca-trustpoint)#hash sha512

asr1k(ca-trustpoint)#revocation-check none

asr1k(ca-trustpoint)#rsakeypair  ROOTCA 2048

asr1k(ca-trustpoint)#crypto pki server ROOTCA

asr1k(cs-server)#issuer-name CN=ROOTCA C=pki

asr1k(cs-server)#lifetime certificate 00 00 15

asr1k(cs-server)#lifetime ca-certificate 00 00 25

asr1k(cs-server)#lifetime crl 6

asr1k(cs-server)#serial-number 0x1

asr1k(cs-server)#auto-rollover 00 00 24

% The archive password is not configured. Rollover CA keys and certificates will not be
 automatically archived.

asr1k(cs-server)#grant auto

asr1k(cs-server)#database url tftp://<ip>//
```

```
% Server database url was changed. You need to move the
% existing database to the new location.
asr1k(cs-server)#database url p12 tftp://<ip>//
asr1k(cs-server)#database level complete
asr1k(cs-server)#database archive pkcs12 password <pwd>
asr1k(cs-server)#end
```

クライアント側の設定例：

```
crypto pki trustpoint client
 enrollment url http://<ip>:80
 usage ike
 subject-name CN=R1 C=pki
 revocation-check crl
 rsakeypair client 2048
 hash sha512
```

Route Processor Redundancy SSO モードの確認例

```
show redundancy states
       my state = 13 -ACTIVE
     peer state = 8  -STANDBY HOT
           Mode = Duplex
           Unit = Primary
        Unit ID = 48

Redundancy Mode (Operational) = sso
Redundancy Mode (Configured)  = sso
Redundancy State              = sso
     Maintenance Mode = Disabled
    Manual Swact = enabled
 Communications = Up

   client count = 132
```

```
 client_notification_TMR = 30000 milliseconds
           RF debug mask = 0x0
show crypto pki server
Certificate Server ROOTCA:
    Status: enabled
    State: enabled
    Server's configuration is locked  (enter "shut" to unlock it)
    Issuer name: CN=ROOTCA C=pki
    CA cert fingerprint: F2BF3707 D9F6F5F3 E0D111D8 A8486437
    Granting mode is: auto
    Last certificate issued serial number (hex): 2
    CA certificate expiration timer: 14:15:50 IST Mar 31 2019
    CRL NextUpdate timer: 14:15:50 IST Mar 31 2019
    Current primary storage dir: tftp://9.45.3.3//
    Current storage dir for .p12 files: tftp://9.45.3.3//
    Database Level: Complete - all issued certs written as <serialnum>.cer
    Auto-Rollover configured, overlap period 0 days
    Autorollover timer: 13:51:50 IST Mar 31 2019
    Redundancy configured.  This is active.
```

（注） サーバーは、アクティブ RP でのみ有効であり、スタンバイモードでは無効状態になります。

```
show crypto pki certificates client
Certificate
  Status: Available
  Certificate Serial Number (hex): 03
  Certificate Usage: General Purpose
  Issuer:
    cn=ROOTCA C=pki
  Subject:
    Name: asr1k
    hostname=asr1k
```

```
    cn=R1 C=pki
  Validity Date:
    start date: 00:42:04 IST Mar 11 2019
    end   date: 01:02:04 IST Mar 11 2019
  Associated Trustpoints: client

CA Certificate
  Status: Available
  Certificate Serial Number (hex): 02
  Certificate Usage: Signature
  Issuer:
    cn=ROOTCA C=pki
  Subject:
    cn=ROOTCA C=pki
  Validity Date:
    start date: 00:40:34 IST Mar 11 2019
    end   date: 00:40:34 IST Mar 9 2020
  Associated Trustpoints: client
```

第 XII 部

ゾーンベース ポリシー ファイアウォール

- IPv6 ファイアウォールに対する FTP66 ALG サポート （1881 ページ）
- 分散型サービス妨害攻撃に対する保護 （1899 ページ）
- ファイアウォール リソース管理の設定 （1933 ページ）
- IPv6 ファイアウォールでの分散型サービス妨害攻撃の防止およびリソース管理のサポート （1941 ページ）
- フローあたりの同時パケットの設定可能数 （1979 ページ）
- ファイアウォール高速ロギング （1991 ページ）
- TCP リセット セグメント制御 （2021 ページ）
- ゾーンベース ポリシー ファイアウォールでの TCP ウィンドウ スケーリングのルーズ チェック オプション （2029 ページ）
- ゾーンベース ポリシー ファイアウォールでの ALG と AIC の有効化 （2037 ページ）
- ファイアウォール TCP SYN Cookie の設定 （2049 ページ）
- ACL のオブジェクト グループ （2061 ページ）
- Cisco ファイアウォール SIP 機能拡張 ALG （2083 ページ）
- ファイアウォールと NAT に対する MSRPC ALG サポート （2095 ページ）
- ファイアウォールと NAT に対する Sun RPC ALG サポート （2107 ページ）
- ゾーンベース ファイアウォール ALG および AIC 条件付きデバッグおよびパケットトレースのサポート （2121 ページ）
- ファイアウォールと NAT に対するハイ アベイラビリティ サポートを使用した ALG - H.323 vTCP （2125 ページ）
- NAT とファイアウォールの SIP ALG 強化 （2135 ページ）
- DoS 攻撃に対する SIP ALG レジリエンス （2147 ページ）

第 122 章

ゾーンベース ポリシー ファイアウォール

このモジュールでは、ゾーンと呼ばれるインターフェイス グループ間の Cisco 単方向ファイアウォール ポリシーについて説明します。Cisco 単方向ファイアウォール ポリシーがリリースされるまでは、Cisco ファイアウォールがインターフェイス上の検査ルールとしてのみ設定されていました。設定されたインターフェイスを出入りするトラフィックは、検査ルールが適用される方向に基づいて検査されました。

（注） Cisco IOS XE は、ゾーンベース ファイアウォール設定上で Virtual Fragmentation Reassembly（VFR）をサポートします。インターフェイスをゾーンに追加してインターフェイス上のファイアウォールを有効にすると、VFR は同じインターフェイス上で自動的に設定されます。

ゾーンベース ポリシー ファイアウォールに関する機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *164 :* ゾーンベース ポリシー ファイアウォールに関する機能情報

機能名	リリース	機能情報
ゾーンベース ファイアウォールの再分類	Cisco IOS XE Bengaluru 17.6.1	ゾーンベース ファイアウォールの再分類機能が導入されました。この機能は、既存のセッションでポリシー設定に変更がある場合に、その変更を適用します。
ASR1000 上のゾーンベース ファイアウォールに対するスマートライセンスサポート	Cisco IOS XE Denali 16.3.1	**show license all** コマンドが変更されました。
ゾーンベース ポリシー ファイアウォールでの Out-of-Order パケット処理	Cisco IOS XE リリース 3.5S	Out-of-Order パケット処理機能は、セッションに DPI が必要ない場合に、OoO パケットのルータの通過を許可し、宛先への到達を可能にします。OoO パケットが含まれるすべてのレイヤ 4 トラフィックに、宛先へのパス スルーが許可されます。ただし、セッションでレイヤ 7 インスペクションが必要な場合は、OoO パケットがドロップされます。
IOS-XE ZBFW と暗号 VPN の相互運用	Cisco IOS XE リリース 3.17S	IOS-XE ZBFW と暗号 VPN の相互運用機能は、FlexVPN DVTI 上でのゾーンベース ファイアウォールの有効化をサポートします。
マルチパス TCP のゾーンベース ファイアウォール サポート	Cisco IOS XE リリース 3.13S	マルチポイント TCP は、ゾーンベース ファイアウォール レイヤ 4 インスペクションとシームレスに連動します。マルチポイント TCP は、アプリケーション レイヤ ゲートウェイ（ALG）とアプリケーション インスペクションおよびコントロール（AIC）とは連動しません。
Firewall：NetMeeting Directory (LDAP) ALG サポート	Cisco IOS XE Release 3.1S	LDAP は、ディレクトリ サービスに保存されている情報の照会および更新に使用されるアプリケーション プロトコルです。ファイアウォール - Netmeeting（LDAP）Directory ALG サポート機能は、Cisco ファイアウォールでレイヤ 4 LDAP インスペクションをデフォルトでサポートできるようにします。 次のコマンドが導入されました。**match protocol**
ゾーンベース ファイアウォールでのデバッグ可能性強化（フェーズ II）	Cisco IOS XE Release 3.10S	デバッグ可能性強化ゾーンベースファイアウォール機能は、デバッグログのシビラティ（重大度）レベルを提供します。

機能名	リリース	機能情報
ゾーンベース ファイアウォール - デフォルト ゾーン	Cisco IOS リリース 2.6	ゾーンベース ファイアウォール - デフォルト ゾーン機能は、ゾーンとデフォルト ゾーンを構成するゾーン ペアでファイアウォール ポリシーを設定可能にするデフォルト ゾーンを導入します。明示的なゾーンメンバーシップのないインターフェイスがデフォルトゾーンに属します。
ゾーンベースポリシーファイアウォール	Cisco IOS リリース 2.1	ゾーンベース ポリシー ファイアウォール機能は、ゾーンと呼ばれるインターフェイスのグループ間に Cisco IOS XE ソフトウェアの単方向ファイアウォール ポリシーを提供します。

ゾーンベース ポリシー ファイアウォールについて

以下のセクションでは、ゾーンベースポリシーファイアウォールについて詳しく説明します。

トップレベル クラス マップとポリシー マップ

トップレベル クラス マップでは、高レベルでトラフィック ストリームを識別できます。これを実現するには、**match access-group** コマンドおよび **match protocol** コマンドを使用します。トップレベル クラス マップは、レイヤ 3 およびレイヤ 4 クラス マップとも呼ばれます。トップレベルポリシーマップでは、**inspect**、**drop**、および **pass** コマンドを使用して、ハイレベルのアクションを定義できます。ポリシー マップは、ターゲット（ゾーン ペア）に付加できます。

（注） ゾーン ペアで設定できるのは、検査タイプのポリシーだけです。

ゾーンの概要

ゾーンとは、同様の機能を果たすインターフェイスのグループです。ゾーンを利用して、Cisco IOS XE ファイアウォールをどこに適用するかを指定できます。たとえば、デバイスで、ギガビット イーサネット インターフェイス 0/0/0 とギガビット イーサネット インターフェイス 0/0/1 をローカル LAN に接続できるとします。これら 2 つのインターフェイスは、内部ネットワークを表している点で同類です。そのため、ファイアウォール設定でゾーンとしてグループ化できます。

デフォルトでは、同じゾーン内のインターフェイス間のトラフィックはポリシーの制約を受けず、自由にゾーンを通過できます。ファイアウォール ゾーンはセキュリティ機能に使用されます。

（注） ゾーンは、異なる VPN ルーティングおよび転送（VRF）インスタンスのインターフェイスまでは拡大できません。

ダイナミックマルチポイントVPN（DMVPN）トンネルの場合、ゾーンベース ファイアウォールは、内部パケットを検査し、評価のみを行います。内部パケットがGeneric Routing Encapsulation（GRE）およびカプセル化セキュリティペイロード（ESP）ペイロードにカプセル化されると、それ以上の検査なしで転送されます。着信パケットの場合、ZBF 評価の前に ESP と GRE のカプセル化が解除されます。セルフから外部または外部からセルフのゾーンペアでのESPおよびGRE トラフィックに関する明示的なルールを設定する必要はありません。

セキュリティ ゾーン

セキュリティ ゾーンとは、ポリシーを適用できるインターフェイスのグループです。

インターフェイスをゾーンにグループ化するには、次の 2 つの手順を実行します。

- インターフェイスを付加できるようにゾーンを作成します。
- インターフェイスを特定のゾーンのメンバーとなるように設定します。

デフォルトでは、トラフィックは、同じゾーンのメンバーであるインターフェイス間を通ります。

インターフェイスがセキュリティゾーンのメンバーである場合、そのインターフェイスと別のゾーンにあるインターフェイスの間を通るすべてのトラフィック（デバイスに送信されるか、デバイスによって開始されたトラフィックを除く）はデフォルトでドロップされます。ゾーンメンバーインターフェイスおよび別のインターフェイスに対する両方向のトラフィックを許可するには、そのゾーンをゾーンペアの一部にして、そのゾーンペアにポリシーを適用する必要があります。ポリシーがinspectまたはpassアクションによってトラフィックを許可する場合、トラフィックはインターフェイスを通過できます。

ゾーンを設定するときに考慮する基本的な規則を次に示します。

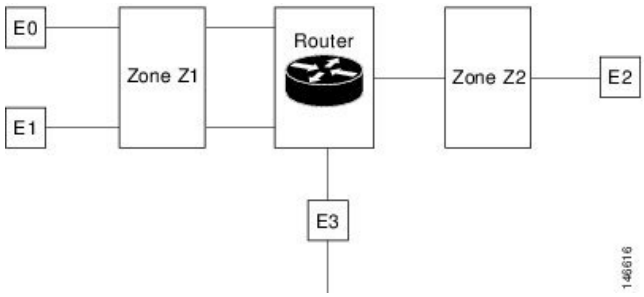
- ゾーンインターフェイスからゾーン外のインターフェイスへのトラフィックまたはゾーン外のインターフェイスからゾーンインターフェイスへのトラフィックは常にドロップされます。ただし、デフォルトゾーンが有効でないことが条件です（デフォルトゾーンはゾーン外のインターフェイスです）。
- 2 つのゾーンインターフェイス間のトラフィックは、各ゾーンにゾーンペアの関係があるかどうか、およびそのゾーンペアにポリシーが設定されているかどうかが検査されます。
- デフォルトでは、同一ゾーン内の2つのインターフェイス間のすべてのトラフィックは常に許可されます。
- ゾーンペアは、ゾーンを送信元ゾーンおよび宛先ゾーンの両方として設定できます。このゾーンペアで検査ポリシーを設定して、2 つのゾーン間のトラフィックを検査、転送、またはドロップできます。
- インターフェイスがメンバーになれるのは、1 つのセキュリティ ゾーンだけです。

- インターフェイスがセキュリティ ゾーンのメンバーの場合、そのゾーンを含むゾーン ペアで明示的なゾーン間ポリシーを設定しない限り、方向に関係なくそのインターフェイスを通過するすべてのトラフィックがブロックされます。
- トラフィックがデバイスのすべてのインターフェイス間を通過するようにするには、これらのインターフェイスが1つのセキュリティゾーンまたは別のセキュリティゾーンのメンバーである必要があります。すべてのデバイスインターフェイスがセキュリティゾーンのメンバーである必要はありません。
- ゾーンに関連付けられたすべてのインターフェイスは、同じ仮想ルーティングおよび転送（VRF）に含まれている必要があります。

図 1 には、次のことが示されています。

- インターフェイス E0 と E1 はセキュリティ ゾーン Z1 のメンバーです。
- インターフェイス E2 は、セキュリティ ゾーン Z2 のメンバーです。
- インターフェイス E3 は、どのセキュリティ ゾーンのメンバーでもありません。

図 *51* : セキュリティ ゾーンの制約



- ゾーン ペアとポリシーは、同じゾーンで設定されます。インターフェイス E0 と E1 は同じセキュリティ ゾーン（Z1）のメンバーなので、2つのインターフェイス間のトラフィックは自由に流れます。
- ポリシーが設定されていない場合、他のインターフェイス間（E0 と E2 の間、E1 と E2 の間、E3 と E1 の間、E3 と E2 の間など）でトラフィックは流れません。
- トラフィックを許可する明示的なポリシーがゾーン Z1 とゾーン Z2 間で設定されている場合だけ、E0 または E1 と E2 間でトラフィックが流れます。
- デフォルトゾーンが有効になっていないかぎり、E3 と E0、E1、または E2 の間でトラフィックは流れません。

（注） Cisco ASR 1000 シリーズ アグリゲーション サービス ルータでは、ファイアウォールは最大 4000 のゾーンをサポートします。

セキュリティ ゾーン ファイアウォール ポリシー

クラスは、一連のパケットをその内容に基づいて識別します。通常は、識別されたトラフィックでポリシーを反映するアクションを適用できるように、クラスを定義します。クラスは、クラス マップを介して指定されます。

アクションは、通常はトラフィック クラスに関連付けられる機能です。ファイアウォールは、次のタイプのアクションをサポートしています。

inspect：分類されると、ファイアウォールセッションが接続テーブルに作成され、パケットの内容が検査されます。

pass：パケットが分類され、トラフィックは、それ以上の検査なしでシステムを通過できます。

drop：パケットが分類されてドロップされます。

セキュリティ ゾーン ファイアウォール ポリシーを作成するには、次の作業を実行する必要があります。

- 一致基準の定義（クラス マップ）。
- 一致基準とアクションの関連付け（ポリシー マップ）。
- ゾーン ペアへのポリシー マップの付加（サービス ポリシー）。

class-map コマンドは、パケットを指定されたクラスに一致させるためのクラスマップを作成します。ターゲット（入力インターフェイス、出力インターフェイス、またはゾーンペアなど）に到達したパケットは、**service-policy** コマンドの設定方法に従って、クラスマップ用に設定された一致基準に基づいてチェックされ、パケットがそのクラスに属しているかどうかが判断されます。

policy-map コマンドは、1 つ以上のターゲットに付加できるポリシーマップを作成または変更し、サービスポリシーを指定します。**policy-map** コマンドを使用して、作成、追加、または修正するポリシーマップの名前を指定してから、クラスマップで一致基準が定義されているクラスのポリシーを設定します。

セキュリティ ゾーンのメンバーとしての仮想インターフェイス

仮想テンプレートインターフェイスは、特定の目的のため、または特定のユーザに共通のコンフィギュレーションを定義するための汎用的なコンフィギュレーション情報と、デバイスに依存した情報を組み合わせて設定された論理インターフェイスです。このテンプレートには、仮想アクセス インターフェイスに適用される Cisco ソフトウェア インターフェイス コマンドが含まれます。仮想テンプレート インターフェイスを設定するには、**interface virtual-template** コマンドを使用します。

ゾーンメンバー情報が RADIUS サーバーから取得され、ダイナミックに作成されたインターフェイスがそのゾーンのメンバーになります。**zone-member security** コマンドは、ダイナミック インターフェイスを対応するゾーンに追加します。

LNS の加入者単位のファイアウォール機能の詳細については、『Release Notes for Cisco ASR 1000 Series Aggregation Services Routers for Cisco IOS XE Release 2』を参照してください。

ゾーン ペア

ゾーン ペアにより、2 つのセキュリティ ゾーン間で単方向のファイアウォール ポリシーを指定できます。

ゾーンペアを定義するには、**zone-pair security** コマンドを使用します。トラフィックの方向は、送信元ゾーンと宛先ゾーンで指定されます。ゾーンペアの送信元ゾーンと宛先ゾーンはセキュリティ ゾーンである必要があります。

デフォルト ゾーンまたはセルフ ゾーンを送信元ゾーンと宛先ゾーンのどちらかとして選択することができます。セルフゾーンは、メンバーとしてインターフェイスを何も持たないシステム定義のゾーンです。セルフゾーンを含むゾーンペアは、関連付けられたポリシーとともに、デバイス宛てのトラフィックまたはデバイスによって生成されたトラフィックに適用されます。デバイスを通過するトラフィックには適用されません。

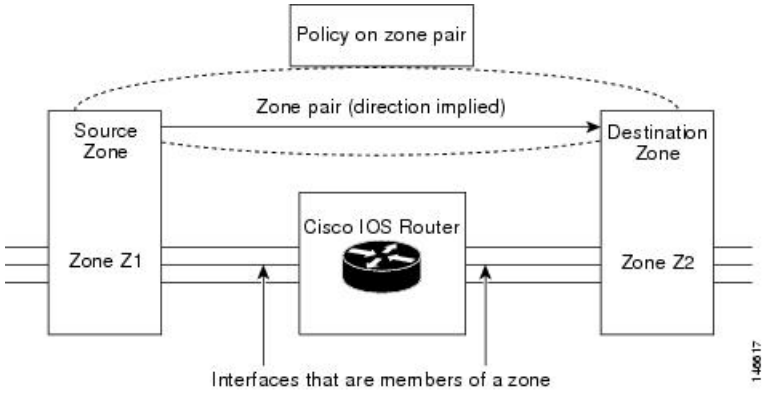
デフォルトゾーンは、セキュリティゾーンが関連付けられていないインターフェイスに適用されます。デフォルトゾーンは、デフォルトでは有効になっていません。デフォルトゾーンを有効にするには、**zone security default** コンフィギュレーション コマンドを使用します。

ファイアウォールの最も一般的な用途は、デバイス経由のトラフィックに適用することです。そのため、少なくとも 2 つのゾーンが必要になります。デバイスとの間のトラフィックの場合、ZBF はセルフゾーンの概念をサポートします。

ゾーン メンバー インターフェイス間のトラフィックを許可するには、そのゾーンと別のゾーンの間のトラフィックを許可（検査または転送）するポリシーを設定する必要があります。ターゲットのゾーンペアにファイアウォールポリシーマップをアタッチするには、**service-policy type inspect** コマンドを使用します。

次の図は、ゾーン Z1 からゾーン Z2 に流れるトラフィックにファイアウォールポリシーを適用する例を示しています。ここでは、トラフィックの入力インターフェイスはゾーン Z1 のメンバー、出力インターフェイスはゾーン Z2 のメンバーです。

図 *52* : ゾーン ペア



2 つのゾーンがあるため、両方向（Z1 から Z2 および Z2 から Z1）のトラフィックにポリシーが必要になる場合があります。トラフィックがいずれかの方向から開始される場合は、2 つのゾーンペアを設定する必要があります。

ゾーン ペア間でポリシーが設定されていない場合は、トラフィックがドロップされます。ただし、リターン トラフィックのためだけにゾーン ペアとサービス ポリシーを設定する必要はありません。デフォルトで、リターン トラフィックは許可されません。サービスポリシーでイニシエータ方向のトラフィックが検査され、リターントラフィック用のゾーンペアとサービスポリシーが存在しない場合は、リターントラフィックが検査されます。

サービス ポリシーで順方向のトラフィックが許可され、リターン トラフィック用のゾーン ペアとサービス ポリシーが存在しない場合は、リターン トラフィックがドロップされます。どちらの場合も、リターン トラフィックを許可するようにゾーン ペアとサービス ポリシーを設定する必要があります。図 2 では、Z2 から Z1 へのリターントラフィックを許可するようにゾーンペアの送信元と宛先を設定する必要はありません。Z1 から Z2 へのゾーンペアに対するサービスポリシーがその役割を果たします。pass アクションの場合は各方向のパケットに対するポリシーが存在する必要があり、inspect アクションの場合はイニシエータからのトラフィックに対するポリシーが存在する必要があります。

レガシー ファイアウォールは、デフォルトでルールまたはポリシーによって明示的に定義されていないパケットを許可するのに対し、ゾーンベース ファイアウォールは、ルールまたはポリシーによって明示的に許可されていないパケットをドロップします。

ゾーンベース ファイアウォールの場合は、内部ゾーンと外部ゾーン間を流れるトラフィックによって、ゾーン内で生成される断続的な Internet Control Message Protocol（ICMP）応答を処理するときの動作が異なります。

Internet Control Message Protocol（ICMP）エラーパケットにはポリシーは必要ありません。

（注） ポリシーは、イニシエータから着信するパケットの ICMP_ECHO（ping）などの ICMP 情報メッセージに対して必要です。

セルフゾーンを送信元とするゾーンペア、および内部ゾーンと外部ゾーン間を流れるトラフィックについて明示的なポリシーが設定されたコンフィギュレーションでは、ICMP_EHCO_REQUEST などの情報 ICMP パケットが生成された場合、ゾーンベース ファイアウォールはセルフゾーンを送信元とするゾーンペアで ICMP の明示的な許可ルールを探します。セルフゾーンを送信元とするゾーンペアに対する ICMP の明示的な検査ルールは、断続的な ICMP 応答に関連するセッションが存在しないという理由で役に立たない場合があります。

ゾーンとインスペクション

ゾーンベース ポリシー ファイアウォールは、ファイアウォール ポリシーに照らして、入力インターフェイスと出力インターフェイスから送信元ゾーンと宛先ゾーンを検査します。インターフェイスを通過するすべてのトラフィックを検査する必要はありません。ゾーンペア全体で適用されるポリシー マップを通して、ゾーン ペアの個々のフローを検査するように指定できます。ポリシー マップには、個々のフローを指定するクラス マップが含まれます。検査アクションを伴うトラフィックは、ファイアウォールテーブル内に接続を構築し、状態チェックの対象になります。通過アクションを伴うトラフィックは、ゾーン ファイアウォールを完全にバイパスして、どのセッションも作成しません。ファイアウォール接続が作成されると、パケットは分類されなくなります。つまり、ポリシーマップが変更されると、基盤となる接続が

認識されなくなります。接続が確立されないため、逆方向のパケットに対するpassアクションを使用して、ミラーリングされたポリシーを作成する必要があります。

TCP しきい値やタイムアウトなどの inspect パラメータをフローあたりで設定することもできます。

ゾーンと ACL

ゾーンのメンバーであるインターフェイスに適用されるアクセス制御リスト（ACL）は、ファイアウォールポリシーがゾーンペアに適用される前に処理されます。送信元ゾーンと宛先ゾーンの間にポリシーが適用されている場合は、そのインターフェイス ACL がポリシー ファイアウォール トラフィックと干渉していないことを確認する必要があります。クラスマップにアクセスリストだけが含まれていて、照合プロトコルが含まれていない場合、ファイアウォールは、フロープロトコルを既知のアプリケーションレベル ゲートウェイ（ALG）と照合し、必要に応じて処理しようとします。

ピンホール（保護されたネットワークへのアプリケーション制御アクセスを許可するファイアウォール経由で開かれるポート）は、インターフェイス ACL 内のリターントラフィックに対して開かれません。

ゾーンベース ポリシー ファイアウォールのクラス マップとポリシー マップ

Quality of Service（QoS）クラス マップには多数の一致基準があります。ファイアウォールの一致基準はそれより少なくなっています。ファイアウォール クラス マップのタイプは inspect であり、この情報により、ファイアウォール クラス マップの下に表示される内容が決まります。

ポリシーとは、トラフィック クラスとアクションの関連付けです。定義されたトラフィック クラスで実行するアクションを指定します。アクションは特定の機能で、通常、トラフィック クラスに関連付けられます。たとえば、inspect、pass、および drop はアクションです。

レイヤ 3 およびレイヤ 4 クラス マップとポリシー マップ

レイヤ3およびレイヤ4クラスマップは、異なるアクションを実行する必要のあるトラフィック ストリームを識別します。

トラフィックの基本的な検査には、レイヤ 3 またはレイヤ 4 ポリシー マップで十分です。

次に、ACL 101 と HTTP プロトコルの一致基準を含むクラスマップ c1 を設定する例を示します。このコマンドにより、パケットが c1 でトラフィックの一部としてドロップされることを指定する、p1 という名前の検査ポリシーマップも作成されます。

```
Device(config)# class-map type inspect match-all c1
Device(config-cmap)# match access-group 101
Device(config-cmap)# match protocol http
Device(config-cmap)# exit
Device(config)# policy-map type inspect p1
Device(config-pmap)# class type inspect c1
```

```
Device(config-pmap-c)# drop
```

（注） Cisco ASR 1000 シリーズ アグリゲーション サービス ルータでは、ファイアウォールが最大 1000 のポリシーマップをサポートし、ポリシーマップあたり 8 のクラスをサポートします。設定できるマッチング ステートメントは、クラス マップごとに最大 16、全体では 1000 です。

クラスマップ設定の制約

トラフィックが複数の一致基準を満たす場合、個別性の高い基準から低い基準の順序で適用する必要があります。たとえば、次のクラス マップの例を考えてみましょう。

```
class-map type inspect match-any my-test-cmap
 match protocol http
 match protocol tcp
```

この例では、HTTP トラフィックが HTTP インスペクションのサービス固有機能によって確実に処理されるように、最初に **match protocol http** コマンドが HTTP トラフィックに適用されます。match 行が逆になっており、**match protocol http** コマンドの前に **match protocol tcp** コマンドがトラフィックに適用されると、そのトラフィックは TCP トラフィックとして分類され、ファイアウォールの TCP インスペクション コンポーネントの機能に従って検査されます。match protocol TCP が最初に設定されると、FTP や TFTP などのサービスの問題や、H.323、Real Time Streaming Protocol（RTSP）、Session Initiation Protocol（SIP）、Skinny Client Control Protocol（SCCP）などのマルチメディアおよび音声シグナリングサービスの問題が発生します。これらのサービスには、より複雑なアクティビティを認識するために追加のインスペクション機能が必要です。

（注） TCP トラフィックフローのウィンドウサイズが 65k を超えないように、デバイスでゾーンベース ファイアウォールを設定します。

class-default クラス マップ

ユーザー定義クラスに加えて、class-default という名前のシステム定義クラスマップは、ポリシーのユーザー定義クラスのどれとも一致しないすべてのパケットを表します。class-default クラスは常に、ポリシー マップの最後のクラスです。

どのユーザ定義クラスにも一致しないパケットのグループに対する明示的なアクションを定義できます。検査ポリシーで class-default クラスに対してアクションを設定しない場合、デフォルトのアクションは drop です。

（注） 検査ポリシーの class-default に対して設定できるアクションは drop と pass だけです。

次の例は、ポリシーマップで class-default クラスを使用する方法を示します。この例では、HTTP トラフィックはドロップされ、残りのトラフィックが検査されます。HTTP トラフィッ

クに対してクラスマップ c1 が定義されており、ポリシーマップ p1 で class-default クラスが使用されています。

```
Device(config)# class-map type inspect match-all c1
Device(config-cmap)# match protocol http
Device(config-cmap)# exit
Device(config)# policy-map type inspect p1
Device(config-pmap)# class type inspect c1
Device(config-pmap-c)# drop
Device(config-pmap-c)# exit
Device(config-pmap)# class class-default
Device(config-pmap-c)# drop
```

レイヤ 3 とレイヤ 4 のサポートされるプロトコル

次のプロトコルがサポートされています。

- FTP
- H.323
- リアルタイム ストリーミング プロトコル（RTSP）
- Skinny Client Control Protocol（SCCP）
- Session Initiation Protocol（SIP）
- Trivial File Transfer Protocol（TFTP）
- ルート収束モニタリングおよび診断（RCMD）
- Lightweight Directory Access Protocol（LDAP）
- HTTP
- ドメイン ネーム システム（DNS）
- Simple Mail Transfer Protocol（SMTP/ESMTP）
- Post Office Protocol 3（POP3）
- Internet Mail Access Protocol（IMAP）
- SUN リモートプロシージャコール（SUNRPC）
- GPRS トンネル プロトコル バージョン 0/1（GTPv1）
- GPRS トンネル プロトコル バージョン 2（GTPv2）
- ポイントツーポイント トンネリング プロトコル（PPTP）

アクセス コントロール リストとクラス マップ

アクセス リストは、パケット分類メカニズムです。アクセスリストでは、ACL が特定のクラスマップに適用されたときに許可または拒否される実際のネットワークトラフィックを定義します。つまり、ACLは、パケットに適用される許可および拒否条件を順番に集めたものです。

ルータは、一度に 1 つずつ ACL の条件に基づいてパケットをテストします。拒否条件は「一致しない」と解釈されます。拒否アクセス制御エントリ（ACE）と一致するパケットの場合、ACL 処理が終了し、クラス内の次の match ステートメントが調べられます。

（注） ACL の変数の範囲をクラスマップの一致基準として設定できます。ファイアウォールでは 5 タプル一致基準だけがサポートされているため、サポートされている一致基準は送信元アドレス、送信元ポート、宛先アドレス、宛先ポート、およびプロトコルだけです。CLI で設定および受け入れられるその他のすべての一致基準は、ファイアウォールではサポートされていません。

クラスマップは、次の基準に基づいて、ACL の一連の変数を照合するために使用されます。

- クラス マップが許可条件または拒否条件に一致しない場合、ACL は失敗します。
- match-all または match-any 条件は、クラスマップ内に含まれる match ステートメントに適用されます。ACL は通常どおりに処理され、その結果が、match-all または match-any と比較するときに使用されます。
- match-all 属性が指定され、どの一致条件、ACL、またはプロトコルもパケットと一致しない場合、現在のクラスの評価はその時点で停止され、ポリシーの次のクラスが調べられます。
- match-any 属性でいずれかの match が成功した場合、class-map 基準が満たされ、ポリシーで定義されたアクションが実行されます。
- ACL が match-any 属性と一致した場合、ファイアウォールは宛先ポートに基づいてレイヤ 7 プロトコルの確認を試みます。

クラスマップで match-all 属性を指定した場合、レイヤ 4 の一致基準（ICMP、TCP、UDP）は設定されますが、レイヤ 7 の一致基準は設定されません。したがって、レイヤ 4 インスペクションが実行され、レイヤ 7 インスペクションは省略されます。

アクセスリストには、「標準アクセスリスト」と「拡張アクセスリスト」という異なる形式があります。標準アクセス リストでは、IP アドレスまたは IP アドレスの範囲を許可または拒否するように定義します。拡張アクセス リストでは、送信元と宛先両方の IP アドレスまたは IP アドレス範囲を定義します。拡張アクセス リストは、パケットの ICMP、TCP、および UDP プロトコルタイプと宛先ポート番号に基づいて、パケットの許可または拒否を定義することもできます。

次に、IP アドレス 10.2.3.4 から受信したパケットを、クラス test1 と照合する例を示します。この例では、アクセス リスト 102 が拒否条件と一致し、アクセス リストの他のエントリの処理を停止します。クラスマップは match all 属性で指定されているため、クラスマップ test1 の照合は失敗します。ただし、このクラスマップがクラスマップ test1 にリストされているプロトコルのいずれかと一致するかどうかが検査されます。

クラスマップ test1 が match-all ではなく match-any 属性を使用していた場合は、ACL は拒否と一致して失敗しますが、HTTP プロトコルと一致し、pmap1 を使用した検査が実行されます。

```
access-list 102 deny ip 10.2.3.4 0.0.0.0 any
access-list 102 permit any any
class-map type inspect match-all test1
 match access-list 102
 match protocol http
!
class-map type inspect match-any test2
 match protocol sip
 match protocol ftp
 match protocol http
!
parameter-map type inspect pmap1
 tcp idle-time 15
!
parameter-map type inspect pmap2
 udp idle-time 3600
!
policy-map type inspect test
 class type inspect test1
  inspect pmap1
!
 class type inspect test2
  inspect pmap2
!
 class type inspect class-default
  drop log
```

階層型ポリシー マップ

ポリシーを別のポリシー内にネストできます。ネストされたポリシーを含むポリシーのことを「階層ポリシー」と呼びます。

階層ポリシーを作成するには、ポリシーをトラフィックのクラスに直接付加します。階層ポリシーには、1 つの子ポリシーと 1 つの親ポリシーが含まれています。子ポリシーは、以前定義したポリシーであり、**service-policy** コマンドを使用して新しいポリシーに関連付けられています。既存のポリシーを使用する新しいポリシーが親ポリシーです。

（注） 階層検査サービスポリシーに作成できる階層レベルは 2 レベルまでです。

たとえば、マーケティングとエンジニアリングの2つのアクセスリストを定義します。2 つのアクセスグループのいずれかと一致するクラスマップを作成します。その後、match-all 条件を持つ前のクラスマップを含み、プロトコル HTTP と一致する、別のクラスマップを作成します。

パラメータ マップ

パラメータマップを使用すると、ポリシーマップで指定したアクションとクラスマップで指定した一致基準の動作を制御するパラメータを指定できます。

パラメータ マップには次の 2 種類があります。

- 検査パラメータマップ：検査パラメータマップは任意です。パラメータ マップを使用しない場合、デフォルトのパラメータが使用されます。inspectアクションに関連付けられたパラメータは、すべてのマップに適用されます。上位レベルと下位レベルの両方でパラメータが指定されている場合、下位レベルのパラメータが優先されます。
- プロトコル固有パラメータマップ：インスタントメッセンジャ（IM）アプリケーション（レイヤ 7）のポリシーマップに必要なパラメータマップです。

ファイアウォールとネットワーク アドレス変換

ネットワークアドレス変換（NAT）は、登録されていないIPアドレスを使用してインターネットへ接続するプライベート IP インターネットワークをイネーブルにします。NAT はデバイス（通常、2 つのネットワークを接続するもの）で動作し、パケットを別のネットワークに転送する前に、社内ネットワークの（グローバルに一意のアドレスではなく）プライベートアドレスを正規のアドレスに変換します。NAT は、ネットワーク全体の 1 つだけのアドレスを外部にアドバタイズするように設定できます。NAT が設定されたデバイスには、内部ネットワークと外部ネットワークのそれぞれに接続するインターフェイスが少なくとも 1 つずつあります。

標準的な環境では、NAT はスタブ ドメインとバックボーンの間の出口デバイスに設定されます。パケットがドメインから出て行くとき、NAT はローカルで意味のある送信元アドレスをグローバルで一意のアドレスに変換します。パケットがドメインに入ってくる際は、NAT はグローバルで一意の宛先アドレスをローカルアドレスに変換します。出力点が複数存在する場合、個々の NAT は同一の変換テーブルを持っていなければなりません。アドレスが足りなくなって、パケットにアドレスを割り当てられなくなった場合、ソフトウェアはそのパケットをドロップし、ICMP ホスト到達不能パケットを送信します。

NAT については、「内部」という用語は組織により所有され、変換を必要とするネットワークを意味します。このドメイン内では、ホストのアドレスは 1 つのアドレス空間に含まれます。NAT が設定されている場合、ホストが外部にあると、そのホストには別のアドレス空間にアドレスがあるように見えます。内部アドレス空間はローカルアドレス空間として参照され、外部アドレス空間はグローバルアドレス空間として参照されます。

NAT が送信元と宛先の両方の IP アドレスを変換するシナリオについて考えてみます。パケットは、送信元アドレス 209.168.1.1 および宛先アドレス 10.1.1.1 を使用して内部 NAT からデバイスに送信されます。NAT はこれらのアドレスを変換し、送信元アドレス 209.165.200.225 および宛先アドレス 209.165.200.224 を使用して外部ネットワークにパケットを送信します。

同様に、外部 NAT から応答が返されると、送信元アドレスは 209.165.200.225 になり、宛先アドレスは 209.165.200.224 になります。したがって NAT 内部では、パケットの送信元アドレスは 10.1.1.1、宛先アドレスは 209.168.1.1 となります。

このシナリオでは、ファイアウォールポリシーで使用されるアプリケーション コントロール エンジン（ACE）を作成する場合は、NAT 前の IP アドレス（内部ローカルアドレスおよび外部グローバルアドレス）209.168.1.1 と 209.165.200.224 を使用する必要があります。一般に、外部グローバルアドレスのマッピングは推奨されません。

Cisco ファイアウォールに対する WAAS サポート

リリースによっては、Wide Area Application Services（WAAS）ファイアウォール ソフトウェアが、セキュリティ対応 WAN およびアプリケーション アクセラレーション ソリューションを最適化する統合型ファイアウォールに次のようなメリットを提供します。

- WAAS ネットワークを透過的に統合します。
- 透過的な WAN 加速化トラフィックを保護します。
- フル ステートフル インスペクション機能を通して WAN を最適化します。
- Payment Card Industry（PCI）コンプライアンスを簡略化します。
- Network Management Equipment-Wide Area Application Engine（NME-WAE）モジュールまたはスタンドアロン WAAS デバイス展開をサポートします。

WAAS は、初期の 3 方向ハンドシェイク中に TCP オプションを使用して WAE デバイスを透過的に識別する自動検出メカニズムを備えています。自動検出後、最適化されたトラフィック フロー（パス）ではTCP シーケンス番号が変化し、エンドポイントは最適化されたトラフィック フローと最適化されてないトラフィック フローを区別できます。

（注） パスは接続と同じ意味で使用されています。

WAAS は、Cisco ファイアウォールで、内部ファイアウォール TCP 状態変数を含む TCP トラフィック フローのステートフルなレイヤ4インスペクションを損なうことなく、シーケンス番号を変更することによって、最適化されたトラフィックを自動的に検出できるようにします。これらの変数は、WAE デバイスの存在に応じて調整されます。

Cisco ファイアウォールは、トラフィック フローが正常に WAAS 自動検出を完了したことを認識すると、トラフィック フロー用の初期シーケンス番号のシフトを許可し、最適化されたトラフィック フローのレイヤ 4 状態を維持します。

（注） クライアント側のステートフルなレイヤ7インスペクションは、最適化されていないトラフィックに対しても実行できます。

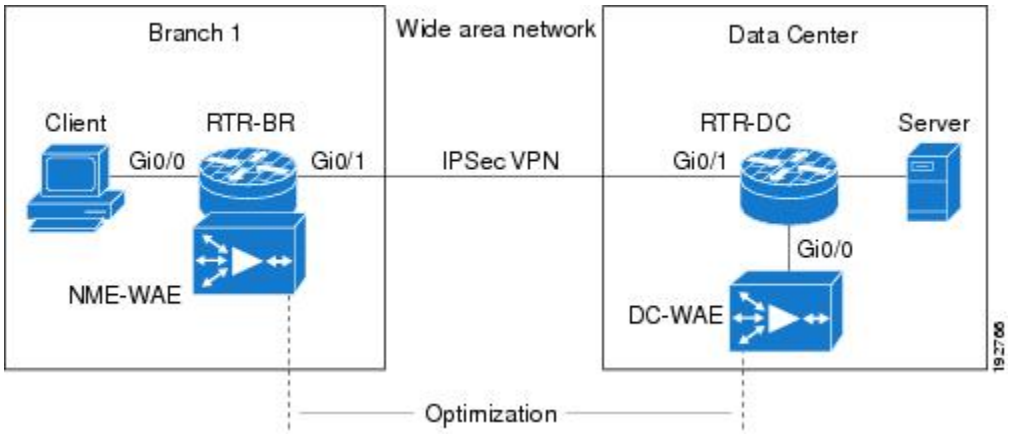
WAAS トラフィック フロー最適化展開シナリオ

ここでは、ブランチ オフィス展開に関する 2 種類の WAAS トラフィック フロー最適化シナリオについて説明します。WAAS トラフィック フロー最適化は、Cisco サービス統合型ルータ（ISR）上の Cisco ファイアウォール機能と連動します。ZBF は、WAAS がパケットの最適化を解除した後に、クリアテキストを検査します。

次の図に、Cisco ファイアウォールを使用したエンドツーエンドの WAAS トラフィックフロー最適化の例を示します。この特定の展開では、NME-WAE が Cisco ファイアウォールと同じデ

バイスに展開されます。Web Cache Communication Protocol（WCCP）が代行受信用にトラフィックをリダイレクトするために使用されます。

図 *53 : エンドツーエンドの WAAS* 最適化パス

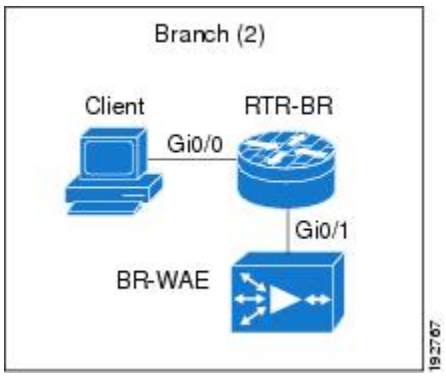


オフパス デバイスを使用した WAAS ブランチ展開

このセクションにある Wide Area Application Services（WAAS）ブランチ展開の図のように、WAE デバイスは、スタンドアロン WAE デバイスにすることも、ISR に統合型サービスエンジンとしてインストールされた NME-WAE デバイスにすることもできます。

次の図は、トラフィックの代行受信のために、WCCP を使用してトラフィックを Off-Path スタンドアロン WAE デバイスにリダイレクトする WAAS 支店の展開例です。このオプションの設定は、NME-WAE を使用した WAAS 支店の展開と同じです。

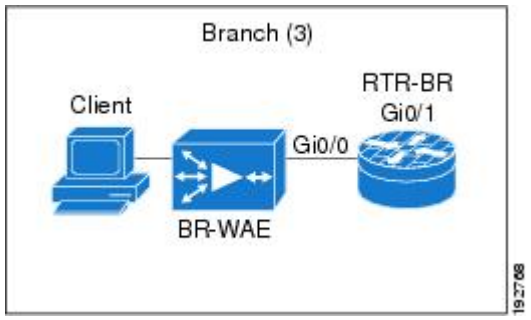
図 *54 : WAAS* オフパス ブランチ展開



インライン デバイスを使用した WAAS ブランチ展開

次の図に、インライン WAE デバイスがサービス統合型ルータ（ISR）の前に配置された WAAS ブランチ展開を示します。WAE デバイスがデバイスの前に配置されているため、Cisco ファイアウォールが WAAS 最適化パケットを受信し、結果的に、クライアント側のレイヤ 7 インスペクションがサポートされません。

図 *55 : WAAS* インライン パス ブランチ展開



Cisco ファイアウォールを使用したエッジ WAAS デバイスを、WAN 接続との間で転送されるトラフィックを検査する必要があるブランチ オフィス サイトで使用します。Cisco ファイアウォールは、トラフィックで最適化インジケータ（TCP オプションと後続の TCP シーケンス番号の変更）をモニターして、最適化されたトラフィックが通過できるようにします。一方、すべてのトラフィックにレイヤ 4 のステートフル インスペクションとディープ パケット インスペクションを適用し、セキュリティを確保することで、WAAS最適化のメリットを享受します。

（注） WAE デバイスがインラインロケーションにある場合、デバイスは自動検出プロセス後にバイパスモードになります。デバイスは、WAAS最適化に直接関与しませんが、最適化インジケータが存在する場合は、Cisco ファイアウォール インスペクションをネットワークトラフィックに適用し最適化アクティビティを考慮に入れるために、WAAS最適化がトラフィックに適用されていることを認識している必要があります。

ゾーンベースファイアウォールでのOut-of-Orderパケット処理のサポート

デフォルトでは、レイヤ 7 ディープ パケット インスペクションが有効にされている場合、またはレイヤ 7 プロトコルマッチングでレイヤ 4 インスペクションが有効にされている場合、Cisco IOS XE ファイアウォールはすべての Out-of-Order（OoO）パケットをドロップします。Out-of-Order パケットのドロップは（送信者の代わりとなる）再送信タイマーが満了するまで行われないため、Out-of-Order パケットがドロップされると終端アプリケーションで大幅な遅延が発生する可能性があります。レイヤ 7 インスペクションはステートフル パケット インスペクションであり、TCP パケットの順序が正しくなければ機能しません。

Cisco IOS XE リリース 3.5S では、セッションに DPI が必要ない場合、OoO パケットは許可されて、ルータをパス スルーして宛先に到達できます。OoO パケットが含まれるすべてのレイヤ4トラフィックに、宛先へのパス スルーが許可されます。一方、セッションにレイヤ7インスペクションが必要な場合は、やはり OoO パケットはドロップされます。DPI が必要ない場合は OoO パケットをドロップしないようにすることで、ドロップされたパケットを再送信する必要がなくなるため、再送信に必要なネットワーク上の帯域幅が削減されます。

デバッグ メッセージのシビラティ（重大度）

デバッグ メッセージのシビラティ（重大度）により、メッセージが記録される問題のタイプが指定されます。ファイアウォールのデバッグを有効にする場合は、ログに記録するメッセージのレベルを指定できます。次の表に、デバッグ メッセージのシビラティ（重大度）の詳細を示します。

表 *165 :* ファイアウォール デバッグ メッセージのシビラティ（重大度）

トレース レベル	シビラティ（重大度）	説明
深刻	1	ゾーンベース ポリシー ファイアウォールが使用できない原因、またはパケットを転送できない原因である問題に適用されます。これはデフォルトです。Critical イベントの例を次に示します。 • ログ メカニズムによりトリガーされたバック プレッシャ。 • リソース制限の超過。 • メモリ割り当ての失敗。 • 新しいセッションを実行できないハイアベイラビリティ状態。
Error	2	すべてのエラー条件とパケット ドロップ条件に適用されます。Error イベントの例を次に示します。 • 同期（SYN）Cookie：最大宛先数に達した。 • イニシエータ パケットではない。 • パケットを送信できなかった。 • アプリケーション レイヤ ゲートウェイ（ALG）のエラー状態。

トレース レベル	シビラティ（重大度）	説明
Information	3	情報メッセージに適用されます。Information イベントの例を次に示します。 • 誤ったポリシー設定、ゾーンチェック失敗、不正なパケット、またはハードコーディングされている制限またはしきい値が原因で発生したパケットドロップ。 • ステート マシン遷移。 • セッションまたは不明確チャネルデータベース情報、検索結果など。 • パケット分類のステータスまたは結果。 • パケット パスまたはパケット ドロップのステータス。 • セッション ヒットまたはセッション ミス。 • 送信されたパケットが TCP リセット（RST）パケットである。 • SYN Cookie イベント。
Detail	4	すべてのログ メッセージを出力します。Detail イベントの例を次に示します。 • データ構造。 • TCAM（Ternary Content Addressable Memory）検索キーと結果構造。 • ファイアウォール イベントの詳細。

ゾーンベース ポリシー ファイアウォールのスマート ライセンスのサポート

Cisco ASR 1000 シリーズ アグリゲーション サービス ルータのゾーンベース ポリシー ファイアウォール機能は、セキュリティパッケージとは別にパッケージ化されているので、ゾーンベースポリシーファイアウォールでは機能を有効または無効にするためのライセンスが必要です。ASR1000 のゾーンベース ファイアウォールのスマートライセンスサポート機能は、Cisco UniversalK9 IOS ソフトウェアイメージにより、Cisco ASR 1000 シリーズアグリゲーション サービス ルータのスマートライセンスを機能レベルで実現します。

この機能を有効にするためにデバイスをリロードする必要はありません。スマート ライセンスは、デフォルトではオンになっていません。スマートラインセンスは、**license smart enable** コマンド、または **zone security** コマンドを使用したゾーンベース ポリシー ファイアウォールの

設定により、グローバルにオンとオフが切り替えられます。スマートライセンスの実装時に **show license all** コマンドを実行すると、スマートライセンスのステータスが表示されます。スマートライセンスがグローバルに有効である場合の **show license all** コマンドの出力例を次に示します。

```
Device# show license all

License Store: Primary License Storage
StoreIndex: 0   Feature: internal_service                 Version: 1.0
        License Type: Evaluation
        License State: Active, In Use
            Evaluation total period: 1  day  0  hour
            Evaluation period left: 18 hours 57 minutes
            Period used: 5  hours 2  minutes
            Expiry date: Mar 18 2016 14:15:02
        License Count: Non-Counted
        License Priority: Low
License Store: Built-In License Storage
StoreIndex: 0   Feature: adventerprise                    Version: 1.0
        License Type: EvalRightToUse
        License State: Active, In Use
            Evaluation total period: 8  weeks 4  days
            Evaluation period left: 8  weeks 3  days
            Period used: 5  hours 13 minutes
            Transition date: May 16 2016 14:03:52
        License Count: Non-Counted
        License Priority: Low          <-- (CSL mode license)

Device(config)# license smart enable
Device(config)# zone security z1
Device(config)# exit
Device# show license all

Smart Licensing Status
----------------------------
Smart Licensing is ENABLED

Registration:
  Status: UNREGISTERED
  Export-Controlled Functionality: Not Allowed

License Authorization:
  Status: EVAL MODE
  Evaluation Period Remaining: 65 days, 14 hours, 19 minutes, 47 seconds

License Usage
--------------

(ASR_1000_AdvEnterprise):
  Description:
  Count: 1
  Version: 1.0
  Status: EVAL MODE

(ASR_1000_firewall):
  Description:
  Count: 1
  Version: 1.0
  Status: EVAL MODE

Product Information
----------------------
UDI: PID:ASR1013,SN:NWG165000A9
```

```
Agent Version
---------------
Smart Agent for Licensing: 1.5.1_rel/29
Component Versions: SA:(1_3_dev)1.0.15, SI:(dev22)1.2.1, CH:(rel5)1.0.3, PK:(dev18)1.0.3
```

次に、スマートライセンスが無効な場合の出力例を示します。

```
Device(config)# no zone security z1
Device(config)# exit
Device# show license all

Smart Licensing Status
----------------------

Smart Licensing is ENABLED

Registration:
  Status: UNREGISTERED
  Export-Controlled Functionality: Not Allowed

License Authorization:
  Status: EVAL MODE
  Evaluation Period Remaining: 65 days, 14 hours, 18 minutes, 58 seconds

License Usage
--------------

(ASR_1000_AdvEnterprise):
  Description:
  Count: 1
  Version: 1.0
  Status: EVAL MODE

Product Information
--------------------
UDI: PID:ASR1013,SN:NWG165000A9

Agent Version
-------------
Smart Agent for Licensing: 1.5.1_rel/29
Component Versions: SA:(1_3_dev)1.0.15, SI:(dev22)1.2.1, CH:(rel5)1.0.3, PK:(dev18)1.0.3

Device(config)# no license smart enable
Device(config)# exit
Device# show license all

License Store: Primary License Storage
StoreIndex: 0   Feature: internal_service                 Version: 1.0
        License Type: Evaluation
        License State: Active, Not in Use, EULA accepted
            Evaluation total period: 1  day  0  hour
            Evaluation period left: 18 hours 54 minutes
            Period used: 5  hours 5  minutes
        License Count: Non-Counted
        License Priority: Low
License Store: Built-In License Storage
StoreIndex: 0   Feature: adventerprise                    Version: 1.0
        License Type: EvalRightToUse
        License State: Active, Not in Use, EULA accepted
            Evaluation total period: 8  weeks 4  days
            Evaluation period left: 8  weeks 3  days
            Period used: 5  hours 17 minutes
```

```
License Count: Non-Counted
License Priority: Low                <--- (back to CSL mode)
```

ゾーンベース ファイアウォールの再分類

Cisco IOS XE 17.6.1 以降では、ZBFW セッションの再分類を設定できます。ZBFW 再分類機能により、ポリシー設定の変更が既存のファイアウォールセッションに適用されます。確立されたセッションでセッションイニシエータからパケットを受信すると、特定のフローが再分類されます。

次に、これが発生する可能性のあるいくつかの例を示します。

- クラスマップでフィルタを追加、削除、または編集するには、次の作業を実行します。
  - 一致プロトコルの削除。
  - アクセスグループの削除。
  - アクセスグループでのアクセス制御エントリ（ACE）の編集。
  - オブジェクトグループの編集。
- Application Visibility and Control（AVC）ポリシーの追加、削除、または編集。

ポリシーへの変更に応じて、次のいずれかのアクションが発生する可能性があります。

- 検査してドロップ：既存のセッションが破棄され、セッションがセッションテーブルから削除されます。
- 検査して転送：ゾーンベース ファイアウォールがフローを検査しないため、既存のセッションが破棄されます。ただし、このシナリオでは、トラフィックフローは続きます。
- 検査して検査：既存のセッションが新しいクラスマップの下に移動されます。
- 転送して検査/ドロップして検査：既存の動作が続行され、フローの途中での再分類がサポートされていないためにフローがブロックされます。

（注） ポリシーの変更がある場合、フローの途中でデータを確立することはできません。

ゾーンベース ポリシー ファイアウォールの前提条件

ゾーンを作成する前に、セキュリティの観点から見ると同様のインターフェイスをグループ化する必要があります。

ゾーンベース ポリシー ファイアウォールの制約事項

- Cisco Wide Area Application Services（WAAS）と Cisco IOS XE ファイアウォール設定では、WAE デバイスによって処理されるすべてのパケットは、両方向とも Cisco IOS XE ファイアウォールを通過して、WCCP 総称ルーティングカプセル化（GRE）リダイレクトをサポートする必要があります。この状況は、レイヤ2リダイレクトが使用できない場合に発生します。レイヤ 2 リダイレクトが WAE で設定されている場合、システムはデフォルトで、GRE リダイレクトを続行させます。
- WCCPがレイヤ2リダイレクト方式で設定されている場合、ゾーンベースファイアウォールは、WAAS および WCCP と相互運用できません。
- ゾーンベース ファイアウォール設定は、Cisco Unity Express Virtual（vCUE）コールフローを含むブリッジ ドメイン インターフェイス（BDI）には適用できません。
- セルフゾーンは、デフォルトの「deny all」ポリシーの唯一の例外です。ルータインターフェイスへのすべてのトラフィックは、トラフィックが明示的に拒否されるまで許可されます。
- WAAS および Cisco IOS XE ファイアウォール構成では、WCCP は、ポリシーベース ルーティング（PBR）を使用したトラフィックのリダイレクトをサポートしていません。
- Cisco ISR-WAAS I/O モジュールを使用して構成された ASR で、汎用 GRE を使用したゾーンベース ポリシー ファイアウォールが有効になっている場合、WCCP トラフィック リダイレクションは機能しません。この構成は、WAN の最適化ソリューションです。WCCP トラフィック リダイレクションを機能させるには、インターフェイスからゾーンベース ポリシーファイアウォール設定を削除します。WAEデバイスを使用している場合、WCCP トラフィック リダイレクションは正しく動作します。

  WAAS の場合、汎用 GRE は最適化が完了すると、WAAS WAE からのパケットを GRE トンネル経由で最初にリダイレクトされたデバイスと同じデバイスに返すのに役立つ、アウトオブパス導入のメカニズムです。
- マルチキャスト トラフィックのステートフル インスペクション サポートは、セルフ ゾーンを含め、すべてのゾーン間でサポートされません。コントロールプレーンをマルチキャスト トラフィックから保護するには、コントロール プレーン ポリシングを使用します。
- 内部から外部へのゾーンベースポリシーがWindowsシステムのICMPに一致するように設定されている場合、**traceroute** コマンドは機能します。ただし Apple システムでは、UDP ベースの traceroute を使用するため、同じ設定は機能しません。この問題を解決するには、**icmp time-exceeded** コマンドおよび **icmp host unreachable** コマンドを **pass** コマンド（**inspect** コマンドではない）とともに使用して、外部から内部へのゾーンベースポリシーを設定します。この制限は Cisco IOS XE リリース 3.1S 以前のリリースに適用されます。
- クラスマップでは ACL がサポートされます。ただし、ACL ベースのパケットカウントはデフォルトで無効になっています。Perfilter の統計情報は Cisco IOS XE リリース 3.13S 以降のゾーンベース ファイアウォールで使用できます。

- オブジェクトグループを使用する ACL ステートメントは、処理のためにランデブーポイント（RP）に送信されるパケットでは無視されます。
- ブリッジドメイン インターフェイスは、すべてのレイヤ4およびレイヤ7インスペクションを含む、ゾーンベース ファイアウォール インスペクションをサポートしていません。
- デバイスで NAT NVI が有効になっている場合、ZBF はトラフィックを検査できません。
- トラフィックがゾーンペアに入ると、ファイアウォールは接続テーブル全体を調べ、入力インターフェイスがゾーンペアに一致しなくても、表内のすべての接続とトラフィックを照合します。このシナリオでは、検査アクションが設定されている場合、ファイアウォール上の非対称にルーティングされたトラフィックがパケットをドロップする可能性があります。

  Cisco IOS XE リリース 3.15S 以降のリリースでは、zone-mismatch drop はクラスパラメータマップで設定されます。zone-mismatch drop が設定されている場合、ゾーンは、パケットの分類時に使用された元のゾーンに対してチェックされます。ゾーンがゾーンペアの一方ではない場合、パケットはドロップされます。zone-mismatch drop が設定されていない場合、ゾーンはチェックされません。
- ZBF が設定されている場合、ゾーンペアの一部であるすべてのインターフェイスに RII が設定されている必要があります。ピアデバイスと一致するインターフェイスには、同じ RII が設定されている必要があります。さらに、2 つのインターフェイス間で開始されたフローは、一方のインターフェイスだけでも RII が割り当てられていない場合、スタンバイに同期されません。
- ゾーンベース ファイアウォールは、デフォルトゾーンのダイナミック インターフェイスでのみサポートされます。これらのインターフェイスは、トラフィックが IPsec または VPN セキュアトンネルにトンネリングされると、動的に作成または削除されます。仮想テンプレートは、特定のタイプのダイナミックインターフェイスをサポートするために使用されます。詳細については、セキュリティ ゾーンのメンバーとしての仮想インターフェイス （1604 ページ）を参照してください。
- インターフェイスに適用されているゾーンベース ファイアウォールの設定を無効にするには、**platform inspect disable-all** コマンドを使用します。同様に、インターフェイスでゾーンベース ファイアウォールを有効にするには、**no platform inspect disable-all** コマンドを使用します。

  platform inspect disable-all コマンドが適用されているかどうかを確認するには、次の **show running** 設定を使用します。

```
show run | sec disable
platform inspect disable-all
```

（注） デフォルトでは、ゾーンベース ファイアウォールは常に有効になっています。

- ユーザー定義クラスまたはポリシーのデフォルトクラスで **droplog** コマンドが設定されていると、**drop** コマンドを設定してドロップされたパケットのロギングを無効にしても、ログメッセージは停止されません。これは既知の問題であり、回避策は、**nodroplog** コマンドを設定した後で、**drop** コマンドを設定し、メッセージのロギングを停止することです。この問題は **pass** コマンドにも適用されます。次の例は問題を示しています。

```
! Logging of dropped packets is enabled by configuring the drop log command.
policy-map type inspect INT-EXT
 class type inspect INT-EXT
  pass
 class class-default
  drop log
!
```

次の例は回避策を示しています。

```
! In this example, the no drop log command is configured before the drop command.
policy-map type inspect INT-EXT
 class type inspect INT-EXT
  pass
 class class-default
  drop log
  no drop log
  drop
!
```

- ZBFWセッション再分類機能を使用する場合、ステートフルトラフィックのフロー途中の検査はサポートされません。たとえば、ポリシー設定の変更により、既存のフローのアクションが、ドロップから検査に変更される可能性があります。この場合、ZBFWは、既存のフローを検査しません。
- ハイアベイラビリティは、ゾーンベース ファイアウォール ポリシー再分類ではサポートされません。

ゾーンベース ポリシー ファイアウォールの設定方法

以下のセクションでは、ゾーンベース ポリシー ファイアウォールの設定を指定するさまざまな作業について説明します。

レイヤ 3 およびレイヤ 4 ファイアウォール ポリシーの設定

レイヤ 3 およびレイヤ 4 のポリシーは、ターゲット（ゾーンペア）に付加される「最上位」のポリシーです。レイヤ 3 およびレイヤ 4 のファイアウォールポリシーを設定するには、次の作業を実行します。

レイヤ 3 およびレイヤ 4 のファイアウォール ポリシーのクラス マップの設定

ネットワーク トラフィックを分類するためのクラス マップを設定するには、次の作業を行います。

（注） ステップ 4、5、6 のうち、少なくとも 1 つのマッチング手順を実行する必要があります。

パケットがアクセス グループ、プロトコル、クラスマップのいずれかにマッチングされると、それらのパケットのトラフィック レートが生成されます。ゾーンベース ファイアウォール ポリシーでは、ポリシーと一致するのは、セッションを作成した最初のパケットのみです。このフローの後続パケットは、設定されたポリシー内のフィルタと一致しませんが、セッションとは直接一致します。後続パケットに関連する統計情報は、検査アクションの一部として表示されます。

手順の概要

1. **enable**
2. **configure terminal**
3. **class-map type inspect** [**match-any** | **match-all**] *class-map-name*
4. **match access-group** {*access-group* | **name** *access-group-name*}
5. **match protocol** *protocol-name* [**signature**]
6. **match class-map** *class-map-name*
7. **end**
8. **show policy-map type inspect zone-pair session**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。プロンプトが表示されたらパスワードを入力します。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**class-map type inspect** [**match-any**	**match-all**] *class-map-name* 例： `Device(config)# class-map type inspect match-all c1`	レイヤ 3 またはレイヤ 4 の検査タイプ クラス マップを作成し、クラスマップ コンフィギュレーション モードを開始します。
ステップ 4	**match access-group** {*access-group*	**name** *access-group-name*} 例： `Device(config-cmap)# match access-group 101`	ACL 名または番号に基づくクラスマップの一致基準を設定します。
ステップ 5	**match protocol** *protocol-name* [**signature**] 例：	指定したプロトコルに基づいてクラスマップの一致基準を設定します。

	コマンドまたはアクション	目的
	`Device(config-cmap)# match protocol http`	• 検査タイプ クラスマップの一致基準には、Cisco ステートフル パケット インスペクションでサポートされているプロトコルのみを使用できます。
ステップ 6	**match class-map** *class-map-name* 例： `Device(config-cmap)# match class-map c1`	すでに定義したクラスをクラスマップの一致基準として指定します。
ステップ 7	**end** 例： `Device(config-cmap)# end`	クラスマップ コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。
ステップ 8	**show policy-map type inspect zone-pair session** 例： `Device(config-cmap)# show policy-map type inspect zone-pair session`	（オプション）指定されたゾーン ペアにポリシーマップが適用されたために作成された、Cisco ステートフル パケット インスペクション セッションを表示します。 （注） **Class-map** フィールドの下に表示される情報は、接続開始トラフィックのみに属するトラフィックのトラフィックレート（ビット/秒）です。接続セットアップ レートが非常に高く、レートが計算される複数のインターバルにわたって高い接続セットアップ レートが持続する場合を除き、接続に関する意味のあるデータは表示されません。

レイヤ 3 およびレイヤ 4 ファイアウォール ポリシーのポリシー マップの作成

後でゾーンペアに付加するレイヤ 3 およびレイヤ 4 ファイアウォールポリシーのポリシーマップを作成するには、次の手順を実行します。

検査タイプのポリシーマップを作成する場合、許容されるアクションは drop、inspect、pass、および service-policy のみである点に注意してください。

（注） ステップ 5、8、9、10 のうち、少なくとも 1 つの手順を実行する必要があります。

手順の概要

1. **enable**
2. **configure terminal**
3. **policy-map type inspect** *policy-map-name*

4. **class type inspect** *class-name*
5. **inspect** [*parameter-map-name*]
6. **drop** [**log**]
7. **pass**
8. **service-policy type inspect** *policy-map-name*
9. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。プロンプトが表示されたらパスワードを入力します。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**policy-map type inspect** *policy-map-name* 例： `Device(config)# policy-map type inspect p1`	レイヤ 3 とレイヤ 4 の検査タイプ ポリシー マップを作成し、ポリシーマップ コンフィギュレーション モードを開始します。
ステップ 4	**class type inspect** *class-name* 例： `Device(config-pmap)# class type inspect c1`	アクションを実行する対象のトラフィッククラスを指定し、ポリシーマップ クラス コンフィギュレーション モードを開始します。
ステップ 5	**inspect** [*parameter-map-name*] 例： `Device(config-pmap-c)# inspect inspect-params`	Cisco ステートフル パケット インスペクションをイネーブルにします。
ステップ 6	**drop** [**log**] 例： `Device(config-pmap-c)# drop`	（任意）定義されたクラスと一致するパケットをドロップします。 （注） **drop** アクションと **pass** アクションは排他的であり、**inspect** アクションと **drop** アクションは相互に排他的です。つまり、両方を同時に指定することはできません。どちらか 1 つだけを指定できます。
ステップ 7	**pass** 例： `Device(config-pmap-c)# pass`	（任意）定義されたクラスと一致するパケットを許可します。

	コマンドまたはアクション	目的
ステップ 8	**service-policy type inspect** *policy-map-name* 例： `Device(config-pmap-c)# service-policy type inspect p1`	ファイアウォール ポリシー マップをゾーン ペアに付加します。
ステップ 9	**end** 例： `Device(config-pmap-c)# end`	ポリシー マップ クラス コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

検査パラメータ マップの作成

手順の概要

1. **enable**
2. **configure terminal**
3. **parameter-map type inspect** {*parameter-map-name* | **global** | **default**}
4. **log** {**dropped-packets** {**disable** | **enable**} | **summary** [**flows** *number*] [**time-interval** *seconds*]}
5. **alert** {**on** | **off**}
6. **audit-trail** {**on** | **off**}
7. **dns-timeout** *seconds*
8. **icmp idle-timeout** *seconds*
9. **max-incomplete** {**low** | **high**} *number-of-connections*
10. **one-minute** {**low** | **high**} *number-of-connections*
11. **sessions maximum** *sessions*
12. **tcp finwait-time** *seconds*
13. **tcp idle-time** *seconds*
14. **tcp max-incomplete host** *threshold* [**block-time** *minutes*]
15. **tcp synwait-time** *seconds*
16. **tcp window-scale-enforcement loose**
17. **udp idle-time** *seconds*
18. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。プロンプトが表示されたらパスワードを入力します。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 3	**parameter-map type inspect** {*parameter-map-name* | **global** | **default**} 例： `Device(config)# parameter-map type inspect eng-network-profile`	接続しきい値、タイムアウト、およびその他の **inspect** アクションに関連するパラメータの検査パラメータマップを設定し、パラメータマップタイプ検査コンフィギュレーションモードを開始します。
ステップ 4	**log** {**dropped-packets** {**disable** | **enable**} | **summary** [**flows** *number*] [**time-interval** *seconds*]} 例： `Device(config-profile)# log summary flows 15 time-interval 30`	（任意）ファイアウォール アクティビティの実行時のパケット ロギングを設定します。 （注） このコマンドが見えるのは、パラメータマップ タイプ検査コンフィギュレーション モードの場合のみです。
ステップ 5	**alert** {**on** | **off**} 例： `Device(config-profile)# alert on`	（任意）コンソールに表示されるCiscoステートフル パケット インスペクション アラート メッセージをイネーブルにします。
ステップ 6	**audit-trail** {**on** | **off**} 例： `Device(config-profile)# audit-trail on`	（任意）監査証跡メッセージをイネーブルにします。
ステップ 7	**dns-timeout** *seconds* 例： `Device(config-profile)# dns-timeout 60`	（任意）ドメインネームシステム（DNS）のアイドルタイムアウト（アクティビティのないときにDNSルックアップセッションを管理する時間の長さ）を指定します。
ステップ 8	**icmp idle-timeout** *seconds* 例： `Device(config-profile)# icmp idle-timeout 90`	（任意）ICMPセッションのタイムアウトを設定します。
ステップ 9	**max-incomplete** {**low** | **high**} *number-of-connections* 例： `Device(config-profile)# max-incomplete low 800`	（任意）Cisco ファイアウォールによるハーフオープンセッションの削除の開始および停止を起動する既存のハーフオープンセッションの数を定義します。
ステップ 10	**one-minute** {**low** | **high**} *number-of-connections* 例： `Device(config-profile)# one-minute low 300`	（任意）システムによるハーフオープン セッションの削除の開始と停止を起動する新規の未確立セッションの数を定義します。
ステップ 11	**sessions maximum** *sessions* 例： `Device(config-profile)# sessions maximum 200`	（任意）1つのゾーンペアに存在できる許可されたセッションの最大数を設定します。このコマンドを使用して、セッションによって使用される帯域幅を制限します。

	コマンドまたはアクション	目的
ステップ 12	**tcp finwait-time** *seconds* 例： `Device(config-profile)# tcp finwait-time 5`	（任意）Cisco ファイアウォールが finish-exchange（FIN-exchange）を検出した後、TCP セッションを管理する時間を指定します。
ステップ 13	**tcp idle-time** *seconds* 例： `Device(config-profile)# tcp idle-time 90`	（任意）TCP セッションのタイムアウトを設定します。
ステップ 14	**tcp max-incomplete host** *threshold* [**block-time** *minutes*] 例： `Device(config-profile)# tcp max-incomplete host 500 block-time 10`	（任意）TCP ホスト固有のサービス妨害（DoS）の検出および回避のために、しきい値とブロックする時間値を指定します。
ステップ 15	**tcp synwait-time** *seconds* 例： `Device(config-profile)# tcp synwait-time 3`	（任意）セッションをドロップする前に、TCP セッションが設定された状態に達するまで待機する時間を指定します。
ステップ 16	**tcp window-scale-enforcement loose** 例： `Device(config-profile)# tcp window-scale-enforcement loose`	（任意）ゾーン ベース ポリシー ファイアウォールにおいて無効なウィンドウ スケール オプションを持つ TCP パケットのウィンドウ スケール オプションのチェックをパラメータ マップでディセーブルにします。
ステップ 17	**udp idle-time** *seconds* 例： `Device(config-profile)# udp idle-time 75`	（任意）ファイアウォールを通る UDP セッションのアイドルタイムアウトしきい値を設定します。
ステップ 18	**end** 例： `Device(config-profile)# end`	パラメータ マップ タイプ検査コンフィギュレーション モードを終了して、特権 EXEC コンフィギュレーション モードに戻ります。

セキュリティ ゾーンとゾーン ペアの作成、およびゾーン ペアへのポリシー マップの付加

ゾーン ペアを作成するには、2 つのセキュリティ ゾーンが必要です。ただし、セキュリティ ゾーンを 1 つだけ作成し、「セルフ」と呼ばれるシステム定義のセキュリティゾーンを使用できます。「セルフ」ゾーンを選択する場合、検査ポリシングは設定できません。

ゾーンペアでは、送信元ゾーンと宛先ゾーンを同じゾーンにすることができます。デフォルトでは、ゾーン内に留まるトラフィックは検査されません。さらに、デフォルトゾーン（ゾーン割り当てのないインターフェイス）が存在し、これも指定できます。

このプロセスを使用して、次の作業を実行します。

- セキュリティ ゾーンにインターフェイスを割り当てます。
- ポリシー マップをゾーン ペアに付加します。
- セキュリティ ゾーンを少なくとも 1 つ作成します。
- ゾーン ペアを定義します。

ヒント　ゾーンを作成する前に、ゾーンの構成要素をよく検討する必要があります。一般的なガイドラインは、セキュリティの観点から同様の性質をもつインターフェイスをグループにすることです。

手順の概要

1. **enable**
2. **configure terminal**
3. **zone security** *zone-name*
4. **description** *line-of-description*
5. **exit**
6. **interface** *type number*
7. **zone-member security** *zone-name*
8. **exit**
9. **zone-pair security** *zone-pair name* [**source** *source-zone-name* | **self** | *default*] **destination** [**self** | *default* | *destination-zone-name*]
10. **description** *line-of-description*
11. **service-policy type inspect** *policy-map-name*
12. **platform inspect match-statistics per-filter**
13. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。プロンプトが表示されたらパスワードを入力します。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**zone security** *zone-name* 例： `Device(config)# zone security z1`	インターフェイスを割り当てることができるセキュリティ ゾーンを作成し、セキュリティ ゾーン コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 4	**description** *line-of-description* 例： `Device(config-sec-zone)# description Internet Traffic`	（任意）ゾーンの説明を入力します。
ステップ 5	**exit** 例： `Device(config-sec-zone)# exit`	セキュリティ ゾーン コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードに戻ります。
ステップ 6	**interface** *type number* 例： `Device(config)# interface GigabitEthernet 0/0/0`	インターフェイスを設定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 7	**zone-member security** *zone-name* 例： `Device(config-if)# zone-member security zone1`	インターフェイスを指定したセキュリティ ゾーンに割り当てます。 （注） インターフェイスをセキュリティゾーンのメンバーにした場合、そのインターフェイスを通して送受信されるすべてのトラフィックは、デフォルトでドロップされます（ただしデバイス宛のトラフィックとデバイス発のトラフィックを除きます）。トラフィックがインターフェイス通過するには、ゾーンをポリシー適用先のゾーンペアの一部にする必要があります。ポリシーがトラフィックを許可すると、トラフィックはそのインターフェイスを通過できます。
ステップ 8	**exit** 例： `Device(config-if)# exit`	インターフェイス コンフィギュレーション モードを終了し、グローバルコンフィギュレーションモードに戻ります。
ステップ 9	**zone-pair security** *zone-pair name* [**source** *source-zone-name* | **self** | *default*] **destination** [**self** | *default* | *destination-zone-name*] 例： `Device(config)# zone-pair security zp source z1 destination z2`	ゾーン ペアを作成し、セキュリティ ゾーンペア コンフィギュレーション モードを開始します。 （注） ポリシーを適用するには、ゾーン ペアを設定する必要があります。
ステップ 10	**description** *line-of-description* 例： `Device(config-sec-zone-pair)# description accounting network to internet`	（任意）ゾーン ペアの説明を入力します。

	コマンドまたはアクション	目的
ステップ 11	**service-policy type inspect** *policy-map-name* 例： `Device(config-sec-zone-pair)# service-policy type inspect p2`	ファイアウォール ポリシー マップを宛先ゾーン ペアに付加します。 （注） ゾーンのペア間でポリシーが設定されない場合、トラフィックはデフォルトでドロップされます。
ステップ 12	**platform inspect match-statistics per-filter** 例： `Device(config-sec-zone-pair)# platform inspect match-statistics per-filter`	ゾーンベース ファイアウォールのフィルタごとの統計を有効にします。 （注） デバイスでフィルタごとの統計を有効にするには、次の手順を実行します。 • デバイスをリロードします。または • すべてのサービスポリシーを削除し、統計に変更を再適用します。**platform inspect match-statistics per-filter** コマンドをアクティブにするには、すべてのサービスポリシーを再適用します。
ステップ 13	**end** 例： `Device(config-sec-zone-pair)# end`	セキュリティ ゾーンペア コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

NetFlow イベント ロギングの設定

グローバル パラメータ マップは、NetFlow イベント ロギングに使用されます。NetFlow イベント ロギングをイネーブルにすると、装置外の高速ログ コレクタにログが送信されます。デフォルトでは、この機能はイネーブルになっていません。この機能をイネーブルにしない場合、ファイアウォールのログは、ルートプロセッサまたはコンソールのロガーバッファに送信されます。

手順の概要

1. **enable**
2. **configure terminal**
3. **parameter-map type inspect-global**
4. **log dropped-packets**
5. **log flow-export v9 udp destination** *ipv4-address port*
6. **log flow-export template timeout-rate** *seconds*
7. **end**

8. **show parameter-map type inspect-global**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。プロンプトが表示されたらパスワードを入力します。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**parameter-map type inspect-global** 例： `Device(config)# parameter-map type inspect-global`	グローバル パラメータ マップを設定し、パラメータ マップ タイプ検査コンフィギュレーション モードを開始します。
ステップ 4	**log dropped-packets** 例： `Device(config-profile)# log dropped-packets`	ファイアウォールによってドロップされるすべてのパケットのロギングをイネーブルにします。
ステップ 5	**log flow-export v9 udp destination** *ipv4-address port* 例： `Device(config-profile)# log flow-export v9 udp destination 192.0.2.0 5000`	NetFlow イベント ロギングをイネーブルにして、コレクタの IP アドレスとポートを指定します。
ステップ 6	**log flow-export template timeout-rate** *seconds* 例： `Device(config-profile)# log flow-export template timeout-rate 5000`	テンプレートのタイムアウト値を指定します。
ステップ 7	**end** 例： `Device(config-profile)# end`	グローバル コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。
ステップ 8	**show parameter-map type inspect-global** 例： `Device# show parameter-map type inspect-global`	グローバル検査タイプパラメータマップ情報を表示します。

WAAS を使用したファイアウォールの設定

トラフィックをインターセプトするために L2 を使用してトラフィックを WAE デバイスにリダイレクトするファイアウォール用のエンドツーエンド WAAS トラフィックフロー最適化を設定するには、次の作業を実行します。ZBFW 環境で WCCP を設定する場合は、L2 または

GRE カプセル化が使用されます。ただし、このシナリオでは、ゾーン ベース ファイアウォールに GRE が必要であるため、L2 リダイレクションが重要です。

Cisco IOS XE ソフトウェアでは WAAS のサポートがデフォルトで有効になっており、WAAS 処理が検出されます。

（注） WAAS を使用したファイアウォールの設定（手順 5 ～ 13）は、Cisco IOS XE リリース 3.5S 以降では必要ありません。手順 5 ～ 12 のコマンドは、Cisco IOS XE リリース 3.5S 以降では廃止されています。

手順の概要

1. **enable**
2. **configure terminal**
3. **ip wccp** *service-id*
4. **ip wccp** *service-id*
5. **log dropped-packets enable**
6. **max-incomplete low**
7. **max-incomplete high**
8. **class-map type inspect** *class-name*
9. **match protocol** *protocol-name* [**signature**]
10. **exit**
11. **policy-map type inspect** *policy-map-name*
12. **class class-default**
13. **class-map type inspect** *class-name*
14. **inspect**
15. **exit**
16. **exit**
17. **zone security** *zone-name*
18. **description** *line-of-description*
19. **exit**
20. **zone-pair security** *zone-pair name* [**source** *source-zone-name* | **self**] **destination** [**self** | *destination-zone-name*]
21. **description** *line-of-description*
22. **exit**
23. **interface** *type number*
24. **description** *line-of-description*
25. **zone-member security** *zone-name*
26. **ip address** *ip-address*
27. **ip wccp** *service-id* {**group-listen** | **redirect** {**in** | **out**}}
28. **exit**
29. **zone-pair security** *zone-pair-name* {**source** *source-zone-name* | **self**} **destination** [**self** | *destination-zone-name*]
30. **service-policy type inspect** *policy-map-name*

31. end

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。プロンプトが表示されたらパスワードを入力します。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ip wccp** *service-id* 例： `Device(config)# ip wccp 61`	WCCP のダイナミックに定義されたサービス識別番号を入力します。
ステップ 4	**ip wccp** *service-id* 例： `Device(config)# ip wccp 62`	WCCP のダイナミックに定義されたサービス識別番号を入力します。
ステップ 5	**log dropped-packets enable** 例： `Device(config-profile)# log dropped-packets enable`	
ステップ 6	**max-incomplete low** 例： `Device(config)# max-incomplete low 18000`	
ステップ 7	**max-incomplete high** 例： `Device(config)# max-incomplete high 20000`	
ステップ 8	**class-map type inspect** *class-name* 例： `Device(config)# class-map type inspect most-traffic`	トラフィック クラス用の検査タイプ クラス マップを作成し、クラス マップ コンフィギュレーション モードを開始します。 （注） **class-map type inspect most-traffic** コマンドは非表示になっています。
ステップ 9	**match protocol** *protocol-name* [**signature**] 例： `Device(config-cmap)# match protocol http`	指定されたプロトコルを基づくクラス マップの一致基準を設定します。検査タイプ クラス マップの一致基準には、Cisco ステートフル パケット インスペクションでサポートされているプロトコルのみを使用できます。

	コマンドまたはアクション	目的
ステップ 10	**exit** 例： `Device(config-cmap)# exit`	クラスマップ コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードに戻ります。
ステップ 11	**policy-map type inspect** *policy-map-name* 例： `Device(config)# policy-map type inspect p1`	レイヤ 3 とレイヤ 4 の検査タイプ ポリシー マップを作成し、ポリシーマップ コンフィギュレーション モードを開始します。
ステップ 12	**class class-default** 例： `Device(config-pmap)# class class-default`	システム デフォルト クラスの照合を指定します。 • システム デフォルト クラスを指定しない場合は、未分類のパケットが照合されます。
ステップ 13	**class-map type inspect** *class-name* 例： `Device(config-pmap)# class-map type inspect most-traffic`	アクションの実行対象となるファイアウォール トラフィック（クラス）マップを指定し、ポリシーマップ クラス コンフィギュレーション モードを開始します。
ステップ 14	**inspect** 例： `Device(config-pmap-c)# inspect`	Cisco ステートフル パケット インスペクションをイネーブルにします。
ステップ 15	**exit** 例： `Device(config-pmap-c)# exit`	ポリシー マップ クラス コンフィギュレーション モードを終了し、ポリシーマップ コンフィギュレーション モードに戻ります。
ステップ 16	**exit** 例： `Device(config-pmap)# exit`	ポリシー マップ コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードに戻ります。
ステップ 17	**zone security** *zone-name* 例： `Device(config)# zone security zone1`	インターフェイスを割り当てることができるセキュリティ ゾーンを作成し、セキュリティ ゾーン コンフィギュレーション モードを開始します。
ステップ 18	**description** *line-of-description* 例： `Device(config-sec-zone)# description Internet Traffic`	（任意）ゾーンの説明を入力します。
ステップ 19	**exit** 例： `Device(config-sec-zone)# exit`	セキュリティ ゾーン コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードに戻ります。

	コマンドまたはアクション	目的
ステップ 20	**zone-pair security** *zone-pair name* [**source** *source-zone-name* | **self**] **destination** [**self** | *destination-zone-name*] 例： `Device(config)# zone-pair security zp source z1 destination z2`	ゾーン ペアを作成し、セキュリティ ゾーン コンフィギュレーション モードを開始します。 （注） ポリシーを適用するには、ゾーン ペアを設定する必要があります。
ステップ 21	**description** *line-of-description* 例： `Device(config-sec-zone)# description accounting network`	（任意）ゾーン ペアの説明を入力します。
ステップ 22	**exit** 例： `Device(config-sec-zone)# exit`	セキュリティ ゾーン コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードに戻ります。
ステップ 23	**interface** *type number* 例： `Device(config)# interface ethernet 0`	インターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 24	**description** *line-of-description* 例： `Device(config-if)# description zone interface`	（任意）インターフェイスについての説明を入力します。
ステップ 25	**zone-member security** *zone-name* 例： `Device(config-if)# zone-member security zone1`	インターフェイスを指定したセキュリティ ゾーンに割り当てます。 （注） インターフェイスをセキュリティ ゾーンのメンバーにした場合、そのインターフェイスを通して送受信されるすべてのトラフィックは、デフォルトでドロップされます（ただしデバイス宛のトラフィックとデバイス発のトラフィックを除きます）。トラフィックがインターフェイス通過するには、ゾーンをポリシーの適用先のゾーン ペアの一部にする必要があります。ポリシーがトラフィックを許可すると、トラフィックはそのインターフェイスを通過できます。
ステップ 26	**ip address** *ip-address* 例： `Device(config-if)# ip address 10.70.0.1 255.255.255.0`	セキュリティ ゾーン用のインターフェイス IP アドレスを割り当てます。

	コマンドまたはアクション	目的
ステップ 27	**ip wccp** *service-id* {**group-listen** | **redirect** {**in** | **out**}} 例： `Device(config-if)# ip wccp 61 redirect in`	インターフェイスで WCCP パラメータを指定します。
ステップ 28	**exit** 例： `Device(config-if)# exit`	インターフェイス コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードに戻ります。
ステップ 29	**zone-pair security** *zone-pair-name* {**source** *source-zone-name* | **self**} **destination** [**self** | *destination-zone-name*] 例： `Device(config)# zone-pair security zp source z1 destination z2`	ゾーン ペアを作成し、セキュリティ ゾーンペア コンフィギュレーション モードを開始します。
ステップ 30	**service-policy type inspect** *policy-map-name* 例： `Device(config-sec-zone-pair)# service-policy type inspect p2`	ファイアウォール ポリシー マップを宛先ゾーン ペアに付加します。 （注） ゾーンのペア間でポリシーが設定されない場合、トラフィックはデフォルトでドロップされます。
ステップ 31	**end** 例： `Device(config-sec-zone-pair)# end`	セキュリティ ゾーン ペア コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

ゾーンベース ファイアウォールの再分類の設定

手順の概要

1. **enable**
2. **configure terminal**
3. **parameter-map type inspect** {*parameter-map-name* | **global** | session-reclassify-allow}

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。プロンプトが表示されたらパスワードを入力します。
ステップ 2	**configure terminal** 例：	グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
	`Device# configure terminal`	
ステップ 3	**parameter-map type inspect** {*parameter-map-name* | **global** | session-reclassify-allow}	**parameter-map type inspect-global** モードで **session-reclassify-allow** 属性を設定して、セッションの再分類を有効にします。 この設定を無効にするには、**session-reclassify-allow** コマンドの **no** 形式を使用します。

ゾーンベース ポリシー ファイアウォールの設定例

ここでは、ゾーンベース ポリシー ファイアウォールの設定に関連する例を示します。

例：レイヤ 3 およびレイヤ 4 ファイアウォール ポリシーの設定

次の例は、レイヤ 3 またはレイヤ 4 トップレベル ポリシーを示します。トラフィックは ACL 199 と一致し、ディープパケット HTTP インスペクションが設定されます。**match access-group 101** を設定すると、レイヤ 4 インスペクションが有効になります。その結果、クラスマップのタイプが match-all である場合を除いて、レイヤ 7 インスペクションが省略されます。

```
class-map type inspect match-all http-traffic
 match protocol http
 match access-group 101
!
policy-map type inspect mypolicy
 class type inspect http-traffic
  inspect
  service-policy http http-policy
```

例：検査パラメータ マップの作成

次の設定例は、検査パラメータマップの作成を示しています。

```
parameter-map type inspect eng-network-profile
 alert on
 audit-trail on
 dns-timeout 60
 icmp idle-timeout 90
 max-incomplete low 800
 one-minute low 300
 sessions maximum 200
 tcp finwait-time 5
 tcp idle-time 90
 tcp max-incomplete host 500 block-time 10
 tcp synwait-time 3
 udp idle-time 75
```

例：セキュリティ ゾーンとゾーン ペアの作成とゾーン ペアへのポリシー マップのアタッチ

例：セキュリティ ゾーンの作成

次に、finance department networks という名前のセキュリティ ゾーン z1 と engineering services network という名前のセキュリティ ゾーン z2 を作成する例を示します。

```
zone security z1
 description finance department networks
!
zone security z2
 description engineering services network
```

例：ゾーン ペアの作成

次に、ゾーン z1 とゾーン z2 を作成し、ゾーン z2 でゾーン間を流れるトラフィックにファイアウォール ポリシー マップが適用されるように指定する例を示します。

```
zone-pair security zp source z1 destination z2
service-policy type inspect p1
```

例：セキュリティ ゾーンへのインターフェイスの割り当て

次に、イーサネット インターフェイス 0 をゾーン z1 に、イーサネット インターフェイス 1 をゾーン z2 にアタッチする例を示します。

```
interface ethernet0
 zone-member security z1
!
interface ethernet1
 zone-member security z2
```

例：ゾーンベース ファイアウォールのフィルタごとの統計

次の設定例は、多数のファイアウォールフィルタが作成される場合にメモリ不足を回避する方法を示しています。メモリ不足を防ぐために、**platform inspect match-statistics per-filter** コマンドを使用してゾーンベース ファイアウォールのフィルタごとの統計を有効にすることができます。この例では、フィルタ（ACL または UDP）ごとに、ゾーンベース ファイアウォールを通過したパケット数とバイト数について使用可能な統計が存在します。

```
Device# show policy-map type inspect zone-pair ogacl_zp
 Zone-pair: ogacl_zp
  Service-policy inspect : ogacl_pm
Class-map: ogacl_cm (match-any)
  Match: access-group name ogacl
        xxx packets, xxx bytes
      Match: protocol udp
        xxx packets, xxx bytes
```

（注） フィルタごとの統計は、match-any フィルタについてのみ使用でき、match-all の場合には適用されません。

（注） Cisco IOS XE 16.3 リリースおよび Cisco IOS XE 16.4 リリースの場合、フィルタごとの統計を有効にするには、**platform inspect match-statistics per-filter** コマンドをアクティブにする前に、デバイスをリロードするかサービスポリシーを削除してから、ゾーンペアにサービスポリシーを再適用します。

Cisco IOS XE 3.17 リリースの場合、このコマンドをアクティブにするには、設定を保存し、システムをリロードする必要があります。

（注） 同様に、フィルタごとの統計を無効にするには、デバイスをリロードするかサービスポリシーを削除してから、ゾーンペアにサービスポリシーを再適用します。

デバイスで使用されている TCAM メモリを確認するには、**show platform hardware qfp active classification feature-manager shm-stats-counter** コマンドを使用します。

```
Device# show platform hardware qfp active classification feature-manager shm-stats-counter
    Shared Memory Information:
    Total shared memory size: 16777216
    Used shared memory size: 14703656
```

（注） トラフィックドロップまたはフィルタごとの統計のカウンタが表示されないときは、多くの場合、使用されている TCAM 共有メモリが TCAM 合計の 75% を超えています。

（注） デバイスで使用されている共有メモリがキャパシティの 75% を超えると、次の警告メッセージが表示されます。

```
%CPP_FM-3-CPP_FM_TCAM_WARNING: SIP1: cpp_sp_svr: TCAM limit exceeded: Already used 75
percent shared memory for per-filter stats.
```

デバイスで使用されている共有メモリが 100% の場合は、次の警告メッセージが表示されます。

```
%CPP_FM-3-CPP_FM_TCAM_WARNING: SIP1: cpp_sp_svr: TCAM limit exceeded: Shared memory for
per-filter stats overflow!
```

例：NetFlow イベント ロギングの設定

次に、NetFlow イベントロギングを設定する例を示します。

```
parameter-map type inspect global
 log dropped-packets
 log flow-export v9 udp destination 192.0.2.0 5000
 log flow-export template timeout rate 5000
```

例：WAAS を使用した Cisco ファイアウォールの設定

次に、WCCP を使用してトラフィックを検査のために WAE デバイスにトラフィックをリダイレクトするファイアウォールのエンドツーエンドの WAAS トラフィックフローを最適化する設定の例を示します。

次に、integrated-service-engine インターフェイスが異なるゾーンで設定され、各セキュリティゾーンメンバーにインターフェイスが割り当てられているために、セキュリティゾーンメンバー間でトラフィックがドロップされないようにする設定例を示します。

```
! Zone-based firewall configuration on your router.
ip wccp 61
ip wccp 62
parameter-map type inspect global
 log dropped-packets enable
 max-incomplete low 18000
 max-incomplete high 20000
!
class-map type inspect match-any most-traffic
 match protocol icmp
 match protocol ftp
 match protocol tcp
 match protocol udp
!
policy-map type inspect p1
 class type inspect most-traffic
  inspect
!
 class class-default
  drop
!
zone security in
!
zone security out
!
zone security waas
!
zone-pair security in-out source in destination out
 service-policy type inspect p1
!
zone-pair security out-in source out destination in
 service-policy type inspect p1
!
zone-pair security waas-out source waas destination out
 service-policy type inspect p1
!
zone-pair security in-waas source in destination waas
 service-policy type inspect p1
```

```
!
interface GigabitEthernet0/0
 description WAN Connection
 no ip dhcp client request tftp-server-address
 no ip dhcp client request router
 ip address dhcp
 ip wccp 62 redirect in
 ip wccp 61 redirect out
 ip flow ingress
 ip nat outside
 ip virtual-reassembly in
 ip virtual-reassembly out
 zone-member security out
 load-interval 30
 delay 30
 duplex auto
 speed auto
!
interface GigabitEthernet0/1
 description Clients
 ip address 172.25.50.1 255.255.255.0
 ip pim sparse-mode
 ip nat inside
 ip virtual-reassembly in
 zone-member security in
 ip igmp version 3
 delay 30
 duplex auto
 speed auto
!
interface Vlan1
 description WAAS Interface
 ip address 172.25.60.1 255.255.255.0
 ip wccp redirect exclude in
 ip nat inside
 ip virtual-reassembly in
 zone-member security waas
 load-interval 30
!
```

次に、ゾーンベース ファイアウォール サポートするための WAE 上での設定例を示します。この設定は、ルータでは行うことができず、WAE でのみ行うことができることに注意してください。

```
!Configuration on the WAE.
primary-interface Virtual 1/0
interface Virtual 1/0
 ip address 172.25.60.12 255.255.255.0
!
ip default-gateway 172.25.60.1
wccp router-list 1 172.25.60.1
wccp tcp-promiscuous service-pair 61 62
 router-list-num 1
 redirect-method gre
 egress-method ip-forwarding
 enable
!
```

例：同じゾーン内の FlexVPN と DVTI を使用したファイアウォールの設定

次に、FlexVPN およびダイナミック仮想トンネルインターフェイス（DVTI）が同じゾーンに設定されたファイアウォールの例を示します。

```
crypto ikev2 proposal PROP
 encryption 3des
 integrity sha256
 group 5
crypto ikev2 policy POL
 match fvrf any
 proposal PROP
crypto ikev2 keyring keyring1
 peer peer
 address 0.0.0.0 0.0.0.0
 pre-shared-key cisco
crypto ikev2 profile prof1
 authentication remote pre-share
 authentication local pre-share
 match identity remote address 0.0.0.0
 match address local interface loopback1
 keyring local keyring1
 no shutdown
 Virtual-Template 1
class-map type inspect match-any cmap
 match protocol icmp
 match protocol tcp
 match protocol udp
policy-map type inspect pmap
 class type inspect cmap
 inspect
 class class-default
 drop log
zone security in
zone security zone1
zone-pair security zp1 source zone1 destination in
 service-policy type inspect pmap
crypto ipsec profile ipsec1
 set ikev2-profile prof1
interface Loopback1
 ip address 51.1.1.1 255.255.255.0
interface Gi0/0/0.2
 encapsulation dot1q 2
 ip address 100.1.1.1 255.255.255.0
 zone-member security in
interface Gi0/0/0.3
 encapsulation dot1q 3
 ip address 100.1.2.1 255.255.255.0
 zone-member security in
interface Gi0/0/0.4
 encapsulation dot1q 4
 ip address 100.1.3.1 255.255.255.0
 zone-member security in
interface Gi0/0/0.5
 encapsulation dot1q 5
 ip address 100.1.4.1 255.255.255.0
 zone-member security in
interface Gi0/0/0.6
 encapsulation dot1q 6
 ip address 100.1.5.1 255.255.255.0
```

```
 zone-member security in
interface Virtual-Template1 type tunnel
 ip unnumbered loopback1
 zone-member security zone1
 tunnel source loopback1
 tunnel mode ipsec ipv4
 tunnel protection ipsec profile ipsec1
ip route 60.0.0.0 255.0.0.0 192.168.2.2
```

例：別のゾーン内の FlexVPN と DVTI を使用したファイアウォールの設定

次に、FlexVPN およびダイナミック仮想トンネルインターフェイス（DVTI）が別のゾーンに設定されたファイアウォールの例を示します。

```
crypto ikev2 proposal PROP
 encryption 3des
 integrity sha256
 group 5
crypto ikev2 policy POL
 match fvrf any
 proposal PROP
crypto ikev2 keyring keyring1
 peer peer1
 address 0.0.0.0 0.0.0.0
 pre-shared-key cisco1
crypto ikev2 keyring keyring2
 peer peer2
 address 0.0.0.0 0.0.0.0
 pre-shared-key cisco2
crypto ikev2 keyring keyring3
 peer peer3
 address 0.0.0.0 0.0.0.0
 pre-shared-key cisco3
crypto ikev2 keyring keyring4
 peer peer4
 address 0.0.0.0 0.0.0.0
 pre-shared-key cisco4
crypto ikev2 keyring keyring5
 peer peer5
 address 0.0.0.0 0.0.0.0
 pre-shared-key cisco5
crypto ikev2 profile prof1
 authentication remote pre-share
 authentication local pre-share
 match identity remote address 0.0.0.0
 match address local interface loopback1
 keyring local keyring1
 no shutdown
 Virtual-Template 1
crypto ikev2 profile prof2
 authentication remote pre-share
 authentication local pre-share
 match identity remote address 0.0.0.0
 match address local interface loopback2
 keyring local keyring2
 no shutdown
 Virtual-Template 2
crypto ikev2 profile prof3
 authentication remote pre-share
 authentication local pre-share
```

```
 match identity remote address 0.0.0.0
 match address local interface loopback3
 keyring local keyring3
crypto ikev2 profile prof4
 authentication remote pre-share
 authentication local pre-share
 match identity remote address 0.0.0.0
 match address local interface loopback4
 keyring local keyring4
 no shutdown
 Virtual-Template 4
crypto ikev2 profile prof5
 authentication remote pre-share
 authentication local pre-share
 match identity remote address 0.0.0.0
 match address local interface loopback5
 keyring local keyring5
 no shutdown
 Virtual-Template 5
class-map type inspect match-any cmap
 match protocol icmp
 match protocol tcp
 match protocol udp
policy-map type inspect pmap
 class type inspect cmap
 inspect
 class class-default
 drop log
zone security in
zone security zone1
zone security zone2
zone security zone3
zone security zone4
zone security zone5
zone-pair security zp1 source zone1 destination in
 service-policy type inspect pmap
zone-pair security zp2 source zone2 destination in
 service-policy type inspect pmap
zone-pair security zp3 source zone3 destination in
 service-policy type inspect pmap
zone-pair security zp4 source zone4 destination in
 service-policy type inspect pmap
zone-pair security zp5 source zone5 destination in
 service-policy type inspect pmap
crypto ipsec profile ipsec1
 set ikev2-profile prof1
crypto ipsec profile ipsec2
 set ikev2-profile prof2
crypto ipsec profile ipsec3
 set ikev2-profile prof3
crypto ipsec profile ipsec4
 set ikev2-profile prof4
crypto ipsec profile ipsec5
 set ikev2-profile prof5
interface Loopback1
 ip address 50.1.1.1 255.255.255.0
interface Loopback2
 ip address 50.1.2.1 255.255.255.0
interface Loopback3
 ip address 50.1.3.1 255.255.255.0
interface Loopback4
 ip address 50.1.4.1 255.255.255.0
interface Loopback5
 ip address 50.1.5.1 255.255.255.0
```

```
interface Gi0/0/0.2
 encapsulation dot1q 2
 ip address 100.1.1.1 255.255.255.0
 zone-member security in
interface Gi0/0/0.3
 encapsulation dot1q 3
 ip address 100.1.2.1 255.255.255.0
 zone-member security in
interface Gi0/0/0.4
 encapsulation dot1q 4
 ip address 100.1.3.1 255.255.255.0
 zone-member security in
interface Gi0/0/0.5
 encapsulation dot1q 5
 ip address 100.1.4.1 255.255.255.0
 zone-member security in
interface Gi0/0/0.6
 encapsulation dot1q 6
 ip address 100.1.5.1 255.255.255.0
 zone-member security in
interface Virtual-Template1 type tunnel
 ip unnumbered loopback1
 zone-member security zone1
 tunnel source loopback1
 tunnel mode ipsec ipv4
 tunnel protection ipsec profile ipsec1
interface Virtual-Template2 type tunnel
 ip unnumbered loopback2
 zone-member security zone2
 tunnel source loopback2
 tunnel mode ipsec ipv4
 tunnel protection ipsec profile ipsec2
interface Virtual-Template3 type tunnel
 ip unnumbered loopback3
 zone-member security zone3
 tunnel source loopback3
 tunnel mode ipsec ipv4
 tunnel protection ipsec profile ipsec3
interface Virtual-Template4 type tunnel
 ip unnumbered loopback4
 zone-member security zone4
 tunnel source loopback4
 tunnel mode ipsec ipv4
 tunnel protection ipsec profile ipsec4
interface Virtual-Template5 type tunnel
 ip unnumbered loopback5
 zone-member security zone5
 tunnel source loopback5
 tunnel mode ipsec ipv4
 tunnel protection ipsec profile ipsec5
ip route 60.0.0.0 255.0.0.0 192.168.2.2
```

ゾーンベース ポリシー ファイアウォールに関する追加情報

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『Cisco IOS Master Command List, All Releases』
ファイアウォール コマンド	• 『Cisco IOS Security Command Reference: Commands A to C』 • 『Cisco IOS Security Command Reference: Commands D to L』 • 『Cisco IOS Security Command Reference: Commands M to R』 • 『Cisco IOS Security Command Reference: Commands S to Z』

シスコのテクニカル サポート

説明	リンク
シスコのサポート Web サイトでは、シスコの製品やテクノロジーに関するトラブルシューティングにお役立ていただけるように、マニュアルやツールをはじめとする豊富なオンライン リソースを提供しています。 お使いの製品のセキュリティ情報や技術情報を入手するために、Cisco Notification Service（Field Notice からアクセス）、Cisco Technical Services Newsletter、Really Simple Syndication（RSS）フィードなどの各種サービスに加入できます。 シスコのサポート Web サイトのツールにアクセスする際は、Cisco.com のユーザ ID およびパスワードが必要です。	http://www.cisco.com/support を使用して無効にすることができます。

第 123 章

ゾーンベース ポリシー ファイアウォールの IPv6 サポート

ゾーンベース ポリシー ファイアウォールは、IPv4 パケットの高度なトラフィック フィルタリングまたはインスペクションを提供します。IPv6 サポートにより、ゾーンベース ポリシー ファイアウォールは、IPv6 パケットのインスペクションをサポートします。IPv6 サポートの前は、ファイアウォールは IPv4 パケットのインスペクションしかサポートしていませんでした。レイヤ 4 プロトコル、Internet Control Messaging Protocol（ICMP）、TCP、および UDP パケットだけが IPv6 パケット インスペクションの対象です。

このモジュールでは、サポートされるファイアウォール機能と IPv6 パケット インスペクション用のファイアウォールの設定方法について説明します。

ゾーンベース ポリシー ファイアウォールの IPv6 サポートに関する制約事項

以下の機能がサポートされません。

- アプリケーション レベル ゲートウェイ（ALG）
- ボックスツーボックス ハイアベイラビリティ（HA）
- 分散型サービス妨害攻撃
- ファイアウォール リソース管理

- レイヤ 7 インスペクション
- マルチキャスト パケット
- サブスクライバ単位のファイアウォールまたはブロードバンド ベース ファイアウォール
- ステートレス ネットワーク アドレス変換 64（NAT64）
- VRF 対応ソフトウェア インフラストラクチャ（VASI）
- Wide Area Application Services（WAAS）と Web Cache Communication Protocol（WCCP）

VASI インターフェイス経由の IPv6 ゾーンベース ファイアウォール サポートに関する情報

ファイアウォール機能の IPv6 サポート

次の表に記載されているファイアウォール機能は、IPv6 パケット インスペクションでサポートされています。

表 *166 : IPv6* でサポートされるファイアウォール機能

機能	設定情報
クラス マップ	「ゾーンベース ポリシー ファイアウォール」モジュール。
Internet Control Message Protocol バージョン 6（ICMPv6）、TCP、および UDP プロトコル	• 「*ICMP* のファイアウォール ステートフル インスペクション」モジュール。 • 「ゾーンベース ポリシー ファイアウォール」モジュール。
IP フラグメンテーション	「仮想フラグメンテーション再構成」モジュール。
シャーシ間 HA	—
エラー メッセージのロギング	「ゾーンベース ポリシー ファイアウォール」モジュール。
ネストされたクラス マップ	「ゾーンベース ポリシー ファイアウォールに対するネストされたクラス マップのサポート」モジュール。

機能	設定情報
Out-of-Order パケットの処理	「ゾーンベース ポリシー ファイアウォール」モジュールの「Out-of-Order パケット処理」の項。
パラメータ マップ（インスペクション タイプ パラメータ マップの場合、パラメータ マップで定義されたセッション数は、IPv4 セッションと IPv6 セッションの合計数に適用されます）	「ゾーンベース ポリシー ファイアウォール」モジュール。
ポリシー マップ	「ゾーンベース ポリシー ファイアウォール」モジュール。
ポートとアプリケーションのマッピング	—
ステートフル ネットワーク アドレス変換 64（NAT64）	『*IP Addressing: NAT Configuration Guide*』の「*Stateful Network Address Translation 64*」モジュール。
TCP SYN Cookie	「ファイアウォール *TCP SYN Cookie* の設定」モジュール。
VPN ルーティングおよび転送（VRF）対応ファイアウォール	「*VRF* 対応 *Cisco IOS XE* ファイアウォール」モジュール。
仮想フラグメンテーション再構成（VFR）	「仮想フラグメンテーション再構成」モジュール。
ゾーン、デフォルト ゾーン、ゾーン ペア	「ゾーンベース ポリシー ファイアウォール」モジュール。

デュアルスタック ファイアウォール

デュアル スタック ファイアウォールは、IPv4 および IPv6 トラフィックを同時に実行するファイアウォールです。デュアル スタック ファイアウォールは、次のシナリオで設定できます。

- IPv4 トラフィックを実行する 1 つのファイアウォール ゾーン、および IPv6 トラフィックを実行する別のファイアウォール ゾーン。
- IPv4 と IPv6 が、ステートフル ネットワーク アドレス変換 64（NAT64）を使用して導入している場合に共存しています。このシナリオでは、トラフィックは IPv6 から IPv4 および IPv4 から IPv6 の方向で流れます。
- 同じゾーン ペアで IPv4 および IPv6 トラフィックの両方が許可されています。

IPv6 ヘッダーのフィールドのファイアウォール アクション

次の表で、IPv6 ヘッダーのフィールドのファイアウォール アクションを（IPv6 ヘッダーで使用可能な順に）説明します。

表 *167 : IPv6* ヘッダーのフィールド

IPv6 ヘッダーのフィールド	IPv6 ヘッダーのフィールドの詳細	ファイアウォール アクション
バージョン	IPv4 パケット ヘッダーのバージョン フィールドに該当しますが、IPv4 で示される数字 4 の代わりに、IPv6 では数字 6 が示されます。	IPv6 である必要があります。
トラフィック クラス	IPv4 パケット ヘッダーのタイプ オブ サービス（ToS）フィールドと同様です。トラフィック クラス フィールドは、差別化されたサービスで使用されるトラフィック クラスのタグをパケットに付けます。	検査されません。
フロー ラベル	IPv6 パケット ヘッダーの新しいフィールドです。フロー ラベル フィールドは、ネットワーク層でパケットを差別化する特定のフローのタグをパケットに付けます。	検査されません。
ペイロード長	IPv4 パケット ヘッダーの合計長フィールドと同様です。ペイロード長フィールドは、パケットのデータ部分の合計長を示します。	ファイアウォールは、いくつかのレイヤ 4 プロトコル（ICMP、TCP など）の長さを計算するためにこのフィールドを限定ベースで使用します。
次ヘッダー長	IPv4 パケット ヘッダーのプロトコル フィールドと同様です。次ヘッダー長フィールドの値により、基本 IPv6 ヘッダーに続く情報のタイプが決まります。基本 IPv6 ヘッダーの後ろに続く情報のタイプは、TCP や UDP パケットなどのトランスポート層パケット、または拡張ヘッダーです。	ファイアウォールは、セッションを作成するためにこのフィールドを認識する必要があります。

IPv6 ヘッダーのフィールド	IPv6 ヘッダーのフィールドの詳細	ファイアウォール アクション
ホップ リミット	IPv4 パケット ヘッダーの存続可能時間（TTL）フィールドと同様です。ホップ リミット フィールドの値は、IPv6 パケットが無効になるまでに通過できるデバイスの最大数を指定します。各デバイスを通過するたびに、ホップ リミットの値が 1 ずつ減少します。IPv6 ヘッダーにはチェックサムがないため、デバイスはチェックサムを計算し直すことなく、値を減少できます。	検査されません。

IPv6 ファイアウォール セッション

トラフィックのステートフルインスペクションを実行するために、ファイアウォールは、トラフィック フローごとに内部セッションを作成します。セッション情報には、送信元と宛先の IP アドレス、送信元と宛先の TCP/UDP ポートまたは ICMP タイプ、レイヤ 4 プロトコル タイプ（ICMP、TCP、UDP）、および VPN ルーティングおよび転送（VRF）ID が含まれます。IPv6 ファイアウォールの場合、送信元アドレスと宛先アドレスには IPv6 アドレスの 128 ビットが含まれます。

ファイアウォールは最初のパケットを受信した後、そのパケットが設定済みポリシーに一致すると、TCP セッションを作成します。ファイアウォールは TCP シーケンス番号をトラッキングし、設定されている範囲内にないシーケンス番号を持つ TCP パケットをドロップします。セッションが削除されるのは、TCP アイドル タイマーが満了した時点、または適切なシーケンス番号を持つリセット（RST）パケットあるいは終了確認（FIN-ACK）パケットを受信した時点です。

ファイアウォールは、設定済みポリシーに一致する最初の UDP パケットを受信すると UDP セッションを作成し、UDP アイドル タイマーが満了した時点でセッションを削除します。マルチキャスト IPv6 アドレスまたは不明な IPv6 アドレスが設定された IPv6 パケットに対しては、ファイアウォールは TCP セッションも UDP セッションも作成しません。

フラグメント化されたパケットのファイアウォールインスペクション

ファイアウォールは、フラグメント化された IPv6 パケットのインスペクションをサポートしています。IP フラグメンテーションは、単一の IP データグラムを小さなサイズの複数のパケットに分割するプロセスです。IPv6 では、エンド ノードはパス最大伝送ユニット（MTU）探索を実行して、送信されるパケットの最大サイズを判別し、MTU サイズよりも大きいパケットについて、フラグメント拡張ヘッダーが含まれる IPv6 パケットを生成します。

ファイアウォールは、仮想フラグメンテーション再構成（VFR）を使用して、フラグメント化されたパケットを検査します。VFR は、順序が正しくないフラグメントのフラグメント拡張

ヘッダーを調べ、インスペクションのためにそれらを正しい順序に配置します。インターフェイスをゾーンに追加してインターフェイス上のファイアウォールを有効にすると、VFRは同じインターフェイス上で自動的に設定されます。明示的に VFR を無効にした場合、ファイアウォールはレイヤ4ヘッダーを持つ最初のフラグメントだけを検査し、残りのフラグメントは検査なしで渡します。

フラグメント拡張ヘッダーは、次のヘッダー順で表示されます。

- IPv6 ヘッダー
- ホップバイホップ オプション ヘッダー
- 宛先オプション ヘッダー
- ルーティング ヘッダー
- フラグメント拡張ヘッダー

Cisco Express Forwarding は、フラグメント拡張ヘッダーが含まれている IPv6 パケットを検査することで、ファイアウォールがパケットを処理する前にさらにチェックする必要がないようにします。

ICMPv6 メッセージ

IPv6 ではICMPv6 を使用して診断機能、エラー レポート、およびネイバー探索を実行します。ICMPv6 メッセージは情報メッセージとエラー メッセージにグループ化されます。

ファイアウォールで検査するのは、次の ICMPv6 メッセージのみです。

- ECHO REQUEST
- ECHO REPLY
- DESTINATION UNREACHABLE
- PACKET TOO BIG
- PARAMETER PROBLEM
- TIME EXCEEDED

（注） ネイバー探索パケットは渡されて、ファイアウォールでは検査されません。

ステートフル NAT64 のファイアウォール サポート

ゾーンベース ポリシー ファイアウォールでは、ステートフル NAT64 をサポートしています。ステートフル NAT64 は、IPv6 パケットを IPv4 パケットに（またはその逆に）変換します。ファイアウォールとステートフル NAT64 の両方をルータ上に設定すると、ファイアウォールはアクセス コントロール リスト（ACL）に含まれる IP アドレスを使用してパケットをフィル

タリングします。ただし、ACL に IPv4 アドレスと IPv6 アドレスを混在させることはできません。ファイアウォールとステートフル NAT64 を連動させるには、先に IPv6 ACL を使用して、IPv4 アドレスを IPv6 ACL に組み込む必要があります。

（注） ステートフル NAT64 は VRF に対応していないため、ファイアウォールとステートフル NAT64 設定とをあわせて VRF を使用することはできません。

ファイアウォールのクラス マップで ACL を使用する場合、ACL ではホスト上の実際の IP アドレスを使用してパケット フローを設定する必要があります。送信元アドレスまたは宛先アドレスのみが必要な場合は、クラス マップ ACL で IPv4 アドレスまたは IPv6 アドレスのいずれかを使用します。送信元アドレスと宛先アドレスの両方に基づいてパケット フローをフィルタリングするには、IPv6 アドレスを使用すること、および ACL に IPv4 アドレスを組み込むことが必要です。ACL では IPv6 アドレスを使用してステートフル NAT64 パケットをフィルタリングする必要があります。

（注） ファイアウォールを使用したステートレス NAT64 はサポートされていません。

ポートとアプリケーションのマッピング

ポートとアプリケーションのマッピング（PAM）を使用して、ネットワーク サービスとアプリケーション用の TCP または UDP ポート番号をカスタマイズできます。ファイアウォールは PAM を使用して、TCP または UDP ポート番号を特定のネットワーク サービスまたはアプリケーションに関連付けます。ポート番号をネットワーク サービスまたはアプリケーションにマッピングすることで、管理者は定義されていないカスタム設定に対して既知のポートを使用することによりファイアウォール インスペクションを適用できます。PAM を設定するには、**ip port-map** コマンドを使用します。

ハイ アベイラビリティおよび ISSU

IPv6 ファイアウォールはボックス内 HA をサポートしています。ファイアウォール セッションはスイッチオーバー用にスタンバイ Embedded Services Processor（ESP）と同期されます。In Service Software Upgrade（ISSU）も IPv6 ファイアウォールでサポートされています。

トラフィック クラスの pass アクション

ファイアウォールでは、トラフィック クラスが一連のパケットをその内容に基づいて識別します。クラスを定義し、識別されたトラフィックにポリシーを反映するアクションを適用できます。アクションは、トラフィック クラスに関連付けられる特定の機能です。クラスに対して、inspect、drop、および pass アクションを設定できます。

pass アクションは、トラフィックをあるゾーンから別のゾーンに渡します。pass アクションを設定すると、ファイアウォールはトラフィックを検査せずに渡します。IPv6 ファイアウォールでは、ゾーンペアと pass アクションを設定したポリシーマップを定義することにより、リターン トラフィックに対して明示的に pass アクションを設定する必要があります。

次の例に、IPv6 トラフィックのポリシー マップ（outside-to-inside-policy および inside-to-outside-policy）で pass アクションを設定する方法を示します。

```
policy-map type inspect outside-to-inside-policy
 class type inspect ipv6-class
  pass (Defines pass action for the ipv6-class from the outside to the inside)
!
 class class-default
!
policy-map type inspect inside-to-outside-policy
 class type inspect ipv4-class
  inspect (Defines inspect action for ipv4-class)
 class type inspect v6_class
  pass (Defines pass action for ipv6-class from the inside to the outside)
 class class-default
!
!
zone security inside
!
zone security outside
!
zone-pair security in-out source inside destination outside
 service-policy type inspect inside-to-outside-policy
!
zone-pair security out-in source outside destination inside
 service-policy type inspect outside-to-inside-policy
```

ゾーンベース ポリシー ファイアウォールの IPv6 サポートの設定方法

IPv6 ファイアウォールの設定

IPv4 ファイアウォールと IPv6 ファイアウォールを設定する手順は同じです。IPv6 ファイアウォールを設定するには、IPv6 アドレス ファミリだけがマッチングされるようにクラス マップを設定する必要があります。

match protocol コマンドは IPv4 トラフィックと IPv6 トラフィックの両方に適用され、IPv4 ポリシーと IPv6 ポリシーのどちらにもこれを含めることができます。

手順の概要

1. **enable**
2. **configure terminal**
3. **vrf-definition** *vrf-name*
4. **address-family ipv6**
5. **exit-address-family**

6. **exit**
7. **parameter-map type inspect** *parameter-map-name*
8. **sessions maximum** セッション
9. **exit**
10. **ipv6 unicast-routing**
11. **ip port-map** *appl-name* **port** *port-num* **list** *list-name*
12. **ipv6 access-list** *access-list-name*
13. **permit ipv6 any any**
14. **exit**
15. **class-map type inspect match-all** *class-map-name*
16. **match access-group name** *access-group-name*
17. **match protocol** *protocol-name*
18. **exit**
19. **policy-map type inspect** *policy-map-name*
20. **class type inspect** *class-map-name*
21. **inspect** [*parameter-map-name*]
22. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを開始します。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**vrf-definition** *vrf-name* 例： `Device(config)# vrf-definition VRF1`	Virtual Routing and Forwarding（VRF）ルーティング テーブルインスタンスを設定し、VRF コンフィギュレーション モードを開始します。
ステップ 4	**address-family ipv6** 例： `Device(config-vrf)# address-family ipv6`	VRF アドレス ファミリ コンフィギュレーション モードを開始して、標準 IPv6 アドレス プレフィックスを伝送するセッションを設定します。
ステップ 5	**exit-address-family** 例： `Device(config-vrf-af)# exit-address-family`	VRF アドレス ファミリ コンフィギュレーション モードを終了し、VRF コンフィギュレーション モードを開始します。
ステップ 6	**exit** 例： `Device(config-vrf)# exit`	VRF コンフィギュレーション モードを終了して、グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 7	**parameter-map type inspect** *parameter-map-name* 例： `Device(config)# parameter-map type inspect ipv6-param-map`	ファイアウォールのグローバル検査タイプ パラメータ マップを、検査アクションに関連するしきい値、タイムアウト、その他のパラメータに接続できるようにし、パラメータ マップ タイプ検査コンフィギュレーション モードを開始します。
ステップ 8	**sessions maximum** セッション 例： `Device(config-profile)# sessions maximum 10000`	ゾーン ペア上に存在可能な最大許容セッション数を設定します。
ステップ 9	**exit** 例： `Device(config-profile)# exit`	パラメータ マップ タイプ検査コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードを開始します。
ステップ 10	**ipv6 unicast-routing** 例： `Device(config)# ipv6 unicast-routing`	IPv6 ユニキャスト データグラムの転送を有効にします。
ステップ 11	**ip port-map** *appl-name* **port** *port-num* **list** *list-name* 例： `Device(config)# ip port-map ftp port 8090 list ipv6-acl`	IPv6 アクセス コントロール リスト（ACL）を使用してポート/アプリケーション間マッピング（PAM）を確立します。
ステップ 12	**ipv6 access-list** *access-list-name* 例： `Device(config)# ipv6 access-list ipv6-acl`	IPv6 アクセスリストを定義し、IPv6 アクセス リスト コンフィギュレーション モードを開始します。
ステップ 13	**permit ipv6 any any** 例： `Device(config-ipv6-acl)# permit ipv6 any any`	IPv6 アクセス リストに許可条件を設定します。
ステップ 14	**exit** 例： `Device(config-ipv6-acl)# exit`	IPv6 アクセス リスト コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードを開始します。
ステップ 15	**class-map type inspect match-all** *class-map-name* 例： `Device(config)# class-map type inspect match-all ipv6-class`	アプリケーション固有の検査タイプ クラス マップを作成し、QoS クラス マップ コンフィギュレーション モードを開始します。
ステップ 16	**match access-group name** *access-group-name* 例： `Device(config-cmap)# match access-group name ipv6-acl`	指定した ACL をベースにクラス マップに対して一致基準を設定します。

	コマンドまたはアクション	目的
ステップ 17	**match protocol** *protocol-name* 例： `Device(config-cmap)# match protocol tcp`	指定されたプロトコルに基づき、クラス マップの一致基準を設定します。
ステップ 18	**exit** 例： `Device(config-cmap)# exit`	QoS クラス マップ コンフィギュレーション モードを終了し、グローバルコンフィギュレーションモードを開始します。
ステップ 19	**policy-map type inspect** *policy-map-name* 例： `Device(config)# policy-map type inspect ipv6-policy`	プロトコル固有の検査タイプ ポリシー マップを作成し、QoS ポリシーマップ コンフィギュレーション モードを開始します。
ステップ 20	**class type inspect** *class-map-name* 例： `Device(config-pmap)# class type inspect ipv6-class`	アクションの実行対象となるトラフィック クラスを指定し、QoS ポリシー マップ クラス コンフィギュレーション モードを開始します。
ステップ 21	**inspect** [*parameter-map-name*] 例： `Device(config-pmap-c)# inspect ipv6-param-map`	ステートフル パケット インスペクションをイネーブルにします。
ステップ 22	**end** 例： `Device(config-pmap-c)# end`	QoS ポリシーマップ クラス コンフィギュレーション モードを終了し、特権 EXEC モードを開始します。

ゾーンの設定とインターフェイスへのゾーンの適用

手順の概要

1. **enable**
2. **configure terminal**
3. **zone security** *zone-name*
4. **exit**
5. **zone security** *zone-name*
6. **exit**
7. **zone-pair security** *zone-pair-name* [**source** *source-zone* **destination** *destination-zone*]
8. **service-policy type inspect** *policy-map-name*
9. **exit**
10. **interface** *type number*
11. **ipv6 address** *ipv6-address/prefix-length*
12. **encapsulation dot1q** *vlan-id*
13. **zone-member security** *zone-name*

14. **end**
15. **show policy-map type inspect zone-pair sessions**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを開始します。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**zone security** *zone-name* 例： `Device(config)# zone security z1`	セキュリティ ゾーンを作成し、セキュリティ ゾーン コンフィギュレーション モードを開始します。
ステップ 4	**exit** 例： `Device(config-sec-zone)# exit`	セキュリティ ゾーン コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードを開始します。
ステップ 5	**zone security** *zone-name* 例： `Device(config)# zone security z2`	セキュリティ ゾーンを作成し、セキュリティ ゾーン コンフィギュレーション モードを開始します。
ステップ 6	**exit** 例： `Device(config-sec-zone)# exit`	セキュリティ ゾーン コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードを開始します。
ステップ 7	**zone-pair security** *zone-pair-name* [**source** *source-zone* **destination** *destination-zone*] 例： `Device(config)# zone-pair security in-2-out source z1 destination z2`	ゾーン ペアを作成し、セキュリティ ゾーンペア コンフィギュレーション モードを開始します。
ステップ 8	**service-policy type inspect** *policy-map-name* 例： `Device(config-sec-zone-pair)# service-policy type inspect ipv6-policy`	ポリシー マップをトップレベル ポリシーに関連付けます。
ステップ 9	**exit** 例： `Device(config-sec-zone-pair)# exit`	セキュリティ ゾーンペア コンフィギュレーション モードを終了し、グローバルコンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 10	**interface** *type number* 例： `Device(config)# interface gigabitethernet 0/0/0.1`	サブインターフェイスを設定し、サブインターフェイス コンフィギュレーション モードを開始します。
ステップ 11	**ipv6 address** *ipv6-address/prefix-length* 例： `Device(config-subif)# ipv6 address 2001:DB8:2222:7272::72/64`	IPv6 の一般的なプレフィックスに基づいて IPv6 アドレスを設定し、インターフェイスまたはサブインターフェイスにおける IPv6 処理をイネーブルにします。
ステップ 12	**encapsulation dot1q** *vlan-id* 例： `Device(config-subif)# encapsulation dot1q 2`	インターフェイスで使用するカプセル化方式を設定します。
ステップ 13	**zone-member security** *zone-name* 例： `Device(config-subif)# zone member security z1`	インターフェイスをゾーン メンバーとして設定します。 • *zone-name* 引数の場合、**zone security** コマンドを使用して設定済みのゾーンの 1 つを設定する必要があります。 • インターフェイスがセキュリティ ゾーンにある場合、そのインターフェイスを通るトラフィックはどちらの方向でもすべて（デバイス宛またはデバイス発のトラフィックを除く）はデフォルトでドロップされます。トラフィックがゾーン メンバーであるインターフェイスを通過するには、そのゾーンをポリシーの適用先のゾーン ペアの一部にする必要があります。ポリシーの inspect または pass アクションによってトラフィックが許可される場合は、そのインターフェイスを通じてトラフィックが流れます。
ステップ 14	**end** 例： `Device(config-subif)# end`	サブインターフェイス コンフィギュレーション モードを終了して、特権 EXEC モードを開始します。
ステップ 15	**show policy-map type inspect zone-pair sessions** 例： `Device# show policy-map type inspect zone-pair sessions`	ポリシー マップは指定されたゾーン ペアに適用されるので、作成されたステートフル パケット インスペクション セッションを表示します。 • このコマンドの出力は、IPv4 と IPv6 の両方のファイアウォール セッションを表示します。

例

次に示す **show policy-map type inspect zone-pair sessions** コマンドの出力例は、IPv6 アドレスから IPpv4 アドレスへ（またはその逆）のパケット変換を表示します。

```
Device# show policy-map type inspect zone-pair sessions

  Zone-pair: in-to-out
  Service-policy inspect : in-to-out

    Class-map: ipv6-class (match-any)
      Match: protocol ftp
      Match: protocol tcp
      Match: protocol udp
      Inspect
        Established Sessions
         Session 110D930C [2001:DB8:1::103]:32847=>(209.165.201.2:21) ftp SIS_OPEN
          Created 00:00:00, Last heard 00:00:00
          Bytes sent (initiator:responder) [37:84]

        Half-open Sessions
         Session 110D930C [2001:DB8:1::104]:32848=>(209.165.201.2:21) ftp SIS_OPENING
          Created 00:00:00, Last heard 00:00:00
          Bytes sent (initiator:responder) [0:0]
```

次に示す **show policy-map type inspect zone-pair sessions** コマンドの出力例は、IPv6 アドレスから IPpv6 アドレスへのパケット変換を表示します。

```
Device# show policy-map type inspect zone-pair sessions

  Zone-pair: in-to-out
  Service-policy inspect : in-to-out

    Class-map: ipv6-class (match-any)
      Match: protocol ftp
      Match: protocol tcp
      Match: protocol udp
      Inspect
        Established Sessions
         Session 110D930C [2001:DB8:1::103]:63=>[2001:DB8:2::102]:63 udp SIS_OPEN
          Created 00:00:02, Last heard 00:00:01
          Bytes sent (initiator:responder) [162:0]
```

IPv6 ファイアウォールおよびステートフル NAT64 ポート アドレス変換の設定

次の作業では、ステートフル NAT64 のダイナミック ポート アドレス変換（PAT）を使用した IPv6 ファイアウォールを設定します。

PAT 設定では、複数の IPv6 ホストを、使用可能な IPv4 アドレス プールに先着順でマッピングします。ダイナミック PAT 設定は、IPv4 インターネット接続を提供しながら、少ない IPv4 アドレス空間を節約するのに直接役立ちます。

手順の概要

1. **enable**
2. **configure terminal**
3. **ipv6 unicast-routing**
4. **interface** *type number*
5. **no ip address**
6. **zone-member security** *zone-name*
7. **negotiation auto**
8. **ipv6 address** *ipv6-address/prefix-length*
9. **ipv6 enable**
10. **nat64 enable**
11. **exit**
12. **interface** *type number*
13. **ip address** *ip-address mask*
14. **zone member security** *zone-name*
15. **negotiation auto**
16. **nat64 enable**
17. **exit**
18. **ipv6 access-list** *access-list-name*
19. **permit ipv6 host** *source-ipv6-address* **host** *destination-ipv6-address*
20. **exit**
21. **ipv6 route** *ipv6-prefix/length interface-type interface-number*
22. **ipv6 neighbor** *ipv6-address interface-type interface-number hardware-address*
23. **nat64 v4 pool** *pool-name start-ip-address end-ip-address*
24. **nat64 v6v4 list** *access-list-name* **pool** *pool-name* **overload**
25. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを開始します。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ipv6 unicast-routing** 例： `Device(config)# ipv6 unicast-routing`	IPv6 ユニキャスト データグラムの転送を有効にします。
ステップ 4	**interface** *type number* 例：	インターフェイスを設定し、インターフェイス コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
	`Device(config)# interface gigabitethernet 0/0/0`	
ステップ 5	**no ip address** 例： `Device(config-if)# no ip address`	IP アドレスを削除するか、IP 処理をディセーブルにします。
ステップ 6	**zone-member security** *zone-name* 例： `Device(config-if)# zone member security z1`	インターフェイスをセキュリティ ゾーンにアタッチします。
ステップ 7	**negotiation auto** 例： `Device(config-if)# negotiation auto`	ギガビットイーサネットインターフェイスの速度、デュプレックス、および自動フロー制御を自動ネゴシエーション プロトコルで設定できるようにします。
ステップ 8	**ipv6 address** *ipv6-address/prefix-length* 例： `Device(config-if)# ipv6 address 2001:DB8:1::2/96`	IPv6 の一般的なプレフィックスに基づいて IPv6 アドレスを設定し、インターフェイスにおける IPv6 処理をイネーブルにします。
ステップ 9	**ipv6 enable** 例： `Device(config-if)# ipv6 enable`	明示的な IPv6 アドレスが設定されていないインターフェイスにおける IPv6 処理をイネーブルにします。
ステップ 10	**nat64 enable** 例： `Device(config-if)# nat64 enable`	インターフェイスで NAT64 をイネーブルにします。
ステップ 11	**exit** 例： `Device(config-if)# exit`	インターフェイス コンフィギュレーション モードを終了し、グローバルコンフィギュレーションモードに入ります。
ステップ 12	**interface** *type number* 例： `Device(config)# interface gigabitethernet 0/0/1`	インターフェイスを設定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 13	**ip address** *ip-address mask* 例： `Device(config-if)# ip address 209.165.201.25 255.255.255.0`	インターフェイスに対するプライマリ IP アドレスまたはセカンダリ IP アドレスを設定します。
ステップ 14	**zone member security** *zone-name* 例： `Device(config-if)# zone member security z2`	インターフェイスをセキュリティ ゾーンにアタッチします。

	コマンドまたはアクション	目的
ステップ 15	**negotiation auto** 例： `Device(config-if)# negotiation auto`	ギガビットイーサネットインターフェイスの速度、デュプレックス、および自動フロー制御を自動ネゴシエーション プロトコルで設定できるようにします。
ステップ 16	**nat64 enable** 例： `Device(config-if)# nat64 enable`	インターフェイスで NAT64 をイネーブルにします。
ステップ 17	**exit** 例： `Device(config-if)# exit`	インターフェイス コンフィギュレーション モードを終了し、グローバルコンフィギュレーションモードに入ります。
ステップ 18	**ipv6 access-list** *access-list-name* 例： `Device(config)# ipv6 access-list ipv6-ipv4-pair`	IPv6 アクセスリストを定義し、IPv6 アクセス リスト コンフィギュレーション モードを開始します。
ステップ 19	**permit ipv6 host** *source-ipv6-address* **host** *destination-ipv6-address* 例： `Device(config-ipv6-acl)# permit ipv6 host 2001:DB8:1::2 host 209.165:201.25`	IPv6 アクセス リスト、送信元 IPv6 ホスト アドレス、および宛先 IPv6 ホスト アドレスの許可条件を設定します。
ステップ 20	**exit** 例： `Device(config-ipv6-acl)# exit`	IPv6 アクセス リスト コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードを開始します。
ステップ 21	**ipv6 route** *ipv6-prefix/length interface-type interface-number* 例： `Device(config)# ipv6 route 2001:DB8:1::2/96 gigabitethernet 0/0/0`	スタティック IPv6 ルートを確立します。
ステップ 22	**ipv6 neighbor** *ipv6-address interface-type interface-number hardware-address* 例： `Device(config)# ipv6 neighbor 2001:DB8:1::2/96 gigabitethernet 0/0/0 0000.29f1.4841`	IPv6 ネイバー探索キャッシュのスタティックエントリを設定します。
ステップ 23	**nat64 v4 pool** *pool-name start-ip-address end-ip-address* 例： `Device(config)# nat64 v4 pool pool1 209.165.201.25 209.165.201.125`	ステートフル NAT64 IPv4 アドレス プールを定義します。

	コマンドまたはアクション	目的
ステップ 24	**nat64 v6v4 list** *access-list-name* **pool** *pool-name* **overload** 例： `Device(config)# nat64 v6v4 list nat64-ipv6-any pool pool1 overload`	NAT64 PAT または過負荷アドレス変換をイネーブルにします。
ステップ 25	**end** 例： `Device(config)# end`	グローバル コンフィギュレーション モードを終了し、特権 EXEC モードを開始します。

ゾーンベース ポリシー ファイアウォールの IPv6 サポートの設定例

例：IPv6 ファイアウォールの設定

```
Device# configure terminal
Device(config)# vrf-definition VRF1
Device(config-vrf)# address-family ipv6
Device(config-vrf-af)# exit-address-family
Device(config-vrf)# exit
Device(config)# parameter-map type inspect ipv6-param-map
Device(config-profile)# sessions maximum 10000
Device(config-profile)# exit
Device(config)# ipv6 unicast-routing
Device(config)# ip port-map ftp port 8090 list ipv6-acl
Device(config)# ipv6 access-list ipv6-acl
Device(config-ipv6-acl)# permit ipv6 any any
Device(config-ipv6-acl)# exit
Device(config)# class-map type inspect match-all ipv6-class
Device(config-cmap)# match access-group name ipv6-acl
Device(config-cmap)# match protocol tcp
Device(config-cmap)# exit
Device(config)# policy-map type inspect ipv6-policy
Device(config-pmap)# class type inspect ipv6-class
Device(config-pmap-c)# inspect ipv6-param-map
Device(config-pmap-c)# end
```

例：ゾーンの設定とインターフェイスへのゾーンの適用

```
Device# configure terminal
Device(config)# zone security z1
Device(config-sec-zone)# exit
Device(config)# zone security z2
Device(config-sec-zone)# exit
Device(config)# zone-pair security in-to-out source z1 destination z2
```

```
Device(config-sec-zone-pair)# service-policy type inspect ipv6-policy
Device(config-sec-zone-pair)# exit
Device(config)# interface gigabitethernet 0/0/0.1
Device(config-if)# ipv6 address 2001:DB8:2222:7272::72/64
Device(config-if)# encapsulation dot1q 2
Device(config-if)# zone member security z1
Device(config-if)# end
```

例：IPv6 ファイアウォールとステートフル NAT64 ポート アドレス変換の設定

```
configure terminal
 ipv6 unicast-routing
 interface gigabitethernet 0/0/0
  no ip address
  zone member security z1
  negotiation auto
  ipv6 address 2001:DB8:1::2/96
  ipv6 enable
  nat64 enable
!
 interface gigabitethernet 0/0/1
  ip address 209.165.201.25 255.255.255.0
  zone member security z2
  negotiation auto
  nat64 enable
!
 ipv6 access-list ipv6-ipv4-pair
  permit ipv6 host 2001:DB8:1::2 host 209.165:201.25
!
 ipv6 route 2001:DB8:1::2/96 gigabitethernet 0/0/0
 ipv6 neighbor 2001:DB8:1::2/96 gigabitethernet 0/0/0 0000.29f1.4841
 nat64 v4 pool pool1 209.165.201.25 209.165.201.125
 nat64 v6v4 list nat64-ipv6-any pool pool1 overload
```

ゾーンベース ポリシー ファイアウォールの IPv6 サポートに関する追加情報

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『Master Commands List, All Releases』

関連項目	マニュアル タイトル
セキュリティ コマンド	• 『Security Command Reference: Commands A to C』 • 『Security Command Reference: Commands D to L』 • 『Security Command Reference: Commands M to R』 • 『Security Command Reference: Commands S to Z』
ステートフル NAT64	『Stateful Network Address Translation 64』

標準および RFC

標準/RFC	タイトル
RFC 2460	『*Internet Protocol, Version 6 (IPv6) Specification*』
RFC 2473	『*Generic Packet Tunneling in IPv6 Specification*』

シスコのテクニカル サポート

説明	リンク
右の URL にアクセスして、シスコのテクニカル サポートを最大限に活用してください。これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

ゾーンベース ポリシー ファイアウォールの IPv6 サポートに関する機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだ

けを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *168 :* ゾーンベース ポリシー ファイアウォールの *IPv6* サポートに関する機能情報

機能名	リリース	機能情報
ゾーンベース ポリシー ファイアウォールの IPv6 サポート	Cisco IOS XE リリース 3.6S	ゾーンベース ポリシー ファイアウォールは、IPv6 パケットのインスペクションをサポートします。 次のコマンドが導入または変更されました。**ip port-map** および **show policy-map type inspect zone-pair**。

第 124 章

VRF 対応 Cisco IOS XE ファイアウォール

サービス プロバイダー（SP）または大企業のエッジ ルータで VRF 対応 Cisco IOS XE ファイアウォールが設定されている場合は、Cisco IOS XE ファイアウォール機能が VPN ルーティングおよび転送（VRF）インターフェイスに適用されます。SP は中小企業市場にマネージドサービスを提供しています。

VRF 対応 Cisco IOS XE ファイアウォールは、さまざまなプロトコルの VRF-Lite（別名 Multi-VRF CE）と Application Inspection and Control（AIC）をサポートします。

VRF 対応ファイアウォールは、さまざまなプロトコルの VRF-Lite（別名 Multi-VRF CE）と Application Inspection and Control（AIC）をサポートします。

（注） Cisco IOS XE リリースは、コンテキストベースのアクセス コントロール（CBAC）ファイアウォールをサポートしません。

VRF 対応 Cisco IOS XE ファイアウォールの前提条件

- Cisco IOS XE ファイアウォールについて理解します。
- VRF を設定します。

VRF 対応 Cisco IOS XE ファイアウォールに関する制約事項

- 2 つの VPN ネットワークに重複するアドレスがある場合、VRF 対応ファイアウォールをサポートするには、VRF 対応ネットワーク アドレス変換（NAT）が必要です。NAT は VRF 間ルーティングはサポートしません。VRF 間ルーティング機能向けの VRF 対応ソフトウェア インフラストラクチャ（VASI）を使用できます。
- 複数の VPN に属するクリプトトンネルが単一のインターフェイスで終端する場合、VRF ごとのファイアウォールポリシーを適用できません。
- VASI インターフェイスのサイト間クリプトマップは、次のプラットフォームではサポートされていません。
  - Cisco 1000 シリーズ サービス統合型ルータ
  - Cisco 4000 シリーズ サービス統合型ルータ
  - Cisco 1000v クラウドサービスルータ
- 同じゾーンは、異なる複数の VRF に設定されたインターフェイスに適用できません。

VRF 対応 Cisco IOS XE ファイアウォールについて

VRF 対応 Cisco IOS XE ファイアウォール

VRF 対応ファイアウォールは、VRF 内で送受信される IP パケットを検査します。VRF では、ルーティングテーブルの複数のインスタンスを単一のルータ内で共存させることができます。これにより、VPN の分離が可能になり、IP アドレス空間の独立した重複が実現されます。VRF では、あるサービス プロバイダーの顧客からのトラフィックを他のサービス プロバイダーの顧客から分離することができます。Cisco IOS XE VRF サポートは、インターフェイス、ルーティングテーブル、および転送テーブルの個別のセットで構成されるそれぞれのルーティング ドメインを使って、ルータを複数のルーティング ドメインに分割します。各ルーティング ドメインは、テーブル ID と呼ばれる固有識別子によって参照されます。グローバル ルーティング ドメインとデフォルト ルーティング ドメイン（どの VRF にも関連付けられていない）は 0 のテーブル ID で解決されます。VRF は重複する IP アドレス空間をサポートするため、相互に重なりのない VRF からのトラフィックに同じ IP アドレスを割り当てることができます。

VRF 対応 Cisco IOS XE ファイアウォールは次のようなメリットを提供します。

- スケーラブルな展開：あらゆるネットワークの帯域幅とパフォーマンスの要件を満たすようにスケールします。
- VPN サポート：Cisco IOS XE IPSec とその他のソフトウェアベースのテクノロジー（Layer 2 Tunneling Protocol（L2TP）トンネリングや Quality of Service（QoS）など）に基づく、すべてが揃った VPN ソリューションを提供します。

- AIC サポート：Internet Message Access Protocol（IMAP）、Post Office Protocol 3（POP3）、Simple Mail Transfer Protocol（SMTP）、および Sun リモート プロシージャ コール（SUN RPC）用のポリシー マップを提供します。
- ユーザは VRF 単位でファイアウォールを設定できます。ファイアウォールは、VRF 内で送受信した IP パケットを検査します。また、2 つの異なる VRF（相互に重なりのある VRF）間のトラフィックも検査します。
- SP は、プロバイダー エッジ（PE）ルータにファイアウォールを展開できます。
- 重複する IP アドレス空間をサポートするため、相互に重なりのない VRF のトラフィックが同じ IP アドレスを持つことができます。
- VRF（グローバルではない）ファイアウォール コマンドパラメータとサービス妨害（DoS）パラメータをサポートするため、VRF 対応ファイアウォールは、さまざまな VPN 顧客に割り当てられた複数のインスタンス（VRF インスタンスを含む）として実行できます。
- VRF ID を含む高速ロギング（HSL）メッセージを生成します。ただし、これらのメッセージは 1 つのコレクタによって収集されます。

VRF 対応ファイアウォールを使用すれば、ファイアウォール セッションの数を制限することができます。ファイアウォール セッションが制限されていない場合は、複数の VRF でルータ リソースを共有することが困難になります。これは、1 つの VRF がリソースのほとんどを消費して、他の VRF のリソースが足りなくなることで、他の VRF でサービス妨害（DoS）が発生する可能性があるためです。

（注） Cisco ASR 1000 シリーズ アグリゲーション サービス ルータでは、ファイアウォールが最大 4000 の VRF をサポートします。

アドレス空間の重複

VRF はデバイスを複数のルーティング ドメインに分割します。これらの各ルーティング ドメインには、インターフェイスおよびルーティング テーブルの固有のセットが含まれています。ルーティング テーブルは、VRF ごとの一意のテーブル ID を使用して参照されます。ゼロは、VPN ルーティングおよび転送（VRF）に関連付けられていないデフォルトのグローバル ルーティング テーブル ID です。

交差しない VRF では、重複するアドレス空間を使用できます（つまり、ある VRF の IP アドレスが他の VRF に含まれることがあります）。

VRF

VPN ルーティングおよび転送（VRF）により、ルーティング テーブルの複数のインスタンスが同じデバイス内に共存できます。VRF はプロバイダー エッジ（PE）デバイス内に VRF テーブルのテンプレートを含みます。

通常、アドレスの重複は、カスタマー ネットワークでプライベート IP アドレスを使用していることから発生します。アドレスの重複は、ピアツーピア（P2P）VPN の実装を展開するうえで主要な障害物の 1 つです。重複アドレスの問題を解消するために、マルチプロトコル ラベル スイッチング（MPLS）VPN テクノロジーを使用できます。

各 VPN は、デバイスに独自のルーティングおよびフォワーディング テーブルがあるため、VPN に属するすべてのカスタマーまたはサイトには、そのテーブルに含まれるルートセットに対してのみアクセス権があります。そのため、MPLS VPN ネットワークの PE デバイスには、多数の VPN 別のルーティング テーブルと、サービス プロバイダー（SP）ネットワーク内の他のデバイスに到達するために使用される 1 つのグローバル ルーティング テーブルが含まれます。事実上、数多くの仮想デバイスが単一の物理デバイスに作成されます。

VRF-Lite

MPLS 対応ファイアウォールを使用しない VRF とも呼ばれる VRF-Lite 対応ファイアウォール機能は、ファイアウォール ゾーンを非 MPLS 対応 VPN ルーティングおよび転送（VRF）インターフェイスに適用できるようにします。

VRF-Lite 対応ファイアウォール機能を使用すれば、サービス プロバイダー（SP）は複数の VPN をサポートし、それらの VPN の間で IP アドレスを重複させることが可能です。VRF-lite は、入力インターフェイスを使用して異なる VPN のルートを区別し、1 つまたは複数のレイヤ 3 インターフェイスを各 VRF に関連付けることで仮想パケット転送テーブルを編成します。VRF には、イーサネット ポートなどの物理インターフェイス、または VLAN スイッチ仮想インターフェイス（SVI）などの論理インターフェイスを使用できます。ただし、1 つのレイヤ 3 インターフェイスは同時に複数の VRF に所属できません。

（注） すべての VRF-Lite インターフェイスをレイヤ 3 インターフェイスにする必要があります。

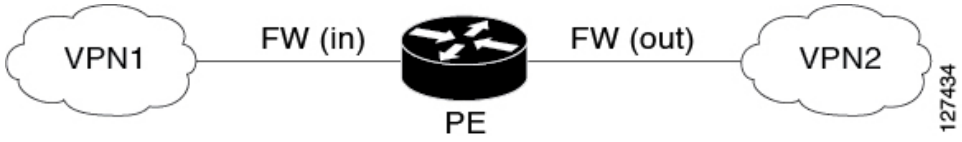
VRF-Lite には、次のデバイスが含まれます。

- カスタマー エッジ（CE）デバイスは、データ リンクによる SP ネットワークへのアクセスを顧客に提供します。CE デバイスは、サイトのローカル ルートをプロバイダー エッジ（PE）デバイスにアドバタイズして、PE デバイスからリモート VPN ルートに関する情報を入手します。
- PE デバイスは、スタティック ルーティングまたはルーティング プロトコル（Border Gateway Protocol（BGP）、Routing Information Protocol バージョン 1（RIPv1）、RIPv2 など）を使用して、CE デバイスとルーティング情報を交換します。
- PE デバイス（またはコア デバイス）は、CE デバイスに接続されていない SP ネットワーク内の任意のデバイスです。
- PE デバイスは、直接接続された VPN に関する VPN ルートのみを維持する必要があるだけで、すべての SP VPN ルートを維持する必要はありません。各 PE デバイスは、直接接続しているサイトごとに VRF を維持します。すべてのサイトが同じ VPN に属している場合は、PE デバイス上の複数のインターフェイスを 1 つの VRF に関連付けることができま

す。各 VPN は、指定された VRF にマッピングされます。CE デバイスからローカル VPN ルートを学習した後、PE デバイスは、内部 BGP（iBGP）を使用して他の PE デバイスと VPN ルーティング情報を交換します。

VRF-Lite を使用すると、複数の顧客が 1 つの CE デバイスを共有できます。その場合は、CE デバイスと PE デバイス間で 1 つの物理リンクのみが使用されます。共有 CE デバイスは、顧客ごとに別々の VRF テーブルを維持し、独自のルーティング テーブルに基づいて、顧客ごとにパケットをスイッチングまたはルーティングします。VRF-Lite は限定された PE デバイスの機能を CE デバイスに拡張して、個別の VRF テーブルを維持する機能を提供し、VPN のプライバシーとセキュリティをブランチ オフィスまで拡張します。

図 *56 : VRF* 間シナリオでのファイアウォール



MPLS VPN

マルチプロトコル ラベル スイッチング（MPLS）VPN 機能を使用すると、サービス プロバイダー（SP）のネットワーク全体で複数のサイトを透過的に相互接続できます。1 つの SP ネットワークで、複数の IP VPN をサポートできます。VPN ユーザから見ると、各 VPN はその他すべてのネットワークとは隔離されたプライベート ネットワークです。1 つの VPN 内では、各拠点は同一 VPN 内のいずれの拠点にも IP パケットを送信できます。

各 VPN は、1 つ以上の VPN ルーティングおよび転送（VRF）インスタンスに関連付けられています。VRF は、1 つの IP ルーティング テーブル、派生した 1 つの Cisco Express Forwarding（CEF）テーブル、およびそのフォワーディング テーブルを使用する一連のインターフェイスで構成されます。

デバイスは、各 VRF に対し別々のルーティングおよび Cisco Express Forwarding テーブルを保持します。これにより、情報が VPN 外に送信されることが回避でき、重複 IP アドレスの問題を起こすことなく同一のサブネットが複数の VPN で使用可能になります。

マルチプロトコル BGP（MP-BGP）を使用しているデバイスは、MP-BGP 拡張コミュニティを使用して VPN のルーティング情報を配布します。

VRF 対応 NAT

ネットワーク アドレス変換（NAT）を使用すると、なんらかの単一のデバイスが、インターネット（またはパブリック ネットワーク）とローカル（またはプライベート）ネットワーク間でエージェントとして機能できます。NAT システムは多様なレベルのセキュリティ機能を提供できますが、主な目的は、アドレス空間を節約することです。

組織が NAT を使用すると、既存のネットワークを持っていてインターネットにアクセスする必要がある場合に、IP アドレスが枯渇する問題を解決できます。ネットワーク インフォメーション センター（NIC）登録 IP アドレスを所有していないサイトは、取得する必要がありま

す。NAT は、何千もの非公開の内部アドレスを取得しやすいアドレスの範囲に動的にマップすることで、NIC 登録 IP アドレスの懸案事項を排除します。

NAT システムは、攻撃者が以下の情報を特定するのを困難にします。

- ネットワーク上で動作しているシステムの数。
- ネットワーク上で動作しているマシンとオペレーティング システムのタイプ。
- ネットワーク トポロジと配置。

NAT とマルチプロトコル ラベル スイッチング（MPLS）VPN の統合により、単一のデバイス上で複数の MPLS VPN を連動するように設定することができます。すべての MPLS VPN で同じ IP アドレス方式が使用されている場合でも、NAT で IP トラフィックを受信する MPLS VPN を区別できます。そのため、複数の MPLS VPN ユーザでサービスを共有しながら、各 MPLS VPN を相互に隔離できます。

インターネット接続、ドメイン ネーム サーバ（DNS）、VoIP サービスなどの付加価値サービスを顧客に提供するには、MPLS サービス プロバイダーが NAT を使用する必要があります。NAT は、MPLS VPN 顧客がネットワーク上で重複した IP アドレスを使用できるようにします。

また、NAT は、カスタマーエッジ（CE）デバイスまたはプロバイダーエッジ（PE）デバイスに実装できます。NAT と MPLS VPN の統合機能により、MPLS クラウド内の PE デバイスへの NAT の実装が可能になります。

VRF 対応 ALG

アプリケーション層ゲートウェイ（ALG）は、アプリケーション パケットのペイロード内の IP アドレス情報を変換するアプリケーションです。ALG は NAT で上書きする必要があるパケット ペイロード内のアドレス情報を特定し、その情報を NAT とファイアウォールに提供してデータが正しく流れるようにするための下位フローまたはドアを作成します（データ フローの一例は FTP データフローです）。ドアは、特定の基準を満たす着信トラフィックを通過させる一時的な構造です。ドアは、完全な NAT セッション エントリを作成するのに十分な情報が得られなかった場合に作成されます。ドアには、送信元と宛先の IP アドレス、および宛先ポートに関する情報が含まれています。ただし、送信元ポートに関する情報は含まれていません。メディア データが到着すると、送信元ポート情報が知らされ、ドアは実際の NAT セッションに昇格します。

VRF 対応 IPSec

VRF 対応 IPsec 機能は、IPsec トンネルを Multiprotocol Label Switching（MPLS）VPN にマップします。VRF 対応 IPsec 機能を使用すれば、単一の公開 IP アドレスを使用して、IPsec トンネルを VPN ルーティングおよび転送（VRF）にマップすることができます。

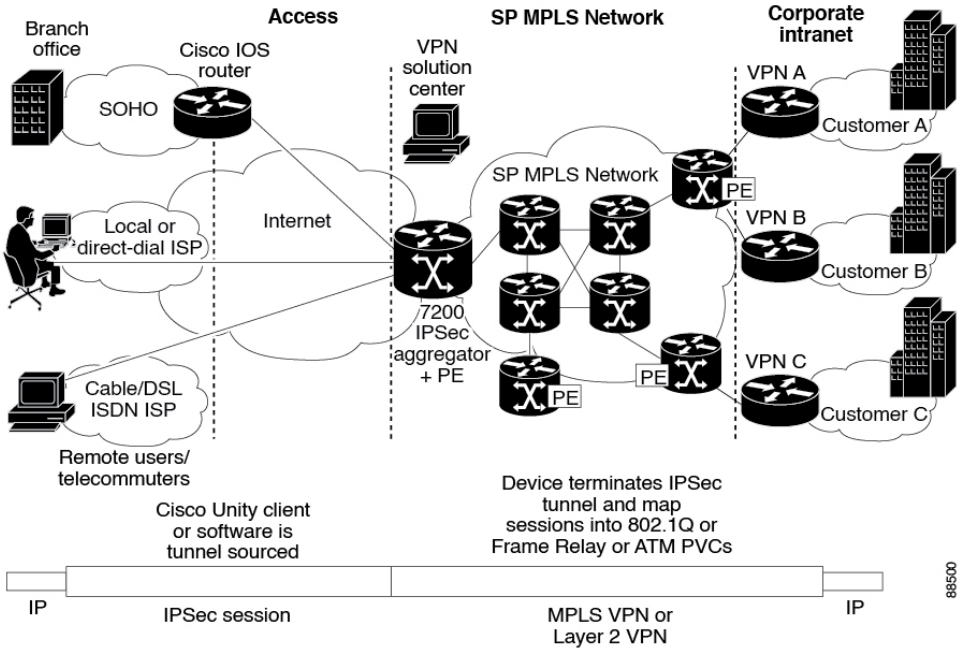
各 IPsec トンネルは、2 つの VRF ドメインに関連付けられます。外部のカプセル化されたパケットは Front Door VRF（FVRF）という VRF ドメインに属します。内部の保護された IP パケットは、Inside VRF（IVRF）というドメインに属します。つまり、IPSec トンネルのローカ

ル エンドポイントは FVRF に属しますが、内部パケットの送信元アドレスと宛先アドレスは IVRF に属すということです。

1 つ以上の IPsec トンネルを、単一のインターフェイス上で終了できます。これらのトンネルのすべての FVRF は同じものであり、そのインターフェイス上で設定されている VRF に設定されます。これらのトンネルの IVRF は異なる可能性があり、クリプト マップ エントリに付加された Security Association and Key Management Protocol（ISAKMP）プロファイル内で定義されている VRF に依存します。

次の図に、IPSec と MPLS VPN およびレイヤ 2 VPN 間のシナリオを示します。

図 *57 : IPsec* と *MPLS VPN* およびレイヤ *2 VPN* 間



VRF 対応ソフトウェア インフラストラクチャ

VRF 対応ソフトウェア インフラストラクチャ（VASI）を使用すれば、2 つの異なる VRF インスタンスを経由するトラフィックにアクセス コントロール リスト（ACL）、NAT、ポリシング、ゾーンベース ファイアウォールなどのサービスを適用することができます。VASI インターフェイスは、ルート プロセッサ（RP）と転送プロセッサ（FP）の冗長性をサポートします。この機能は、VASI インターフェイス上で IPv4 と IPv6 のユニキャスト トラフィックをサポートします。

VASI の主な用途は、VRF のより適切な分離を実現することです。VASI は、共通のインターフェイスを共有している（すべての VRF がインターネット向けの同じインターフェイスを共有している場合など）他の VRF に影響を与えることなく、各 VRF 固有の機能を VASI インターフェイスに適用できるようにします。ファイアウォールでは、この機能により、ゾーンを VASI に適用することができます。

VASI は、仮想インターフェイスのペアを使用して実装されます。ペア内の各インターフェイスが別々の VRF に関連付けられます。VASI 仮想インターフェイスは、この 2 つの VRF 間で切り替える必要があるすべてのパケットのネクスト ホップ インターフェイスです。VASI インターフェイスは、2 つの VRF 間で NAT をサポートする必要があるフレームワークを提供します。

各インターフェイス ペアは、異なる 2 つの VRF インスタンスに関連付けられています。2 つの仮想インターフェイスのペア（vasileft と vasiright）は、論理的にバックツーバックで接続されており、完全な対称性を有しています。各インターフェイスにはインデックスがあります。ペアリングの関連付けは、vasileft が自動的に vasiright にペア化されるように、2 つのインターフェイス インデックスに基づいて自動的に実行されます。BGP、Enhanced Interior Gateway Routing Protocol（EIGRP）、または Open Shortest Path First（OSPF）を使用して、スタティック ルーティングとダイナミック ルーティングのどちらかを設定することができます。BGP ダイナミック ルーティング プロトコルの制約事項とコンフィギュレーションが、VASI インターフェイス間の BGP ルーティング コンフィギュレーションに適用されます。VASI の詳細については、「*VRF* 対応ソフトウェア インフラストラクチャの設定」機能を参照してください。

セキュリティ ゾーン

セキュリティ ゾーンとは、ポリシーを適用できるインターフェイスのグループです。

インターフェイスをゾーンにグループ化するには、次の 2 つの手順を実行します。

- インターフェイスを付加できるようにゾーンを作成します。
- インターフェイスを特定のゾーンのメンバーとなるように設定します。

デフォルトでは、トラフィックは、同じゾーンのメンバーであるインターフェイス間を通ります。

インターフェイスがセキュリティゾーンのメンバーである場合、そのインターフェイスと別のゾーンにあるインターフェイスの間を通るすべてのトラフィック（デバイスに送信されるか、デバイスによって開始されたトラフィックを除く）はデフォルトでドロップされます。ゾーンメンバーインターフェイスおよび別のインターフェイスに対する両方向のトラフィックを許可するには、そのゾーンをゾーンペアの一部にして、そのゾーンペアにポリシーを適用する必要があります。ポリシーが inspect または pass アクションによってトラフィックを許可する場合、トラフィックはインターフェイスを通過できます。

ゾーンを設定するときに考慮する基本的な規則を次に示します。

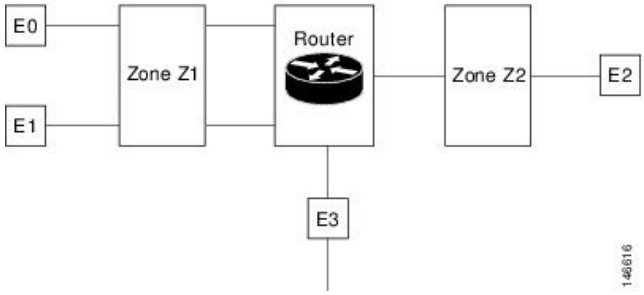
- ゾーンインターフェイスからゾーン外のインターフェイスへのトラフィックまたはゾーン外のインターフェイスからゾーンインターフェイスへのトラフィックは常にドロップされます。ただし、デフォルトゾーンが有効でないことが条件です（デフォルトゾーンはゾーン外のインターフェイスです）。
- 2 つのゾーンインターフェイス間のトラフィックは、各ゾーンにゾーンペアの関係があるかどうか、およびそのゾーンペアにポリシーが設定されているかどうかが検査されます。
- デフォルトでは、同一ゾーン内の 2 つのインターフェイス間のすべてのトラフィックは常に許可されます。

- ゾーン ペアは、ゾーンを送信元ゾーンおよび宛先ゾーンの両方として設定できます。このゾーンペアで検査ポリシーを設定して、2 つのゾーン間のトラフィックを検査、転送、またはドロップできます。
- インターフェイスがメンバーになれるのは、1 つのセキュリティ ゾーンだけです。
- インターフェイスがセキュリティ ゾーンのメンバーの場合、そのゾーンを含むゾーン ペアで明示的なゾーン間ポリシーを設定しない限り、方向に関係なくそのインターフェイスを通過するすべてのトラフィックがブロックされます。
- トラフィックがデバイスのすべてのインターフェイス間を通過するようにするには、これらのインターフェイスが 1 つのセキュリティゾーンまたは別のセキュリティゾーンのメンバーである必要があります。すべてのデバイスインターフェイスがセキュリティゾーンのメンバーである必要はありません。
- ゾーンに関連付けられたすべてのインターフェイスは、同じ仮想ルーティングおよび転送（VRF）に含まれている必要があります。

図 1 には、次のことが示されています。

- インターフェイス E0 と E1 はセキュリティ ゾーン Z1 のメンバーです。
- インターフェイス E2 は、セキュリティ ゾーン Z2 のメンバーです。
- インターフェイス E3 は、どのセキュリティ ゾーンのメンバーでもありません。

図 *58*：セキュリティ ゾーンの制約



- ゾーン ペアとポリシーは、同じゾーンで設定されます。インターフェイス E0 と E1 は同じセキュリティ ゾーン（Z1）のメンバーなので、2 つのインターフェイス間のトラフィックは自由に流れます。
- ポリシーが設定されていない場合、他のインターフェイス間（E0 と E2 の間、E1 と E2 の間、E3 と E1 の間、E3 と E2 の間など）でトラフィックは流れません。
- トラフィックを許可する明示的なポリシーがゾーン Z1 とゾーン Z2 間で設定されている場合だけ、E0 または E1 と E2 間でトラフィックが流れます。
- デフォルトゾーンが有効になっていないかぎり、E3 と E0、E1、または E2 の間でトラフィックは流れません。

（注） Cisco ASR 1000 シリーズ アグリゲーション サービス ルータでは、ファイアウォールは最大 4000 のゾーンをサポートします。

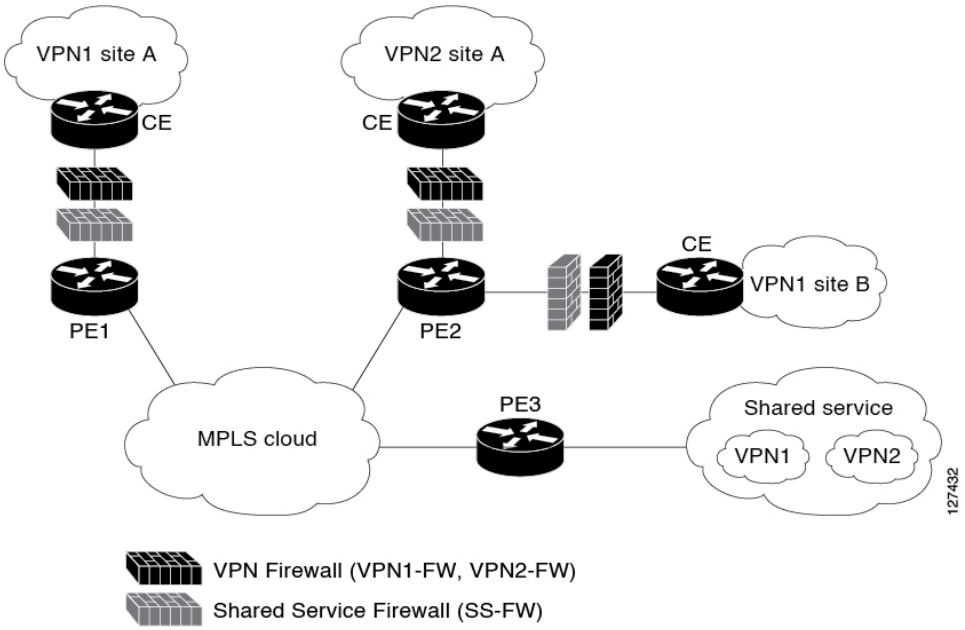
VRF 対応シスコ ファイアウォールの展開

ファイアウォールをネットワーク内の複数のポイントに展開することで、VPN サイトと共有サービス（またはインターネット）を双方向で保護できます。ここでは、次のファイアウォール展開シナリオについて説明します。

VRF 対応のシスコ ファイアウォールを擁する分散ネットワーク

次の図は、サービス プロバイダー（SP）がファイアウォール サービスを VPN カスタマーの VPN1 および VPN2 に提供し、VPN サイトと外部ネットワーク（共有サービスやインターネットなど）を双方向で保護するという一般的な状況について示します。

図 *59 :* 分散ネットワーク



この例では、VPN1 には、マルチプロトコル ラベル スイッチング（MPLS）コア全体を対象とする Site A と Site B という 2 つのサイトがあります。Site A は PE1 に接続され、Site B は PE2 に接続されています。VPN2 には、PE2 に接続している 1 つのサイトのみがあります。各 VPN には、PE3 上の対応する VLAN サブインターフェイスに接続されている共有サービス内の VLAN セグメントがあります。

各 VPN（VPN1 および VPN2）には 2 つのファイアウォール ルールがあります。1 つは VPN サイトを共有サービスから保護するためのもので、もう 1 つは共有サービスを VPN サイトから保護するためのものです。VPN サイトを共有サービスから保護するファイアウォールは VPN ファイアウォールと呼ばれ、共有サービスを VPN サイトから保護するファイアウォールは共

有サービス ファイアウォールと呼ばれます。両方のファイアウォール ルールが、VPN サイトに接続された各入力プロバイダー エッジ（PE）デバイスの VPN ルーティングおよび転送（VRF）インターフェイスに適用されます。VPN ファイアウォール ルールは、VRF インターフェイスが VPN サイトへの入力であるため、入力方向に適用されます。共有サービス ファイアウォール ルールは、VRF インターフェイスが共有サービスへの出力であるため、出力方向に適用されます。

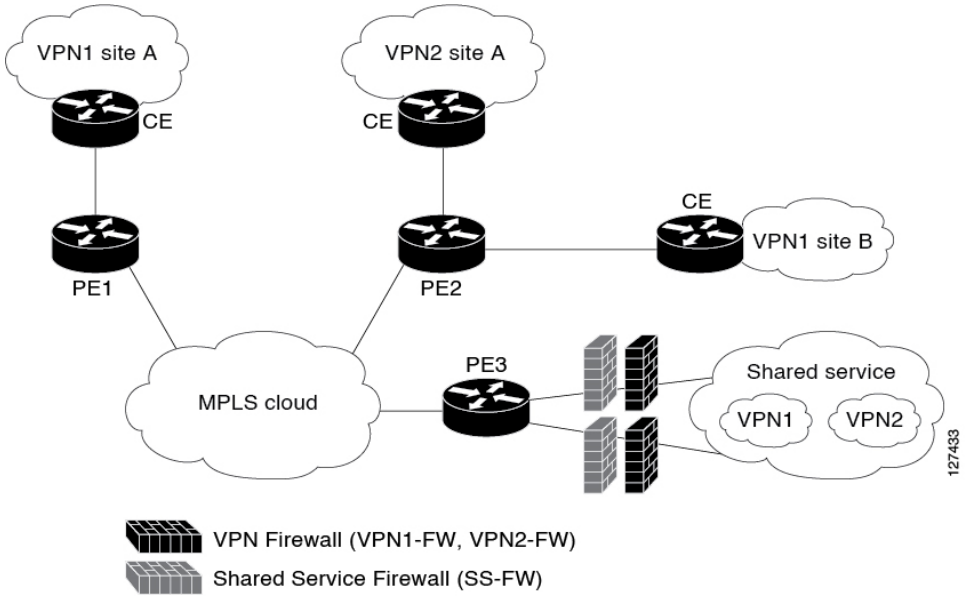
分散ネットワークを使用する利点は次のとおりです。

- ファイアウォールの導入はマルチプロトコル ラベル スイッチング（MPLS）クラウドで分散されるため、ファイアウォールの処理負荷はすべての入力PEデバイスに分散されます。
- 共有サービスは、入力 PE デバイスの VPN サイトから保護されるため、VPN サイトから送信された悪意のあるパケットは、MPLS クラウドに入る前に、入力 PE デバイスでフィルタリングされます。
- VPN ファイアウォール機能はインバウンド方向に導入できます。

VRF 対応のシスコ ファイアウォールを擁するハブアンドスポーク ネットワーク

次の図に、すべての VPN サイトのファイアウォールが、共有サービスに接続されている出力 PE デバイス PE3 に適用されるハブアンドスポーク ネットワークを示します。

図 *60* : ハブアンドスポーク ネットワーク



一般的に、個々の VPN には、共有サービスに接続されている VLAN と VPN ルーティングおよび転送（VRF）サブインターフェイスの両方または一方があります。パケットがマルチプロトコル ラベル スイッチング（MPLS）インターフェイスに到着すると、MPLS はそのパケットを、共有サービスに接続されている対応するサブインターフェイスにルーティングします。各 VPN 上のファイアウォール ポリシーが、対応するサブインターフェイス（VRF インターフェイス）に適用されます（上記の図を参照）。VPNサイトにとってはサブインターフェイスは出

力インターフェイスであるため、VPN ファイアウォール ルールは出力方向で適用されます。共有サービスにとってはサブインターフェイスは入力インターフェイスであるため、共有サービス ファイアウォールは入力方向で適用されます。

ハブアンドスポーク ネットワークの利点は次のとおりです。

- ファイアウォールは出力プロバイダーエッジ（PE）デバイス（PE3）に集中的に導入されるため、ファイアウォールの導入および管理が容易になります。
- 共有サービス ファイアウォール機能は、入力方向で適用できます。
- VPN サイトは出力 PE デバイスで共有サービスから保護されるため、パケットが MPLS クラウドに入る前に、共有サービスからの悪意のあるパケットが PE デバイスでフィルタリングされます。

VRF 対応 Cisco IOS XE ファイアウォールの設定方法

VRF、クラスマップ、およびポリシーマップの定義

手順の概要

1. **enable**
2. **configure terminal**
3. **ip vrf** *vrf-name*
4. **rd** *route-distinguisher*
5. **route-target export** *route-target-ext-community*
6. **route-target import** *route-target-ext-community*
7. **exit**
8. **class-map type inspect match-any** *class-map-name*
9. **match protocol tcp**
10. **match protocol h323**
11. **exit**
12. **policy-map type inspect** *policy-map-name*
13. **class type inspect** *class-map-name*
14. **inspect** [*parameter-map-name*]
15. **exit**
16. **class class-default**
17. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例：	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。

	コマンドまたはアクション	目的
	`Router> enable`	
ステップ 2	**configure terminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ip vrf** *vrf-name* 例： `Router(config)# ip vrf vrf1`	VRFインスタンスを定義し、VRFコンフィギュレーション モードを開始します。
ステップ 4	**rd** *route-distinguisher* 例： `Router(config-vrf)# rd 10:1`	VRFインスタンスのルート識別子（RD）を指定します。
ステップ 5	**route-target export** *route-target-ext-community* 例： `Router(config-vrf)# route-target export 10:1`	VRF インスタンスのルート ターゲット拡張コミュニティを作成し、ターゲットVPN拡張コミュニティへのルーティング情報をエクスポートします。
ステップ 6	**route-target import** *route-target-ext-community* 例： `Router(config-vrf)# route-target import 10:1`	VRF インスタンスのルート ターゲット拡張コミュニティを作成し、ターゲットVPN拡張コミュニティへルーティング情報をインポートします。
ステップ 7	**exit** 例： `Router(config-vrf)# exit`	VRF コンフィギュレーション モードを終了して、グローバル コンフィギュレーション モードを開始します。
ステップ 8	**class-map type inspect match-any** *class-map-name* 例： `Router(config)# class-map type inspect match-any class-map1`	レイヤ 3 およびレイヤ 4（アプリケーション固有）検査タイプ クラスマップを作成し、クラス マップ コンフィギュレーション モードを開始します。
ステップ 9	**match protocol tcp** 例： `Router(config-cmap)# match protocol tcp`	指定されたプロトコルに基づいて、クラス マップの一致基準を設定します。
ステップ 10	**match protocol h323** 例： `Router(config-cmap)# match protocol h323`	指定されたプロトコルに基づいて、クラス マップの一致基準を設定します。
ステップ 11	**exit** 例： `Router(config-cmap)# exit`	クラス マップ コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 12	**policy-map type inspect** *policy-map-name* 例： `Router(config)# policy-map type inspect global-vpn1-pmap`	レイヤ 3 およびレイヤ 4（プロトコル固有）検査タイプ ポリシーマップを作成し、ポリシーマップ コンフィギュレーション モードを開始します。
ステップ 13	**class type inspect** *class-map-name* 例： `Router(config-pmap)# class type inspect class-map1`	アクションを実行する対象のトラフィック（クラス）を指定し、ポリシー マップ クラス コンフィギュレーション モードを開始します。
ステップ 14	**inspect** [*parameter-map-name*] 例： `Router(config-pmap-c)# inspect class-map1`	Cisco IOS XE ステートフル パケット インスペクションをイネーブルにします。
ステップ 15	**exit** 例： `Router(config-pmap-c)# exit`	ポリシー マップ クラス コンフィギュレーション モードを終了し、ポリシーマップ コンフィギュレーション モードを開始します。
ステップ 16	**class class-default** 例： `Router(config-pmap)# class class-default`	ポリシーを設定または変更できるようデフォルト クラスを指定します。 • class-default クラスはデフォルトで定義されます。**class class-default** コマンドを設定して、class-default に関連付けられるデフォルトのドロップ属性を変更します。
ステップ 17	**end** 例： `Router(config-pmap)# end`	ポリシーマップ コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードを開始します。

ゾーンとゾーン ペアの定義

手順の概要

1. **enable**
2. **configure terminal**
3. **zone security** *security-zone-name*
4. **exit**
5. **zone security** *security-zone-name*
6. **exit**
7. **zone-pair security** *zone-pair-name* **source** *source-zone* **destination** *destination-zone*
8. **service-policy type inspect** *policy-map-name*
9. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**zone security** *security-zone-name* 例： `Router(config)# zone security vpn1-zone`	セキュリティ ゾーンを作成し、セキュリティ ゾーン コンフィギュレーション モードを開始します。
ステップ 4	**exit** 例： `Router(config-sec-zone)# exit`	セキュリティ ゾーン コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードを開始します。
ステップ 5	**zone security** *security-zone-name* 例： `Router(config)# zone security global-zone`	セキュリティ ゾーンを作成し、セキュリティ ゾーン コンフィギュレーション モードを開始します。
ステップ 6	**exit** 例： `Router(config-sec-zone)# exit`	セキュリティ ゾーン コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードを開始します。
ステップ 7	**zone-pair security** *zone-pair-name* **source** *source-zone* **destination** *destination-zone* 例： `Router(config)# zone-pair security vpn1-global-zone-pair source vpn1-zone destination global-zone`	ゾーン ペアを作成し、セキュリティ ゾーンペア コンフィギュレーション モードを開始します。 • *zone-pair-name*：インターフェイスに付加されているゾーンの名前。 • **source** *source-zone*：トラフィックの送信元ルータの名前を指定します。 • **destination** *destination-zone*：トラフィックの宛先ルータの名前を指定します。
ステップ 8	**service-policy type inspect** *policy-map-name* 例： `Router(config-sec-zone-pair)# service-policy type inspect global-vpn1-pmap`	レイヤ 7 ポリシー マップをトップレベル ポリシーに関連付けます。
ステップ 9	**end** 例：	ゾーン ペア コンフィギュレーション モードを終了して、特権 EXEC モードを開始します。

	コマンドまたはアクション	目的
	`Router(config-sec-zone-pair)# end`	

インターフェイスへのゾーンの適用とルートの定義

手順の概要

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **ip vrf forwarding** *name*
5. **ip address** *ip-address mask*
6. **zone-member security** *zone-name*
7. **negotiation auto**
8. **exit**
9. **interface** *type number*
10. **ip address** *ip-address mask*
11. **zone-member security** *zone-name*
12. **negotiation auto**
13. **exit**
14. **ip route vrf** *vrf-name destination-ip-address destination-prefix interface-type number* [**global**]
15. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface** *type number* 例： `Router(config)# interface gigabitethernet 0/0/0`	インターフェイスを設定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	**ip vrf forwarding** *name* 例： `Router(config-if)# ip vrf forwarding vrf1`	VRF をインターフェイスまたはサブインターフェイスと関連付けます。

	コマンドまたはアクション	目的
ステップ 5	**ip address** *ip-address mask* 例： `Router(config-if)# ip address 10.1.1.1 255.255.255.0`	インターフェイスに対するプライマリ IP アドレスまたはセカンダリ IP アドレスを設定します。
ステップ 6	**zone-member security** *zone-name* 例： `Router(config-if)# zone-member security vpn1-zone`	インターフェイスをセキュリティ ゾーンにアタッチします。
ステップ 7	**negotiation auto** 例： `Router(config-if)# negotiation auto`	ギガビットイーサネットインターフェイスの速度、デュプレックス、および自動フロー制御を自動ネゴシエーション プロトコルで設定できるようにします。
ステップ 8	**exit** 例： `Router(config-if)# exit`	インターフェイス コンフィギュレーション モードを終了し、グローバルコンフィギュレーションモードに入ります。
ステップ 9	**interface** *type number* 例： `Router(config)# interface gigabitethernet 1/1/1`	インターフェイスを設定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 10	**ip address** *ip-address mask* 例： `Router(config-if)# ip address 10.111.111.111 255.255.255.0`	インターフェイスに対するプライマリ IP アドレスまたはセカンダリ IP アドレスを設定します。
ステップ 11	**zone-member security** *zone-name* 例： `Router(config-if)# zone-member security global-zone`	インターフェイスをセキュリティ ゾーンにアタッチします。
ステップ 12	**negotiation auto** 例： `Router(config-if)# negotiation auto`	ギガビットイーサネットインターフェイスの速度、デュプレックス、および自動フロー制御を自動ネゴシエーション プロトコルで設定できるようにします。
ステップ 13	**exit** 例： `Router(config-if)# exit`	インターフェイス コンフィギュレーション モードを終了し、グローバルコンフィギュレーションモードに入ります。
ステップ 14	**ip route vrf** *vrf-name destination-ip-address destination-prefix interface-type number* [**global**] 例：	VRF インスタンス用のスタティック ルートを確立します。

	コマンドまたはアクション	目的
	`Router(config)# ip route vrf vpn1 10.111.111.0 255.255.255.0 gigabitethernet 1/1/1 global`	
ステップ 15	**end** 例： `Router(config)# end`	グローバル コンフィギュレーション モードを終了し、特権 EXEC モードを開始します。

VRF 対応 Cisco IOS XE ファイアウォールの設定例

例：VRF、クラス マップ、およびポリシー マップの定義

```
Router# configure terminal
Router(config)# ip vrf vrf1
Router(config-vrf)# rd 10:1
Router(config-vrf)# route-target export 10:1
Router(config-vrf)# route-target import 10:1
Router(config-vrf)# exit
Router(config)# class-map type inspect match-any class-map1
Router(config-cmap)# match protocol tcp
Router(config-cmap)# match protocol h323
Router(config-cmap)# exit
Router(config)# policy-map type inspect global-vpn1-pmap
Router(config-pmap)# class type inspect match-acl-111
Router(config-pmap-c)# inspect match-acl-111
Router(config-pmap-c)# exit
Router(config-pmap)# class class-default
Router(config-pmap)# end
```

例：ポリシー マップ、ゾーン、およびゾーン ペアの定義

```
Router# configure terminal
Router(config)# zone security vpn1-zone
Router(config-sec-zone)# exit
Router(config)# zone security global-zone
Router(config-sec-zone)# exit
Router(config)# zone-pair security vpn1-global-zone-pair source vpn1-zone destination
global-zone
Router(config-sec-zone-pair)# service-policy type inspect vpn1-global-pmap
Router(config-sec-zone-pair)# end
```

例：インターフェイスへのゾーンの適用とルートの定義

```
Router# configure terminal
Router(config)# interface gigabitethernet 0/0/0
Router(config-if)# ip vrf forwarding vrf1
Router(config-if)# ip address 10.1.1.1 255.255.255.0
```

```
Router(config-if)# zone-member security vpn1-zone
Router(config-if)# negotiation auto
Router(config-if)# exit
Router(config)# interface gigabitethernet 1/1/1
Router(config-if)# ip address 10.111.111.111 255.255.255.0
Router(config-if)# zone-member security global-zone
Router(config-if)# negotiation auto
Router(config-if)# exit
Router(config)# ip route vrf vpn1 10.111.111.0 255.255.255.0 gigabitethernet 1/1/1 global
Router(config)# end
```

VRF 対応 Cisco IOS XE ファイアウォールに関する追加情報

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『Cisco IOS Master Command List, All Releases』
セキュリティ コマンド	• 『Cisco IOS Security Command Reference Commands A to C』 • 『Cisco IOS Security Command Reference Commands D to L』 • 『Cisco IOS Security Command Reference Commands M to R』 • 『Cisco IOS Security Command Reference Commands S to Z』
NAT	『Configuring Network Address Translation: Getting Started』
MPLS VPN	『*onfiguring a Basic MPLS VPN*』
ゾーンベース ポリシー ファイアウォール	『*Zone-based Policy Firewall*』

シスコのテクニカル サポート

説明	リンク
右の URL にアクセスして、シスコのテクニカル サポートを最大限に活用してください。これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

VRF 対応 Cisco IOS XE ファイアウォールに関する機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *169 : VRF* 対応 *Cisco IOS XE* ファイアウォールに関する機能情報

機能名	リリース	機能情報
VRF 対応 Cisco IOS XE ファイアウォール	Cisco IOS XE リリース 2.5	SP または大企業のエッジルータで VRF 対応 Cisco IOS XE ファイアウォールが設定されている場合は、Cisco IOS XE ファイアウォール機能が VRF インターフェイスに適用されます。
ファイアウォール - VRF 対応 ALG サポート	Cisco IOS XE リリース 2.5	ファイアウォール - VRF 対応 ALG サポート機能を使用すれば、正しい IP アドレス VRF ID ペアが必要な ALG トークンを作成するときに、ALG で、キャッシュされた情報から正しい IP アドレスと VRF ID を抽出することができます。

用語集

C3PL：Cisco Common Classification Policy Language。ポリシー マップとクラス マップを使用してイベント、条件、アクションに基づくトラフィック ポリシーを作成する、構造化された機能固有の設定コマンドです。

EHLO：機能のネゴシエーションを開始するための拡張 HELO 代替コマンド。このコマンドは、ESMTP プロトコルを使用してリモート SMTP サーバに接続する送信者（クライアント）を識別します。

ESMTP：Extended Simple Mail Transfer Protocol（拡張 Simple Mail Transfer Protocol）。送達通知やセッション配信などの追加機能が含まれる、Simple Mail Transfer Protocol（SMTP）の拡張バージョンです。ESMTP は、RFC 1869「SMTP Service Extensions」で定義されています。

HELO：SMTP 機能のネゴシエーションを開始するコマンド。このコマンドは、完全修飾 DNS ホスト名を使用してリモート SMTP サーバに接続する送信者（クライアント）を識別します。

MAIL FROM：電子メールメッセージの開始部分。送信者の電子メールアドレス（および使用されている場合は名前）をメッセージの From: フィールドに示して識別します。

MIME：Multipurpose Internet Mail Extension。電子メールで、テキスト以外のデータ（つまり、プレーン ASCII コードでは表現できないデータ）を転送するための規格。たとえば、バイナリ、外国語テキスト（ロシア語や中国語など）、オーディオ、ビデオなどのデータです。MIME は RFC 2045 で定義されています。

RCPT TO：受信者の電子メールアドレス（および使用されている場合は名前）。単一のメッセージを複数の受信者に配信するようなメッセージでは、複数回繰り返すことができます。

SMTP：Simple Mail Transfer Protocol。電子メール サービスを提供するインターネット プロトコル。

第 125 章

レイヤ2 トランスペアレント ファイアウォール

レイヤ2 トランスペアレント ファイアウォールは、ブリッジされたパケットに対して動作し、ローカル スイッチド イーサネット ポートのペアで有効になります。これらのポート経由で転送される埋め込み IP パケットは、ルーティング ネットワーク内の通常の IP パケットと同様に検査されます。トランスペアレント ファイアウォール設定では、ゾーンベース ファイアウォールまたはレイヤ 3 ファイアウォール設定をレイヤ 2 インターフェイスに適用できます。

このモジュールでは、レイヤ 2 トランスペアレント ファイアウォール機能の概要を紹介します。

レイヤ2 トランスペアレント ファイアウォールのサポートに関する制約事項

- アドレス解決プロトコル（ARP）インスペクションはサポートされていません。
- ブリッジ ドメイン、ブリッジ ドメイン インターフェイス（BDI）、オーバーレイ トランスポート仮想化（OTV）、X-Connect、仮想プライベート LAN サービス（VPLS）、VxLAN、非 IP フローといったレイヤ 2 フォワーディング テクノロジーはサポートされません。
- イーサネット フレームでは、通常の IP または単純な VLAN のみがサポートされています。トランスペアレント ファイアウォールは TCP リセット（RST）パケットを生成し、これらのパケットをサポートされているイーサネット フレームで送信します。

- TCP RST はボックス内高可用性スイッチオーバーの後ではサポートされません。
- 仮想 TCP（vTCP）はサポートされません。
- ネットワーク アドレス変換（NAT）、ボックスツーボックス（B2B）高可用性、マルチプロトコルラベル スイッチング（MPLS）、仮想ルーティングおよび転送（VRF）インスタンス、VRF 対応ソフトウェア インフラストラクチャ（VASI）、Locator-ID Separation Protocol（LISP）はレイヤ 2 スイッチ パスではサポートされません。
- イーサネット運用管理および保守（OAM）、接続障害管理（CFM）といった非 IP パケット フローはサポートされません。
- トランスペアレント ファイアウォール クラス マップでは、レイヤ 2 ベースのアクセス コントロール リスト（ACL）はサポートされません。

レイヤ 2 トランスペアレント ファイアウォールについて

レイヤ 2 トランスペアレント ファイアウォールのサポート

従来のゾーンベース ファイアウォールは、ネットワーク内でレイヤ3 ノードのように機能し、ノードをパス スルーする IP トラフィックを検査します。従来のファイアウォールはルーテッドホップであり、保護されたサブネットのいずれかに接続するホストのデフォルト ゲートウェイとして機能します。ただし、このレイヤ3 ファイアウォールを既存のネットワークに配置するには、ネットワークを再びサブネット化しなければならないため、多くの時間とリソースが必要です。レイヤ2 トランスペアレント ファイアウォールはネットワークに対して透過的であり、セグメント間でレイヤ3 の分離は必要ありません。トランスペアレント ファイアウォールは、「Bump In The Wire」または「ステルス ファイアウォール」のように動作し、接続されたデバイスへのルータ ホップとしては認識されません。トランスペアレント ファイアウォールはルーティング対象のホップではないので、既存のネットワークに容易に導入できます。IP 再アドレッシングは不要です。トランスペアレント ファイアウォールはブリッジされたパケットに対して動作し、レイヤ3 ファイアウォールはルーティングされるパケットに対して動作します。

トランスペアレント ファイアウォールは、ローカル スイッチド イーサネット ポートのペアで有効になります。これらのポート経由で転送される埋め込み IP パケットは、ルーティング ネットワーク内の通常の IP パケットと同様に検査されます。トランスペアレント ファイアウォールが検査するのは IP パケットのみです。

トランスペアレント ファイアウォール セッションは、5 タプル情報（送信元 IP アドレス、宛先 IP アドレス、送信元ポート、宛先ポート、プロトコル）が格納された IP レイヤ 3 およびレイヤ 4 ヘッダーを使用して作成されます。トランスペアレント ファイアウォールはレイヤ 2 プロトコルとしてイーサネットのみをサポートし、IPv4 アドレスと IPv6 アドレスの両方をサポートします。

トランスペアレント ファイアウォール設定では、ゾーンベース ファイアウォールまたはレイヤ 3 ファイアウォール設定をレイヤ 2 インターフェイスに適用できます。レイヤ 3 ファイア

ウォールとレイヤ2トランスペアレントファイアウォールの両方を同じデバイスで共存させることができます。

トランスペアレントファイアウォールでは、次のトポロジでIP（Internet Control Message Protocol（ICMP）、TCP、UDP）インスペクションをサポートします。

- 2 つの GigabitEthernet インターフェイス間。
- GigabitEthernet インターフェイスと GigabitEthernet サブインターフェイス間。
- 2 つの GigabitEthernet サブインターフェイス間。

トランスペアレントファイアウォールは、ポリシーを関連付けずに次のパケットを渡します。

- アドレス解決プロトコル（ARP）
- マルチキャスト パケット：Routing Information Protocol（RIP）、Open Shortest Path First（OSPF）、OSPF バージョン 3（OSPFv3）、Enhanced Interior Gateway Routing Protocol（EIGRP）IPv4 および IPv6 パケット、Intermediate System-to-Intermediate System（ISIS）IPv4 および IPv6 パケット
- Protocol-Independent Multicast（PIM）IPv4 および IPv6 パケット
- Hot Standby Router Protocol（HSRP）、Virtual Router Redundancy Protocol（VRRP）、および Gateway Load Balancing Protocol（GLBP）
- Internet Group Management Protocol（IGMP）およびマルチキャスト リスナー検出（MLD）

レイヤ 2 トランスペアレント ファイアウォールの設定方法

ゾーンベース ファイアウォールと同じ設定を使用してレイヤ 2 トランスペアレント ファイアウォールを設定できます。詳細は、「ゾーンベース ファイアウォール」モジュールを参照してください。

レイヤ 2 トランスペアレント ファイアウォールの設定例

例：レイヤ 2 トランスペアレント ファイアウォールの設定

次に、TCPインスペクションとUDPインスペクションを使用してレイヤ2トランスペアレント ファイアウォールを設定する例を示します。

- クラス マップを定義します。
- ポリシー マップを定義します。

- ゾーンとゾーン ペアを定義します。
- インターフェイス GigabitEthernet 0/0/0 と GigabitEthernet 0/0/1 をファイアウォール ゾーンにアタッチします。
- GigabitEthernet 0/0/0 と GigabitEthernet 0/0/1 を接続することにより、ローカル スイッチングを有効にします。

```
!Class map configuration
Device# configure terminal
Device(config)# class-map typ inspect match-any lan-wan-inspect-tcp
Device(config-cmap)# match protocol tcp
Device(config-cmap)# match protocol udp
Device(config-cmap)# match protocol icmp
Device(config-cmap)# exit
Device(config-cmap)# exit
Device(config)# class-map type inspect match-any wan-lan-inspect-udp
Device(config-cmap)# match protocol tcp
Device(config-cmap)# match protocol udp
Device(config-cmap)# match protocol icmp
Device(config-cmap)# exit

Device(config-cmap)# exit

!Policy map configuration
Device(config)# policy-map type inspect policy-wan-lan
Device(config-pmap)# class type inspect lan-wan-inspect-tcp
Device(config-pmap-c)# inspect
Device(config-pmap-c)# exit
Device(config-pmap)# class class-default
Device(config-pmap)# class type inspect wan-lan-inspect-udp
Device(config-pmap-c)# inspect
Device(config-pmap-c)# exit
Device(config-pmap)# class class-default
Device(config-pmap-c)# exit
Device(config-pmap)# exit

!Zones and zone pair configuration
Device(config)# zone security lan
Device(config-sec-zone)# exit
Device(config)# zone security wan
Device(config-sec-zone)# exit
Device(config)# zone-pair security lan2wan source lan destination wan
Device(config-sec-zone-pair)# service-policy type inspect policy-lan-wan
Device(config-sec-zone-pair)# exit
Device(config)# zone-pair security wan2lan source wan destination lan
Device(config-sec-zone-pair)# service-policy type inspect policy-wan-lan
Device(config-sec-zone-pair)# exit

! Interface configuration
Device(config)# interface gigabitethernet 0/0/0
Device(config-if)# no ip address
Device(config-if)# zone-member security lan
Device(config-if)# exit
Device(config)# interface gigiabitethernet 0/0/1
Device(config-if)# no ip address
Device(config-if)# zone-member security wan
Device(config-if)# exit

!Local switching configuration
Device(config)# connect l2fw-conn gigabitethernet 0/0/0 gigabitethernet 0/0/1
```

```
Device(config)# end
```

レイヤ 2 トランスペアレント ファイアウォールに関する追加情報

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『Cisco IOS Master Command List, All Releases』
セキュリティ コマンド	• 『Cisco IOS Security Command Reference: Commands A to C』 • 『Cisco IOS Security Command Reference: Commands D to L』 • 『Cisco IOS Security Command Reference: Commands M to R』 • 『Cisco IOS Security Command Reference: Commands S to Z』
ゾーンベースのファイアウォール	『*Zone-Based Policy Firewalls*, Configuration Guide』の「Zone-Based Policy Firewalls」モジュール

シスコのテクニカル サポート

説明	リンク
シスコのサポート Web サイトでは、シスコの製品やテクノロジーに関するトラブルシューティングにお役立ていただけるように、マニュアルやツールをはじめとする豊富なオンライン リソースを提供しています。 お使いの製品のセキュリティ情報や技術情報を入手するために、Cisco Notification Service（Field Notice からアクセス）、Cisco Technical Services Newsletter、Really Simple Syndication（RSS）フィードなどの各種サービスに加入できます。 シスコのサポート Web サイトのツールにアクセスする際は、Cisco.com のユーザ ID およびパスワードが必要です。	http://www.cisco.com/support

レイヤ 2 トランスペアレント ファイアウォールに関する機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *170* : レイヤ *2* トランスペアレント ファイアウォールに関する機能情報

機能名	リリース	機能情報
レイヤ2トランスペアレント ファイアウォール	Cisco IOS XE 3.15S	レイヤ 2 トランスペアレント ファイアウォールは、ブリッジされたパケットに対して動作し、ローカル スイッチド イーサネット ポートのペアで有効になります。これらのポート経由で転送される埋め込みIPパケットは、ルーティング ネットワーク内の通常の IP パケットと同様に検査されます。トランスペアレント ファイアウォール設定では、ゾーンベース ファイアウォールまたはレイヤ3ファイアウォール設定をレイヤ 2 インターフェイスに適用できます。 この機能は、Cisco ASR 1000 シリーズ アグリゲーション サービス ルータとシスコ クラウド サービス ルータ 1000V シリーズでサポートされます。 この機能のために導入または変更されたコマンドはありません。

第 126 章

ゾーンベース ポリシー ファイアウォールに対するネストされたクラスマップサポート

ゾーンベース ポリシー ファイアウォールに対するネストされたクラス マップ サポート機能は、Cisco IOS XE ファイアウォールに単一のトラフィック クラスとして複数のトラフィック クラスを設定する機能（ネストされたクラスマップまたは階層型クラスマップとも呼ばれる）を提供します。パケットが複数の一致基準を満たしている場合は、単一のトラフィック ポリシーに関連付けることが可能な複数のクラス マップを設定できます。Cisco IOS XE ファイアウォールは、最大 3 レベルのクラス マップ階層をサポートします。

ゾーンベース ポリシー ファイアウォールに対するネストされたクラス マップ サポートに関する前提条件

ネストされたクラス マップを設定する前に、モジュラ Quality of Service（QoS）CLI（MQC）に精通しておく必要があります。

ゾーンベース ポリシー ファイアウォールに対するネストされたクラス マップ サポートに関する情報

ネストされたクラス マップ

Cisco IOS XE リリース 3.5S 以降のリリースでは、複数のトラフィック クラスを単一のトラフィック クラスとして設定できます（これらのトラフィック クラスは、ネストされたクラス マップまたは階層型クラスマップとも呼ばれます）。パケットが複数の一致基準を満たしている場合は、単一のトラフィック ポリシーに関連付けることが可能な複数のクラス マップを設定できます。クラスマップをネストするには、**match class-map** コマンドを設定します。1 つのトラフィッククラスで match-any 特性と match-all 特性を組み合わせる唯一の方法は、**class-map** コマンドを使用することです。

class-map コマンドの match-all キーワードと match-any キーワード

トラフィッククラスを作成するには、**match-all** および **match-any** キーワードを指定した **class-map** コマンドを設定する必要があります。**match-all** キーワードと **match-any** キーワードの指定が必要になるのは、トラフィッククラスで複数の一致基準を設定する場合だけです。**match-all** および **match-any** キーワードには次のルールが適用されます。

- 指定したトラフィッククラスにパケットを分類するために、そのパケットがトラフィック クラス内のすべての一致基準に一致する必要がある場合、**match-all** キーワードを使用します。
- 指定したトラフィッククラスにパケットを分類するために、そのパケットがトラフィック クラス内のいずれかの一致基準にのみ一致する必要がある場合、**match-any** キーワードを使用します。
- **match-all** キーワードと **match-any** キーワードのどちらも指定しないと、トラフィッククラスは **match-all** キーワードを指定した場合と同じように動作します。

ゾーンベース ポリシー ファイアウォールの設定は、次の条件が満たされる場合にネストされたクラス マップをサポートします。

- 階層の個々のクラスマップで複数の **match class-map** コマンドが参照されている場合。
- 階層の個々のクラスマップに **match class-map** コマンド以外の一致ルールが含まれている場合。

ゾーンベースポリシーファイアウォールに対するネストされたクラス マップ サポートの設定方法

2 レイヤ ネスト クラス マップの設定

手順の概要

1. **enable**
2. **configure terminal**
3. **class-map match-any** *class-map-name*
4. **match protocol** *protocol-name*
5. **exit**
6. **class-map match-any** *class-map-name*
7. **match protocol** *protocol-name*
8. **exit**
9. **class-map match-any** *class-map-name*
10. **match class-map** *class-map-name*
11. **match class-map** *class-map-name*
12. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**class-map match-any** *class-map-name* 例： `Router(config)# class-map match-any child1`	レイヤ 3 またはレイヤ 4 のクラスマップを作成し、クラス マップ コンフィギュレーション モードを開始します。
ステップ 4	**match protocol** *protocol-name* 例： `Router(config-cmap)# match protocol tcp`	指定されたプロトコルを基づくクラス マップの一致基準を設定します。

	コマンドまたはアクション	目的
ステップ 5	**exit** 例： `Router(config-cmap)# exit`	クラス マップ コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードを開始します。
ステップ 6	**class-map match-any** *class-map-name* 例： `Router(config)# class-map match-any child2`	レイヤ 3 またはレイヤ 4 のクラス マップを作成し、クラス マップ コンフィギュレーション モードを開始します。
ステップ 7	**match protocol** *protocol-name* 例： `Router(config-cmap)# match protocol udp`	指定されたプロトコルを基づくクラス マップの一致基準を設定します。
ステップ 8	**exit** 例： `Router(config-cmap)# exit`	クラス マップ コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードを開始します。
ステップ 9	**class-map match-any** *class-map-name* 例： `Router(config)# class-map match-any parent`	レイヤ 3 またはレイヤ 4 のクラス マップを作成し、クラス マップ コンフィギュレーション モードを開始します。
ステップ 10	**match class-map** *class-map-name* 例： `Router(config-cmap)# match class-map child1`	トラフィック クラスを分類ポリシーとして設定します。
ステップ 11	**match class-map** *class-map-name* 例： `Router(config-cmap)# match class-map child2`	トラフィック クラスを分類ポリシーとして設定します。
ステップ 12	**end** 例： `Router(config-cmap)# end`	クラス マップ コンフィギュレーション モードを終了し、特権 EXEC モードを開始します。

ネストされたクラス マップ用のポリシー マップの設定

手順の概要

1. **enable**
2. **configure terminal**
3. **policy-map type inspect** *policy-map-name*
4. **class-type inspect** *class-map-name*
5. **inspect**
6. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**policy-map type inspect** *policy-map-name* 例： `Router(config)# policy-map type inspect pmap`	レイヤ 3 またはレイヤ 4 の検査タイプ ポリシーマップを作成し、ポリシーマップ コンフィギュレーション モードを開始します。
ステップ 4	**class-type inspect** *class-map-name* 例： `Router(config-pmap)# class-type inspect parent`	アクションを実行する対象のトラフィック（クラス）を指定し、ポリシーマップ クラス コンフィギュレーション モードを開始します。
ステップ 5	**inspect** 例： `Router(config-pmap-c)# inspect`	Cisco IOS XE ステートフル パケット インスペクションをイネーブルにします。
ステップ 6	**end** 例： `Router(config-pmap-c)# end`	ポリシーマップ クラス コンフィギュレーション モードを終了し、特権 EXEC モードを開始します。

ゾーン ペアへのポリシー マップのアタッチ

手順の概要

1. **enable**
2. **configure terminal**
3. **zone security** *zone-name*
4. **exit**
5. **zone security** *zone-name*
6. **exit**
7. **zone-pair security** *zone-pair-name* [**source** *zone-name* **destination** [*zone-name*]]
8. **service-policy type inspect** *policy-map-name*
9. **exit**
10. **interface** *type number*
11. **zone-member security** *zone-name*
12. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**zone security** *zone-name* 例： `Router(config)# zone security source-zone`	インターフェイスを割り当てることができるセキュリティ ゾーンを作成し、セキュリティ ゾーン コンフィギュレーション モードを開始します。
ステップ 4	**exit** 例： `Router(config-sec-zone)# exit`	セキュリティ ゾーン コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードを開始します。
ステップ 5	**zone security** *zone-name* 例： `Router(config)# zone security destination-zone`	インターフェイスを割り当てることができるセキュリティ ゾーンを作成し、セキュリティ ゾーン コンフィギュレーション モードを開始します。
ステップ 6	**exit** 例： `Router(config-sec-zone)# exit`	セキュリティ ゾーン コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードを開始します。
ステップ 7	**zone-pair security** *zone-pair-name* [**source** *zone-name* **destination** [*zone-name*]] 例： `Router(config)# zone-pair security secure-zone source source-zone destination destination-zone`	ゾーン ペアを作成し、セキュリティ ゾーンペア コンフィギュレーション モードを開始します。 • ポリシーを適用するには、ゾーン ペアを設定する必要があります。
ステップ 8	**service-policy type inspect** *policy-map-name* 例： `Router(config-sec-zone-pair)# service-policy type inspect pmap`	ファイアウォール ポリシー マップを宛先ゾーン ペアに付加します。 （注） ゾーンのペア間でポリシーが設定されない場合、トラフィックはデフォルトでドロップされます。
ステップ 9	**exit** 例： `Router(config-sec-zone-pair)# exit`	セキュリティ ゾーン ペア コンフィギュレーション モードを終了して、グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 10	**interface** *type number* 例： `Router(config)# interface gigabitethernet 0/0/1`	インターフェイスを設定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 11	**zone-member security** *zone-name* 例： `Router(config-if)# zone-member security source-zone`	インターフェイスを指定したセキュリティ ゾーンに割り当てます。 • インターフェイスをセキュリティ ゾーンのメンバーにした場合、方向に関係なくインターフェイスを通過するすべてのトラフィック（ルータ宛のトラフィックまたはルータ発信のトラフィックを除く）は、デフォルトでドロップされます。トラフィックがインターフェイス通過するには、ゾーンをポリシーの適用先のゾーン ペアの一部にする必要があります。ポリシーがトラフィックを許可すると、トラフィックはそのインターフェイスを通過できます。
ステップ 12	**end** 例： `Router(config-if)# end`	インターフェイス コンフィギュレーション モードを終了し、特権 EXEC モードを開始します。

ゾーンベース ポリシー ファイアウォールに対するネストされたクラス マップ サポートの設定例

例：2 レイヤ ネストされたクラス マップの設定

```
Router# configure terminal
Router(config)# class-map match-any child1
Router(config-cmap)# match protocol tcp
Router(config-cmap)# exit
Router(config)# class-map match-any child2
Router(config-cmap)# match protocol udp
Router(config-cmap)# exit
Router(config)# class-map match-any parent
Router(config-cmap)# match class-map child1
Router(config-cmap)# match class-map child2
Router(config-cmap)# end
```

例：ネストされたクラス マップのポリシー マップの設定

```
Router# configure terminal
Router(config)# policy-map type inspect pmap
Router(config-pmap)# class-type inspect parent
Router(config-pmap-c)# inspect
Router(config-pmap-c)# end
```

例：ゾーン ペアへのポリシー マップのアタッチ

```
Router# configure terminal
Router(config)# zone security source-zone
Router(config-sec-zone)# exit
Router(config)# zone security destination-zone
Router(config-sec-zone)# exit
Router(config)# zone-pair security secure-zone source source-zone destination
destination-zone
Router(config-sec-zone-pair)# service-policy type inspect pmap
Router(config-sec-zone-pair)# exit
Router(config)# interface gigabitethernet 0/0/1
Router(config-if)# zone-member security source-zone
Router(config-if)# end
```

ゾーンベース ポリシー ファイアウォールに対するネストされたクラス マップ サポートに関する追加情報

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『Cisco IOS Master Command List, All Releases』
セキュリティ コマンド	• 『Cisco IOS Security Command Reference: Commands A to C』 • 『Cisco IOS Security Command Reference: Commands D to L』 • 『Cisco IOS Security Command Reference: Commands M to R』 • 『Cisco IOS Security Command Reference: Commands S to Z』
ゾーンベース ポリシー ファイアウォール	『*Zone-Based Policy Firewall*』

シスコのテクニカル サポート

説明	リンク
右の URL にアクセスして、シスコのテクニカル サポートを最大限に活用してください。これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

ゾーンベース ポリシー ファイアウォールに対するネストされたクラス マップ サポートに関する機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *171 :* ゾーンベース ポリシー ファイアウォールに対するネストされたクラス マップ サポートに関する機能情報

機能名	リリース	機能情報
ゾーンベース ポリシー ファイアウォールに対するネストされたクラス マップ サポート	Cisco IOS XE リリース 3.5S	ゾーンベース ポリシー ファイアウォールに対するネストされたクラス マップ サポート機能は、Cisco IOS XE ファイアウォールに単一のトラフィック クラスとして複数のトラフィック クラスを設定する機能（ネストされたクラス マップまたは階層型クラス マップとも呼ばれる）を提供します。パケットが複数の一致基準を満たしている場合は、単一のトラフィック ポリシーに関連付けることが可能な複数のクラス マップを設定できます。

第 127 章

ゾーン不一致処理

ゾーン不一致処理機能を使用すれば、既存のセッションに関連付けられたゾーンペアを検証して、そのゾーンペアと一致するトラフィックをネットワークに転送することができます。セッションに関連付けられたゾーンペアを検証せずにネットワークへのトラフィックの転送を許可すると、セキュリティの脆弱性につながる可能性があります。

このモジュールでは、機能の概要とその設定方法について説明します。

ゾーン不一致処理に関する制約事項

zone-mismatch drop コマンドは、**parameter-map type inspect-vrf** コマンド、**parameter-map type inspect-zone** コマンド、および **parameter-map type inspect global** コマンドの下で設定できません。

ゾーン不一致処理に関する情報

ゾーン不一致処理の概要

ゾーンベース ファイアウォールは、送信元ゾーンから宛先ゾーンに流れるトラフィック用のセッションを作成し、そのトラフィックが宛先ゾーンから送信元ゾーンに戻るときに照合を行います。ゾーンとは、同様の機能を果たすインターフェイスのグループです。ゾーンペアを使用すれば、その一部である 2 つのセキュリティ ゾーン間の単方向ファイアウォール ポリシーを指定することができます。

トラフィックの最初のパケットに対して、ファイアウォールがパケットの入力インターフェイスと出力インターフェイスに関連付けられたゾーンペアをチェックし、パケットを検証してから、検査可能なトラフィック用のセッションを作成します。また、リターン トラフィックが戻ってきたら、ファイアウォールが最初のパケットに基づいてセッション ルックアップを実行し、既存のセッションを検索します。ファイアウォールが一致するセッションを見つけると、トラフィックの通過を許可し、リターン トラフィックに関連付けられたゾーンが既存のセッションに関連付けられたゾーンペアと一致するかどうかをチェックしません。セッションに関連付けられたゾーンペアを検証せずにネットワークへのトラフィックの転送を許可すると、セキュリティの脆弱性につながる可能性があります。

ゾーン不一致処理機能を使用すれば、既存のセッションに関連付けられたゾーンペアを検証して、そのゾーン ペアと一致するトラフィックをネットワークに転送することができます。**zone-mismatch drop** コマンドを設定する場合、ファイアウォールは、既存のセッションと一致するもののパケットが出入りするゾーンとゾーンペアが一致しないすべてのパケット（IPv4 と IPv6）をドロップします。この機能は、ハイ アベイラビリティおよび In-Service Software Upgrade（ISSU）と連動します。

parameter-map type inspect-global コマンドの下で **zone-mismatch drop** コマンドを設定する場合、ゾーン不一致処理の設定がグローバルファイアウォールの設定に適用されます。すべてのゾーン間のトラフィックでゾーン ペア不一致が検査されます。

parameter-map type inspect コマンドの下で **zone-mismatch drop** コマンドを設定することもできます。この場合は、ゾーン不一致処理機能をポリシー単位で適用することができます。

zone-mismatch drop コマンドを設定する場合、その設定は新しいセッションにのみ適用されます。既存のセッションでは、そのセッションが同じゾーンペアに属していなくても、トラフィックはドロップされません。

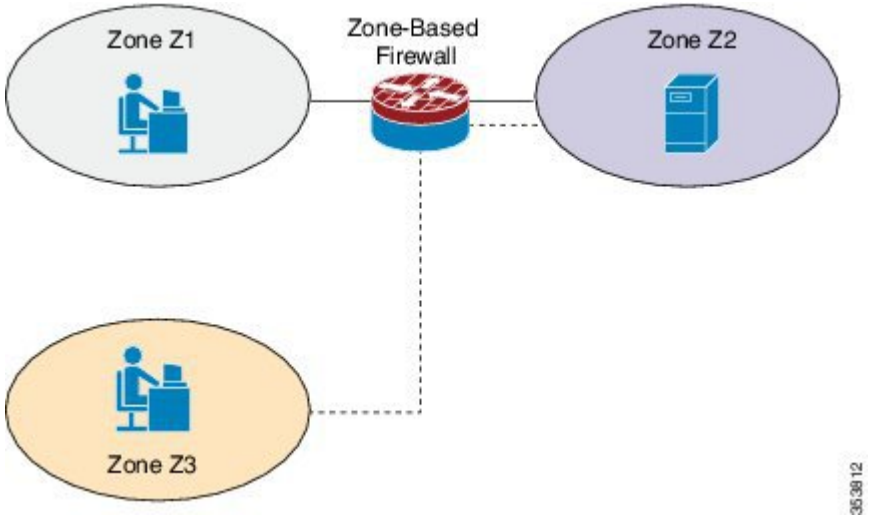
ゾーン不一致処理機能の導入シナリオ

ここでは、ゾーン不一致処理機能が導入される一般的なシナリオについて説明します。

ゾーンベース ファイアウォール アプリケーションによるトラフィック インスペクション

次の図は、ゾーン不一致処理機能が有効な場合のファイアウォールによるトラフィック インスペクションを示します。

図 *61* : ゾーンベース ファイアウォール アプリケーションによるトラフィック インスペクション



ゾーン Z1 と Z2 は同一のゾーンペアに含まれており、このゾーンペアには、**zone-mismatch drop** コマンドが設定されているパラメータマップがあります。ゾーン Z3 はゾーン ペアに含まれていないため、Z3 からのトラフィックは、インターフェイス 1 とインターフェイス 2 の間のファイアウォール セッションに一致する場合でも、ドロップされます。

ゾーン Z3 が追加されたゾーンペアに関連付けられているパラメータマップに対して **zone-mismatch drop** コマンドを設定すると、Z1 と Z2 の間で確立されるセッションに対しては、その設定は反映されません。ただし、**parameter-map type inspect-global** コマンドの下で **zone-mismatch drop** コマンドを設定すると、すべてのゾーン間のトラフィックに対してその設定が適用されます。

ゾーンベース ファイアウォールで設定されたアプリケーション レイヤ ゲートウェイ

一部のアプリケーション レイヤ ゲートウェイ（ALG）はアプリケーション レベル ゲートウェイとも呼ばれ、動作するには複数のコントロールおよびメディア チャネルが必要です。ゾーンベース ファイアウォールでは、制御チャネルおよびメディア チャネルが ALG の同一ゾーンペアに含まれることは義務付けられません。メディアチャネルまたはデータチャネルに対して **zone-mismatch drop** コマンドを設定する場合、この設定が有効になるのは、不明確なセッションから明確なセッションにメディアチャネルまたはデータチャネルが昇格した後です。ゾーンベースファイアウォールは、これらの明確なセッションを通常のセッションと同様にチェックします。不明確なセッションとは、5 タプル情報が含まれていないセッションです。

ゾーン不一致処理の設定方法

ゾーン不一致処理の設定

zone-mismatch drop コマンドは、**parameter-map type inspect-vrf**、**parameter-map type inspect-zone**、および **parameter-map type inspect global** コマンドの下で設定できません。

zone-mismatch drop コマンドを **parameter-map type inspect-global** コマンドの下で設定した場合、ゾーン不一致処理の設定はグローバルファイアウォール設定に適用されます。

手順の概要

1. **enable**
2. **configure terminal**
3. 次のいずれかを実行します。
   - **parameter-map type inspect** *parameter-map-name*
   - **parameter-map type inspect-global**
4. **zone-mismatch drop**
5. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	ユーザ EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。

ステップ 3	次のいずれかを実行します。
	• **parameter-map type inspect** *parameter-map-name*
	• **parameter-map type inspect-global**
	例：
	`Device(config)# parameter-map type inspect pmap1`
	`or`
	`Device(config)# parameter-map type inspect-global`
		接続しきい値、タイムアウト、およびその他の inspect アクションに関連するパラメータの検査タイプ パラメータ マップを設定し、パラメータ マップ タイプ検査コンフィギュレーション モードを開始します。

ステップ 4	**zone-mismatch drop** 例： `Device(config-profile)# zone-mismatch drop`	既存のセッションに接続しているゾーン ペアを検証し、ゾーン ペアに一致するトラフィックをネットワークに対して許可します。着信セッションのゾーン ペアがセッションが到着または離脱するゾーンと一致しない場合、ファイアウォールはこれらのパケットをドロップします。
ステップ 5	**end** 例： `Device(config-profile)# end`	パラメータ マップ タイプ検査コンフィギュレーション モードを終了して、特権 EXEC モードに戻ります。

ゾーン不一致処理の設定例

例：ゾーン不一致処理の設定

次の例では、ゾーン不一致処理機能がパラメータ マップ pmap-fw に対して有効になっています。

```
! Configuring zones
Device(config)# zone security private
Device(config-sec-zone)# exit
Device(config)# zone security public
Device(config-sec-zone)# exit
Device(config)# zone security internet
Device(config-sec-zone)# exit

! Attaching zones to interfaces
Device(config)# interface GigabitEthernet 0/1/5
Device(config-if)# ip address 172.16.1.1 255.255.255.0
Device(config-if)# zone-member security private
Device(config-if)# no shutdown
Device(config-if)# exit
Device(config)# interface GigabitEthernet 0/1/6
Device(config-if)# ip address 209.165.200.226 255.255.255.0
Device(config-if)# zone-member security public
Device(config-if)# no shutdown
Device(config-if)# exit
Device(config)# interface GigabitEthernet 0/1/1
Device(config-if)# ip address 198.51.100.1 255.255.255.0
Device(config-if)# zone-member security internet
Device(config-if)# no shutdown
Device(config-if)# exit

!Configuring the Zone Mismatch Handling feature
Device(config)# parameter-map type inspect pmap-fw
Device(config-profile)# zone-mismatch drop
Device(config-profile)# exit

!Configuring class maps
Device(config)# class-map type inspect match-any internet-traffic-class
Device(config-cmap)# match protocol tcp
Device(config-cmap)# match protocol udp
Device(config-cmap)# match protocol icmp
Device(config-cmap)# exit

! Configuring policy maps and class matching
Device(config)# policy-map type inspect private-internet-policy
Device(config-pmap)# class type inspect internet-traffic-class
Device(config-pmap-c)# inspect pmap-fw
Device(config-pmap-c)# exit
Device(config-pmap)# class class-default
Device(config-pmap-c)# drop
Device(config-pmap-c)# exit
Device(config-pmap)# exit

! Configuring zone pairs
Device(config)# zone-pair security private-internet source private destination internet
Device(config-sec-zone-pair)# service-policy type inspect private-internet-policy
```

```
Device(config-sec-zone-pair)# end
```

ゾーン不一致処理に関する追加情報

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『Cisco IOS Master Command List, All Releases』
セキュリティ コマンド	• 『Cisco IOS Security Command Reference: Commands A to C』 • 『Cisco IOS Security Command Reference: Commands D to L』 • 『Cisco IOS Security Command Reference: Commands M to R』 • 『Cisco IOS Security Command Reference: Commands S to Z』

シスコのテクニカル サポート

説明	リンク
シスコのサポート Web サイトでは、シスコの製品やテクノロジーに関するトラブルシューティングにお役立ていただけるように、マニュアルやツールをはじめとする豊富なオンライン リソースを提供しています。 お使いの製品のセキュリティ情報や技術情報を入手するために、Cisco Notification Service（Field Notice からアクセス）、Cisco Technical Services Newsletter、Really Simple Syndication（RSS）フィードなどの各種サービスに加入できます。 シスコのサポート Web サイトのツールにアクセスする際は、Cisco.com のユーザ ID およびパスワードが必要です。	http://www.cisco.com/support

ゾーン不一致処理に関する機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだ

けを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *172*：ゾーン不一致処理に関する機能情報

機能名	リリース	機能情報
ゾーン不一致処理	Cisco IOS XE 3.15S	ゾーン不一致処理機能を使用すれば、既存のセッションに関連付けられたゾーン ペアを検証して、そのゾーンペアと一致するトラフィックをネットワークに転送することができます。 この機能は、Cisco 4400 シリーズ サービス統合型ルータ、Cisco ASR 1000 シリーズ アグリゲーション サービス ルータ、およびシスコ クラウド サービス ルータ 1000V シリーズでサポートされます。 次のコマンドが導入されました：**zone-mismatch handling**

第 128 章

ファイアウォール ステートフル シャーシ間冗長性の設定

ファイアウォール ステートフル シャーシ間冗長性機能を使用すると、相互にバックアップとして動作するルータのペアを設定できます。この機能を設定し、複数のフェールオーバー条件に基づいてアクティブ ルータを判断できます。フェールオーバーが発生すると、中断なくスタンバイ ルータが引き継ぎ、トラフィック フォワーディング サービスの実行とダイナミック ルーティング テーブルのメンテナンスを開始します。

ファイアウォールステートフルシャーシ間冗長性の前提条件

- ファイアウォールに接続しているインターフェイスは、同じ冗長インターフェイス識別子（RII）を持つ必要があります。
- アクティブ デバイスおよびスタンバイ デバイスは、Cisco IOS XE ゾーンベース ファイアウォールの設定を同じにする必要があります。
- アクティブデバイスとスタンバイ デバイスは、同じバージョンの Cisco IOS XE ソフトウェアで実行する必要があります。アクティブデバイスとスタンバイは、スイッチを介して接続する必要があります。
- 組み込みサービス プロセッサ（ESP）は、アクティブ デバイスとスタンバイ デバイスの両方で一致する必要があります。

ファイアウォールステートフルシャーシ間冗長性に関する制約事項

- LAN および MESH シナリオはサポートされません。
- ボックス間の高可用性（HA）とボックス内の HA の共存はサポートされていないので、シャーシ内にデュアル エンベデッド サービス プロセッサ（ESP）またはデュアル ルート プロセッサ（RP）を持つCisco ASR 1006およびCisco ASR 1013プラットフォームはサポートされていません。

  シャーシ内に単一の ESP と単一の RP を持つ Cisco ASR 1006 および Cisco ASR 1013 プラットフォームは、シャーシ間冗長性をサポートします。
- デュアル IOS デーモン（IOSd）が設定されている場合、デバイスはファイアウォール ステートフル シャーシ間冗長性の設定をサポートしません。

ファイアウォールステートフルシャーシ間冗長性について

ファイアウォール ステートフル シャーシ間冗長性の機能

相互にホット スタンバイとして動作するようにルータのペアを設定できます。この冗長性は、インターフェイスベースで設定します。冗長インターフェイスのペアは、冗長グループと呼ばれます。次の図に、アクティブ/スタンバイ デバイスのシナリオを示します。また、1 つの発信インターフェイスを持つルータのペアについて、冗長グループを設定する方法を示します。アクティブ/アクティブ デバイス シナリオを表現する「冗長グループの設定：*2* つの発信インターフェイス」の図に、2 つの発信インターフェイスを使用するルータのペアに 2 つの冗長グループを設定する方法を示します。

いずれの場合でも、設定可能なコントロール リンクおよびデータ同期リンクによって冗長ルータは参加します。コントロール リンクは、ルータのステータスを通信するために使用されます。データ同期リンクは、ネットワーク アドレス変換（NAT）およびファイアウォールからステートフル情報を転送し、これらのアプリケーションについてステートフルデータベースを同期するために使用されます。

また、いずれの場合でも、冗長インターフェイスのペアは、同じ固有ID番号（RIIと呼ばれます）で設定されます。

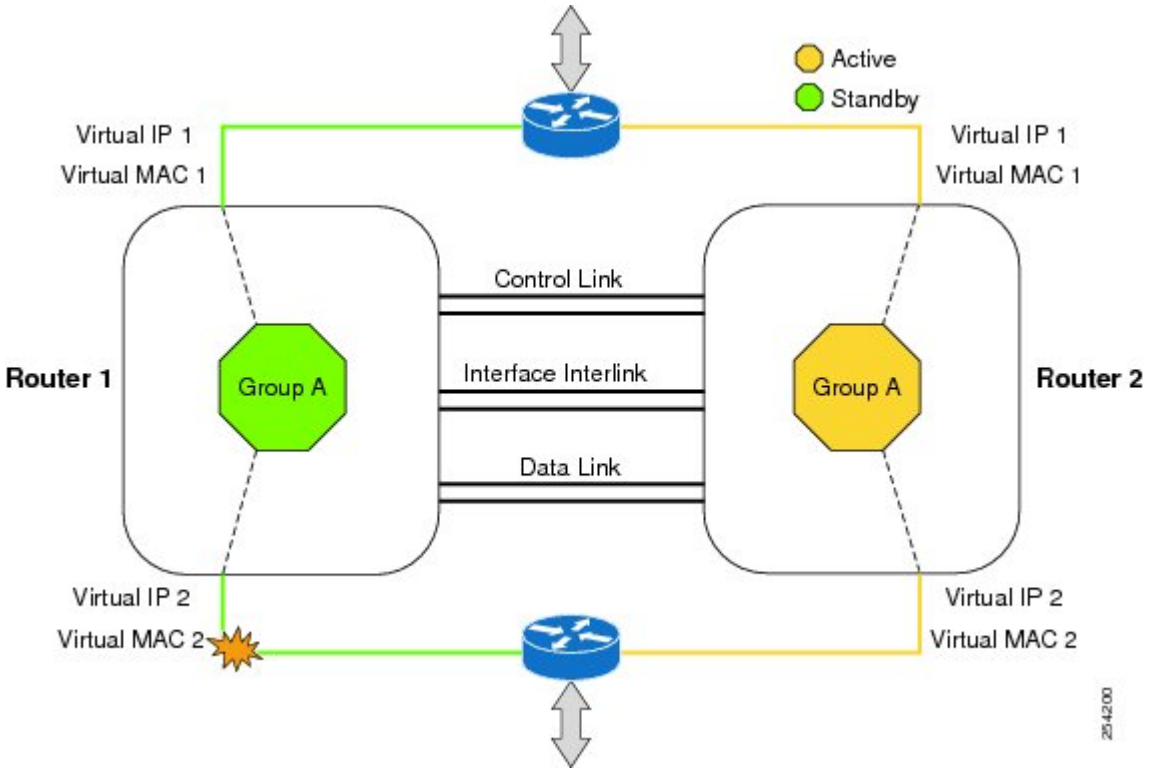
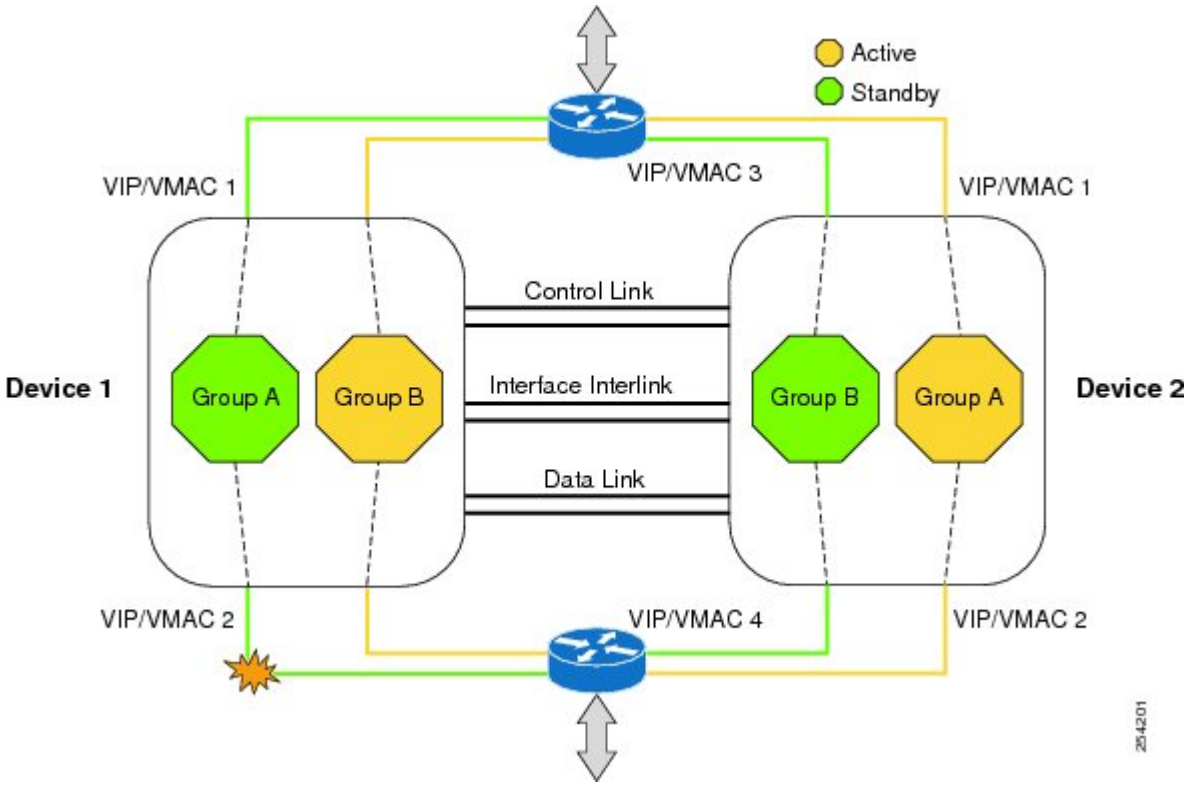


図 *62 :* 冗長グループの設定：*2* つの発信インターフェイス



冗長グループ メンバーのステータスは、コントロール リンクで送信される hello メッセージを使用することで判断できます。設定可能な時間内に、いずれかのルータが hello メッセージに応答しない場合、エラーが発生したと見なされ、スイッチオーバーが開始されます。ミリ秒単位でエラーを検出するには、双方向フォワーディング検出（BFD）プロトコルと統合されたフェールオーバー プロトコルをコントロール リンクで実行します。hello メッセージについて次のパラメータを設定できます。

- Active timer
- Standby timer
- hellotime：hello メッセージが送信される間隔
- holdtime：アクティブまたはスタンバイ ルータをダウン状態と宣言するまでの時間

hellotime は、Hot Standby Router Protocol（HSRP）に合わせてデフォルトで 3 秒に設定されます。holdtime のデフォルトは 10 秒です。これらのタイマーは、**timers hellotime msec** コマンドを使用してミリ秒単位で設定することもできます。

スイッチオーバーの影響を受けるインターフェイスのペアを判断するには、冗長インターフェイスの各ペアについて、固有の ID 番号を設定する必要があります。この ID 番号は RII と呼ばれ、インターフェイスに関連付けられています。

また、スタンバイ ルータに対するスイッチオーバーは、他の条件でも発生する可能性があります。スイッチオーバーが発生する別の要因として、各ルータで設定可能な優先順位設定があります。最も優先度が高いルータがアクティブ ルータになります。アクティブ ルータまたはスタンバイ ルータで障害が発生した場合、重みと呼ばれる設定可能な数値分、ルータの優先度が減らされます。アクティブ ルータの優先度が、スタンバイ ルータの優先度を下回る場合、スイッチオーバーが発生し、スタンバイ ルータがアクティブ ルータになります。このデフォルトの動作を無効にするには、冗長グループについて preemption 属性をディセーブルにします。また、インターフェイスの L1 状態がダウン状態になった場合、各インターフェイスを設定して優先度を減らします。この数は、冗長グループに設定されているデフォルトの値よりも優先されます。

冗長グループの優先度が変更されるエラー イベントごとに、タイム スタンプ、影響を受けた冗長グループ、以前の優先度、新しい優先度、およびエラー イベントの原因の説明を含む syslog エントリが生成されます。

スイッチオーバーが発生する原因となるもう 1 つの状況は、ルータまたはインターフェイスの優先度が、設定可能なしきい値レベルを下回る場合です。

一般的に、スタンバイ ルータへのスイッチオーバーは次の条件で発生します。

- アクティブ ルータで停電またはリロードが発生した場合（クラッシュも含まれます）。
- アクティブ ルータのランタイム優先度が、スタンバイ ルータの優先度を下回った場合。
- アクティブ ルータのランタイム優先度が、設定したしきい値を下回った場合。
- アクティブルータの冗長グループを手動でリロードするには、**redundancy application reload group** *rg-number* コマンドを使用します。

- 任意のモニタ対象インターフェイスで 2 つの連続する hello メッセージに失敗した場合、インターフェイスは強制的にテストモードになります。この問題が発生すると、いずれのユニットもまずインターフェイス上のリンク ステータスを確認してから、次のテストを実行します。
  - ネットワーク アクティビティ テスト
  - ARP テスト
  - ブロードキャスト ping テスト

ファイアウォール ステートフル シャーシ間冗長性機能では、冗長グループのトラフィックは、その冗長グループの入力インターフェイスに関連付けられている仮想 IP アドレスを使用してルーティングされます。仮想 IP アドレスに送信されたトラフィックは、冗長グループがアクティブ状態になっているルータで受信されます。冗長グループのフェールオーバー中は、仮想 IP アドレスへのトラフィックが新しくアクティブになった冗長グループに自動的にルーティングされます。

冗長グループのトラフィックがスタンバイ ルータの物理 IP アドレスを使用してルーティングされてスタンバイ冗長グループに到達した場合、ファイアウォールはスタンバイ冗長グループに到達したトラフィックをドロップします。一方、トラフィックがアクティブ冗長グループに到達した場合は、確立された TCP または UDP セッションがスタンバイ冗長グループに同期されます。

排他的仮想 IP アドレスと排他的仮想 MAC アドレス

仮想 IP（VIP）アドレスと仮想 MAC（VMAC）アドレスは、セキュリティ アプリケーションが、トラフィックを受信するインターフェイスを制御するために使用します。インターフェイスは別のインターフェイスとペアにされ、これらのインターフェイスは同じ冗長グループ（RG）に関連付けられます。アクティブな RG に関連付けられているインターフェイスは、VIP アドレスと VMAC を排他的に所有します。アクティブ デバイスの Address Resolution Protocol（ARP）プロセスによって、VIP への ARP 要求に対する ARP 応答が送信されます。また、インターフェイスのイーサネット コントローラは、VMAC 宛てのパケットを受信するようにプログラミングされます。RG のフェールオーバーが発生すると、VIP と VMAC の所有権は変化します。新しくアクティブになった RG に関連付けられたインターフェイスは、gratuitous ARP を送信し、インターフェイスのイーサネット コントローラをプログラミングして、VMAC 宛てのパケットを受け入れます。

IPv6 のサポート

各冗長グループ（RG）を、同じ冗長インターフェイス識別子（RII）で IPv4 と IPv6 の両方の仮想 IP（VIP）アドレスのトラフィック インターフェイスに割り当てることができます。各 RG は RII ごとに一意の仮想 MAC（VMAC）アドレスを使用します。RG では、IPv6 リンクローカル VIP とグローバル VIP がインターフェイス上に共存します。

トラフィック インターフェイス上の各 RG に対して IPv4 VIP、リンクローカル IPv6 VIP、および/またはグローバル IPv6 VIP を設定できます。IPv6 リンクローカル VIP は、スタティック ルートまたはデフォルト ルートを設定する場合に主に使用されます。IPv6 グローバル VIP は、LAN トポロジと WAN トポロジの両方で広く使用されています。

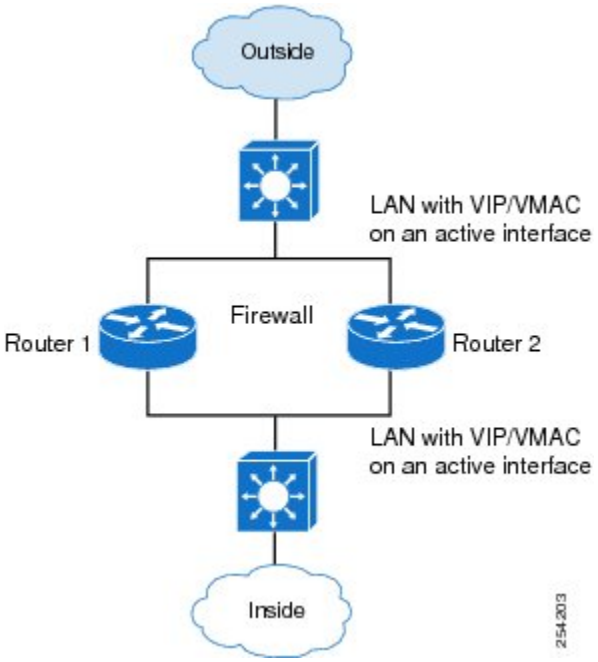
IPv4 VIP を設定する前に、物理 IP アドレスを設定する必要があります。

サポートされるトポロジ

LAN-LAN トポロジは、ファイアウォール ステートフル シャーシ間冗長性アーキテクチャでサポートされます。

LAN/LAN

次の図に、LAN/LAN トポロジを示します。専用のアプリケーションベースのファイアウォール ソリューションを使用するときに、アップストリームまたはダウンストリーム ルータから適切な仮想 IP アドレスへのスタティック ルーティングを設定することで、多くの場合、トラフィックは適切なファイアウォールに送信されます。さらに、Aggregation Services Router（ASR）は、アップストリームまたはダウンストリーム ルータとのダイナミック ルーティングに参加します。LAN 方向のインターフェイスでサポートされるダイナミック ルーティング構成では、ルーティング プロトコルのコンバージェンスへの依存が生じないようにしてください。依存があると、高速フェールオーバー要件に適合しなくなります。



LAN/LAN の設定の詳細については、「例：LAN/LAN の設定」を参照してください。

ゾーンベース ファイアウォールでの VRF 対応シャーシ間冗長性

Cisco IOS XE リリース 3.14S では、ゾーンベース ファイアウォールが VRF 対応シャーシ間冗長性をサポートします。アクティブ デバイスとスタンバイ デバイスの VPN ルーティングおよび転送（VRF）名は同じにする必要があります。アクティブ デバイスとスタンバイ デバイスの両方で同じ VRF 設定を使用できる必要があります。

ゾーンベース ファイアウォールでの VRF 対応シャーシ間冗長性機能では、アクティブ デバイスとスタンバイ デバイス上でボックスツーボックス ハイ アベイラビリティ セッション同期メッセージと一緒に VRF ハッシュ キーを送信する VRF マッピング機能が使用されます。

ファイアウォール ステートフル シャーシ間冗長性の設定方法

冗長アプリケーション グループの設定

手順の概要

1. **enable**
2. **configure terminal**
3. **redundancy**
4. **application redundancy**
5. **group** *id*
6. **name** *group-name*
7. **shutdown**
8. **priority** *value* [**failover threshold** *value*]
9. **preempt**
10. **track** *object-number* {**decrement** *value* | **shutdown**}
11. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**redundancy** 例： `Device(config)# redundancy`	冗長コンフィギュレーションモードを開始します。
ステップ 4	**application redundancy** 例： `Device(config-red)# application redundancy`	冗長アプリケーションコンフィギュレーションモードを開始します。

	コマンドまたはアクション	目的
ステップ 5	**group** *id* 例： `Device(config-red-app)# group 1`	冗長アプリケーション グループ コンフィギュレーション モードを開始します。
ステップ 6	**name** *group-name* 例： `Device(config-red-app-grp)# name group1`	（任意）プロトコル インスタンスに任意のエイリアスを指定します。
ステップ 7	**shutdown** 例： `Device(config-red-app-grp)# shutdown`	（任意）冗長グループを手動でシャットダウンします。
ステップ 8	**priority** *value* [**failover threshold** *value*] 例： `Device(config-red-app-grp)# priority 100 failover threshold 50`	（任意）冗長グループの初期優先度とフェールオーバーしきい値を指定します。
ステップ 9	**preempt** 例： `Device(config-red-app-grp)# preempt`	グループでのプリエンプションをイネーブルにし、優先度とは無関係にスタンバイ デバイスがアクティブ デバイスをプリエンプション処理できるようにします。
ステップ 10	**track** *object-number* {**decrement** *value* | **shutdown**} 例： `Device(config-red-app-grp)# track 200 decrement 200`	冗長グループの優先度を指定します。この値は、イベントが発生した場合に減らされます。
ステップ 11	**end** 例： `Device(config-red-app-grp)# end`	冗長アプリケーション グループ コンフィギュレーション モードを終了して特権 EXEC モードを開始します。

冗長グループ プロトコルの設定

手順の概要

1. **enable**
2. **configure terminal**
3. **redundancy**
4. **application redundancy**
5. **protocol** *id*
6. **name** *group-name*
7. **timers hellotime** {*seconds* | **msec** *milliseconds*} **holdtime** {*seconds* | **msec** *milliseconds*}

8. **authentication** {**text** *string* | **md5 key-string** [**0** | **7**] *key-string* **timeout** *seconds* | **key-chain** *key-chain-name*}
9. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**redundancy** 例： `Device(config)# redundancy`	冗長コンフィギュレーション モードを開始します。
ステップ 4	**application redundancy** 例： `Device(config-red)# application redundancy`	冗長アプリケーション コンフィギュレーション モードを開始します。
ステップ 5	**protocol** *id* 例： `Device(config-red-app)# protocol 1`	コントロールインターフェイスに接続されるプロトコルインスタンスを指定し、冗長アプリケーション プロトコル コンフィギュレーション モードを開始します。
ステップ 6	**name** *group-name* 例： `Device(config-red-app-prtcl)# name prot1`	（任意）名前を使用して冗長グループ（RG）を設定します。
ステップ 7	**timers hellotime** {*seconds* | **msec** *milliseconds*} **holdtime** {*seconds* | **msec** *milliseconds*} 例： `Device(config-red-app-prtcl)# timers hellotime 3 holdtime 9`	hello メッセージが送信される間隔と、デバイスがダウン状態と宣言されるまでの時間を指定します。
ステップ 8	**authentication** {**text** *string* | **md5 key-string** [**0** | **7**] *key-string* **timeout** *seconds* | **key-chain** *key-chain-name*} 例： `Device(config-red-app-prtcl)# authentication md5 key-string 0 n1 timeout 100`	認証情報を指定します。

	コマンドまたはアクション	目的
ステップ 9	**end** 例： `Device(config-red-app-prtcl)# end`	冗長アプリケーションプロトコルコンフィギュレーションモードを終了し、特権EXECモードを開始します。

仮想 IP アドレスおよび冗長インターフェイス識別子の設定

手順の概要

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **redundancy rii** *id*
5. **redundancy group** *id* **ip** *virtual-ip* **exclusive** [**decrement** *value*]
6. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface** *type number* 例： `Device(config)# interface GigabitEthernet 0/1/1`	インターフェイスを設定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	**redundancy rii** *id* 例： `Device(config-if)# redundancy rii 600`	冗長グループ用に冗長インターフェイス識別子（RII）を設定します。 • 有効な範囲は 1 ～ 65535 です。
ステップ 5	**redundancy group** *id* **ip** *virtual-ip* **exclusive** [**decrement** *value*] 例： `Device(config-if)# redundancy group 1 ip 10.10.1.1 exclusive decrement 20`	インターフェイスを冗長グループに関連付け、仮想 IP アドレスをイネーブルにします。

	コマンドまたはアクション	目的
ステップ 6	**end** 例： `Device(config-if)# end`	インターフェイス コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

コントロール インターフェイスおよびデータ インターフェイスの設定

手順の概要

1. **enable**
2. **configure terminal**
3. **redundancy**
4. **application redundancy**
5. **group** *ID*
6. **data** *interface-type interface-number*
7. **control** *interface-type interface-number* **protocol** *id*
8. **timers delay** *seconds* [**reload** *seconds*]
9. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**redundancy** 例： `Device(config)# redundancy`	冗長コンフィギュレーションモードを開始します。
ステップ 4	**application redundancy** 例： `Device(config-red)# application redundancy`	冗長アプリケーションコンフィギュレーションモードを開始します。
ステップ 5	**group** *ID* 例： `Device(config-red-app)# group 1`	冗長アプリケーション グループ コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 6	**data** *interface-type interface-number* 例： `Device(config-red-app-grp)# data GigabitEthernet 0/0/0`	冗長グループに使用されるデータインターフェイスを指定します。
ステップ 7	**control** *interface-type interface-number* **protocol** *id* 例： `Device(config-red-app-grp)# control gigabitethernet 0/0/2 protocol 1`	冗長グループに使用されるコントロール インターフェイスを指定します。 • このインターフェイスは、コントロール インターフェイスプロトコルのインスタンスにも関連付けられます。
ステップ 8	**timers delay** *seconds* [**reload** *seconds*] 例： `Device(config-red-app-grp)# timers delay 100 reload 400`	障害の発生後、またはシステムのリロード後に起動するロールのネゴシエートを遅らせるために、冗長グループが待機する時間を指定します。
ステップ 9	**end** 例： `Device(config-red-app-grp)# end`	冗長アプリケーション グループ コンフィギュレーションモードを終了して特権EXECモードを開始します。

ファイアウォール ステートフル シャーシ間冗長性の管理とモニタリング

ファイアウォール ステートフル シャーシ間冗長性機能を管理およびモニタするには、次のコマンドを使用します。

手順の概要

1. **enable**
2. **debug redundancy application group config** {**all** | **error** | **event** | **func**}
3. **debug redundancy application group faults** {**all** | **error** | **event** | **fault** | **func**}
4. **debug redundancy application group media** {**all** | **error** | **event** | **nbr** | **packet** {**rx** | **tx**} | **timer**}
5. **debug redundancy application group protocol** {**all** | **detail** | **error** | **event** | **media** | **peer**}
6. **debug redundancy application group rii** {**error** | **event**}
7. **debug redundancy application group transport** {**db** | **error** | **event** | **packet** | **timer** | **trace**}
8. **debug redundancy application group vp** {**error** | **event**}
9. **show redundancy application group** [*group-id* | **all**]
10. **show redundancy application transport** {**client** | **group** [*group-id*]}
11. **show redundancy application control-interface group** [*group-id*]
12. **show redundancy application faults group** [*group-id*]
13. **show redundancy application protocol** {*protocol-id* | **group** [*group-id*]
14. **show redundancy application if-mgr group** [*group-id*]

15. **show redundancy application data-interface group** [*group-id*]
16. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**debug redundancy application group config** {**all** | **error** | **event** | **func**} 例： `Device# debug redundancy application group config all`	冗長グループ アプリケーションの設定を表示します。
ステップ 3	**debug redundancy application group faults** {**all** | **error** | **event** | **fault** | **func**} 例： `Device# debug redundancy application group faults error`	冗長グループ アプリケーションの障害を表示します。
ステップ 4	**debug redundancy application group media** {**all** | **error** | **event** | **nbr** | **packet** {**rx** | **tx**} | **timer**} 例： `Device# debug redundancy application group media timer`	冗長グループ アプリケーションのグループ メディア情報を表示します。
ステップ 5	**debug redundancy application group protocol** {**all** | **detail** | **error** | **event** | **media** | **peer**} 例： `Device# debug redundancy application group protocol peer`	冗長グループ アプリケーションのグループ プロトコル情報を表示します。
ステップ 6	**debug redundancy application group rii** {**error** | **event**} 例： `Device# debug redundancy application group rii event`	冗長グループ アプリケーションのグループ RII 情報を表示します。
ステップ 7	**debug redundancy application group transport** {**db** | **error** | **event** | **packet** | **timer** | **trace**} 例：	冗長グループ アプリケーションのグループ トランスポート情報を表示します。

	コマンドまたはアクション	目的
	`Device# debug redundancy application group transport trace`	
ステップ 8	**debug redundancy application group vp** {**error** | **event**} 例： `Device# debug redundancy application group vp event`	冗長グループ アプリケーションのグループ VP 情報を表示します。
ステップ 9	**show redundancy application group** [*group-id* | **all**] 例： `Device# show redundancy application group all`	冗長グループ情報を表示します。
ステップ 10	**show redundancy application transport** {**client** | **group** [*group-id*]} 例： `Device# show redundancy application transport group 1`	冗長グループのトランスポート固有の情報を表示します。
ステップ 11	**show redundancy application control-interface group** [*group-id*] 例： `Device# show redundancy application control-interface group 2`	冗長グループのコントロール インターフェイス情報を表示します。
ステップ 12	**show redundancy application faults group** [*group-id*] 例： `Device# show redundancy application faults group 2`	冗長グループの障害固有の情報を表示します。
ステップ 13	**show redundancy application protocol** {*protocol-id* | **group** [*group-id*] 例： `Device# show redundancy application protocol 3`	冗長グループのプロトコル固有の情報を表示します。
ステップ 14	**show redundancy application if-mgr group** [*group-id*] 例： `Device# show redundancy application if-mgr group 2`	冗長グループのインターフェイス マネージャ情報を表示します。
ステップ 15	**show redundancy application data-interface group** [*group-id*]	データインターフェイス固有の情報を表示します。

	コマンドまたはアクション	目的
	例： `Device# show redundancy application data-interface group 1`	
ステップ 16	**end** 例： `Device# end`	現在のコンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

ファイアウォールステートフルシャーシ間冗長性の設定例

例：冗長アプリケーション グループの設定

次に、優先順位属性とプリエンプション属性のある group1 という名前の冗長グループを設定する例を示します。

```
Device# configure terminal
Device(config)# redundancy
Device(config-red)# application redundancy
Device(config-red-app)# group 1
Device(config-red-app-grp)# name group1
Device(config-red-app-grp)# priority 100 failover-threshold 50
Device(config-red-app-grp)# preempt
Device(config-red-app-grp)# track 200 decrement 200
Device(config-red-app-grp)# end
```

例：冗長グループ プロトコルの設定

次に、hello time メッセージと hold time メッセージ用のタイマーが設定されている冗長グループを設定する例を示します。

```
Device# configure terminal
Device(config)# redundancy
Device(config-red)# application redundancy
Device(config-red-app)# protocol 1
Device(config-red-app-prtcl)# timers hellotime 3 holdtime 9
Device(config-red-app-prtcl)# authentication md5 key-string 0 n1 timeout 100
Device(config-red-app-prtcl)# bfd
Device(config-red-app-prtcl)# end
```

例：仮想 IP アドレスと冗長インターフェイス識別子の設定

次に、ギガビット イーサネット インターフェイス 0/1/1 の冗長グループ仮想 IP アドレスを設定する例を示します。

```
Device# configure terminal
Device(config)# interface GigabitEthernet 0/1/1
Device(conf-if)# redundancy rii 600
Device(config-if)# redundancy group 2 ip 10.2.3.4 exclusive decrement 200
Device(config-if)# end
```

例：コントロール インターフェイスとデータ インターフェイスの設定

```
Device# configure terminal
Device(config-red)# application redundancy
Device(config-red-app-grp)# group 1
Device(config-red-app-grp)# data GigabitEthernet 0/0/0
Device(config-red-app-grp)# control GigabitEthernet 0/0/2 protocol 1
Device(config-red-app-grp)# timers delay 100 reload 400
Device(config-red-app-grp)# end
```

例：LAN-LAN トポロジの設定

次のサンプルLAN-LAN構成で、ステートフルな冗長性を確保するために、2つの発信インターフェイスを備えたルータのペアを設定する方法を示します。この例では、GigabitEthernet 0/1/1が入力インターフェイスで、GigabitEthernet 0/2/1 が出力インターフェイスです。両方のインターフェイスがゾーンに割り当てられ、ゾーン間のトラフィックを記述するためのクラスマップが定義されます。また、冗長性を確保するようにインターフェイスが設定されます。「検査」アクションがアプリケーション レベル ゲートウェイ（ALG）を呼び出して、ピンホールを開き、他のポート上のトラフィックを許可します。ピンホールは、保護されたネットワークへの制御されたアクセスを特定のアプリケーションが取得できるようにするためにALG経由で開かれるポートです。

アクティブ デバイスである Device 1 の設定を以下に示します。

```
! Configures redundancy, control and data interfaces
redundancy
 mode none
 application redundancy
  group 2
   preempt
   priority 200 failover threshold 100
   control GigabitEthernet 0/0/4 protocol 2
   data GigabitEthernet 0/0/3
!
  protocol 2
   timers hellotime ms 250 holdtime ms 750
!
! Configures a VRF
ip vrf vrf1
!
! Configures parameter maps to add parameters that control the behavior of actions and
match criteria.
parameter-map type inspect pmap-udp
 redundancy
  redundancy delay 10
!
parameter-map type inspect pmap-tcp
```

```
 redundancy
  redundancy delay 10
!
! Defines class-maps to describes traffic between zones
class-map type inspect match-any cmap-udp
 match protocol udp
!
class-map type inspect match-any cmap-ftp-tcp
 match protocol ftp
 match protocol tcp
!
! Associates class-maps with policy-maps to define actions to be applied
policy-map type inspect p1
 class type inspect cmap-udp
  inspect pmap-udp
!
 class type inspect cmap-ftp-tcp
  inspect pmap-tcp
!
! Identifies and defines network zones
zone security z-int
!
zone security z-hi
!
! Sets zone pairs for any policy other than deny all and assign policy-maps to zone-pairs
 by defining a service-policy
zone-pair security hi2int source z-hi destination z-int
 service-policy type inspect p1
!
! Assigns interfaces to zones
interface GigabitEthernet 0/0/1
 ip vrf forwarding vrf1
 ip address 10.1.1.3 255.255.0.0
 ip virtual-reassembly
 zone-member security z-hi
 negotiation auto
 redundancy rii 20
 redundancy group 2 ip 10.1.1.10 exclusive decrement 50
!
interface GigabitEthernet 0/0/2
 ip vrf forwarding vrf1
 ip address 192.0.2.2 255.255.255.240
 ip virtual-reassembly
 zone-member security z-int
 negotiation auto
 redundancy rii 21
 redundancy group 2 ip 192.0.2.12 exclusive decrement 50
!
interface GigabitEthernet 0/0/4
 ip address 198.51.100.17 255.255.255.240
!
interface GigabitEthernet 0/0/4
 ip address 203.0.113.49 255.255.255.240
!
ip route vrf vrf1 192.0.2.0 255.255.255.240 GigabitEthernet0/0/2 10.1.1.4
ip route vrf vrf1 10.1.0.0 255.255.0.0 GigabitEthernet0/0/1 10.1.0.4
!
```

スタンバイ デバイスである Device 2 の設定を以下に示します。

```
! Configures redundancy, control and data interfaces
redundancy
 mode none
 application redundancy
  group 2
```

```
   preempt
   priority 200 failover threshold 100
   control GigabitEthernet 0/0/4 protocol 2
   data GigabitEthernet 0/0/3
!
  protocol 2
   timers hellotime ms 250 holdtime ms 750
!
! Configures a VRF
ip vrf vrf1
!
! Configures parameter maps to add parameters that control the behavior of actions and
match criteria.
parameter-map type inspect pmap-udp
 redundancy
  redundancy delay 10
!
parameter-map type inspect pmap-tcp
 redundancy
  redundancy delay 10
!
! Defines class-maps to describes traffic between zones
class-map type inspect match-any cmap-udp
 match protocol udp
!
class-map type inspect match-any cmap-ftp-tcp
 match protocol ftp
 match protocol tcp
!
! Associates class-maps with policy-maps to define actions to be applied
policy-map type inspect p1
 class type inspect cmap-udp
  inspect pmap-udp
!
 class type inspect cmap-ftp-tcp
  inspect pmap-tcp
!
! Identifies and defines network zones
zone security z-int
!
zone security z-hi
!
! Sets zone pairs for any policy other than deny all and assign policy-maps to zone-pairs
 by defining a service-policy
zone-pair security hi2int source z-hi destination z-int
 service-policy type inspect p1
!
! Assigns interfaces to zones
interface GigabitEthernet 0/0/1
 ip vrf forwarding vrf1
 ip address 10.1.1.6 255.255.0.0
 ip virtual-reassembly
 zone-member security z-hi
 negotiation auto
 redundancy rii 20
 redundancy group 2 ip 10.1.1.12 exclusive decrement 50
!
interface GigabitEthernet 0/0/2
 ip vrf forwarding vrf1
 ip address 192.0.2.5 255.255.255.240
 ip virtual-reassembly
 zone-member security z-int
 negotiation auto
 redundancy rii 21
```

```
 redundancy group 2 ip 192.0.2.10 exclusive decrement 50
!
interface GigabitEthernet 0/0/4
 ip address 198.51.100.21 255.255.255.240
!
interface GigabitEthernet 0/0/4
 ip address 203.0.113.53 255.255.255.240
!
ip route vrf vrf1 192.0.2.0 255.255.255.240 GigabitEthernet0/0/2 10.1.1.4
ip route vrf vrf1 10.1.0.0 255.255.0.0 GigabitEthernet0/0/1 10.1.0.4
!
```

ファイアウォール ステートフル シャーシ間冗長性に関する追加情報

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『Master Command List, All Releases』
セキュリティ コマンド	• 『Security Command Reference: Commands A to C』 • 『Security Command Reference: Commands D to L』 • 『Security Command Reference: Commands M to R』 • 『Security Command Reference: Commands S to Z』

シスコのテクニカル サポート

説明	リンク
右の URL にアクセスして、シスコのテクニカル サポートを最大限に活用してください。これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

ファイアウォール ステートフル シャーシ間冗長性に関する機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *173* : ファイアウォール ステートフル シャーシ間冗長性に関する機能情報

機能名	リリース	機能情報
ファイアウォール ステートフル シャーシ間冗長性	Cisco IOS XE リリース 3.1(S)	ファイアウォール ステートフル シャーシ間冗長性機能を使用すれば、デバイスのペアを互いのバックアップとして機能するように設定することができます。 次のコマンドが導入または変更されました。**application redundancy**、**authentication**、**control**、**data**、**debug redundancy application group config**、**debug redundancy application group faults**、**debug redundancy application group media**、**debug redundancy application group protocol**、**debug redundancy application group rii**、**debug redundancy application group transport**、**debug redundancy application group vp**、**group**、**name**、**preempt**、**priority**、**protocol**、**redundancy rii**、**redundancy group**、**track**、**timers delay**、**timers hellotime**、**show redundancy application group**、**show redundancy application transport**、**show redundancy application control-interface**、**show redundancy application faults**、**show redundancy application protocol**、**show redundancy application if-mgr**、**show redundancy application data-interface**。

機能名	リリース	機能情報
ゾーンベース ファイアウォールでの VRF 対応ステートフル シャーシ間冗長性	Cisco IOS XE リリース 3.14S	Cisco IOS XE リリース 3.14S では、ゾーンベース ファイアウォールが VRF 対応シャーシ間冗長性をサポートします。アクティブ デバイスとスタンバイ デバイスの VPN ルーティングおよび転送（VRF）名は同じにする必要があります。アクティブ デバイスとスタンバイ デバイスの両方で同じ VRF 設定を使用できる必要があります。

第 129 章

Cisco CSR1000v ルータに対するファイアウォール ボックスツーボックス ハイ アベイラビリティ サポート

Cisco CSR1000v ルータのファイアウォール ボックスツーボックス ハイ アベイラビリティ サポート機能を使用すると、相互にバックアップとして動作するルータのペアを設定できます。この機能を設定し、複数のフェールオーバー条件に基づいてアクティブ ルータを判断できます。フェールオーバーが発生すると、中断なくスタンバイ ルータが引き継ぎ、トラフィック フォワーディング サービスの実行とダイナミック ルーティング テーブルのメンテナンスを開始します。

Cisco CSR1000v ルータのファイアウォール ボックスツーボックス ハイ アベイラビリティ サポートの前提条件

- ファイアウォールに接続しているインターフェイスは、同じ冗長インターフェイス識別子（RII）を持つ必要があります。

- アクティブ デバイスおよびスタンバイ デバイスは、Cisco IOS XE ゾーンベース ファイアウォールの設定を同じにする必要があります。
- アクティブ デバイスとスタンバイ デバイスは、同じバージョンの Cisco IOS XE ソフトウェアで実行する必要があります。アクティブ デバイスとスタンバイは、スイッチを介して接続する必要があります。

Cisco CSR1000v ルータのファイアウォール ボックスツーボックス ハイ アベイラビリティ サポートに関する制約事項

- デュアル IOS デーモン（IOSd）が設定されている場合、デバイスはファイアウォール ボックスツーボックス ハイ アベイラビリティの設定をサポートしません。

Cisco CSR1000v ルータのファイアウォール ボックスツーボックス高可用性サポートについて

Cisco CSR1000v でのファイアウォール ボックスツーボックス高可用性サポートの機能

相互にホット スタンバイとして動作するようにルータのペアを設定できます。この冗長性は、インターフェイス ベースで設定します。冗長インターフェイスのペアは、冗長グループと呼ばれます。次の図に、アクティブ/スタンバイ デバイスのシナリオを示します。また、1 つの発信インターフェイスを持つルータのペアについて、冗長グループを設定する方法を示します。アクティブ/アクティブ デバイス シナリオを表現する「冗長グループの設定：2 つの発信インターフェイス」の図に、2 つの発信インターフェイスを使用するルータのペアに 2 つの冗長グループを設定する方法を示します。

いずれの場合でも、設定可能なコントロール リンクおよびデータ同期リンクによって冗長ルータは参加します。コントロール リンクは、ルータのステータスを通信するために使用されます。データ同期リンクは、ネットワーク アドレス変換（NAT）およびファイアウォールからステートフル情報を転送し、これらのアプリケーションについてステートフル データベースを同期するために使用されます。

また、いずれの場合でも、冗長インターフェイスのペアは、同じ固有 ID 番号（RII と呼ばれます）で設定されます。

図 *63 :* 冗長グループの設定：*2* つの発信インターフェイス

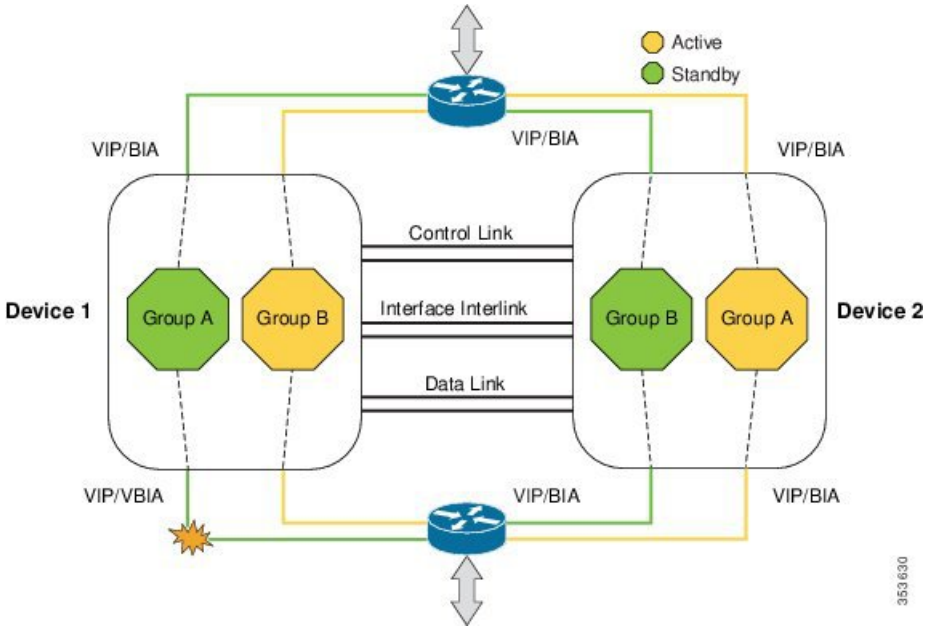
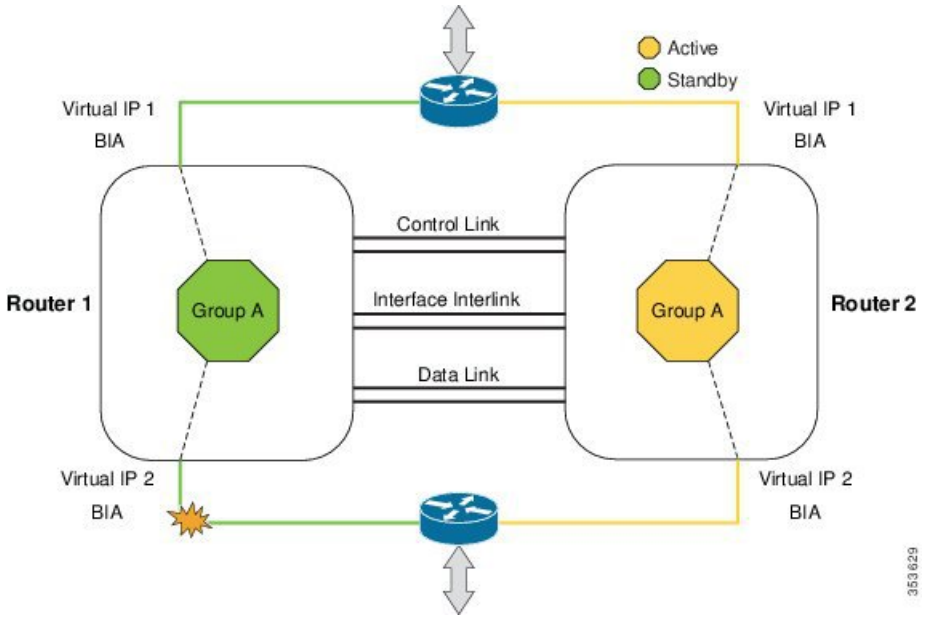
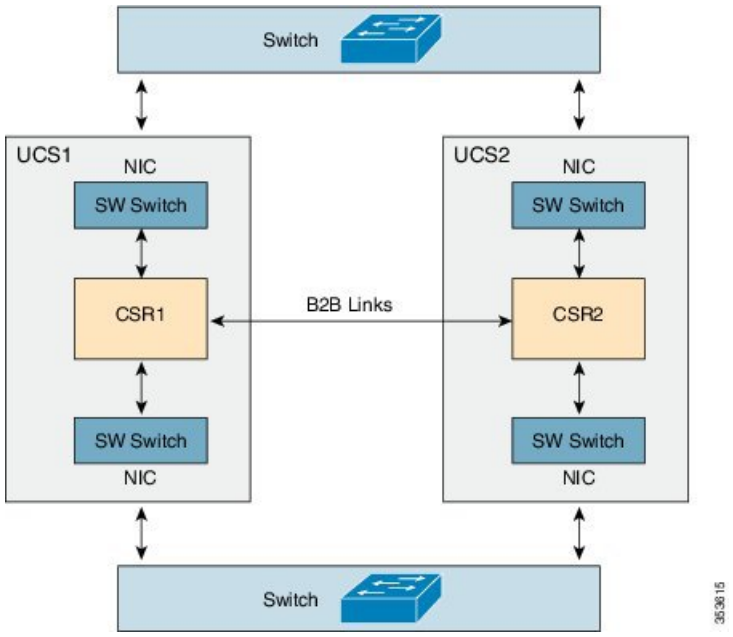


図 *64 :* 冗長グループの設定



以下のシナリオは、Cisco CSR1000v ルータにボックスツーボックス高可用性を導入する例です。

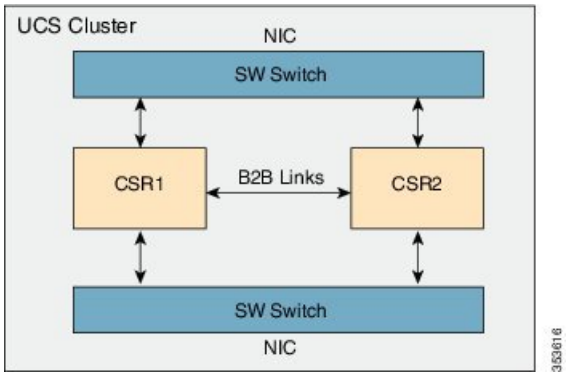
図 *65 : 2* つの独立したサーバでの *CSR1000v* ボックスツーボックス高可用性



この導入では、2 つの冗長 Cisco CSR 1000v ルータがそれぞれ異なる独立した UCS サーバ内にあります。2 つの Cisco Unified Computing System（UCS）サーバは、同じデータセンター内に配置することも、異なる地域の 2 つの異なるデータセンター内に配置することもできます。ボックスツーボックス高可用性データ リンクおよびコントロール リンクには、2 つの別個の物理接続を設定することを推奨します。ただし、2 つの専用物理リンクが使用できない場合は、ボックスツーボックス高可用性データ トラフィックおよびコントロール トラフィックにそれぞれ異なる LAN 拡張接続を経由できます。その場合、遅延の増加を考慮してボックスツーボックス高可用性パラメータ（ハート ビート期間など）を調整する必要があります。

各 Cisco CSR 1000v ルータの LAN インターフェイスは、スイッチ（ESXi L2 SW など）を介して UCS 物理ネットワーク インターフェイス カード（NIC）のインターフェイスと接続します。それぞれの UCS にある 2 つの物理 NIC は外部スイッチに接続されてボックスツーボックス ペアを形成します。Gratuitous Address Resolution Protocol（ARP）は、CSR LAN インターフェイスから送信されて物理スイッチとそのスイッチの組み込みアドレス（BIA）に到達します。

図 *66 :* クラスタ サーバでの *CSR1000v* ボックスツーボックス高可用性



上記の導入例での NAT とゾーンベース ファイアウォール（ZBFW）のボックスツーボックス高可用性は UCS クラスタ構成でも機能します。クラスタ構成の場合、ボックスツーボックス コントロール リンクおよびデータ リンクはクラスタ内の仮想接続を経由します。スイッチ（ESXi L2 SW など）を使用して接続された 2 つの冗長 Cisco CSR 1000v ルータがボックスツーボックス高可用性ペアを形成します。それぞれの Cisco CSR 1000v ルータ上の LAN インターフェイスは SW スイッチに直接接続され、クラスタ UCS の 2 つの物理 NIC は外部ネットワークと通信するために SW スイッチに接続されます。

設定および設定例について詳しくは、「ファイアウォール ステートフル シャーシ間冗長性の設定」モジュールを参照してください。

Cisco CSR1000v ルータのファイアウォール ボックスツーボックス ハイ アベイラビリティ サポートの設定例

例：Cisco CSR1000v ルータのファイアウォール ボックスツーボックス ハイ アベイラビリティの設定

次に、冗長アプリケーション グループ、冗長グループ プロトコル、仮想 IP アドレスと冗長インターフェイス識別子、および制御インターフェイスとデータ インターフェイスを設定する例を示します。

```
!Configures a redundancy application group
Device# configure terminal
Device(config)# redundancy
Device(config-red)# application redundancy
Device(config-red-app)# group 1
Device(config-red-app-grp)# name group1
Device(config-red-app-grp)# priority 100 failover-threshold 50
Device(config-red-app-grp)# preempt
Device(config-red-app-grp)# track 200 decrement 200
Device(config-red-app-grp)# exit

!Configures a redundancy group protocol
Device(config-red-app)# protocol 1
Device(config-red-app-prtcl)# timers hellotime 3 holdtime 9
Device(config-red-app-prtcl)# authentication md5 key-string 0 n1 timeout 100
Device(config-red-app-prtcl)# bfd
Device(config-red-app-prtcl)# end

! Configures a Virtual IP Address and Redundant Interface Identifier
Device# configure terminal
Device(config)# interface GigabitEthernet0/1/1
Device(conf-if)# redundancy rii 600
Device(config-if)# redundancy group 2 ip 10.2.3.4 exclusive decrement 200
Device(config)# redundancy
Device(config-red-app-grp)# data GigabitEthernet0/0/0
Device(config-red-app-grp)# control GigabitEthernet0/0/2 protocol 1
Device(config-red-app-grp)# end
```

```
!Configures control and data interfaces
Device# configure terminal
Device(config-red)# application redundancy
Device(config-red-app-grp)# group 1
Device(config-red-app-grp)# data GigabitEthernet 0/0/0
Device(config-red-app-grp)# control GigabitEthernet 0/0/2 protocol 1
Device(config-red-app-grp)# end
```

Cisco CSR1000v ルータのファイアウォール ボックスツーボックス ハイ アベイラビリティに関する追加情報

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『Master Command List』、すべてのリリース
セキュリティ コマンド	• 『Security Command Reference: Commands A to C』 • 『Security Command Reference: Commands D to L』 • 『Security Command Reference: Commands M to R』 • 『Security Command Reference: Commands S to Z』
ファイアウォール ステートフル シャーシ間冗長性	• 『Configuring Firewall Stateful Interchassis Redundancy』

シスコのテクニカル サポート

説明	リンク
右の URL にアクセスして、シスコのテクニカル サポートを最大限に活用してください。これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

Cisco CSR1000v ルータのファイアウォール ボックスツーボックス ハイ アベイラビリティに関する機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *174*: ファイアウォール ステートフル シャーシ間冗長性に関する機能情報

機能名	リリース	機能情報
Cisco CSR1000v ルータに対するファイアウォール ボックスツーボックス ハイ アベイラビリティ	Cisco IOS XE リリース 3.14S	Cisco CSR1000v ルータに対するファイアウォール ボックスツーボックス ハイ アベイラビリティ機能を使用すれば、Cisco CSR1000v ルータのペアを互いのバックアップとして機能するように設定することができます。

第 130 章

ゾーンベース ファイアウォールと NAT に対するシャーシ間非対称ルーティング サポート

ゾーンベース ファイアウォールおよび NAT のシャーシ間非対称ルーティングサポート機能では、スタンバイ冗長グループからアクティブ冗長グループへのパケット処理のためのパケット転送がサポートされています。この機能が有効になっていない場合は、初期同期（SYN）メッセージを受信しなかったルータに転送されたリターン TCP パケットがドロップされます。これは、パケットが既知のセッションに属していないためです。

このモジュールでは、非対称ルーティングの概要とその設定方法について説明します。

ゾーンベース ファイアウォールと NAT に対するシャーシ間非対称ルーティング サポートに関する制約事項

次の制約事項が、シャーシ間非対称ルーティング サポート機能に適用されます。

- 仮想 IP アドレスと仮想 MAC（VMAC）アドレスを使用する LAN は、非対称ルーティングをサポートしません。
- In Service Software Upgrade（ISSU）はサポートされません。

以下の機能は、VRF 対応非対称ルーティング サポート機能でサポートされません。

- Cisco Trustsec
- エッジ スイッチング サービス
- ヘッダー圧縮
- IPSec
- Policy Based Routing（PBR）
- ポート バンドル
- 合法的傍受
- レイヤ 2 トンネリング プロトコル（L2TP）
- Locator/ID Separation Protocol（LISP）内部パケット インスペクション
- セキュア シェル（SSL）VPN
- セッション ボーダー コントローラ（SBC）

ゾーンベース ファイアウォールと NAT に対するシャーシ間非対称ルーティング サポートに関する情報

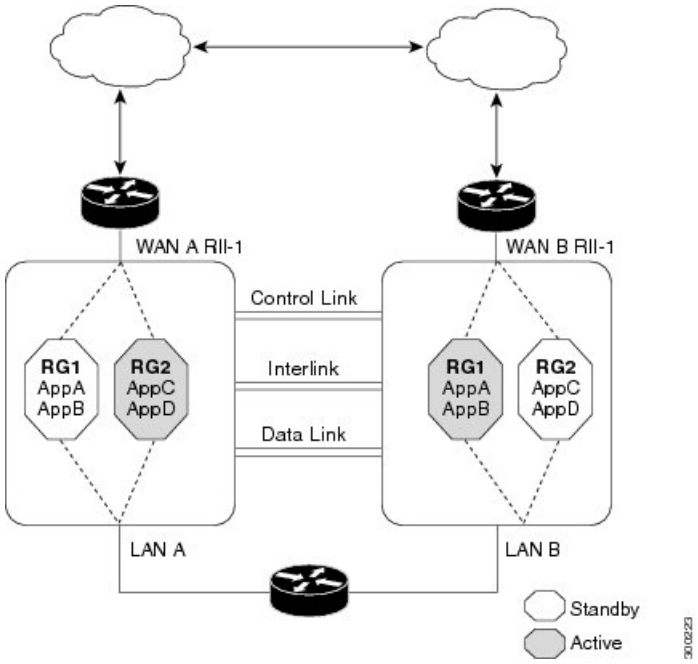
非対称ルーティングの概要

非対称ルーティングは、TCP または UDP 接続の複数のパケットが、異なるルートを経由して異なる方向に送信される場合に発生します。非対称ルーティングでは、1 つの TCP または UDP 接続に属しているパケットは、冗長グループ（RG）の 1 つのインターフェイスを介して転送されますが、同じ RG の別のインターフェイスを介して戻されます。非対称ルーティングでは、パケットフローは同じ RG に残ります。非対称ルーティングを設定する場合、スタンバイ RG で受信したパケットは、処理のためにアクティブ RG にリダイレクトされます。非対称ルーティングが設定されていない場合、スタンバイ RG で受信したパケットはドロップされる可能性があります。

非対称ルーティングは、特定のトラフィックフローの RG を決定します。RG の状態は、パケット処理の決定において重要です。RG がアクティブの場合は、通常のパケットの処理が実行されます。RG がスタンバイ状態で、非対称ルーティングおよび **asymmetric-routing always-divert enable** コマンドを設定している場合、パケットはアクティブ RG に転送されます。スタンバイ RG で受信したパケットをアクティブ RG に常に転送するには、 **asymmetric-routing always-divert enable** コマンドを使用します。

次の図は、別の非対称ルーティング インターリンク インターフェイスを使用して、パケットをアクティブ RG に転送する非対称ルーティング シナリオを示しています。

図 *67* : 非対称ルーティング シナリオ



非対称ルーティングには次のルールが適用されます。

- 冗長インターフェイス識別子（RII）とインターフェイス間のマッピングは 1:1 です。
- インターフェイスと RG 間のマッピングは 1:*n* です。（1 つの非対称ルーティング インターフェイスは複数の RG との間でトラフィックを送受信できます。非対称ルーティング インターフェイス以外のインターフェイス（通常の LAN インターフェイス）では、インターフェイスと RG 間のマッピングは 1:1 です）
- RG およびその RG を使用するアプリケーション間のマッピングは 1:*n* です。（複数のアプリケーションが同じ RG を使用できます）。
- RG とトラフィック フロー間のマッピングは 1:1 です。トラフィック フローは、単一 RG だけにマッピングされる必要があります。トラフィック フローが複数の RG にマッピングされると、エラーが発生します。
- 非対称ルーティング インターリンクに、すべての RG インターリンク トラフィックをサポートできる十分な帯域幅がある限り、RG と非対称ルーティング インターリンク間のマッピングは 1:1 または 1:*n* です。

非対称ルーティングは、転送されるすべてのトラフィックを処理するインターリンク インターフェイスで構成されます。非対称ルーティング インターリンク インターフェイスの帯域幅は、転送が予期されるすべてのトラフィックを処理できるだけの十分な大きさが必要です。IPv4 アドレスは、非対称ルーティング インターリンク インターフェイスで設定され、非対称ルーティング インターフェイスの IP アドレスは、このインターフェイスから到達可能である必要があります。

（注） 非対称ルーティング インターリンク インターフェイスは、インターリンク トラフィックのみに使用し、ハイ アベイラビリティ制御インターフェイスまたはデータ インターフェイスと共有しないことを推奨します。これは、非対称ルーティング インターリンク インターフェイス上のトラフィック量が非常に高くなる可能性があるためです。

ファイアウォールでの非対称ルーティング サポート

ボックス内非対称ルーティングのサポートのために、ファイアウォールは、Internet Control Message Protocol（ICMP）、TCP、およびUDPパケットのステートフル レイヤ3およびレイヤ4インスペクションを行います。ファイアウォールは、パケットのウィンドウサイズと順序を確認して、TCPパケットのステートフル インスペクションを実行します。ファイアウォールでは、ステートフルインスペクションのためにトラフィックの双方向からのステート情報も必要です。ファイアウォールはICMP情報フローの限定的なインスペクションを行います。ICMPエコー要求および応答に関連付けられているシーケンス番号が確認されます。ファイア ウォールでスタンバイ冗長グループ（RG）とパケットフローの同期が行われるのは、そのパケットに対してセッションが確立された後です。確立されるセッションは、TCP、UDPの2番目のパケット、およびICMPの情報メッセージに対するスリーウェイ ハンドシェイクです。すべてのICMP フローはアクティブ RG に送信されます。

ファイアウォールにより、ICMP、TCP、およびUDPプロトコルに属さないパケットについて、ポリシーのステートレス検証が行われます。

ファイアウォールは、双方向トラフィックを使用して、パケットフローがエージングアウトする時期を決定し、すべての検査対象パケット フローをアクティブ RG に転送します。パス ポリシーを持つパケットフローと、ポリシーなしまたはドロップポリシーと同じゾーンが含まれるパケット フローは転送されません。

（注） スタンバイ RG で受信したパケットをアクティブ RG へ転送する **asymmetric-routing always-divert enable** コマンドは、ファイアウォールではサポートされていません。デフォルトでは、ファイアウォールはすべてのパケット フローをアクティブ RG に強制的に転送します。

NAT での非対称ルーティング

デフォルトでは、非対称ルーティングが設定されている場合、ネットワーク アドレス変換（NAT）は非 ALG パケットをアクティブ RG に転送するのではなく、スタンバイ RG で処理します。NAT のみの設定（ファイアウォールが設定されていない場合）では、パケットの処理にアクティブ RG およびスタンバイ RG の両方を使用できます。NAT のみの設定を使用しており、非同期ルーティングを設定している場合、デフォルトの非同期ルーティング ルールは、NAT がスタンバイ RG でパケットを選択的に処理するというルールです。スタンバイ RG で受信したパケットをアクティブ RG へ転送するように **asymmetric-routing always-divert enable** コ

マンドを設定できます。あるいは、NAT と共にファイアウォールを設定している場合は、デフォルトの非同期ルーティング ルールではパケットが常にアクティブ RG に転送されます。

NAT がスタンバイ RG でパケットを受信したときに、パケットの転送が設定されていない場合、NAT は検索を実行してそのパケットのセッションが存在するかどうかを確認します。セッションが存在しており、そのセッションに関連付けられた ALG がない場合、NAT はスタンバイ RG でパケットを処理します。セッションが存在している場合にスタンバイ RG でパケットを処理すると、NAT トラフィックの帯域幅が大幅に増加します。

NAT ではペイロードの特定と変換、および子フローの作成に ALG が使用されます。ALG が適切に機能するには、双方向トラフィックが必要です。NAT は、ALG に関連付けられているすべてのパケット フローのトラフィックをアクティブ RG に転送する必要があります。このため、セッションに関連付けられている ALG データがスタンバイ RG で検出されたかどうかを確認します。ALG データが存在している場合、非対称ルーティングのためにパケットが転送されます。

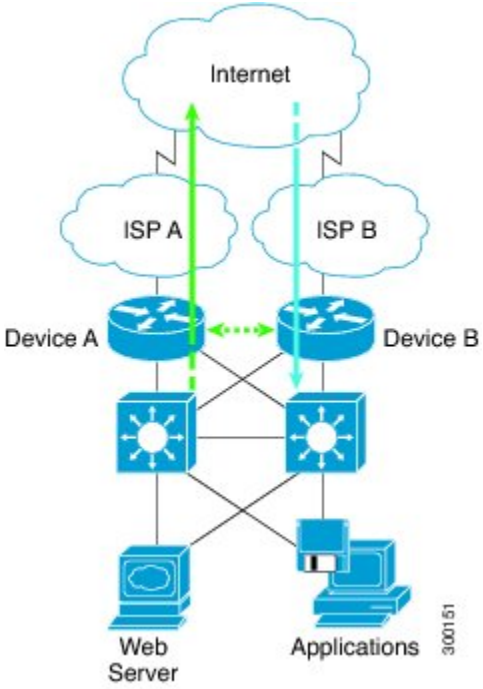
VRF 対応ソフトウェア インフラストラクチャ（VASI）サポートが Cisco IOS XE リリース 3.16S で追加されました。マルチプロトコル ラベル スイッチング（MPLS）非対称ルーティングもサポートされています。

Cisco IOS XE リリース 3.16S では、NAT は ALG、キャリア グレード NAT（CGN）、および Virtual Routing and Forwarding（VRF）インスタンスによる非対称ルーティングをサポートしています。ALG、CGN、または VRF による非対称ルーティングを有効にするために設定を変更する必要はありません。詳細については、「例：VRF による非対称ルーティングの設定」を参照してください。

WAN-LAN トポロジでの非対称ルーティング

非対称ルーティングでは WAN-LAN トポロジだけがサポートされています。WAN-LAN トポロジでは、デバイスが内部の LAN インターフェイスおよび外部の WAN インターフェイスを介して接続されます。WAN リンク経由で受信されるリターン トラフィックのルーティングは制御できません。非対称ルーティングは、WAN-LAN トポロジの WAN リンク経由で受信したリターン トラフィックのルーティングを制御します。次に、WAN-LAN トポロジを示します。

図 *68 : WAN-LAN* トポロジでの非対称ルーティング



ゾーンベース ファイアウォールでの VRF 対応非対称ルーティング

Cisco IOS XE リリース 3.14S では、ゾーンベース ファイアウォールで、VRF 対応シャーシ間非対称ルーティング機能がサポートされます。この機能は、マルチプロトコル ラベル スイッチング（MPLS）をサポートします。

非対称ルーティング転送中に、VPN ルーティングおよび転送（VRF）名ハッシュ値が転送パケットとともに送信されます。VRF 名ハッシュ値は、転送後にアクティブ デバイス上でローカル VRF ID とテーブル ID に変換されます。

転送パケットが、ネットワーク アドレス変換（NAT）とゾーンベース ファイアウォールが設定されたアクティブ デバイスに到着すると、ファイアウォールが NAT または NAT64 から VRF ID を取得して、それをファイアウォール セッション キーに保存します。

ここでは、ゾーンベース ファイアウォールのみがデバイスに設定されている場合の非対称ルーティング パケット フローについて説明します。

- デバイスに MPLS が設定されている場合は、転送パケットの VRF ID 処理が非対称ルーティング転送パケットの処理と同じになります。MPLS パケットは、スタンバイ デバイスで MPLS ラベルが削除される場合でも、アクティブ デバイスに転送されます。ゾーンベース ファイアウォールは、出力インターフェイスでパケットを検査し、このインターフェイスで MPLS が検出された場合は、出力 VRF ID を 0 に設定します。入力インターフェイスで MPLS が設定されている場合は、ファイアウォールが入力 VRF ID を 0 に設定します。

- マルチプロトコル ラベル スイッチング（MPLS）パケットがスタンバイ デバイスからアクティブ デバイスに転送されるときに、非対称ルーティング転送が実行される前にMPLSラベルが削除されます。
- デバイスで MPLS が設定されていない場合は、IP パケットがアクティブ デバイスに転送され、VRF ID が設定されます。ファイアウォールは、出力インターフェイスでパケットを検査するときに、ローカル VRF ID を取得します。

アクティブ デバイスとスタンバイ デバイス間の VRF マッピングは、コンフィギュレーションの変更を必要としません。

NAT での VRF 対応非対称ルーティング

Cisco IOS XE リリース 3.14S では、ネットワーク アドレス変換で VRF 対応シャーシ間非対称ルーティングがサポートされます。VRF 対応シャーシ間非対称ルーティングでは、VPN ルーティングおよび転送（VRF）名のメッセージ ダイジェスト（MD）5 ハッシュを使用して、アクティブ デバイスとスタンバイ デバイス内の VRF とデータパスを特定し、VRF 名ハッシュからローカル VRF ID を、またはローカル VRF ID から VRF 名ハッシュを取得します。

VRF 対応シャーシ間非対称ルーティングでは、アクティブ デバイスとスタンバイ デバイスの VRF に同じ VRF 名を付ける必要があります。ただし、VRF ID は、非対称ルーティング転送またはボックスツーボックス ハイ アベイラビリティ同期の最中にスタンバイ デバイスとアクティブ デバイスの VRF 名に基づいてマップされるため、両方のデバイスで同じにする必要はありません。

VRF 名の MD5 ハッシュ衝突が発生した場合は、VRF に属しているファイアウォール セッションと NAT セッションがスタンバイ デバイスと同期しません。

アクティブ デバイスとスタンバイ デバイス間の VRF マッピングは、コンフィギュレーションの変更を必要としません。

ゾーンベース ファイアウォールと NAT に対するシャーシ間非対称ルーティング サポートの設定方法

冗長アプリケーション グループおよび冗長グループ プロトコルの設定

冗長グループは、次の設定要素で構成されています。

- オブジェクトごとに優先度が減らされる量。
- 優先度を減少させる障害（オブジェクト）
- フェールオーバー優先度

- フェールオーバーしきい値
- グループ インスタンス
- グループ名
- 初期化遅延タイマー

手順の概要

1. **enable**
2. **configure terminal**
3. **redundancy**
4. **application redundancy**
5. **group** *id*
6. **name** *group-name*
7. **priority** *value* [**failover threshold** *value*]
8. **preempt**
9. **track** *object-number* **decrement** *number*
10. **exit**
11. **protocol** *id*
12. **timers hellotime** {*seconds* | **msec** *msec*} **holdtime** {*seconds* | **msec** *msec*}
13. **authentication** {**text** *string* | **md5 key-string** [**0** | **7**] *key* [**timeout** *seconds*] | **key-chain** *key-chain-name*}
14. **bfd**
15. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**redundancy** 例： `Device(config)# redundancy`	冗長コンフィギュレーションモードを開始します。
ステップ 4	**application redundancy** 例： `Device(config-red)# application redundancy`	アプリケーション冗長性を設定し、冗長性アプリケーション コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 5	**group** *id* 例： `Device(config-red-app)# group 1`	冗長性グループを設定し、冗長性アプリケーション グループ コンフィギュレーション モードを開始します。
ステップ 6	**name** *group-name* 例： `Device(config-red-app-grp)# name group1`	プロトコル インスタンス用に、任意指定のエイリアスを指定します。
ステップ 7	**priority** *value* [**failover threshold** *value*] 例： `Device(config-red-app-grp)# priority 100 failover threshold 50`	冗長グループの初期優先度とフェールオーバーしきい値を指定します。
ステップ 8	**preempt** 例： `Device(config-red-app-grp)# preempt`	冗長グループでのプリエンプションをイネーブルにし、スタンバイ デバイスがアクティブ デバイスをプリエンプション処理できるようにします。 • スタンバイ デバイスは、優先度がアクティブ デバイスよりも高いときにのみプリエンプション処理します。
ステップ 9	**track** *object-number* **decrement** *number* 例： `Device(config-red-app-grp)# track 50 decrement 50`	冗長グループの優先度値を指定します。この値は、トラッキング対象のオブジェクトでイベントが発生した場合に減らされます。
ステップ 10	**exit** 例： `Device(config-red-app-grp)# exit`	冗長アプリケーション グループ コンフィギュレーション モードを終了して、冗長アプリケーション コンフィギュレーション モードを開始します。
ステップ 11	**protocol** *id* 例： `Device(config-red-app)# protocol 1`	コントロール インターフェイスに接続されるプロトコルインスタンスを指定し、冗長アプリケーション プロトコル コンフィギュレーション モードを開始します。
ステップ 12	**timers hellotime** {*seconds* | **msec** *msec*} **holdtime** {*seconds* | **msec** *msec*} 例： `Device(config-red-app-prtcl)# timers hellotime 3 holdtime 10`	hello メッセージが送信される間隔、およびデバイスがダウン状態と宣言されるまでの時間を指定します。 • 保留時間は、hellotime の少なくとも 3 倍でなければなりません。
ステップ 13	**authentication** {**text** *string* | **md5 key-string** [**0** | **7**] *key* [**timeout** *seconds*] | **key-chain** *key-chain-name*}	認証情報を指定します。

	コマンドまたはアクション	目的
	例： `Device(config-red-app-prtcl)# authentication md5 key-string 0 n1 timeout 100`	
ステップ 14	**bfd** 例： `Device(config-red-app-prtcl)# bfd`	双方向フォワーディング検出（BFD）を使用してコントロール インターフェイスで実行されているフェールオーバー プロトコルを統合し、ミリ秒単位での障害検出を達成できるようにします。 • BFD はデフォルトでイネーブルになっています。
ステップ 15	**end** 例： `Device(config-red-app-prtcl)# end`	冗長アプリケーションプロトコルコンフィギュレーション モードを終了し、特権 EXEC モードを開始します。

データ、コントロール、および非対称ルーティングインターフェイスの設定

この作業では、次の冗長グループ（RG）要素を設定します。

- コントロール インターフェイスとして使用されるインターフェイス。
- データ インターフェイスとして使用されるインターフェイス。
- 非対称ルーティングに使用されるインターフェイス。これはオプションのタスクです。この作業は、ネットワーク アドレス変換（NAT）の非対称ルーティングを設定する場合にのみ実行します。

（注） 別個のインターフェイスで非対称ルーティング、データ、およびコントロールを設定する必要があります。

手順の概要

1. **enable**
2. **configure terminal**
3. **redundancy**
4. **application redundancy**
5. **group** *id*
6. **data** *interface-type interface-number*
7. **control** *interface-type interface-number* **protocol** *id*
8. **timers delay** *seconds* [**reload** *seconds*]

9. **asymmetric-routing interface** *type number*
10. **asymmetric-routing always-divert enable**
11. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**redundancy** 例： `Device(config)# redundancy`	冗長コンフィギュレーションモードを開始します。
ステップ 4	**application redundancy** 例： `Device(config-red)# application redundancy`	アプリケーション冗長性を設定し、冗長性アプリケーション コンフィギュレーション モードを開始します。
ステップ 5	**group** *id* 例： `Device(config-red-app)# group 1`	冗長性グループ（RG）を設定し、冗長性アプリケーション グループ コンフィギュレーション モードを開始します。
ステップ 6	**data** *interface-type interface-number* 例： `Device(config-red-app-grp)# data GigabitEthernet 0/0/1`	RG で使用されるデータ インターフェイスを指定します。
ステップ 7	**control** *interface-type interface-number* **protocol** *id* 例： `Device(config-red-app-grp)# control GigabitEthernet 1/0/0 protocol 1`	RG で使用されるコントロール インターフェイスを指定します。 • また、コントロール インターフェイスは、コントロール インターフェイス プロトコルのインスタンスにも関連付けられます。
ステップ 8	**timers delay** *seconds* [**reload** *seconds*] 例： `Device(config-red-app-grp)# timers delay 100 reload 400`	障害の発生後、またはシステムのリロード後に開始されるロール ネゴシエーションを RG で遅延させるのに必要な時間を指定します。
ステップ 9	**asymmetric-routing interface** *type number* 例：	RG で使用される非対称ルーティング インターフェイスを指定します。

	コマンドまたはアクション	目的
	`Device(config-red-app-grp)# asymmetric-routing interface GigabitEthernet 0/1/1`	
ステップ 10	**asymmetric-routing always-divert enable** 例： `Device(config-red-app-grp)# asymmetric-routing always-divert enable`	スタンバイ RGから受信したパケットをアクティブ RG に常に転送します。
ステップ 11	**end** 例： `Device(config-red-app-grp)# end`	冗長アプリケーション グループ コンフィギュレーション モードを終了して特権 EXEC モードを開始します。

インターフェイスでの冗長インターフェイス識別子および非対称ルーティングの設定

（注）
- データ インターフェイスまたはコントロール インターフェイスとして設定されているインターフェイスでは、冗長インターフェイス識別子（RII）を設定してはなりません。
- アクティブ デバイスとスタンバイ デバイスの両方で RII および非対称ルーティングを設定する必要があります。
- 仮想 IP アドレスが設定されているインターフェイスでは、非対称ルーティングをイネーブルにすることはできません。

手順の概要

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **redundancy rii** *id*
5. **redundancy group** *id* [**decrement** *number*]
6. **redundancy asymmetric-routing enable**
7. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。

	コマンドまたはアクション	目的
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface** *type number* 例： `Device(config)# interface GigabitEthernet 0/1/3`	冗長グループ（RG）に関連付けるインターフェイスを選択し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	**redundancy rii** *id* 例： `Device(config-if)# redundancy rii 600`	冗長性インターフェイス識別子（RII）を設定します。
ステップ 5	**redundancy group** *id* [**decrement** *number*] 例： `Device(config-if)# redundancy group 1 decrement 20`	RG 冗長性トラフィック インターフェイスの設定をイネーブルにし、インターフェイスのダウン時に優先度から減らされる量を指定します。 （注） 非対称ルーティングがイネーブルになっているトラフィック インターフェイスで RG を設定する必要はありません。
ステップ 6	**redundancy asymmetric-routing enable** 例： `Device(config-if)# redundancy asymmetric-routing enable`	各 RG の非対称フロー転送トンネルを確立します。
ステップ 7	**end** 例： `Device(config-if)# end`	インターフェイス コンフィギュレーション モードを終了し、特権 EXEC モードを開始します。

非対称ルーティングを使用したダイナミック内部送信元変換の設定

次の設定は、非対称ルーティングを使用したダイナミック内部送信元変換の例です。非対称ルーティングを設定する際に使用できる NAT 設定のタイプは、ダイナミック外部送信元、スタティック内部および外部送信元、ポートアドレス変換（PAT）内部および外部送信元変換です。NAT 設定のそれぞれのタイプの詳細については、「IP アドレス節約のための NAT 設定」の章を参照してください。

手順の概要

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **ip address** *ip-address mask*

5. **ip nat outside**
6. **exit**
7. **redundancy**
8. **application redundancy**
9. **group** *id*
10. **asymmetric-routing always-divert enable**
11. **end**
12. **configure terminal**
13. **ip nat pool** *name start-ip end-ip* {*mask* | **prefix-length** *prefix-length*}
14. **exit**
15. **ip nat inside source list** *acl-number* **pool** *name* **redundancy** *redundancy-id* **mapping-id** *map-id*
16. **access-list** *standard-acl-number* **permit** *source-address wildcard-bits*
17. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface** *type number* 例： `Device(config)# interface gigabitethernet 0/1/3`	インターフェイスを設定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	**ip address** *ip-address mask* 例： `Device(config-if)# ip address 10.1.1.1 255.255.255.0`	インターフェイスのプライマリ IP アドレスを設定します。
ステップ 5	**ip nat outside** 例： `Device(config-if)# ip nat outside`	外部と接続されることを示すマークをインターフェイスに付けます。
ステップ 6	**exit** 例： `Device(config-if)# exit`	インターフェイス コンフィギュレーション モードを終了し、グローバルコンフィギュレーションモードに入ります。
ステップ 7	**redundancy** 例：	冗長性を設定し、冗長性コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
	`Device(config)# redundancy`	
ステップ 8	**application redundancy** 例： `Device(config-red)# application redundancy`	アプリケーション冗長性を設定し、冗長性アプリケーション コンフィギュレーション モードを開始します。
ステップ 9	**group** *id* 例： `Device(config-red-app)# group 1`	冗長性グループを設定し、冗長性アプリケーション グループ コンフィギュレーション モードを開始します。
ステップ 10	**asymmetric-routing always-divert enable** 例： `Device(config-red-app-grp)# asymmetric-routing always-divert enable`	アクティブデバイスにトラフィックを転送します。
ステップ 11	**end** 例： `Device(config-red-app-grp)# end`	冗長アプリケーション グループ コンフィギュレーション モードを終了して特権 EXEC モードを開始します。
ステップ 12	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 13	**ip nat pool** *name start-ip end-ip* {*mask* | **prefix-length** *prefix-length*} 例： `Device(config)# ip nat pool pool1 prefix-length 24`	グローバル アドレスのプールを定義します。 • IP NAT プール コンフィギュレーション モードを開始します。
ステップ 14	**exit** 例： `Device(config-ipnat-pool)# exit`	IP NAT プール コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードを開始します。
ステップ 15	**ip nat inside source list** *acl-number* **pool** *name* **redundancy** *redundancy-id* **mapping-id** *map-id* 例： `Device(config)# ip nat inside source list pool pool1 redundancy 1 mapping-id 100`	内部送信元アドレスの NAT を有効にし、マッピング ID を使用して NAT を冗長グループに関連付けます。
ステップ 16	**access-list** *standard-acl-number* **permit** *source-address wildcard-bits* 例： `Device(config)# access-list 10 permit 10.1.1.1 255.255.255.0`	変換される内部アドレス用の標準アクセス リストを定義します。

	コマンドまたはアクション	目的
ステップ 17	**end** 例： `Device(config)# end`	グローバル コンフィギュレーション モードを終了し、特権 EXEC モードを開始します。

ゾーンベース ファイアウォールと NAT に対するシャーシ間非対称ルーティング サポートの設定例

例：冗長アプリケーション グループと冗長グループ プロトコルの設定

```
Device# configure terminal
Device(config)# redundancy
Device(config-red)# application redundancy
Device(config-red-app)# group 1
Device(config-red-app-grp)# name group1
Device(config-red-app-grp)# priority 100 failover threshold 50
Device(config-red-app-grp)# preempt
Device(config-red-app-grp)# track 50 decrement 50
Device(config-red-app-grp)# exit
Device(config-red-app)# protocol 1
Device(config-red-app-prtcl)# timers hellotime 3 holdtime 10
Device(config-red-app-prtcl)# authentication md5 key-string 0 n1 timeout 100
Device(config-red-app-prtcl)# bfd
Device(config-red-app-prtcl)# end
```

例：データ、コントロール、および非対称ルーティングインターフェイスの設定

```
Device# configure terminal
Device(config)# redundancy
Device(config-red)# application redundancy
Device(config-red-app)# group 1
Device(config-red-app-grp)# data GigabitEthernet 0/0/1
Device(config-red-app-grp)# control GigabitEthernet 1/0/0 protocol 1
Device(config-red-app-grp)# timers delay 100 reload 400
Device(config-red-app-grp)# asymmetric-routing interface GigabitEthernet 0/1/1
Device(config-red-app-grp)# asymmetric-routing always-divert enable
Device(config-red-app-grp)# end
```

例：インターフェイスでの冗長インターフェイス識別子と非対称ルーティングの設定

```
Device# configure terminal
Device(config)# interface GigabitEthernet 0/1/3
Device(config-if)# redundancy rii 600
Device(config-if)# redundancy group 1 decrement 20
Device(config-if)# redundancy asymmetric-routing enable
Device(config-if)# end
```

例：非対称ルーティングを使用したダイナミック内部送信元変換の設定

```
Device(config)# interface gigabitethernet 0/1/3
Device(config-if)# ip address 10.1.1.1 255.255.255.0
Device(config-if)# ip nat outside
Device(config-if)# exit
Device(config)# redundancy
Device(config-red)# application redundancy
Device(config-red-app)# group 1
Device(config-red-app-grp)# asymmetric-routing always-divert enable
Device(config-red-app-grp)# end
Device# configure terminal
Device(config)# ip nat pool pool1 prefix-length 24
Device(config-ipnat-pool)# exit
Device(config)# ip nat inside source list pool pool1 redundancy 1 mapping-id 100
Device(config)# access-list 10 permit 10.1.1.1 255.255.255.0
```

例：対称ルーティング ボックスツーボックス冗長性を使用した WAN-WAN トポロジ用の VRF 対応 NAT の設定

次に、WAN 間対称ルーティング設定の例を示します。

```
vrf definition Mgmt-intf
 address-family ipv4
  exit-address-family
!
address-family ipv6
 exit-address-family
!
!
vrf definition VRFA
 rd 100:1
 route-target export 100:1
 route-target import 100:1
 address-family ipv4
  exit-address-family
!
!
```

```
no logging console
no aaa new-model
!
multilink bundle-name authenticated
!
redundancy
 mode sso
 application redundancy
  group 1
   preempt
   priority 120
   control GigabitEthernet 0/0/1 protocol 1
   data GigabitEthernet 0/0/2
!
!
!
!
ip tftp source-interface GigabitEthernet0
ip tftp blocksize 8192
!
track 1 interface GigabitEthernet 0/0/4 line-protocol
!
interface Loopback 0
 ip address 209.165.201.1 255.255.255.224
!
interface GigabitEthernet 0/0/0
 vrf forwarding VRFA
 ip address 192.168.0.1 255.255.255.248
 ip nat inside
 negotiation auto
 bfd interval 50 min_rx 50 multiplier 3
 redundancy rii 2
!
interface GigabitEthernet 0/0/1
 ip address 209.165.202.129 255.255.255.224
 negotiation auto
!
interface GigabitEthernet 0/0/2
 ip address 192.0.2.1 255.255.255.224
 negotiation auto
!
interface GigabitEthernet 0/0/3
 ip address 198.51.100.1 255.255.255.240
 negotiation auto
!
interface GigabitEthernet 0/0/4
 ip address 203.0.113.1 255.255.255.240
 negotiation auto
!
interface GigabitEthernet 0
 vrf forwarding Mgmt-intf
 ip address 172.16.0.1 255.255.0.0
 negotiation auto
!
interface vasileft 1
 vrf forwarding VRFA
 ip address 10.4.4.1 255.255.0.0
 ip nat outside
 no keepalive
!
interface vasiright 1
ip address 10.4.4.2 255.255.0.0
no keepalive
!
```

```
router mobile
!
router bgp 577
 bgp router-id 1.1.1.1
 bgp log-neighbor-changes
 neighbor 203.0.113.1 remote-as 223
 neighbor 203.0.113.1 description PEERING to PTNR neighbor 10.4.4.1 remote-as 577
 neighbor 10.4.4.1 description PEEERING to VASI VRFA interface
!
address-family ipv4
 network 203.0.113.1 mask 255.255.255.240
 network 10.4.0.0 mask 255.255.0.0
 network 209.165.200.224 mask 255.255.255.224
 neighbor 203.0.113.1 activate
 neighbor 10.4.4.1 activate
 neighbor 10.4.4.1 next-hop-self
 exit-address-family
!
address-family ipv4 vrf VRFA
 bgp router-id 4.4.4.4
 network 192.168.0.0 mask 255.255.255.248
 network 10.4.0.0 mask 255.255.0.0
 redistribute connected
 redistribute static
 neighbor 192.168.0.2 remote-as 65004
 neighbor 192.168.0.2 fall-over bfd
 neighbor 192.168.0.2 activate
 neighbor 10.4.4.2 remote-as 577
 neighbor 10.4.4.2 description PEERING to VASI Global intf
 neighbor 10.4.4.2 activate
 exit-address-family
!
ip nat switchover replication http
ip nat pool att_pool 209.165.200.225 209.165.200.225 prefix-length 16
ip nat inside source list 4 pool att_pool redundancy 1 mapping-id 100 vrf VRFA overload
ip forward-protocol nd
!
no ip http server
no ip http secure-server
ip route 203.0.113.1 255.255.255.224 10.4.4.1
ip route 192.168.0.0 255.255.0.0 10.4.4.1
ip route 209.165.200.224 255.255.255.224 10.4.4.1
ip route vrf Mgmt-intf 209.165.200.1 255.255.255.224 172.16.0.0
!
ip prefix-list VRF_Pool seq 5 permit 209.165.200.0/27
ip prefix-list p1-adv-1 seq 5 permit 209.165.200.0/27
ip prefix-list p1-exist-1 seq 5 permit 203.0.113.193/27
logging esm config
access-list 4 permit 203.0.113.193 255.255.255.224
!
control-plane
line console 0
 stopbits 1
!
line vty 0 3
 login
!
line vty 4
 password lab
 login
!
end
```

例：VRF を使用した非対称ルーティングの設定

次に、Virtual Routing and Forwarding（VRF）インスタンスを使用して非対称ルーティングを設定する例を示します。

```
Device(config)# redundancy
Device(config-red)# mode sso
Device(config-red)# application redundancy
Device(config-red-app)# group 1
Device(config-red-app-grp)# name RG1
Device(config-red-app-grp)# preempt
Device(config-red-app-grp)# priority 100 failover threshold 40
Device(config-red-app-grp)# control GigabitEthernet 1/0/3 protocol 1
Device(config-red-app-grp)# data GigabitEthernet 1/0/3
Device(config-red-app-grp)# asymmetric-routing interface GigabitEthernet 1/0/4
Device(config-red-app-grp)# asymmetric-routing always-divert enable
Device(config-red-app-grp)# exit
Device(config-red-app)# exit
Device(config-red)# exit
!
Device(config)# interface TenGigabitEthernet 2/0/0
Device(config-if)# ip vrf forwarding vrf001
Device(config-if)# ip address 10.0.0.1 255.255.255.0
Device(config-if)# ip nat inside
Device(config-if)# exit
!
Device(config)# interface TenGigabitEthernet 3/0/0
Device(config-if)# ip vrf forwarding vrf001
Device(config-if)# ip address 192.0.2.1 255.255.255.0
Device(config-if)# ip nat outside
Device(config-if)# exit
!
Device(config-if)# ip nat pool pool-vrf001 209.165.201.1 209.165.201.30 prefix-length
24
Device(config-if)# ip nat inside source list 1 pool pool-vrf001 redundancy 1 mapping-id
 1 vrf vrf001 match-in-vrf overload
Device(config-if)# end
```

ゾーンベース ファイアウォールと NAT に対するシャーシ間非対称ルーティング サポートに関する追加情報

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『Cisco IOS Master Command List, All Releases』

関連項目	マニュアル タイトル
セキュリティ コマンド	• 『Cisco IOS Security Command Reference Commands A to C』 • 『Cisco IOS Security Command Reference Commands D to L』 • 『Cisco IOS Security Command Reference Commands M to R』 • 『Cisco IOS Security Command Reference Commands S to Z』
ファイアウォール シャーシ間冗長性	「ファイアウォール ステートフル シャーシ間冗長性の設定」モジュール
NAT シャーシ間冗長性	「ステートフル シャーシ間冗長性の設定」モジュール

シスコのテクニカル サポート

説明	リンク
右の URL にアクセスして、シスコのテクニカル サポートを最大限に活用してください。これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

ゾーンベース ファイアウォールおよびNATのシャーシ間非対称ルーティング サポートの機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *175 :* ゾーンベース ファイアウォールおよび *NAT* のシャーシ間非対称ルーティング サポートの機能情報

機能名	リリース	機能情報
NAT44 対応の非対称ルーティング拡張	Cisco IOS XE リリース 3.16S	NAT 44 対応の非対称ルーティング拡張機能は、CGN、ALG、VRF、VASI、および MPLS を使用した非対称ルーティングをサポートしています。 追加または変更されたコマンドはありません。
ゾーンベース ファイアウォールと NAT に対するシャーシ間非対称ルーティング サポート	Cisco IOS XE Release 3.5S	ゾーンベース ファイアウォールおよび NAT のシャーシ間非対称ルーティングサポート機能では、スタンバイ冗長グループからアクティブ冗長グループへのパケット処理のためのパケット転送がサポートされています。 次のコマンドが導入または変更されました。**asymmetric-routing**、**redundancy asymmetric-routing enable**
ゾーンベース ファイアウォールの VRF 対応シャーシ間非対称ルーティング サポート	Cisco IOS XE リリース 3.14S	ゾーンベース ファイアウォールでは、VRF 対応シャーシ間非対称ルーティング機能がサポートされています。この機能は MPLS をサポートしています。この機能については設定の変更はありません。 追加または変更されたコマンドはありません。
NAT の VRF 対応シャーシ間非対称ルーティング サポート	Cisco IOS XE リリース 3.14S	NAT では、VRF 対応シャーシ間非対称ルーティング機能がサポートされています。この機能は MPLS をサポートしています。この機能については設定の変更はありません。 追加または変更されたコマンドはありません。

第 131 章

IPv6 ゾーンベース ファイアウォールのボックスツーボックス ハイ アベイラビリティ サポート

IPv6 ゾーンベース ファイアウォールのボックスツーボックス ハイ アベイラビリティ サポート機能では、IPv6 ファイアウォールの冗長グループ（RG）に基づいてハイ アベイラビリティ（HA）がサポートされています。この機能により、相互にバックアップとして動作するデバイスのペアを設定できます。この機能を設定し、複数のフェールオーバー条件に基づいてアクティブ デバイスを判断できます。この機能は、IPv6 パケット インスペクションの FTP66 アプリケーション レイヤ ゲートウェイ（ALG）をサポートしています。

このモジュールでは、ボックスツーボックス（B2B）HA サポートに関する情報を提供し、この機能を設定する方法について説明します。

IPv6 ゾーンベース ファイアウォールに対するボックスツーボックス ハイ アベイラビリティ サポートに関する前提条件

- ファイアウォールにアタッチされたインターフェイスは、冗長インターフェイス識別子（RII）を同じにする必要があります。
- アクティブ デバイスとスタンバイ デバイスは、ゾーンベース ポリシー ファイアウォール設定を同じにする必要があります。
- アクティブ デバイスとスタンバイ デバイスは、同じバージョンのシスコ ソフトウェア上で動作する必要があります。アクティブ デバイスとスタンバイ デバイスは、スイッチ経由で接続する必要があります。
- アクティブ デバイスとスタンバイ デバイスの両方のボックスツーボックス（B2B）設定は同じにする必要があります。これは、これらのデバイス間の設定の自動同期機能がないためです。
- 非対称ルーティング トラフィックを通過させるためには、class-default クラスの通過アクションを設定する必要があります。class-default クラスは、ポリシー内のユーザ定義クラスのどれとも一致しないすべてのパケットを表すシステム定義のクラス マップです。
- 2 つの LAN インターフェイス間でゾーン ペアを設定する場合は、両方のインターフェイス上で同じ冗長グループ（RG）が設定されていることを確認します。ゾーンペア設定は、LAN インターフェイスが別の RG に属している場合はサポートされません。

IPv6 ゾーンベース ファイアウォールに対するボックスツーボックス ハイ アベイラビリティ サポートに関する制約事項

- ボックスツーボックス（B2B）リンク間インターフェイスでは、IPv4 のみがサポートされます。
- マルチプロトコル ラベル スイッチング（MPLS）と Virtual Routing and Forwarding（VRF）はサポートされません。
- シャーシ内のデュアル エンベデッド サービス プロセッサ（ESP）またはデュアル ルート プロセッサ（RP）を搭載した Cisco ASR 1006 および 1013 アグリゲーション サービス ルータはサポートされません。これは、ボックス間ハイ アベイラビリティ（HA）とボックス内 HA の共存がサポートされないためです。

シャーシ内のシングル ESP とシングル RP を搭載した Cisco ASR 1006 および Cisco ASR 1013 アグリゲーション サービス ルータは、シャーシ間冗長性をサポートします。

- デュアル IOS デーモン（IOSd）が設定されている場合、デバイスはファイアウォール ステートフル シャーシ間冗長性の設定をサポートしません。
- IPv6 ファイアウォールを使用したステートレス ネットワーク アドレス変換 64（NAT64）はサポートされません。

IPv6 ゾーンベース ファイアウォールに対するボックス ツーボックス ハイ アベイラビリティ サポートに関する情報

ゾーンベース ポリシー ファイアウォール ハイ アベイラビリティの概要

ハイアベイラビリティは、ネットワークのどの場所でも起こり得る障害からの迅速な回復を可能にすることで、ネットワーク全体の保護を実現します。ハイ アベイラビリティは、ユーザ アプリケーションやネットワーク アプリケーションの中断からの迅速な回復を可能にします。

ゾーンベースポリシーファイアウォールは、アクティブ/アクティブおよびアクティブ/スタンバイ ハイ アベイラビリティ フェールオーバーと非対称ルーティングをサポートします。

アクティブ/アクティブ フェールオーバーは、フェールオーバーに関与している両方のデバイスが同時にトラフィックを転送できるようにします。

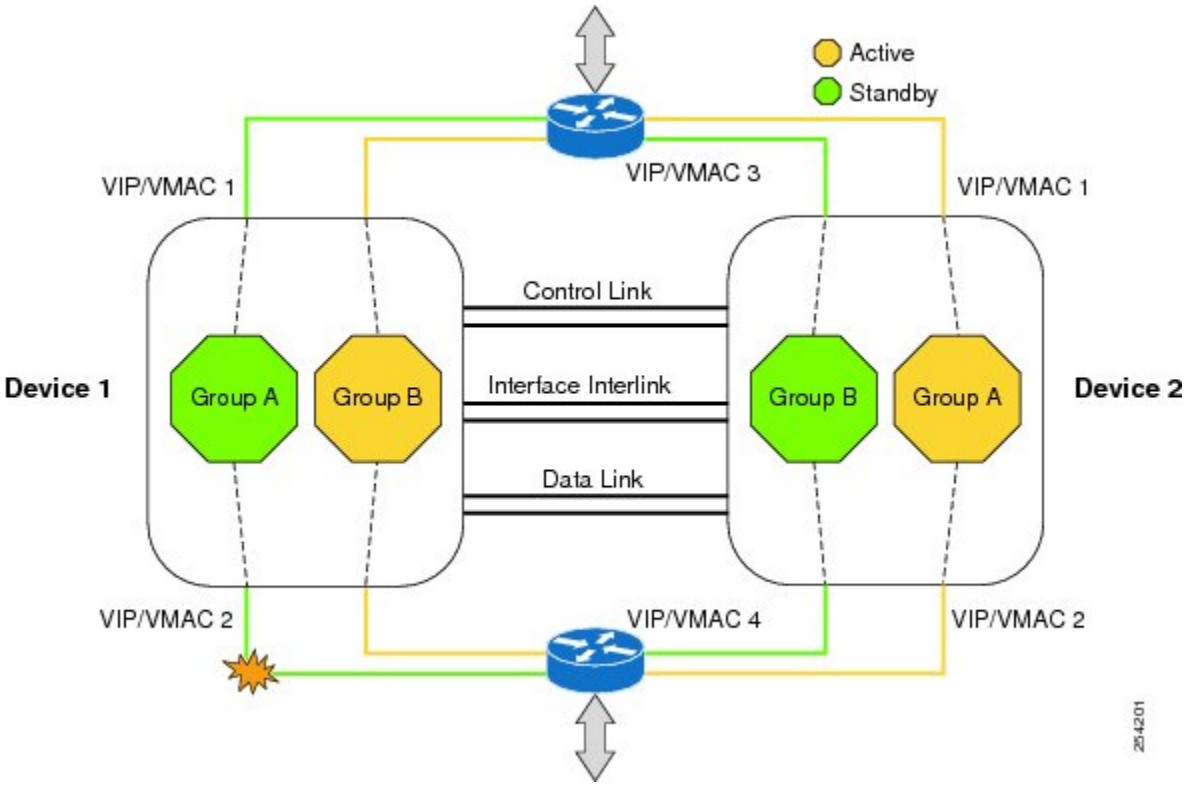
アクティブ/スタンバイ ハイ アベイラビリティ フェールオーバーが設定されている場合は、一度にフェールオーバーに関与している一方のデバイスだけがトラフィックを処理し、もう一方のデバイスはスタンバイ モードに入って定期的にアクティブ デバイスからセッション情報を同期します。

非対称ルーティングは、パケット処理のためのスタンバイ冗長グループからアクティブ冗長グループへのパケットの転送をサポートします。この機能が有効になっていない場合は、初期同期（SYN）メッセージを受信しなかったデバイスに転送されたリターンTCPパケットがドロップされます。これは、パケットが既知のセッションに属していないためです。

ボックスツーボックス ハイアベイラビリティの動作

相互にホットスタンバイとして動作するようにデバイスのペアを設定できます。冗長性はインターフェイスごとに設定します。冗長インターフェイスのペアは、冗長グループ（RG）と呼ばれます。図 1 は、アクティブ/アクティブ フェールオーバー シナリオを示しています。2 つの発信インターフェイスを持つデバイスのペアに対して2つの冗長グループがどのように設定されているかを示します。

図 *69 :* 冗長グループの設定：*2* つの発信インターフェイス



冗長デバイスは、設定可能なコントロール リンク、データ同期リンク、およびインターリンク インターフェイスによって結合されます。コントロール リンクは、デバイスのステータスを通信するために使用されます。データ同期リンクは、ファイアウォールからステートフル情報を転送し、ステートフルデータベースを同期するために使用されます。冗長インターフェイスのペアは、同じ固有 ID 番号（冗長インターフェイス識別子（RII）と呼ばれます）を使用して設定されます。ルーティング テーブルは、アクティブからスタンバイには同期されません。

非対称ルーティングは、ファイアウォール HA の一部としてサポートされています。リターン トラフィックがスタンバイ デバイスに入る LAN-WAN シナリオでは、非対称ルーティングがサポートされます。非対称ルーティングの機能を実装するには、非対称トラフィックの専用インターフェイス（インターリンク インターフェイス）で両方の冗長デバイスを設定します。この専用インターフェイスは、スタンバイ WAN インターフェイスに着信するトラフィックを、アクティブ デバイスにリダイレクトします。

冗長グループ メンバーのステータスは、コントロール リンクで送信される hello メッセージを使用することで判断できます。いずれかのデバイスが、設定された時間内に hello メッセージに応答しない場合、ソフトウェアは障害が発生したと見なし、スイッチオーバーが開始されます。ミリ秒単位でエラーを検出するには、フェールオーバー プロトコルをコントロール リンクで実行します。hello メッセージについて次のパラメータを設定できます。

- Active timer。
- Standby timer。

- Hello time：hello メッセージが送信される間隔。
- Hold time：アクティブ デバイスまたはスタンバイ デバイスがダウンしていると宣言されるまでの時間。

Hello time のデフォルトは、Hot Standby Router Protocol（HSRP）に合わせるために 3 秒です。Hold time のデフォルトは 10 秒です。これらのタイマーは、**timers hellotime msec** コマンドを使用してミリ秒単位で設定することもできます。

スイッチオーバーの影響を受けるインターフェイスのペアを判断するには、冗長インターフェイスの各ペアに対して固有の ID を設定する必要があります。この ID は、インターフェイスに関連付けられている RII です。

スイッチオーバーの原因

スイッチオーバーが発生する別の要因として、各デバイスで設定可能な優先度設定があります。優先度が最も高いデバイスがアクティブ デバイスになります。アクティブ デバイスまたはスタンバイ デバイスで障害が発生した場合、重みと呼ばれる設定可能な数値分、ルータの優先度が下がります。アクティブ デバイスの優先度が、スタンバイ デバイスの優先度を下回る場合、スイッチオーバーが発生し、スタンバイ デバイスがアクティブ デバイスになります。このデフォルトの動作を無効にするには、冗長グループの preemption 属性を無効にします。また、インターフェイスのレイヤ 1 状態がダウンになった場合、各インターフェイスを設定して優先度を下げます。設定された優先度が、冗長グループのデフォルトの 優先度を上書きします。

冗長グループの優先度が変更されるエラー イベントごとに、タイム スタンプ、影響を受けた冗長グループ、変更前の優先度、変更後の優先度、およびエラーイベントの原因の説明を含む syslog エントリが生成されます。

スイッチオーバーが発生する原因となるもう 1 つの状況は、デバイスまたはインターフェイスの優先度が、設定可能なしきい値レベルを下回る場合です。

スタンバイ デバイスへのスイッチオーバーは次の条件で発生します。

- アクティブデバイスで停電またはリロードが発生した場合（クラッシュも含まれます）。
- アクティブ デバイスのランタイム優先度が、スタンバイ デバイスの優先度を下回った場合。
- アクティブ デバイスのランタイム優先度が、設定したしきい値レベルを下回った場合。
- アクティブデバイスの冗長グループを手動でリロードするには、**redundancy application reload group** *rg-number* コマンドを使用します。
- 任意のモニタ対象インターフェイスで 2 つの連続する hello メッセージに失敗した場合、インターフェイスは強制的にテストモードになります。いずれのデバイスもインターフェイス上のリンク ステータスを確認してから、次のテストを実行します。
  - ネットワーク アクティビティ テスト
  - Address Resolution Protocol（ARP）テスト
  - ブロードキャスト ping テスト

アクティブ/アクティブ フェールオーバー

アクティブ/アクティブ フェールオーバー構成では、両方のデバイスがネットワーク トラフィックを渡すことができます。アクティブ/アクティブ フェールオーバーでは、各冗長グループ（RG）のインターフェイスの仮想 MAC（VMAC）アドレスが生成されます。

アクティブ/アクティブ フェールオーバー ペアの 1 つのデバイスがプライマリ（アクティブ）デバイスとして指定され、もう1つのデバイスがセカンダリ（スタンバイ）デバイスとして指定されます。アクティブ/スタンバイ フェールオーバーの場合とは異なり、両方のデバイスが同時に起動された場合、この指定ではどちらのデバイスがアクティブになるかは指示しません。代わりに、プライマリまたはセカンダリの指定によって次の点が決定します。

- デバイスが同時に起動したときに、実行コンフィギュレーションをフェールオーバー ペアに提供するデバイス。
- デバイスが同時に起動したときに、フェールオーバー RG がアクティブ状態のデバイス。このコンフィギュレーションの各フェールオーバー RG は、プライマリまたはセカンダリ デバイス プリファレンスで設定されます。1 つのデバイスで両方のフェールオーバー RG がアクティブ状態であり、スタンバイ フェールオーバー RG がもう一方のデバイスにあるように設定できます。また、1 つのフェールオーバー RG をアクティブ状態にし、もう 1 つの RG を 1 つのデバイスでスタンバイ状態に設定することもできます。

アクティブ/スタンバイ フェールオーバー

アクティブ/スタンバイ フェールオーバーでは、スタンバイ デバイスを使用して、障害が発生したデバイスの機能を引き継ぐことができます。障害が発生したアクティブデバイスはスタンバイ状態になり、スタンバイデバイスがアクティブ状態になります。アクティブ状態になったデバイスは、障害が発生したデバイスのIPアドレスとMACアドレスを引き継いで、トラフィックの処理を開始します。スタンバイ状態になったデバイスは、スタンバイ IP アドレスと MAC アドレスを引き継ぎます。ネットワーク デバイスは MAC to IP アドレス ペアでの変更を認識しないため、ネットワーク上のいずれの場所でも Address Resolution Protocol（ARP）エントリが変更されたり、タイムアウトが生じたりすることはありません。

アクティブ/スタンバイ シナリオでは、フェールオーバー ペアの 2 つのデバイス間の主な違いは、どのデバイスがアクティブで、どのデバイスがスタンバイであるか、つまり、どの IP アドレスを使用し、どのデバイスがアクティブにトラフィックを渡すかということに関連します。両方のデバイスが同時にスタートアップした場合（さらに動作ヘルスが等しい場合）、アクティブ デバイスは常にアクティブ デバイスになります。アクティブ デバイスの MAC アドレスは常に、アクティブ IP アドレスと組み合わせられます。

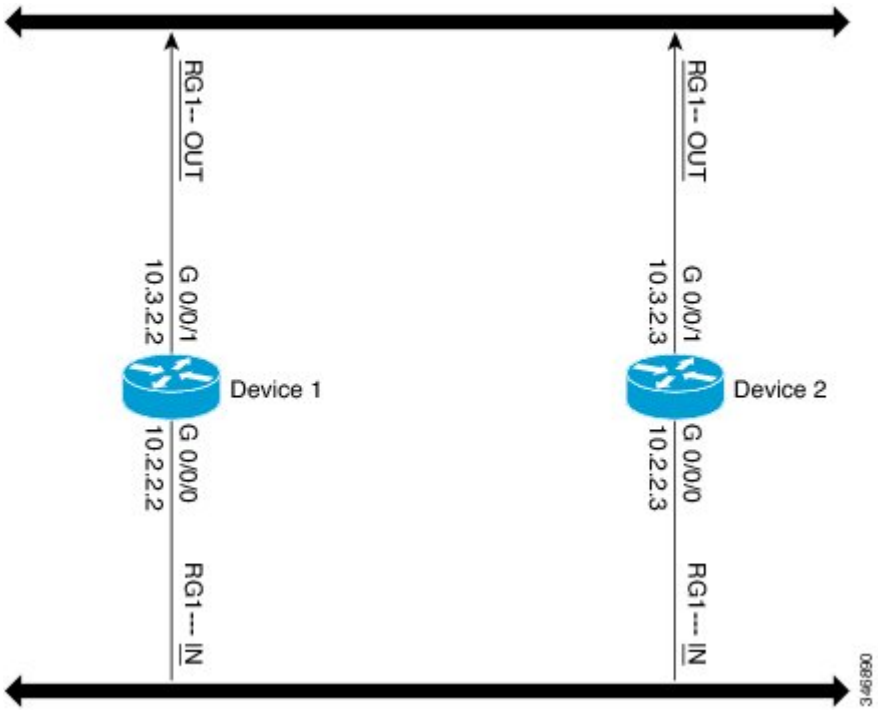
NAT ボックスツーボックス高可用性 LAN/LAN トポロジ

LAN/LANトポロジに参加するすべてのデバイスは、内部と外部の両方でLANインターフェイスを介して相互接続されます。次の図に、NATボックスツーボックスLAN/LANトポロジを示します。ネットワーク アドレス変換（NAT）はアクティブ/スタンバイ モードで行われ、ピア

は 1 つの冗長グループ（RG）にまとめられます。すべてのトラフィックまたはトラフィックのサブセットに NAT 変換が適用されます。

（注） フェールオーバーは、RGインフラストラクチャでリッスンする障害によってのみ発生します。

図 *70 : NAT* ボックスツーボックス高可用性 *LAN/LAN* トポロジ



WAN-LAN トポロジ

WAN-LAN トポロジでは、2 つのデバイスが内部の LAN インターフェイスと外部の WAN インターフェイスを介して接続されます。WAN リンク経由で受信されるリターン トラフィックのルーティングは制御できません。

WAN リンクは、同じサービス プロバイダーまたは別のサービス プロバイダーから提供できます。ほとんどの場合、WAN リンクは別のサービス プロバイダーから提供されます。WAN リンクを最大限に活用するには、フェールオーバーを提供するように外部デバイスを設定します。

LAN ベースのインターフェイスでは、クライアント情報の交換とフェールオーバーの高速化のために、ハイ アベイラビリティ仮想 IP アドレスが必要です。WAN ベースのインターフェイスでは、フェールオーバーに **redundancy group** *id* **ip** *virtual-ip* **decrement** *value* コマンドが使用されます。

排他的仮想 IP アドレスと排他的仮想 MAC アドレス

仮想 IP（VIP）アドレスと仮想 MAC（VMAC）アドレスは、セキュリティ アプリケーションが、トラフィックを受信するインターフェイスを制御するために使用します。インターフェイスは別のインターフェイスとペアにされ、これらのインターフェイスは同じ冗長グループ（RG）に関連付けられます。アクティブな RG に関連付けられているインターフェイスは、VIP アドレスと VMAC を排他的に所有します。アクティブデバイスの Address Resolution Protocol（ARP）プロセスによって、VIP への ARP 要求に対する ARP 応答が送信されます。また、インターフェイスのイーサネット コントローラは、VMAC 宛てのパケットを受信するようにプログラミングされます。RG のフェールオーバーが発生すると、VIP と VMAC の所有権は変化します。新しくアクティブになった RG に関連付けられたインターフェイスは、gratuitous ARP を送信し、インターフェイスのイーサネット コントローラをプログラミングして、VMAC 宛てのパケットを受け入れます。

IPv6 のサポート

各冗長グループ（RG）を、同じ冗長インターフェイス識別子（RII）で IPv4 と IPv6 の両方の仮想 IP（VIP）アドレスのトラフィック インターフェイスに割り当てることができます。各 RG は RII ごとに一意の仮想 MAC（VMAC）アドレスを使用します。RG では、IPv6 リンクローカル VIP とグローバル VIP がインターフェイス上に共存します。

トラフィック インターフェイス上の各 RG に対して IPv4 VIP、リンクローカル IPv6 VIP、および/またはグローバル IPv6 VIP を設定できます。IPv6 リンクローカル VIP は、スタティック ルートまたはデフォルト ルートを設定する場合に主に使用されます。IPv6 グローバル VIP は、LAN トポロジと WAN トポロジの両方で広く使用されています。

IPv4 VIP を設定する前に、物理 IP アドレスを設定する必要があります。

FTP66 ALG サポートの概要

ファイアウォールでは、IPv6 パケットとステートフル ネットワーク アドレス変換 64（NAT64）のインスペクションをサポートしています。FTP を IPv6 パケット インスペクションに基づいて機能させるには、アプリケーション層ゲートウェイ（ALG）（別名アプリケーション レベル ゲートウェイ（ALG））FTP66 が必要です。FTP66 ALG は、オールインワン FTP ALG およびワン FTP ALG とも呼ばれています。

FTP66 ALG では、次の機能をサポートしています。

- ファイアウォール IPv4 パケット インスペクション
- ファイアウォール IPv6 パケット インスペクション
- NAT の設定
- NAT64 の設定（FTP64 サポートを使用）
- NAT とファイアウォールの設定
- NAT64 とファイアウォールの設定

FTP66 ALG には、次のセキュリティ上の脆弱性があります。

- パケット セグメンテーション攻撃：FTP ALG ステート マシンではセグメント化されたパケットを検出できます。完全なパケットを受信するまで、ステートマシンの処理は停止します。
- バウンス攻撃：FTP ALG は、番号が 1024 未満のデータ ポートでドア（NAT の場合）やピンホール（ファイアウォールの場合）を作成しません。バウンス攻撃の防止がアクティブになるのは、ファイアウォールが有効にされている場合のみです。

IPv6 ゾーンベース ファイアウォールに対するボックスツーボックス ハイ アベイラビリティ サポートの設定方法

冗長グループ プロトコルの設定

手順の概要

1. **enable**
2. **configure terminal**
3. **redundancy**
4. **application redundancy**
5. **protocol** *id*
6. **name** *group-name*
7. **timers hellotime** {*seconds* | **msec** *milliseconds*} **holdtime** {*seconds* | **msec** *milliseconds*}
8. **authentication** {**text** *string* | **md5 key-string** [**0** | **7**] *key-string* **timeout** *seconds* | **key-chain** *key-chain-name*}
9. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 3	**redundancy** 例： `Device(config)# redundancy`	冗長コンフィギュレーションモードを開始します。
ステップ 4	**application redundancy** 例： `Device(config-red)# application redundancy`	冗長アプリケーションコンフィギュレーションモードを開始します。
ステップ 5	**protocol** *id* 例： `Device(config-red-app)# protocol 1`	コントロールインターフェイスに接続されるプロトコルインスタンスを指定し、冗長アプリケーションプロトコル コンフィギュレーション モードを開始します。
ステップ 6	**name** *group-name* 例： `Device(config-red-app-prtcl)# name prot1`	（任意）名前を使用して冗長グループ（RG）を設定します。
ステップ 7	**timers hellotime** {*seconds* | **msec** *milliseconds*} **holdtime** {*seconds* | **msec** *milliseconds*} 例： `Device(config-red-app-prtcl)# timers hellotime 3 holdtime 9`	helloメッセージが送信される間隔と、デバイスがダウン状態と宣言されるまでの時間を指定します。
ステップ 8	**authentication** {**text** *string* | **md5 key-string** [**0** | **7**] *key-string* **timeout** *seconds* | **key-chain** *key-chain-name*} 例： `Device(config-red-app-prtcl)# authentication md5 key-string 0 n1 timeout 100`	認証情報を指定します。
ステップ 9	**end** 例： `Device(config-red-app-prtcl)# end`	冗長アプリケーションプロトコルコンフィギュレーションモードを終了し、特権EXECモードを開始します。

冗長アプリケーション グループの設定

手順の概要

1. **enable**
2. **configure terminal**
3. **redundancy**
4. **application redundancy**
5. **group** *id*
6. **name** *group-name*

7. **shutdown**
8. **priority** *value* [**failover threshold** *value*]
9. **preempt**
10. **track** *object-number* {**decrement** *value* | **shutdown**}
11. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**redundancy** 例： `Device(config)# redundancy`	冗長コンフィギュレーションモードを開始します。
ステップ 4	**application redundancy** 例： `Device(config-red)# application redundancy`	冗長アプリケーションコンフィギュレーションモードを開始します。
ステップ 5	**group** *id* 例： `Device(config-red-app)# group 1`	冗長アプリケーション グループ コンフィギュレーション モードを開始します。
ステップ 6	**name** *group-name* 例： `Device(config-red-app-grp)# name group1`	（任意）プロトコル インスタンスに任意のエイリアスを指定します。
ステップ 7	**shutdown** 例： `Device(config-red-app-grp)# shutdown`	（任意）冗長グループを手動でシャットダウンします。
ステップ 8	**priority** *value* [**failover threshold** *value*] 例： `Device(config-red-app-grp)# priority 100 failover threshold 50`	（任意）冗長グループの初期優先度とフェールオーバーしきい値を指定します。
ステップ 9	**preempt** 例：	グループでのプリエンプションをイネーブルにし、優先度とは無関係にスタンバイデバイスがアクティ

	コマンドまたはアクション	目的
	`Device(config-red-app-grp)# preempt`	ブ デバイスをプリエンプション処理できるようにします。
ステップ 10	**track** *object-number* {**decrement** *value* | **shutdown**} 例： `Device(config-red-app-grp)# track 200 decrement 200`	冗長グループの優先度を指定します。この値は、イベントが発生した場合に減らされます。
ステップ 11	**end** 例： `Device(config-red-app-grp)# end`	冗長アプリケーション グループ コンフィギュレーション モードを終了して特権 EXEC モードを開始します。

コントロール インターフェイスおよびデータ インターフェイスの設定

手順の概要

1. **enable**
2. **configure terminal**
3. **redundancy**
4. **application redundancy**
5. **group** *ID*
6. **data** *interface-type interface-number*
7. **control** *interface-type interface-number* **protocol** *id*
8. **timers delay** *seconds* [**reload** *seconds*]
9. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**redundancy** 例： `Device(config)# redundancy`	冗長コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 4	**application redundancy** 例： `Device(config-red)# application redundancy`	冗長アプリケーション コンフィギュレーション モードを開始します。
ステップ 5	**group** *ID* 例： `Device(config-red-app)# group 1`	冗長アプリケーション グループ コンフィギュレーション モードを開始します。
ステップ 6	**data** *interface-type interface-number* 例： `Device(config-red-app-grp)# data GigabitEthernet 0/0/0`	冗長グループに使用されるデータ インターフェイスを指定します。
ステップ 7	**control** *interface-type interface-number* **protocol** *id* 例： `Device(config-red-app-grp)# control gigabitethernet 0/0/2 protocol 1`	冗長グループに使用されるコントロール インターフェイスを指定します。 • このインターフェイスは、コントロール インターフェイス プロトコルのインスタンスにも関連付けられます。
ステップ 8	**timers delay** *seconds* [**reload** *seconds*] 例： `Device(config-red-app-grp)# timers delay 100 reload 400`	障害の発生後、またはシステムのリロード後に起動するロールのネゴシエートを遅らせるために、冗長グループが待機する時間を指定します。
ステップ 9	**end** 例： `Device(config-red-app-grp)# end`	冗長アプリケーション グループ コンフィギュレーション モードを終了して特権 EXEC モードを開始します。

LAN トラフィック インターフェイスの設定

手順の概要

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **description** *string*
5. **encapsulation dot1q** *vlan-id*
6. **ip vrf forwarding** *name*
7. **ipv6 address** {*ipv6-prefix/prefix-length* | *prefix-name sub-bits/prefix-length*}
8. **zone-member security** *zone-name*
9. **redundancy rii** *RII-identifier*

10. **redundancy group** *id* {**ip** *virtual-ip* | **ipv6** {*link-local-address* | *ipv6-address/prefix-length*} | **autoconfig**} [**exclusive**] [**decrement** *value*]
11. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface** *type number* 例： `Device(config)# interface gigabitethernet 2/0/2`	インターフェイスを設定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	**description** *string* 例： `Device(config-if)# description lan interface`	（任意）インターフェイス設定に説明を追加します。
ステップ 5	**encapsulation dot1q** *vlan-id* 例： `Device(config-if)# encapsulation dot1q 18`	インターフェイスで使用するカプセル化方式を設定します。
ステップ 6	**ip vrf forwarding** *name* 例： `Device(config-if)# ip vrf forwarding trust`	VPN ルーティングおよび転送（VRF）インスタンスをインターフェイスまたはサブインターフェイスに関連付けます。 • 指定された VRF が設定されていない場合、コマンドは設定されません。
ステップ 7	**ipv6 address** {*ipv6-prefix*/*prefix-length* | *prefix-name sub-bits*/*prefix-length*} 例： `Device(config-if)# ipv6 address 2001:0DB8:1:1:FFFF:FFFF:FFFF:FFFE/64`	IPv6 の一般的なプレフィックスに基づいて IPv6 アドレスを設定し、インターフェイスにおける IPv6 処理をイネーブルにします。
ステップ 8	**zone-member security** *zone-name* 例： `Device(config-if)# zone member security z1`	インターフェイスをゾーン メンバーとして設定します。 • *zone-name* 引数の場合、ファイアウォール設定時に **zone security** コマンドを使って設定したゾーンの 1 つを設定する必要があります。

	コマンドまたはアクション	目的
		• インターフェイスがセキュリティ ゾーン内にある場合、そのインターフェイスを通して送受信されるすべてのトラフィックはデフォルトでドロップされます（ただしルータ宛またはルータ発のトラフィックを除く）。ゾーン メンバーであるインターフェイスをトラフィックが通過できるようにするには、ポリシー適用対象のゾーン ペアにそのゾーンを含める必要があります。ポリシーの inspect または pass アクションによってトラフィックが許可される場合は、そのインターフェイスを通じてトラフィックが流れます。
ステップ 9	**redundancy rii** *RII-identifier* 例： `Device(config-if)# redundancy rii 100`	冗長グループで保護されたトラフィック インターフェイス用に RII を設定します。
ステップ 10	**redundancy group** *id* {**ip** *virtual-ip* | **ipv6** {*link-local-address* | *ipv6-address/prefix-length*} | **autoconfig**} [**exclusive**] [**decrement** *value*] 例： `Device(config-if)# redundancy group 1 ipv6 2001:0DB8:1:1:FFFF:FFFF:FFFF:FFFE/64 exclusive decrement 50`	冗長グループ（RG）トラフィック インターフェイス設定をイネーブルにします。
ステップ 11	**end** 例： `Device(config-if)# end`	インターフェイス コンフィギュレーション モードを終了し、特権 EXEC モードを開始します。

WAN トラフィック インターフェイスの設定

手順の概要

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **description** *string*
5. **ipv6 address** {*ipv6-prefix/prefix-length* | *prefix-name sub-bits/prefix-length*}
6. **zone-member security** *zone-name*
7. **ip tcp adjust-mss** *max-segment-size*
8. **redundancy rii** *RII-identifier*
9. **redundancy asymmetric-routing enable**
10. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface** *type number* 例： `Device(config)# interface gigabitethernet 2/1/0`	インターフェイスを設定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	**description** *string* 例： `Device(config-if)# description wan interface`	（任意）インターフェイス設定に説明を追加します。
ステップ 5	**ipv6 address** {*ipv6-prefix*/*prefix-length* | *prefix-name sub-bits*/*prefix-length*} 例： `Device(config-if)# ipv6 address 2001:DB8:2222::/48`	IPv6 の一般的なプレフィックスに基づいて IPv6 アドレスを設定し、インターフェイスにおける IPv6 処理をイネーブルにします。
ステップ 6	**zone-member security** *zone-name* 例： `Device(config-if)# zone-member security z2`	ファイアウォールを設定する際に、インターフェイスをゾーン メンバーとして設定します。 • *zone-name* 引数の場合、**zone security** コマンドを使用して設定済みのゾーンの 1 つを設定する必要があります。 • インターフェイスがセキュリティ ゾーン内にある場合、そのインターフェイスを通して送受信されるすべてのトラフィックはデフォルトでドロップされます（ただしルータ宛またはルータ発のトラフィックを除く）。ゾーン メンバーであるインターフェイスをトラフィックが通過できるようにするには、ポリシー適用対象のゾーン ペアにそのゾーンを含める必要があります。ポリシーの inspect または pass アクションによってトラフィックが許可される場合は、そのインターフェイスを通じてトラフィックが流れます。

	コマンドまたはアクション	目的
ステップ 7	**ip tcp adjust-mss** *max-segment-size* 例： `Device(config-if)# ip tcp adjust-mss 1360`	ルータを通過する TCP SYN パケットの最大セグメント サイズ（MSS）の値を調整します。
ステップ 8	**redundancy rii** *RII-identifier* 例： `Device(config-if)# redundancy rii 360`	冗長グループで保護されたトラフィック インターフェイス用に RII を設定します。
ステップ 9	**redundancy asymmetric-routing enable** 例： `Device(config-if)# redundancy asymmetric-routing enable`	冗長グループを、非対称ルーティングに使用されるインターフェイスに関連付けます。
ステップ 10	**end** 例： `Device(config-if)# end`	インターフェイス コンフィギュレーション モードを終了し、特権 EXEC モードを開始します。

IPv6 ファイアウォールの設定

IPv4 ファイアウォールと IPv6 ファイアウォールを設定する手順は同じです。IPv6 ファイアウォールを設定するには、IPv6 アドレス ファミリだけがマッチングされるようにクラス マップを設定する必要があります。

match protocol コマンドは IPv4 トラフィックと IPv6 トラフィックの両方に適用され、IPv4 ポリシーと IPv6 ポリシーのどちらにもこれを含めることができます。

手順の概要

1. **enable**
2. **configure terminal**
3. **vrf-definition** *vrf-name*
4. **address-family ipv6**
5. **exit-address-family**
6. **exit**
7. **parameter-map type inspect** *parameter-map-name*
8. **sessions maximum** セッション
9. **exit**
10. **ipv6 unicast-routing**
11. **ip port-map** *appl-name* **port** *port-num* **list** *list-name*
12. **ipv6 access-list** *access-list-name*
13. **permit ipv6 any any**
14. **exit**
15. **class-map type inspect match-all** *class-map-name*

16. **match access-group name** *access-group-name*
17. **match protocol** *protocol-name*
18. **exit**
19. **policy-map type inspect** *policy-map-name*
20. **class type inspect** *class-map-name*
21. **inspect** [*parameter-map-name*]
22. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを開始します。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**vrf-definition** *vrf-name* 例： `Device(config)# vrf-definition VRF1`	Virtual Routing and Forwarding（VRF）ルーティング テーブルインスタンスを設定し、VRF コンフィギュレーション モードを開始します。
ステップ 4	**address-family ipv6** 例： `Device(config-vrf)# address-family ipv6`	VRF アドレス ファミリ コンフィギュレーション モードを開始して、標準 IPv6 アドレス プレフィックスを伝送するセッションを設定します。
ステップ 5	**exit-address-family** 例： `Device(config-vrf-af)# exit-address-family`	VRF アドレス ファミリ コンフィギュレーション モードを終了し、VRF コンフィギュレーション モードを開始します。
ステップ 6	**exit** 例： `Device(config-vrf)# exit`	VRF コンフィギュレーション モードを終了して、グローバル コンフィギュレーション モードを開始します。
ステップ 7	**parameter-map type inspect** *parameter-map-name* 例： `Device(config)# parameter-map type inspect ipv6-param-map`	ファイアウォールのグローバル検査タイプ パラメータ マップを、検査アクションに関連するしきい値、タイムアウト、その他のパラメータに接続できるようにし、パラメータ マップ タイプ検査コンフィギュレーション モードを開始します。
ステップ 8	**sessions maximum** セッション 例： `Device(config-profile)# sessions maximum 10000`	ゾーン ペア上に存在可能な最大許容セッション数を設定します。

	コマンドまたはアクション	目的
ステップ 9	**exit** 例： `Device(config-profile)# exit`	パラメータ マップ タイプ検査コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードを開始します。
ステップ 10	**ipv6 unicast-routing** 例： `Device(config)# ipv6 unicast-routing`	IPv6 ユニキャスト データグラムの転送を有効にします。
ステップ 11	**ip port-map** *appl-name* **port** *port-num* **list** *list-name* 例： `Device(config)# ip port-map ftp port 8090 list ipv6-acl`	IPv6 アクセス コントロール リスト（ACL）を使用してポート/アプリケーション間マッピング（PAM）を確立します。
ステップ 12	**ipv6 access-list** *access-list-name* 例： `Device(config)# ipv6 access-list ipv6-acl`	IPv6 アクセスリストを定義し、IPv6 アクセス リスト コンフィギュレーション モードを開始します。
ステップ 13	**permit ipv6 any any** 例： `Device(config-ipv6-acl)# permit ipv6 any any`	IPv6 アクセス リストに許可条件を設定します。
ステップ 14	**exit** 例： `Device(config-ipv6-acl)# exit`	IPv6 アクセス リスト コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードを開始します。
ステップ 15	**class-map type inspect match-all** *class-map-name* 例： `Device(config)# class-map type inspect match-all ipv6-class`	アプリケーション固有の検査タイプ クラス マップを作成し、QoS クラス マップ コンフィギュレーション モードを開始します。
ステップ 16	**match access-group name** *access-group-name* 例： `Device(config-cmap)# match access-group name ipv6-acl`	指定した ACL をベースにクラス マップに対して一致基準を設定します。
ステップ 17	**match protocol** *protocol-name* 例： `Device(config-cmap)# match protocol tcp`	指定されたプロトコルに基づき、クラス マップの一致基準を設定します。
ステップ 18	**exit** 例： `Device(config-cmap)# exit`	QoS クラス マップ コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 19	**policy-map type inspect** *policy-map-name* 例： `Device(config)# policy-map type inspect ipv6-policy`	プロトコル固有の検査タイプ ポリシー マップを作成し、QoS ポリシーマップ コンフィギュレーション モードを開始します。
ステップ 20	**class type inspect** *class-map-name* 例： `Device(config-pmap)# class type inspect ipv6-class`	アクションの実行対象となるトラフィック クラスを指定し、QoS ポリシー マップ クラス コンフィギュレーション モードを開始します。
ステップ 21	**inspect** [*parameter-map-name*] 例： `Device(config-pmap-c)# inspect ipv6-param-map`	ステートフル パケット インスペクションをイネーブルにします。
ステップ 22	**end** 例： `Device(config-pmap-c)# end`	QoS ポリシーマップ クラス コンフィギュレーション モードを終了し、特権 EXEC モードを開始します。

ゾーンの設定とインターフェイスへのゾーンの適用

手順の概要

1. **enable**
2. **configure terminal**
3. **zone security** *zone-name*
4. **exit**
5. **zone security** *zone-name*
6. **exit**
7. **zone-pair security** *zone-pair-name* [**source** *source-zone* **destination** *destination-zone*]
8. **service-policy type inspect** *policy-map-name*
9. **exit**
10. **interface** *type number*
11. **ipv6 address** *ipv6-address/prefix-length*
12. **encapsulation dot1q** *vlan-id*
13. **zone-member security** *zone-name*
14. **end**
15. **show policy-map type inspect zone-pair sessions**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを開始します。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**zone security** *zone-name* 例： `Device(config)# zone security z1`	セキュリティ ゾーンを作成し、セキュリティ ゾーン コンフィギュレーション モードを開始します。
ステップ 4	**exit** 例： `Device(config-sec-zone)# exit`	セキュリティ ゾーン コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードを開始します。
ステップ 5	**zone security** *zone-name* 例： `Device(config)# zone security z2`	セキュリティ ゾーンを作成し、セキュリティ ゾーン コンフィギュレーション モードを開始します。
ステップ 6	**exit** 例： `Device(config-sec-zone)# exit`	セキュリティ ゾーン コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードを開始します。
ステップ 7	**zone-pair security** *zone-pair-name* [**source** *source-zone* **destination** *destination-zone*] 例： `Device(config)# zone-pair security in-2-out source z1 destination z2`	ゾーン ペアを作成し、セキュリティ ゾーンペア コンフィギュレーション モードを開始します。
ステップ 8	**service-policy type inspect** *policy-map-name* 例： `Device(config-sec-zone-pair)# service-policy type inspect ipv6-policy`	ポリシー マップをトップレベル ポリシーに関連付けます。
ステップ 9	**exit** 例： `Device(config-sec-zone-pair)# exit`	セキュリティ ゾーンペア コンフィギュレーション モードを終了し、グローバルコンフィギュレーション モードを開始します。
ステップ 10	**interface** *type number* 例： `Device(config)# interface gigabitethernet 0/0/0.1`	サブインターフェイスを設定し、サブインターフェイスコンフィギュレーションモードを開始します。

	コマンドまたはアクション	目的
ステップ 11	**ipv6 address** *ipv6-address/prefix-length* 例： `Device(config-subif)# ipv6 address 2001:DB8:2222:7272::72/64`	IPv6 の一般的なプレフィックスに基づいて IPv6 アドレスを設定し、インターフェイスまたはサブインターフェイスにおける IPv6 処理をイネーブルにします。
ステップ 12	**encapsulation dot1q** *vlan-id* 例： `Device(config-subif)# encapsulation dot1q 2`	インターフェイスで使用するカプセル化方式を設定します。
ステップ 13	**zone-member security** *zone-name* 例： `Device(config-subif)# zone member security z1`	インターフェイスをゾーン メンバーとして設定します。 • *zone-name* 引数の場合、**zone security** コマンドを使用して設定済みのゾーンの 1 つを設定する必要があります。 • インターフェイスがセキュリティ ゾーンにある場合、そのインターフェイスを通るトラフィックはどちらの方向でもすべて（デバイス宛またはデバイス発のトラフィックを除く）はデフォルトでドロップされます。トラフィックがゾーン メンバーであるインターフェイスを通過するには、そのゾーンをポリシーの適用先のゾーン ペアの一部にする必要があります。ポリシーの inspect または pass アクションによってトラフィックが許可される場合は、そのインターフェイスを通じてトラフィックが流れます。
ステップ 14	**end** 例： `Device(config-subif)# end`	サブインターフェイス コンフィギュレーション モードを終了して、特権 EXEC モードを開始します。
ステップ 15	**show policy-map type inspect zone-pair sessions** 例： `Device# show policy-map type inspect zone-pair sessions`	ポリシー マップは指定されたゾーン ペアに適用されるので、作成されたステートフル パケット インスペクション セッションを表示します。 • このコマンドの出力は、IPv4 と IPv6 の両方のファイアウォール セッションを表示します。

例

次に示す **show policy-map type inspect zone-pair sessions** コマンドの出力例は、IPv6 アドレスから IPpv4 アドレスへ（またはその逆）のパケット変換を表示します。

```
Device# show policy-map type inspect zone-pair sessions

  Zone-pair: in-to-out
  Service-policy inspect : in-to-out

    Class-map: ipv6-class (match-any)
      Match: protocol ftp
      Match: protocol tcp
      Match: protocol udp
      Inspect
        Established Sessions
         Session 110D930C [2001:DB8:1::103]:32847=>(209.165.201.2:21) ftp SIS_OPEN
          Created 00:00:00, Last heard 00:00:00
          Bytes sent (initiator:responder) [37:84]

        Half-open Sessions
         Session 110D930C [2001:DB8:1::104]:32848=>(209.165.201.2:21) ftp SIS_OPENING
          Created 00:00:00, Last heard 00:00:00
          Bytes sent (initiator:responder) [0:0]
```

次に示す **show policy-map type inspect zone-pair sessions** コマンドの出力例は、IPv6 アドレスから IPpv6 アドレスへのパケット変換を表示します。

```
Device# show policy-map type inspect zone-pair sessions

  Zone-pair: in-to-out
  Service-policy inspect : in-to-out

    Class-map: ipv6-class (match-any)
      Match: protocol ftp
      Match: protocol tcp
      Match: protocol udp
      Inspect
        Established Sessions
         Session 110D930C [2001:DB8:1::103]:63=>[2001:DB8:2::102]:63 udp SIS_OPEN
          Created 00:00:02, Last heard 00:00:01
          Bytes sent (initiator:responder) [162:0]
```

IPv6 ゾーンベース ファイアウォールに対するボックス ツーボックス ハイ アベイラビリティ サポートの設定例

例：冗長グループ プロトコルの設定

次に、hello time メッセージと hold time メッセージ用のタイマーが設定されている冗長グループを設定する例を示します。

```
Device# configure terminal
Device(config)# redundancy
Device(config-red)# application redundancy
Device(config-red-app)# protocol 1
Device(config-red-app-prtcl)# timers hellotime 3 holdtime 9
Device(config-red-app-prtcl)# authentication md5 key-string 0 n1 timeout 100
Device(config-red-app-prtcl)# bfd
Device(config-red-app-prtcl)# end
```

例：冗長アプリケーション グループの設定

次に、優先順位属性とプリエンプション属性のある group1 という名前の冗長グループを設定する例を示します。

```
Device# configure terminal
Device(config)# redundancy
Device(config-red)# application redundancy
Device(config-red-app)# group 1
Device(config-red-app-grp)# name group1
Device(config-red-app-grp)# priority 100 failover-threshold 50
Device(config-red-app-grp)# preempt
Device(config-red-app-grp)# track 200 decrement 200
Device(config-red-app-grp)# end
```

例：コントロール インターフェイスとデータ インターフェイスの設定

```
Device# configure terminal
Device(config-red)# application redundancy
Device(config-red-app-grp)# group 1
Device(config-red-app-grp)# data GigabitEthernet 0/0/0
Device(config-red-app-grp)# control GigabitEthernet 0/0/2 protocol 1
Device(config-red-app-grp)# timers delay 100 reload 400
Device(config-red-app-grp)# end
```

例：LAN トラフィック インターフェイスの設定

```
Device# configure terminal
Device(config-if)# interface gigabitethernet 2/0/2
Device(config-if)# description lan interface
Device(config-if)# encapsulation dot1q 18
Device(config-if)# ip vrf forwarding trust
Device(config-if)# ipv6 address 2001:0DB8:1:1:FFFF:FFFF:FFFF:FFFE/64
Device(config-if)# zone member security z1
Device(config-if)# redundancy rii 100
Device(config-if)# redundancy group 1 ipv6 2001:0DB8:1:1:FFFF:FFFF:FFFF:FFFE exclusive
decrement 50
Device(config-if)# end
```

例：WAN トラフィック インターフェイスの設定

次に、WAN-LAN シナリオ用の冗長グループを設定する例を示します。

```
Device# configure terminal
Device(config-if)# interface gigabitethernet 2/1/0
Device(config-if)# description wan interface
Device(config-if)# ipv6 address 2001:DB8:2222::/48
Device(config-if)# zone-member security z2
Device(config-if)# ip tcp adjust-mss 1360
Device(config-if)# redundancy rii 360
Device(config-if)# redundancy asymmetric-routing enable
Device(config-if)# end
```

例：IPv6 ファイアウォールの設定

```
Device# configure terminal
Device(config)# vrf-definition VRF1
Device(config-vrf)# address-family ipv6
Device(config-vrf-af)# exit-address-family
Device(config-vrf)# exit
Device(config)# parameter-map type inspect ipv6-param-map
Device(config-profile)# sessions maximum 10000
Device(config-profile)# exit
Device(config)# ipv6 unicast-routing
Device(config)# ip port-map ftp port 8090 list ipv6-acl
Device(config)# ipv6 access-list ipv6-acl
Device(config-ipv6-acl)# permit ipv6 any any
Device(config-ipv6-acl)# exit
Device(config)# class-map type inspect match-all ipv6-class
Device(config-cmap)# match access-group name ipv6-acl
Device(config-cmap)# match protocol tcp
Device(config-cmap)# exit
Device(config)# policy-map type inspect ipv6-policy
Device(config-pmap)# class type inspect ipv6-class
Device(config-pmap-c)# inspect ipv6-param-map
Device(config-pmap-c)# end
```

例：ゾーンの設定とインターフェイスへのゾーンの適用

```
Device# configure terminal
Device(config)# zone security z1
Device(config-sec-zone)# exit
Device(config)# zone security z2
Device(config-sec-zone)# exit
Device(config)# zone-pair security in-to-out source z1 destination z2
Device(config-sec-zone-pair)# service-policy type inspect ipv6-policy
Device(config-sec-zone-pair)# exit
Device(config)# interface gigabitethernet 0/0/0.1
Device(config-if)# ipv6 address 2001:DB8:2222:7272::72/64
Device(config-if)# encapsulation dot1q 2
Device(config-if)# zone member security z1
Device(config-if)# end
```

IPv6 ゾーンベース ファイアウォールに対するボックスツーボックス ハイ アベイラビリティ サポートに関する追加情報

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『Cisco IOS Master Command List, All Releases』
ファイアウォール コマンド	• 『Cisco IOS Security Command Reference: Commands A to C』 • 『Cisco IOS Security Command Reference: Commands D to L』 • 『Cisco IOS Security Command Reference: Commands M to R』 • 『Cisco IOS Security Command Reference: Commands S to Z』

シスコのテクニカル サポート

説明	リンク
右の URL にアクセスして、シスコのテクニカル サポートを最大限に活用してください。これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

IPv6 ゾーンベース ファイアウォールのボックスツーボックス ハイ アベイラビリティ サポートの機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *176 : IPv6* ゾーンベース ファイアウォールのボックスツーボックス ハイ アベイラビリティ サポートの機能情報

機能名	リリース	機能情報
IPv6 ゾーンベース ファイアウォールのボックスツーボックス ハイ アベイラビリティ サポート	Cisco IOS XE Release 3.8S	IPv6 ゾーンベース ファイアウォールのボックスツーボックス ハイ アベイラビリティ サポート機能では、IPv6 ファイアウォールの冗長グループ（RG）に基づいてハイ アベイラビリティ（HA）がサポートされています。この機能により、相互にバックアップとして動作するデバイスのペアを設定できます。この機能を設定し、複数のフェールオーバー条件に基づいてアクティブ デバイスを判断できます。 追加または変更されたコマンドはありません。
IPv6 ゾーン ベースのファイアウォールのボックスツーボックス ハイ アベイラビリティ サポート	Cisco IOS XE Release 3.8S	Cisco IOS XE リリース 3.10S では、Cisco ISR 4400 シリーズ ルータのサポートが追加されました。

第 132 章

ICMP のファイアウォール ステートフル インスペクション

ICMP のファイアウォール ステートフル インスペクションは、Internet Control Management Protocol バージョン 4（ICMPv4）メッセージを悪意のあるメッセージまたは無害なメッセージのいずれかに分類する機能です。ファイアウォールではステートフルインスペクションを使用して、プライベートネットワーク内で生成された無害なICMPv4メッセージを信頼し、関連付けられた ICMP 応答がネットワーク内に入ることを許可します。ICMP のファイアウォール ステートフルインスペクション機能は、侵入者がネットワークに入り込まないようICMPを使用してネットワークの問題をデバッグするネットワーク管理者に役立ちます。

このモジュールでは、ICMPv4メッセージのファイアウォールステートフルインスペクションの概要を紹介し、ICMPv4 メッセージを検査するようにファイアウォールを設定する方法を説明します。

ICMP のファイアウォール ステートフル インスペクションの前提条件

- ICMP のファイアウォール ステートフル インスペクション機能を設定するには、その前に、シスコ ファイアウォールを設定する必要があります。

- ネットワークで、すべての ICMP トラフィックにセキュリティ アプライアンス インターフェイスのパス スルーが許可される必要があります。
- セキュリティアプライアンスのインターフェイスで終端する ICMP トラフィックに対してアクセス ルールを設定する必要があります。

ICMP のファイアウォール ステートフル インスペクションの制約事項

この機能は UDP traceroute ユーティリティとは連動しません。この場合、ICMP パケットの代わりに UDP データグラムが送信されます。UDP traceroute は UNIX システムのデフォルトです。UNIX ホストでファイアウォールによって検査される ICMP traceroute パケットが生成されるようにするには、 **traceroute** コマンドで「-I」オプションを使用します。

ICMP のファイアウォール ステートフル インスペクションについて

ICMP のファイアウォール ステートフル インスペクションの概要

Internet Control Management Protocol（ICMP）は、ネットワークに関する情報を提供し、ネットワーク内のエラーを報告するネットワーク プロトコルです。ネットワーク管理者は ICMP を使用して、ネットワークの接続上の問題をデバッグします。ICMP を使用してプライベート ネットワークのトポロジを発見する可能性がある侵入者から保護するために、プライベート ネットワーク内に入らないように ICMPv4 メッセージをブロックすることはできますが、その場合、ネットワーク管理者がネットワークをデバッグできなくなります。

シスコ ルータでアクセス コントロール リスト（ACL）を使用することで、ICMPv4 メッセージを完全に許可または拒否するように設定できます。ICMPv4 メッセージに対して ACL を使用する場合、メッセージのインスペクションが、設定済みの allow または deny アクションよりも優先されます。

IP プロトコルを使用する ICMPv4 メッセージは、次の 2 つのタイプに分類することができます。

- 単純な要求/応答メカニズムを使用する情報メッセージ。
- IP パケットの配信中に何らかのエラーが発生したことを示すエラー メッセージ。

（注） ICMP 攻撃で宛先到達不能エラー メッセージが使用されないようにするために、1 つのセッションにつき 1 つの宛先到達不能メッセージだけがファイアウォールで許可されます。

ファイアウォールを経由する UDP セッションを処理しているホストが、宛先到達不能メッセージを含む ICMP エラー パケットを生成する場合があります。その場合、そのセッションでは 1 つの宛先到達不能メッセージだけがファイアウォールの通過を許可されます。

サポートされている ICMPv4 パケット タイプは以下のとおりです。

表 *177 : ICMPv4* パケット タイプ

パケット タイプ	名前	説明
0	エコー応答	エコー要求（タイプ 8）に対する応答。
3	到達不能	どの要求にも可能性のある応答。
8	エコー要求	ping または traceroute 要求。
11	時間超過	パケットの存続可能時間（TTL）のサイズがゼロの場合の応答。
13	タイムスタンプ要求	要求。
14	タイムスタンプ応答	タイムスタンプ要求（タイプ 13）に対する応答。

ICMPv4 パケット タイプ 0 と 8 は宛先に対する ping に使用されます。送信元がエコー要求パケットを送信すると、宛先はエコー応答パケットで応答します。パケット タイプ 0、8、および 11 は、ICMPv4 traceroute に使用されます（つまり、送信されるエコー要求パケットは、TTL サイズ 1 で開始されます）。TTL サイズはホップごとに増分されます。エコー要求パケットに対し、中間ホップは時間超過パケットで応答し、最終宛先はエコー応答パケットで応答します。

ICMPv4 エラー パケットが組み込みパケットである場合、その組み込みパケットは、該当するパケットに対して設定されたプロトコルとポリシーに応じて処理されます。たとえば、組み込みパケットが TCP パケットであり、そのパケットに対して drop アクションが設定されている場合、ICMPv4 では pass アクションを設定しているとしても、この組み込みパケットはドロップされます。

次のシナリオで、ICMPv4 パケットがファイアウォールをパス スルーするプロセスを説明します。

1. ICMPv4 パケットが送信元インターフェイスに到達します。ファイアウォールは、パケットの送信元アドレスと宛先アドレスを変更せずにそのまま使用して、パケット インスペクションを実行します。ファイアウォールは IP アドレス（送信元と宛先）、ICMP タイプ、およびプロトコルを使用してセッション キーの作成およびルックアップを行います。
2. パケットがファイアウォール インスペクションに合格します。
3. リターン トラフィックが宛先インターフェイスから戻ると、ファイアウォールは ICMPv4 メッセージ タイプに応じてセッション ルックアップ キーを作成します。
4. 1. 応答メッセージが情報メッセージの場合、ファイアウォールはパケットの送信元アドレスと宛先アドレスを変更せずにそのまま使用して、パケット インスペクションを実行します。ここで、宛先ポートは ICMPv4 メッセージの要求タイプです。
   2. 応答メッセージが ICMPv4 エラー メッセージの場合、ファイアウォールは ICMP エラー パケットに含まれるペイロード パケットを使用して、セッション ルックアップ用のセッション キーを作成します。
5. ファイアウォール セッション ルックアップが成功すると、パケットはファイアウォール インスペクションに合格します。

ICMP インスペクション チェック

ICMP の戻りパケットは、アクセス コントロール リスト（ACL）ではなくインスペクション コードによってチェックされます。インスペクション コードは各出力パケットの宛先アドレスをトラッキングし、返されるそれぞれのパケットをチェックします。エコー応答とタイムスタンプ応答のパケットについては、リターンアドレスがチェックされます。到達不能パケットおよび時間超過パケットについては、パケットデータから目的の宛先アドレスが抽出されてチェックされます。

ICMP のファイアウォール ステートフル インスペクションの設定方法

ICMP のファイアウォール ステートフル インスペクションの設定

次の項目を含む、ICMP のファイアウォール ステートフル インスペクションを設定しするには、この作業を実行します。

- ICMP トラフィックに一致するクラス マップ。
- 検査アクションを含むポリシー マップ。
- セキュリティ ゾーンおよびゾーン ペア（ファイアウォール ポリシー マップをゾーン ペアにアタッチするために必要）。

手順の概要

1. **enable**
2. **configure terminal**
3. **access-list** *access-list-number* {**deny | permit**} **icmp** *source source-wildcard destination destination-wildcard*
4. **class-map type inspect** *class-map-name*
5. **match protocol** *protocol-name*
6. **exit**
7. **policy-map type inspect** *policy-map-name*
8. **class** *class-map-name*
9. **inspect**
10. **exit**
11. **exit**
12. **zone security** *zone-name*
13. **exit**
14. **zone-pair security** *zone-pair-name* **source** *source-zone* **destination** *destination-zone*
15. **service-policy type inspect** *policy-map-name*
16. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**access-list** *access-list-number* {**deny	permit**} **icmp** *source source-wildcard destination destination-wildcard* 例： `Device(config)# access-list 102 permit icmp 192.168.0.1 255.255.255.0 192.168.2.22 255.255.255.0`	拡張 IP アクセス リストを定義します。
ステップ 4	**class-map type inspect** *class-map-name* 例： `Device(config)# class-map type inspect c1`	アクションの実行対象となるクラスを定義し、QoS クラスマップ コンフィギュレーション モードを開始します。
ステップ 5	**match protocol** *protocol-name* 例： `Device(config-cmap)# match protocol icmp`	指定されたプロトコルに基づき、クラス マップの一致基準を設定します。

	コマンドまたはアクション	目的
ステップ 6	**exit** 例： `Device(config-cmap)# exit`	QoS クラス マップ コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードを開始します。
ステップ 7	**policy-map type inspect** *policy-map-name* 例： `Device(config)# policy-map type inspect p1`	プロトコル固有の検査タイプ ポリシー マップを作成し、QoS ポリシーマップ コンフィギュレーション モードを開始します。
ステップ 8	**class** *class-map-name* 例： `Device(config-pmap)# class c1`	アクションの実行対象となるクラスを定義し、QoS ポリシーマップ クラス コンフィギュレーション モードを開始します。
ステップ 9	**inspect** 例： `Device(config-pmap-c)# inspect`	ステートフル パケット インスペクションをイネーブルにします。
ステップ 10	**exit** 例： `Device(config-pmap-c)# exit`	QoS ポリシーマップ クラス コンフィギュレーション モードを終了し、QoS ポリシー マップ コンフィギュレーション モードを開始します。
ステップ 11	**exit** 例： `Device(config-pmap)# exit`	QoS ポリシーマップ コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードを開始します。
ステップ 12	**zone security** *zone-name* 例： `Device(config)# zone security z1`	セキュリティ ゾーンを作成し、セキュリティ ゾーン コンフィギュレーション モードを開始します。 • 設定では送信元ゾーンと宛先ゾーンという、ゾーン ペアを作成するための 2 つのセキュリティ ゾーンが必要です。 • ゾーンペアでは、送信元ゾーンまたは宛先ゾーンとしてデフォルト ゾーンを使用できます。
ステップ 13	**exit** 例： `Device(config-sec-zone)# exit`	セキュリティ ゾーン コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードを開始します。
ステップ 14	**zone-pair security** *zone-pair-name* **source** *source-zone* **destination** *destination-zone* 例： `Device(config)# zone-pair security inout source z1 destination z2`	インターフェイスを割り当てることができるゾーンペアを作成し、セキュリティ ゾーンペア コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 15	**service-policy type inspect** *policy-map-name* 例： `Device(config-sec-zone-pair)# service-policy type inspect p1`	ファイアウォール ポリシー マップをゾーン ペアに付加します。
ステップ 16	**end** 例： `Device(config-sec-zone-pair)# end`	セキュリティ ゾーン ペア コンフィギュレーション モードを終了し、特権EXECモードを開始します。

ICMP のファイアウォール ステートフル インスペクションの確認

次の **show** コマンドは任意の順序で使用できます。

手順の概要

1. **enable**
2. **show ip access-lists**
3. **show policy-map type inspect** *policy-map-name*
4. **show policy-map type inspect zone-pair** *zone-pair-name*
5. **show zone security** *zone-name*
6. **show zone-pair security** [**source** *source-zone* **destination** *destination-zone*]

手順の詳細

ステップ 1 enable

例：

```
Device> enable
```

特権 EXEC モードを有効にします。

- パスワードを入力します（要求された場合）。

ステップ 2 show ip access-lists

例：

```
Device# show ip access-lists
```

指定されたポリシー マップに関する情報を表示します。

ステップ 3 show policy-map type inspect *policy-map-name*

例：

```
Device# show policy-map type inspect p1
```

指定されたポリシー マップに関する情報を表示します。

ステップ 4 **show policy-map type inspect zone-pair** *zone-pair-name*

例：

```
Device# show policy-map type inspect zone-pair inout
```

ゾーン ペアのランタイム検査タイプ ポリシー マップ統計情報を表示します。

ステップ 5 **show zone security** *zone-name*

例：

```
Device# show zone security z1
```

ゾーン セキュリティ情報を表示します。

ステップ 6 **show zone-pair security** [**source** *source-zone* **destination** *destination-zone*]

例：

```
Device# show zone-pair security source z1 destination z2
```

送信元および宛先のゾーンとゾーン ペアに付加されたポリシーを表示します。

例：

次に示す **show ip access-lists** コマンドの出力例は、ホストから ping パケットのみが発行された ICMP セッションに対して ACL が作成されるしくみを示します。

```
Device# show ip access-lists

 Extended IP access list 102
     permit icmp any host 192.168.133.3 time-exceeded
     permit icmp any host 192.168.133.3 unreachable
     permit icmp any host 192.168.133.3 timestamp-reply
     permit icmp any host 192.168.133.3 echo-reply (4 matches)
```

次に、**show policy-map type inspect p1** コマンドの出力例を示します。

```
Device# show policy-map type inspect p1

 Policy Map type inspect p1
  Class c1
   Inspect
```

次に、**show policy-map type inspect zone-pair inout** コマンドの出力例を示します。

```
Device# show policy-map type inspect zone-pair inout

 Zone-pair: inout
  Service-policy : p1
   Class-map: c1 (match-all)
    Match: protocol icmp
    Inspect
     Session creations since subsystem startup or last reset 0
     Current session counts (estab/half-open/terminating) [0:0:0]
     Maxever session counts (estab/half-open/terminating) [0:0:0]
     Last session created never
     Last statistic reset never
```

```
    Last session creation rate 0
    half-open session total 0
  Class-map: class-default (match-any)
   Match: any
   Drop
    0 packets, 0 bytes
```

次に、**show zone security** コマンドの出力例を示します。

```
Device# show zone security

zone self
Description: System defined zone
```

次に、**show zone-pair security** コマンドの出力例を示します。

```
Device# show zone-pair security source z1 destination z2

zone-pair name inout
  Source-Zone z1  Destination-Zone z2
  service-policy p1
```

ICMP のファイアウォール ステートフル インスペクションの設定例

例：ICMP のファイアウォール ステートフル インスペクションの設定

```
Device# configure terminal
Device(config)# access-list 102 permit icmp 192.168.0.1 255.255.255.0 192.168.2.22
255.255.255.0
Device(config)# class-map type inspect c1
Device(config-cmap)# match protocol icmp
Device(config-cmap)# exit
Device(config)# policy-map type inspect p1
Device(config-pmap)# class c1
Device(config-pmap-c)# inspect
Device(config-pmap-c)# exit
Device(config-pmap)# exit
Device(config)# zone security z1
Device(config-sec-zone)# exit
Device(config)# zone security z2
Device(config-sec-zone)# exit
Device(config)# zone-pair security inout source z1 destination z2
Device(config-sec-zone-pair)# service-policy type inspect p1
Device(config-sec-zone-pair)# end
```

ICMP のファイアウォール ステートフル インスペクションに関する追加情報

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『Master Command List』、すべてのリリース
セキュリティ コマンド	• 『Security Command Reference: Commands A to C』 • 『Security Command Reference: Commands D to L』 • 『Security Command Reference: Commands M to R』 • 『Security Command Reference: Commands S to Z』

標準と RFC

標準および RFC	タイトル
RFC 792	インターネット制御メッセージプロトコル（*ICMP*）
RFC 950	『*Internet Standard Subnetting Procedure*』
RFC 1700	『*Assigned Numbers*』

シスコのテクニカル サポート

説明	リンク
右の URL にアクセスして、シスコのテクニカル サポートを最大限に活用してください。これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

ICMP のファイアウォール ステートフル インスペクションに関する機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *178 : ICMP* のファイアウォール ステートフル インスペクションに関する機能情報

機能名	リリース	機能情報
ICMP のファイアウォール ステートフルインスペクション	Cisco IOS XE リリース 2.1 Cisco IOS XE リリース 3.2S	ICMP のファイアウォール ステートフル インスペクション機能は、ICMPv4 メッセージを「悪意のある」と「無害」のどちらかに分類します。ファイアウォールは、ステートフルインスペクションを使用して、プライベートネットワーク内で生成された無害の ICMP メッセージを信頼し、関連する ICMP 応答のエントリを許可します。

第 133 章

LISP とゾーンベース ファイアウォールの統合と相互運用性

LISP およびゾーンベース ファイアウォールの統合および相互運用性の機能により、デバイスをパス スルーするすべての Locator/ID Separation Protocol（LISP）データ パケットの内部パケット インスペクションが可能になります。LISP 内部パケットインスペクションを有効にするには、**lisp inner-packet inspection** コマンドを設定する必要があります。LISP 内部パケット インスペクションが行われないと、LISP ネットワーク内のエンドポイント ID（EID）デバイスはファイアウォールで保護されません。

このモジュールでは、この機能を設定する方法を説明します。

LISP とゾーンベース ファイアウォールの統合と相互運用性に関する機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *179 : LISP* とゾーンベース ファイアウォールの統合と相互運用性に関する機能情報

機能名	リリース	機能情報
LISP とゾーンベース ファイアウォールの統合と相互運用性	Cisco IOS XE リリース 3.13S	LISP およびゾーンベース ファイアウォールの統合および相互運用性の機能により、デバイスをパス スルーするすべての Locator/ID Separation Protocol（LISP）データ パケットの内部パケット インスペクションが可能になります。LISP 内部パケット インスペクションを有効にするには、lisp inner-packet inspection コマンドを設定する必要があります。LISP 内部インスペクションを使用しない場合は、LISP ネットワーク内のエンドポイント識別子（EID）デバイスにファイアウォール保護が設定されません。 この機能により、次のコマンドが導入または変更されました。**lisp inner-packet-inspection**、**show parameter-map type inspect-global**、および **show parameter-map type inspect global**。
ゾーンベース ファイアウォールおよび LISP 統合のシャーシ内およびシャーシ間ハイ アベイラビリティ	Cisco IOS XE リリース 3.14S	Cisco IOS XE リリース 3.14S では、LISP およびゾーンベース ファイアウォール統合および相互運用性機能により、シャーシ内ハイ アベイラビリティとシャーシ間ハイ アベイラビリティの両方がサポートされています。 この機能によって導入または変更されたコマンドはありません。

LISP およびゾーンベース ファイアウォールの統合と相互運用性の前提条件

- アクティブ デバイスとスタンバイ デバイスのシャーシ間高可用性設定は同一でなければなりません。

LISP およびゾーンベース ファイアウォールの統合と相互運用性に関する制約事項

次の機能はサポートされていません。

- Locator ID Separator Protocol（LISP）モビリティ
- ゾーンベース ファイアウォール、LISP 、および Web Cache Control Protocol（WCCP）の相互運用性
- VRF 相互運用性を備えたゾーンベース ファイアウォールと LISP サブインターフェイス

LISP 内部パケットインスペクションが有効な場合、次の機能はサポートされません。

- 非対称ルーティング
- LISP 制御メッセージ インスペクション
- LISP 内部パケット フラグメンテーション
- ネットワーク アドレス変換（NAT）および NAT 64
- TCP リセット
- VPN ルーティングおよび転送（VRF）
- 仮想 TCP（vTCP）
- VRF 対応ソフトウェア インフラストラクチャ（VASI）
- Web Cache Communication Protocol（WCCP）

LISP とゾーンベース ファイアウォールの統合と相互運用性に関する情報

LISP の概要

Locator/ID Separation Protocol（LISP）は、ネットワーク アーキテクチャ兼プロトコルです。LISP は、単一の IP アドレスを 2 つのナンバリング スペースで置き換えます。ナンバリング スペースの一方は、ネットワーク接続ポイントにトポロジ的に割り当てられ、そのネットワーク経由のパケットのルーティングおよび転送に使用されるルーティング ロケータ（RLOC）です。もう一方は、ネットワーク トポロジとは関係なく割り当てられ、ナンバリング デバイスに使用されて管理境界で集約されるエンドポイント ID です。

LISP が定義しているのは、これら 2 つのナンバリング スペースをマッピングし、ルーティング不可能な EID を使用してデバイスから発信されたトラフィックを、ルーティングと転送に RLOC を使用するネットワーク インフラストラクチャで転送できるようにカプセル化するための機能です。LISP では、デバイスがルーティング不可能な EID をルーティング可能な RLOC にマップする際に使用する情報を交換するための一連の機能を提供しています。

LISP を使用するには、LISP 関連の 1 つ以上のデバイス（LISP 出力トンネル ルータ（ETR）、入力トンネル ルータ（ITR）、プロキシ ETR（PETR）、Proxy Ingress Tunnel Router（PITR）、マップ リゾルバ（MR）、マップ サーバ（MS）、LISP 代替論理トポロジ（ALT）デバイスなど）からなる LISP 固有の構成が必要です。

ゾーンベース ファイアウォールと LISP の相互運用性の概要

ゾーンベース ファイアウォールは、ネットワーク内でのエッジ ルータ（Cisco ASR 1000 アグリゲーション サービス ルータなどのルータ）の配置場所に応じて、Locator/ID Separation Protocol（LISP）xTR デバイスのサウスバウンドまたはノースバウンドに導入できます。入力トンネル ルータ（ITR）と出力トンネル ルータ（ETR）は xTR デバイスと総称されています。

ゾーンベース ファイアウォールが xTR デバイスのノースバウンドに位置する場合、ファイアウォールはネットワークをパス スルーする LISP カプセル化パケット（LISP トンネル化パケットなど）を確認できます。

ゾーンベース ファイアウォールが xTR デバイスのサウスバウンドに位置する場合、ファイアウォールはオリジナル パケットを確認できます。ただし、ゾーンベース ファイアウォールが LISP xTR 処理を認識したり、LISP ヘッダーを確認することはできません。出力パケットについては、xTR デバイスはファイアウォール インスペクションの後に LISP カプセル化を行い、LISP ヘッダーをオリジナル パケットの先頭に追加します。入力パケットについては、xTR デバイスはファイアウォール インスペクションの前に LISP カプセル化解除（LISP ヘッダーの削除）を行うため、ファイアウォール インスペクションではオリジナル パケットだけを検査します。したがって、LISP との対話はありません。

この項では、LISP xTR デバイスのサウスバウンドでゾーンベース ファイアウォールを導入する場合のシナリオを説明します:

LISP カプセル化およびカプセル化解除機能を実行する LISP xTR としてエッジ ルータを設定する場合、ゾーンベース ファイアウォールは、LISP インターフェイスと同じエッジ ルータ上の LISP ローカル エンドポイント ID（EID）デバイスに対応するインターフェイスとの間に設定できます。LISP ヘッダーのカプセル化解除は、LISP インターフェイスに位置するゾーンベース ファイアウォールにヘッダーが入力される前に実行されます。LISP ヘッダーのカプセル化は、LISP インターフェイスに位置するゾーンベース ファイアウォールからパケットが出力された後に実行されます。ファイアウォールは EID スペースのネイティブ トラフィックだけを検査します。

この項では、LISP xTR デバイスのノースバウンドでゾーンベース ファイアウォールを導入する場合のシナリオを説明します。

xTR デバイスのノースバウンドでロード シェアリング ルータとして複数のエッジ ルータを導入する場合、エッジ ルータ上のファイアウォールは xTR デバイスのノースバウンドと見なされます。この場合、ゾーンベース ファイアウォールをパス スルーするすべてのパケットが、

LISP カプセル化パケットになります。パケットが到着すると、ファイアウォールは LISP パケットの内部ヘッダーまたは外部ヘッダーのいずれかを検査します。デフォルトでは、外部ヘッダーだけが検査されます。内部ヘッダーのインスペクションを有効にするには、**lisp inner-packet-inspection** コマンドを使用します。

Cisco IOS XE リリースでは、LISP 内部パケット インスペクションが有効にされていると、ファイアウォールはフラグメント化された最初の内部パケットだけを検査し、後続の内部パケットはインスペクションされずにファイアウォールをパス スルーします。LISP 内部パケット インスペクションが有効になっている場合、LISP インスタンス ID が Virtual Routing and Forwarding（VRF）ID として扱われ、異なるインスタンス ID に属する LISP パケットは別のゾーンベース ファイアウォール セッションに関連付けられます。

LISP 機能の相互運用性

Cisco IOS XE リリース 3.13S では LISP およびゾーンベース ファイアウォール統合および相互運用性機能が次の機能と連携します。

- IPv4 内部ヘッダーおよび外部ヘッダー
- IPv6 内部ヘッダーおよび外部ヘッダー
- LISP マルチテナンシー
- アプリケーション レイヤ ゲートウェイ（ALG）
- アプリケーション インスペクションおよびコントロール（AIC）
- マルチプロトコル ラベル スイッチング（MPLS）
- インサービス ソフトウェア アップグレード（ISSU）
- PxTR ケース

ゾーンベース ファイアウォールおよび LISP 統合のシャーシ内およびシャーシ間ハイ アベイラビリティ

Cisco IOS XE リリース 3.14S では、LISP およびゾーンベース ファイアウォール統合および相互運用性機能により、シャーシ内ハイ アベイラビリティとシャーシ間ハイ アベイラビリティの両方がサポートされています。Location/ID Separation Protocol（LISP）内部パケット インスペクションが有効な場合、xTR ノースバウンド デバイスでシャーシ内およびシャーシ間冗長性がサポートされています。

ノースバウンド デバイスでの LISP 内部パケット インスペクションでは、LISP インスタンス ID が Virtual Routing and Forwarding（VRF）インスタンスとして使用されます。LISP 内部パケット インスペクションが有効な場合、ノースバウンド デバイスの VRF 設定は無視されます。

2 つのデバイスが xTR デバイスのノースバウンドに配置されており、xTR デバイスがクラウド内部に配置されている場合、この両方のデバイスで LISP 内部パケット インスペクションが有

効であると、LISP 内部パケット フローに対して作成されたゾーンベース ファイアウォール セッションがスタンバイ デバイスと同期されます。

一般的なシャーシ間（ボックスツーボックス）ハイ アベイラビリティ トポロジでは、xTR デバイスのノースバウンドのルーティング ロケータ（RLOC）スペースに 2 つのデバイスがあります。xTR デバイスは、内部ネットワークに配置されます。LISP 内部パケット インスペクションがこの両方のデバイスで有効であると、LISP 内部パケットに対して作成されたゾーンベース ファイアウォール セッションがスタンバイ デバイスと同期されます。

シャーシ内冗長性については設定の変更はありません。

LISP とゾーンベース ファイアウォールの統合と相互運用性の設定方法

LISP 内部パケット インスペクションの有効化

parameter-map type inspect global コマンドまたは **parameter-map type inspect-global** コマンドを設定した後で、LISP 内部パケットインスペクションを設定できます。

（注） これらのコマンドの両方を同時には設定できません。

手順の概要

1. **enable**
2. **configure terminal**
3. **parameter-map type inspect global**
4. **lisp inner-packet-inspection**
5. **end**
6. **show parameter-map type** {**inspect global** | **inspect-global**}

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 3	**parameter-map type inspect global** 例： `Device(config)# parameter-map type inspect global`	接続しきい値、タイムアウト、およびその他の検査アクションに関連するパラメータのグローバル検査タイプパラメータ マップを設定し、パラメータ マップ タイプ検査コンフィギュレーション モードを開始します。
ステップ 4	**lisp inner-packet-inspection** 例： `Device(config-profile)# lisp inner-packet-inspection`	LISP 内部パケット インスペクションをイネーブルにします。
ステップ 5	**end** 例： `Device(config-profile)# end`	パラメータ マップ タイプ検査コンフィギュレーション モードを終了して、特権 EXEC モードに戻ります。
ステップ 6	**show parameter-map type** {**inspect global** | **inspect-global**} 例： `Device# show parameter-map type inspect-global`	グローバル検査タイプ パラメータ マップ情報を表示します。

例

次に示す **show parameter-map type inspect-global** コマンドの出力例は、LISP 内部パケットインスペクションが有効であることを表示します。

```
Device# show parameter-map type inspect-global

parameter-map type inspect-global
  log dropped-packet off
  alert on
  aggressive aging disabled
  syn_flood_limit  unlimited
  tcp window scaling enforcement loose off
  max incomplete unlimited  aggressive aging disabled
  max_incomplete TCP unlimited
  max_incomplete UDP unlimited
  max_incomplete ICMP unlimited
  application-inspect all
  vrf default inspect vrf-default
  vrf vrf2 inspect vrf-default
  vrf vrf3 inspect vrf-default
  lisp inner-packet-inspection
```

LISP 内部パケット インスペクションのシャーシ間ハイ アベイラビリティの設定

シャーシ間ハイ アベイラビリティのための xTR サウスバウンド インターフェイスの設定

始める前に

前提条件

- ゾーンとゾーン ペアを設定する必要があります。
- 冗長性と冗長グループを設定する必要があります。詳細については、『*Zone-Based Policy Firewall Configuration Guide*』の「Configuring Firewall Stateful Interchassis Redundancy」モジュールを参照してください。

手順の概要

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **vrf forwarding** *vrf-name*
5. **description** *string*
6. **ip address** *ip-address mask*
7. **exit**
8. **interface** *type number*
9. **description** *string*
10. **zone-member security** *zone-name*
11. **exit**
12. **interface** *type number*
13. **description** *string*
14. **ip address** *ip-address mask*
15. **zone-member security** *zone-name*
16. **cdp enable**
17. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。

	コマンドまたはアクション	目的
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface** *type number* 例： `Device(config)# interface TenGigabitEthernet 1/3/0`	インターフェイスを設定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	**vrf forwarding** *vrf-name* 例： `Device(config-if)# vrf forwarding lower`	VRF インスタンスまたは仮想ネットワークをインターフェイスまたはサブインターフェイスに関連付けます。
ステップ 5	**description** *string* 例： `Device(config-if)# description facing RLOC and the LISP cloud; has a LISP header.`	インターフェイスの設定に説明を加えます。 • ゾーンベース ファイアウォールは、このインターフェイスには設定できません。
ステップ 6	**ip address** *ip-address mask* 例： `Device(config-if)# ip address 192.0.1.27 255.255.255.0`	インターフェイスに対するプライマリ IP アドレスまたはセカンダリ IP アドレスを設定します。
ステップ 7	**exit** 例： `Device(config-if)# exit`	インターフェイス設定モードを終了し、グローバル設定モードに戻ります。
ステップ 8	**interface** *type number* 例： `Device(config)# interface LISP 0`	インターフェイスを設定し、インターフェイス コンフィギュレーション モードを開始します。 • これは LISP 仮想インターフェイスです。

ステップ 9	**description** *string*
	例：
	`Device(config-if)# description LISP virtual interface.`
	`Adds LISP header after firewall inspection or removes LISP header before firewall inspection.`
		インターフェイスの設定に説明を加えます。

ステップ 10	**zone-member security** *zone-name* 例： `Device(config-if)# zone-member security ge0-0-3a`	インターフェイスをセキュリティ ゾーンにアタッチします。
ステップ 11	**exit** 例：	インターフェイス設定モードを終了し、グローバル設定モードに戻ります。

	コマンドまたはアクション	目的
	`Device(config-if)# exit`	
ステップ 12	**interface** *type number* 例： `Device(config)# interface tengigabitethernet 0/3/0`	インターフェイスを設定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 13	**description** *string* 例： `Device(config-if)# description facing internal network, does not have a LISP header.`	インターフェイスの設定に説明を加えます。
ステップ 14	**ip address** *ip-address mask* 例： `Device(config-if)# ip address 192.0.2.5 255.255.255.0`	インターフェイスに対するプライマリ IP アドレスまたはセカンダリ IP アドレスを設定します。
ステップ 15	**zone-member security** *zone-name* 例： `Device(config-if)# zone-member security ge0-0-0`	インターフェイスをセキュリティ ゾーンにアタッチします。
ステップ 16	**cdp enable** 例： `Device(config-if)# cdp enable`	インターフェイスで Cisco Discovery Protocol（CDP）を有効にします。
ステップ 17	**end** 例： `Device(config-if)# end`	インターフェイス コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

LISP 内部パケット インスペクションのための xTR ノースバウンド インターフェイスの設定

この設定では、ノースバウンドで LISP ヘッダーが検査されないので、Locator ID Separation Protocol（LISP）仮想インターフェイスは必要ありません。ただし、ゾーンベースのファイアウォールを設定して、LISP 内部パケットまたは外部パケットのどちらかを検査できます。

始める前に

- ゾーンとゾーン ペアを設定する必要があります。
- 冗長性と冗長グループを設定する必要があります。詳細については、『*Zone-Based Policy Firewall Configuration Guide*』の「Configuring Firewall Stateful Interchassis Redundancy」モジュールを参照してください。

手順の概要

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **description** *string*
5. **ip address** *ip-address mask*
6. **zone-member security** *zone-name*
7. **negotiation auto**
8. **redundancy rii** *id*
9. **redundancy group** *id* **ip** *virtual-ip* **exclusive decrement** *value*
10. **exit**
11. **interface** *type number*
12. **description** *string*
13. **ip address** *ip-address mask*
14. **zone-member security** *zone-name*
15. **negotiation auto**
16. **redundancy rii** *id*
17. **redundancy group** *id* **ip** *virtual-ip* **exclusive decrement** *value*
18. **ip virtual-reassembly**
19. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface** *type number* 例： `Device(config)# interface GigabitEthernet 1/2/1`	インターフェイスを設定し、インターフェイス コンフィギュレーション モードを開始します。 • このインターフェイスは LISP パケット全体を認識できます。
ステップ 4	**description** *string* 例： `Device(config-if)# description RLOC-space/north LAN`	インターフェイスの設定に説明を加えます。
ステップ 5	**ip address** *ip-address mask* 例：	インターフェイスに対するプライマリ IP アドレスまたはセカンダリ IP アドレスを設定します。

	コマンドまたはアクション	目的
	`Device(config-if)# ip address 198.51.100.8 255.255.255.0`	
ステップ 6	**zone-member security** *zone-name* 例： `Device(config-if)# zone-member security ge0-0-3`	インターフェイスをセキュリティ ゾーンにアタッチします。
ステップ 7	**negotiation auto** 例： `Device(config-if)# negotiation auto`	ギガビット イーサネット インターフェイス上で速度、デュプレックス モード、およびフロー制御のアドバタイズをイネーブルにします。
ステップ 8	**redundancy rii** *id* 例： `Device(config-subif)# redundancy rii 200`	冗長グループが保護するトラフィック インターフェイス用に冗長インターフェイス識別子（RII）を設定します。
ステップ 9	**redundancy group** *id* **ip** *virtual-ip* **exclusive decrement** *value* 例： `Device(config-if)# redundancy group 1 ip 198.51.100.12 exclusive decrement 50`	冗長グループ（RG）トラフィック インターフェイス設定をイネーブルにします。
ステップ 10	**exit** 例： `Device(config-if)# exit`	インターフェイス設定モードを終了し、グローバル設定モードに戻ります。
ステップ 11	**interface** *type number* 例： `Device(config)# interface GigabitEthernet 0/0/3`	インターフェイスを設定し、インターフェイス コンフィギュレーション モードを開始します。 • このインターフェイスは LISP パケット全体を認識できます。
ステップ 12	**description** *string* 例： `Device(config-if)# description RLOC-space/south LAN`	インターフェイスの設定に説明を加えます。
ステップ 13	**ip address** *ip-address mask* 例： `Device(config-if)# ip address 198.51.100.27 255.255.255.0`	インターフェイスに対するプライマリ IP アドレスまたはセカンダリ IP アドレスを設定します。
ステップ 14	**zone-member security** *zone-name* 例： `Device(config-if)# zone-member security ge0-0-0`	インターフェイスをセキュリティ ゾーンにアタッチします。

	コマンドまたはアクション	目的
ステップ 15	**negotiation auto** 例： `Device(config-if)# negotiation auto`	ギガビット イーサネット インターフェイス上で速度、デュプレックス モード、およびフロー制御のアドバタイズをイネーブルにします。
ステップ 16	**redundancy rii** *id* 例： `Device(config-subif)# redundancy rii 300`	冗長グループが保護するトラフィック インターフェイス用に冗長インターフェイス識別子（RII）を設定します。
ステップ 17	**redundancy group** *id* **ip** *virtual-ip* **exclusive decrement** *value* 例： `Device(config-if)# redundancy group 1 ip 194.88.4.1 exclusive decrement 50`	RG トラフィック インターフェイス設定を有効にします。
ステップ 18	**ip virtual-reassembly** 例： `Device(config-if)# ip virtual-reassembly`	インターフェイス上の仮想フラグメント再構成（VFR）を有効にします。
ステップ 19	**end** 例： `Device(config-if)# end`	インターフェイス コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

LISP とゾーンベース ファイアウォールの統合と相互運用性の設定例

例：LISP 内部パケット インスペクションの有効化

```
Device# configure terminal
Device(config)# parameter-map type inspect-global
Device(config-profile)# lisp inner-packet-inspection
Device(config-profile)# end
```

次に、LISP 内部パケット インスペクションを有効にしたゾーンベース ファイアウォール設定の例を示します。

```
 address-family ipv4
 exit-address-family
 !
 address-family ipv6
 exit-address-family

class-map type inspect match-any c-ftp-tcp
```

```
 match protocol ftp
 match protocol telnet
 match protocol http
 match protocol tcp
 match protocol udp
!
policy-map type inspect p1
 class type inspect c-ftp-tcp
  inspect
 class class-default
!
zone security ge0-0-0
!
zone security ge0-0-3
!
zone-pair security zp-ge000-ge003 source ge0-0-0 destination ge0-0-3
 service-policy type inspect p1
!
zone-pair security zp-ge003-ge000 source ge0-0-3 destination ge0-0-0
 service-policy type inspect p1
!
interface TenGigabitEthernet 1/3/0
 ip address 192.168.1.1 255.255.255.0
 ipv6 address 2001:DB8:100::2/64
 zone-member security ge0-0-0
!
interface TenGigabitEthernet 0/3/0
 ip address 192.168.2.1 255.255.255.0
 ipv6 address 2001:DB8:200::2/64
 zone-member security ge0-0-3
!
parameter-map type inspect global
 lisp inner-packet-inspection
 log dropped-packet off
  alert on
!
```

LISP 内部パケット インスペクションのシャーシ間ハイ アベイラビリティの設定

LISP とゾーンベース ファイアウォールの統合と相互運用性に関する追加情報

関連資料

関連項目	マニュアル タイトル
Cisco コマンド	『Master Command List, All Releases』

関連項目	マニュアル タイトル
セキュリティ コマンド	• 『Security Command Reference: Commands A to C』 • 『Security Command Reference: Commands D to L』 • 『Security Command Reference: Commands M to R』 • 『Security Command Reference: Commands S to Z』
LISP コマンド	『Cisco IOS IP Routing: LISP Command Reference』
LISP 設定ガイド	『*IP Routing: LISP Configuration Guide*』

標準および RFC

標準/RFC	タイトル
RFC 6830	『*The Locator/ID Separation Protocol (LISP)*』

シスコのテクニカル サポート

説明	リンク
シスコのサポート Web サイトでは、シスコの製品やテクノロジーに関するトラブルシューティングにお役立ていただけるように、マニュアルやツールをはじめとする豊富なオンライン リソースを提供しています。 お使いの製品のセキュリティ情報や技術情報を入手するために、Cisco Notification Service（Field Notice からアクセス）、Cisco Technical Services Newsletter、Really Simple Syndication（RSS）フィードなどの各種サービスに加入できます。 シスコのサポート Web サイトのツールにアクセスする際は、Cisco.com のユーザ ID およびパスワードが必要です。	http://www.cisco.com/support

第 134 章

アプリケーション認識型ファイアウォール

このドキュメントでは、NBAR が検出してゾーンベース ファイアウォール アプリケーションを認識させることができるアプリケーションに基づいて、ゾーンベース ファイアウォール ポリシーを定義する方法について説明します。アプリケーションファイアウォールは、トラフィックを検査し、アプリケーション、カテゴリ、アプリケーションファミリ、またはアプリケーショングループに基づいてトラフィックをブロックします。このアプリケーション認識型ファイアウォールの機能には、次の利点があります。

- アプリケーションの可視性ときめ細かな制御
- 1400 以上のレイヤ 7 アプリケーションの分類
- アプリケーション、カテゴリ、アプリケーションファミリ、またはアプリケーショングループごとのトラフィックの許可またはブロック

アプリケーション認識型ファイアウォールに関する機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

機能名	リリース	機能情報
アプリケーション認識型ゾーンベースFW	Cisco IOS XE Fuji 16.9.1	このドキュメントでは、NBARが検出してゾーンベース ファイアウォール アプリケーションを認識させることができるアプリケーションに基づいて、ゾーンベース ファイアウォール ポリシーを定義する方法について説明します。アプリケーション ファイアウォールは、トラフィックを検査し、アプリケーション、カテゴリ、アプリケーションファミリ、またはアプリケーショングループに基づいてトラフィックをブロックします。 次のコマンドが導入または変更されました： **show class-map***avc-classmap-name* **show policy-map type inspect zone-pair** **show policy-map type inspect zone-pair sessions** **show policy-map type inspect avc** **show platform hardware qfpactive feature firewall drop**

ゾーンベース FW でのアプリケーション認識に関する情報

アプリケーション認識型ファイアウォールの前提条件

- トラフィックがレイヤ3/レイヤ4検査クラスマップと一致していることを確認します。トラフィックがファイアウォール検査に一致しない場合、AVC ポリシーはトラフィックを認識できません。
- AVC サービスポリシーが適用されている同じクラスマップの DNS を検査します。

アプリケーション認識型ゾーンベース FW に関する制約事項

- セルフゾーンへのトラフィックはサポートされません。
- AVC 検査ポリシーは、すべてのアプリケーションを許可し、特定のアプリケーションのみを拒否する必要があります。これは、多くのアプリケーションが相互に依存しているため、あるアプリケーションを許可し、他のすべてのアプリケーションを拒否することは常に機能するわけではないためです。

- 各アプリケーション クラスマップは、最大 16 のフィルタ（各一致がフィルタと見なされます）を持つことができます。
- AVC ポリシーマップは、最大 32 のクラスマップ（class-default を含む）を持つことができます。
- **match protocol attribute category** コマンドを使用してカテゴリを指定する場合は、**match protocol attribute application-family** または **match protocol attribute application-group** を設定できません。

クラスマップやポリシーマップを設定する前に、**parameter-map type inspect** を使用して、ドロップされたパケットをログに記録するようにパラメータマップタイプを設定してください。

```
Device (config)# parameter-map type inspect
Device (config-map)# log dropped-packets
```

ネットワークレイヤ L3/L4 に基づくポリシー

ゾーンベース ファイアウォールは、ネットワークレイヤ L3/L4 に基づくポリシーを使用します。たとえば、クラスマップは、ACL と L4 プロトコル TCP/UDP/ICMP または L7 プロトコル FTP および SIP に基づいています。L7 プロトコルを使用して定義されたポリシーは、プロトコルの宛先ポートを使用してパケットを分類します。ZBF にはアプリケーションの可視性がなく、FTP ALG を介した FTP 検査をサポートし、ポート 21 に基づくプロトコルのみを識別します。

（注） FTP 制御フローがランダムなポートで開かれると、ゾーンベース ファイアウォールはアプリケーションを識別できません。

ZBFW での NBAR ベースアプリケーション認識の設定方法

レイヤ 4 ゾーンベース ファイアウォールの設定

```
Device(config-profile)#class-map type inspect match-any cm1
Device(config-cmap)#match protocol http
Device(config-cmap)#match protocol https
Device(config-cmap)#match protocol dns
Device(config-cmap)#match protocol tcp
Device(config-cmap)#match protocol udp
Device(config-cmap)#match protocol icmp
Device(config-cmap)#exit
Device(config)#class-map match-any nbar-class1
Device(config-cmap)#match protocol yahoo-mail
Device(config-cmap)#match protocol amazon
```

```
Device(config-cmap)#match protocol attribute category consumer-internet
Device(config-cmap)#exit
```

アプリケーション認識型ファイアウォールの L7 サービスポリシー

手順

	コマンドまたはアクション	目的

ステップ 1	検査用のクラスマップを設定します。
	例：
	`class-map type inspect match-any cm1`
	` match protocol http`
	` match protocol https`
	` match protocol dns`
	` match protocol tcp`
	` match protocol udp`
	` match protocol icmp`
		class-map type inspect コマンドと **match protocol** コマンドを使用して、プロトコルとカテゴリを定義します。

ステップ 2	アプリケーション ファイアウォール ポリシーを使用して、アクション（この場合はAVC）を定義します。
	例：
	`policy-map type inspect avc nbar-policy1`
	`class nbar-class1`
	`deny`
	`class class-default`
	`allow`
		deny コマンドを使用して、`nbar-class1` クラスマップにリストされているリモートネットワーク管理プロトコルを拒否します。

ステップ 3	アプリケーション ファイアウォール ポリシーを使用して、ドロップされたパケットをログに記録します。
	例：
	`policy-map type inspect pm1`
	`class type inspect cm1`
	`  inspect`
	`  service-policy avc nbar-policy1`
	`class class-default`
	`  drop log`
	nbar-class1 での Amazon からのトラフィックは、ポリシーによって拒否されます。たとえば、ドロップされたパケットは、次のドロップログメッセージに示されます。
	`Oct 17 12:44:08.101: %IOSXE-6-PLATFORM: R0/0:`
	`cpp_cp:`
	`QFP:0.0 Thread:000 TS:00000002517650404876`
	`%FW-6-DROP_PKT:`
	`Dropping dns/amazon pkt from GigabitEthernet3`
	`171.70.168.183:53 =>`
	`171.10.1.101:50877(target:class)`	

	コマンドまたはアクション	目的
	-(in_to_out:cm1) due to AVC Policy drop:classify result with ip ident 65434	

次のタスク

入力インターフェイスに **ip nbar protocol-discovery ipv4** コマンドを追加します。その後、**show ip nbar protocol-discovery interface** [**intf-name**] コマンドを使用して、アプリケーションの分類を確認します。

例：アプリケーション認識型 show コマンド

この例では、**show policy-map type inspect zone-pair** コマンドにより、ポリシーマップの統計とその他の情報（指定されたゾーンペアに存在するセッションに関する情報など）が表示されます。`Class-map: nbar-class1 (match-any)` に続く行には、トラフィックが nbar-class1 クラスと一致するたびに増加するパケットカウンタ値（`7 packets`）が含まれています。

```
Device# show policy-map type inspect zone-pair

Zone-pair: in_to_out
Service-policy inspect : pm1

Class-map: cm1 (match-any)
Match: protocol http
Match: protocol https
Match: protocol dns
Match: protocol tcp
Match: protocol udp
Match: protocol icmp
Inspect
Packet inspection statistics [process switch:fast switch]
tcp packets: [0:485]
dns packets: [0:51]

Session creations since subsystem startup or last reset 21
Current session counts (estab/half-open/terminating) [13:0:0]
Maxever session counts (estab/half-open/terminating) [13:2:0]
Last session created 00:00:00
Last statistic reset 00:00:19
Last session creation rate 151
Last half-open session total 0

Service-policy inspect avc : nbar-policy1

Class-map: nbar-class1 (match-any)
7 packets, 1449 bytes
30 second offered rate 1000 bps, drop rate 0000 bps
Match: protocol amazon
Match: protocol yahoo-mail
Match: protocol attribute category consumer-internet
Deny

Class-map: class-default (match-any)
211 packets, 94091 bytes
30 second offered rate 27000 bps, drop rate 0000 bps
```

```
Match: any
Allow

Class-map: class-default (match-any)
Match: any
Drop
0 packets, 0 bytes
```

```
Device# show platform hardware qfp active feature firewall drop
-------------------------------------------------------------------------------
Drop Reason                                                             Packets
-------------------------------------------------------------------------------
AVC Policy drop:classify result                                              38
```

```
Device# show platform hardware qfp active feature firewal datapath scb
[s=session  i=imprecise channel c=control channel  d=data channel A/D=appfw action
allow/deny]
Session ID:0x0000DA5B  171.10.1.101 64204 171.70.168.183 53 proto 17 (0:0) (1456:0xd000208)
 [scA]
Session ID:0x0000DA18  171.10.1.101 58836 74.125.199.103 443 proto 6 (0:0) (1456:0xd000208)
 [sdA]
Session ID:0x0000DA5A  171.10.1.101 64206 8.8.8.8 53 proto 17 (0:0) (0:0xd000001) [sc]
Session ID:0x0000DA11  171.10.1.101 58833 74.125.199.84 443 proto 6 (0:0) (1440:0xd000210)
 [sdA]
Session ID:0x0000DA57  171.10.1.101 64205 173.36.131.10 53 proto 17 (0:0) (1761:0xd00033f)
 [scD]
Session ID:0x0000DA2C  171.10.1.101 58839 74.125.199.94 443 proto 6 (0:0) (1456:0xd000208)
 [sdA]
Session ID:0x0000DA59  171.10.1.101 64203 173.36.131.10 53 proto 17 (0:0) (1761:0xd00033f)
 [scD]
Session ID:0x0000DA0B  171.10.1.101 58831 74.125.199.94 443 proto 6 (0:0) (1456:0xd000208)
 [sdA]
Session ID:0x0000DA5C  171.10.1.101 64207 8.8.4.4 53 proto 17 (0:0) (0:0xd000001) [sc]
Session ID:0x0000DA58  171.10.1.101 64203 171.70.168.183 53 proto 17 (0:0) (1761:0xd00033f)
 [scD]
```

ファイアウォール ステートフル シャーシ間冗長性に関する追加情報

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『Master Command List, All Releases』

関連項目	マニュアル タイトル
セキュリティ コマンド	• 『Security Command Reference: Commands A to C』 • 『Security Command Reference: Commands D to L』 • 『Security Command Reference: Commands M to R』 • 『Security Command Reference: Commands S to Z』

シスコのテクニカル サポート

説明	リンク
右の URL にアクセスして、シスコのテクニカル サポートを最大限に活用してください。これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

第 135 章

Skinny Client Control Protocol のファイアウォール サポート

Skinny Client Control Protocol のファイアウォール サポート機能は、Cisco IOS XE ファイアウォールで VoIP と Skinny Client Control Protocol（SCCP）をサポートできるようにします。Cisco IP 電話は、SCCP を使用して Cisco Unified Communications Manager に接続および登録を行います。スケーラブルな環境で IP 電話と Cisco Unified Communications Manager 間の Cisco IOS XE ファイアウォールを設定できるようにするには、ファイアウォールが SCCP を検出して、メッセージ内で渡される情報を理解できる必要があります。Skinny Client Control Protocol のファイアウォール サポート機能によって、ファイアウォールは、Skinny クライアント（IP 電話など）と Cisco Unified Communications Manager 間で交換される Skinny コントロール パケットを検査し、Skinny データ チャネルがルータを通過できるようにルータを設定します。この機能は、ビデオ チャネルに対応するように SCCP のサポートを拡張します。

Skinny Client Control Protocol のファイアウォール サポートに関する前提条件

- システムは、Cisco IOS XE リリース 2.1 以降のリリースを実行している必要があります。
- SCCP アプリケーション レベル ゲートウェイ（ALG）が機能するためにはファイアウォールを有効にする必要があります。

- SCCP が機能するためには TFTP ALG を有効にする必要があります。これは、Skinny を使用する IP 電話には Cisco Unified Communications Manager からの TFTP コンフィギュレーション ファイルが必要なためです。

Skinny Client Control Protocol のファイアウォール サポートに関する制約事項

- IPv6 アドレスのインスペクションと変換はサポートされません。
- TCP セグメンテーションはサポートされません。

Skinny Client Control Protocol のファイアウォール サポートに関する情報

アプリケーション レベル ゲートウェイ

アプリケーション レベル ゲートウェイ（ALG）は、アプリケーション レイヤ ゲートウェイとも呼ばれ、アプリケーションパケットのペイロード内のIPアドレス情報を変換するアプリケーションです。ALG は、アプリケーション レイヤ プロトコルを解釈し、ファイアウォールおよびネットワーク アドレス変換（NAT）アクションを実行するために使用されます。これらのアクションは、ファイアウォールおよび NAT の設定に応じて次の 1 つまたは複数のアクションになります。

- クライアント アプリケーションが、ダイナミック TCP または UDP ポートを使用してサーバ アプリケーションと通信できるようにします。
- アプリケーション固有のコマンドを認識し、これらのコマンドに対するきめ細かいセキュリティ制御を提供します。
- データ交換を行う 2 つのホスト間の複数のデータ ストリームまたはデータ セッションを同期します。
- アプリケーション ペイロードで使用できるネットワーク層アドレス情報を変換します。

ファイアウォールがピンホールを開き、アプリケーション レイヤ データストリームの送信元 IP アドレスおよび宛先 IP アドレスを伝送しない TCP または UDP トラフィックに対する変換サービスをNATが実行します。IPアドレス情報を埋め込む特定のプロトコルまたはアプリケーションには ALG のサポートが必要です。

SCCP インスペクションの概要

SCCP インスペクションでは、Cisco Unified Communications Manager を使用して、2 つの SCCP クライアント間での音声通信が可能です。Cisco Unified Communications Manager は TCP ポート 2000（デフォルトの SCCP ポート）を使用して、SCCP クライアントにサービスを提供します。初めに SCCP クライアントは TCP 接続を確立することでプライマリ Cisco Unified Communications Manager に接続し、その後、使用可能であればセカンダリ Cisco Unified Communications Manager に接続します。TCP 接続が確立された後、SCCP クライアントはプライマリ Cisco Unified Communications Manager に登録されます。プライマリ Cisco Unified Communications Manager はリブートするか、またはキープアライブ障害が発生するまで、制御 Cisco Unified Communications Manager として使用されます。したがって、SCCP クライアントと Cisco Unified Communications Manager 間の TCP 接続は永続的に存在し、クライアントとのコールを確立するために使用されます。TCP 接続が失敗すると、セカンダリ Cisco Unified Communications Manager が使用されます。最初の Cisco Unified Communications Manager と確立されたすべてのデータ チャネルは、コールの終了後に閉じられるまでアクティブのままです。

SCCP プロトコルは、ローカルで生成または終了した SCCP 制御チャネルを検査し、ファイアウォールを送信先または送信元とするメディア チャネルのピンホールを開閉します。ピンホールは、保護されたネットワークに対するアプリケーションで制御されたアクセスを可能するために、ファイアウォールを通じて開かれるポートです。

データ セッションの開閉に必要なメッセージのセットを下の表に示します。SCCP インスペクションは、アクセス リスト ピンホールを開閉するために使用されるデータ セッションを検査します。

表 *180 : SCCP* データ セッション メッセージ

Skinny インスペクション メッセージ	**説明**
CloseReceiveChannel	コールを中断する必要があることを示します。このメッセージが受信されると、ファイアウォールおよびNATにより作成されたすべての中間セッションはクリーンアップする必要があります。
OpenReceiveChannelACK	電話機が Cisco Unified Communications Manager から受信した OpenReceiveChannel メッセージを確認していることを示します。
StartMediaTransmission	コールの送信元または宛先である電話の Realtime Transport Protocol（RTP）情報が含まれます。メッセージには、IP アドレス、他方の電話がリッスンしている RTP ポート、およびコールを一意に識別するコール ID が含まれます。
StopMediaTransmission	通話が終了したことを表します。このメッセージを受信した後、セッションをクリーンアップすることができます。

Skinny インスペクション メッセージ	説明
StationCloseReceiveChannel	Skinny クライアント（このメッセージ中の情報に基づく）に受信チャネルを閉じるように指示します。
StationOpenMultiMediaReceiveChannelAck	このメッセージを送信する Skinny クライアントの IP アドレスおよびポート情報が含まれます。また、クライアントがビデオおよびデータ チャネルを受信する用意があるかどうかのステータスも含まれます。
StationOpenReceiveChannelAck	このメッセージを送信する Skinny クライアントの IP アドレスおよびポート情報が含まれます。このメッセージには、クライアントが音声トラフィックを受信する用意があるかどうかのステータスも含みます。
StationStartMediaTransmission	リモート Skinny クライアントの IP アドレスおよびポート情報を含みます。
StationStartMultiMediaTransmit	Cisco Unified Communications Manager がビデオまたはデータ チャネルの OpenLogicalChannelAck メッセージを受信したことを示します。
StationStopMediaTransmission	Skinny クライアント（このメッセージ中の情報に基づく）に音声トラフィックの送信を停止するように指示します。
StationStopSessionTransmission	Skinny クライアント（このメッセージ中の情報に基づく）に指定されたセッションを終了するように指示します。

ALG--SCCP バージョン 17 サポート

ALG - SCCP バージョン 17 サポート機能は、SCCP ALG で SCCP バージョン 17 パケットを解析できるようにします。Cisco Unified Communications Manager 7.0 および Cisco Unified Communications Manager 7.0 を使用する IP フォンでは、SCCP バージョン 17 のメッセージだけがサポートされています。IPv6 に対応するため、SCCP の形式はバージョン 17 から変更されました。SCCP ALG は、メッセージのプレフィックス内の SCCP バージョンをチェックしてから、バージョンに応じて解析します。SCCP メッセージのバージョンはメッセージヘッダーから抽出され、バージョンが 17 よりも大きい場合そのメッセージはバージョン 17 形式を使用して解析され、IPv4 アドレスおよびポート情報が抽出されます。SCCP ALG は、SCCP メッセージの IPv4 アドレス情報の検査および変換をサポートしています。

（注） IPv6 アドレスの検査および変換はサポートされていません。

次の SCCP ALG 処理メッセージの IP アドレス形式は、バージョン 17 で変更されました。

- StationOpenMultiMediaReceiveChannelAck
- StationOpenReceiveChannelAckMessage
- StationRegisterMessage
- StationStartMediaTransmissionAckMessage
- StationStartMultiMediaTransmissionAckMessage
- StationStartMediaTransmissionMessage
- StationStartMultiMediaTransmissionMessage

Skinny Client Control Protocol のファイアウォール サポートの設定方法

Skinny クラス マップとポリシー マップの設定

ファイアウォール設定で（**match protocol** コマンドを使用して）SCCP をイネーブルにする場合、（**match protocol** コマンドを使用して）TFTP をイネーブルにする必要があります。そうしないと、SCCP を使用する IP フォンは Cisco Unified Communications Manager と通信できません。SCCP は、Cisco Unified Communications Manager を使用して、2 つの Skinny クライアント間の音声通信を可能にします。

手順の概要

1. **enable**
2. **configure terminal**
3. **class-map type inspect match-any** *class-map-name*
4. **match protocol** *protocol-name*
5. **match protocol** *protocol-name*
6. **exit**
7. **policy-map type inspect** *policy-map-name*
8. **class type inspect** *class-map-name*
9. **inspect**
10. **exit**
11. **class class-default**
12. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例：	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。

	コマンドまたはアクション	目的
	`Router> enable`	
ステップ 2	**configure terminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**class-map type inspect match-any** *class-map-name* 例： `Router(config)# class-map type inspect match-any cmap1`	検査タイプ クラス マップを作成し、クラス マップ コンフィギュレーション モードを開始します。
ステップ 4	**match protocol** *protocol-name* 例： `Router(config-cmap)# match protocol skinny`	Skinny クラス マップの一致基準を設定します。
ステップ 5	**match protocol** *protocol-name* 例： `Router(config-cmap)# match protocol tftp`	TFTP クラス マップの一致基準を設定します。
ステップ 6	**exit** 例： `Router(config-cmap)# exit`	クラスマップ コンフィギュレーション モードを終了します。
ステップ 7	**policy-map type inspect** *policy-map-name* 例： `Router(config)# policy-map type inspect pmap1`	検査タイプ ポリシー マップを作成し、ポリシー マップ コンフィギュレーション モードを開始します。
ステップ 8	**class type inspect** *class-map-name* 例： `Router(config-pmap)# class type inspect cmap1`	アクションを実行するクラスを指定し、ポリシー マップ クラス コンフィギュレーション モードを開始します。
ステップ 9	**inspect** 例： `Router(config-pmap-c)# inspect`	ステートフル パケット インスペクションをイネーブルにします。
ステップ 10	**exit** 例： `Router(config-pmap-c)# exit`	ポリシー マップ クラス コンフィギュレーション モードを終了し、ポリシーマップ コンフィギュレーション モードを開始します。
ステップ 11	**class class-default** 例： `Router(config-pmap)# class class-default`	これらのポリシー マップ設定が事前に定義したデフォルト クラスに適用されることを指定します。 • 設定済みクラス マップの一致基準のいずれともトラフィックが一致しない場合、事前に定義されたデフォルト クラスに誘導されます。

	コマンドまたはアクション	目的
ステップ 12	**end** 例： `Router(config-pmap)# end`	ポリシーマップ コンフィギュレーション モードを終了し、特権 EXEC モードを開始します。

ゾーン ペアの設定および SCCP ポリシー マップのアタッチ

手順の概要

1. **enable**
2. **configure terminal**
3. **zone security** {*zone-name* | **default**}
4. **exit**
5. **zone security** {*zone-name* | **default**}
6. **exit**
7. **zone-pair security** *zone-pair-name* [**source** {*source-zone-name* | **self** | **default**} **destination** [*destination-zone-name* | **self** | **default**]]
8. **service-policy type inspect** *policy-map-name*
9. **exit**
10. **interface** *type number*
11. **zone-member security** *zone-name*
12. **exit**
13. **interface** *type number*
14. **zone-member security** *zone-name*
15. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**zone security** {*zone-name*	**default**} 例： `Router(config)# zone security zone1`	インターフェイスを割り当てることができるセキュリティ ゾーンを作成し、セキュリティ ゾーン コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 4	**exit** 例： `Router(config-sec-zone)# exit`	セキュリティ ゾーン コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードを開始します。
ステップ 5	**zone security** {*zone-name* | **default**} 例： `Router(config)# zone security zone2`	インターフェイスを割り当てることができるセキュリティ ゾーンを作成し、セキュリティ ゾーン コンフィギュレーション モードを開始します。
ステップ 6	**exit** 例： `Router(config-sec-zone)# exit`	セキュリティ ゾーン コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードを開始します。
ステップ 7	**zone-pair security** *zone-pair-name* [**source** {*source-zone-name* | **self** | **default**} **destination** [*destination-zone-name* | **self** | **default**]] 例： `Router(config)# zone-pair security in-out source zone1 destination zone2`	ゾーン ペアを作成し、セキュリティ ゾーンペア コンフィギュレーション モードを開始します。 （注） ポリシーを適用するには、ゾーン ペアを設定する必要があります。
ステップ 8	**service-policy type inspect** *policy-map-name* 例： `Router(config-sec-zone-pair)# service-policy type inspect pmap1`	ファイアウォール ポリシー マップを宛先ゾーン ペアに付加します。 （注） ゾーンのペア間でポリシーが設定されない場合、トラフィックはデフォルトでドロップされます。
ステップ 9	**exit** 例： `Router(config-sec-zone-pair)# exit`	セキュリティ ゾーンペア コンフィギュレーション モードを終了し、グローバルコンフィギュレーション モードを開始します。
ステップ 10	**interface** *type number* 例： `Router(config)# interface gigabitethernet 0/0/0`	インターフェイスを設定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 11	**zone-member security** *zone-name* 例：	インターフェイスを指定したセキュリティ ゾーンに割り当てます。

	コマンドまたはアクション	目的
	`Router(config-if)# zone-member security zone1`	（注） インターフェイスをセキュリティ ゾーンのメンバーにした場合、方向に関係なくインターフェイスを通過するすべてのトラフィック（ルータ宛のトラフィックまたはルータ発信のトラフィックを除く）が、デフォルトでドロップされます。トラフィックがインターフェイス通過するには、ゾーンをポリシーの適用先のゾーン ペアの一部にする必要があります。ポリシーがトラフィックを許可すると、トラフィックはそのインターフェイスを通過できます。
ステップ 12	**exit** 例： `Router(config-if)# exit`	インターフェイス コンフィギュレーション モードを終了し、グローバルコンフィギュレーションモードに入ります。
ステップ 13	**interface** *type number* 例： `Router(config)# interface gigabitethernet 0/1/1`	インターフェイスを設定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 14	**zone-member security** *zone-name* 例： `Router(config-if)# zone-member security zone2`	インターフェイスを指定したセキュリティ ゾーンに割り当てます。
ステップ 15	**end** 例： `Router(config-if)# end`	インターフェイス コンフィギュレーション モードを終了し、特権 EXEC モードを開始します。

Skinny Control Protocol のファイアウォール サポートの設定例

例：SCCP クラス マップとポリシー マップの設定

```
Router# configure terminal
Router(config)# class-map type inspect match-any cmap1
Router(config-cmap)# match protocol skinny
Router(config-cmap)# match protocol tftp
Router(config-cmap)# exit
Router(config)# policy-map type inspect pmap1
Router(config-pmap)# class type inspect cmap1
```

```
Router(config-pmap-c)# inspect
Router(config-pmap-c)# exit
Router(config-pmap)# class class-default
Router(config-pmap)# end
```

例：ゾーン ペアの設定と SCCP ポリシー マップのアタッチ

```
Router# configure terminal
Router(config)# zone security zone1
Router(config-sec-zone)# exit
Router(config)# zone security zone2
Router(config-sec-zone)# exit
Router(config)# zone-pair security in-out source zone1 destination zone2
Router(config-sec-zone-pair)# service-policy type inspect pmap1
Router(config-sec-zone-pair)# exit
Router(config)# interface gigabitethernet 0/0/0
Router(config-if)# zone-member security zone1
Router(config-if)# exit
Router(config)# interface gigabitethernet 0/1/1
Router(config-if)# zone-member security zone2
Router(config-if)# end
```

Skinny Client Control Protocol のファイアウォール サポートに関する追加情報

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『Cisco IOS Master Commands List, All Releases』
セキュリティ コマンド	• 『Cisco IOS Security Command Reference: Commands A to C』 • 『Cisco IOS Security Command Reference: Commands D to L』 • 『Cisco IOS Security Command Reference: Commands M to R』 • 『Cisco IOS Security Command Reference: Commands S to Z』

シスコのテクニカル サポート

説明	リンク
右の URL にアクセスして、シスコのテクニカル サポートを最大限に活用してください。これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

Skinny Client Control Protocol のファイアウォール サポートに関する機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *181 : Skinny Client Control Protocol* のファイアウォール サポートに関する機能情報

機能名	リリース	機能情報
ALG - SCCP V17 サポート	Cisco IOS XE リリース 3.5S	ALG - SCCP バージョン 17 サポート機能は、SCCP ALG で SCCP バージョン 17 パケットを解析できるようにします。SCCP 形式はバージョン 17 から IPv6 をサポートするように変更されました。

機能名	リリース	機能情報
ファイアウォール：SCCP ビデオ ALG サポート	Cisco IOS XE リリース 2.4	SCCP は、Cisco Unified Communications Manager を使用して、2 つの Skinny クライアント間の音声通信を可能にします。この機能は、Cisco ファイアウォールで、Skinny クライアントと Cisco Unified Communications Manager 間で交換される Skinny 制御パケットを検査できるようにします。 **match protocol** コマンドが変更されました。

機能名	リリース	機能情報
Skinny Client Control Protocol のファイアウォール サポート	Cisco IOS XE リリース 2.1	Skinny Client Control Protocol のファイアウォール サポート機能は、Cisco IOS XE ファイアウォールで VoIP と SCCP をサポートできるようにします。Cisco IP 電話は、SCCP を使用して Cisco Unified Communications Manager に接続および登録を行います。スケーラブルな環境で IP 電話と Cisco Unified Communications Manager 間の Cisco IOS XE ファイアウォールを設定できるようにするには、ファイアウォールが SCCP を検出して、メッセージ内で渡される情報を理解できる必要があります。Skinny Client Control Protocol のファイアウォール サポート機能によって、ファイアウォールは、Skinny クライアント（IP 電話など）と Cisco Unified Communications Manager 間で交換される Skinny コントロール パケットを検査し、Skinny データ チャネルがルータを通過できるようにルータを設定します。この機能は、ビデオ チャネルに対応するように SCCP のサポートを拡張します。

第 136 章

VASI インターフェイス経由の IPv6 ゾーンベース ファイアウォール サポート

この機能は、IPv6 ファイアウォールでの VRF 対応サービス インフラストラクチャ（VASI）インターフェイスをサポートします。この機能により、アクセス コントロール リスト（ACL）、ネットワーク アドレス変換（NAT）、ポリシング、ゾーンベース ファイアウォールなどのサービスを、2 つの異なる Virtual Routing and Forwarding（VRF）インスタンスの間を流れるトラフィックに適用できます。VASI インターフェイスは、ルート プロセッサ（RP）とフォワーディング プロセッサ（FP）の冗長性をサポートします。VASI インターフェイスは IPv4 および IPv6 ユニキャスト トラフィックをサポートします。

このモジュールでは、VASI インターフェイスの概要を紹介し、VASI インターフェイスを設定する方法を説明します。

VASI インターフェイス経由の IPv6 ゾーンベース ファイアウォール サポートに関する制約事項

- VRF 対応ソフトウェア インフラストラクチャ（VASI）インターフェイス経由のマルチプロトコル ラベル スイッチング（MPLS）トラフィックはサポートされません。

- IPv4 と IPv6 のマルチキャスト トラフィックはサポートされません。
- VASI インターフェイスは、キュー ベース機能のアタッチメントをサポートしません。以下のコマンドは、VASI インターフェイスにアタッチされたモジュラ QoS CLI（MQC）ポリシーでサポートされません。
  - **bandwidth (policy-map class)**
  - **fair-queue**
  - **priority**
  - **queue-limit**
  - **random-detect**
  - **shape**

VASI インターフェイス経由の IPv6 ゾーンベース ファイアウォール サポートに関する情報

VASI の概要

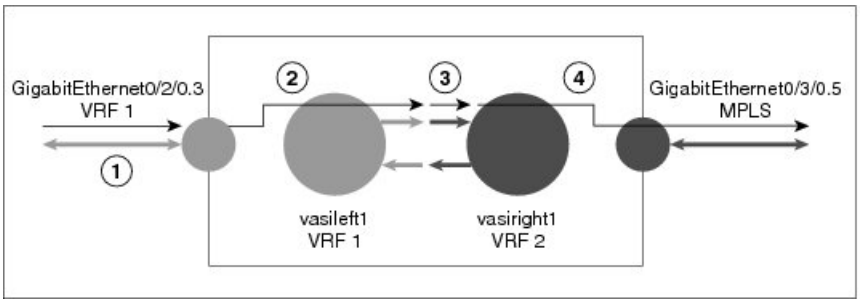
VRF 対応ソフトウェア インフラストラクチャ（VASI）を使用すると、ファイアウォール、GETVPN、IPsec、およびネットワークアドレス変換（NAT）などのサービスを、異なる仮想ルーティングおよび転送（VRF）インスタンスを横断するトラフィックに適用できます。VASI は仮想インターフェイスのペアを使用して実行され、ペア内の各インターフェイスは別の VRF インスタンスに関連付けられます。VASI 仮想インターフェイスは、これら 2 つの VRF インスタンス間で切り替える必要がある、すべてのパケットのネクストホップ インターフェイスです。VASI インターフェイスは、VRF インスタンス間にファイアウォールまたは NAT を設定するためのフレームワークを提供します。

各インターフェイス ペアは、異なる 2 つの VRF インスタンスに関連付けられています。ペアリングは、vasileft インターフェイスが自動的に vasiright インターフェイスへのペアとなるように、2 つのインターフェイスのインデックスに基づいて自動的に行われます。たとえば、下の図では、vasileft1 と vasiright1 は自動的にペアになり、vasileft1 に入るパケットは vasiright1 に内部的に渡されます。

VASI インターフェイスでは、内部ボーダー ゲートウェイ プロトコル（IBGP）、Enhanced Interior Gateway Routing Protocol（EIGRP）、および Open Shortest Path First（OSPF）を使用して、スタティック ルーティングまたはダイナミック ルーティングのいずれかを設定できます。

次の図は、同じデバイスの VRF 間 VASI 設定を示しています。

図 *71 : VRF* 間 *VASI* 設定



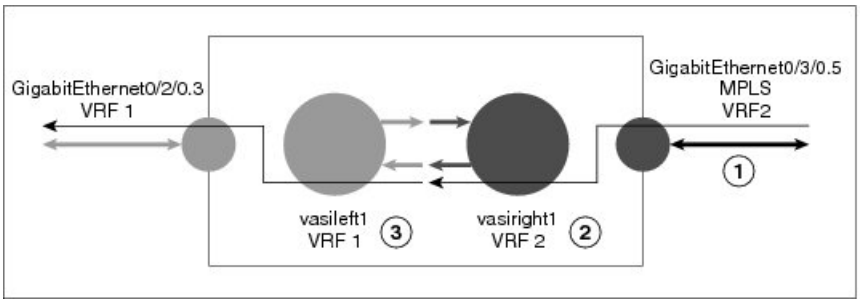
VRF 間 VASI が同じデバイス上で設定されている場合、パケット フローは次の順序で発生します。

1. パケットが VRF 1（ギガビット イーサネット 0/2/0.3）に属する物理インターフェイスに入ります。
2. パケットを転送する前に、VRF1 ルーティング テーブルでフォワーディング ルックアップが実行されます。Vasileft1 がネクスト ホップとして選択され、存続可能時間（TTL）値がパケットから引かれます。通常、フォワーディング アドレスは VRF のデフォルト ルートに基づいて選択されます。ただし、フォワーディング アドレスはスタティック ルートまたは学習したルートになる可能性もあります。パケットは vasileft1 の出力パスに送信されてから、vasiright1 入力パスに自動的に送信されます。
3. パケットが vasiright1 に入ると、VRF 2 ルーティング テーブルでフォワーディング ルックアップが実行され、TTL が再度減らされます（このパケットでは 2 回目）。
4. VRF 2 はパケットを物理インターフェイス、ギガビット イーサネット 0/3/0.5 へ転送します。

次の図は VASI がマルチプロトコル ラベル スイッチング（MPLS）VPN 設定で機能するしくみを示します。

（注） 次の図で、MPLS はギガビット イーサネット インターフェイスで有効になっていますが、MPLS トラフィックは VASI ペア間ではサポートされていません。

図 *72 : MPLS VPN* 設定を使用する *VASI*



VASI がマルチプロトコル ラベル スイッチング（MPLS）VPN を使用して設定されている場合、パケット フローは次の順序で発生します。

1. パケットが VPN ラベルを持つ MPLS インターフェイスに到着します。
2. VPN ラベルがパケットから取り除かれ、VRF 2 でフォワーディング ルックアップが実行され、パケットが vasiright1 に転送されます。TTL 値がパケットから引かれます。
3. パケットが入力パスの vasileft1 に入り、別のフォワーディング ルックアップが VRF1 で行われます。パケットが VRF1 の出力物理インターフェイス（ギガビット イーサネット 0/2/0.3）に送信されます。TTL がパケットから再度減らされます。

VASI インターフェイス経由の IPv6 ゾーンベース ファイアウォール サポートの設定方法

VRF とアドレス ファミリ セッションの設定

手順の概要

1. **enable**
2. **configure terminal**
3. **vrf definition** *vrf-name*
4. **address-family ipv6**
5. **exit-address-family**
6. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**vrf definition** *vrf-name* 例： `Device(config)# vrf definition VRF1`	Virtual Routing and Forwarding（VRF）ルーティング テーブル インスタンスを設定し、VRF コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 4	**address-family ipv6** 例： `Device(config-vrf)# address-family ipv6`	アドレス ファミリ コンフィギュレーション モードを開始し、標準の IPv6 アドレス プレフィックスを伝送するセッションを設定します。
ステップ 5	**exit-address-family** 例： `Device(config-vrf-af)# exit-address-family`	アドレス ファミリ コンフィギュレーション モードを終了して、VRF コンフィギュレーション モードを開始します。
ステップ 6	**end** 例： `Device(config-vrf)# end`	VRF コンフィギュレーション モードを終了して、特権 EXEC モードを開始します。

VASI サポート用のクラス マップとポリシー マップの設定

手順の概要

1. **enable**
2. **configure terminal**
3. **ipv6 unicast-routing**
4. **class-map type inspect match-any** *class-map-name*
5. **match protocol** *name*
6. **match protocol** *name*
7. **exit**
8. **policy-map type inspect** *policy-map-name*
9. **class type inspect** *class-map-name*
10. **inspect**
11. **exit**
12. **class class-default**
13. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 3	**ipv6 unicast-routing** 例： `Device(config)# ipv6-unicast routing`	IPv6 ユニキャスト データグラムの転送を有効にします。
ステップ 4	**class-map type inspect match-any** *class-map-name* 例： `Device(config)# class-map type inspect match-any c-map`	検査タイプ クラス マップを作成し、QoS クラス マップ コンフィギュレーション モードを開始します。
ステップ 5	**match protocol** *name* 例： `Device(config-cmap)# match protocol icmp`	指定されたプロトコルに基づいて、クラス マップ一致基準を設定します。
ステップ 6	**match protocol** *name* 例： `Device(config-cmap)# match protocol tcp`	指定されたプロトコルに基づいて、クラス マップ一致基準を設定します。
ステップ 7	**exit** 例： `Device(config-cmap)# exit`	QoS クラス マップ コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードを開始します。
ステップ 8	**policy-map type inspect** *policy-map-name* 例： `Device(config)# policy-map type inspect p-map`	プロトコル固有の検査タイプ ポリシー マップを作成して、QoS ポリシーマップ コンフィギュレーション モードを開始します。
ステップ 9	**class type inspect** *class-map-name* 例： `Device(config-pmap)# class type inspect c-map`	アクションの実行対象となるトラフィック クラスを指定し、QoS ポリシー マップ クラス コンフィギュレーション モードを開始します。
ステップ 10	**inspect** 例： `Device(config-pmap-c)# inspect`	ステートフル パケット インスペクションをイネーブルにします。
ステップ 11	**exit** 例： `Device(config-pmap-c)# exit`	QoS ポリシーマップ クラス コンフィギュレーション モードを終了し、QoS ポリシーマップ コンフィギュレーション モードを開始します。
ステップ 12	**class class-default** 例： `Device(config-pmap)# class class-default`	定義済みのデフォルト クラスにポリシー マップ設定を適用して、QoS ポリシー マップ クラス コンフィギュレーション モードを開始します。 • 設定済みクラス マップの一致基準のいずれともトラフィックが一致しない場合、事前に定義されたデフォルト クラスに誘導されます。

	コマンドまたはアクション	目的
ステップ 13	**end** 例： `Device(config-pmap-c)# end`	QoS ポリシーマップ クラス コンフィギュレーション モードを終了し、特権 EXEC モードを開始します。

VASI サポートのゾーンおよびゾーン ペアの設定

手順の概要

1. **enable**
2. **configure terminal**
3. **zone security** *zone-name*
4. **exit**
5. **zone-pair security** *zone-pair-name* **source** *source-zone* **destination** *destination-zone*
6. **service-policy type inspect** *policy-map-name*
7. **exit**
8. **interface** *type number*
9. **vrf forwarding** *vrf-name*
10. **no ip address**
11. **zone member security** *zone-name*
12. **ipv6 address** *ipv6-address/prefix-length*
13. **ipv6 enable**
14. **negotiation auto**
15. **exit**
16. **interface** *type number*
17. **no ip address**
18. **ipv6 address** *ipv6-address/prefix-length*
19. **ipv6 enable**
20. **negotiation auto**
21. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 3	**zone security** *zone-name* 例： `Device(config)# zone security in`	セキュリティ ゾーンを作成し、セキュリティ ゾーン コンフィギュレーション モードを開始します。 • ゾーンペアを作成するには2つのセキュリティ ゾーン（送信元ゾーンと宛先ゾーン）が設定に含まれる必要があります。 • ゾーンペアでは、送信元ゾーンまたは宛先ゾーンとしてデフォルト ゾーンを使用できます。
ステップ 4	**exit** 例： `Device(config-sec-zone)# exit`	セキュリティ ゾーン コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードを開始します。
ステップ 5	**zone-pair security** *zone-pair-name* **source** *source-zone* **destination** *destination-zone* 例： `Device(config)# zone-pair security in-out source in destination out`	ゾーン ペアを作成し、セキュリティ ゾーンペア コンフィギュレーション モードを開始します。 • ポリシーを適用するには、ゾーン ペアを設定する必要があります。
ステップ 6	**service-policy type inspect** *policy-map-name* 例： `Device(config-sec-zone-pair)# service-policy type inspect p-map`	ポリシー マップをトップレベル ポリシーに関連付けます。 • ゾーンのペア間でポリシーが設定されない場合、トラフィックはデフォルトでドロップされます。
ステップ 7	**exit** 例： `Device(config-sec-zone-pair)# exit`	セキュリティ ゾーンペア コンフィギュレーション モードを終了し、グローバルコンフィギュレーション モードを開始します。
ステップ 8	**interface** *type number* 例： `Device(config)# interface gigabitethernet 0/0/0`	インターフェイスを設定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 9	**vrf forwarding** *vrf-name* 例： `Device(config-if)# vrf forwarding VRF1`	インターフェイスまたはサブインターフェイスに Virtual Routing and Forwarding（VRF）インスタンスまたは仮想ネットワークを関連付けます。
ステップ 10	**no ip address** 例： `Device(config-if)# no ip address`	IP アドレスを削除するか、IP 処理をディセーブルにします。

	コマンドまたはアクション	目的
ステップ 11	**zone member security** *zone-name* 例： `Device(config-if)# zone member security in`	インターフェイスをセキュリティ ゾーンにアタッチします。
ステップ 12	**ipv6 address** *ipv6-address/prefix-length* 例： `Device(config-if)# ipv6 address 2001:DB8:2:1234/64`	IPv6 の一般的なプレフィックスに基づいて IPv6 アドレスを設定し、インターフェイスにおける IPv6 処理をイネーブルにします。
ステップ 13	**ipv6 enable** 例： `Device(config-if)# ipv6 enable`	明示的な IPv6 アドレスが設定されていないインターフェイスにおける IPv6 処理をイネーブルにします。
ステップ 14	**negotiation auto** 例： `Device(config-if)# negotiation auto`	ギガビット イーサネット インターフェイス上で速度、デュプレックス モード、およびフロー制御のアドバタイズをイネーブルにします。
ステップ 15	**exit** 例： `Device(config-if)# exit`	インターフェイス コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードに入ります。
ステップ 16	**interface** *type number* 例： `Device(config)# interface gigabitethernet 0/0/1`	インターフェイスを設定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 17	**no ip address** 例： `Device(config-if)# no ip address`	IP アドレスを削除するか、IP 処理をディセーブルにします。
ステップ 18	**ipv6 address** *ipv6-address/prefix-length* 例： `Device(config-if)# ipv6 address 2001:DB8:3:1234/64`	IPv6 の一般的なプレフィックスに基づいて IPv6 アドレスを設定し、インターフェイスにおける IPv6 処理をイネーブルにします。
ステップ 19	**ipv6 enable** 例： `Device(config-if)# ipv6 enable`	明示的な IPv6 アドレスが設定されていないインターフェイスにおける IPv6 処理をイネーブルにします。
ステップ 20	**negotiation auto** 例： `Device(config-if)# negotiation auto`	ギガビット イーサネット インターフェイス上で速度、デュプレックス モード、およびフロー制御のアドバタイズをイネーブルにします。

	コマンドまたはアクション	目的
ステップ 21	**end** 例： `Device(config-if)# end`	インターフェイス コンフィギュレーション モードを終了し、特権 EXEC モードを開始します。

VASI インターフェイスの設定

手順の概要

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **vrf forwarding** *vrf-name*
5. **ipv6 address** *ipv6-address/prefix-length* **link-local**
6. **ipv6 address** *ipv6-address/prefix-length*
7. **ipv6 enable**
8. **no keepalive**
9. **zone member security** *zone-name*
10. **exit**
11. **interface** *type number*
12. **ipv6 address** *ipv6-address/prefix-length* **link-local**
13. **ipv6 address** *ipv6-address/prefix-length*
14. **ipv6 enable**
15. **no keepalive**
16. **exit**
17. **ipv6 route** *ipv6-prefix/prefix-length interface-type interface-number ipv6-address*
18. **ipv6 route vrf** *vrf-name ipv6-prefix/prefix-length interface-type interface-number ipv6-address*
19. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface** *type number* 例：	VASI インターフェイスを設定し、インターフェイス コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
	`Device(config)# interface vasileft 1`	
ステップ 4	**vrf forwarding** *vrf-name* 例： `Device(config-if)# vrf forwarding VRF1`	インターフェイスまたはサブインターフェイスに Virtual Routing and Forwarding（VRF）インスタンスまたは仮想ネットワークを関連付けます。
ステップ 5	**ipv6 address** *ipv6-address/prefix-length* **link-local** 例： `Device(config-if)# ipv6 address FE80::8EB6:4FFF:FE6C:E701 link-local`	インターフェイスの IPv6 リンクローカル アドレスを設定し、そのインターフェイスでの IPv6 処理をイネーブルにします。
ステップ 6	**ipv6 address** *ipv6-address/prefix-length* 例： `Device(config-if)# ipv6 address 2001:DB8:4:1234/64`	IPv6 の一般的なプレフィックスに基づいて IPv6 アドレスを設定し、インターフェイスにおける IPv6 処理をイネーブルにします。
ステップ 7	**ipv6 enable** 例： `Device(config-if)# ipv6 enable`	明示的な IPv6 アドレスが設定されていないインターフェイスにおける IPv6 処理をイネーブルにします。
ステップ 8	**no keepalive** 例： `Device(config-if)# no keepalive`	キープアライブ パケットをディセーブルにします。
ステップ 9	**zone member security** *zone-name* 例： `Device(config-if)# zone member security out`	インターフェイスをセキュリティ ゾーンにアタッチします。
ステップ 10	**exit** 例： `Device(config-if)# exit`	インターフェイス コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードに入ります。
ステップ 11	**interface** *type number* 例： `Device(config)# interface vasiright 1`	VASI インターフェイスを設定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 12	**ipv6 address** *ipv6-address/prefix-length* **link-local** 例： `Device(config-if)# ipv6 address FE80::260:3EFF:FE11:6770 link-local`	インターフェイスの IPv6 リンクローカル アドレスを設定し、そのインターフェイスでの IPv6 処理をイネーブルにします。
ステップ 13	**ipv6 address** *ipv6-address/prefix-length* 例： `Device(config-if)# ipv6 address 2001:DB8:4:1234/64`	IPv6 の一般的なプレフィックスに基づいて IPv6 アドレスを設定し、インターフェイスにおける IPv6 処理をイネーブルにします。

	コマンドまたはアクション	目的
ステップ 14	**ipv6 enable** 例： `Device(config-if)# ipv6 enable`	明示的なIPv6アドレスが設定されていないインターフェイスにおけるIPv6処理をイネーブルにします。
ステップ 15	**no keepalive** 例： `Device(config-if)# no keepalive`	キープアライブパケットをディセーブルにします。
ステップ 16	**exit** 例： `Device(config-if)# exit`	インターフェイス コンフィギュレーション モードを終了し、グローバルコンフィギュレーションモードに入ります。
ステップ 17	**ipv6 route** *ipv6-prefix/prefix-length interface-type interface-number ipv6-address* 例： `Device(config)# ipv6 route 2001::/64 vasileft 1 2001::/64`	スタティック IPv6 ルートを確立します。
ステップ 18	**ipv6 route vrf** *vrf-name ipv6-prefix/prefix-length interface-type interface-number ipv6-address* 例： `Device(config)# ipv6 route vrf vrf1 2001::/64 vasiright 1 2001::/64`	IPv6 アドレスのすべての VRF テーブルまたは特定の VRF テーブルを指定します。
ステップ 19	**end** 例： `Device(config# end`	グローバル コンフィギュレーション モードを終了し、特権 EXEC モードを開始します。

VASI インターフェイス経由の IPv6 ゾーンベース ファイアウォール サポートの設定例

例：VRF とアドレス ファミリ セッションの設定

```
Device# configure terminal
Device(config)# vrf definition VRF1
Device(config-vrf)# address-family ipv6
Device(config-vrf-af)# exit-address-family
Device(config-vrf)# end
```

例：VASI サポート用のクラス マップとポリシー マップの設定

```
Device# configure terminal
Device(config)# ipv6-unicast routing
Device(config)# class-map type inspect match-any c-map
Device(config-cmap)# match protocol icmp
Device(config-cmap)# match protocol tcp
Device(config-cmap)# match protocol udp
Device(config-cmap)# exit
Device(config)# policy-map type inspect p-map
Device(config-pmap)# class type inspect c-map
Device(config-pmap-c)# inspect
Device(config-pmap-c)# exit
Device(config-pmap)# class class-default
Device(config-pmap-c)# end
```

例：VASI サポート用のゾーンとゾーン ペアの設定

```
Device# configure terminal
Device(config)# zone security in
Device(config)# exit
Device(config)# zone security out
Device(config)# exit
Device(config)# zone-pair security in-out source in destination out
Device(config-sec-zone-pair)# service-policy type inspect p-map
Device(config-sec-zone-pair)# exit
Device(config)# interface gigabitethernet 0/0/0
Device(config-if)# vrf forwarding VRF1
Device(config-if)# no ip address
Device(config-if)# zone member security in
Device(config-if)# ipv6 address 2001:DB8:2:1234/64
Device(config-if)# ipv6 enable
Device(config-if)# negotiation auto
Device(config-if)# exit
Device(config)# interface gigabitethernet 0/0/1
Device(config-if)# no ip address
Device(config-if)# ipv6 address 2001:DB8:3:1234/64
Device(config-if)# ipv6 enable
Device(config-if)# negotiation auto
Device(config-if)# end
```

例：VASI インターフェイスの設定

```
Device# configure terminal
Device(config)# interface vasileft 1
Device(config-if)# vrf forwarding VRF1
Device(config-if)# ipv6 address FE80::8EB6:4FFF:FE6C:E701 link-local
Device(config-if)# ipv6 address 2001:DB8:4:1234/64
Device(config-if)# ipv6 enable
Device(config-if)# no keepalive
Device(config-if)# zone-member security out
Device(config-if)# exit
Device(config)# interface vasiright 1
Device(config-if)# ipv6 address FE80::260:3EFF:FE11:6770 link-local
Device(config-if)# ipv6 address 2001:DB8:4:1234/64
```

```
Device(config-if)# ipv6 enable
Device(config-if)# no keepalive
Device(config-if)# exit
Device(config)# ipv6 route 2001::/64 vasileft 1 2001::/64
Device(config)# ipv6 route vrf vrf1 2001::/64 vasiright 1 2001::/64
Device(config)# end
```

ファイアウォール ステートフル シャーシ間冗長性に関する追加情報

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『Master Command List, All Releases』
セキュリティ コマンド	• 『Security Command Reference: Commands A to C』 • 『Security Command Reference: Commands D to L』 • 『Security Command Reference: Commands M to R』 • 『Security Command Reference: Commands S to Z』

シスコのテクニカル サポート

説明	リンク
右の URL にアクセスして、シスコのテクニカル サポートを最大限に活用してください。これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

VASI インターフェイス経由の IPv6 ゾーンベース ファイアウォール サポートに関する機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだ

けを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *182 : VASI* インターフェイス経由の *IPv6* ゾーンベース ファイアウォール サポートに関する機能情報

機能名	リリース	機能情報
VASI インターフェイス経由の IPv6 ゾーンベース ファイアウォール サポート	Cisco IOS XE リリース 3.7S	この機能は、IPv6 ファイアウォール経由の VASI インターフェイスをサポートします。この機能により、アクセス コントロール リスト（ACL）、ネットワーク アドレス変換（NAT）、ポリシング、ゾーンベース ファイアウォールなどのサービスを、2 つの異なる Virtual Routing and Forwarding（VRF）インスタンスの間を流れるトラフィックに適用できます。VASI インターフェイスは、ルート プロセッサ（RP）とフォワーディング プロセッサ（FP）の冗長性をサポートします。VASI インターフェイスは IPv4 および IPv6 ユニキャスト トラフィックをサポートします。 この機能について導入または変更されたコマンドはありません。

第 137 章

VRF 対応ソフトウェア インフラストラクチャの設定

VRF 対応ソフトウェア インフラストラクチャ機能を使用すると、アクセス コントロール リスト（ACL）、ネットワーク アドレス変換（NAT）、ポリシング、ゾーンベース ファイアウォールなどのサービスを、2 つの異なる仮想ルーティングおよび転送（VRF）インスタンスを通過するトラフィックに適用できます。VRF 対応ソフトウェア インフラストラクチャ（VASI）インターフェイスは、ルート プロセッサ（RP）と転送プロセッサ（FP）の冗長性、IPSec、および IPv4 と IPv6 のユニキャストおよびマルチキャスト トラフィックをサポートします。

このモジュールでは、VASI インターフェイスを設定する方法について説明します。

VRF 対応ソフトウェア インフラストラクチャに関する制約事項

- VRF 対応ソフトウェア インフラストラクチャ（VASI）インターフェイス経由のマルチプロトコル ラベル スイッチング（MPLS）トラフィックはサポートされません。
- VASI インターフェイスは、キュー ベース機能のアタッチメントをサポートしません。以下のコマンドは、VASI インターフェイスにアタッチされたモジュラ QoS CLI（MQC）ポリシーでサポートされません。
  - **bandwidth (policy-map class)**
  - **fair-queue**
  - **priority**
  - **queue-limit**

- **random-detect**
- **shape**

- VASI 2000 ペアは、Open Shortest Path First（OSPF）でサポートされていません。
- VASI インターフェイス上のマルチキャスト ファースト ホップおよびマルチキャスト パント パケットがサポートされていないため、VASI はサポートされません。
- Web Cache Communication Protocol（WCCP）はサポートされていません。

VRF 対応ソフトウェア インフラストラクチャの設定について

VASI の概要

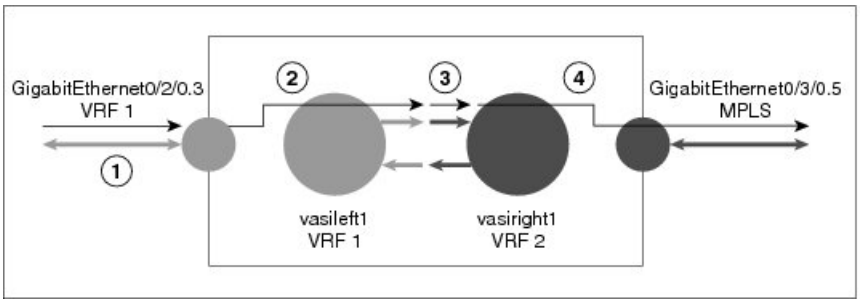
VRF 対応ソフトウェア インフラストラクチャ（VASI）を使用すると、ファイアウォール、GETVPN、IPsec、およびネットワークアドレス変換（NAT）などのサービスを、異なる仮想ルーティングおよび転送（VRF）インスタンスを横断するトラフィックに適用できます。VASI は仮想インターフェイスのペアを使用して実行され、ペア内の各インターフェイスは別の VRF インスタンスに関連付けられます。VASI 仮想インターフェイスは、これら 2 つの VRF インスタンス間で切り替える必要がある、すべてのパケットのネクストホップ インターフェイスです。VASI インターフェイスは、VRF インスタンス間にファイアウォールまたは NAT を設定するためのフレームワークを提供します。

各インターフェイス ペアは、異なる 2 つの VRF インスタンスに関連付けられています。ペアリングは、vasileft インターフェイスが自動的に vasiright インターフェイスへのペアとなるように、2 つのインターフェイスのインデックスに基づいて自動的に行われます。たとえば、下の図では、vasileft1 と vasiright1 は自動的にペアになり、vasileft1 に入るパケットは vasiright1 に内部的に渡されます。

VASI インターフェイスでは、内部ボーダー ゲートウェイ プロトコル（IBGP）、Enhanced Interior Gateway Routing Protocol（EIGRP）、および Open Shortest Path First（OSPF）を使用して、スタティック ルーティングまたはダイナミック ルーティングのいずれかを設定できます。

次の図は、同じデバイスの VRF 間 VASI 設定を示しています。

図 *73 : VRF* 間 *VASI* 設定



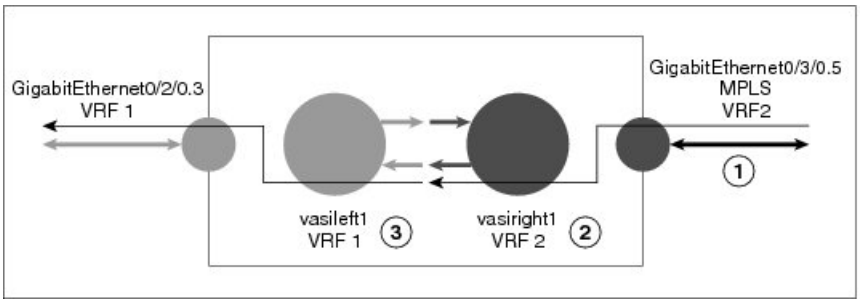
VRF 間 VASI が同じデバイス上で設定されている場合、パケット フローは次の順序で発生します。

1. パケットが VRF 1（ギガビット イーサネット 0/2/0.3）に属する物理インターフェイスに入ります。
2. パケットを転送する前に、VRF1 ルーティング テーブルでフォワーディング ルックアップが実行されます。Vasileft1 がネクスト ホップとして選択され、存続可能時間（TTL）値がパケットから引かれます。通常、フォワーディング アドレスは VRF のデフォルト ルートに基づいて選択されます。ただし、フォワーディング アドレスはスタティック ルートまたは学習したルートになる可能性もあります。パケットは vasileft1 の出力パスに送信されてから、vasiright1 入力パスに自動的に送信されます。
3. パケットが vasiright1 に入ると、VRF 2 ルーティング テーブルでフォワーディング ルックアップが実行され、TTL が再度減らされます（このパケットでは 2 回目）。
4. VRF 2 はパケットを物理インターフェイス、ギガビット イーサネット 0/3/0.5 へ転送します。

次の図は VASI がマルチプロトコル ラベル スイッチング（MPLS）VPN 設定で機能するしくみを示します。

（注） 次の図で、MPLS はギガビット イーサネット インターフェイスで有効になっていますが、MPLS トラフィックは VASI ペア間ではサポートされていません。

図 *74 : MPLS VPN* 設定を使用する *VASI*



VASI がマルチプロトコル ラベル スイッチング（MPLS）VPN を使用して設定されている場合、パケット フローは次の順序で発生します。

1. パケットが VPN ラベルを持つ MPLS インターフェイスに到着します。
2. VPN ラベルがパケットから取り除かれ、VRF 2 でフォワーディング ルックアップが実行され、パケットが vasiright1 に転送されます。TTL 値がパケットから引かれます。
3. パケットが入力パスの vasileft1 に入り、別のフォワーディング ルックアップが VRF1 で行われます。パケットが VRF1 の出力物理インターフェイス（ギガビット イーサネット 0/2/0.3）に送信されます。TTL がパケットから再度減らされます。

VASI でのマルチキャストおよびマルチキャスト VPN

VRF 対応サービス インフラストラクチャ（VASI）は、ゾーンベース ファイアウォール、ネットワーク アドレス変換（NAT）、IPsec などのサービスを、異なる Virtual Routing and Forwarding（VRF）インスタンスの間を移動するトラフィックに適用します。VASI 上のマルチキャストと MVPN 機能は、VASI インターフェイスで IPv4 と IPv6 のマルチキャストとマルチキャスト VPN（MVPN）をサポートします。この機能は、顧客サイトで設定されたマルチキャスト モード（Sparse や Source-Specific Multicast（SSM）など）や、コア ネットワーク内の MVPN モード（Generic Routing Encapsulation（GRE）ベースまたは Multicast Label Distribution Protocol（MLDP）ベース）に影響されません。

マルチキャストは単一の情報ストリームを場合によっては何千もの受信者に同時に配信することによって、ネットワーク内のトラフィックを削減します。マルチキャストは送信元または受信者に負荷をかけることなくアプリケーションから複数の受信者にソース トラフィックを配信するため、最小限のネットワーク帯域幅が使用されることになります。マルチキャスト VPN（MVPN）機能は、レイヤ 3 VPN 上でマルチキャストをサポートできるようにします。

VASI の実装に使用する仮想インターフェイスのペアは、それぞれに異なる VRF に関連付けられます。VASI 仮想インターフェイスは、この 2 つの VRF 間でスイッチングする必要があるすべてのパケットのネクスト ホップ インターフェイスになります。VASI インターフェイスは仮想インターフェイスであり、IP アドレスや、他の論理インターフェイスなどの他のサービスを設定できます。この機能を有効にするには、VASI インターフェイス ペアでマルチキャストを有効にする必要があります。

VRF 対応ソフトウェア インフラストラクチャの設定方法

VASI インターフェイス ペアの設定

VRF 対応ソフトウェア インフラストラクチャ（VASI）のインターフェイスペアを設定するには、1 つのインターフェイスで **interface vasileft** コマンドを設定し、2 番目のインターフェイスで **interface vasiright** コマンドを設定する必要があります。vasileft を vasiright とペアにするにはインターフェイス番号を同じにする必要があります。任意の VASI インターフェイスで Virtual Routing and Forwarding（VRF）インスタンスを設定できます。

手順の概要

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **vrf forwarding** *table-name*
5. **ip address** {*ip-address mask* [**secondary**] | **pool** *pool-name*}
6. **exit**
7. **ip route** [**vrf** *vrf-name*] *destination-prefix destination-prefix-mask interface-type interface-number*
8. **interface** *type number*
9. **vrf forwarding** *table-name*
10. **ip address** {*ip-address mask* [**secondary**] | **pool** *pool-name*}
11. **exit**
12. **ip route** [**vrf** *vrf-name*] *destination-prefix destination-prefix-mask interface-type interface-number*
13. **end**

手順の詳細

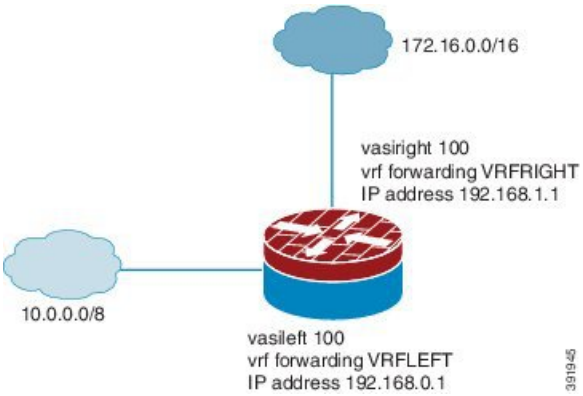
	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface** *type number* 例： `Device(config)# interface vasileft 100`	VASI インターフェイスを設定し、インターフェイス コンフィギュレーション モードを開始します。 • この例では、vasileft インターフェイスが設定されます。
ステップ 4	**vrf forwarding** *table-name* 例： `Device(config-if)# vrf forwarding VRFLEFT`	VRF テーブルを設定します。 （注） 任意の VASI インターフェイスで VRF 転送を設定できます。両方の VASI インターフェイスで VRF インスタンスを設定する必要はありません。
ステップ 5	**ip address** {*ip-address mask* [**secondary**]	**pool** *pool-name*} 例： `Device(config-if)# ip address 192.168.0.1 255.255.255.0`	インターフェイスのプライマリ IP アドレスまたはセカンダリ IP アドレスを設定します。

	コマンドまたはアクション	目的
ステップ 6	**exit** 例： `Device(config-if)# exit`	インターフェイス コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードに入ります。
ステップ 7	**ip route** [**vrf** *vrf-name*] *destination-prefix destination-prefix-mask interface-type interface-number* 例： `Device(config)# ip route vrf VRFLEFT 172.16.0.0 255.255.0.0 VASILEFT 100`	VRF インスタンスおよび VASI インターフェイスのスタティック ルートを確立します。 （注） VRF インスタンスの IP ルートを追加するには、**vrf** キーワードを指定する必要があります。
ステップ 8	**interface** *type number* 例： `Device(config)# interface vasiright 100`	VASI インターフェイスを設定し、インターフェイス コンフィギュレーション モードを開始します。 • この例では、vasiright インターフェイスが設定されます。
ステップ 9	**vrf forwarding** *table-name* 例： `Device(config-if)# vrf forwarding VRFRIGHT`	VRF テーブルを設定します。
ステップ 10	**ip address** {*ip-address mask* [**secondary**] | **pool** *pool-name*} 例： `Device(config-if)# ip address 192.168.1.1 255.255.255.0`	インターフェイスのプライマリ IP アドレスまたはセカンダリ IP アドレスを設定します。
ステップ 11	**exit** 例： `Device(config-if)# exit`	インターフェイス コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードに入ります。
ステップ 12	**ip route** [**vrf** *vrf-name*] *destination-prefix destination-prefix-mask interface-type interface-number* 例： `Device(config)# ip route vrf VRFRIGHT 10.0.0.0 255.0.0.0 VASIRIGHT 100`	VRF インスタンスおよび VASI インターフェイスのスタティック ルートを確立します。 （注） VRF インスタンスの IP ルートを追加するには、**vrf** キーワードを指定する必要があります。
ステップ 13	**end** 例： `Device(config)# end`	グローバル コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

VRF 対応ソフトウェア インフラストラクチャの設定例

例：VASI インターフェイス ペアの設定

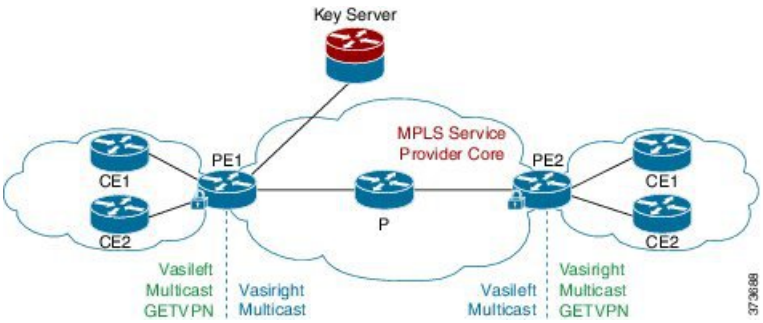
Virtual Routing and Forwarding（VRF）インスタンスは、VASI ペア（VASILEFT と VASIRIGHT）のインターフェイスごとに有効にする必要があります。次に、VASI インターフェイス ペアを設定する例を示します。




```
Device(config)# interface vasileft 100
Device(config-if)# vrf forwarding VRFLEFT
Device(config-if)# ip address 192.168.0.1 255.255.255.0
Device(config-if)# exit
Device(config)# ip route vrf VRFLEFT 172.16.0.0 255.255.0.0 vasileft 100
Device(config)# interface vasiright 100
Device(config-if)# vrf forwarding VRFRIGHT
Device(config-if)# ip address 192.168.1.1 255.255.255.0
Device(config-if)# exit
Device(config)# ip route vrf VRFRIGHT 10.0.0.0 255.0.0.0 vasiright 100
Device(config)# end
```

例：VASI 上のマルチキャストと MVPN の設定

図 *75 : GRE* ベースの *MVPN* と *GETVPN* の設定



次に、VASI インターフェイス ペア上で Generic Routing Encapsulation（GRE）ベースのマルチキャスト VPN（MVPN）と GETVPN を設定する例を示します。ここでは、暗号マップが vasileft インターフェイスに適用されます。vasileft インターフェイスは、カスタマーエッジ（CE）デバイスとして機能し、暗号化を実行します。このインターフェイスは、vrf-cust1 Virtual Routing and Forwarding（VRF）インスタンスの一部です。vasiright インターフェイスは、マルチプロトコル ラベル スイッチング（MPLS）コア上と適用先の暗号サービス宛てにトラフィックを通過させる vrf-core1 VRF インスタンスの一部です。コア ネットワークはマルチキャストをサポートし、VRF 内のマルチキャストはステートフル スイッチオーバー（SSO）モードになります。

```
! PE1 Configuration
Device(config)# vrf definition Mgmt-intf
Device(config-vrf)# address-family ipv4
Device(config-vrf-af)# exit-address-family
Device(config-vrf)# address-family ipv6
Device(config-vrf-af)# exit-address-family
Device(config-vrf)# exit
!
Device(config)# vrf definition vrf-core1
Device(config-vrf)# rd 2:1
Device(config-vrf)# address-family ipv4
Device(config-vrf-af)# mdt default 203.0.113.1 ! Enables GRE-based MVPN and mdt default
 tree
Device(config-vrf-af)# mdt data 203.0.113.33 255.255.255.224 ! Enables the mdt data tree
Device(config-vrf-af)# route-target export 2:1
Device(config-vrf-af)# route-target import 2:1
Device(config-vrf-af)# exit-address-family
Device(config-vrf)# address-family ipv6
Device(config-vrf-af)# mdt default 203.0.113.1
Device(config-vrf-af)# mdt data 203.0.113.33 255.255.255.224
Device(config-vrf-af)# route-target export 2:1
Device(config-vrf-af)# route-target import 2:1
Device(config-vrf-af)# exit-address-family
Device(config-vrf)# exit
!
Device(config)# vrf definition vrf-cust1
Device(config-vrf)# rd 1:1
Device(config-vrf)# address-family ipv4
Device(config-vrf-af)# exit-address-family
Device(config-vrf)# address-family ipv6
Device(config-vrf-af)# exit-address-family
Device(config-vrf)# exit
!
Device(config)# logging buffered 10000000
Device(config)# no logging console
!
Device(config)# no aaa new-model
Device(config)# clock timezone CST 8 0
!
Device(config)# ip multicast-routing distributed
Device(config)# ip multicast-routing vrf vrf-core1 distributed
Device(config)# ip multicast-routing vrf vrf-cust1 distributed
!
Device(config)# ipv6 unicast-routing
Device(config)# ipv6 multicast-routing
Device(config)# ipv6 multicast-routing vrf vrf-core1
Device(config)# ipv6 multicast-routing vrf vrf-cust1
!
Device(config)# subscriber templating
```

```
Device(config)# mpls label protocol ldp
Device(config)# multilink bundle-name authenticated
Device(config)# spanning-tree extend system-id
!
Device(config)# cdp run
Device(config)# ip ftp source-interface GigabitEthernet 0
Device(config)# ip tftp source-interface GigabitEthernet 0
Device(config)# ip tftp blocksize 8192
!
Device(config)# class-map match-any maincampus-ratelimit
Device(config-cmap)# match access-group 101
Device(config-cmap)# exit
!
Device(config)# policy-map transit-limt
Device(config-pmap)# description 160mb transit rate limit
Device(config-pmap)# class maincampus-ratelimit
Device(config-pmap-c)# police 160000000 30000000 60000000 conform-action transmit
exceed-action drop
Device(config-pmap-c-police)# exit
Device(config-pmap-c)# exit
Device(config-pmap)# exit
!
Device(config)# crypto keyring vrf-cust1 vrf vrf-cust1 ! enables GETVPN
Device(conf-keyring)# pre-shared-key address 0.0.0.0 0.0.0.0 key cisco
Device(conf-keyring)# exit
!
Device(config)# crypto isakmp policy 1
Device(config-isakmp)# encryption 3des
Device(config-isakmp)# authentication pre-share
Device(config-isakmp)# group 2
Device(config-isakmp)# exit
Device(config)# crypto isakmp key cisco address 10.0.3.2
!
Device(config)# crypto gdoi group secure-wan
Device(config-gkm-group)# identity number 12345
Device(config-gkm-group)# server address ipv4 10.0.3.4
Device(config-gkm-group)# exit
!
Device(config)# crypto gdoi group ipv6 ipv6-secure-wan
Device(config-gkm-group)# identity number 123456
Device(config-gkm-group)# server address ipv4 10.0.3.6
Device(config-gkm-group)# exit
!
Device(config)# crypto map getvpn 1 gdoi
Device(config-crypto-map)# set group secure-wan
Device(config-crypto-map)# exit
!
Device(config)# crypto map ipv6 getvpn-v6 1 gdoi
Device(config-crypto-map)# set group ipv6-secure-wan
Device(config-crypto-map)# exit
!
Device(config)# interface loopback 0
Device(config-if)# ip address 198.51.100.241 255.255.255.240
Device(config-if)# ip pim sparse-mode
Device(config-if)# ipv6 address 2001:DB8::1/32
Device(config-if)# ipv6 enable
Device(config-if)# ospfv3 100 ipv6 area 0
Device(config-if)# exit
!
Device(config)# interface GigabitEthernet 0/0/0
Device(config-if)# vrf forwarding vrf-cust1
Device(config-if)# ip address 192.0.2.1 255.255.255.240
```

```
Device(config-if)# shutdown
Device(config-if)# negotiation auto
!
Device(config)# interface GigabitEthernet 0/0/1
Device(config-if)# no ip address
Device(config-if)# negotiation auto
Device(config-if)# exit
!
Device(config)# interface GigabitEthernet 0/2/0
Device(config-if)# ip address 192.0.2.18 255.255.255.240
Device(config-if)# ip pim sparse-mode
Device(config-if)# negotiation auto
Device(config-if)# mpls ip
Device(config-if)# exit
!
Device(config)# interface GigabitEthernet 0/2/1
Device(config-if)# vrf forwarding vrf-cust1
Device(config-if)# ip address 10.0.3.1 255.255.255.0
Device(config-if)# negotiation auto
Device(config-if)# exit
!
Device(config)# interface GigabitEthernet 0/2/2
Device(config-if)# no ip address
Device(config-if)# negotiation auto
Device(config-if)# exit
!
Device(config)# interface GigabitEthernet 0/2/3
Device(config-if)# vrf forwarding vrf-cust1
Device(config-if)# ip address 192.0.2.34 255.255.255.240
Device(config-if)# ip pim sparse-mode
Device(config-if)# ip igmp version 3
Device(config-if)# negotiation auto
Device(config-if)# ipv6 address 2001:DB8:0000:0000:0000:0000:0000:0001/48
Device(config-if)# ospfv3 100 ipv6 area 0
Device(config-if)# exit
!
Device(config)# interface GigabitEthernet 0/2/4
Device(config-if)# no ip address
Device(config-if)# negotiation auto
Device(config-if)# exit
!
Device(config)# interface GigabitEthernet 0
Device(config-if)# vrf forwarding Mgmt-intf
Device(config-if)# ip address 10.74.30.161 255.255.255.0
Device(config-if)# negotiation auto
Device(config-if)# exit
!
Device(config)# interface vasileft 1 ! On the vasileft interface, enable multicast and
GETVPN.
Device(config-if)# vrf forwarding vrf-cust1
Device(config-if)# ip address 209.165.202.129 255.255.255.0
Device(config-if)# ip pim sparse-mode
Device(config-if)# ipv6 address FE80::CEEF:48FF:FEEA:C501 link-local
Device(config-if)# ipv6 address 2001:B000::2/64
Device(config-if)# ipv6 crypto map getvpn-v6
Device(config-if)# ospfv3 100 ipv6 area 0
Device(config-if)# no keepalive
Device(config-if)# crypto map getvpn
Device(config-if)# exit
!
Device(config)# interface vasiright 1 ! On the vasiright interface, only enable multicast.
Device(config-if)# vrf forwarding vrf-core1
```

```
Device(config-if)# ip address 209.165.202.130 255.255.255.0
Device(config-if)# ip pim sparse-mode
Device(config-if)# ipv6 address 2001:B000::1/64
Device(config-if)# ospfv3 100 ipv6 area 0
Device(config-if)# no keepalive
Device(config-if)# exit
!
Device(config)# router ospfv3 100
Device(config-router)# address-family ipv6 unicast
Device(config-router-af)# redistribute bgp 1
Device(config-router-af)# exit-address-family
!
Device(config-router)# address-family ipv6 unicast vrf vrf-cust1
Device(config-router-af)# redistribute bgp 1
Device(config-router-af)# exit-address-family
!
Device(config-router)# address-family ipv6 unicast vrf vrf-core1
Device(config-router-af)# redistribute bgp 1
Device(config-router-af)# exit-address-family
!
Device(config)# router ospf 1
Device(config-router)# network 1.1.1.1 0.0.0.0 area 0
Device(config-router)# network 192.0.2.0 0.0.0.255 area 0
Device(config-router)# exit
!
Device(config)# router bgp 1 ! Use BGP routing protocol to broadcast vrf-cust1 routing
entry.
Device(config-router)# bgp log-neighbor-changes
Device(config-router)# neighbor 172.16.0.1 remote-as 1
Device(config-router)# neighbor 172.16.0.1 update-source Loopback0
!
Device(config-router)# address-family ipv4
Device(config-router-af)# neighbor 172.16.0.1 activate
Device(config-router-af)# neighbor 172.16.0.1 send-community both
Device(config-router-af)# exit-address-family
!
Device(config-router)# address-family vpnv4
Device(config-router-af)# neighbor 172.16.0.1 activate
Device(config-router-af)# neighbor 172.16.0.1 send-community both
Device(config-router-af)# exit-address-family
!
Device(config-router)# address-family ipv4 mdt ! For MVPN neighbor setup
Device(config-router-af)# neighbor 172.16.0.1 activate
Device(config-router-af)# neighbor 172.16.0.1 send-community both
Device(config-router-af)# exit-address-family
!
Device(config-router)# address-family vpnv6
Device(config-router-af)# neighbor 192.168.0.1 activate
Device(config-router-af)# neighbor 192.168.0.1 send-community both
Device(config-router-af)# exit-address-family
!
Device(config-router)# address-family ipv4 vrf vrf-core1
Device(config-router-af)# bgp router-id 209.165.202.130
Device(config-router-af)# redistribute connected
Device(config-router-af)# neighbor 209.165.202.129 remote-as 65002
Device(config-router-af)# neighbor 209.165.202.129 local-as 65001 no-prepend replace-as
Device(config-router-af)# neighbor 209.165.202.129 activate
Device(config-router-af)# exit-address-family
!
Device(config-router)# address-family ipv6 vrf vrf-core1
Device(config-router-af)# redistribute connected
Device(config-router-af)# redistribute ospf 100 include-connected
```

```
Device(config-router-af)# bgp router-id 209.165.202.130
Device(config-router-af)# neighbor 2001:B000::2 remote-as 10000
Device(config-router-af)# neighbor 2001:B000::2 local-as 65000 no-prepend replace-as
Device(config-router-af)# neighbor 2001:B000::2 activate
Device(config-router-af)# exit-address-family
!
Device(config-router)# address-family ipv4 vrf vrf-cust1
Device(config-router-af)# bgp router-id 209.165.202.129
Device(config-router-af)# redistribute connected
Device(config-router-af)# neighbor 209.165.202.130 remote-as 65001
Device(config-router-af)# neighbor 209.165.202.130 local-as 65002 no-prepend replace-as
Device(config-router-af)# neighbor 209.165.202.130 activate
Device(config-router-af)# exit-address-family
Device(config-router)# exit
!
Device(config-router)# address-family ipv6 vrf vrf-cust1
Device(config-router-af)# redistribute connected
Device(config-router-af)# redistribute ospf 100 include-connected
Device(config-router-af)# bgp router-id 209.165.202.129
Device(config-router-af)# neighbor 2001:B000::1 remote-as 65000
Device(config-router-af)# neighbor 2001:B000::1 local-as 10000 no-prepend replace-as
Device(config-router-af)# neighbor 2001:B000::1 activate
Device(config-router-af)# exit-address-family
!
Device(config)# ip forward-protocol nd
!
Device(config)# no ip http server
Device(config)# no ip http secure-server
Device(config)# ip pim rp-address 1.1.1.1
Device(config)# ip pim vrf vrf-core1 ssm default
Device(config)# ip pim vrf vrf-cust1 ssm default
Device(config)# ip route 192.0.2.0 255.255.255.240 10.11.12.10
Device(config)# ip route vrf Mgmt-intf 0.0.0.0 0.0.0.0 10.74.9.1
!
Device(config)# ip access-list standard bidir
Device(config-std-nacl)# exit
!
Device(config)# access-list 101 deny ip 198.51.100.1 255.255.255.240 198.51.100.177
255.255.255.240
Device(config)# ipv6 router eigrp 300
Device(config-rtr)# passive-interface Loopback 0
Device(config-rtr)# redistribute connected
Device(config-rtr)# exit
!
Device(config)# mpls ldp router-id Loopback 0
Device(config)# control-plane
Device(config-cp)# exit
!
Device(config)# line con 0
Device(config-line)# exec-timeout 0 0
Device(config-line)# privilege level 15
Device(config-line)# logging synchronous
Device(config-line)# stopbits 1
Device(config-line)# exit
Device(config)# line vty 0 4
Device(config-line)# exec-timeout 0 0
Device(config-line)# privilege level 15
Device(config-line)# logging synchronous
Device(config-line)# no login
Device(config-line)# end
```

マルチキャスト VASI 設定の確認

マルチキャスト VRF 対応ソフトウェア インフラストラクチャ（VASI）設定を確認するには、次のコマンドを使用します。

手順の概要

1. **enable**
2. **show ip mroute**
3. **show ip mroute vrf**

手順の詳細

ステップ 1 enable

特権 EXEC モードを有効にします。

- パスワードを入力します（要求された場合）。

例：

```
Device> enable
```

ステップ 2 show ip mroute

マルチキャスト ルーティング（mroute）テーブルの内容を表示します。

例：

```
Device# show ip mroute

IP Multicast Routing Table
Flags: D - Dense, S - Sparse, B - Bidir Group, s - SSM Group, C - Connected,
       L - Local, P - Pruned, R - RP-bit set, F - Register flag,
       T - SPT-bit set, J - Join SPT, M - MSDP created entry, E - Extranet,
       X - Proxy Join Timer Running, A - Candidate for MSDP Advertisement,
       U - URD, I - Received Source Specific Host Report,
       Z - Multicast Tunnel, z - MDT-data group sender,
       Y - Joined MDT-data group, y - Sending to MDT-data group,
       G - Received BGP C-Mroute, g - Sent BGP C-Mroute,
       N - Received BGP Shared-Tree Prune, n - BGP C-Mroute suppressed,
       Q - Received BGP S-A Route, q - Sent BGP S-A Route,
       V - RD & Vector, v - Vector, p - PIM Joins on route,
       x - VxLAN group
Outgoing interface flags: H - Hardware switched, A - Assert winner, p - PIM Join
 Timers: Uptime/Expires
 Interface state: Interface, Next-Hop or VCD, State/Mode
(*, 203.0.113.1), 04:33:39/stopped, RP 0.0.0.0, flags: D
  Incoming interface: Null, RPF nbr 0.0.0.0
  Outgoing interface list:
    GigabitEthernet0/0/2, Forward/Sparse-Dense, 04:33:39/stopped
    GigabitEthernet0/0/0, Forward/Sparse-Dense, 04:33:39/stopped
(10.0.0.3, 203.0.113.1), 04:33:36/00:00:36, flags: T
  Incoming interface: GigabitEthernet0/0/2, RPF nbr 10.1.1.3
  Outgoing interface list:
    GigabitEthernet0/0/0, Forward/Sparse-Dense, 04:33:36/stopped
(10.0.0.1, 203.0.113.1), 04:33:39/00:02:44, flags: T
  Incoming interface: GigabitEthernet0/0/0, RPF nbr 10.1.1.0
  Outgoing interface list:
```

```
    GigabitEthernet0/0/2, Forward/Sparse-Dense, 04:33:39/stopped
```

ステップ 3　show ip mroute vrf

出力をフィルタして、*vrf-name* 引数で指定された、マルチキャスト VPN（MVPN）ルーティングおよび転送（MVRF）インスタンスに関する、マルチキャスト ルーティング テーブルの内容だけを表示します。

例：

```
Device# show ip mroute vrf cust1

(10.2.1.1, 203.1.113.4), 00:40:09/00:02:44, flags: sTI
  Incoming interface: vasileft1, RPF nbr 36.1.1.2
  Outgoing interface list:
    GigabitEthernet0/0/1.1, Forward/Sparse-Dense, 00:40:09/00:02:44
PE1#sh ip mroute vrf cust1-core
(10.2.1.1, 203.1.113.4), 04:22:09/00:02:50, flags: sT
  Incoming interface: Tunnel0, RPF nbr 10.0.0.3
  Outgoing interface list:
    vasiright1, Forward/Sparse-Dense, 04:22:09/00:02:50
PE1#sh ip mroute
(*, 203.1.113.4), 21:08:36/stopped, RP 0.0.0.0, flags: DCZ
  Incoming interface: Null, RPF nbr 0.0.0.0
  Outgoing interface list:
    GigabitEthernet0/0/0, Forward/Sparse-Dense, 04:27:50/stopped
    MVRF cust1-core, Forward/Sparse-Dense, 21:06:53/stopped
(10.0.0.3, 203.1.113.4), 04:26:53/00:01:22, flags: TZ
  Incoming interface: GigabitEthernet0/0/0, RPF nbr 10.1.1.1
  Outgoing interface list:
    MVRF cust1-core, Forward/Sparse-Dense, 04:26:53/stopped
```

VRF 対応ソフトウェア インフラストラクチャの設定に関する追加情報

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『Cisco IOS Master Command List, All Releases』

関連項目	マニュアル タイトル
セキュリティ コマンド	• 『Cisco IOS Security Command Reference: Commands A to C』 • 『Cisco IOS Security Command Reference: Commands D to L』 • 『Cisco IOS Security Command Reference: Commands M to R』 • 『Cisco IOS Security Command Reference: Commands S to Z』

シスコのテクニカル サポート

説明	リンク
右の URL にアクセスして、シスコのテクニカル サポートを最大限に活用してください。これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

VRF 対応ソフトウェア インフラストラクチャの設定に関する機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *183 : VRF* 対応ソフトウェア インフラストラクチャの設定に関する機能情報

機能名	リリース	機能情報
VASI でのマルチキャストおよびマルチキャスト VPN	Cisco IOS XE リリース 3.14S	VASI 上のマルチキャストと MVPN 機能は、VASI インターフェイスで IPv4 と IPv6 のマルチキャストとマルチキャスト VPN（MVPN）をサポートします。この機能は、顧客サイトで設定されたマルチキャストモード（Sparse や Source-Specific Multicast（SSM）など）や、コア ネットワーク内の MVPN モード（Generic Routing Encapsulation（GRE）ベースまたは Multicast Label Distribution Protocol（MLDP）ベース）に影響されません。 この機能のために導入または変更された新しいコマンドはありません。
VRF 対応ソフトウェア インフラストラクチャ	Cisco IOS XE リリース 2.6	VRF 対応ソフトウェア インフラストラクチャ機能を使用すれば、2 つの異なる VRF インスタンスを経由するトラフィックに ACL、NAT、ポリシング、ゾーンベースファイアウォールなどのサービスを適用することができます。VRF 対応ソフトウェア インフラストラクチャ（VASI）インターフェイスは、RP と FP の冗長性をサポートします。この機能は、VASI インターフェイス上で IPv4 と IPv6 のユニキャスト トラフィックとマルチキャスト トラフィックをサポートします。
VASI（VRF 対応ソフトウェア インフラストラクチャ）拡張機能フェーズ I	Cisco IOS XE リリース 3.1S	VASI 強化フェーズ I 機能は、以下の強化を VASI に提供します。 • 500 VASI インターフェイスのサポート。 • VASI インターフェイス間の IBGP ダイナミック ルーティングのサポート。

機能名	リリース	機能情報
VASI（VRF 対応ソフトウェア インフラストラクチャ）強化フェーズ II	Cisco IOS XE リリース 3.2S	VASI 強化フェーズ II 機能は、以下の強化を VASI に提供します。 • VASI インターフェイス上の IPv6 ユニキャスト トラフィックのサポート。 • VASI インターフェイス間の OSPF および EIGRP ダイナミック ルーティングのサポート。
VASI（VRF 対応ソフトウェア インフラストラクチャ）スケール	Cisco IOS XE リリース 3.3S	VASI スケール機能は、1000 VASI インターフェイスをサポートします。 次のコマンドが導入または変更されました。**interface (VASI)**。
VASI（VRF 対応ソフトウェア インフラストラクチャ）スケール	Cisco IOS XE リリース 3.7.2S	VASI スケール機能は、VASI インターフェイス間の eBGP ダイナミックルーティングをサポートします。
VASI 2000 ペア スケール	Cisco IOS XE リリース 3.10S	VASI 2000 ペア スケール機能は、2000 VASI インターフェイスをサポートします。2000 VASI インターフェイスは、Border Gateway Protocol（BGP）でサポートされます。 次のコマンドが導入または変更されました。**interface (VASI)**。

第 138 章

IPv6 ファイアウォールに対する FTP66 ALG サポート

IPv6 ファイアウォールの FTP66 ALG サポート機能により、FTP を IPv6 ファイアウォールと連動させることができます。このモジュールでは、FTP66 アプリケーション レベル ゲートウェイ（ALG）と連動するようにファイアウォール、ネットワーク アドレス変換（NAT）、およびステートフル NAT64 を設定する方法を説明します。

IPv6 ファイアウォールに対する FTP66 ALG サポートに関する制約事項

FTP66 ALG は以下をサポートしません。

- ボックスツーボックス ハイアベイラビリティ。
- サブスクライバ単位のファイアウォール。
- ステートレス ネットワーク アドレス変換 64（NAT64）。
- ステートフル NAT64 が設定されている場合の Virtual Routing and Forwarding（VRF）。
- 仮想 TCP（vTCP）または変換後の小パケットへのパケット分割。

IPv6 ファイアウォールに対する FTP66 ALG サポートに関する情報

アプリケーション レベル ゲートウェイ

アプリケーション レベル ゲートウェイ（ALG）は、アプリケーション レイヤ ゲートウェイとも呼ばれ、アプリケーションパケットのペイロード内のIPアドレス情報を変換するアプリケーションです。ALG は、アプリケーション レイヤ プロトコルを解釈し、ファイアウォールおよびネットワーク アドレス変換（NAT）アクションを実行するために使用されます。これらのアクションは、ファイアウォールおよび NAT の設定に応じて次の 1 つまたは複数のアクションになります。

- クライアント アプリケーションが、ダイナミック TCP または UDP ポートを使用してサーバ アプリケーションと通信できるようにします。
- アプリケーション固有のコマンドを認識し、これらのコマンドに対するきめ細かいセキュリティ制御を提供します。
- データ交換を行う 2 つのホスト間の複数のデータ ストリームまたはデータ セッションを同期します。
- アプリケーション ペイロードで使用できるネットワーク層アドレス情報を変換します。

ファイアウォールがピンホールを開き、アプリケーション レイヤ データストリームの送信元 IP アドレスおよび宛先 IP アドレスを伝送しない TCP または UDP トラフィックに対する変換サービスを NAT が実行します。IP アドレス情報を埋め込む特定のプロトコルまたはアプリケーションには ALG のサポートが必要です。

FTP66 ALG サポートの概要

ファイアウォールでは、IPv6 パケットとステートフル ネットワーク アドレス変換 64（NAT64）のインスペクションをサポートしています。FTP を IPv6 パケット インスペクションに基づいて機能させるには、アプリケーション層ゲートウェイ（ALG）（別名アプリケーション レベル ゲートウェイ（ALG））FTP66 が必要です。FTP66 ALG は、オールインワン FTP ALG およびワン FTP ALG とも呼ばれています。

FTP66 ALG では、次の機能をサポートしています。

- ファイアウォール IPv4 パケット インスペクション
- ファイアウォール IPv6 パケット インスペクション
- NAT の設定
- NAT64 の設定（FTP64 サポートを使用）

- NAT とファイアウォールの設定
- NAT64 とファイアウォールの設定

FTP66 ALG には、次のセキュリティ上の脆弱性があります。

- パケット セグメンテーション攻撃：FTP ALG ステート マシンではセグメント化されたパケットを検出できます。完全なパケットを受信するまで、ステートマシンの処理は停止します。
- バウンス攻撃：FTP ALG は、番号が 1024 未満のデータ ポートでドア（NAT の場合）やピンホール（ファイアウォールの場合）を作成しません。バウンス攻撃の防止がアクティブになるのは、ファイアウォールが有効にされている場合のみです。

FTP66 ALG でサポートされる FTP コマンド

FTP66 アプリケーション レベル ゲートウェイ（ALG）は、RFC 959 に基づいています。この項では、FTP66 ALG が処理する、RFC 959 および RFC 2428 の主要な FTP コマンドと応答について説明します。

PORT コマンド

PORT コマンドは、アクティブ FTP モードで使用されます。PORT コマンドでは、サーバの接続先とするアドレスとポート番号を指定します。このコマンドを使用する際の引数は、32 ビットのインターネットホストアドレスと 16 ビットの TCP ポートアドレスを連結したものです。このアドレス情報は 8 ビットのフィールドに分割されて、各フィールドの値が 10 進数（文字列表現）として送信されます。フィールドはカンマで区切ります。

次に示す PORT コマンドの例では、*h1* がインターネット ホスト アドレスの最上位 8 ビットです。

```
PORT h1,h2,h3,h4,p1,p2
```

PASV コマンド

PASV コマンドは、サーバに対し、TRANSFER コマンドの受信時に別の接続を開始するのではなく、サーバのデフォルト以外のデータ ポートでリッスンして接続を待機するよう要求します。PASV コマンドへの応答には、サーバがリッスンしているホストおよびポート アドレスが組み込まれます。

拡張 FTP コマンド

拡張 FTP コマンドは、FTP で IPv4 以外のネットワーク プロトコルのデータ接続エンドポイント情報を伝える手段になります。拡張 FTP コマンドは、RFC 2428 で規定されています。RFC 2428 では、拡張 FTP コマンドの EPRT と EPSV が FTP コマンドの PORT と PASV にそれぞれ置き換わっています。

EPRT コマンド

EPRTコマンドでは、データ接続の拡張アドレスを指定できます。拡張アドレスは、ネットワークプロトコル、ネットワークアドレス、トランスポートアドレスで構成する必要があります。EPRT コマンドの形式は次のとおりです。

```
EPRT<space><d><net-prt><d><net-addr><d><tcp-port><d>
```

- <net-prt> 引数はアドレス ファミリ番号であり、次の表に示すように定義する必要があります。

表 *184 : <net-prt>* 引数の定義

アドレス ファミリ番号	プロトコル
1	IPv4（Pos81a）
2	IPv6（DH96）

- <net-addr>引数は、プロトコル固有のネットワーク アドレスの文字列表現です。上記の表で指定されているアドレス ファミリ番号（アドレス ファミリ番号1と2）は、次の表に記載するアドレス形式にする必要があります。

アドレス ファミリ番号	アドレス形式	例
1	ドット付き 10 進法	10.135.1.2
2	DH96 で定義されている IPv6 文字列形式	2001:DB8:1::1

- <tcp-port> 引数は、ホストがデータ接続をリッスンしている TCP ポート番号の文字列形式にする必要があります。
- 次のコマンドは、サーバに対し、IPv4 アドレスを使用してホスト 10.235.1.2 へのデータ接続を TCP ポート 6275 で開くように指示する方法を示しています。

```
EPRT |1|10.235.1.2|6275|
```

- 次のコマンドは、サーバに対し、IPv6 ネットワーク プロトコルとネットワーク アドレスを使用して TCP データ接続をポート 5282 で開くように指示する方法を示しています。

```
EPRT |2|2001:DB8:2::2:417A|5282|
```

- <d> 引数は区切り文字です。この引数は、ASCII 形式の 33 から 126 までの範囲の値にする必要があります。

EPSV コマンド

EPSV コマンドでは、サーバに対し、データ ポートでリッスンして接続を待機するよう要求します。このコマンドの応答には、リッスンする接続の TCP ポート番号だけが組み込まれます。拡張アドレスを使用してパッシブ モードを開始するための応答コードは 229 です。

EPSV コマンドに対して返されるテキストは、次の形式になります。

```
(<d><d><d><tcp-port><d>)
```

- カッコで囲まれた文字列の部分は、EPRT コマンドでデータ接続を開くために必要な文字列と正確に一致する必要があります。

  カッコ内の最初の2つのフィールドは空白でなければなりません。3番目のフィールドは、サーバがデータ接続をリッスンしている TCP ポート番号の文字列表現でなければなりません。データ接続で使用されるネットワーク プロトコルは、制御接続で使用されるネットワーク プロトコルと同じです。データ接続を確立するために使用されるネットワーク アドレスは、制御接続に使用されるネットワーク アドレスと同じです。

- 次に、応答文字列の例を示します。

  ```
  Entering Extended Passive Mode (|||6446|)
  ```

次の FTP 応答およびコマンドも、FTP66 ALG によって処理されます。これらのコマンドの実行結果は、ステート マシンの遷移を操作するために使用されます。

- 230 応答メッセージ
- AUTH
- USER
- PASS

IPv6 ファイアウォールに対する FTP66 ALG サポートの設定方法

FTP66 ALG サポート用のファイアウォールの設定

match protocol ftp コマンドを使用して FTP66 ALG を明示的にイネーブルにする必要があります。

手順の概要

1. **enable**
2. **configure terminal**
3. **class-map type inspect match-any** *class-map-name*
4. **match protocol** *protocol-name*
5. **exit**
6. **policy-map type inspect** *policy-map-name*
7. **class type inspect** *class-map-name*
8. **inspect**
9. **exit**
10. **class class-default**
11. **exit**

12. **exit**
13. **zone security** *zone-name*
14. **exit**
15. **zone-pair security** *zone-pair* **source** *source-zone* **destination** *destination-zone*
16. **service-policy type inspect** *policy-map-name*
17. **exit**
18. **interface** *type number*
19. **no ip address**
20. **ip virtual-reassembly**
21. **zone-member security** *zone-name*
22. **negotiation auto**
23. **ipv6 address** *ipv6-address/prefix-length*
24. **cdp enable**
25. **exit**
26. **ipv6 route** *ipv6-prefix/prefix-length interface-type interface-number*
27. **ipv6 neighbor** *ipv6-address interface-type interface-number hardware-address*
28. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**class-map type inspect match-any** *class-map-name* 例： `Device(config)# class-map type inspect match-any in2out-class`	検査タイプ クラス マップを作成し、QoS クラス マップ コンフィギュレーション モードを開始します。
ステップ 4	**match protocol** *protocol-name* 例： `Device(config-cmap)# match protocol ftp`	指定されたプロトコルに基づいて、クラス マップの一致基準を設定します。
ステップ 5	**exit** 例： `Device(config-cmap)# exit`	QoS クラス マップ コンフィギュレーション モードを終了し、グローバルコンフィギュレーションモードを開始します。

	コマンドまたはアクション	目的
ステップ 6	**policy-map type inspect** *policy-map-name* 例： `Device(config)# policy-map type inspect in-to-out`	検査タイプ ポリシー マップを作成し、QoS ポリシー マップ コンフィギュレーション モードを開始します。
ステップ 7	**class type inspect** *class-map-name* 例： `Device(config-pmap)# class type inspect in2out-class`	アクションを実行する対象のクラスを指定し、QoS ポリシー マップ クラス コンフィギュレーション モードを開始します。
ステップ 8	**inspect** 例： `Device(config-pmap-c)# inspect`	ステートフル パケット インスペクションをイネーブルにします。
ステップ 9	**exit** 例： `Device(config-pmap-c)# exit`	QoS ポリシー マップ クラス コンフィギュレーション モードを終了し、QoS ポリシー マップ コンフィギュレーション モードを開始します。
ステップ 10	**class class-default** 例： `Device(config-pmap)# class class-default`	定義済みのデフォルト クラスにポリシー マップ設定を適用して、QoS ポリシー マップ クラス コンフィギュレーション モードを開始します。 • 設定済みクラス マップのどの一致基準ともトラフィックが一致しない場合、事前に定義されたデフォルト クラスに誘導されます。
ステップ 11	**exit** 例： `Device(config-pmap-c)# exit`	QoS ポリシー マップ クラス コンフィギュレーション モードを終了し、QoS ポリシー マップ コンフィギュレーション モードを開始します。
ステップ 12	**exit** 例： `Device(config-pmap)# exit`	QoS ポリシー マップ コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードを開始します。
ステップ 13	**zone security** *zone-name* 例： `Device(config)# zone security inside`	インターフェイスを割り当てることができるセキュリティ ゾーンを作成し、セキュリティ ゾーン コンフィギュレーション モードを開始します。 • ゾーン ペアを作成するには2つのセキュリティ ゾーン（送信元ゾーンと宛先ゾーン）が設定に含まれる必要があります。 • ゾーン ペアでは、送信元ゾーンまたは宛先ゾーンとしてデフォルト ゾーンを使用できます。

	コマンドまたはアクション	目的
ステップ 14	**exit** 例： `Device(config-sec-zone)# exit`	セキュリティ ゾーン コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードを開始します。
ステップ 15	**zone-pair security** *zone-pair* **source** *source-zone* **destination** *destination-zone* 例： `Device(config)# zone-pair security in2out source inside destination outside`	セキュリティ ゾーンのペアを作成して、セキュリティ ゾーン コンフィギュレーション モードを開始します。 • ポリシーを適用するには、ゾーン ペアを設定する必要があります。
ステップ 16	**service-policy type inspect** *policy-map-name* 例： `Device(config-sec-zone-pair)# service-policy type inspect in-to-out`	ファイアウォール ポリシー マップを宛先ゾーン ペアに付加します。 • ゾーンのペア間でポリシーが設定されない場合、トラフィックはデフォルトでドロップされます。
ステップ 17	**exit** 例： `Device(config-sec-zone-pair)# exit`	セキュリティ ゾーンペア コンフィギュレーション モードを終了し、グローバルコンフィギュレーション モードを開始します。
ステップ 18	**interface** *type number* 例： `Device(config)# interface gigabitethernet 0/0/1`	インターフェイスを設定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 19	**no ip address** 例： `Device(config-if)# no ip address`	IP アドレスを削除するか、IP 処理をディセーブルにします。
ステップ 20	**ip virtual-reassembly** 例： `Device(config-if)# ip virtual-reassembly`	インターフェイスでの仮想フラグメンテーション再構成（VFR）をイネーブルにします。
ステップ 21	**zone-member security** *zone-name* 例： `Device(config-if)# zone-member security inside`	インターフェイスを指定したセキュリティ ゾーンに割り当てます。 • インターフェイスをセキュリティ ゾーンのメンバーにした場合、そのインターフェイスを通して送受信されるすべてのトラフィックは、デフォルトでドロップされます（ただしデバイス宛のトラフィックとデバイス発のトラフィックを除く）。トラフィックがインターフェイス通過するには、ゾーンをポリシーの適用先のゾー

	コマンドまたはアクション	目的
		ンペアの一部にする必要があります。ポリシーがトラフィックを許可すると、トラフィックはそのインターフェイスを通過できます。
ステップ 22	**negotiation auto** 例： `Device(config-if)# negotiation auto`	ギガビットイーサネットインターフェイスの速度、デュプレックス、および自動フロー制御を自動ネゴシエーション プロトコルで設定できるようにします。
ステップ 23	**ipv6 address** *ipv6-address/prefix-length* 例： `Device(config-if)# ipv6 address 2001:DB8:1::1/96`	IPv6 の一般的なプレフィックスに基づいて IPv6 アドレスを設定し、インターフェイスにおける IPv6 処理をイネーブルにします。
ステップ 24	**cdp enable** 例： `Device(config-if)# cdp enable`	インターフェイスで Cisco Discovery Protocol をイネーブルにします。
ステップ 25	**exit** 例： `Device(config-if)# exit`	インターフェイス コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードに入ります。
ステップ 26	**ipv6 route** *ipv6-prefix/prefix-length interface-type interface-number* 例： `Device(config)# ipv6 route 2001::/96 gigabitethernet 0/0/1`	スタティック IPv6 ルートを確立します。
ステップ 27	**ipv6 neighbor** *ipv6-address interface-type interface-number hardware-address* 例： `Device(config)# ipv6 neighbor 2001:DB8:1::1 gigabitethernet 0/0/1 0000.29f1.4841`	IPv6 ネイバー探索キャッシュのスタティックエントリを設定します。
ステップ 28	**end** 例： `Device(config)# end`	グローバル コンフィギュレーション モードを終了し、特権 EXEC モードを開始します。

FTP66 ALG サポート用の NAT の設定

手順の概要

1. **enable**
2. **configure terminal**

3. **interface** *type number*
4. **ip address** *ip-address mask*
5. **ip nat inside**
6. **zone-member security** *zone-name*
7. **exit**
8. **interface** *type number*
9. **ip address** *ip-address mask*
10. **ip nat outside**
11. **zone-member security** *zone-name*
12. **exit**
13. **ip nat inside source static** *local-ip global-ip*
14. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface** *type number* 例： `Device(config)# interface gigabitethernet 0/1/2`	インターフェイスを設定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	**ip address** *ip-address mask* 例： `Device(config-if)# ip address 10.1.1.1 255.255.255.0`	インターフェイスに対するプライマリ IP アドレスまたはセカンダリ IP アドレスを設定します。
ステップ 5	**ip nat inside** 例： `Device(config-if)# ip nat inside`	インターフェイスが内部ネットワーク（NAT 変換の対象となるネットワーク）に接続されていることを示します。
ステップ 6	**zone-member security** *zone-name* 例： `Device(config-if)# zone-member security inside`	インターフェイスを指定したセキュリティ ゾーンに割り当てます。 • インターフェイスをセキュリティ ゾーンのメンバーにした場合、そのインターフェイスを通して送受信されるすべてのトラフィックは、デフォルトでドロップされます（ただしデバイス宛のトラフィックとデバイス発のトラフィックを除く）。トラフィックがインターフェイス通

	コマンドまたはアクション	目的
		過するには、ゾーンをポリシーの適用先のゾーンペアの一部にする必要があります。ポリシーがトラフィックを許可すると、トラフィックはそのインターフェイスを通過できます。
ステップ 7	**exit** 例： `Device(config-if)# exit`	インターフェイス コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードに入ります。
ステップ 8	**interface** *type number* 例： `Device(config)# interface gigabitethernet 0/1/1`	インターフェイスを設定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 9	**ip address** *ip-address mask* 例： `Device(config-if)# ip address 10.2.1.1 255.255.255.0`	インターフェイスが内部ネットワーク（NAT 変換の対象となるネットワーク）に接続されていることを示します。
ステップ 10	**ip nat outside** 例： `Device(config-if)# ip nat outside`	インターフェイスが外部ネットワークに接続されていることを示します。
ステップ 11	**zone-member security** *zone-name* 例： `Device(config-if)# zone-member security outside`	インターフェイスを指定したセキュリティ ゾーンに割り当てます。 • インターフェイスをセキュリティ ゾーンのメンバーにした場合、そのインターフェイスを通して送受信されるすべてのトラフィックは、デフォルトでドロップされます（ただしデバイス宛のトラフィックとデバイス発のトラフィックを除く）。トラフィックがインターフェイス通過するには、ゾーンをポリシーの適用先のゾーンペアの一部にする必要があります。ポリシーがトラフィックを許可すると、トラフィックはそのインターフェイスを通過できます。
ステップ 12	**exit** 例： `Device(config-if)# exit`	インターフェイス コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードに入ります。
ステップ 13	**ip nat inside source static** *local-ip global-ip* 例： `Device(config)# ip nat inside source static 10.1.1.10 10.1.1.80`	内部送信元アドレスの NAT をイネーブルにします。

	コマンドまたはアクション	目的
ステップ 14	**end** 例： `Device(config)# end`	グローバル コンフィギュレーション モードを終了し、特権 EXEC モードを開始します。

FTP66 ALG サポート用 NAT64 の設定

手順の概要

1. **enable**
2. **configure terminal**
3. **ipv6 unicast-routing**
4. **interface** *type number*
5. **no ip address**
6. **ipv6 virtual-reassembly**
7. **zone-member security** *zone-name*
8. **negotiation auto**
9. **ipv6 address** *ipv6-address*
10. **ipv6 enable**
11. **nat64 enable**
12. **cdp enable**
13. **exit**
14. **interface** *type number*
15. **ip address** *type number*
16. **ip virtual-reassembly**
17. **zone member security** *zone-name*
18. **negotiation auto**
19. **nat64 enable**
20. **exit**
21. **ipv6 route** *ipv6-address interface-type interface-number*
22. **ipv6 neighbor** *ipv6-address interface-type interface-number hardware-address*
23. **nat64 v6v4 static** *ipv6-address ipv4-address*
24. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。

	コマンドまたはアクション	目的
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ipv6 unicast-routing** 例： `Device(config)# ipv6 unicast-routing`	IPv6 ユニキャスト データグラムの転送を有効にします。
ステップ 4	**interface** *type number* 例： `Device(config)# interface gigabitethernet 0/0/0`	インターフェイスを設定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 5	**no ip address** 例： `Device(config-if)# no ip address`	IP アドレスを削除するか、IP 処理をディセーブルにします。
ステップ 6	**ipv6 virtual-reassembly** 例： `Device(config-if)# ipv6 virtual-reassembly`	インターフェイスでの仮想フラグメンテーション再構成（VFR）をイネーブルにします。
ステップ 7	**zone-member security** *zone-name* 例： `Device(config-if)# zone-member security inside`	インターフェイスを指定したセキュリティ ゾーンに割り当てます。 • インターフェイスをセキュリティ ゾーンのメンバーにした場合、そのインターフェイスを通して送受信されるすべてのトラフィックは、デフォルトでドロップされます（ただしデバイス宛のトラフィックとデバイス発のトラフィックを除く）。トラフィックがインターフェイス通過するには、ゾーンをポリシーの適用先のゾーンペアの一部にする必要があります。ポリシーがトラフィックを許可すると、トラフィックはそのインターフェイスを通過できます。
ステップ 8	**negotiation auto** 例： `Device(config-if)# negotiation auto`	ギガビットイーサネットインターフェイスの速度、デュプレックス、および自動フロー制御を自動ネゴシエーション プロトコルで設定できるようにします。
ステップ 9	**ipv6 address** *ipv6-address* 例： `Device(config-if)# ipv6 address 2001:DB8:1::2/96`	IPv6 の一般的なプレフィックスに基づいて IPv6 アドレスを設定し、インターフェイスにおける IPv6 処理をイネーブルにします。

	コマンドまたはアクション	目的
ステップ 10	**ipv6 enable** 例： `Device(config-if)# ipv6 enable`	明示的なIPv6アドレスが設定されていないインターフェイスにおけるIPv6処理をイネーブルにします。
ステップ 11	**nat64 enable** 例： `Device(config-if)# nat64 enable`	インターフェイスで NAT64 をイネーブルにします。
ステップ 12	**cdp enable** 例： `Device(config-if)# cdp enable`	インターフェイスで Cisco Discovery Protocol をイネーブルにします。
ステップ 13	**exit** 例： `Device(config-if)# exit`	インターフェイス コンフィギュレーション モードを終了し、グローバルコンフィギュレーションモードに入ります。
ステップ 14	**interface** *type number* 例： `Device(config)# interface gigabitethernet 0/1/1`	インターフェイスを設定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 15	**ip address** *type number* 例： `Device(config-if)# ip address 209.165.201.25 255.255.255.0`	インターフェイスに対するプライマリ IP アドレスまたはセカンダリ IP アドレスを設定します。
ステップ 16	**ip virtual-reassembly** 例： `Device(config-if)# ip virtual-reassembly`	インターフェイスで VFR をイネーブルにします。
ステップ 17	**zone member security** *zone-name* 例： `Device(config-if)# zone member security outside`	インターフェイスを指定したセキュリティ ゾーンに割り当てます。 • インターフェイスをセキュリティ ゾーンのメンバーにした場合、方向に関係なくインターフェイスを通過するすべてのトラフィック（ルータ宛のトラフィックまたはルータ発信のトラフィックを除く）は、デフォルトでドロップされます。トラフィックがインターフェイス通過するには、ゾーンをポリシーの適用先のゾーン ペアの一部にする必要があります。ポリシーがトラフィックを許可すると、トラフィックはそのインターフェイスを通過できます。

	コマンドまたはアクション	目的
ステップ 18	**negotiation auto** 例： `Device(config-if)# negotiation auto`	ギガビットイーサネットインターフェイスの速度、デュプレックス、および自動フロー制御を自動ネゴシエーション プロトコルで設定できるようにします。
ステップ 19	**nat64 enable** 例： `Device(config-if)# nat64 enable`	インターフェイスで NAT64 をイネーブルにします。
ステップ 20	**exit** 例： `Device(config-if)# exit`	インターフェイス コンフィギュレーション モードを終了し、グローバルコンフィギュレーションモードに入ります。
ステップ 21	**ipv6 route** *ipv6-address interface-type interface-number* 例： `Device(config)# ipv6 route 2001:DB8:1::2/96 gigabitethernet 0/0/0`	スタティック IPv6 ルートを確立し、指定したネットワークへの到達に使用できるネクスト ホップの IPv6 アドレスを指定します。
ステップ 22	**ipv6 neighbor** *ipv6-address interface-type interface-number hardware-address* 例： `Device(config)# ipv6 neighbor 2001:DB8:1::103 gigabitethernet 0/0/0 0000.29f1.4841`	IPv6 ネイバー探索キャッシュのスタティックエントリを設定します。
ステップ 23	**nat64 v6v4 static** *ipv6-address ipv4-address* 例： `Device(config)# nat64 v6v4 static 2001:DB8:1::103 209.165.201.32`	NAT64 の IPv6 送信元アドレスを IPv4 送信元アドレスに、および IPv4 宛先アドレスを IPv6 宛先アドレスに変換します。
ステップ 24	**end** 例： `Device(config)# end`	グローバル コンフィギュレーション モードを終了し、特権 EXEC モードを開始します。

IPv6 ファイアウォールに対する FTP66 ALG サポートの設定例

例：FTP66 ALG サポート用の IPv6 ファイアウォールの設定

```
Device# configure terminal
Device(config)# class-map type inspect match-any in2out-class
Device(config-cmap)# match protocol ftp
```

```
Device(config-cmap)# exit
Device(config)# policy-map type inspect in-to-out
Device(config-pmap)# class type inspect in2out-class
Device(config-pmap-c)# inspect
Device(config-pmap-c)# exit
Device(config-pmap)# class class-default
Device(config-pmap-c)# exit
Device(config-pmap)# exit
Device(config)# zone security inside
Device(config-sec-zone)# exit
Device(config)# zone security outside
Device(config-sec-zone)# exit
Device(config)# zone-pair security in2out source inside destination outside
Device(config-sec-zone-pair)# service-policy type inspect in-to-out
Device(config-sec-zone-pair)# exit
Device(config)# interface gigabitethernet 0/0/1
Device(config-if)# no ip address
Device(config-if)# ip virtual-reassembly
Device(config-if)# zone-member security inside
Device(config-if)# negotiation auto
Device(config-if)# ipv6 address 2001:DB8:1::1/96
Device(config-if)# cdp enable
Device(config-if)# exit
Device(config)# interface gigabitethernet 0/1/1
Device(config-if)# no ip address
Device(config-if)# ip virtual-reassembly
Device(config-if)# zone-member security outside
Device(config-if)# negotiation auto
Device(config-if)# ipv6 address 2001:DB8:2::2/96
Device(config-if)# exit
Device(config)# ipv6 route 2001::/96 gigabitethernet 0/0/1
Device(config)# ipv6 route 2001::/96 gigabitethernet 0/1/1
Device(config)# ipv6 neighbor 2001:DB8:1::1 gigabitethernet 0/0/1 0000.29f1.4841
Device(config)# ipv6 neighbor 2001:DB8:2::2 gigabitethernet 0/1/1 0000.29f1.4842
Device(config)# end
```

例：FTP66 ALG サポート用の NAT の設定

```
Device# configure terminal
Device(config)# interface gigabitethernet 0/1/2
Device(config-if)# ip address 10.1.1.1 255.255.255.0
Device(config-if)# ip nat inside
Device(config-if)# zone-member security inside
Device(config-if)# exit
Device(config)# interface gigabitethernet 0/1/1
Device(config-if)# ip address 10.2.1.1 255.255.255.0
Device(config-if)# ip nat outside
Device(config-if)# zone-member security outside
Device(config-if)# exit
Device(config-if)# ip nat inside source static 10.1.1.10 10.1.1.80
```

例：FTP66 ALG サポート用の NAT64 の設定

```
Device# configure terminal
Device(config)# ipv6 unicast-routing
```

```
Device(config)# interface gigabitethernet 0/0/0
Device(config-if)# no ip address
Device(config-if)# ipv6 virtual-reassembly
Device(config-if)# zone-member security inside
Device(config-if)# negotiation auto
Device(config-if)# ipv6 address 2001:DB8:1::2/96
Device(config-if)# ipv6 enable
Device(config-if)# nat64 enable
Device(config-if)# cdp enable
Device(config-if)# exit
Device(config)# interface gigabitethernet 0/1/1
Device(config-if)# ip address 209.165.201.25 255.255.255.0
Device(config-if)# ip virtual-reassembly
Device(config-if)# zone member security outside
Device(config-if)# negotiation auto
Device(config-if)# nat64 enable
Device(config-if)# exit
Device(config)# ipv6 route 2001:DB8:1::2/96 gigabitethernet 0/0/0
Device(config)# 2001:DB8:1::103 gigabitethernet 0/0/0 0000.29f1.4841
Device(config)# nat64 v6v4 static 2001:DB8:1::103 209.165.201.32
```

IPv6 ファイアウォールに対する FTP66 ALG サポートに関する追加情報

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『Master Command List, All Releases』
セキュリティ コマンド	• 『Security Command Reference: Commands A to C』 • 『Security Command Reference: Commands D to L』 • 『Security Command Reference: Commands M to R』 • 『Security Command Reference: Commands S to Z』
NAT コマンド	『IP Addressing Command Reference』

標準および RFC

標準/RFC	タイトル
RFC 959	『*File Transfer Protocol*』

標準/RFC	タイトル
RFC 2428	『*FTP Extensions for IPv6 and NATs*』

シスコのテクニカル サポート

説明	リンク
右の URL にアクセスして、シスコのテクニカル サポートを最大限に活用してください。これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

IPv6 ファイアウォールに対する FTP66 ALG サポートに関する機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *185 : IPv6* ファイアウォールに対する *FTP66 ALG* サポートに関する機能情報

機能名	リリース	機能情報
IPv6 ファイアウォールに対する FTP66 ALG サポート	Cisco IOS XE リリース 3.7S	IPv6 ファイアウォールの FTP66 ALG サポート機能により、FTP を IPv6 ファイアウォールと連動させることができます。このモジュールでは、FTP66 アプリケーション レベル ゲートウェイ（ALG）と連動するように、ファイアウォール、ネットワーク アドレス変換（NAT）、および NAT64 を設定する方法について説明します。

第 139 章

分散型サービス妨害攻撃に対する保護

分散型サービス妨害攻撃の防止機能は、グローバル レベル（すべてのファイアウォール セッション）およびVPNルーティングおよび転送（VRF）レベルでのサービス妨害（DoS）攻撃からの保護を提供します。Cisco IOS XE リリース 3.4S 以降のリリースでは、分散型 DoS 攻撃を防ぐために、ファイアウォールセッションのアグレッシブエージング、ファイアウォールセッションのイベント レート モニタリング、ハーフオープン接続制限、およびグローバル TCP SYN Cookie 保護を設定できます。

分散型サービス妨害攻撃に対する保護に関する情報

ファイアウォール セッションのアグレッシブ エージング

アグレッシブエージング機能により、ファイアウォールは、セッションを積極的にエージングアウトし、新しいセッションのためのスペースを確保することで、ファイアウォールセッションデータベースがいっぱいになるのを防ぐことができます。ファイアウォールはそのリソースを保護するため、アイドル セッションを削除します。アグレッシブ エージング機能により、ファイアウォールセッションが存在できる時間は、タイマーで定義されている時間（エージングアウト時間）よりも短くなります。

アグレッシブ エージング機能には、アグレッシブ エージング期間の開始と終了を定義するしきい値（高位水準点と低位水準点）があります。アグレッシブエージング期間は、セッションテーブルが高位水準点を超えると開始され、低位水準点を下回ると終了します。アグレッシブエージングの期間中、セッションの存続期間は、エージングアウト時間を使用して設定した期間よりも短くなります。ファイアウォールがセッションを終了する時間よりも短い時間で攻撃者がセッションを開始する場合、セッションを作成するために割り当てられているすべてのリソースが使用され、新しいすべての接続が拒否されます。このような攻撃を防ぐには、セッ

ションを積極的にエージングアウトするようにアグレッシブエージング機能を設定できます。この機能はデフォルトで無効に設定されています。

ボックス レベル（ボックスはファイアウォール セッション テーブル全体を示します）および Virtual Routing and Forwarding（VRF）レベルで、ハーフオープン セッションおよび総セッションにアグレッシブ エージングを設定できます。この機能を総セッションに対して設定している場合、ファイアウォールセッション リソースを使用するすべてのセッションが考慮されます。総セッションは、確立されたセッション、ハーフオープンセッション、および不明確セッション データベース内のセッションで構成されます。（確立状態に達していない TCP セッションはハーフオープン セッションと呼ばれます）。

ファイアウォールには 2 つのセッション データベースがあります。1 つはセッション データベースで、もう 1 つは不正確なセッションデータベースです。セッションデータベースには、5 タプル（送信元 IP アドレス、宛先 IP アドレス、送信元ポート、宛先ポート、およびプロトコル）が設定されているセッションが含まれます。タプルは、要素の番号付きリストです。不正確なセッション データベースには、5 つ未満のタプル（欠落した IP アドレス、ポート番号など）のセッションが含まれます。ハーフオープン セッションのアグレッシブ エージングでは、ハーフオープン セッションだけが考慮されます。

Internet Control Message Protocol（ICMP）、TCP、および UDP ファイアウォール セッションにはアグレッシブ エージングアウト時間を設定できます。エージングアウト時間は、デフォルトではアイドル時間に設定されます。

イベント レート モニタリング機能

イベント レート モニタリング機能は、ゾーンの事前定義イベントのレートをモニタします。イベント レート モニタリング機能には基本脅威検出機能が含まれています。これはセキュリティデバイスの機能であり、ファイアウォールの内側にあるリソースで発生する可能性のある脅威、異常、および攻撃を検出し、それらに対するアクションを実行します。イベントの基本脅威検出レートを設定できます。特定タイプのイベントの着信レートが、設定されている脅威検出レートを超えると、イベント レート モニタリング機能はこのイベントを脅威と見なし、脅威を阻止するためのアクションを実行します。脅威検出機能は、入力ゾーンでのみイベントを検査します（イベント レート モニタリング機能が入力ゾーンで有効な場合）。

ネットワーク管理者に対し、発生する可能性のある脅威に関する情報がアラート メッセージ（syslog または高速ロガー（HSL））で通知されます。ネットワーク管理者は攻撃ベクトルの検出、攻撃元ゾーンの検出、または特定の動作やトラフィックをブロックするようにネットワーク上のデバイスを設定するなどのアクションを実行できます。

イベント レート モニタリング機能は、次のタイプのイベントをモニタします。

- 基本ファイアウォールチェックが失敗したためにファイアウォールがドロップする：これには、ゾーンまたはゾーンペアのチェック失敗、ドロップアクションを使用して設定されたファイアウォール ポリシーなどがあります。
- レイヤ 4 インスペクションの失敗が原因でファイアウォールがドロップする：これには、1 番目の TCP パケットが同期（SYN）パケットではないために失敗した TCP インスペクションが含まれることがあります。

- TCP SYN Cookie 攻撃：これには、ドロップされた SYN パケットの数と、スプーフィング攻撃として送信された SYN Cookie の数の集計が含まれることがあります。

イベント レート モニタリング機能は、さまざまなイベントの平均レートとバースト レートをモニタします。各イベント タイプにはレート オブジェクトがあります。レート オブジェクトは、設定可能なパラメータ（平均しきい値、バーストしきい値、期間）が含まれる関連レートにより制御されます。期間はタイム スロットに分割されます。各タイム スロットは期間の 1/30 です。

平均レートは、イベント タイプごとに計算されます。各レート オブジェクトは、30 個の完了済みサンプリング値と、現在進行中のサンプリング期間を保持するための 1 つの値を保持します。計算済みの最も古い値が現在のサンプリング値で置き換えられ、平均が再計算されます。平均レートは各期間で計算されます。平均レートが平均しきい値を超えると、イベント レート モニタリング機能はこれを潜在的な脅威と解釈し、統計情報を更新し、ネットワーク管理者に通知します。

バースト レートは、トークン バケット アルゴリズムを使用して実装されます。各タイムスロットで、トークン バケットがトークンで埋められます。発生する（特定のイベント タイプの）イベントごとに、バケットからトークンが削除されます。空のバケットは、バーストしきい値に到達したことを意味し、管理者が syslog または HSL からアラームを受信します。 **show policy-firewall stats zone** コマンドの出力から、脅威検出統計情報を確認し、ゾーン内でさまざまなイベントに対する潜在的な脅威を理解することができます。

最初に **threat-detection basic-threat** コマンドを使用して、基本脅威検出機能を有効にする必要があります。基本脅威検出機能を設定したら、脅威検出レートを設定できます。脅威検出レートを設定するには、**threat-detection rate** コマンドを使用します。

次の表では、イベント レート モニタリング機能が有効な場合に適用可能な基本脅威検出のデフォルト設定について説明します。

表 *186 :* 基本的な脅威の検出のデフォルト設定

パケット ドロップの理由	脅威検出の設定
基本的なファイアウォール ドロップ	平均レート 400 パケット/秒（pps） バースト レート 1600 pps レート間隔 600 秒
インスペクション ベースのファイアウォール ドロップ	平均レート 400 pps バースト レート 1600 pps レート間隔 600 秒
SYN 攻撃ファイアウォール ドロップ	平均レート 100 pps バースト レート 200 pps レート間隔 600 秒

ハーフオープン接続の制限

ファイアウォール セッション テーブルでは、ファイアウォールのハーフオープン接続数を制限できるようになっています。ハーフオープンセッション数を制限することで、ハーフオープン セッションでボックスごとのレベルや Virtual Routing and Forwarding（VRF）レベルでファイアウォール セッション テーブルをいっぱいにしてセッションを確立できないようにする攻撃に対し、ファイアウォールを防御できます。ハーフオープン接続の制限は、レイヤ4プロトコル、Internet Control Message Protocol（ICMP）、TCP、UDP に対して設定できます。UDP ハーフオープンセッション数に対して設定された制限は、TCP や ICMP のハーフオープンセッションには影響しません。設定されたハーフオープンセッションの制限を超えると、すべての新規セッションが拒否され、ログ メッセージが Syslog または高速ロガー（HSL）に生成されます。

次のセッションはハーフオープン セッションと見なされます。

- 3 ウェイ ハンドシェイクを完了していない TCP セッション。
- UDP フローで 1 つのパケットだけが検出された UDP セッション。
- ICMP エコー要求または ICMP タイムスタンプ要求に対する応答を受信していない ICMP セッション。

TCP SYN フラッド攻撃

グローバルの TCP SYN フラッド制限を設定して、SYN フラッド攻撃を制限できます。TCP SYN フラッド攻撃は、サービス妨害（DoS）攻撃の一種です。設定済みの TCP SYN フラッド制限に達すると、ファイアウォールは、さらにセッションを作成する前に、セッションの送信元を確認します。通常は、TCP SYN パケットはファイアウォールの背後のターゲット エンドホストまたはサブネット アドレスの範囲に送信されます。これらの TCP SYN パケットによって、送信元 IP アドレスがスプーフィングされます。スプーフィング攻撃では、個人やプログラムが偽のデータを使用してネットワーク内のリソースにアクセスしようとします。TCP SYN フラッディングは、ファイアウォールまたはエンドホスト上のすべてのリソースを乗っ取る可能性があるため、サービス妨害がトラフィックを正当化することになります。TCP SYN フラッド保護は、VRF レベルとゾーン レベルで設定できます。

SYN フラッド攻撃は、次の 2 つのタイプに分類されます。

- ホスト フラッド：SYN フラッド パケットが単一のホストに送信され、そのホスト上のすべてのリソースを使用することが意図されます。
- ファイアウォールセッションテーブルフラッド：SYN フラッドパケットがファイアウォールの背後のアドレスの範囲に送信され、ファイアウォール上のセッションテーブルリソースを枯渇させ、その結果、リソースの拒否がファイアウォールを通過するトラフィックを正当化することが意図されます。

分散型サービス妨害攻撃に対する防御の設定方法

ファイアウォールの設定

このタスクの内容は以下のとおりです。

- ファイアウォールを設定します。
- セキュリティ送信元ゾーンを作成します。
- セキュリティ宛先ゾーンを作成します。
- 設定された送信元ゾーンと宛先ゾーンを使用してセキュリティ ゾーン ペアを作成します。
- インターフェイスをゾーン メンバーとして設定します。

手順の概要

1. **enable**
2. **configure terminal**
3. **class-map type inspect match-any** *class-map-name*
4. **match protocol** {**icmp** | **tcp** | **udp**}
5. **exit**
6. **parameter-map type inspect global**
7. **redundancy**
8. **exit**
9. **policy-map type inspect** *policy-map-name*
10. **class type inspect** *class-map-name*
11. **inspect**
12. **exit**
13. **class class-default**
14. **drop**
15. **exit**
16. **exit**
17. **zone security** *security-zone-name*
18. **exit**
19. **zone security** *security-zone-name*
20. **exit**
21. **zone-pair security** *zone-pair-name* **source** *source-zone* **destination** *destination-zone*
22. **service-policy type inspect** *policy-map-name*
23. **exit**
24. **interface** *type number*
25. **ip address** *ip-address mask*
26. **encapsulation dot1q** *vlan-id*
27. **zone-member security** *security-zone-name*

28. **end**
29. ゾーンを別のインターフェイスにアタッチするには、ステップ21～25を繰り返します。

手順の詳細

	コマンドまたはアクション	目的
ステップ1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ3	**class-map type inspect match-any** *class-map-name* 例： `Device(config)# class-map type inspect match-any ddos-class`	アプリケーション固有の検査タイプ クラス マップを作成し、QoS クラス マップ コンフィギュレーション モードを開始します。
ステップ4	**match protocol** {**icmp** | **tcp** | **udp**} 例： `Device(config-cmap)# match protocol tcp`	指定したプロトコルに基づいて、クラス マップの一致基準を設定します。
ステップ5	**exit** 例： `Device(config-cmap)# exit`	QoS クラス マップ コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードを開始します。
ステップ6	**parameter-map type inspect global** 例： `Device(config)# parameter-map type inspect global`	グローバル検査パラメータ マップを定義し、パラメータ マップ タイプ検査コンフィギュレーション モードを開始します。
ステップ7	**redundancy** 例： `Device(config-profile)# redundancy`	ファイアウォールの高可用性を有効にします。
ステップ8	**exit** 例： `Device(config-profile)# exit`	パラメータマップタイプ検査コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードを開始します。
ステップ9	**policy-map type inspect** *policy-map-name* 例： `Device(config)# policy-map type inspect ddos-fw`	プロトコル固有の検査タイプ ポリシー マップを作成し、QoS ポリシーマップ コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 10	**class type inspect** *class-map-name* 例： `Device(config-pmap)# class type inspect ddos-class`	アクションの実行対象となるトラフィック クラスを指定し、QoS ポリシー マップ クラス コンフィギュレーション モードを開始します。
ステップ 11	**inspect** 例： `Device(config-pmap-c)# inspect`	ステートフル パケット インスペクションをイネーブルにします。
ステップ 12	**exit** 例： `Device(config-pmap-c)# exit`	QoS ポリシー マップ クラス コンフィギュレーション モードを終了し、QoS ポリシー マップ コンフィギュレーション モードを開始します。
ステップ 13	**class class-default** 例： `Device(config-pmap)# class class-default`	アクションの実行対象となるデフォルト クラスを設定し、QoS ポリシー マップ クラス コンフィギュレーション モードを開始します。
ステップ 14	**drop** 例： `Device(config-pmap-c)# drop`	同じゾーンの 2 つのインターフェイス間でトラフィックの受け渡しが可能になりす。
ステップ 15	**exit** 例： `Device(config-pmap-c)# exit`	QoS ポリシー マップ クラス コンフィギュレーション モードを終了し、QoS ポリシー マップ コンフィギュレーション モードを開始します。
ステップ 16	**exit** 例： `Device(config-pmap)# exit`	QoS ポリシー マップ コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードを開始します。
ステップ 17	**zone security** *security-zone-name* 例： `Device(config)# zone security private`	セキュリティ ゾーンを作成し、セキュリティ ゾーン コンフィギュレーション モードを開始します。 • （送信元ゾーンと宛先ゾーンからなる）ゾーン ペアを作成するには、2つのセキュリティ ゾーンが必要です。
ステップ 18	**exit** 例： `Device(config-sec-zone)# exit`	セキュリティ ゾーン コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 19	**zone security** *security-zone-name* 例： `Device(config)# zone security public`	セキュリティ ゾーンを作成し、セキュリティ ゾーン コンフィギュレーション モードを開始します。 • （送信元ゾーンと宛先ゾーンからなる）ゾーン ペアを作成するには、2つのセキュリティ ゾーンが必要です。
ステップ 20	**exit** 例： `Device(config-sec-zone)# exit`	セキュリティ ゾーン コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードを開始します。
ステップ 21	**zone-pair security** *zone-pair-name* **source** *source-zone* **destination** *destination-zone* 例： `Device(config)# zone-pair security private2public source private destination public`	ゾーン ペアを作成し、セキュリティ ゾーンペア コンフィギュレーション モードを開始します。
ステップ 22	**service-policy type inspect** *policy-map-name* 例： `Device(config-sec-zone-pair)# service-policy type inspect ddos-fw`	ポリシー マップをトップレベル ポリシーに関連付けます。
ステップ 23	**exit** 例： `Device(config-sec-zone-pair)# exit`	セキュリティ ゾーンペア コンフィギュレーション モードを終了し、グローバルコンフィギュレーション モードを開始します。
ステップ 24	**interface** *type number* 例： `Device(config)# interface gigabitethernet 0/1/0.1`	サブインターフェイスを設定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 25	**ip address** *ip-address mask* 例： `Device(config-subif)# ip address 10.1.1.1 255.255.255.0`	サブインターフェイスにIPアドレスを設定します。
ステップ 26	**encapsulation dot1q** *vlan-id* 例： `Device(config-subif)# encapsulation dot1q 2`	インターフェイスで使用するカプセル化方式を設定します。
ステップ 27	**zone-member security** *security-zone-name* 例： `Device(config-subif)# zone-member security private`	インターフェイスをゾーン メンバーとして設定します。 • *security-zone-name* 引数の場合、**zone security** コマンドを使用して設定済みのゾーンの1つを設定する必要があります。

	コマンドまたはアクション	目的
		• インターフェイスがセキュリティ ゾーンにある場合、そのインターフェイスを通るトラフィックはどちらの方向でもすべて（デバイス宛またはデバイス発のトラフィックを除く）はデフォルトでドロップされます。ゾーン メンバーであるインターフェイスをトラフィックが通過できるようにするには、ポリシー適用対象のゾーン ペアにそのゾーンを含める必要があります。ポリシーの **inspect** または **pass** アクションによってトラフィックが許可される場合は、そのインターフェイスを通じてトラフィックが流れます。
ステップ 28	**end** 例： `Device(config-subif)# end`	サブインターフェイス コンフィギュレーション モードを終了して、特権 EXEC モードを開始します。
ステップ 29	ゾーンを別のインターフェイスにアタッチするには、ステップ 21 ～ 25 を繰り返します。	—

ファイアウォール セッションのアグレッシブ エージングの設定

アグレッシブ エージング機能は、ボックス単位（ボックス単位とは、ファイアウォール セッション テーブル全体を意味します）、デフォルト VRF、および VRF 単位のファイアウォール セッションに設定できます。アグレッシブ エージング機能が動作するには、ファイアウォール セッションのアグレッシブ エージングおよびエージング アウト時間を設定する必要があります。

ファイアウォール セッションのアグレッシブ エージングを設定するには、次の作業を実行します。

ボックス単位のアグレッシブ エージングの設定

ボックス単位とは、ファイアウォールセッションテーブル全体という意味です。**parameter-map type inspect-global** コマンドに続くすべての設定がボックスに適用されます。

手順の概要

1. **enable**
2. **configure terminal**
3. 次のいずれかのコマンドを入力します。
   - **parameter-map type inspect-global**
   - **parameter-map type inspect global**

4. **per-box max-incomplete** *number* **aggressive-aging high** {*value* **low** *value* | **percent** *percent* **low percent** *percent*}
5. **per-box aggressive-aging high** {*value* **low** *value* | **percent** *percent* **low percent** *percent*}
6. **exit**
7. **parameter-map type inspect** *parameter-map-name*
8. **tcp synwait-time** *seconds* [**ageout-time** *seconds*]
9. **end**
10. **show policy-firewall stats global**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。

ステップ 3	次のいずれかのコマンドを入力します。
	• **parameter-map type inspect-global**
	• **parameter-map type inspect global**
	例：
	`Device(config)# parameter-map type inspect-global`
	`Device(config)# parameter-map type inspect global`
		接続しきい値およびタイムアウトのグローバル パラメータ マップを設定し、パラメータ マップ タイプ検査コンフィギュレーション モードを開始します。
		• リリースに基づいて、**parameter-map type inspect-global** コマンドと **parameter-map type inspect global** コマンドがサポートされます。これら両方のコマンドを一緒に設定することはできません。
		• **parameter-map type inspect-global** コマンドを設定する場合は、手順4と手順5をスキップしてください。
		（注） **parameter-map type inspect-global** コマンドを設定する場合は、**per-box** コンフィギュレーションがサポートされません。これは、デフォルトですべての **per-box** コンフィギュレーションがすべてのファイアウォールセッションに適用されるためです。

	コマンドまたはアクション	目的
ステップ 4	**per-box max-incomplete** *number* **aggressive-aging high** {*value* **low** *value* | **percent** *percent* **low percent** *percent*} 例： `Device(config-profile)# per-box max-incomplete 2000 aggressive-aging high 1500 low 1200`	ファイアウォール セッション テーブル内のハーフオープンセッションの上限およびアグレッシブエージング レートを設定します。
ステップ 5	**per-box aggressive-aging high** {*value* **low** *value* | **percent** *percent* **low percent** *percent*} 例： `Device(config-profile)# per-box aggressive-aging high 1700 low 1300`	総セッションのアグレッシブ エージング制限を設定します。
ステップ 6	**exit** 例： `Device(config-profile)# exit`	パラメータマップ タイプ検査コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードを開始します。
ステップ 7	**parameter-map type inspect** *parameter-map-name* 例： `Device(config)# parameter-map type inspect pmap1`	接続しきい値、タイムアウト、およびその他の **inspect** アクションに関連するパラメータの検査タイプパラメータマップを設定し、パラメータマップ タイプ検査コンフィギュレーション モードを開始します。
ステップ 8	**tcp synwait-time** *seconds* [**ageout-time** *seconds*] 例： `Device(config-profile)# tcp synwait-time 30 ageout-time 10`	セッションをドロップする前に、TCP セッションが確立状態になるのを待機する時間を指定します。 • アグレッシブ エージングがイネーブルになった後、最も古い TCP 接続の SYN 待機タイマーが、デフォルトから設定済みエージアウト時間にリセットされます。この例では、接続がタイムアウトするまで 30 秒待機する代わりに、最も古い TCP 接続のタイムアウトが 10 秒に設定されます。接続が低ウォーターマークを下回ると、アグレッシブ エージングはディセーブルになります。
ステップ 9	**end** 例： `Device(config-profile)# end`	パラメータマップ タイプ検査コンフィギュレーション モードを終了し、特権 EXEC モードを開始します。
ステップ 10	**show policy-firewall stats global** 例： `Device# show policy-firewall stats global`	グローバル ファイアウォール統計情報を表示します。

デフォルト VRF のアグレッシブ エージングの設定

max-incomplete aggressive-aging command, it applies to the default VRF. を設定する場合

手順の概要

1. **enable**
2. **configure terminal**
3. 次のいずれかのコマンドを入力します：
   - **parameter-map type inspect-global**
   - **parameter-map type inspect global**
4. **max-incomplete** *number* **aggressive-aging high** {*value* **low** *value* | **percent** *percent* **low percent** *percent*}
5. **session total** *number* [**aggressive-aging high** {*value* **low** *value* | **percent** *percent* **low percent** *percent*}]
6. **exit**
7. **parameter-map type inspect** *parameter-map-name*
8. **tcp synwait-time** *seconds* [**ageout-time** *seconds*]
9. **end**
10. **show policy-firewall stats vrf global**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。

ステップ 3	次のいずれかのコマンドを入力します：
	• **parameter-map type inspect-global**
	• **parameter-map type inspect global**
	例：
	`Device(config)# parameter-map type inspect-global`
	`Device(config)# parameter-map type inspect global`
		接続しきい値およびタイムアウトのグローバル パラメータ マップを設定し、パラメータ マップ タイプ検査コンフィギュレーション モードを開始します。
		• リリースに基づいて、**parameter-map type inspect-global** コマンドと **parameter-map type inspect global** コマンドがサポートされます。これら両方のコマンドを一緒に設定することはできません。

	コマンドまたはアクション	目的
		• **parameter-map type inspect-global** コマンドを設定する場合は、手順5をスキップしてください。 （注） **parameter-map type inspect-global** コマンドを設定する場合は **per-box** コンフィギュレーションがサポートされません。これは、デフォルトですべての **per-box** コンフィギュレーションがすべてのファイアウォールセッションに適用されるためです。
ステップ 4	**max-incomplete** *number* **aggressive-aging high** {*value* **low** *value* | **percent** *percent* **low percent** *percent*} 例： `Device(config-profile)# max-incomplete 3455 aggressive-aging high 2345 low 2255`	ハーフオープン ファイアウォール セッションの上限およびアグレッシブ エージング制限を設定します。
ステップ 5	**session total** *number* [**aggressive-aging high** {*value* **low** *value* | **percent** *percent* **low percent** *percent*}] 例： `Device(config-profile)# session total 1000 aggressive-aging high percent 80 low percent 60`	総ファイアウォール セッションの合計制限およびアグレッシブ エージング制限を設定します。
ステップ 6	**exit** 例： `Device(config-profile)# exit`	パラメータマップ タイプ検査コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードを開始します。
ステップ 7	**parameter-map type inspect** *parameter-map-name* 例： `Device(config)# parameter-map type inspect pmap1`	接続しきい値、タイムアウト、およびその他の **inspect** アクションに関連するパラメータの検査タイプパラメータマップを設定し、パラメータマップ タイプ検査コンフィギュレーション モードを開始します。
ステップ 8	**tcp synwait-time** *seconds* [**ageout-time** *seconds*] 例： `Device(config-profile)# tcp synwait-time 30 ageout-time 10`	セッションをドロップする前に、TCP セッションが確立状態になるのを待機する時間を指定します。 • アグレッシブ エージングがイネーブルになった後、最も古い TCP 接続の SYN 待機タイマーが、デフォルトから設定済みエージアウト時間にリセットされます。この例では、接続がタイムアウトするまで 30 秒待機する代わりに、最も古い TCP 接続のタイムアウトが 10 秒に設定されます。接続が低ウォーターマークを下回る

	コマンドまたはアクション	目的
		と、アグレッシブ エージングはディセーブルになります。
ステップ 9	**end** 例： `Device(config-profile)# end`	パラメータマップタイプ検査コンフィギュレーション モードを終了し、特権 EXEC モードを開始します。
ステップ 10	**show policy-firewall stats vrf global** 例： `Device# show policy-firewall stats vrf global`	グローバル VRF ファイアウォール ポリシー統計を表示します。

ファイアウォール セッションのエージング アウトの設定

ICMP、TCP、またはUDPファイアウォールセッションのエージングアウトを設定できます。

手順の概要

1. **enable**
2. **configure terminal**
3. 次のいずれかのコマンドを入力します。
   - **parameter-map type inspect-global**
   - **parameter-map type inspect global**
4. **vrf** *vrf-name* **inspect** *vrf-pmap-name*
5. **exit**
6. **parameter-map type inspect** *parameter-map-name*
7. **tcp idle-time** *seconds* [**ageout-time** *seconds*]
8. **tcp synwait-time** *seconds* [**ageout-time** *seconds*]
9. **exit**
10. **policy-map type inspect** *policy-map-name*
11. **class type inspect match-any** *class-map-name*
12. **inspect** *parameter-map-name*
13. **end**
14. **show policy-firewall stats vrf** *vrf-pmap-name*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。

	コマンドまたはアクション	目的
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。

ステップ 3	次のいずれかのコマンドを入力します。
	• **parameter-map type inspect-global**
	• **parameter-map type inspect global**
	例：
	`Device(config)# parameter-map type inspect-global`
	`Device(config)# parameter-map type inspectglobal`
		グローバル パラメータ マップを設定し、パラメータ マップ タイプ検査コンフィギュレーション モードを開始します。
		• リリースに基づいて、**parameter-map type inspect-global** コマンドと **parameter-map type inspect global** コマンドがサポートされます。これら両方のコマンドを一緒に設定することはできません。
		• **parameter-map type inspect-global** コマンドを設定する場合は、手順4をスキップしてください。
		（注） **parameter-map type inspect-global** コマンドを設定する場合は、**per-box** コンフィギュレーションがサポートされません。これは、デフォルトですべての **per-box** コンフィギュレーションがすべてのファイアウォールセッションに適用されるためです。

ステップ 4	**vrf** *vrf-name* **inspect** *vrf-pmap-name* 例： `Device(config-profile)# vrf vrf1 inspect vrf1-pmap`	パラメータ マップに VRF をバインドします。
ステップ 5	**exit** 例： `Device(config-profile)# exit`	パラメータマップ タイプ検査コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードを開始します。
ステップ 6	**parameter-map type inspect** *parameter-map-name* 例： `Device(config)# parameter-map type inspect pmap1`	接続しきい値、タイムアウト、およびその他の **inspect** アクションに関連するパラメータの検査タイプパラメータマップを設定し、パラメータマップ タイプ検査コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 7	**tcp idle-time** *seconds* [**ageout-time** *seconds*] 例： `Device(config-profile)# tcp idle-time 3000 ageout-time 100`	アイドル状態の TCP セッションのタイムアウト、および TCP セッションのアグレッシブ エージング アウト時間を設定します。 • また、**tcp finwait-time** コマンドを設定すると、終了（FIN）交換がファイアウォールで検出された後に TCP セッションを管理する時間の長さを指定できます。または **tcp synwait-time** コマンドを設定すると、セッションをドロップする前に TCP セッションが確立状態になるのを待機する時間を指定できます。
ステップ 8	**tcp synwait-time** *seconds* [**ageout-time** *seconds*] 例： `Device(config-profile)# tcp synwait-time 30 ageout-time 10`	セッションをドロップする前に、TCP セッションが確立状態になるのを待機する時間を指定します。 • アグレッシブ エージングがイネーブルになると、最も古い TCP 接続の SYN 待機タイマーが、デフォルトから設定済みエージアウト時間にリセットされます。この例では、接続がタイムアウトするまで 30 秒待機する代わりに、最も古い TCP 接続のタイムアウトが 10 秒に設定されます。接続が低ウォーターマークを下回ると、アグレッシブ エージングがイネーブルになります。
ステップ 9	**exit** 例： `Device(config-profile)# exit`	パラメータ マップ タイプ検査コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードを開始します。
ステップ 10	**policy-map type inspect** *policy-map-name* 例： `Device(config)# policy-map type inspect ddos-fw`	プロトコル固有の検査タイプ ポリシー マップを作成し、QoS ポリシーマップ コンフィギュレーション モードを開始します。
ステップ 11	**class type inspect match-any** *class-map-name* 例： `Device(config-pmap)# class type inspect match-any ddos-class`	アクションの実行対象となるトラフィック クラスを指定し、QoS ポリシー マップ クラス コンフィギュレーション モードを開始します。
ステップ 12	**inspect** *parameter-map-name* 例： `Device(config-pmap-c)# inspect pmap1`	パラメータ マップのステートフル パケット インスペクションをディセーブルにします。

	コマンドまたはアクション	目的
ステップ 13	**end** 例： `Device(config-pmap-c)# end`	QoS ポリシーマップ クラス コンフィギュレーション モードを終了し、特権 EXEC モードを開始します。
ステップ 14	**show policy-firewall stats vrf** *vrf-pmap-name* 例： `Device# show policy-firewall stats vrf vrf1-pmap`	VRF レベル ポリシー ファイアウォール統計情報を表示します。

例

次に、**show policy-firewall stats vrf vrf1-pmap** コマンドの出力例を示します。

```
Device# show policy-firewall stats vrf vrf1-pmap

 VRF: vrf1, Parameter-Map: vrf1-pmap
  Interface reference count: 2
       Total Session Count(estab + half-open): 270, Exceed: 0
       Total Session Aggressive Aging Period Off, Event Count: 0

                Half Open
       Protocol Session Cnt     Exceed
       -------- -----------     ------
       All      0               0
       UDP      0               0
       ICMP     0               0
       TCP      0               0

       TCP Syn Flood Half Open Count: 0, Exceed: 12
       Half Open Aggressive Aging Period Off, Event Count: 0
```

VRF 単位のアグレッシブ エージングの設定

手順の概要

1. **enable**
2. **configure terminal**
3. **ip vrf** *vrf-name*
4. **rd** *route-distinguisher*
5. **route-target export** *route-target-ext-community*
6. **route-target import** *route-target-ext-community*
7. **exit**
8. **parameter-map type inspect-vrf** *vrf-pmap-name*
9. **max-incomplete** *number* **aggressive-aging high** {*value* **low** *value* | **percent** *percent* **low percent** *percent*}
10. **session total** *number* [**aggressive-aging** {**high** *value* **low** *value* | **percent** *percent* **low percent** *percent*}]
11. **alert on**
12. **exit**

13. 次のいずれかのコマンドを入力します。
    - **parameter-map type inspect-global**
    - **parameter-map type inspect global**
14. **vrf** *vrf-name* **inspect** *vrf-pmap-name*
15. **exit**
16. **parameter-map type inspect** *parameter-map-name*
17. **tcp idle-time** *seconds* [**ageout-time** *seconds*]
18. **tcp synwait-time** *seconds* [**ageout-time** *seconds*]
19. **exit**
20. **policy-map type inspect** *policy-map-name*
21. **class type inspect match-any** *class-map-name*
22. **inspect** *parameter-map-name*
23. **end**
24. **show policy-firewall stats vrf** *vrf-pmap-name*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ip vrf** *vrf-name* 例： `Device(config)# ip vrf ddos-vrf1`	VRF インスタンスを定義し、VRF コンフィギュレーション モードを開始します。
ステップ 4	**rd** *route-distinguisher* 例： `Device(config-vrf)# rd 100:2`	VRF インスタンスのルート識別子（RD）を指定します。
ステップ 5	**route-target export** *route-target-ext-community* 例： `Device(config-vrf)# route-target export 100:2`	ルートターゲット拡張コミュニティを作成し、ルーティング情報をターゲット VPN 拡張コミュニティにエクスポートします。
ステップ 6	**route-target import** *route-target-ext-community* 例： `Device(config-vrf)# route-target import 100:2`	ルートターゲット拡張コミュニティを作成し、ターゲット VPN 拡張コミュニティからルーティング情報をインポートします。

	コマンドまたはアクション	目的
ステップ 7	**exit** 例： `Device(config-vrf)# exit`	VRF コンフィギュレーション モードを終了して、グローバル コンフィギュレーション モードを開始します。
ステップ 8	**parameter-map type inspect-vrf** *vrf-pmap-name* 例： `Device(config)# parameter-map type inspect-vrf vrf1-pmap`	VRF 検査タイプ パラメータ マップを設定し、パラメータ マップ タイプ検査コンフィギュレーション モードを開始します。
ステップ 9	**max-incomplete** *number* **aggressive-aging high** {*value* **low** *value* | **percent** *percent* **low percent** *percent*} 例： `Device(config-profile)# max-incomplete 2000 aggressive-aging high 1500 low 1200`	ハーフ オープン セッションの上限およびアグレッシブ エージング制限を設定します。
ステップ 10	**session total** *number* [**aggressive-aging** {**high** *value* **low** *value* | **percent** *percent* **low percent** *percent*}] 例： `Device(config-profile)# session total 1000 aggressive-aging high percent 80 low percent 60`	総セッション制限および総セッションに関するアグレッシブ エージング制限を設定します。 • 総セッション制限は、絶対値またはパーセンテージとして設定できます。
ステップ 11	**alert on** 例： `Device(config-profile)# alert on`	ステートフル パケット インスペクションのアラート メッセージのコンソール表示をイネーブルにします。
ステップ 12	**exit** 例： `Device(config-profile)# exit`	パラメータ マップ タイプ検査コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードを開始します。

ステップ 13	次のいずれかのコマンドを入力します。
	• **parameter-map type inspect-global**
	• **parameter-map type inspect global**
	例：
	`Device(config)# parameter-map type inspect-global`
	`Device(config)# parameter-map type inspect global`
		グローバル パラメータ マップを設定し、パラメータ マップ タイプ検査コンフィギュレーション モードを開始します。
		• リリースに基づいて、**parameter-map type inspect-global** コマンドと **parameter-map type inspect global** コマンドがサポートされます。これら両方のコマンドを一緒に設定することはできません。
		• **parameter-map type inspect-global** コマンドを設定する場合は、手順 14 をスキップしてください。

	コマンドまたはアクション	目的
		（注） **parameter-map type inspect-global** コマンドを設定する場合は、**per-box** コンフィギュレーションがサポートされません。これは、デフォルトですべての **per-box** コンフィギュレーションがすべてのファイアウォールセッションに適用されるためです。
ステップ 14	**vrf** *vrf-name* **inspect** *vrf-pmap-name* 例： `Device(config-profile)# vrf vrf1 inspect vrf1-pmap`	パラメータ マップに VRF をバインドします。
ステップ 15	**exit** 例： `Device(config-profile)# exit`	パラメータマップタイプ検査コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードを開始します。
ステップ 16	**parameter-map type inspect** *parameter-map-name* 例： `Device(config)# parameter-map type inspect pmap1`	接続しきい値、タイムアウト、およびその他の **inspect** アクションに関連するパラメータの検査タイプパラメータマップを設定し、パラメータマップタイプ検査コンフィギュレーション モードを開始します。
ステップ 17	**tcp idle-time** *seconds* [**ageout-time** *seconds*] 例： `Device(config-profile)# tcp idle-time 3000 ageout-time 100`	アイドル状態の TCP セッションのタイムアウト、および TCP セッションのアグレッシブ エージングアウト時間を設定します。
ステップ 18	**tcp synwait-time** *seconds* [**ageout-time** *seconds*] 例： `Device(config-profile)# tcp synwait-time 30 ageout-time 10`	セッションをドロップする前に、TCP セッションが確立状態になるのを待機する時間を指定します。 • アグレッシブ エージングがイネーブルになると、最も古い TCP 接続の SYN 待機タイマーが、デフォルトから設定済みエージアウト時間にリセットされます。この例では、接続がタイムアウトするまで 30 秒待機する代わりに、最も古い TCP 接続のタイムアウトが 10 秒に設定されます。接続が低ウォーターマークを下回ると、アグレッシブ エージングはディセーブルになります。
ステップ 19	**exit** 例： `Device(config-profile)# exit`	パラメータマップタイプ検査コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 20	**policy-map type inspect** *policy-map-name* 例： `Device(config)# policy-map type inspect ddos-fw`	プロトコル固有の検査タイプ ポリシー マップを作成し、QoS ポリシーマップ コンフィギュレーション モードを開始します。
ステップ 21	**class type inspect match-any** *class-map-name* 例： `Device(config-pmap)# class type inspect match-any ddos-class`	アクションの実行対象となるトラフィック（クラス）を指定し、QoS ポリシー マップ クラス コンフィギュレーション モードを開始します。
ステップ 22	**inspect** *parameter-map-name* 例： `Device(config-pmap-c)# inspect pmap1`	パラメータ マップのステートフル パケット インスペクションをディセーブルにします。
ステップ 23	**end** 例： `Device(config-pmap-c)# end`	QoS ポリシーマップ クラス コンフィギュレーション モードを終了し、特権 EXEC モードを開始します。
ステップ 24	**show policy-firewall stats vrf** *vrf-pmap-name* 例： `Device# show policy-firewall stats vrf vrf1-pmap`	VRF レベル ポリシー ファイアウォール統計情報を表示します。

例

次に、**show policy-firewall stats vrf vrf1-pmap** コマンドの出力例を示します。

```
Device# show policy-firewall stats vrf vrf1-pmap

VRF: vrf1, Parameter-Map: vrf1-pmap
  Interface reference count: 2
       Total Session Count(estab + half-open): 80, Exceed: 0
       Total Session Aggressive Aging Period Off, Event Count: 0

                Half Open
       Protocol Session Cnt     Exceed
       -------- -----------     ------
       All      0               0
       UDP      0               0
       ICMP     0               0
       TCP      0               0

       TCP Syn Flood Half Open Count: 0, Exceed: 116
       Half Open Aggressive Aging Period Off, Event Count: 0
```

ファイアウォール イベント レート モニタリングの設定

手順の概要

1. **enable**
2. **configure terminal**
3. **parameter-map type inspect-zone** *zone-pmap-name*
4. **alert on**
5. **threat-detection basic-threat**
6. **threat-detection rate fw-drop average-time-frame** *seconds* **average-threshold** *packets-per-second* **burst-threshold** *packets-per-second*
7. **threat-detection rate inspect-drop average-time-frame** *seconds* **average-threshold** *packets-per-second* **burst-threshold** *packets-per-second*
8. **threat-detection rate syn-attack average-time-frame** *seconds* **average-threshold** *packets-per-second* **burst-threshold** *packets-per-second*
9. **exit**
10. **zone security** *security-zone-name*
11. **protection** *parameter-map-name*
12. **exit**
13. **zone-pair security** *zone-pair-name* **source** *source-zone* **destination** *destination-zone*
14. **end**
15. **show policy-firewall stats zone**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**parameter-map type inspect-zone** *zone-pmap-name* 例： `Device(config)# parameter-map type inspect-zone zone-pmap1`	ゾーン検査パラメータ マップを設定し、パラメータ マップ タイプ検査コンフィギュレーション モードを開始します。
ステップ 4	**alert on** 例： `Device(config-profile)# alert on`	ゾーンに関するステートフル パケット インスペクションのアラート メッセージのコンソール表示を有効にします。 • **log** コマンドを使用すると、アラートのロギングを Syslog または高速ロガー（HSL）のいずれかに設定できます。

	コマンドまたはアクション	目的
ステップ 5	**threat-detection basic-threat** 例： `Device(config-profile)# threat-detection basic-threat`	ゾーンの基本脅威検出を設定します。
ステップ 6	**threat-detection rate fw-drop average-time-frame** *seconds* **average-threshold** *packets-per-second* **burst-threshold** *packets-per-second* 例： `Device(config-profile)# threat-detection rate fw-drop average-time-frame 600 average-threshold 100 burst-threshold 100`	ファイアウォール ドロップ イベントの脅威検出レートを設定します。 • **threat-detection rate** コマンドを設定する前に、**threat-detection basic-threat** コマンドを設定する必要があります。
ステップ 7	**threat-detection rate inspect-drop average-time-frame** *seconds* **average-threshold** *packets-per-second* **burst-threshold** *packets-per-second* 例： `Device(config-profile)# threat-detection rate inspect-drop average-time-frame 600 average-threshold 100 burst-threshold 100`	ファイアウォール インスペクション ベースのドロップ イベントに関する脅威検出レートを設定します。
ステップ 8	**threat-detection rate syn-attack average-time-frame** *seconds* **average-threshold** *packets-per-second* **burst-threshold** *packets-per-second* 例： `Device(config-profile)# threat-detection rate syn-attack average-time-frame 600 average-threshold 100 burst-threshold 100`	TCP SYN 攻撃イベントの脅威検出レートを設定します。
ステップ 9	**exit** 例： `Device(config-profile)# exit`	パラメータ マップ タイプ検査コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードを開始します。
ステップ 10	**zone security** *security-zone-name* 例： `Device(config)# zone security public`	セキュリティ ゾーンを作成し、セキュリティ ゾーン コンフィギュレーション モードを開始します。
ステップ 11	**protection** *parameter-map-name* 例： `Device(config-sec-zone)# protection zone-pmap1`	ゾーン検査パラメータ マップをゾーンにアタッチし、ゾーン検査パラメータ マップで設定されている機能をゾーンに適用します。
ステップ 12	**exit** 例： `Device(config-sec-zone)# exit`	セキュリティ ゾーン コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 13	**zone-pair security** *zone-pair-name* **source** *source-zone* **destination** *destination-zone* 例： `Device(config)# zone-pair security private2public source private destination public`	ゾーン ペアを作成し、セキュリティ ゾーンペア コンフィギュレーション モードを開始します。
ステップ 14	**end** 例： `Device(config-sec-zone-pair)# end`	セキュリティ ゾーン ペア コンフィギュレーション モードを終了し、特権EXECモードを開始します。
ステップ 15	**show policy-firewall stats zone** 例： `Device# show policy-firewall stats zone`	ゾーン レベルでのポリシー ファイアウォール統計情報を表示します。

ボックス単位のハーフオープン セッション制限の設定

ボックス単位とは、ファイアウォールセッションテーブル全体という意味です。**parameter-map type inspect-global** コマンドに続くすべての設定がボックスに適用されます。

手順の概要

1. **enable**
2. **configure terminal**
3. 次のいずれかのコマンドを入力します。
   - **parameter-map type inspect-global**
   - **parameter-map type inspect global**
4. **alert on**
5. **per-box max-incomplete** *number*
6. **session total** *number*
7. **end**
8. **show policy-firewall stats global**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的

ステップ 3	次のいずれかのコマンドを入力します。
	• **parameter-map type inspect-global**
	• **parameter-map type inspect global**
	例：
	`Device(config)# parameter-map type inspect-global`
	`Device(config)# parameter-map type inspect global`
		接続しきい値およびタイムアウトのグローバル パラメータ マップを設定し、パラメータ マップ タイプ検査コンフィギュレーション モードを開始します。
		• リリースに基づいて、**parameter-map type inspect-global** コマンドと **parameter-map type inspect global** コマンドがサポートされます。これら両方のコマンドを一緒に設定することはできません。
		• **parameter-map type inspect-global** コマンドを設定する場合は、手順 5 および手順 6 をスキップしてください。
		（注） **parameter-map type inspect-global** コマンドを設定する場合は、**per-box** コンフィギュレーションがサポートされません。これは、デフォルトですべての **per-box** コンフィギュレーションがすべてのファイアウォールセッションに適用されるためです。

ステップ 4	**alert on** 例： `Device(config-profile)# alert on`	ステートフル パケット インスペクションのアラート メッセージのコンソール表示をイネーブルにします。
ステップ 5	**per-box max-incomplete** *number* 例： `Device(config-profile)# per-box max-incomplete 12345`	ファイアウォールセッションテーブルのハーフオープン接続の最大数を設定します。
ステップ 6	**session total** *number* 例： `Device(config-profile)# session total 34500`	ファイアウォール セッション テーブルの合計セッション制限を設定します。
ステップ 7	**end** 例： `Device(config-profile)# end`	パラメータ マップ タイプ検査コンフィギュレーション モードを終了し、特権 EXEC モードを開始します。
ステップ 8	**show policy-firewall stats global** 例： `Device# show policy-firewall stats global`	グローバル ファイアウォール統計情報を表示します。

VRF検査パラメータ マップ用のハーフオープンセッション制限の設定

手順の概要

1. **enable**
2. **configure terminal**
3. **parameter-map type inspect-vrf** *vrf-name*
4. **alert on**
5. **max-incomplete** *number*
6. **session total** *number*
7. **exit**
8. 次のいずれかのコマンドを入力します。
   - **parameter-map type inspect-global**
   - **parameter-map type inspect global**
9. **alert on**
10. **vrf** *vrf-name* **inspect** *vrf-pmap-name*
11. **end**
12. **show policy-firewall stats vrf** *vrf-pmap-name*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**parameter-map type inspect-vrf** *vrf-name* 例： `Device(config)# parameter-map type inspect-vrf vrf1-pmap`	VRF 検査パラメータ マップを設定し、パラメータ マップ タイプ検査コンフィギュレーション モードを開始します。
ステップ 4	**alert on** 例： `Device(config-profile)# alert on`	ステートフル パケット インスペクションのアラート メッセージのコンソール表示をイネーブルにします。
ステップ 5	**max-incomplete** *number* 例： `Device(config-profile)# max-incomplete 2000`	VRF ごとのハーフ オープン接続の最大数を設定します。

	コマンドまたはアクション	目的
ステップ 6	**session total** *number* 例： `Device(config-profile)# session total 34500`	VRF の総セッション制限を設定します。
ステップ 7	**exit** 例： `Device(config-profile)# exit`	パラメータ マップ タイプ検査コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードを開始します。

ステップ 8	次のいずれかのコマンドを入力します。
	• **parameter-map type inspect-global**
	• **parameter-map type inspect global**
	例：
	`Device(config)# parameter-map type inspect-global`
	`Device(config)# parameter-map type inspect global`
		接続しきい値およびタイムアウトのグローバル パラメータ マップを設定し、パラメータ マップ タイプ検査コンフィギュレーション モードを開始します。
		• リリースに基づいて、**parameter-map type inspect-global** コマンドまたは **parameter-map type inspect global** コマンドのいずれかを使用できます。これら両方のコマンドを一緒に設定することはできません。
		• **parameter-map type inspect-global** コマンドを設定する場合は、手順 10 をスキップしてください。
		（注） **parameter-map type inspect-global** コマンドを設定する場合は **per-box** コンフィギュレーションがサポートされません。これは、デフォルトですべての **per-box** コンフィギュレーションがすべてのファイアウォールセッションに適用されるためです。

ステップ 9	**alert on** 例： `Device(config-profile)# alert on`	ステートフル パケット インスペクションのアラート メッセージのコンソール表示をイネーブルにします。
ステップ 10	**vrf** *vrf-name* **inspect** *vrf-pmap-name* 例： `Device(config-profile)# vrf vrf1 inspect vrf1-pmap`	グローバル パラメータ マップに VRF をバインドします。
ステップ 11	**end** 例： `Device(config-profile)# end`	パラメータ マップ タイプ検査コンフィギュレーション モードを終了し、特権 EXEC モードを開始します。

	コマンドまたはアクション	目的
ステップ 12	**show policy-firewall stats vrf** *vrf-pmap-name* 例： `Device# show policy-firewall stats vrf vrf1-pmap`	VRF レベル ポリシー ファイアウォール統計情報を表示します。

グローバル TCP SYN フラッド制限の設定

手順の概要

1. **enable**
2. **configure terminal**
3. 次のいずれかのコマンドを入力します。
   - **parameter-map type inspect-global**
   - **parameter-map type inspect global**
4. **alert on**
5. **per-box tcp syn-flood limit** *number*
6. **end**
7. **show policy-firewall stats vrf global**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。

ステップ 3	次のいずれかのコマンドを入力します。
	• **parameter-map type inspect-global**
	• **parameter-map type inspect global**
	例：
	`Device(config)# parameter-map type inspect-global`
	`Device(config)# parameter-map type inspect global`
		グローバル パラメータ マップを設定し、パラメータ マップ タイプ検査コンフィギュレーション モードを開始します。
		• リリースに基づいて、**parameter-map type inspect-global** コマンドまたは **parameter-map type inspect global** コマンドのいずれかを設定できます。これら両方のコマンドを一緒に設定することはできません。
		• **parameter-map type inspect-global** コマンドを設定する場合は、手順 5 をスキップしてください。

	コマンドまたはアクション	目的
		（注） **parameter-map type inspect-global** コマンドを設定する場合は、**per-box** コンフィギュレーションがサポートされません。これは、デフォルトですべての **per-box** コンフィギュレーションがすべてのファイアウォールセッションに適用されるためです。
ステップ 4	**alert on** 例： `Device(config-profile)# alert on`	ステートフル パケット インスペクションのアラート メッセージのコンソール表示をイネーブルにします。
ステップ 5	**per-box tcp syn-flood limit** *number* 例： `Device(config-profile)# per-box tcp syn-flood limit 500`	新しい SYN パケットの SYN Cookie 処理をトリガーする TCP ハーフ オープン セッションの数を制限します。
ステップ 6	**end** 例： `Device(config-profile)# end`	パラメータ マップ タイプ検査コンフィギュレーション モードを終了し、特権 EXEC モードを開始します。
ステップ 7	**show policy-firewall stats vrf global** 例： `Device# show policy-firewall stats vrf global`	（任意）グローバル VRF ファイアウォール ポリシーのステータスを表示します。 • 存在する TCP ハーフ オープン セッションの数もまたコマンド出力に表示されます。

例

次に、**show policy-firewall stats vrf global** コマンドの出力例を示します。

```
Device# show policy-firewall stats vrf global

Global table statistics
       total_session_cnt: 0
       exceed_cnt:        0
       tcp_half_open_cnt: 0
       syn_exceed_cnt:    0
```

分散型サービス妨害攻撃に対する保護の設定例

例：ファイアウォールの設定

```
Router# configure terminal
Router(config)# class-map type inspect match-any ddos-class
Router(config-cmap)# match protocol tcp
Router(config-cmap-c)# exit
Router(config)# parameter-map type inspect global
Router(config-profile)# redundancy
Router(config-profile)# exit
Router(config)# policy-map type inspect ddos-fw
Router(config-pmap)# class type inspect ddos-class
Router(config-pmap-c)# inspect
Router(config-pmap-c)# exit
Router(config-pmap)# class class-default
Router(config-pmap-c)# drop
Router(config-pmap-c)# exit
Router(config-pmap)# exit
Router(config)# zone security private
Router(config-sec-zone)# exit
Router(config)# zone security public
Router(config-sec-zone)# exit
Router(config)# zone-pair security private2public source private destination public
Router((config-sec-zone-pair)# service-policy type inspect ddos-fw
Router((config-sec-zone-pair)# exit
Router(config)# interface gigabitethernet 0/1/0.1
Router(config-subif)# ip address 10.1.1.1 255.255.255.0
Router(config-subif)# encapsulation dot1q 2
Router(config-subif)# zone-member security private
Router(config-subif)# exit
Router(config)# interface gigabitethernet 1/1/0.1
Router(config-subif)# ip address 10.2.2.2 255.255.255.0
Router(config-subif)# encapsulation dot1q 2
Router(config-subif)# zone-member security public
Router(config-subif)# end
```

例：ファイアウォール セッションのアグレッシブ エージングの設定

例：ボックス単位のアグレッシブ エージングの設定

```
Device# configure terminal
Device(config)# parameter-map type inspect global
Device(config-profile)# per-box max-incomplete 2000 aggressive-aging 1500 low 1200
Device(config-profile)# per-box aggressive-aging high 1700 low 1300
Device(config-profile)# exit
Device(config)# parameter-map type inspect pmap1
Device(config-profile)# tcp synwait-time 30 ageout-time 10
Device(config-profile)# end
```

例：デフォルト VRF のアグレッシブ エージングの設定

```
Device# configure terminal
Device(config)# parameter-map type inspect global
Device(config-profile)# max-incomplete 2000 aggressive-aging high 1500 low 1200
Device(config-profile)# session total 1000 aggressive-aging high percent 80 low percent
 60
Device(config-profile)# exit
Device(config)# parameter-map type inspect pmap1
Device(config-profile)# tcp synwait-time 30 ageout-time 10
Device(config-profile)# end
```

例：ファイアウォール セッションのエージング アウトの設定

```
Device# configure terminal
Device(config-profile)# exit
Device(config)# parameter-map type inspect global
Device(config-profile)# vrf vrf1 inspect vrf1-pmap
Device(config-profile)# exit
Device(config)# parameter-map type inspect pmap1
Device(config-profile)# tcp idle-time 3000 ageout-time 100
Device(config-profile)# tcp synwait-time 30 ageout-time 10
Device(config-profile)# exit
Device(config)# policy-map type inspect ddos-fw
Device(config-profile)# class type inspect match-any ddos-class
Device(config-profile)# inspect pmap1
Device(config-profile)# end
```

例：VRF 単位のアグレッシブ エージングの設定

```
Device# configure terminal
Device(config)# ip vrf ddos-vrf1
Device(config-vrf)# rd 100:2
Device(config-vrf)# route-target export 100:2
Device(config-vrf)# route-target import 100:2
Device(config-vrf)# exit
Device(config)# parameter-map type inspect-vrf vrf1-pmap
Device(config-profile)# max-incomplete 3455 aggressive-aging high 2345 low 2255
Device(config-profile)# session total 1000 aggressive-aging high percent 80 low percent
 60
Device(config-profile)# alert on
Device(config-profile)# exit
Device(config)# parameter-map type inspect global
Device(config-profile)# vrf vrf1 inspect vrf1-pmap
Device(config-profile)# exit
Device(config)# parameter-map type inspect pmap1
Device(config-profile)# tcp idle-time 3000 ageout-time 100
Device(config-profile)# tcp synwait-time 30 ageout-time 10
Device(config-profile)# exit
Device(config)# policy-map type inspect ddos-fw
Device(config-pmap)# class type inspect match-any ddos-class
Device(config-pmap-c)# inspect pmap1
Device(config-profile)# end
```

例：ファイアウォール イベント レート モニタリングの設定

```
Device> enable
Device# configure terminal
Device(config)# parameter-map type inspect zone zone-pmap1
Device(config-profile)# alert on
Device(config-profile)# threat-detection basic-threat
Device(config-profile)# threat-detection rate fw-drop average-time-frame 600
average-threshold 100 burst-threshold 100
Device(config-profile)# threat-detection rate inspect-drop average-time-frame 600
average-threshold 100 burst-threshold 100
Device(config-profile)# threat-detection rate syn-attack average-time-frame 600
average-threshold 100 burst-threshold 100
Device(config-profile)# exit
Device(config)# zone security public
Device(config-sec-zone)# protection zone-pmap1
Device(config-sec-zone)# exit
Device(config)# zone-pair security private2public source private destination public
Device(config-sec-zone-pair)# end
```

例：ボックス単位のハーフオープン セッション制限の設定

```
Device# configure terminal
Device(config)# parameter-map type inspect global
Device(config-profile)# alert on
Device(config-profile)# per-box max-incomplete 12345
Device(config-profile)# session total 34500
Device(config-profile)# end
```

例：検査 VRF パラメータ マップに対するハーフオープン セッション制限の設定

```
Device# configure terminal
Device(config)# parameter-map type inspect vrf vrf1-pmap
Device(config-profile)# alert on
Device(config-profile)# max-incomplete 3500
Device(config-profile)# session total 34500
Device(config-profile)# exit
Device(config)# parameter-map type inspect global
Device(config-profile)# alert on
Device(config-profile)# vrf vrf1 inspect vrf1-pmap
Device(config-profile)# end
```

例：グローバル TCP SYN フラッド制限の設定

```
Device# configure terminal
Device(config)# parameter-map type inspect global
```

```
Device(config-profile)# alert on
Device(config-profile)# per-box tcp syn-flood limit 500
Device(config-profile)# end
```

分散型サービス妨害攻撃に対する保護に関する追加情報

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『Cisco IOS Master Command List, All Releases』
セキュリティ コマンド	『Cisco IOS セキュリティ コマンド リファレンス』
ファイアウォール リソース管理	『*Configuring Firewall Resource Management feature*』
ファイアウォール TCP SYN Cookie	『*Configuring Firewall TCP SYN Cookie feature*』

シスコのテクニカル サポート

説明	リンク
右の URL にアクセスして、シスコのテクニカル サポートを最大限に活用してください。これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

分散型サービス妨害攻撃に対する保護に関する機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *187 :* 分散型サービス妨害攻撃に対する保護に関する機能情報

機能名	リリース	機能情報
分散型サービス妨害攻撃に対する保護	Cisco IOS XE リリース 3.4S	分散型サービス妨害攻撃に対する保護機能は、ボックス単位レベル（すべてのファイアウォール セッションに対応）と VRF レベルでの DoS 攻撃に対する保護を提供します。DDoS 攻撃を防ぐために、ファイアウォール セッションのアグレッシブ エージング、ファイアウォール セッションのイベント レート モニタリング、ハーフオープン接続制限、およびグローバル TCP SYN Cookie 保護を設定できます。 次のコマンドが導入または変更されました。**clear policy-firewall stats global**、**max-incomplete**、**max-incomplete aggressive-aging**、**per-box aggressive-aging**、**per-box max-incomplete**、**per-box max-incomplete aggressive-aging**、**per-box tcp syn-flood limit**、**session total**、**show policy-firewall stats global**、**show policy-firewall stats zone**、**threat-detection basic-threat**、**threat-detection rate**、および **udp half-open**。

第 140 章

ファイアウォール リソース管理の設定

ファイアウォール リソース管理機能は、ルータで設定される VPN ルーティングおよび転送（VRF）セッションとグローバル ファイアウォール セッションの数を制限します。

ファイアウォールリソース管理の設定に関する制約事項

- グローバル レベルまたは VRF レベルのセッション制限を設定した後、その制限値を下回るセッション制限を再設定すると、新しいセッションは追加されなくなります。ただし、現在のセッションはドロップされません。

ファイアウォール リソース管理の設定について

ファイアウォール リソース管理

リソース管理では、デバイス上の共有リソースの利用レベルが制限されます。デバイス上の共有リソースには次のものがあります。

- 帯域幅
- 接続状態
- メモリ使用率（テーブル単位）
- セッションまたはコールの数
- Packets per second（1 秒あたりのパケット数）

- Ternary content addressable memory（TCAM）エントリ

ファイアウォール リソース管理機能は、ゾーンベースのファイアウォール リソース管理をクラス レベルから VRF レベルおよびグローバル レベルに拡張します。クラス レベルのリソース管理は、クラス レベルでファイアウォール セッションのリソースを保護します。たとえば、最大セッション制限、セッション レート制限、不完全セッション制限などのパラメータは、ファイアウォール リソース（チャンク メモリなど）を保護し、これらのリソースが単一クラスによって使い果たされないようにします。

複数の Virtual Routing and Forwarding（VRF）インスタンスが同じポリシーを共有する場合、1 つの VRF インスタンスからのファイアウォール セッション設定要求によって総セッション数が最大制限に達する可能性があります。1 つの VRF がデバイス上で最大量のリソースを消費すると、他の VRF インスタンスがデバイス リソースを共有することが難しくなります。VRF ファイアウォール セッションの数を制限するには、ファイアウォール リソース管理機能を使用できます。

グローバル レベルでは、ファイアウォール リソース管理機能により、グローバル ルーティング ドメインでのファイアウォール セッションによるリソースの使用を制限できます。

VRF 対応 Cisco IOS XE ファイアウォール

サービス プロバイダー（SP）または大企業のエッジ ルータで VRF 対応 Cisco IOS XE ファイアウォールが設定されている場合は、Cisco IOS XE ファイアウォール機能が VPN ルーティングおよび転送（VRF）インターフェイスに適用されます。SP は中小企業市場にマネージドサービスを提供しています。

VRF 対応 Cisco IOS XE ファイアウォールは、さまざまなプロトコルの VRF-Lite（別名 Multi-VRF CE）と Application Inspection and Control（AIC）をサポートします。

VRF 対応ファイアウォールは、さまざまなプロトコルの VRF-Lite（別名 Multi-VRF CE）と Application Inspection and Control（AIC）をサポートします。

（注） Cisco IOS XE リリースは、コンテキストベースのアクセス コントロール（CBAC）ファイアウォールをサポートしません。

ファイアウォール セッション

セッション定義

Virtual Routing and Forwarding（VRF）レベルでは、ファイアウォール リソース管理機能により、各 VRF インスタンスのファイアウォール セッション数が追跡されます。グローバル レベルでは、ファイアウォール リソース管理機能により、デバイス レベルではなくグローバル ルーティング ドメインでのファイアウォール セッションの合計数が追跡されます。VRF とグローバル レベルの両方では、セッション数はオープン セッションとハーフオープン セッションと

不正確なファイアウォール セッション データベース内のセッションの合計です。まだ確立状態に達していない TCP セッションは、ハーフオープン セッションと呼ばれます。

ファイアウォールには 2 つのセッション データベースがあります。1 つはセッション データベースで、もう 1 つは不正確なセッションデータベースです。セッションデータベースには、5 つのタプル（送信元 IP アドレス、宛先 IP アドレス、送信元ポート、宛先ポート、およびプロトコル）のセッションが含まれます。タプルは、要素の番号付きリストです。不正確なセッションデータベースには、5 つ未満のタプル（欠落した IP アドレス、ポート番号など）のセッションが含まれます。

次の規則は、セッション制限の設定に適用されます。

- クラスレベル セッションの上限は、グローバルの制限を超える可能性があります。
- クラスレベル セッションの上限は、関連する VRF セッションの最大値を超える可能性があります。
- VRF 制限値の合計は、グローバルなコンテキストを含め、ハードコーディングされたセッションの制限を超える可能性があります。

セッション レート

セッション レートは、セッションが特定の時間間隔で確立されるレートです。最大および最小セッション レート制限を定義できます。セッション レートが指定された最大レートを超えると、ファイアウォールは新しいセッションのセットアップ要求を拒否し始めます。

リソース管理の観点から最大および最小セッション レート制限を設定すると、多数のファイアウォール セッションのセットアップ要求が受信された場合に、Cisco Packet Processor が過負荷になることを防ぐのに役立ちます。

未完了またはハーフオープン セッション

未完了セッションはハーフオープンセッションです。未完了セッションで使用されるリソースがカウントされ、未完了セッション数の増加は最大セッション数制限を設定することにより制限されます。

ファイアウォール リソース管理セッション

ファイアウォール リソース管理セッションには次のルールが適用されます。

- デフォルトでは、オープン セッションまたはハーフオープン セッションのセッション制限は無制限です。
- オープン セッションまたはハーフオープン セッションは、パラメータで制限され、個別にカウントされます。
- オープン セッションの数またはハーフオープン セッションの数には、Internet Control Message Protocol（ICMP）、TCP、または UDP セッションが含まれます。
- オープン セッションの数とレートを制限できます。

• ハーフオープン セッションではセッションの数だけを制限できます。

ファイアウォール リソース管理の設定方法

ファイアウォール リソース管理の設定

（注） グローバル パラメータ マップは、ルータ レベルではなく、グローバル ルーティング ドメインで有効になります。

手順の概要

1. **enable**
2. **configure terminal**
3. **parameter-map type inspect-vrf** *vrf-pmap-name*
4. **session total** *number*
5. **tcp syn-flood limit** *number*
6. **exit**
7. **parameter-map type inspect-global**
8. **vrf** *vrf-name* **inspect** *parameter-map-name*
9. **exit**
10. **parameter-map type inspect-vrf vrf-default**
11. **session total** *number*
12. **tcp syn-flood limit** *number*
13. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**parameter-map type inspect-vrf** *vrf-pmap-name* 例： `Device(config)# parameter-map type inspect-vrf vrf1-pmap`	VRF 検査タイプ パラメータ マップを設定し、パラメータ マップ タイプ検査コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 4	**session total** *number* 例： `Device(config-profile)# session total 1000`	セッションの総数を設定します。
ステップ 5	**tcp syn-flood limit** *number* 例： `Device(config-profile)# tcp syn-flood limit 2000`	新しい SYN パケットの同期（SYN）Cookie 処理をトリガーする TCP ハーフ オープン セッションの数を制限します。
ステップ 6	**exit** 例： `Device(config-profile)# exit`	パラメータ マップ タイプ検査コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードを開始します。
ステップ 7	**parameter-map type inspect-global** 例： `Device(config)# parameter-map type inspect-global`	グローバル パラメータ マップを設定し、パラメータ マップ タイプ検査コンフィギュレーション モードを開始します。
ステップ 8	**vrf** *vrf-name* **inspect** *parameter-map-name* 例： `Device(config-profile)# vrf vrf1 inspect vrf1-pmap`	VRF をパラメータ マップにバインドします。
ステップ 9	**exit** 例： `Device(config-profile)# exit`	パラメータ マップ タイプ検査コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードを開始します。
ステップ 10	**parameter-map type inspect-vrf vrf-default** 例： `Device(config)# parameter-map type inspect-vrf vrf-default`	デフォルトの VRF 検査タイプ パラメータ マップを設定します。
ステップ 11	**session total** *number* 例： `Device(config-profile)# session total 6000`	セッションの総数を設定します。 • VRF 検査タイプパラメータマップ用およびグローバルパラメータマップ用に **session total** コマンドを設定できます。VRF 検査タイプパラメータマップ用に **session total** コマンドを設定する場合、VRF 検査タイプパラメータマップにセッションが関連付けられます。グローバルパラメータマップ用に **session total** コマンドを設定する場合、このコマンドはグローバル ルーティング ドメインに適用されます。

	コマンドまたはアクション	目的
ステップ 12	**tcp syn-flood limit** *number* 例： `Device(config-profile)# tcp syn-flood limit 7000`	新しいSYNパケットのSYN Cookie処理をトリガーするTCPハーフ オープン セッションの数を制限します。
ステップ 13	**end** 例： `Device(config-profile)# end`	パラメータマップタイプ検査コンフィギュレーション モードを終了し、特権 EXEC モードを開始します。

ファイアウォール リソース管理の設定例

例：ファイアウォール リソース管理の設定

```
Device# configure terminal
Device(config)# parameter-map type inspect-vrf vrf1-pmap
Device(config-profile)# session total 1000
Device(config-profile)# tcp syn-flood limit 2000
Device(config-profile)# exit
Device(config)# parameter-map type inspect-global
Device(config-profile)# vrf vrf1 inspect pmap1
Device(config-profile)# exit
Device(config)# parameter-map type inspect-vrf vrf-default
Device(config-profile)# session total 6000
Device(config-profile)# tcp syn-flood limit 7000
Device(config-profile)# end
```

その他の参考資料

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『Cisco IOS Master Commands List, All Releases』
セキュリティ コマンド	• 『Security Command Reference: Commands A to C』 • 『Security Command Reference: Commands D to L』 • 『Security Command Reference: Commands M to R』 • 『Security Command Reference: Commands S to Z』
VRF 対応ファイアウォール	「VRF 対応 Cisco IOS XE ファイアウォール」モジュール

関連項目	マニュアル タイトル
ゾーンベース ポリシー ファイアウォール	「ゾーンベース ポリシー ファイアウォール」モジュール

シスコのテクニカル サポート

説明	リンク
右の URL にアクセスして、シスコのテクニカル サポートを最大限に活用してください。これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

ファイアウォール リソース管理の設定に関する機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *188* : ファイアウォール リソース管理の設定に関する機能情報

機能名	リリース	機能情報
ファイアウォール リソース管理	Cisco IOS XE リリース 3.3S	ファイアウォール リソース管理機能は、ルータで設定される VPN ルーティングおよび転送（VRF）セッションとグローバル ファイアウォール セッションの数を制限します。 次のコマンドが導入または変更されました。**parameter-map type inspect-vrf**。

第 141 章

IPv6 ファイアウォールでの分散型サービス妨害攻撃の防止およびリソース管理のサポート

IPv6 ゾーンベース ファイアウォールでは、分散型サービス妨害攻撃の防止およびリソース管理がサポートされています。

分散型サービス妨害攻撃の防止機能は、グローバル レベル（すべてのファイアウォール セッション）および VPN ルーティングおよび転送（VRF）レベルでのサービス妨害（DoS）攻撃からの保護を提供します。分散型サービス妨害攻撃からの保護機能により、分散型 DoS 攻撃を防止するため、ファイアウォール セッションのアグレッシブ エージング、ファイアウォール セッションのイベント レート モニタ、ハーフオープン接続制限、およびグローバル TCP 同期（SYN）Cookie 保護を設定できます。

ファイアウォール リソース管理機能では、デバイスで設定されているグローバル ファイアウォール セッションと VPN ルーティングおよび転送（VRF）インスタンスの数が制限されます。

このモジュールでは、分散型サービス妨害攻撃からの保護機能とファイアウォール リソース管理機能を設定する方法について説明します。

IPv6 ファイアウォールでの分散型サービス妨害攻撃からの保護およびリソース管理のサポートの制約事項

ファイアウォール リソース管理機能には次の制約事項が適用されます。

- グローバル レベルまたは Virtual Routing and Forwarding（VRF）レベルでのセッション制限を設定し、その後このセッション制限を再設定すると、グローバル レベルまたは VRF レベルのセッション制限が初期設定セッション数を下回っている場合に、新しいセッションが追加されません。ただし、現在のセッションはドロップされません。

IPv6 ファイアウォールでの分散型サービス妨害攻撃の防止およびリソース管理のサポートに関する情報

ファイアウォール セッションのアグレッシブ エージング

アグレッシブエージング機能により、ファイアウォールは、セッションを積極的にエージングアウトし、新しいセッションのためのスペースを確保することで、ファイアウォールセッションデータベースがいっぱいになるのを防ぐことができます。ファイアウォールはそのリソースを保護するため、アイドル セッションを削除します。アグレッシブ エージング機能により、ファイアウォールセッションが存在できる時間は、タイマーで定義されている時間（エージングアウト時間）よりも短くなります。

アグレッシブ エージング機能には、アグレッシブ エージング期間の開始と終了を定義するしきい値（高位水準点と低位水準点）があります。アグレッシブエージング期間は、セッションテーブルが高位水準点を超えると開始され、低位水準点を下回ると終了します。アグレッシブエージングの期間中、セッションの存続期間は、エージングアウト時間を使用して設定した期間よりも短くなります。ファイアウォールがセッションを終了する時間よりも短い時間で攻撃者がセッションを開始する場合、セッションを作成するために割り当てられているすべてのリソースが使用され、新しいすべての接続が拒否されます。このような攻撃を防ぐには、セッションを積極的にエージングアウトするようにアグレッシブエージング機能を設定できます。この機能はデフォルトで無効に設定されています。

ボックス レベル（ボックスはファイアウォール セッション テーブル全体を示します）および Virtual Routing and Forwarding（VRF）レベルで、ハーフオープン セッションおよび総セッションにアグレッシブエージングを設定できます。この機能を総セッションに対して設定している場合、ファイアウォールセッション リソースを使用するすべてのセッションが考慮されます。総セッションは、確立されたセッション、ハーフオープンセッション、および不明確セッション データベース内のセッションで構成されます。（確立状態に達していない TCP セッションはハーフオープン セッションと呼ばれます）。

ファイアウォールには 2 つのセッション データベースがあります。1 つはセッション データベースで、もう 1 つは不正確なセッション データベースです。セッション データベースには、5 タプル（送信元 IP アドレス、宛先 IP アドレス、送信元ポート、宛先ポート、およびプロトコル）が設定されているセッションが含まれます。タプルは、要素の番号付きリストです。不正確なセッション データベースには、5 つ未満のタプル（欠落した IP アドレス、ポート番号など）のセッションが含まれます。ハーフオープン セッションのアグレッシブ エージングでは、ハーフオープン セッションだけが考慮されます。

Internet Control Message Protocol（ICMP）、TCP、および UDP ファイアウォール セッションにはアグレッシブ エージングアウト時間を設定できます。エージングアウト時間は、デフォルトではアイドル時間に設定されます。

イベント レート モニタリング機能

イベント レート モニタリング機能は、ゾーンの事前定義イベントのレートをモニタします。イベント レート モニタリング機能には基本脅威検出機能が含まれています。これはセキュリティ デバイスの機能であり、ファイアウォールの内側にあるリソースで発生する可能性のある脅威、異常、および攻撃を検出し、それらに対するアクションを実行します。イベントの基本脅威検出レートを設定できます。特定タイプのイベントの着信レートが、設定されている脅威検出レートを超えると、イベント レート モニタリング機能はこのイベントを脅威と見なし、脅威を阻止するためのアクションを実行します。脅威検出機能は、入力ゾーンでのみイベントを検査します（イベント レート モニタリング機能が入力ゾーンで有効な場合）。

ネットワーク管理者に対し、発生する可能性のある脅威に関する情報がアラート メッセージ（syslog または高速ロガー（HSL））で通知されます。ネットワーク管理者は攻撃ベクトルの検出、攻撃元ゾーンの検出、または特定の動作やトラフィックをブロックするようにネットワーク上のデバイスを設定するなどのアクションを実行できます。

イベント レート モニタリング機能は、次のタイプのイベントをモニタします。

- 基本ファイアウォール チェックが失敗したためにファイアウォールがドロップする：これには、ゾーンまたはゾーンペアのチェック失敗、ドロップ アクションを使用して設定されたファイアウォール ポリシーなどがあります。
- レイヤ 4 インスペクションの失敗が原因でファイアウォールがドロップする：これには、1 番目の TCP パケットが同期（SYN）パケットではないために失敗した TCP インスペクションが含まれることがあります。
- TCP SYN Cookie 攻撃：これには、ドロップされた SYN パケットの数と、スプーフィング攻撃として送信された SYN Cookie の数の集計が含まれることがあります。

イベント レート モニタリング機能は、さまざまなイベントの平均レートとバースト レートをモニタします。各イベント タイプにはレート オブジェクトがあります。レート オブジェクトは、設定可能なパラメータ（平均しきい値、バーストしきい値、期間）が含まれる関連レートにより制御されます。期間はタイム スロットに分割されます。各タイム スロットは期間の 1/30 です。

平均レートは、イベント タイプごとに計算されます。各レート オブジェクトは、30 個の完了済みサンプリング値と、現在進行中のサンプリング期間を保持するための 1 つの値を保持しま

す。計算済みの最も古い値が現在のサンプリング値で置き換えられ、平均が再計算されます。平均レートは各期間で計算されます。平均レートが平均しきい値を超えると、イベント レート モニタリング機能はこれを潜在的な脅威と解釈し、統計情報を更新し、ネットワーク管理者に通知します。

バースト レートは、トークン バケット アルゴリズムを使用して実装されます。各タイムスロットで、トークン バケットがトークンで埋められます。発生する（特定のイベント タイプの）イベントごとに、バケットからトークンが削除されます。空のバケットは、バーストしきい値に到達したことを意味し、管理者が syslog または HSL からアラームを受信します。 **show policy-firewall stats zone** コマンドの出力から、脅威検出統計情報を確認し、ゾーン内でさまざまなイベントに対する潜在的な脅威を理解することができます。

最初に **threat-detection basic-threat** コマンドを使用して、基本脅威検出機能を有効にする必要があります。基本脅威検出機能を設定したら、脅威検出レートを設定できます。脅威検出レートを設定するには、**threat-detection rate** コマンドを使用します。

次の表では、イベント レート モニタリング機能が有効な場合に適用可能な基本脅威検出のデフォルト設定について説明します。

表 *189 :* 基本的な脅威の検出のデフォルト設定

パケット ドロップの理由	脅威検出の設定
基本的なファイアウォール ドロップ	平均レート 400 パケット/秒（pps） バースト レート 1600 pps レート間隔 600 秒
インスペクション ベースのファイアウォール ドロップ	平均レート 400 pps バースト レート 1600 pps レート間隔 600 秒
SYN 攻撃ファイアウォール ドロップ	平均レート 100 pps バースト レート 200 pps レート間隔 600 秒

ハーフオープン接続の制限

ファイアウォール セッション テーブルでは、ファイアウォールのハーフオープン接続数を制限できるようになっています。ハーフオープンセッション数を制限することで、ハーフオープン セッションでボックスごとのレベルや Virtual Routing and Forwarding（VRF）レベルでファイアウォール セッション テーブルをいっぱいにしてセッションを確立できないようにする攻撃に対し、ファイアウォールを防御できます。ハーフオープン接続の制限は、レイヤ4プロトコル、Internet Control Message Protocol（ICMP）、TCP、UDP に対して設定できます。UDP ハーフオープンセッション数に対して設定された制限は、TCP や ICMP のハーフオープンセッショ

ンには影響しません。設定されたハーフオープンセッションの制限を超えると、すべての新規セッションが拒否され、ログメッセージがSyslogまたは高速ロガー（HSL）に生成されます。

次のセッションはハーフオープン セッションと見なされます。

- 3 ウェイ ハンドシェイクを完了していない TCP セッション。
- UDP フローで 1 つのパケットだけが検出された UDP セッション。
- ICMP エコー要求または ICMP タイムスタンプ要求に対する応答を受信していない ICMP セッション。

TCP SYN フラッド攻撃

グローバルの TCP SYN フラッド制限を設定して、SYN フラッド攻撃を制限できます。TCP SYN フラッド攻撃は、サービス妨害（DoS）攻撃の一種です。設定済みの TCP SYN フラッド制限に達すると、ファイアウォールは、さらにセッションを作成する前に、セッションの送信元を確認します。通常は、TCP SYN パケットはファイアウォールの背後のターゲット エンドホストまたはサブネット アドレスの範囲に送信されます。これらの TCP SYN パケットによって、送信元 IP アドレスがスプーフィングされます。スプーフィング攻撃では、個人やプログラムが偽のデータを使用してネットワーク内のリソースにアクセスしようとします。TCP SYN フラッディングは、ファイアウォールまたはエンドホスト上のすべてのリソースを乗っ取る可能性があるため、サービス妨害がトラフィックを正当化することになります。TCP SYN フラッド保護は、VRF レベルとゾーン レベルで設定できます。

SYN フラッド攻撃は、次の 2 つのタイプに分類されます。

- ホスト フラッド：SYN フラッド パケットが単一のホストに送信され、そのホスト上のすべてのリソースを使用することが意図されます。
- ファイアウォールセッションテーブルフラッド：SYN フラッドパケットがファイアウォールの背後のアドレスの範囲に送信され、ファイアウォール上のセッションテーブルリソースを枯渇させ、その結果、リソースの拒否がファイアウォールを通過するトラフィックを正当化することが意図されます。

ファイアウォール リソース管理

リソース管理では、デバイス上の共有リソースの利用レベルが制限されます。デバイス上の共有リソースには次のものがあります。

- 帯域幅
- 接続状態
- メモリ使用率（テーブル単位）
- セッションまたはコールの数
- Packets per second（1 秒あたりのパケット数）

- Ternary content addressable memory（TCAM）エントリ

ファイアウォール リソース管理機能は、ゾーンベースのファイアウォール リソース管理をクラス レベルから VRF レベルおよびグローバル レベルに拡張します。クラス レベルのリソース管理は、クラス レベルでファイアウォール セッションのリソースを保護します。たとえば、最大セッション制限、セッション レート制限、不完全セッション制限などのパラメータは、ファイアウォール リソース（チャンク メモリなど）を保護し、これらのリソースが単一クラスによって使い果たされないようにします。

複数の Virtual Routing and Forwarding（VRF）インスタンスが同じポリシーを共有する場合、1 つの VRF インスタンスからのファイアウォール セッション設定要求によって総セッション数が最大制限に達する可能性があります。1 つの VRF がデバイス上で最大量のリソースを消費すると、他の VRF インスタンスがデバイス リソースを共有することが難しくなります。VRF ファイアウォール セッションの数を制限するには、ファイアウォール リソース管理機能を使用できます。

グローバル レベルでは、ファイアウォール リソース管理機能により、グローバル ルーティング ドメインでのファイアウォール セッションによるリソースの使用を制限できます。

ファイアウォール セッション

セッション定義

Virtual Routing and Forwarding（VRF）レベルでは、ファイアウォール リソース管理機能により、各 VRF インスタンスのファイアウォール セッション数が追跡されます。グローバル レベルでは、ファイアウォール リソース管理機能により、デバイス レベルではなくグローバル ルーティング ドメインでのファイアウォール セッションの合計数が追跡されます。VRF とグローバル レベルの両方では、セッション数はオープン セッションとハーフオープン セッションと不正確なファイアウォール セッション データベース内のセッションの合計です。まだ確立状態に達していない TCP セッションは、ハーフオープン セッションと呼ばれます。

ファイアウォールには 2 つのセッション データベースがあります。1 つはセッション データベースで、もう 1 つは不正確なセッション データベースです。セッション データベースには、5 つのタプル（送信元 IP アドレス、宛先 IP アドレス、送信元ポート、宛先ポート、およびプロトコル）のセッションが含まれます。タプルは、要素の番号付きリストです。不正確なセッション データベースには、5 つ未満のタプル（欠落した IP アドレス、ポート番号など）のセッションが含まれます。

次の規則は、セッション制限の設定に適用されます。

- クラス レベル セッションの上限は、グローバルの制限を超える可能性があります。
- クラス レベル セッションの上限は、関連する VRF セッションの最大値を超える可能性があります。
- VRF 制限値の合計は、グローバルなコンテキストを含め、ハードコーディングされたセッションの制限を超える可能性があります。

セッション レート

セッション レートは、セッションが特定の時間間隔で確立されるレートです。最大および最小セッション レート制限を定義できます。セッション レートが指定された最大レートを超えると、ファイアウォールは新しいセッションのセットアップ要求を拒否し始めます。

リソース管理の観点から最大および最小セッション レート制限を設定すると、多数のファイアウォール セッションのセットアップ要求が受信された場合に、Cisco Packet Processor が過負荷になることを防ぐのに役立ちます。

未完了またはハーフオープン セッション

未完了セッションはハーフオープンセッションです。未完了セッションで使用されるリソースがカウントされ、未完了セッション数の増加は最大セッション数制限を設定することにより制限されます。

ファイアウォール リソース管理セッション

ファイアウォール リソース管理セッションには次のルールが適用されます。

- デフォルトでは、オープン セッションまたはハーフオープン セッションのセッション制限は無制限です。
- オープン セッションまたはハーフオープン セッションは、パラメータで制限され、個別にカウントされます。
- オープン セッションの数またはハーフオープン セッションの数には、Internet Control Message Protocol（ICMP）、TCP、または UDP セッションが含まれます。
- オープン セッションの数とレートを制限できます。
- ハーフオープン セッションではセッションの数だけを制限できます。

IPv6 ファイアウォールでの分散型サービス妨害攻撃の防止およびリソース管理のサポートの設定方法

IPv6 ファイアウォールの設定

IPv4 ファイアウォールと IPv6 ファイアウォールを設定する手順は同じです。IPv6 ファイアウォールを設定するには、IPv6 アドレス ファミリだけがマッチングされるようにクラス マップを設定する必要があります。

match protocol コマンドは IPv4 トラフィックと IPv6 トラフィックの両方に適用され、IPv4 ポリシーと IPv6 ポリシーのどちらにもこれを含めることができます。

手順の概要

1. **enable**
2. **configure terminal**
3. **vrf-definition** *vrf-name*
4. **address-family ipv6**
5. **exit-address-family**
6. **exit**
7. **parameter-map type inspect** *parameter-map-name*
8. **sessions maximum** セッション
9. **exit**
10. **ipv6 unicast-routing**
11. **ip port-map** *appl-name* **port** *port-num* **list** *list-name*
12. **ipv6 access-list** *access-list-name*
13. **permit ipv6 any any**
14. **exit**
15. **class-map type inspect match-all** *class-map-name*
16. **match access-group name** *access-group-name*
17. **match protocol** *protocol-name*
18. **exit**
19. **policy-map type inspect** *policy-map-name*
20. **class type inspect** *class-map-name*
21. **inspect** [*parameter-map-name*]
22. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを開始します。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**vrf-definition** *vrf-name* 例： `Device(config)# vrf-definition VRF1`	Virtual Routing and Forwarding（VRF）ルーティング テーブルインスタンスを設定し、VRF コンフィギュレーション モードを開始します。
ステップ 4	**address-family ipv6** 例： `Device(config-vrf)# address-family ipv6`	VRF アドレス ファミリ コンフィギュレーション モードを開始して、標準 IPv6 アドレス プレフィックスを伝送するセッションを設定します。

	コマンドまたはアクション	目的
ステップ 5	**exit-address-family** 例： `Device(config-vrf-af)# exit-address-family`	VRF アドレス ファミリ コンフィギュレーション モードを終了し、VRF コンフィギュレーション モードを開始します。
ステップ 6	**exit** 例： `Device(config-vrf)# exit`	VRF コンフィギュレーション モードを終了して、グローバル コンフィギュレーション モードを開始します。
ステップ 7	**parameter-map type inspect** *parameter-map-name* 例： `Device(config)# parameter-map type inspect ipv6-param-map`	ファイアウォールのグローバル検査タイプ パラメータ マップを、検査アクションに関連するしきい値、タイムアウト、その他のパラメータに接続できるようにし、パラメータ マップ タイプ検査コンフィギュレーション モードを開始します。
ステップ 8	**sessions maximum** セッション 例： `Device(config-profile)# sessions maximum 10000`	ゾーン ペア上に存在可能な最大許容セッション数を設定します。
ステップ 9	**exit** 例： `Device(config-profile)# exit`	パラメータ マップ タイプ検査コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードを開始します。
ステップ 10	**ipv6 unicast-routing** 例： `Device(config)# ipv6 unicast-routing`	IPv6 ユニキャスト データグラムの転送を有効にします。
ステップ 11	**ip port-map** *appl-name* **port** *port-num* **list** *list-name* 例： `Device(config)# ip port-map ftp port 8090 list ipv6-acl`	IPv6 アクセス コントロール リスト（ACL）を使用してポート/アプリケーション間マッピング（PAM）を確立します。
ステップ 12	**ipv6 access-list** *access-list-name* 例： `Device(config)# ipv6 access-list ipv6-acl`	IPv6 アクセスリストを定義し、IPv6 アクセス リスト コンフィギュレーション モードを開始します。
ステップ 13	**permit ipv6 any any** 例： `Device(config-ipv6-acl)# permit ipv6 any any`	IPv6 アクセス リストに許可条件を設定します。
ステップ 14	**exit** 例： `Device(config-ipv6-acl)# exit`	IPv6 アクセス リスト コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 15	**class-map type inspect match-all** *class-map-name* 例： `Device(config)# class-map type inspect match-all ipv6-class`	アプリケーション固有の検査タイプ クラス マップを作成し、QoS クラス マップ コンフィギュレーション モードを開始します。
ステップ 16	**match access-group name** *access-group-name* 例： `Device(config-cmap)# match access-group name ipv6-acl`	指定した ACL をベースにクラスマップに対して一致基準を設定します。
ステップ 17	**match protocol** *protocol-name* 例： `Device(config-cmap)# match protocol tcp`	指定されたプロトコルに基づき、クラス マップの一致基準を設定します。
ステップ 18	**exit** 例： `Device(config-cmap)# exit`	QoS クラス マップ コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードを開始します。
ステップ 19	**policy-map type inspect** *policy-map-name* 例： `Device(config)# policy-map type inspect ipv6-policy`	プロトコル固有の検査タイプ ポリシー マップを作成し、QoS ポリシーマップ コンフィギュレーション モードを開始します。
ステップ 20	**class type inspect** *class-map-name* 例： `Device(config-pmap)# class type inspect ipv6-class`	アクションの実行対象となるトラフィック クラスを指定し、QoS ポリシー マップ クラス コンフィギュレーション モードを開始します。
ステップ 21	**inspect** [*parameter-map-name*] 例： `Device(config-pmap-c)# inspect ipv6-param-map`	ステートフル パケット インスペクションをイネーブルにします。
ステップ 22	**end** 例： `Device(config-pmap-c)# end`	QoS ポリシーマップ クラス コンフィギュレーション モードを終了し、特権 EXEC モードを開始します。

ファイアウォール セッションのアグレッシブ エージングの設定

アグレッシブ エージング機能は、ボックス単位（ボックス単位とは、ファイアウォール セッション テーブル全体を意味します）、デフォルト VRF、および VRF 単位のファイアウォール セッションに設定できます。アグレッシブ エージング機能が動作するには、ファイアウォール セッションのアグレッシブ エージングおよびエージング アウト時間を設定する必要があります。

ファイアウォール セッションのアグレッシブ エージングを設定するには、次の作業を実行します。

ボックス単位のアグレッシブ エージングの設定

ボックス単位とは、ファイアウォールセッションテーブル全体という意味です。**parameter-map type inspect-global** コマンドに続くすべての設定がボックスに適用されます。

手順の概要

1. **enable**
2. **configure terminal**
3. 次のいずれかのコマンドを入力します。
   - **parameter-map type inspect-global**
   - **parameter-map type inspect global**
4. **per-box max-incomplete** *number* **aggressive-aging high** {*value* **low** *value* | **percent** *percent* **low percent** *percent*}
5. **per-box aggressive-aging high** {*value* **low** *value* | **percent** *percent* **low percent** *percent*}
6. **exit**
7. **parameter-map type inspect** *parameter-map-name*
8. **tcp synwait-time** *seconds* [**ageout-time** *seconds*]
9. **end**
10. **show policy-firewall stats global**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。

ステップ 3	次のいずれかのコマンドを入力します。
	• **parameter-map type inspect-global**
	• **parameter-map type inspect global**
	例：
	`Device(config)# parameter-map type inspect-global`
	`Device(config)# parameter-map type inspect global`
		接続しきい値およびタイムアウトのグローバル パラメータ マップを設定し、パラメータ マップ タイプ検査コンフィギュレーション モードを開始します。
		• リリースに基づいて、**parameter-map type inspect-global** コマンドと **parameter-map type inspect global** コマンドがサポートされます。これら両方のコマンドを一緒に設定することはできません。

	コマンドまたはアクション	目的
		• **parameter-map type inspect-global** コマンドを設定する場合は、手順4と手順5をスキップしてください。 （注） **parameter-map type inspect-global** コマンドを設定する場合は、**per-box** コンフィギュレーションがサポートされません。これは、デフォルトですべての **per-box** コンフィギュレーションがすべてのファイアウォールセッションに適用されるためです。
ステップ 4	**per-box max-incomplete** *number* **aggressive-aging high** {*value* **low** *value* | **percent** *percent* **low percent** *percent*} 例： `Device(config-profile)# per-box max-incomplete 2000 aggressive-aging high 1500 low 1200`	ファイアウォール セッション テーブル内のハーフオープンセッションの上限およびアグレッシブエージング レートを設定します。
ステップ 5	**per-box aggressive-aging high** {*value* **low** *value* | **percent** *percent* **low percent** *percent*} 例： `Device(config-profile)# per-box aggressive-aging high 1700 low 1300`	総セッションのアグレッシブ エージング制限を設定します。
ステップ 6	**exit** 例： `Device(config-profile)# exit`	パラメータマップタイプ検査コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードを開始します。
ステップ 7	**parameter-map type inspect** *parameter-map-name* 例： `Device(config)# parameter-map type inspect pmap1`	接続しきい値、タイムアウト、およびその他の **inspect** アクションに関連するパラメータの検査タイプパラメータマップを設定し、パラメータマップタイプ検査コンフィギュレーション モードを開始します。
ステップ 8	**tcp synwait-time** *seconds* [**ageout-time** *seconds*] 例： `Device(config-profile)# tcp synwait-time 30 ageout-time 10`	セッションをドロップする前に、TCP セッションが確立状態になるのを待機する時間を指定します。 • アグレッシブ エージングがイネーブルになった後、最も古いTCP接続のSYN待機タイマーが、デフォルトから設定済みエージアウト時間にリセットされます。この例では、接続がタイムアウトするまで30秒待機する代わりに、最も古いTCP接続のタイムアウトが10秒に設定されます。接続が低ウォーターマークを下回る

	コマンドまたはアクション	目的
		と、アグレッシブ エージングはディセーブルになります。
ステップ 9	**end** 例： `Device(config-profile)# end`	パラメータ マップ タイプ検査コンフィギュレーション モードを終了し、特権 EXEC モードを開始します。
ステップ 10	**show policy-firewall stats global** 例： `Device# show policy-firewall stats global`	グローバル ファイアウォール統計情報を表示します。

デフォルト VRF のアグレッシブ エージングの設定

max-incomplete aggressive-aging `command, it applies to the default VRF.` を設定する場合

手順の概要

1. **enable**
2. **configure terminal**
3. 次のいずれかのコマンドを入力します：
   - **parameter-map type inspect-global**
   - **parameter-map type inspect global**
4. **max-incomplete** *number* **aggressive-aging high** {*value* **low** *value* | **percent** *percent* **low percent** *percent*}
5. **session total** *number* [**aggressive-aging high** {*value* **low** *value* | **percent** *percent* **low percent** *percent*}]
6. **exit**
7. **parameter-map type inspect** *parameter-map-name*
8. **tcp synwait-time** *seconds* [**ageout-time** *seconds*]
9. **end**
10. **show policy-firewall stats vrf global**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例：	グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
	`Device# configure terminal`	

ステップ 3	次のいずれかのコマンドを入力します：
	• **parameter-map type inspect-global**
	• **parameter-map type inspect global**
	例：
	`Device(config)# parameter-map type inspect-global`
	`Device(config)# parameter-map type inspect global`
		接続しきい値およびタイムアウトのグローバル パラメータ マップを設定し、パラメータ マップ タイプ検査コンフィギュレーション モードを開始します。
		• リリースに基づいて、**parameter-map type inspect-global** コマンドと **parameter-map type inspect global** コマンドがサポートされます。これら両方のコマンドを一緒に設定することはできません。
		• **parameter-map type inspect-global** コマンドを設定する場合は、手順5をスキップしてください。
		（注） **parameter-map type inspect-global** コマンドを設定する場合は **per-box** コンフィギュレーションがサポートされません。これは、デフォルトですべての **per-box** コンフィギュレーションがすべてのファイアウォールセッションに適用されるためです。

ステップ 4	**max-incomplete** *number* **aggressive-aging high** {*value* **low** *value* | **percent** *percent* **low percent** *percent*} 例： `Device(config-profile)# max-incomplete 3455 aggressive-aging high 2345 low 2255`	ハーフオープン ファイアウォール セッションの上限およびアグレッシブ エージング制限を設定します。
ステップ 5	**session total** *number* [**aggressive-aging high** {*value* **low** *value* | **percent** *percent* **low percent** *percent*}] 例： `Device(config-profile)# session total 1000 aggressive-aging high percent 80 low percent 60`	総ファイアウォール セッションの合計制限およびアグレッシブ エージング制限を設定します。
ステップ 6	**exit** 例： `Device(config-profile)# exit`	パラメータ マップ タイプ検査コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードを開始します。
ステップ 7	**parameter-map type inspect** *parameter-map-name* 例： `Device(config)# parameter-map type inspect pmap1`	接続しきい値、タイムアウト、およびその他の **inspect** アクションに関連するパラメータの検査タイプパラメータマップを設定し、パラメータマップ

	コマンドまたはアクション	目的
		タイプ検査コンフィギュレーション モードを開始します。
ステップ 8	**tcp synwait-time** *seconds* [**ageout-time** *seconds*] 例： `Device(config-profile)# tcp synwait-time 30 ageout-time 10`	セッションをドロップする前に、TCP セッションが確立状態になるのを待機する時間を指定します。 • アグレッシブ エージングがイネーブルになった後、最も古い TCP 接続の SYN 待機タイマーが、デフォルトから設定済みエージアウト時間にリセットされます。この例では、接続がタイムアウトするまで 30 秒待機する代わりに、最も古い TCP 接続のタイムアウトが 10 秒に設定されます。接続が低ウォーターマークを下回ると、アグレッシブ エージングはディセーブルになります。
ステップ 9	**end** 例： `Device(config-profile)# end`	パラメータ マップ タイプ検査コンフィギュレーション モードを終了し、特権 EXEC モードを開始します。
ステップ 10	**show policy-firewall stats vrf global** 例： `Device# show policy-firewall stats vrf global`	グローバル VRF ファイアウォール ポリシー統計を表示します。

VRF 単位のアグレッシブ エージングの設定

手順の概要

1. **enable**
2. **configure terminal**
3. **ip vrf** *vrf-name*
4. **rd** *route-distinguisher*
5. **route-target export** *route-target-ext-community*
6. **route-target import** *route-target-ext-community*
7. **exit**
8. **parameter-map type inspect-vrf** *vrf-pmap-name*
9. **max-incomplete** *number* **aggressive-aging high** {*value* **low** *value* | **percent** *percent* **low percent** *percent*}
10. **session total** *number* [**aggressive-aging** {**high** *value* **low** *value* | **percent** *percent* **low percent** *percent*}]
11. **alert on**
12. **exit**
13. 次のいずれかのコマンドを入力します。

- **parameter-map type inspect-global**
- **parameter-map type inspect global**

14. **vrf** *vrf-name* **inspect** *vrf-pmap-name*
15. **exit**
16. **parameter-map type inspect** *parameter-map-name*
17. **tcp idle-time** *seconds* [**ageout-time** *seconds*]
18. **tcp synwait-time** *seconds* [**ageout-time** *seconds*]
19. **exit**
20. **policy-map type inspect** *policy-map-name*
21. **class type inspect match-any** *class-map-name*
22. **inspect** *parameter-map-name*
23. **end**
24. **show policy-firewall stats vrf** *vrf-pmap-name*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ip vrf** *vrf-name* 例： `Device(config)# ip vrf ddos-vrf1`	VRF インスタンスを定義し、VRF コンフィギュレーション モードを開始します。
ステップ 4	**rd** *route-distinguisher* 例： `Device(config-vrf)# rd 100:2`	VRF インスタンスのルート識別子（RD）を指定します。
ステップ 5	**route-target export** *route-target-ext-community* 例： `Device(config-vrf)# route-target export 100:2`	ルートターゲット拡張コミュニティを作成し、ルーティング情報をターゲット VPN 拡張コミュニティにエクスポートします。
ステップ 6	**route-target import** *route-target-ext-community* 例： `Device(config-vrf)# route-target import 100:2`	ルートターゲット拡張コミュニティを作成し、ターゲット VPN 拡張コミュニティからルーティング情報をインポートします。
ステップ 7	**exit** 例： `Device(config-vrf)# exit`	VRF コンフィギュレーション モードを終了して、グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 8	**parameter-map type inspect-vrf** *vrf-pmap-name* 例： `Device(config)# parameter-map type inspect-vrf vrf1-pmap`	VRF 検査タイプ パラメータ マップを設定し、パラメータ マップ タイプ検査コンフィギュレーション モードを開始します。
ステップ 9	**max-incomplete** *number* **aggressive-aging high** {*value* **low** *value* | **percent** *percent* **low percent** *percent*} 例： `Device(config-profile)# max-incomplete 2000 aggressive-aging high 1500 low 1200`	ハーフ オープン セッションの上限およびアグレッシブ エージング制限を設定します。
ステップ 10	**session total** *number* [**aggressive-aging** {**high** *value* **low** *value* | **percent** *percent* **low percent** *percent*}] 例： `Device(config-profile)# session total 1000 aggressive-aging high percent 80 low percent 60`	総セッション制限および総セッションに関するアグレッシブ エージング制限を設定します。 • 総セッション制限は、絶対値またはパーセンテージとして設定できます。
ステップ 11	**alert on** 例： `Device(config-profile)# alert on`	ステートフル パケット インスペクションのアラート メッセージのコンソール表示をイネーブルにします。
ステップ 12	**exit** 例： `Device(config-profile)# exit`	パラメータ マップ タイプ検査コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードを開始します。

ステップ 13	次のいずれかのコマンドを入力します。
	• **parameter-map type inspect-global**
	• **parameter-map type inspect global**
	例：
	`Device(config)# parameter-map type inspect-global`
	`Device(config)# parameter-map type inspect global`
		グローバル パラメータ マップを設定し、パラメータ マップ タイプ検査コンフィギュレーション モードを開始します。
		• リリースに基づいて、**parameter-map type inspect-global** コマンドと **parameter-map type inspect global** コマンドがサポートされます。これら両方のコマンドを一緒に設定することはできません。
		• **parameter-map type inspect-global** コマンドを設定する場合は、手順 14 をスキップしてください。

	コマンドまたはアクション	目的
		（注） **parameter-map type inspect-global** コマンドを設定する場合は、**per-box** コンフィギュレーションがサポートされません。これは、デフォルトですべての **per-box** コンフィギュレーションがすべてのファイアウォールセッションに適用されるためです。
ステップ 14	**vrf** *vrf-name* **inspect** *vrf-pmap-name* 例： `Device(config-profile)# vrf vrf1 inspect vrf1-pmap`	パラメータ マップに VRF をバインドします。
ステップ 15	**exit** 例： `Device(config-profile)# exit`	パラメータマップタイプ検査コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードを開始します。
ステップ 16	**parameter-map type inspect** *parameter-map-name* 例： `Device(config)# parameter-map type inspect pmap1`	接続しきい値、タイムアウト、およびその他の **inspect** アクションに関連するパラメータの検査タイプパラメータマップを設定し、パラメータマップタイプ検査コンフィギュレーション モードを開始します。
ステップ 17	**tcp idle-time** *seconds* [**ageout-time** *seconds*] 例： `Device(config-profile)# tcp idle-time 3000 ageout-time 100`	アイドル状態の TCP セッションのタイムアウト、および TCP セッションのアグレッシブ エージングアウト時間を設定します。
ステップ 18	**tcp synwait-time** *seconds* [**ageout-time** *seconds*] 例： `Device(config-profile)# tcp synwait-time 30 ageout-time 10`	セッションをドロップする前に、TCP セッションが確立状態になるのを待機する時間を指定します。 • アグレッシブ エージングがイネーブルになると、最も古い TCP 接続の SYN 待機タイマーが、デフォルトから設定済みエージアウト時間にリセットされます。この例では、接続がタイムアウトするまで 30 秒待機する代わりに、最も古い TCP 接続のタイムアウトが 10 秒に設定されます。接続が低ウォーターマークを下回ると、アグレッシブ エージングはディセーブルになります。
ステップ 19	**exit** 例： `Device(config-profile)# exit`	パラメータマップタイプ検査コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 20	**policy-map type inspect** *policy-map-name* 例： `Device(config)# policy-map type inspect ddos-fw`	プロトコル固有の検査タイプ ポリシー マップを作成し、QoS ポリシーマップ コンフィギュレーション モードを開始します。
ステップ 21	**class type inspect match-any** *class-map-name* 例： `Device(config-pmap)# class type inspect match-any ddos-class`	アクションの実行対象となるトラフィック（クラス）を指定し、QoS ポリシー マップ クラス コンフィギュレーション モードを開始します。
ステップ 22	**inspect** *parameter-map-name* 例： `Device(config-pmap-c)# inspect pmap1`	パラメータ マップのステートフル パケット インスペクションをディセーブルにします。
ステップ 23	**end** 例： `Device(config-pmap-c)# end`	QoS ポリシーマップ クラス コンフィギュレーション モードを終了し、特権 EXEC モードを開始します。
ステップ 24	**show policy-firewall stats vrf** *vrf-pmap-name* 例： `Device# show policy-firewall stats vrf vrf1-pmap`	VRF レベル ポリシー ファイアウォール統計情報を表示します。

例

次に、**show policy-firewall stats vrf vrf1-pmap** コマンドの出力例を示します。

```
Device# show policy-firewall stats vrf vrf1-pmap

VRF: vrf1, Parameter-Map: vrf1-pmap
  Interface reference count: 2
       Total Session Count(estab + half-open): 80, Exceed: 0
       Total Session Aggressive Aging Period Off, Event Count: 0

                Half Open
       Protocol Session Cnt     Exceed
       -------- -----------     ------
       All      0               0
       UDP      0               0
       ICMP     0               0
       TCP      0               0

       TCP Syn Flood Half Open Count: 0, Exceed: 116
       Half Open Aggressive Aging Period Off, Event Count: 0
```

ファイアウォール セッションのエージング アウトの設定

ICMP、TCP、またはUDPファイアウォールセッションのエージングアウトを設定できます。

手順の概要

1. **enable**
2. **configure terminal**
3. 次のいずれかのコマンドを入力します。
   - **parameter-map type inspect-global**
   - **parameter-map type inspect global**
4. **vrf** *vrf-name* **inspect** *vrf-pmap-name*
5. **exit**
6. **parameter-map type inspect** *parameter-map-name*
7. **tcp idle-time** *seconds* [**ageout-time** *seconds*]
8. **tcp synwait-time** *seconds* [**ageout-time** *seconds*]
9. **exit**
10. **policy-map type inspect** *policy-map-name*
11. **class type inspect match-any** *class-map-name*
12. **inspect** *parameter-map-name*
13. **end**
14. **show policy-firewall stats vrf** *vrf-pmap-name*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。

ステップ 3	次のいずれかのコマンドを入力します。
	• **parameter-map type inspect-global**
	• **parameter-map type inspect global**
	例：
	`Device(config)# parameter-map type inspect-global`
	`Device(config)# parameter-map type inspectglobal`
		グローバル パラメータ マップを設定し、パラメータ マップ タイプ検査コンフィギュレーション モードを開始します。
		• リリースに基づいて、**parameter-map type inspect-global** コマンドと **parameter-map type inspect global** コマンドがサポートされます。これら両方のコマンドを一緒に設定することはできません。
		• **parameter-map type inspect-global** コマンドを設定する場合は、手順4をスキップしてください。

	コマンドまたはアクション	目的
		（注） **parameter-map type inspect-global** コマンドを設定する場合は、**per-box** コンフィギュレーションがサポートされません。これは、デフォルトですべての **per-box** コンフィギュレーションがすべてのファイアウォールセッションに適用されるためです。
ステップ 4	**vrf** *vrf-name* **inspect** *vrf-pmap-name* 例： `Device(config-profile)# vrf vrf1 inspect vrf1-pmap`	パラメータ マップに VRF をバインドします。
ステップ 5	**exit** 例： `Device(config-profile)# exit`	パラメータマップ タイプ検査コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードを開始します。
ステップ 6	**parameter-map type inspect** *parameter-map-name* 例： `Device(config)# parameter-map type inspect pmap1`	接続しきい値、タイムアウト、およびその他の **inspect** アクションに関連するパラメータの検査タイプパラメータマップを設定し、パラメータマップ タイプ検査コンフィギュレーション モードを開始します。
ステップ 7	**tcp idle-time** *seconds* [**ageout-time** *seconds*] 例： `Device(config-profile)# tcp idle-time 3000 ageout-time 100`	アイドル状態の TCP セッションのタイムアウト、および TCP セッションのアグレッシブ エージングアウト時間を設定します。 • また、**tcp finwait-time** コマンドを設定すると、終了（FIN）交換がファイアウォールで検出された後に TCP セッションを管理する時間の長さを指定できます。または **tcp synwait-time** コマンドを設定すると、セッションをドロップする前に TCP セッションが確立状態になるのを待機する時間を指定できます。
ステップ 8	**tcp synwait-time** *seconds* [**ageout-time** *seconds*] 例： `Device(config-profile)# tcp synwait-time 30 ageout-time 10`	セッションをドロップする前に、TCP セッションが確立状態になるのを待機する時間を指定します。 • アグレッシブ エージングがイネーブルになると、最も古い TCP 接続の SYN 待機タイマーが、デフォルトから設定済みエージアウト時間にリセットされます。この例では、接続がタイムアウトするまで 30 秒待機する代わりに、最も古い TCP 接続のタイムアウトが 10 秒に設定されます。接続が低ウォーターマークを下回る

	コマンドまたはアクション	目的
		と、アグレッシブ エージングがイネーブルになります。
ステップ 9	**exit** 例： `Device(config-profile)# exit`	パラメータ マップ タイプ検査コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードを開始します。
ステップ 10	**policy-map type inspect** *policy-map-name* 例： `Device(config)# policy-map type inspect ddos-fw`	プロトコル固有の検査タイプ ポリシー マップを作成し、QoS ポリシーマップ コンフィギュレーション モードを開始します。
ステップ 11	**class type inspect match-any** *class-map-name* 例： `Device(config-pmap)# class type inspect match-any ddos-class`	アクションの実行対象となるトラフィック クラスを指定し、QoS ポリシー マップ クラス コンフィギュレーション モードを開始します。
ステップ 12	**inspect** *parameter-map-name* 例： `Device(config-pmap-c)# inspect pmap1`	パラメータ マップのステートフル パケット インスペクションをディセーブルにします。
ステップ 13	**end** 例： `Device(config-pmap-c)# end`	QoS ポリシーマップ クラス コンフィギュレーション モードを終了し、特権 EXEC モードを開始します。
ステップ 14	**show policy-firewall stats vrf** *vrf-pmap-name* 例： `Device# show policy-firewall stats vrf vrf1-pmap`	VRF レベル ポリシー ファイアウォール統計情報を表示します。

例

次に、**show policy-firewall stats vrf vrf1-pmap** コマンドの出力例を示します。

```
Device# show policy-firewall stats vrf vrf1-pmap

 VRF: vrf1, Parameter-Map: vrf1-pmap
  Interface reference count: 2
       Total Session Count(estab + half-open): 270, Exceed: 0
       Total Session Aggressive Aging Period Off, Event Count: 0

                Half Open
       Protocol Session Cnt     Exceed
       -------- -----------     ------
       All      0               0
       UDP      0               0
       ICMP     0               0
       TCP      0               0
```

```
TCP Syn Flood Half Open Count: 0, Exceed: 12
Half Open Aggressive Aging Period Off, Event Count: 0
```

ファイアウォール イベント レート モニタリングの設定

手順の概要

1. **enable**
2. **configure terminal**
3. **parameter-map type inspect-zone** *zone-pmap-name*
4. **alert on**
5. **threat-detection basic-threat**
6. **threat-detection rate fw-drop average-time-frame** *seconds* **average-threshold** *packets-per-second* **burst-threshold** *packets-per-second*
7. **threat-detection rate inspect-drop average-time-frame** *seconds* **average-threshold** *packets-per-second* **burst-threshold** *packets-per-second*
8. **threat-detection rate syn-attack average-time-frame** *seconds* **average-threshold** *packets-per-second* **burst-threshold** *packets-per-second*
9. **exit**
10. **zone security** *security-zone-name*
11. **protection** *parameter-map-name*
12. **exit**
13. **zone-pair security** *zone-pair-name* **source** *source-zone* **destination** *destination-zone*
14. **end**
15. **show policy-firewall stats zone**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**parameter-map type inspect-zone** *zone-pmap-name* 例： `Device(config)# parameter-map type inspect-zone zone-pmap1`	ゾーン検査パラメータ マップを設定し、パラメータ マップ タイプ検査コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 4	**alert on** 例： `Device(config-profile)# alert on`	ゾーンに関するステートフル パケット インスペクションのアラート メッセージのコンソール表示を有効にします。 • **log** コマンドを使用すると、アラートのロギングを Syslog または高速ロガー（HSL）のいずれかに設定できます。
ステップ 5	**threat-detection basic-threat** 例： `Device(config-profile)# threat-detection basic-threat`	ゾーンの基本脅威検出を設定します。
ステップ 6	**threat-detection rate fw-drop average-time-frame** *seconds* **average-threshold** *packets-per-second* **burst-threshold** *packets-per-second* 例： `Device(config-profile)# threat-detection rate fw-drop average-time-frame 600 average-threshold 100 burst-threshold 100`	ファイアウォール ドロップ イベントの脅威検出レートを設定します。 • **threat-detection rate** コマンドを設定する前に、**threat-detection basic-threat** コマンドを設定する必要があります。
ステップ 7	**threat-detection rate inspect-drop average-time-frame** *seconds* **average-threshold** *packets-per-second* **burst-threshold** *packets-per-second* 例： `Device(config-profile)# threat-detection rate inspect-drop average-time-frame 600 average-threshold 100 burst-threshold 100`	ファイアウォール インスペクション ベースのドロップ イベントに関する脅威検出レートを設定します。
ステップ 8	**threat-detection rate syn-attack average-time-frame** *seconds* **average-threshold** *packets-per-second* **burst-threshold** *packets-per-second* 例： `Device(config-profile)# threat-detection rate syn-attack average-time-frame 600 average-threshold 100 burst-threshold 100`	TCP SYN 攻撃イベントの脅威検出レートを設定します。
ステップ 9	**exit** 例： `Device(config-profile)# exit`	パラメータ マップ タイプ検査コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードを開始します。
ステップ 10	**zone security** *security-zone-name* 例： `Device(config)# zone security public`	セキュリティ ゾーンを作成し、セキュリティ ゾーン コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 11	**protection** *parameter-map-name* 例： `Device(config-sec-zone)# protection zone-pmap1`	ゾーン検査パラメータ マップをゾーンにアタッチし、ゾーン検査パラメータ マップで設定されている機能をゾーンに適用します。
ステップ 12	**exit** 例： `Device(config-sec-zone)# exit`	セキュリティ ゾーン コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードを開始します。
ステップ 13	**zone-pair security** *zone-pair-name* **source** *source-zone* **destination** *destination-zone* 例： `Device(config)# zone-pair security private2public source private destination public`	ゾーン ペアを作成し、セキュリティ ゾーンペア コンフィギュレーション モードを開始します。
ステップ 14	**end** 例： `Device(config-sec-zone-pair)# end`	セキュリティ ゾーン ペア コンフィギュレーション モードを終了し、特権EXECモードを開始します。
ステップ 15	**show policy-firewall stats zone** 例： `Device# show policy-firewall stats zone`	ゾーン レベルでのポリシー ファイアウォール統計情報を表示します。

ボックス単位のハーフオープン セッション制限の設定

ボックス単位とは、ファイアウォールセッションテーブル全体という意味です。**parameter-map type inspect-global** コマンドに続くすべての設定がボックスに適用されます。

手順の概要

1. **enable**
2. **configure terminal**
3. 次のいずれかのコマンドを入力します。
   - **parameter-map type inspect-global**
   - **parameter-map type inspect global**
4. **alert on**
5. **per-box max-incomplete** *number*
6. **session total** *number*
7. **end**
8. **show policy-firewall stats global**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。

ステップ 3	次のいずれかのコマンドを入力します。
	• **parameter-map type inspect-global**
	• **parameter-map type inspect global**
	例：
	`Device(config)# parameter-map type inspect-global`
	`Device(config)# parameter-map type inspect global`
		接続しきい値およびタイムアウトのグローバル パラメータ マップを設定し、パラメータ マップ タイプ検査コンフィギュレーション モードを開始します。
		• リリースに基づいて、**parameter-map type inspect-global** コマンドと **parameter-map type inspect global** コマンドがサポートされます。これら両方のコマンドを一緒に設定することはできません。
		• **parameter-map type inspect-global** コマンドを設定する場合は、手順 5 および手順 6 をスキップしてください。
		（注） **parameter-map type inspect-global** コマンドを設定する場合は、**per-box** コンフィギュレーションがサポートされません。これは、デフォルトですべての **per-box** コンフィギュレーションがすべてのファイアウォールセッションに適用されるためです。

ステップ 4	**alert on** 例： `Device(config-profile)# alert on`	ステートフル パケット インスペクションのアラート メッセージのコンソール表示をイネーブルにします。
ステップ 5	**per-box max-incomplete** *number* 例： `Device(config-profile)# per-box max-incomplete 12345`	ファイアウォール セッション テーブルのハーフオープン接続の最大数を設定します。
ステップ 6	**session total** *number* 例： `Device(config-profile)# session total 34500`	ファイアウォール セッション テーブルの合計セッション制限を設定します。

	コマンドまたはアクション	目的
ステップ 7	**end** 例： `Device(config-profile)# end`	パラメータ マップ タイプ検査コンフィギュレーション モードを終了し、特権 EXEC モードを開始します。
ステップ 8	**show policy-firewall stats global** 例： `Device# show policy-firewall stats global`	グローバル ファイアウォール統計情報を表示します。

VRF検査パラメータ マップ用のハーフオープンセッション制限の設定

手順の概要

1. **enable**
2. **configure terminal**
3. **parameter-map type inspect-vrf** *vrf-name*
4. **alert on**
5. **max-incomplete** *number*
6. **session total** *number*
7. **exit**
8. 次のいずれかのコマンドを入力します。
   - **parameter-map type inspect-global**
   - **parameter-map type inspect global**
9. **alert on**
10. **vrf** *vrf-name* **inspect** *vrf-pmap-name*
11. **end**
12. **show policy-firewall stats vrf** *vrf-pmap-name*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 3	**parameter-map type inspect-vrf** *vrf-name* 例： `Device(config)# parameter-map type inspect-vrf vrf1-pmap`	VRF 検査パラメータ マップを設定し、パラメータ マップ タイプ検査コンフィギュレーション モードを開始します。
ステップ 4	**alert on** 例： `Device(config-profile)# alert on`	ステートフル パケット インスペクションのアラート メッセージのコンソール表示をイネーブルにします。
ステップ 5	**max-incomplete** *number* 例： `Device(config-profile)# max-incomplete 2000`	VRF ごとのハーフ オープン接続の最大数を設定します。
ステップ 6	**session total** *number* 例： `Device(config-profile)# session total 34500`	VRF の総セッション制限を設定します。
ステップ 7	**exit** 例： `Device(config-profile)# exit`	パラメータマップ タイプ検査コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードを開始します。

ステップ 8	次のいずれかのコマンドを入力します。
	• **parameter-map type inspect-global**
	• **parameter-map type inspect global**
	例：
	`Device(config)# parameter-map type inspect-global`
	`Device(config)# parameter-map type inspect global`
		接続しきい値およびタイムアウトのグローバル パラメータ マップを設定し、パラメータ マップ タイプ検査コンフィギュレーション モードを開始します。
		• リリースに基づいて、**parameter-map type inspect-global** コマンドまたは **parameter-map type inspect global** コマンドのいずれかを使用できます。これら両方のコマンドを一緒に設定することはできません。
		• **parameter-map type inspect-global** コマンドを設定する場合は、手順 10 をスキップしてください。
		（注） **parameter-map type inspect-global** コマンドを設定する場合は **per-box** コンフィギュレーションがサポートされません。これは、デフォルトですべての **per-box** コンフィギュレーションがすべてのファイアウォールセッションに適用されるためです。

	コマンドまたはアクション	目的
ステップ 9	**alert on** 例： `Device(config-profile)# alert on`	ステートフル パケット インスペクションのアラート メッセージのコンソール表示をイネーブルにします。
ステップ 10	**vrf** *vrf-name* **inspect** *vrf-pmap-name* 例： `Device(config-profile)# vrf vrf1 inspect vrf1-pmap`	グローバル パラメータ マップに VRF をバインドします。
ステップ 11	**end** 例： `Device(config-profile)# end`	パラメータ マップ タイプ検査コンフィギュレーション モードを終了し、特権 EXEC モードを開始します。
ステップ 12	**show policy-firewall stats vrf** *vrf-pmap-name* 例： `Device# show policy-firewall stats vrf vrf1-pmap`	VRF レベル ポリシー ファイアウォール統計情報を表示します。

グローバル TCP SYN フラッド制限の設定

手順の概要

1. **enable**
2. **configure terminal**
3. 次のいずれかのコマンドを入力します。
   - **parameter-map type inspect-global**
   - **parameter-map type inspect global**
4. **alert on**
5. **per-box tcp syn-flood limit** *number*
6. **end**
7. **show policy-firewall stats vrf global**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的

ステップ 3	次のいずれかのコマンドを入力します。
	• **parameter-map type inspect-global**
	• **parameter-map type inspect global**
	例：
	`Device(config)# parameter-map type inspect-global`
	`Device(config)# parameter-map type inspect global`
		グローバル パラメータ マップを設定し、パラメータ マップ タイプ検査コンフィギュレーション モードを開始します。
		• リリースに基づいて、**parameter-map type inspect-global** コマンドまたは **parameter-map type inspect global** コマンドのいずれかを設定できます。これら両方のコマンドを一緒に設定することはできません。
		• **parameter-map type inspect-global** コマンドを設定する場合は、手順 5 をスキップしてください。
		（注） **parameter-map type inspect-global** コマンドを設定する場合は、**per-box** コンフィギュレーションがサポートされません。これは、デフォルトですべての **per-box** コンフィギュレーションがすべてのファイアウォールセッションに適用されるためです。

ステップ 4	**alert on** 例： `Device(config-profile)# alert on`	ステートフル パケット インスペクションのアラート メッセージのコンソール表示をイネーブルにします。
ステップ 5	**per-box tcp syn-flood limit** *number* 例： `Device(config-profile)# per-box tcp syn-flood limit 500`	新しい SYN パケットの SYN Cookie 処理をトリガーする TCP ハーフ オープン セッションの数を制限します。
ステップ 6	**end** 例： `Device(config-profile)# end`	パラメータ マップ タイプ検査コンフィギュレーション モードを終了し、特権 EXEC モードを開始します。
ステップ 7	**show policy-firewall stats vrf global** 例： `Device# show policy-firewall stats vrf global`	（任意）グローバル VRF ファイアウォール ポリシーのステータスを表示します。 • 存在する TCP ハーフ オープン セッションの数もまたコマンド出力に表示されます。

例

次に、**show policy-firewall stats vrf global** コマンドの出力例を示します。

```
Device# show policy-firewall stats vrf global

Global table statistics
       total_session_cnt: 0
       exceed_cnt:        0
       tcp_half_open_cnt: 0
       syn_exceed_cnt:    0
```

ファイアウォール リソース管理の設定

（注） グローバル パラメータ マップは、ルータ レベルではなく、グローバル ルーティング ドメインで有効になります。

手順の概要

1. **enable**
2. **configure terminal**
3. **parameter-map type inspect-vrf** *vrf-pmap-name*
4. **session total** *number*
5. **tcp syn-flood limit** *number*
6. **exit**
7. **parameter-map type inspect-global**
8. **vrf** *vrf-name* **inspect** *parameter-map-name*
9. **exit**
10. **parameter-map type inspect-vrf vrf-default**
11. **session total** *number*
12. **tcp syn-flood limit** *number*
13. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**parameter-map type inspect-vrf** *vrf-pmap-name* 例： `Device(config)# parameter-map type inspect-vrf vrf1-pmap`	VRF 検査タイプ パラメータ マップを設定し、パラメータ マップ タイプ検査コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 4	**session total** *number* 例： `Device(config-profile)# session total 1000`	セッションの総数を設定します。
ステップ 5	**tcp syn-flood limit** *number* 例： `Device(config-profile)# tcp syn-flood limit 2000`	新しい SYN パケットの同期（SYN）Cookie 処理をトリガーする TCP ハーフ オープン セッションの数を制限します。
ステップ 6	**exit** 例： `Device(config-profile)# exit`	パラメータ マップ タイプ検査コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードを開始します。
ステップ 7	**parameter-map type inspect-global** 例： `Device(config)# parameter-map type inspect-global`	グローバル パラメータ マップを設定し、パラメータ マップ タイプ検査コンフィギュレーション モードを開始します。
ステップ 8	**vrf** *vrf-name* **inspect** *parameter-map-name* 例： `Device(config-profile)# vrf vrf1 inspect vrf1-pmap`	VRF をパラメータ マップにバインドします。
ステップ 9	**exit** 例： `Device(config-profile)# exit`	パラメータ マップ タイプ検査コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードを開始します。
ステップ 10	**parameter-map type inspect-vrf vrf-default** 例： `Device(config)# parameter-map type inspect-vrf vrf-default`	デフォルトの VRF 検査タイプ パラメータ マップを設定します。
ステップ 11	**session total** *number* 例： `Device(config-profile)# session total 6000`	セッションの総数を設定します。 • VRF 検査タイプパラメータマップ用およびグローバルパラメータマップ用に **session total** コマンドを設定できます。VRF 検査タイプパラメータマップ用に **session total** コマンドを設定する場合、VRF 検査タイプパラメータマップにセッションが関連付けられます。グローバルパラメータマップ用に **session total** コマンドを設定する場合、このコマンドはグローバル ルーティング ドメインに適用されます。

	コマンドまたはアクション	目的
ステップ 12	**tcp syn-flood limit** *number* 例： `Device(config-profile)# tcp syn-flood limit 7000`	新しいSYNパケットのSYN Cookie処理をトリガーするTCPハーフ オープン セッションの数を制限します。
ステップ 13	**end** 例： `Device(config-profile)# end`	パラメータ マップ タイプ検査コンフィギュレーション モードを終了し、特権 EXEC モードを開始します。

IPv6 ファイアウォールでの分散型サービス妨害攻撃の防止およびリソース管理のサポートの設定例

例：IPv6 ファイアウォールの設定

```
Device# configure terminal
Device(config)# vrf-definition VRF1
Device(config-vrf)# address-family ipv6
Device(config-vrf-af)# exit-address-family
Device(config-vrf)# exit
Device(config)# parameter-map type inspect ipv6-param-map
Device(config-profile)# sessions maximum 10000
Device(config-profile)# exit
Device(config)# ipv6 unicast-routing
Device(config)# ip port-map ftp port 8090 list ipv6-acl
Device(config)# ipv6 access-list ipv6-acl
Device(config-ipv6-acl)# permit ipv6 any any
Device(config-ipv6-acl)# exit
Device(config)# class-map type inspect match-all ipv6-class
Device(config-cmap)# match access-group name ipv6-acl
Device(config-cmap)# match protocol tcp
Device(config-cmap)# exit
Device(config)# policy-map type inspect ipv6-policy
Device(config-pmap)# class type inspect ipv6-class
Device(config-pmap-c)# inspect ipv6-param-map
Device(config-pmap-c)# end
```

例：ファイアウォール セッションのアグレッシブ エージングの設定

例：ボックス単位のアグレッシブ エージングの設定

```
Device# configure terminal
Device(config)# parameter-map type inspect global
Device(config-profile)# per-box max-incomplete 2000 aggressive-aging 1500 low 1200
Device(config-profile)# per-box aggressive-aging high 1700 low 1300
Device(config-profile)# exit
```

```
Device(config)# parameter-map type inspect pmap1
Device(config-profile)# tcp synwait-time 30 ageout-time 10
Device(config-profile)# end
```

例：デフォルト VRF のアグレッシブ エージングの設定

```
Device# configure terminal
Device(config)# parameter-map type inspect global
Device(config-profile)# max-incomplete 2000 aggressive-aging high 1500 low 1200
Device(config-profile)# session total 1000 aggressive-aging high percent 80 low percent
 60
Device(config-profile)# exit
Device(config)# parameter-map type inspect pmap1
Device(config-profile)# tcp synwait-time 30 ageout-time 10
Device(config-profile)# end
```

例：VRF 単位のアグレッシブ エージングの設定

```
Device# configure terminal
Device(config)# ip vrf ddos-vrf1
Device(config-vrf)# rd 100:2
Device(config-vrf)# route-target export 100:2
Device(config-vrf)# route-target import 100:2
Device(config-vrf)# exit
Device(config)# parameter-map type inspect-vrf vrf1-pmap
Device(config-profile)# max-incomplete 3455 aggressive-aging high 2345 low 2255
Device(config-profile)# session total 1000 aggressive-aging high percent 80 low percent
 60
Device(config-profile)# alert on
Device(config-profile)# exit
Device(config)# parameter-map type inspect global
Device(config-profile)# vrf vrf1 inspect vrf1-pmap
Device(config-profile)# exit
Device(config)# parameter-map type inspect pmap1
Device(config-profile)# tcp idle-time 3000 ageout-time 100
Device(config-profile)# tcp synwait-time 30 ageout-time 10
Device(config-profile)# exit
Device(config)# policy-map type inspect ddos-fw
Device(config-pmap)# class type inspect match-any ddos-class
Device(config-pmap-c)# inspect pmap1
Device(config-profile)# end
```

例：ファイアウォール セッションのエージング アウトの設定

```
Device# configure terminal
Device(config-profile)# exit
Device(config)# parameter-map type inspect global
Device(config-profile)# vrf vrf1 inspect vrf1-pmap
Device(config-profile)# exit
Device(config)# parameter-map type inspect pmap1
Device(config-profile)# tcp idle-time 3000 ageout-time 100
Device(config-profile)# tcp synwait-time 30 ageout-time 10
Device(config-profile)# exit
Device(config)# policy-map type inspect ddos-fw
Device(config-profile)# class type inspect match-any ddos-class
```

```
Device(config-profile)# inspect pmap1
Device(config-profile)# end
```

例：ファイアウォール イベント レート モニタリングの設定

```
Device> enable
Device# configure terminal
Device(config)# parameter-map type inspect zone zone-pmap1
Device(config-profile)# alert on
Device(config-profile)# threat-detection basic-threat
Device(config-profile)# threat-detection rate fw-drop average-time-frame 600
average-threshold 100 burst-threshold 100
Device(config-profile)# threat-detection rate inspect-drop average-time-frame 600
average-threshold 100 burst-threshold 100
Device(config-profile)# threat-detection rate syn-attack average-time-frame 600
average-threshold 100 burst-threshold 100
Device(config-profile)# exit
Device(config)# zone security public
Device(config-sec-zone)# protection zone-pmap1
Device(config-sec-zone)# exit
Device(config)# zone-pair security private2public source private destination public
Device(config-sec-zone-pair)# end
```

例：ボックス単位のハーフオープン セッション制限の設定

```
Device# configure terminal
Device(config)# parameter-map type inspect global
Device(config-profile)# alert on
Device(config-profile)# per-box max-incomplete 12345
Device(config-profile)# session total 34500
Device(config-profile)# end
```

例：検査 VRF パラメータ マップに対するハーフオープン セッション制限の設定

```
Device# configure terminal
Device(config)# parameter-map type inspect vrf vrf1-pmap
Device(config-profile)# alert on
Device(config-profile)# max-incomplete 3500
Device(config-profile)# session total 34500
Device(config-profile)# exit
Device(config)# parameter-map type inspect global
Device(config-profile)# alert on
Device(config-profile)# vrf vrf1 inspect vrf1-pmap
Device(config-profile)# end
```

例：グローバル TCP SYN フラッド制限の設定

```
Device# configure terminal
Device(config)# parameter-map type inspect global
Device(config-profile)# alert on
Device(config-profile)# per-box tcp syn-flood limit 500
Device(config-profile)# end
```

例：ファイアウォール リソース管理の設定

```
Device# configure terminal
Device(config)# parameter-map type inspect-vrf vrf1-pmap
Device(config-profile)# session total 1000
Device(config-profile)# tcp syn-flood limit 2000
Device(config-profile)# exit
Device(config)# parameter-map type inspect-global
Device(config-profile)# vrf vrf1 inspect pmap1
Device(config-profile)# exit
Device(config)# parameter-map type inspect-vrf vrf-default
Device(config-profile)# session total 6000
Device(config-profile)# tcp syn-flood limit 7000
Device(config-profile)# end
```

IPv6 ファイアウォールでの分散型サービス妨害攻撃の防止およびリソース管理のサポートに関する追加情報

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『Cisco IOS Master Command List, All Releases』
セキュリティ コマンド	• 『Security Command Reference: Commands A to C』 • 『Security Command Reference: Commands D to L』 • 『Security Command Reference: Commands M to R』 • 『Security Command Reference: Commands S to Z』

シスコのテクニカル サポート

説明	リンク
右の URL にアクセスして、シスコのテクニカル サポートを最大限に活用してください。これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

IPv6 ファイアウォールでの分散型サービス妨害攻撃の防止およびリソース管理のサポートの機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *190 : IPv6* ファイアウォールでの分散型サービス妨害攻撃の防止およびリソース管理のサポートの機能情報

機能名	リリース	機能情報
IPv6 ファイアウォールでの分散型サービス妨害攻撃の防止およびリソース管理のサポート	Cisco IOS XE Release 3.7S	IPv6 ゾーンベース ファイアウォールでは、分散型サービス妨害攻撃の防止およびリソース管理がサポートされています。 分散型サービス妨害攻撃の防止機能は、グローバル レベル（すべてのファイアウォール セッション）および VPN ルーティングおよび転送（VRF）レベルでのサービス妨害（DoS）攻撃からの保護を提供します。分散型 DoS 攻撃を防止するため、ファイアウォール セッションのアグレッシブ エージング、ファイアウォールセッションのイベント レート モニタ、ハーフオープン接続制限、およびグローバル TCP SYN Cookie 保護を設定できます。 ファイアウォール リソース管理機能では、デバイスで設定されているグローバル ファイアウォール セッションと VPN ルーティングおよび転送（VRF）インスタンスの数が制限されます。
IPv6 ファイアウォールでの分散型サービス妨害攻撃の防止およびリソース管理のサポート	Cisco IOS XE Release 3.10S	Cisco IOS XE リリース 3.10S では、Cisco CSR 1000 シリーズ ルータのサポートが追加されました。

第 142 章

フローあたりの同時パケットの設定可能数

ゾーンベース ポリシー ファイアウォールでは、フローあたりの同時パケットの数は 25 に制限されており、この制限を超えるパケットはドロップされます。この制限に達したためにパケットのドロップが発生すると、ネットワークのパフォーマンスに影響します。フローあたりの設定可能な同時パケット数機能では、フローあたりの同時パケットの数を 25 ～ 100 の範囲で設定できます。

このモジュールではこの機能について概説し、この機能を設定する方法を説明します。

フローあたりの同期パケットの設定可能数に関する制約事項

- TCP ウィンドウ スケール オプションが設定されている場合、ファイアウォールはフローあたりの多すぎる TCP パケットを同時に処理できないため、設定された制限を超えたパケットはドロップされます。TCP ウィンドウ スケール オプションが有効になっている場合は、使用可能な最大ウィンドウ サイズが 1 GB になります。

  標準の TCP ウィンドウ サイズは 2～65,535 バイトの間です。TCP ペイロード サイズが 655 バイト未満の場合は、1 つの TCP ウィンドウに属しているすべての TCP パケットを 100 個の同時パケットに含めることができないため、パケット ドロップが発生する可能性があります。パケット ドロップを回避するには、TCP ペイロード サイズを大きくするか、TCP ウィンドウ サイズを小さくすることをお勧めします。

- 各プラットフォームで利用可能な総スレッド数は有効なライセンス レベルによって異なります。設定されたフローあたりの同時パケット数が利用可能なハードウェア スレッド数を超えている場合は、同時パケット数の設定が無効になります。

フローあたりの同時パケットの設定可能数に関する情報

設定可能なフローごとの同時パケット数の概要

フローごとの同時パケット数は設定可能であるため、フローごとにネットワークに入ることができる同時パケット数を増やすことができます。フローごとの同時パケット数は、25から100まで増加させることができます。デフォルトの同時パケット数は25です。

マルチスレッド環境では、ゾーンベース ポリシー ファイアウォールが単一のトラフィック フローで複数のパケットを同時に受信する場合があります。ファイアウォールがパケットの処理中に使用するロックのタイプには、フロー ロックとソフトウェア ロックの2つがあります。フロー ロックでは、同じフローに属するパケットが正しい順序で処理されるようになります。通常のソフトウェア ロックは、クリティカルセクションまたは共通データ構造（メモリなど）に対して、複数の Power Processing Element（PPE）スレッドが同時に読み取りや書き込みを試行する際に使用されます。

フローごとの同時パケット数が大きいと、スレッドがロックを要求して取得するまでの時間が大幅に長くなります。この遅延は、リソースの再利用やとハートビート処理などといったタイムクリティカルなインフラストラクチャに悪影響を与えます。遅延を制御するために、同時パケットの数は25に制限され、25を超えるパケットはドロップされていました。

ただし、パケットのドロップはシステムパフォーマンスに多大な影響を与えます。パケットのドロップを最小限に抑えるために、設定可能なフローごとの同時パケット数の機能が導入されました。フローごとの同時パケット数をデフォルトの25から最大100までに変更して設定できます。

フローごとの同時パケット数を変更するには、**parameter-map type inspect** *parameter-map-name* コマンドまたは **parameter-map type inspect global** コマンドの後に **session packet** コマンドを続けて設定する必要があります。**parameter-map type inspect** *parameter-map-name* コマンドで設定された制限は、**parameter-map type inspect global** コマンドで設定された制限より優先されます。

ファイアウォールは、Session Initiation Protocol（SIP）トランクのトラフィックを単一のセッションと見なします。ただし、SIP トランクのトラフィックには、さまざまなユーザのアプリケーション層ゲートウェイ（ALG）フローが多数含まれます。SIP トランクのトラフィックのスループットが他のトラフィックに比べて高いと、同時パケット数の制限によってパケットがドロップされて、ユーザのコールが終了される可能性があります。

フローあたりの同時パケット数の設定方法

フローあたりの同時パケットのクラス マップとポリシー マップの設定

手順の概要

1. **enable**
2. **configure terminal**
3. **class-map type inspect** {**match-any** | **match-all**} *class-map-name*
4. **match protocol** *protocol-name*
5. **exit**
6. **policy-map type inspect** *policy-map-name*
7. **class type inspect** *class-map-name*
8. **inspect**
9. **exit**
10. **class class-default**
11. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。 • パスワードを入力します（要求された場合）。
ステップ 3	**class-map type inspect** {**match-any** | **match-all**} *class-map-name* 例： `Device(config)# class-map type inspect match-any cmap-protocols`	検査タイプ クラス マップを作成して、クラス マップ コンフィギュレーション モードを開始します。
ステップ 4	**match protocol** *protocol-name* 例： `Device(config-cmap)# match protocol tcp`	指定されたプロトコルを基づくクラス マップの一致基準を設定します。

	コマンドまたはアクション	目的
ステップ 5	**exit** 例： `Device(config-cmap)# exit`	クラス マップ コンフィギュレーション モードを終了して、グローバル コンフィギュレーション モードに戻ります。
ステップ 6	**policy-map type inspect** *policy-map-name* 例： `Device(config)# policy-map type inspect policy1`	検査タイプ ポリシー マップを作成して、ポリシー マップ コンフィギュレーション モードを開始します。
ステップ 7	**class type inspect** *class-map-name* 例： `Device(config-pmap)# class type inspect cmap-protocols`	アクションを実行する対象のトラフィック クラスを指定し、ポリシー マップ クラス コンフィギュレーション モードを開始します。
ステップ 8	**inspect** 例： `Device(config-pmap-c)# inspect`	ステートフル パケット インスペクションをイネーブルにします。
ステップ 9	**exit** 例： `Device(config-pmap-c)# exit`	ポリシー マップ クラス コンフィギュレーション モードを終了して、ポリシー マップ コンフィギュレーション モードに戻ります。
ステップ 10	**class class-default** 例： `Device(config-pmap)# class class-default`	デフォルト クラスのポリシーを設定または変更します。
ステップ 11	**end** 例： `Device(config-pmap)# end`	ポリシー マップ コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

フローあたりの同時パケット数の設定

parameter-map type inspect コマンドまたは **parameter-map type inspect global** コマンドのいずれかを設定した後で、フローあたりの同時パケットの数を設定できます。**parameter-map type inspect** コマンドで設定されたフローあたりの同時パケット数は、**parameter-map type inspect global** コマンドで設定された数を上書きします。

フローあたりの同時パケットの数を設定するには、**session packet** コマンドを設定する必要があります。

（注） ステップ 3 と 4 またはステップ 6 と 7 のどちらかを設定する必要があります。

手順の概要

1. **enable**
2. **configure terminal**
3. **parameter-map type inspect** *parameter-map-name*
4. **session packet** *number-of-simultaneous-packets*
5. **exit**
6. **parameter-map type inspect global**
7. **session packet** *number-of-simultaneous-packets*
8. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。 • パスワードを入力します（要求された場合）。
ステップ 3	**parameter-map type inspect** *parameter-map-name* 例： `Device(config)# parameter-map type inspect param1`	（オプション）接続しきい値、タイムアウト、および検査アクションに関連するその他のパラメータを設定する、検査タイプ パラメータ マップを定義します。また、parameter-map タイプ検査コンフィギュレーション モードを開始します。
ステップ 4	**session packet** *number-of-simultaneous-packets* 例： `Device(config-profile)# session packet 55`	（オプション）セッションごとに設定可能な同時トラフィック パケットの数を設定します。 • *number-of-simultaneous-packets* 引数の有効値は 25 ～ 55 です。
ステップ 5	**exit** 例： `Device(config-profile)# exit`	パラメータマップ タイプ検査コンフィギュレーション モードを終了して、グローバル コンフィギュレーション モードに戻ります。
ステップ 6	**parameter-map type inspect global** 例： `Device(config)# parameter-map type inspect global`	（オプション）グローバル検査パラメータ マップを定義して、parameter-map タイプ検査コンフィギュレーション モードを開始します。
ステップ 7	**session packet** *number-of-simultaneous-packets* 例： `Device(config-profile)# session packet 35`	（オプション）セッションごとに設定可能な同時トラフィック パケットの数を設定します。 • *number-of-simultaneous-packets* 引数の有効値は 25 ～ 55 です。

	コマンドまたはアクション	目的
ステップ 8	**end** 例： `Device(config-profile)# end`	パラメータ マップ タイプ検査コンフィギュレーション モードを終了して、特権 EXEC モードに戻ります。

フローあたりの同時パケットのゾーンの設定

この作業では、セキュリティ ゾーン、ゾーン ペアを設定し、ゾーン メンバーとしてインターフェイスを割り当てる方法を示します。

手順の概要

1. **enable**
2. **configure terminal**
3. **zone security** *security-zone*
4. **exit**
5. **zone security** *security-zone*
6. **exit**
7. **zone-pair security** *zone-pair-name* **source** *source-zone* **destination** *destination-zone*
8. **service-policy type inspect** *policy-map-name*
9. **exit**
10. **interface** *type number*
11. **zone-member security** *zone-name*
12. **exit**
13. **interface** *type number*
14. **zone-member security** *zone-name*
15. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 3	**zone security** *security-zone* 例： `Device(config)# zone security z1`	インターフェイスを割り当てることができるセキュリティ ゾーンを作成し、セキュリティ ゾーン コンフィギュレーション モードを開始します。 • 送信元ゾーンと宛先ゾーンという、ゾーン ペアを作成するための 2 つのセキュリティ ゾーンが必要です。
ステップ 4	**exit** 例： `Device(config-sec-zone)# exit`	セキュリティ ゾーン コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードに戻ります。
ステップ 5	**zone security** *security-zone* 例： `Device(config)# zone security z2`	インターフェイスを割り当てることができるセキュリティ ゾーンを作成し、セキュリティ ゾーン コンフィギュレーション モードを開始します。 • 送信元ゾーンと宛先ゾーンという、ゾーン ペアを作成するための 2 つのセキュリティ ゾーンが必要です。
ステップ 6	**exit** 例： `Device(config-sec-zone)# exit`	セキュリティ ゾーン コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードに戻ります。
ステップ 7	**zone-pair security** *zone-pair-name* **source** *source-zone* **destination** *destination-zone* 例： `Device(config)# zone-pair security zp-security source z1 destination z2`	ゾーン ペアを作成し、セキュリティ ゾーンペア コンフィギュレーション モードを開始します。
ステップ 8	**service-policy type inspect** *policy-map-name* 例： `Device(config-sec-zone-pair)# service-policy type inspect policy1`	ファイアウォール ポリシー マップを宛先ゾーン ペアに付加します。 • ゾーンのペア間でポリシーが設定されない場合、トラフィックはデフォルトでドロップされます。
ステップ 9	**exit** 例： `Device(config-sec-zone-pair)# exit`	セキュリティ ゾーン ペア コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードに戻ります。
ステップ 10	**interface** *type number* 例： `Device(config)# interface gigabitethernet 0/0/0`	インターフェイスを設定し、インターフェイス コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 11	**zone-member security** *zone-name* 例： `Device(config-if)# zone-member security z1`	インターフェイスを指定したセキュリティ ゾーンに割り当てます。 • インターフェイスをセキュリティ ゾーンのメンバーにした場合、そのインターフェイスを通して送受信されるすべてのトラフィックは、デフォルトでドロップされます（ただしデバイス宛のトラフィックとデバイス発のトラフィックを除く）。トラフィックがインターフェイス通過するには、ゾーンをポリシーの適用先のゾーンペアの一部にする必要があります。ポリシーがトラフィックを許可すると、トラフィックはそのインターフェイスを通過できます。
ステップ 12	**exit** 例： `Device(config-if)# exit`	インターフェイス設定モードを終了し、グローバル設定モードに戻ります。
ステップ 13	**interface** *type number* 例： `Device(config)# interface gigabitethernet 0/0/3`	インターフェイスを設定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 14	**zone-member security** *zone-name* 例： `Device(config-if)# zone-member security z2`	インターフェイスを指定したセキュリティ ゾーンに割り当てます。
ステップ 15	**end** 例： `Device(config-if)# end`	インターフェイス コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

フローあたりの同時パケットの設定可能数の設定例

例：フローあたりの同時パケットのクラス マップとポリシー マップの設定

```
Device# configure terminal
Device(config)# class-map type inspect match-any cmap-protocols
Device(config-cmap)# match protocol tcp
Device(config-cmap)# exit
Device(config)# policy-map type inspect policy1
Device(config-pmap)# class type inspect cmap-protocols
Device(config-pmap-c)# inspect
```

```
Device(config-pmap-c)# exit
Device(config-pmap)# class class-default
Device(config-pmap)# end
```

例：フローあたりの同時パケット数の設定

parameter-map type inspect コマンドまたは **parameter-map type inspect global** コマンドのいずれかを設定した後で、フローあたりの同時パケットの数を設定できます。**parameter-map type inspect** コマンドで設定されたフローあたりの同時パケット数は、**parameter-map type inspect global** コマンドで設定された数を上書きします。

```
Device# configure terminal
Device(config)# parameter-map type inspect param1
Device(config-profile)# session packet 55
Device(config-profile)# exit
Device(config)# parameter-map type inspect global
Device(config-profile)# session packet 35
Device(config-profile)# end
```

例：フローあたりの同時パケットのゾーンの設定

```
Device# configure terminal
Device(config)# zone security z1
Device(config-sec-zone)# exit
Device(config)# zone security z2
Device(config-sec-zone)# exit
Device(config)# zone-pair security zp-security source z1 destination z2
Device(config-sec-zone-pair)# service-policy type inspect policy1
Device(config-sec-zone-pair)# exit
Device(config)# interface gigabitethernet 0/0/0
Device(config-if)# zone-member security z1
Device(config-if)# exit
Device(config)# interface gigabitethernet 0/0/3
Device(config-if)# zone-member security z2
Device(config-if)# end
```

フローあたりの同時パケットの設定可能数に関する追加情報

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『Cisco IOS Master Command List, All Releases』

関連項目	マニュアル タイトル
ファイアウォール コマンド	• 『Cisco IOS Security Command Reference: Commands A to C』 • 『Cisco IOS Security Command Reference: Commands D to L』 • 『Cisco IOS Security Command Reference: Commands M to R』 • 『Cisco IOS Security Command Reference: Commands S to Z』

シスコのテクニカル サポート

説明	リンク
シスコのサポートWebサイトでは、シスコの製品やテクノロジーに関するトラブルシューティングにお役立ていただけるように、マニュアルやツールをはじめとする豊富なオンライン リソースを提供しています。 お使いの製品のセキュリティ情報や技術情報を入手するために、Cisco Notification Service（Field Notice からアクセス）、Cisco Technical Services Newsletter、Really Simple Syndication（RSS）フィードなどの各種サービスに加入できます。 シスコのサポート Web サイトのツールにアクセスする際は、Cisco.com のユーザ ID およびパスワードが必要です。	http://www.cisco.com/support

フローあたりの同時パケットの設定可能数に関する機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *191 :* フローあたりの同時パケットの設定可能数に関する機能情報

機能名	リリース	機能情報
フローあたりの同時パケットの設定可能数	Cisco IOS XE リリース 3.11S	ゾーンベース ポリシー ファイアウォールでは、フローあたりの同時パケット数が 25 に制限され、その制限を超えたパケットはドロップされました。上限に達したことによるパケットのドロップは、ネットワーク パフォーマンスに影響します。フローあたりの設定可能な同時パケット数機能では、フローあたりの同時パケットの数を 25 ～ 100 の範囲で設定できます。 Cisco IOS XE リリース 3.11S では、この機能が Cisco ASR 1000 シリーズ アグリゲーション サービス ルータ、Cisco 4400 シリーズ サービス統合型ルータ、およびシスコ クラウド サービス ルータ 1000V シリーズで導入されました。 次のコマンドが導入または変更されました。**session packet**、**show parameter-map type inspect**、**show platform hardware qfp feature firewall datapath scb**、**show platform hardware qfp feature firewall zone-pair**、および **show platform software firewall parameter-map**。

第 143 章

ファイアウォール高速ロギング

ファイアウォール高速ロギング機能は、エクスポート フォーマットとして NetFlow バージョン 9 を使用して、ファイアウォール メッセージの高速ロギング（HSL）をサポートします。

このモジュールでは、ゾーンベース ポリシー ファイアウォールで HSL を設定する方法について説明します。

ファイアウォール高速ロギングに関する機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *192*：ファイアウォール高速ロギングに関する機能情報

機能名	リリース	機能情報
ファイアウォール高速ロギング	Cisco IOS XE リリース 2.1	ファイアウォール高速ロギング サポート機能は、NetFlow バージョン 9 をエクスポート形式として使用したファイアウォール HSL のサポートを導入します。 次のコマンドが導入または変更されました。**log dropped-packet**、**log flow-export v9 udp destination**、**log flow-export template timeout-rate**、**parameter-map type inspect global**。

機能名	リリース	機能情報
高速ロギングを使用したゾーンベースファイアウォールの設定	Cisco IOS XE Gibraltar 16.11.1	このリリースでは、送信元インターフェイスのサポートが追加されました。 次のコマンドが導入または変更されました。**log flow-export v9 udp destination source interface** *interface-name*

ファイアウォール高速ロギングに関する情報

ファイアウォール高速ロギングの概要

ゾーンベース ファイアウォールでは、高速ロギング（HSL）がサポートされています。HSL が設定されている場合、ファイアウォールは（NetFlow バージョン 9 レコードと同様に）ルーティングデバイスを介して外部コレクタに伝送されるパケットのログを提供します。レコードは、セッションの作成時と破棄時に送信されます。セッション レコードには、完全な 5 タプル情報（送信元 IP アドレス、宛先 IP アドレス、送信元ポート、宛先ポート、およびプロトコル）が含まれます。タプルは、要素の番号付きリストです。

HSL により、ファイアウォールは、パケット処理への影響を最小限に抑えてレコードをログに記録できます。ファイアウォールは HSL にバッファ モードを使用します。バッファ モードでは、ファイアウォールは、高速ロガーバッファにレコードを直接記録し、パケットを個別にエクスポートします。

（注） 高速ロギング（HSL）は、VASI インターフェイスを介してルーティングできません。

（注） ゾーンベース ファイアウォールでは、最大 4 つの HSL 宛先を設定できます。

ファイアウォールは、次のタイプのイベントをログに記録します。

- 監査：セッションの作成および削除の通知。
- アラート：ハーフオープンおよび最大オープン TCP セッションの通知。
- ドロップ：パケット ドロップの通知。
- 通過：（設定済みレート制限に基づく）パケット通過の通知。
- サマリー：ポリシー ドロップと通過サマリーの通知。

NetFlow コレクタは、**show platform software interface F0 brief** コマンドを発行して、インターフェイス名に FW_SRC_INTF_ID および FW_DST_INTF_ID インターフェイス ID をマッピングします。

次に示す **show platform software interface F0 brief** コマンドの出力例は、[ID] カラムがインターフェイス ID をインターフェイス名（[Name] カラム）にマッピングすることを示しています。

```
Device# show platform software interface F0 brief

Name                            ID      QFP ID
GigabitEthernet0/2/0            16         9
GigabitEthernet0/2/1            17        10
GigabitEthernet0/2/2            18        11
GigabitEthernet0/2/3            19        12
```

NetFlow フィールド ID の説明

次の表に、ファイアウォールの NetFlow テンプレート内で使用される NetFlow フィールド ID を記載します。

表 *193 : NetFlow* フィールド *ID*

フィールド ID	タイプ	長さ	説明
NetFlow ID フィールド（レイヤ 3 IPv4）			
FW_SRC_ADDR_IPV4	8	4	発信元 IPv4 アドレス
FW_DST_ADDR_IPV4	12	4	送信先 IPv4 アドレス
FW_SRC_ADDR_IPV6	27	16	発信元 IPv6 アドレス
FW_DST_ADDR_IPV6	28	16	送信先 IPv6 アドレス
FW_PROTOCOL	4	1	IP プロトコル値
FW_IPV4_IDENT	54	4	IPv4 ID
FW_IP_PROTOCOL_VERSION	60	1	IP プロトコル バージョン
フロー ID フィールド（レイヤ 4）			
FW_TCP_FLAGS	6	1	TCP フラグ
FW_SRC_PORT	7	2	送信元ポート
FW_DST_PORT	11	2	宛先ポート
FW_ICMP_TYPE	176	1	ICMP（[7]）タイプ値
FW_ICMP_CODE	177	1	ICMP コード値

フィールド ID	タイプ	長さ	説明
FW_ICMP_IPV6_TYPE	178	1	ICMP バージョン 6（ICMPv6）タイプ値
FW_ICMP_IPV6_CODE	179	1	ICMPv6 コード値
FW_TCP_SEQ	184	4	TCP シーケンス番号
FW_TCP_ACK	185	4	TCP 確認応答番号
フロー ID フィールド（レイヤ 7）			
FW_L7_PROTOCOL_ID	95	2	レイヤ 7 プロトコル ID。ファイアウォール インスペクションで使用されるレイヤ 7 アプリケーション分類を識別します。通常のレコードでは 2 バイトを使用しますが、オプション レコードでは 4 バイトを使用します。
フロー名フィールド（レイヤ 7）			
FLOW_FIELD_L7_PROTOCOL_NAME	96	32	レイヤ 7 プロトコル名。レイヤ 7 プロトコル ID（FW_L7_PROTOCOL_ID）に対応するレイヤ 7 プロトコル名を識別します。
フロー ID フィールド（インターフェイス）			
FW_SRC_INTF_ID	10	2	入力 SNMP（[8]）ifIndex
FW_DST_INTF_ID	14	2	出力 SNMP ifIndex
FW_SRC_VRF_ID	234	4	入力（イニシエータ）VRF（[9]）ID
FW_DST_VRF_ID	235	4	出力（レスポンダ）VRF ID
FW_VRF_NAME	236	32	VRF 名
マッピングされたフロー ID フィールド（ネットワーク アドレス変換）			
FW_XLATE_SRC_ADDR_IPV4	225	4	マッピングされた発信元 IPv4 アドレス
FW_XLATE_DST_ADDR_IPV4	226	4	マッピングされた送信先 IPv4 アドレス
FW_XLATE_SRC_PORT	227	2	マッピングされた発信元ポート

フィールド ID	タイプ	長さ	説明
FW_XLATE_DST_PORT	228	2	マッピングされた送信先ポート
ステータスおよびイベント フィールド			
FW_EVENT	233	1	高レベルのイベント コード • 0：無視（無効） • 1：フローが作成されました。 • 2：フローが削除されました。 • 3：フローが拒否されました。 • 4：フロー アラート
FW_EXT_EVENT	35,001	2	拡張イベント コード通常のレコードでの長さは2バイト、オプションレコードでの長さは4バイトです。
タイムスタンプおよび統計情報フィールド			
FW_EVENT_TIME_MSEC	323	8	イベントが発生した時間（ミリ秒単位）（1970 年 1 月 1 日 00:00（UTC[10]）からの経過時間。イベントがマイクロイベントの場合は 324、ナノイベントの場合は 325 を使用）
FW_INITIATOR_OCTETS	231	4	イニシエータから到着したパケットフローに含まれるレイヤ4ペイロードの合計バイト数
FW_RESPONDER_OCTETS	232	4	レスポンダから到着したパケットフローに含まれるレイヤ4ペイロードの合計バイト数
AAA フィールド			
FW_USERNAME	40,000	テンプレートに応じて20または64	AAA（[11]）ユーザ名
FW_USERNAME_MAX	40,000	64	最大許容サイズの AAA ユーザ名
アラート フィールド			

フィールド ID	タイプ	長さ	説明
FW_HALFOPEN_CNT	35,012	4	ハーフオープン セッション エントリ数
FW_BLACKOUT_SECS	35,004	4	宛先がブロックされたか、使用できなかった時間（秒単位）
FW_HALFOPEN_HIGH	35,005	4	1 分間でログに記録される TCP ハーフオープン セッション エントリ数に対して設定された最大レート
FW_HALFOPEN_RATE	35,006	4	1 分間でログに記録される TCP ハーフオープン セッション エントリ数の現在のレート
FW_MAX_SESSIONS	35,008	4	このゾーン ペアまたはクラス ID に許可される最大セッション数
その他（Miscellaneous）			
FW_ZONEPAIR_ID	35,007	4	ゾーン ペア ID
FW_CLASS_ID	51	4	クラス ID
FW_ZONEPAIR_NAME	35,009	64	ゾーン ペア名
FW_CLASS_NAME	100	64	クラス名
FW_EXT_EVENT_DESC	35,010	32	拡張イベントの説明
FLOW_FIELD_CTS_SRC_GROUP_TAG	34000	2	Cisco TrustSec ソース タグ
FW_SUMMARY_PKT_CNT	35,011	4	ドロップ/パス サマリ レコードに示されたパケット数
FW_EVENT_LEVEL	33003	4	ログに記録されたイベントのレベルを定義します。 • 0x01：ボックスごと • 0x02：VRF • 0x03：ゾーン • 0x04：クラス マップ • その他の値は未定義

フィールド ID	タイプ	長さ	説明
FW_EVENT_LEVEL_ID	33,004	4	FW_EVENT_LEVEL フィールドの ID を定義します。 • FW_EVENT_LEVEL が 0x02（VRF）の場合、このフィールドは VRF_ID を表します。 • FW_EVENT_LEVEL が 0x03（ゾーン）の場合、このフィールドは ZONE_ID を表します。 • FW_EVENT_LEVEL が 0x04（クラス マップ）の場合、このフィールドは CLASS_ID を表します。 • その他すべてのクラスでは、このフィールド ID は 0（ゼロ）になります。 FW_EVENT_LEVEL が存在しない場合、このフィールドの値はゼロになります。
FW_CONFIGURED_VALUE	33,005	4	設定済みのハーフオープン、アグレッシブ エージング、およびイベント レート モニタリングの制限を表す値。このフィールドの値の意味は、関連付けられた FW_EXT_EVENT フィールドによって異なります。
FW_ERM_EXT_EVENT	33,006	2	拡張イベント レート モニタリング コード
FW_ERM_EXT_EVENT_DESC	33,007	N（文字列）	拡張イベント レート モニタリング イベントを説明する文字列

[7] Internet Control Message Protocol
[8] Simple Network Management Protocol
[9] Virtual Routing and Forwarding
[10] 協定世界時
[11] 認証、認可、アカウンティング

HSL メッセージ

以下に、Cisco ASR 1000 シリーズ アグリゲーション サービス ルータからの Syslog メッセージの例を記載します。

表 *194 : Syslog* メッセージおよびそのテンプレート

メッセージ ID	メッセージの説明	HSL テンプレート
FW-6-DROP_PKT タイプ：情報	Dropping %s pkt from %s %CA:%u => %CA:%u (target:class)-(%s:%s) %s %s with ip ident %u %s %s 説明：ファイアウォールインスペクションによりパケットがドロップされました。 %s：tcp/udp/icmp/不明なプロトコル/L7 プロトコル %s：インターフェイス %CA:%u：IP/IP6 アドレス:ポート %s:%s：ゾーンペアの名前/クラス名 %s：「原因（due to）」 %s：fw_ext_event 名 %u：IP 識別子 %s：TCP の場合、TCP SEQ/ACK 番号および TCP フラグ %s：ユーザ名	FW_TEMPLATE_DROP_V4 または FW_TEMPLATE_DROP_V6

メッセージ ID	メッセージの説明	HSL テンプレート
FW-6-SESS_AUDIT_TRAIL_START タイプ：情報	(target:class)-(%s:%s):Start %s session: initiator (%CA:%u) -- responder (%CA:%u) from %s %s %s 説明：インスペクションセッションが開始されました。このメッセージは、各インスペクションセッションの開始時に発行され、送信元/宛先アドレスおよびポートを記録します。 %s:%s：ゾーンペアの名前/クラス名 %s：L4/L7 プロトコル名 %CA:%u：IP/IP6 アドレス:ポート %s：インターフェイス %s：ユーザ名 %s：TODO 実際のログ： *Jan 21 20:13:01.078: %IOSXE-6-PLATFORM: F0: cpp_cp: CPP:00 Thread:125 TS:00000010570290947309 %FW-6-SESS_AUDIT_TRAIL_START: Start tcp session: initiator (10.1.1.1:43365) -- responder (10.3.21.1:23) from FastEthernet0/1/0	FW_TEMPLATE_START_AUDIT_V4 または FW_TEMPLATE_START_AUDIT_V6

メッセージ ID	メッセージの説明	HSL テンプレート
FW-6-SESS_AUDIT_TRAIL タイプ：情報	(target:class)-(%s:%s):Stop %s session: initiator (%CA:%u) sent %u bytes -- responder (%CA:%u) sent %u bytes , from %s %s 説明：ネットワーク アクティビティのセッションごとのトランザクション ログ。このメッセージは、各インスペクションセッションの終了時に発行され、送信元/宛先アドレスおよびポート、クライアントとサーバから送信されたバイト数を記録します。 %s:%s：ゾーンペアの名前/クラス名 %s：L4/L7 プロトコル名 %CA:%u：IP/IP6 アドレス:ポート %u：バイト カウンタ %s：インターフェイス %s：TODO 実際のログ： *Jan 21 20:13:15.889: %IOSXE-6-PLATFORM: F0: cpp_cp: CPP:00 Thread:036 TS:00000010585102587819 %FW-6-SESS_AUDIT_TRAIL: Stop tcp session: initiator (10.1.1.1:43365) sent 35 bytes -- responder (11.1.1.1:23) sent 95 bytes, from FastEthernet0/1/0	FW_TEMPLATE_STOP_AUDIT_V4 または FW_TEMPLATE_STOP_AUDIT_V6

メッセージ ID	メッセージの説明	HSL テンプレート
FW-4-UNBLOCK_HOST タイプ：警告	(target:class)-(%s:%s):New TCP connections to host %CA no longer blocked 説明：指定のホストへの新しい TCP 接続試行がブロックされなくなりました。このメッセージは、指定のホストへの新しい TCP 接続試行のブロッキングが解除されたことを意味します。 %s:%s：ゾーンペアの名前/クラス名 %CA：IP/IP6 アドレス	FW_TEMPLATE_ALERT_TCP_HALF_OPEN_V4 または FW_TEMPLATE_ALERT_TCP_HALF_OPEN_V6、fw_ext_event ID：FW_EXT_ALERT_UNBLOCK_HOST
FW4HOST_TCP_ALERT_ON タイプ：警告	"(target:class)-(%s:%s):Max tcp half-open connections (%u) exceeded for host %CA. 説明：ハーフオープン TCP 接続の max-incomplete host 制限を超えました。このメッセージは、保護対象のサーバに対するハーフオープン接続数が多く、SYN フラッド攻撃が進行中であることを示す可能性があることを意味します。 %s:%s：ゾーンペアの名前/クラス名 %u：ハーフオープン接続数 %CA：IP/IP6 アドレス	FW_TEMPLATE_ALERT_TCP_HALF_OPEN_V4 または FW_TEMPLATE_ALERT_TCP_HALF_OPEN_V6、fw_ext_event ID：FW_EXT_ALERT_HOST_TCP_ALERT_ON

メッセージ ID	メッセージの説明	HSL テンプレート
FW-2-BLOCK_HOST タイプ：クリティカル	(target:class)-(%s:%s):Blocking new TCP connections to host %CA for %u minute%s (half-open count %u exceeded). 説明：ハーフオープン TCP 接続の max-incomplete host しきい値を超えました。指定のホストに対する以降の新しい TCP 接続試行は拒否され、ブロッキング オプションが以降の新しい接続すべてをブロックするように設定されます。設定されたブロック時間が満了すると、ブロッキングが解除されます。 %s:%s：ゾーン ペアの名前/クラス名 %CA：IP/IP6 アドレス %u：ブロック時間（分） %s：ブロック時間が 1 分を超える場合「s」 %u：ハーフオープン カウンタ	FW_TEMPLATE_ALERT_TCP_HALF_OPEN_V4 または FW_TEMPLATE_ALERT_TCP_HALF_OPEN_V6、fw_ext_event ID：FW_EXT_ALERT_BLOCK_HOST

メッセージ ID	メッセージの説明	HSL テンプレート
FW-4-ALERT_ON タイプ：警告	(target:class)-(%s:%s):%s, count (%u/%u) current rate: %u 説明：ハーフオープン接続の max-incomplete high しきい値または新しい接続開始レートのいずれかを超えました。このエラーメッセージは、ファイアウォールからの新しい着信接続レートが異常に高く、DOS攻撃が進行中であることを示す可能性があることを意味します。このメッセージが発行されるのは、max-incomplete high しきい値を上回った場合のみです。 %s:%s：ゾーンペアの名前/クラス名 %s：「アグレッシブな状態（getting aggressive）」 %u/%u：ハーフオープン接続数/高 %u：現在のレート	FW_TEMPLATE_ALERT_HALFOPEN_V4 または FW_TEMPLATE_ALERT_HALFOPEN_V6、fw_ext_event ID：FW_EXT_SESS_RATE_ALERT_ON
FW-4-ALERT_OFF タイプ：警告	(target:class)-(%s:%s):%s, count (%u/%u) current rate: %u 説明：ハーフオープン接続数または新しい接続開始レートのいずれかが、max-incomplete low しきい値を下回りました。このメッセージは、新しい着信接続のレートが低下したことを意味します。新しい接続は、max-incomplete low しきい値を下回った場合にのみ実行されます。 %s:%s：ゾーンペアの名前/クラス名 %s：「沈静化中（calming down）」 %u/%u：ハーフオープン接続数/高 %u：現在のレート	FW_TEMPLATE_ALERT_HALFOPEN_V4 または FW_TEMPLATE_ALERT_HALFOPEN_V6、fw_ext_event ID：FW_EXT_SESS_RATE_ALERT_OFF

メッセージ ID	メッセージの説明	HSL テンプレート
FW-4-SESSIONS_MAXIMUM タイプ：警告	Number of sessions for the firewall policy on "(target:class)-(%s:%s) exceeds the configured sessions maximum value %u 説明：確立済みの セッション数が、設定されているセッション最大数の制限を超えました。 %s:%s：ゾーンペアの名前/クラス名 %u：最大セッション数	FW_TEMPLATE_ALERT_MAX_SESSION
FW-6-PASS_PKT タイプ：情報	Passing %s pkt from %s %CA:%u => %CA:%u (target:class)-(%s:%s) %s %s with ip ident %u 説明：ファイアウォールインスペクションによりパケットが渡されました。 %s：tcp/udp/icmp/不明なプロトコル %s：インターフェイス %CA:%u：送信元 IP/IP6 アドレス:ポート %CA:%u：宛先 IP/IP6 アドレス:ポート %s:%s：ゾーンペアの名前/クラス名 %s %s：「原因（due to）」、「ポリシーマップで PASS アクションを検出（PASS action found in policy-map）」 %u：IP 識別子	FW_TEMPLATE_PASS_V4 または FW_TEMPLATE_PASS_V6

メッセージ ID	メッセージの説明	HSL テンプレート
FW-6-LOG_SUMMARY タイプ：情報	%u packet%s %s from %s %CA:%u => %CA:%u (target:class)-(%s:%s) %s 説明：ドロップされたパケット数と渡されたパケット数のログサマリ %u %s：パケット数、「s were」または「was」 %s：「ドロップ（dropped）」/「パス（passed）」 %s：インターフェイス %CA:%u：送信元 IP/IP6 アドレス:ポート %CA:%u：宛先 IP/IP6 アドレス:ポート %s:%s：ゾーンペアの名前/クラス名 %s：ユーザ名	FW_TEMPLATE_SUMMARY_V4 または FW_TEMPLATE_SUMMARY_V6、FW_EVENT として 3 - drop 4 - pass を使用

ファイアウォール拡張イベント

ファイアウォール拡張イベントのイベント名により、ファイアウォール拡張イベント値とイベント ID が対応付けられます。イベント名オプション レコードを使用して、イベント値とイベント ID の対応付けを確認します。

拡張イベントは標準ファイアウォールイベント（inpect、pass、drop）の一部ではありません。

次の表に、Cisco IOS XE リリース 3.9S より前のリリースに適用されるファイアウォール拡張イベントについて説明します。

表 *195 : Cisco IOS XE* リリース *3.9S* 以前のファイアウォール拡張イベントおよびイベントの説明

値	イベント ID	説明
0	FW_EXT_LOG_NONE	特定の拡張イベントはありません。
1	FW_EXT_ALERT_UNBLOCK_HOST	指定したホストに対する新規の TCP 接続試行はブロックされません。
2	FW_EXT_ALERT_HOST_TCP_ALERT_ON	ハーフオープン TCP 接続の最大不完全ホスト制限を超えました。

値	イベント ID	説明
3	FW_EXT_ALERT_BLOCK_HOST	指定されたホストに対する後続の TCP 接続試行はすべて拒否されます。これは、ハーフオープン TCP 接続の最大不完全ホストしきい値を超えており、かつ後続の新規接続をブロックするようにブロッキング オプションが設定されているためです。
4	FW_EXT_SESS_RATE_ALERT_ON	ハーフオープン接続の最大不完全上限しきい値を超えたか、または新規接続開始レートを超えました。
5	FW_EXT_SESS_RATE_ALERT_OFF	ハーフオープン TCP 接続の数が、最大不完全下限しきい値を下回っているか、または新規接続開始レートが最大不完全下限しきい値を下回りました。
6	FW_EXT_RESET	接続をリセットします。
7	FW_EXT_DROP	接続をドロップします。
10	FW_EXT_L4_NO_NEW_SESSION	新規セッションは許可されません。
12	FW_EXT_L4_INVALID_SEG	無効な TCP セグメント。
13	FW_EXT_L4_INVALID_SEQ	無効な TCP シーケンス番号。
14	FW_EXT_L4_INVALID_ACK	無効な TCP 確認応答（ACK）。
15	FW_EXT_L4_INVALID_FLAGS	無効な TCP フラグ。
16	FW_EXT_L4_INVALID_CHKSM	無効な TCP チェックサム。
18	FW_EXT_L4_INVALID_WINDOW_SCALE	無効な TCP ウィンドウ スケール。
19	FW_EXT_L4_INVALID_TCP_OPTIONS	無効な TCP オプション。
20	FW_EXT_L4_INVALID_HDR	無効なレイヤ 4 ヘッダー。
21	FW_EXT_L4_OOO_INVALID_SEG	OoO [12]無効セグメント。
24	FW_EXT_L4_SYNFLOOD_DROP	同期（SYN）フラッド パケットがドロップされます。
25	FW_EXT_L4_SCB_CLOSED	セッションがパケット受信中にセッションが終了しました。
26	FW_EXT_L4_INTERNAL_ERR	ファイアウォールの内部エラーです。

値	イベント ID	説明
27	FW_EXT_L4_OOO_SEG	OoO セグメント。
28	FW_EXT_L4_RETRANS_INVALID_FLAGS	無効な再送信パケット。
29	FW_EXT_L4_SYN_IN_WIN	無効な SYN フラグ。
30	FW_EXT_L4_RST_IN_WIN	無効なリセット（RST）フラグ。
31	FW_EXT_L4_STRAY_SEG	遊離 TCP セグメント。
32	FW_EXT_L4_RST_TO_RESP	応答側へのリセット メッセージの送信。
33	FW_EXT_L4_CLOSE_SCB	セッションの終了。
34	FW_EXT_L4_ICMP_INVAL_RET	無効な ICMP [13] パケット。
37	FW_EXT_L4_MAX_HALFSESSION	最大ハーフオープン セッション制限を超えています。
38	FW_EXT_NO_RESOURCE	リソース（メモリ）が使用できません。
40	FW_EXT_INVALID_ZONE	無効なゾーン。
41	FW_EXT_NO_ZONE_PAIR	ゾーン ペアは使用できません。
42	FW_EXT_NO_TRAFFIC_ALLOWED	トラフィックは許可されていません。
43	FW_EXT_FRAGMENT	パケット フラグメントがドロップされます。
44	FW_EXT_PAM_DROP	PAM [14] アクションがドロップされます。
45	FW_EXT_NOT_INITIATOR	セッション開始パケットではありません。 これは、次のいずれかの理由で発生します。 • プロトコルが TCP の場合、1 番目のパケットが SYN パケットではありません。 • プロトコルが ICMP の場合、1 番目のパケットが ECHO パケットまたは TIMESTAMP パケットではありません。

値	イベント ID	説明
48	FW_EXT_ICMP_ERROR_PKTS_BURST	ICMP エラー パケットがバースト モードになりました。バースト モードでは、応答側インターフェイスからの応答を待たずにパケットが繰り返し送信されます。
49	FW_EXT_ICMP_ERROR_MULTIPLE_UNREACH	「宛先到達不能」タイプの ICMP エラーを複数受信しました。
50	FW_EXT_ICMP_ERROR_L4_INVALID_SEQ	ICMP エラー メッセージに埋め込まれたパケットに無効なシーケンス番号があります。
51	FW_EXT_ICMP_ERROR_L4_INVALID_ACK	ICMP エラー メッセージに埋め込まれたパケットに無効な確認応答（ACK）番号があります。
52	FW_EXT_MAX	未使用。

[12] 順序外
[13] Internet Control Message Protocol
[14] Port-to-Application Mapping

次の表では、Cisco IOS XE リリース 3.9S 以降のリリースに適用されるファイアウォール拡張イベントについて説明します。

表 *196 : Cisco IOS XE* リリース *3.9S* 以降のファイアウォール拡張イベントおよびイベントの説明

値	イベント ID	説明
0	FW_EXT_LOG_NONE	特定の拡張イベントはありません。
1	FW_EXT_FW_DROP_L4_TYPE_INVALID_HDR	レイヤ 4 ICMP、TCP、または UDP ヘッダーを組み込むことができない小さいデータグラム。
2	FW_EXT_FW_DROP_L4_TYPE_INVALID_ACK_FLAG	ACK フラグが含まれていないか、または TCP スリーウェイ ハンドシェイクにおいて SYN/ACK パケットに RST フラグが設定されており、パケットに無効なシーケンス番号がありました。

値	イベント ID	説明
3	FW_EXT_FW_DROP_L4_TYPE_INVALID_ACK_NUM	これは、次のいずれかの理由で発生します。 • パケットの ACK 値が、接続の最も古い応答未確認シーケンス番号よりも小さい場合。 • パケットの ACK 値が、接続の次のシーケンス番号よりも大きい場合。 • スリーウェイ ハンドシェイク中に受信した SYN/ACK または ACK パケットで、シーケンス番号が初期シーケンス番号に 1 を加算した値と等しくない場合。
4	FW_EXT_FW_DROP_L4_TYPE_INVALID_TCP_INITIATOR	フローの 1 番目のパケットが SYN パケットではありませんでした。
5	FW_EXT_FW_DROP_L4_TYPE_SYN_WITH_DATA	SYN パケットにペイロードが含まれています。このような SYN パケットはサポートされていません。
6	FW_EXT_FW_DROP_L4_TYPE_INVALID_TCP_WIN_SCALE_OPTION	TCP ウィンドウ スケール オプションの長さが無効です。
7	FW_EXT_FW_DROP_L4_TYPE_INVALID_SEG_SYNSENT_STATE	SYNSENT 状態の無効な TCP セグメントを受信しました。 これは、次のいずれかの理由で発生します。 • SYN/ACK にペイロードが含まれています。 • SYN/ACK にその他のフラグ（push（PSH）、urgent（URG）、finish（FIN））が設定されています。 • ペイロードまたは無効な TCP フラグ（ACK、PSH、URG、FIN、RST）が設定されている再送信 SYN メッセージを受信しました。 • イニシエータから SYN 以外のパケットを受信しました。

値	イベント ID	説明
8	FW_EXT_FW_DROP_L4_TYPE_INVALID_SEG_SYNRCVD_STATE	再送信された SYN パケットにペイロードが含まれているか、または応答側からパケットを受信しました。
9	FW_EXT_FW_DROP_L4_TYPE_INVALID_SEG_PKT_TOO_OLD	パケットが、受信側の現在の TCP ウィンドウよりも古い（小さい）パケットです。
10	FW_EXT_FW_DROP_L4_TYPE_INVALID_SEG_PKT_WIN_OVERFLOW	パケットのシーケンス番号は、受信側の TCP ウィンドウの範囲外（大きい）です。
11	FW_EXT_FW_DROP_L4_TYPE_INVALID_SEG_PYLD_AFTER_FIN_SEND	FIN メッセージの受信後に、ペイロードを含むパケットを送信元から受信しました。
12	FW_EXT_FW_DROP_L4_TYPE_INVALID_FLAGS	パケットに関連付けられた TCP フラグが無効です。この問題は、次の理由で発生する場合があります。 • 初期パケットで、SYN フラグとともにその他のフラグが設定されていた。初期パケットでは SYN フラグだけが許可されています。 • 予期される SYN/ACK に SYN フラグが含まれていなかったか、SYN/ACK にスリーウェイ ハンドシェイクの 2 番目のパケットの余分なフラグが含まれていました。

値	イベント ID	説明
13	FW_EXT_FW_DROP_L4_TYPE_INVALID_SEQ	無効なシーケンス番号。 これは、次のいずれかの理由で発生します。 • シーケンス番号が ISN[15] よりも小さい。 • シーケンス番号が ISN と等しく、SYN パケットと等しくない。 • 受信ウィンドウ サイズがゼロでパケットにデータが含まれている場合、またはシーケンス番号が最終 ACK 番号よりも大きい場合。 • シーケンス番号が TCP ウィンドウの範囲外である。
14	FW_EXT_FW_DROP_L4_TYPE_RETRANS _INVALID_FLAGS	再送信されたパケットは、受信側によりすでに確認応答済みです。
15	FW_EXT_FW_DROP_L4_TYPE_L7_OOO _SEG	パケットに、予期されている次のセグメントよりも前に到着した TCP セグメントが含まれています。
16	FW_EXT_FW_DROP_L4_TYPE_SYN _FLOOD_DROP	ポリシーに設定されている最大最大不完全セッション数を越え、ホストがブロック期間に入りました。
17	FW_EXT_FW_DROP_L4_TYPE_MAX _HALFSESSION	許可されているハーフオープン セッションの数を超えました。
18	FW_EXT_FW_DROP_L4_TYPE_ TOO_MANY_PKTS	フローあたりの同時インスペクション可能なパケットの最大数を超えました。現在、最大 25 個の同時パケットのインスペクションが許可されています。同時インスペクションにより、1 つのフローがプロセッサ リソースを占有することが防止されます。
19	FW_EXT_FW_DROP_L4_TYPE_TOO _MANY_ICMP_ERR_PKTS	フローあたりの ICMP エラー パケット最大数を超えました。このログは、ファイアウォール ベース インスペクションによってトリガーされます。

値	イベント ID	説明
20	FW_EXT_FW_DROP_L4_TYPE_UNEXPECT _TCP_PYLD	レスポンダから再送信された SYN/ACK にペイロードが含まれています。TCP スリーウェイ ハンドシェイク ネゴシエーションの実行中はペイロードは許可されません。
21	FW_EXT_FW_DROP_L4_TYPE_INTERNAL _ERR_UNDEFINED_DIR	パケットの方向が未定義です。
22	FW_EXT_FW_DROP_L4_TYPE_SYN _IN_WIN	確立されたセッションの TCP パケットが、SYN フラグが設定された状態で到着しました。スリーウェイ ハンドシェイクの最初の 2 つのパケットの後は、SYN フラグは許可されていません。
23	FW_EXT_FW_DROP_L4_TYPE_RST _IN_WIN	RST フラグが設定された TCP パケットを受信しましたが、そのシーケンス番号が最後に受信した確認応答の外部でした。このパケットは誤った順序で送信された可能性があります。
24	FW_EXT_FW_DROP_L4_TYPE_ STRAY_SEG	フローの切断後に予期しないパケットを受信したか、またはイニシエータが有効な SYN フラグを送信する前に応答側からパケットを受信しました。
25	FW_EXT_FW_DROP_L4_TYPE_RST_TO_RESP	応答側からの SYN/ACK フラグが予期されていました。しかし、無効なシーケンス番号のパケットを受信しました。ゾーンベース ファイアウォールから RST フラグが応答側に送信されました。
26	FW_EXT_FW_DROP_L4_TYPE _I NTERNAL_ERR_ICMP_NO_NAT	ICMP パケットは NAT [16]変換されていますが、内部 NAT 情報がありません。内部エラーです。
27	FW_EXT_FW_DROP_L4_TYPE _ INTERNAL_ERR_ICMP_ALLOC_FAIL	ICMP インスペクション中に ICMP エラー パケットを割り当てることができませんでした。
28	FW_EXT_FW_DROP_L4_TYPE _INTERNAL_ERR_ICMP_GET_STAT_BLK_FAIL	分類結果に、必要な統計情報メモリがありませんでした。ポリシー情報がデータ プレーンに正しくダウンロードされていません。

値	イベント ID	説明
29	FW_EXT_FW_DROP_L4_TYPE _INTERNAL_ERR_ICMP_DIR_NOT_IDENTIFIED	パケットの方向が未定義です。
30	FW_EXT_FW_DROP_L4_TYPE_ ICMP_SCB_CLOSE	セッションの切断中にICMPパケットを受信しました。
31	FW_EXT_FW_DROP_L4_TYPE_ ICMP_PKT_NO_IP_HDR	ICMPエラーパケットのペイロードにIP ヘッダーがありません。
32	FW_EXT_FW_DROP_L4_TYPE_ ICMP_ERROR_NO _IP_NO_ICMP	ICMP エラー パケットに IP または ICMPがありません。これは、不正なパケットが原因で発生している可能性があります。
33	FW_EXT_FW_DROP_L4_TYPE_ICMP_ERROR _PKTS_BURST	ICMPエラーパケットがバースト制限10 を超えています。
34	FW_EXT_FW_DROP_L4_TYPE_ICMP_ERROR _MULTIPLE_UNREACH	ICMPエラーパケットが「到達不能」制限を超えています。1番目の到達不能パケットだけが通過できます。
35	FW_EXT_FW_DROP_L4_TYPE_ICMP_ERROR _L4_INVALID_SEQ	埋め込みパケットのシーケンス番号が、ICMPエラーパケットをトリガーした TCP パケットのシーケンス番号と一致しません。
36	FW_EXT_FW_DROP_L4_TYPE_ICMP_ERROR _L4_INVALID_ACK	ICMP エラー パケット ペイロードに含まれている TCP パケットに、これまでに確認されていない ACK フラグが含まれています。
37	FW_EXT_FW_DROP_L4_TYPE_ ICMP_PKT_TOO _SHORT	ICMP エラー パケットの長さが、IP ヘッダー長とICMPヘッダー長の合計よりも短くなっています。
38	FW_EXT_FW_DROP_L4_TYPE_ SESSION_LIMIT	不明確なチャネルの入力を求めている間に、リソースがセッション制限を超えました。
39	FW_EXT_FW_DROP_L4_TYPE_ SCB_CLOSE	終了したセッションで TCP パケットが受信されました。
40	FW_EXT_FW_DROP_INSP_TYPE_ POLICY_NOT_PRESENT	ゾーン ペア内にポリシーがありません。

値	イベント ID	説明
41	FW_EXT_FW_DROP_INSP_TYPE_ SESS_MISS_POLICY _NOT_PRESENT	ゾーン ペアは同一ゾーンで設定されていますが、このゾーンにポリシーが含まれていません。
44	FW_EXT_FW_DROP_INSP_TYPE_ CLASS_ACTION_DROP	分類アクションは、ICMP、TCP、および UDP 以外のパケットのドロップです。
45	FW_EXT_FW_DROP_INSP_TYPE_ PAM_LOOKUP_FAIL	分類アクションは、PAM エントリのドロップです。
48	FW_EXT_FW_DROP_INSP_TYPE_ INTERNAL_ERR_ GET_STAT_BLK_FAIL	分類結果バイトから統計ブロックを取得できませんでした。
49	FW_EXT_FW_DROP_SYNCOOKIE_ TYPE_SYNCOOKIE _MAX_DST	SYN フラッド パケットの最大エントリ制限に達しました。
50	FW_EXT_FW_DROP_SYNCOOKIE_ TYPE_INTERNAL _ERR_ALLOC_FAIL	宛先テーブル エントリにメモリを割り当てることができません。
51	FW_EXT_FW_DROP_SYNCOOKIE_ TYPE_SYN_COOKIE _TRIGGER	SYN Cookie ロジックがトリガーされました。SYN Cookie を含む SYN/ACK が送信され、元の SYN パケットがドロップされたことを示します。
52	FW_EXT_FW_DROP_POLICY_ TYPE_FRAG_DROP	VFR[17]パケットの 1 番目のフラグメントがドロップされ、関連付けられているその他のフラグメントがすべてドロップされます。
53	FW_EXT_FW_DROP_POLICY_ TYPE_ACTION_DROP	分類アクションは、パケットのドロップです。
54	FW_EXT_FW_DROP_POLICY_ TYPE_ICMP_ACTION_DROP	ICMP 埋め込みパケットのポリシー アクションは DROP です。
55	FW_EXT_FW_DROP_L7_TYPE_ NO_SEG	レイヤ 7 ALG[18]は、検査セグメント化パケットを検査しません。
56	FW_EXT_FW_DROP_L7_TYPE_ NO_FRAG	レイヤ 7 ALG は、フラグメント化パケットを検査しません。
57	FW_EXT_FW_DROP_L7_TYPE_ UNKNOWN_PROTO	不明なアプリケーション プロトコル タイプ。
58	FW_EXT_FW_DROP_L7_TYPE_ ALG_RET_DROP	レイヤ 7 ALG インスペクションの結果、パケットがドロップされました。

値	イベント ID	説明
59	FW_EXT_FW_DROP_NONSESSION _TYPE	セッションの作成に失敗しました。
60	FW_EXT_FW_DROP_NO_NEW _SESSION_TYPE	初期 HA [19]状態では新規セッションは許可されていません。
61	FW_EXT_FW_DROP_NOT_ INITIATOR_TYPE	セッション イニシエータ パケットではありません。
62	FW_EXT_FW_DROP_INVALID _ZONE_TYPE	デフォルトのゾーンが無効な場合、セキュリティ ゾーンに関連付けられているインターフェイス間でのみトラフィックが許可されます。
64	FW_EXT_FW_DROP_NO_FORWARDING_TYPE	ファイアウォールが設定されていません。
65	FW_EXT_FW_DROP_ BACKPRESSURE_TYPE	ファイアウォール バックプレッシャを有効にできるのは、HSL [20]が有効であり、かつ HSL ロガーがログ メッセージを送信できない場合です。バックプレッシャは、HSL がログを送信できるようになるまで有効なままになります。
66	FW_EXT_FW_DROP_L4_TYPE_INTERNAL _ERR _SYNFLOOD_ALLOC_HOSTDB_FAIL	SYN 処理中にホスト レート制限が追跡されます。ホスト エントリを割り当てることができませんでした。
67	FW_EXT_FW_DROP_L4_TYPE_ SYNFLOOD_BLACKOUT_DROP	ブラックアウト時間が設定されている場合に、設定されているハーフオープン接続の制限を超えると、指定されている IP アドレスへの新規接続はすべてドロップされます。
68	FW_EXT_FW_DROP_L7_TYPE_ PROMOTE_FAIL_NO_ZONE_PAIR	失敗したポリシー。ゾーン ペアが設定されていないために AGL がセッションのレベルを上げようとすると、ポリシーが失敗します。
69	FW_EXT_FW_DROP_L7_TYPE_ PROMOTE_FAIL_NO_POLICY	失敗したポリシー。ポリシーがないために ALG がセッションのレベルを上げようとすると、ポリシーが失敗します。

値	イベント ID	説明
	FW_EXT_FW_DROP_L4_TYPE_ONEFW_SCB_CLOSE	コンテキスト認識型ファイウォール（CXSC）がティアダウンを要求した後でパケットを受信しました。
	FW_EXT_FW_DROP_L4_TYPE_ONEFW_FAIL_CLOSE	CXSC が動作していません。

[15] 初期シーケンス番号
[16] ネットワーク アドレス変換
[17] フラグメンテーション再構成
[18] アプリケーション レイヤ ゲートウェイ
[19] ハイ アベイラビリティ
[20] 高速ロギング

ファイアウォール高速ロギングの設定方法

グローバル パラメータ マップの高速ロギングの有効化

デフォルトでは、高速ロギング（HSL）は有効ではなく、ファイアウォールのログはルート プロセッサ（RP）またはコンソールのロガー バッファに送信されます。HSL をイネーブルにすると、ログはボックス外の高速ログ コレクタに送信されます。パラメータ マップはファイアウォールに到達するトラフィック対してアクションを実行する手段を提供し、グローバル パラメータ マップはファイアウォール セッション テーブル全体に適用されます。グローバル パラメータ マップの高速ロギングを有効にするには、次の作業を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **parameter-map type inspect global**
4. **log dropped-packets**
5. **log flow-export v9 udp destination** *ip-address port-number*
6. **log flow-export template timeout-rate** *seconds*
7. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。

	コマンドまたはアクション	目的
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**parameter-map type inspect global** 例： `Device(config)# parameter-map type inspect global`	グローバル パラメータ マップを設定し、パラメータ マップ タイプ検査コンフィギュレーション モードを開始します。
ステップ 4	**log dropped-packets** 例： `Device(config-profile)# log dropped-packets`	ドロップされたパケットのロギングをイネーブルにします。
ステップ 5	**log flow-export v9 udp destination** *ip-address port-number* 例： `Device(config-profile)# log flow-export v9 udp destination 10.0.2.0 5000`	NetFlow イベント ロギングをイネーブルにし、ログ コレクタの IP アドレスとポート番号を提供します。
ステップ 6	**log flow-export template timeout-rate** *seconds* 例： `Device(config-profile) log flow-export template timeout-rate 5000`	テンプレートのタイムアウト値を指定します。
ステップ 7	**end** 例： `Device(config-profile)# end`	パラメータ マップ タイプ検査コンフィギュレーション モードを終了して、特権 EXEC モードに戻ります。

ファイアウォール アクションの高速ロギングの有効化

検査タイプ パラメータ マップを設定している場合、高速ロギングを有効にするには、次の作業を実行します。パラメータマップはファイアウォールのインスペクション動作を指定し、ファイアウォールのインスペクション パラメータマップは検査タイプとして設定されます。

手順の概要

1. **enable**
2. **configure terminal**
3. **parameter-map type inspect** *parameter-map-name*
4. **audit-trail on**
5. **alert on**
6. **one-minute** {**low** *number-of-connections* | **high** *number-of-connections*}
7. **tcp max-incomplete host** しきい値
8. **exit**

9. **policy-map type inspect** *policy-map-name*
10. **class type inspect** *class-map-name*
11. **inspect** *parameter-map-name*
12. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**parameter-map type inspect** *parameter-map-name* 例： `Device(config)# parameter-map type inspect parameter-map-hsl`	接続しきい値、タイムアウト、その他の **inspect** キーワードに関連するパラメータに対する検査パラメータマップを設定し、パラメータマップタイプ検査コンフィギュレーション モードを開始します。
ステップ 4	**audit-trail on** 例： `Device(config-profile)# audit-trail on`	監査証跡メッセージをイネーブルにします。 • パラメータマップに対する監査証跡を有効にして、接続またはセッションの開始、停止、および継続時間、および送信元と宛先の IP アドレスを記録できます。
ステップ 5	**alert on** 例： `Device(config-profile)# alert on`	コンソールに表示されるステートフル パケット インスペクション アラート メッセージをイネーブルにします。
ステップ 6	**one-minute** {**low** *number-of-connections* | **high** *number-of-connections*} 例： `Device(config-profile)# one-minute high 10000`	システムによるハーフオープン セッションの削除の開始と停止を起動する新規の未確立セッションの数を定義します。
ステップ 7	**tcp max-incomplete host** しきい値 例： `Device(config-profile)# tcp max-incomplete host 100`	TCP ホスト固有のサービス妨害（DoS）の検出および回避のために、しきい値とブロックする時間値を指定します。
ステップ 8	**exit** 例： `Device(config-profile)# exit`	パラメータマップ タイプ検査コンフィギュレーション モードを終了して、グローバル コンフィギュレーション モードに戻ります。

	コマンドまたはアクション	目的
ステップ 9	**policy-map type inspect** *policy-map-name* 例： `Device(config)# policy-map type inspect policy-map-hsl`	検査タイプ ポリシー マップを作成して、ポリシー マップ コンフィギュレーション モードを開始します。
ステップ 10	**class type inspect** *class-map-name* 例： `Device(config-pmap)# class type inspect class-map-tcp`	アクションを実行する対象のトラフィック クラスを指定し、ポリシー マップ クラス コンフィギュレーション モードを開始します。
ステップ 11	**inspect** *parameter-map-name* 例： `Device(config-pmap-c)# inspect parameter-map-hsl`	（任意）ステートフル パケット インスペクションをイネーブルにします。
ステップ 12	**end** 例： `Device(config-pmap-c)# end`	ポリシー マップ クラス コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

ファイアウォール高速ロギングの設定例

例：グローバル パラメータ マップの高速ロギングの有効化

次に、ドロップされたパケットのロギングを有効にし、NetFlow バージョン 9 形式のエラー メッセージを外部 IP アドレスに記録する例を示します。

```
Device# configure terminal
Device(config)# parameter-map type inspect global
Device(config-profile)# log dropped-packets
Device(config-profile)# log flow-export v9 udp destination 10.0.2.0 5000
Device(config-profile)# log flow-export template timeout-rate 5000
Device(config-profile)# end
```

例：ファイアウォール アクションの高速ロギングの有効化

次に、inspect-type parameter-map parameter-map-hsl の高速ロギング（HSL）を設定する例を示します。

```
Device# configure terminal
Device(config)# parameter-map type inspect parameter-map-hsl
Device(config-profile)# audit trail on
Device(config-profile)# alert on
Device(config-profile)# one-minute high 10000
Device(config-profile)# tcp max-incomplete host 100
Device(config-profile)# exit
```

```
Device(config)# poliy-map type inspect policy-map-hsl
Device(config-pmap)# class type inspect class-map-tcp
Device(config-pmap-c)# inspect parameter-map-hsl
Device(config-pmap-c)# end
```

ファイアウォール高速ロギングに関する追加情報

関連資料

関連項目	マニュアル タイトル
セキュリティ コマンド	• 『Cisco IOS Security Command Reference: Commands A to C』[英語] • 『Cisco IOS Security Command Reference: Commands D to L』[英語] • 『Cisco IOS Security Command Reference: Commands M to R』 • 『Cisco IOS Security Command Reference: Commands S to Z』[英語]

シスコのテクニカル サポート

説明	リンク
右の URL にアクセスして、シスコのテクニカル サポートを最大限に活用してください。これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

第 144 章

TCP リセット セグメント制御

TCP リセットセグメント制御機能は、ハーフクローズ、ハーフオープン、またはアイドルセッションに対して、セッション削除が発生したときに TCP リセット（RST）セグメントを送信する必要があるかどうかを設定するメカニズムを提供します。

TCP リセット セグメント制御について

TCP リセット セグメント制御

TCP ヘッダーには、リセット（RST）フラグというフラグが含まれます。TCP セグメントは、参照される接続の条件を満たしていないセグメントが到着するたびに、RST フラグとともに送信されます。たとえば、接続要求が宛先ポートで受信されたにもかかわらず、そのポートでリッスンしているプロセスがない場合、TCP セグメントは RST フラグとともに送信されます。

この動作は、ホスト間通信用に RFC 793 の伝送制御プロトコルで定義され、さまざまなベンダーによって実装されています。ただし、ホスト間のネットワークにあるネットワークデバイスに関しては、セッション（ハーフオープン、アイドル、ハーフクローズ）のクリア時に、デバイスが接続の発信側、受信側、またはその両方に TCP RST セグメントを送信する必要があるかどうかを判別するための特定の規則が定義されていません。一部のデバイスはセッションのクリア時に送信側と受信側の両方のポートに TCP RST セグメントを送信しますが、TCP RST セグメントを送信せずにセッションテーブルのセッションを暗黙的に削除するデバイスもあります。

TCP リセットセグメント制御機能は、ハーフクローズ、ハーフオープン、またはアイドルセッションに対して、セッションがクリアされるときに TCP RST セグメントを送信する必要があるかどうかを設定するメカニズムを提供します。

ハーフオープン セッションは TCP 同期（SYN）セグメントによって開始された未確立のセッションで、TCP スリーウェイ ハンドシェイクのみが発生し、タイマーが開始されるため、不完全です。

TCPは、接続の一端で出力を終了すると同時に、接続のもう他端からデータを受信し続ける機能を提供します。この TCP 状態は、ハーフクローズと呼ばれます。セッションは最初の TCP FINセグメントを受信し、タイマーが起動すると、ハーフクローズ状態になります。セッションがタイム アウトになる前に別のセグメントを受信した場合、タイマーが再開されます。

ハーフオープンおよびハーフクローズのセッションのタイムアウト値は、それぞれ **tcp synwait-time** コマンドと **tcp finwait-time** コマンドを使用して設定できます。デフォルトのタイムアウト値は 30 秒です。

アイドル セッションは、2 つのデバイス間でアクティブで、長時間どちらのデバイスからもデータが送信されていない TCP セッションです。アイドルセッションのタイムアウト値は、**tcp idle-time** コマンドを使用して設定できます。アイドル セッションのデフォルトのタイムアウト値は 3600 秒です。

TCPセッションでタイムアウトが発生し、セッションがクリアされると、TCP RSTセグメントが送信され、セッションに TCP リセット セグメント制御が設定されている場合に限り、セッションがリセットされます。

TCP リセット セグメント制御の設定方法

ハーフオープン セッションの TCP リセットの設定

ハーフオープンセッションとは、TCP同期（SYN）セグメントによって開始されたが、3 ウェイ ハンドシェイクがまだ完了していない未確立セッションです。未完了 3 ウェイ ハンドシェイクが発生すると、ただちにタイマーが開始します。**tcp synwait-time** コマンドを使用すると、ハーフオープン セッション タイムアウトのタイマー値を設定できます。このようなセッションのデフォルト タイムアウト値は 30 秒です。

ハーフオープンTCPセッションでタイムアウトが発生してセッションがクリアされると、セッションで TCP リセット セグメント制御が設定されている場合にのみ、TCP リセット（RST）セグメントが送信されてセッションがリセットされます。

tcp half-open reset on コマンドを設定すると、セッションがクリアされたときにハーフオープンセッションの両端に TCP RST セグメントが送信されます。**tcp half-open reset off** コマンドを設定すると、セッションがクリアされても TCP RST セグメントは伝送されません。

手順の概要

1. **enable**
2. **configure terminal**
3. **parameter-map type inspect** *parameter-map-name*
4. **tcp synwait-time** *seconds*
5. **tcp half-open reset** {**off** | **on**}

6. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**parameter-map type inspect** *parameter-map-name* 例： `Device(config)# parameter-map type inspect pmap-name`	（任意）接続しきい値、タイムアウト、その他の **inspect** キーワードに関連するパラメータに対する検査パラメータマップを設定し、パラメータマップタイプ検査コンフィギュレーション モードを開始します。
ステップ 4	**tcp synwait-time** *seconds* 例： `Device(config-profile)# tcp synwait-time 10`	セッションをドロップする前に、TCP セッションが確立状態になるのを待機する時間を指定します。
ステップ 5	**tcp half-open reset** {**off** | **on**} 例： `Device(config-profile)# tcp half-open reset on`	ハーフオープンセッションのタイムアウトが発生してセッションがクリアされた場合に、TCP RST セグメントが送信されるかどうかを指定します。
ステップ 6	**end** 例： `Device(config-profile)# end`	パラメータ マップ タイプ検査コンフィギュレーション モードを終了し、特権 EXEC モードを開始します。

ハーフクローズ セッションの TCP リセットの設定

TCP では、接続の一方の終端が出力を終了しても、接続のもう一方の終端から引き続きデータを受信することができます。この TCP 状態は、ハーフクローズと呼ばれます。セッションは最初の TCP 終了（FIN）セグメントを受信するとハーフクローズ状態になり、タイマーを開始します。セッションがタイムアウトになる前に別のセグメントを受信した場合、タイマーが再開されます。**tcp finwait-time** コマンドを使用すると、ハーフクローズセッションのタイムアウト値を設定できます。ハーフクローズ セッションのデフォルト タイムアウト値は 30 秒です。

ハーフクローズ TCP セッションでタイムアウトが発生すると、セッションで TCP リセット セグメント制御が設定されている場合にのみ、TCP RST セグメントが送信されてセッションがリセットされます。

tcp half-close reset on コマンドを設定すると、タイムアウトが発生してセッションがクリアされたときに、ハーフオープンセッションの両端に TCP RST セグメントが送信されます。**tcp half-close reset off** コマンドを設定すると、セッションタイムアウトが発生してセッションがクリアされたときに TCP RST セグメントが伝送されません。

手順の概要

1. **enable**
2. **configure terminal**
3. **parameter-map type inspect** *parameter-map-name*
4. **tcp finwait-time** *seconds*
5. **tcp half-close reset** {**off** | **on**}
6. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**parameter-map type inspect** *parameter-map-name* 例： `Device(config)# parameter-map type inspect pmap-name`	接続しきい値、タイムアウト、その他の **inspect** キーワードに関連するパラメータに対する検査パラメータマップを設定し、パラメータマップタイプ検査コンフィギュレーション モードを開始します。
ステップ 4	**tcp finwait-time** *seconds* 例： `Device(config-profile)# tcp finwait-time 10`	（任意）ファイアウォールが FIN-exchange を検出してから TCP セッションが管理される時間を指定します。
ステップ 5	**tcp half-close reset** {**off** | **on**} 例： `Device(config-profile)# tcp half-close reset on`	ハーフオープンセッションでセッション削除が発生した場合に TCP RST セグメントが送信されるかどうかを指定します。
ステップ 6	**end** 例： `Device(config-profile)# end`	パラメータ マップ タイプ検査コンフィギュレーション モードを終了し、特権 EXEC モードを開始します。

アイドル セッションの TCP リセットの設定

アイドルセッションとは、2つのデバイス間でアクティブな、長時間にわたっていずれのデバイスからもデータが送信されない TCP セッションです。アイドルセッションのタイムアウト値は、**tcp idle-time** コマンドを使用して設定できます。アイドル セッションのデフォルトのタイムアウト値は 3600 秒です。

アイドル TCP セッションでタイムアウトが発生すると、セッションで TCP リセット セグメント制御が設定されている場合には TCP RST セグメントが送信され、セッションがリセットされます。

tcp idle reset on コマンドを設定すると、タイムアウトが発生してセッションがクリアされたときに、アイドルセッションの両端に TCP RST セグメントが送信されます。**tcp idle reset off** コマンドを設定すると、セッションタイムアウトが発生してセッションがクリアされたときに TCP RST セグメントが伝送されません。

手順の概要

1. **enable**
2. **configure terminal**
3. **parameter-map type inspect** *parameter-map-name*
4. **tcp idle-time** *seconds*
5. **tcp idle reset** {**off** | **on**}
6. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**parameter-map type inspect** *parameter-map-name* 例： `Device(config)# parameter-map type inspect pmap-name`	接続しきい値、タイムアウト、その他の **inspect** キーワードに関連するパラメータに対する検査パラメータマップを設定し、パラメータマップタイプ検査コンフィギュレーション モードを開始します。
ステップ 4	**tcp idle-time** *seconds* 例： `Device(config-profile)# tcp idle-time 90`	（任意）TCP セッションのタイムアウトを設定します。

	コマンドまたはアクション	目的
ステップ 5	**tcp idle reset** {**off** | **on**} 例： `Device(config-profile)# tcp idle reset on`	アイドルセッションでセッション削除が発生した場合にTCP RSTセグメントが送信されるかどうかを指定します。
ステップ 6	**end** 例： `Device(config-profile)# end`	パラメータ マップ タイプ検査コンフィギュレーション モードを終了し、特権 EXEC モードを開始します。

TCP リセット セグメント制御の設定例

例：ハーフオープン セッションの TCP リセットの設定

```
Device> enable
Device# configure terminal
Device(config)# parameter-map type inspect pmap-name
Device(config-profile)# tcp synwait-time 10
Device(config-profile)# tcp half-open reset on
Device(config-profile)# end
```

例：ハーフクローズ セッションの TCP リセットの設定

```
Device> enable
Device# configure terminal
Device(config)# parameter-map type inspect pmap-name
Device(config-profile)# tcp finwait-time 10
Device(config-profile)# tcp half-close reset on
Device(config-profile)# end
```

例：アイドル セッションの TCP リセットの設定

```
Device> enable
Device# configure terminal
Device(config)# parameter-map type inspect pmap-name
Device(config-profile)# tcp idle-time 90
Device(config-profile)# tcp idle reset on
Device(config-profile)# end
```

TCP リセット セグメント制御に関する追加情報

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『Cisco IOS Master Command List, All Releases』
ファイアウォール コマンド	• 『Cisco IOS Security Command Reference: Commands A to C』 • 『Cisco IOS Security Command Reference: Commands D to L』 • 『Cisco IOS Security Command Reference: Commands M to R』 • 『Cisco IOS Security Command Reference: Commands S to Z』

標準および RFC

標準/RFC	タイトル
RFC 793	『Transmission Control Protocol』

シスコのテクニカル サポート

説明	リンク
右の URL にアクセスして、シスコのテクニカル サポートを最大限に活用してください。これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

TCP リセット セグメント制御に関する機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *197 : TCP* リセット セグメント制御に関する機能情報

機能名	リリース	機能情報
TCP リセット セグメント制御	Cisco IOS XE リリース 3.8S	TCP リセット セグメント制御機能は、ハーフオープン、ハーフクローズ、およびアイドル セッションに関するセッションがクリアされたときに TCP RST ビットが送出されるように設定するための一貫したメカニズムを提供します。 次のコマンドが導入または変更されました。**tcp idle reset**、**tcp half-close reset**、**tcp half-open reset**

第 145 章

ゾーンベース ポリシー ファイアウォールでの TCP ウィンドウ スケーリングのルーズ チェック オプション

ゾーンベース ポリシー ファイアウォール機能の TCP ウィンドウ スケーリング オプションのルーズ チェックは、ファイアウォールでの TCP ウィンドウ スケーリング オプションの厳格なチェックを無効にします。

ゾーンベース ポリシー ファイアウォールでの TCP ウィンドウ スケーリングのルーズ チェック オプションに関する情報

TCP ウィンドウ スケーリングのルーズ チェック オプションの概要

TCP は、高帯域幅および高速データ パスでのパフォーマンスを向上させる、さまざまな TCP 拡張機能を提供しています。このような拡張機能の 1 つが、TCP ウィンドウ スケーリング オプションです。TCP ウィンドウ スケーリングのルーズ チェック オプションは、RFC 1323 に記述されているウィンドウ スケーリング オプションの厳密なチェックを無効にします。

広帯域高遅延ネットワーク（LFN）と呼ばれる大きな帯域遅延積の特性を持つネットワーク経路での TCP のパフォーマンスを改善するため、より大きなウィンドウ サイズが推奨されます。

TCP ウィンドウ スケーリングにより、TCP ウィンドウの定義は 32 ビットに拡大され、スケール ファクタを使用して TCP ヘッダーの 16 ビット ウィンドウ フィールドでこの 32 ビットの値を伝送します。ウィンドウ サイズはスケール係数 14 まで大きくすることができます。典型的なアプリケーションは、広帯域高遅延ネットワークで動作するときにスケール係数 3 を使います。

ファイアウォールの実装により、TCP ウィンドウ スケーリング オプションの厳密なチェックが適用されます。この場合、ファイアウォールは、TCP スリーウェイ ハンドシェイクの初期同期（SYN）パケットで TCP ウィンドウ スケーリング オプションを受信しなかった場合、TCP ウィンドウ スケーリング オプションを使用する SYN/ACK パケットをドロップします。ウィンドウ スケーリング オプションは SYN ビットがオンに設定された SYN セグメントでのみ送信されます。したがって、接続のオープン時にウィンドウ スケールが各方向で固定されます。

tcp window-scale-enforcement loose コマンドを使用すると、TCP SYN セグメントでの TCP ウィンドウ スケーリング オプションの厳格なチェックが無効になります。

ゾーンベース ポリシー ファイアウォールでの TCP ウィンドウ スケーリングのルーズ チェック オプションの設定方法

ファイアウォールの TCP ウィンドウ スケーリング オプションの設定

手順の概要

1. **enable**
2. **configure terminal**
3. **parameter-map type inspect** {*parameter-map-name* | **global** | **default**}
4. **tcp window-scale-enforcement loose**
5. **exit**
6. **class-map type inspect** {**match-any** | **match-all**} *class-map-name*
7. **match protocol** [*parameter-map*] [**signature**]
8. **exit**
9. **policy-map type inspect***policy-map-name*
10. **class type inspect** *class-map-name*
11. **inspect** [*parameter-map-name*]
12. **exit**
13. **class** *name*
14. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**parameter-map type inspect** {*parameter-map-name* | **global** | **default**} 例： `Device(config)# parameter-map type inspect pmap-fw`	検査パラメータ マップを設定し、プロファイル コンフィギュレーション モードを開始します。
ステップ 4	**tcp window-scale-enforcement loose** 例： `Device(config-profile)# tcp window-scale-enforcement loose`	ファイアウォールでの TCP ウィンドウ スケーリング オプションの厳密なチェックを無効にします。
ステップ 5	**exit** 例： `Device(config-profile)# exit`	プロファイル コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードに戻ります。
ステップ 6	**class-map type inspect** {**match-any** | **match-all**} *class-map-name* 例： `Device(config)# class-map type inspect match-any internet-traffic-class`	検査タイプ クラス マップを作成して、QoS クラス マップ コンフィギュレーション モードを開始します。
ステップ 7	**match protocol** [*parameter-map*] [**signature**] 例： `Device(config-cmap)# match protocol tcp`	指定されたプロトコルに基づいてクラス マップの一致基準を設定します。
ステップ 8	**exit** 例： `Device(config-cmap)# exit`	QoS クラス マップ コンフィギュレーション モードを終了し、グローバルコンフィギュレーションモードに戻ります。
ステップ 9	**policy-map type inspect***policy-map-name* 例： `Device(config)# policy-map type inspect private-internet-policy`	検査タイプ ポリシー マップを作成して、QoS ポリシー マップ コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 10	**class type inspect** *class-map-name* 例： `Device(config-pmap)# class type inspect internet-traffic-class`	アクションを実行する対象のトラフィック クラスを指定し、ポリシー マップ クラス コンフィギュレーション モードを開始します。
ステップ 11	**inspect** [*parameter-map-name*] 例： `Device(config-pmap-c)# inspect pmap-fw`	ステートフル パケット インスペクションをイネーブルにします。
ステップ 12	**exit** 例： `Device(config-pmap-c)# exit`	QoS ポリシー マップ クラス コンフィギュレーション モードを終了し、QoS ポリシー マップ コンフィギュレーション モードに戻ります。
ステップ 13	**class** *name* 例： `Device(config-pmap)# class class-default`	指定したデータリンク接続識別子（DLCI）にマップ クラスを関連付けます。
ステップ 14	**end** 例： `Device(config-pmap)# end`	QoS ポリシー マップ コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

TCP ウィンドウ スケーリングのゾーンとゾーン ペアの設定

手順の概要

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **ip address** *ip-address*
5. **zone-member security** *security-zone-name*
6. **exit**
7. **interface** *type number*
8. **ip address** *ip-address*
9. **zone-member security** *security-zone-name*
10. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。

	コマンドまたはアクション	目的
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface** *type number* 例： `Device(config)# interface GigabitEthernet 0/1/5`	インターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	**ip address** *ip-address* 例： `Device(config-if)# ip address 10.1.1.1 255.255.255.0`	インターフェイス IP アドレスを割り当てます。
ステップ 5	**zone-member security** *security-zone-name* 例： `Device(config-if)# zone-member security private`	インターフェイスをゾーン メンバーとして設定します。
ステップ 6	**exit** 例： `Device(config-if)# exit`	インターフェイス設定モードを終了し、グローバル設定モードに戻ります。
ステップ 7	**interface** *type number* 例： `Device(config)# interface GigabitEthernet 0/1/6`	インターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 8	**ip address** *ip-address* 例： `Device(config-if)# ip address 209.165.200.225 255.255.255.0`	IP アドレスをインターフェイスに割り当てます。
ステップ 9	**zone-member security** *security-zone-name* 例： `Device(config-if)# zone-member security internet`	インターフェイスをゾーン メンバーとして設定します。
ステップ 10	**end** 例： `Device(config-if)# end`	インターフェイス コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

TCP ウィンドウ スケーリングの設定例

例：ファイアウォールの TCP ウィンドウ スケーリング オプションの設定

```
Device> enable
Device# configure terminal
Device(config)# parameter-map type inspect pmap-fw
Device(config-profile)# tcp window-scale-enforcement loose
Device(config-profile)# exit
Device(config)# class-map type inspect match-any internet-traffic-class
Device(config-cmap)# match protocol tcp
Device(config-cmap)# exit
Device(config)# policy-map type inspect private-internet-policy
Device(config-pmap)# class type inspect internet-traffic-class
Device(config-pmap-c)# inspect pmap-fw
Device(config-pmap-c)#exit
Device(config-pmap)# class class-default
Device(config-pmap)#end
```

例：TCP ウィンドウ スケーリングのゾーンとゾーン ペアの設定

```
Device# enable
Device# configure terminal
Device(config)# interface GigabitEthernet 0/1/5
Device(config-if)# ip address 10.1.1.1 255.255.255.0
Device(config-if)# zone-member security private
Device(config-if)# exit
Device(config)# interface GigabitEthernet 0/1/6
Device(config-if)# ip address 209.165.200.225 255.255.255.0
Device(config-if)# zone-member security internet
Device(config-if)# end
```

ゾーンベース ポリシー ファイアウォールでの TCP ウィンドウ スケーリングのルーズ チェック オプションに関する機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *198*：ゾーンベース ポリシー ファイアウォールでの *TCP* ウィンドウ スケーリングのルーズ チェック オプションに関する機能情報

機能名	リリース	機能情報
ゾーンベースポリシーファイアウォールでの TCP ウィンドウ スケーリングのルーズ チェック オプション	Cisco IOS XE リリース 3.10S	ゾーンベース ポリシー ファイアウォールでの TCP ウィンドウ スケーリングのルーズ チェック オプション機能は、IOS-XE ファイアウォール内の TCP ウィンドウ スケーリング オプションの厳密なチェックを無効にします。 次のコマンドが導入または変更されました。**tcp window-scale-enforcement loose** Cisco IOS XE リリース 3.10S で、Cisco CSR 1000 シリーズルータのサポートが追加されました。

第 146 章

ゾーンベース ポリシー ファイアウォールでの ALG と AIC の有効化

ゾーンベース ポリシー ファイアウォールでは、アプリケーション レベル ゲートウェイ（ALG）およびアプリケーション インスペクションおよびコントロール（AIC）と、レイヤ 7 アプリケーション プロトコル インスペクションがサポートされています。レイヤ 7 アプリケーション プロトコル インスペクションを使用すると、セキュリティ モジュールを通過するプロトコルの動作の確認や、不要なトラフィックや悪意のあるトラフィックの識別が可能です。

ゾーンベース ポリシー ファイアウォールでの ALG および AIC の有効化機能の導入前は、ALG/AIC 設定とともにレイヤ 7 プロトコル インスペクションが自動的に有効になりました。この機能を使用すると、**no application-inspect** コマンドを使用して、レイヤ 7 インスペクションを有効または無効にすることができます。

このモジュールでは、ゾーンベース ポリシー ファイアウォールでの ALG および AIC の有効化機能について概説し、この機能を設定する方法について説明します。

ゾーンベース ポリシー ファイアウォールでの ALG と AIC の有効化に関する情報

アプリケーション レベル ゲートウェイ

アプリケーション レベル ゲートウェイ（ALG）は、アプリケーション レイヤ ゲートウェイとも呼ばれ、アプリケーションパケットのペイロード内のIPアドレス情報を変換するアプリケーションです。ALG は、アプリケーション レイヤ プロトコルを解釈し、ファイアウォールおよびネットワーク アドレス変換（NAT）アクションを実行するために使用されます。これらのアクションは、ファイアウォールおよび NAT の設定に応じて次の 1 つまたは複数のアクションになります。

- クライアント アプリケーションが、ダイナミック TCP または UDP ポートを使用してサーバ アプリケーションと通信できるようにします。
- アプリケーション固有のコマンドを認識し、これらのコマンドに対するきめ細かいセキュリティ制御を提供します。
- データ交換を行う 2 つのホスト間の複数のデータ ストリームまたはデータ セッションを同期します。
- アプリケーション ペイロードで使用できるネットワーク層アドレス情報を変換します。

ファイアウォールがピンホールを開き、アプリケーション レイヤ データストリームの送信元 IP アドレスおよび宛先 IP アドレスを伝送しない TCP または UDP トラフィックに対する変換サービスをNATが実行します。IPアドレス情報を埋め込む特定のプロトコルまたはアプリケーションには ALG のサポートが必要です。

レイヤ7アプリケーション プロトコル インスペクションの有効化の概要

ゾーンベース ポリシー ファイアウォールでは、アプリケーション レベル ゲートウェイ（ALG）およびアプリケーション インスペクションおよびコントロール（AIC）と、レイヤ 7 プロトコル インスペクションがサポートされています。レイヤ 7 プロトコル インスペクションは ALG/AIC 設定とともに自動的に有効になります。

レイヤ 7 アプリケーション プロトコル インスペクションは、アプリケーション層プロトコルを解釈または理解し、適切なファイアウォールまたはネットワーク アドレス変換（NAT）アクションを実行する手法です。アプリケーションによっては、パケットがデバイスのセキュリティ モジュールを通過する際、パケットのデータ部分に特別な処理をする必要があります。レイヤ 7 アプリケーション プロトコル インスペクションを使用すると、セキュリティ モジュールを通過するプロトコルの動作の確認や、不要なトラフィックや悪意のあるトラフィックの識別が可能です。セキュリティ モジュールは、設定されているトラフィック ポリシーに基づい

てパケットの受け入れまたは拒否を行い、アプリケーションおよびサービスを安全に使用できるようにします。

アプリケーション インスペクションの実装の問題が原因で、アプリケーション パケットがドロップされることや、ネットワークが不安定になることがあります。ゾーンベース ポリシー ファイアウォールでの ALG および AIC の有効化機能の導入前は、アプリケーション インスペクションを無効にするには、ターゲット レイヤ 7 プロトコル ポートを使用してアクセス コントロール リスト（ACL）を定義し、特定のレイヤ7プロトコルのインスペクションをバイパスするために、この ACL と、TCP または UDP プロトコルに一致するクラス マップを定義する必要がありました。

ゾーンベース ポリシー ファイアウォールでの ALG および AIC の有効化機能が導入されたことで、**application-inspect** コマンドを使用して、特定のプロトコルまたはサポートされているすべてのレイヤ7プロトコルに対して、レイヤ7プロトコルインスペクションを有効または無効にできます。パラメータ マップの設定の変更は、新しいセッションにのみ適用されます。たとえば、FTP レイヤ 7 インスペクションを無効にすると、新規に作成されたセッションは FTP レイヤ7インスペクションをスキップしますが、この設定変更前にすでに確立されていた既存のセッションはFTP レイヤ7インスペクションを実行します。すべてのセッションで設定の変更を行う場合は、すべてのセッションを削除してから再作成する必要があります。

レイヤ 7 アプリケーション プロトコル インスペクションは、個々のパラメータ マップまたはグローバル ファイアウォールに対して有効にできます。

ゾーンベース ポリシー ファイアウォールでの ALG と AIC の有効化方法

ファイアウォールのレイヤ7アプリケーション プロトコル インスペクションの有効化

アプリケーション プロトコル インスペクションはデフォルトではイネーブルです。**no application-inspect** コマンドを使用して、アプリケーション プロトコル インスペクションを無効にします。

何らかの理由でアプリケーション プロトコル インスペクションを無効化した場合、**application-inspect** コマンドを使用して再設定します。**application-inspect** コマンドを設定する前に、**parameter-map type inspect** コマンドまたは **parameter-map type inspect-global** コマンドのいずれかを設定します。

いつでも **parameter-map type inspect** コマンドまたは **parameter-map type inspect-global** コマンドのいずれかのみを設定できます。

使用

手順の概要

1. **enable**
2. **configure terminal**
3. 次のいずれかを実行します。
   - **parameter-map type inspect** *parameter-map-name*
   - **parameter-map type inspect-global**
4. **application-inspect** {**all** | *protocol-name*}
5. **exit**
6. **class-map type inspect** {**match-all** | **match-any**} *class-map-name*
7. **match protocol** *protocol-name*
8. **exit**
9. **policy-map type inspect** *policy-map-name*
10. **class type inspect** {*class-map-name* | **class-default**}
11. **inspect** *parameter-map-name*
12. **exit**
13. **class** {*class-map-name* | **class-default**}
14. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。

ステップ 3	次のいずれかを実行します。
	• **parameter-map type inspect** *parameter-map-name*
	• **parameter-map type inspect-global**
	例：
	`Device(config)# parameter-map type inspect pmap-fw`
	または
	`Device(config)# parameter-map type inspect-global`
		• （任意）接続しきい値、タイムアウト、およびその他の検査アクションに関連するパラメータに対して、ファイアウォールの検査タイプ パラメータ マップを有効にして、パラメータ マップ タイプ検査コンフィギュレーション モードを開始します。
		• （任意）グローバル パラメータ マップを有効にし、パラメータ マップ タイプ検査コンフィギュレーション モードを開始します。

ステップ 4	**application-inspect** {**all**	*protocol-name*} 例： `Device(config-profile)# application-inspect msrpc`	指定されたプロトコルについてアプリケーション インスペクションをイネーブルにします。

	コマンドまたはアクション	目的
ステップ 5	**exit** 例： `Device(config-profile)# exit`	パラメータ マップ タイプ検査コンフィギュレーション モードを終了して、グローバル コンフィギュレーション モードに戻ります。
ステップ 6	**class-map type inspect** {**match-all** | **match-any**} *class-map-name* 例： `Device(config)# class-map type inspect match-any internet-traffic-class`	検査タイプ クラス マップを作成し、クラス マップ コンフィギュレーション モードを開始します。
ステップ 7	**match protocol** *protocol-name* 例： `Device(config-cmap)# match protocol msrpc`	指定したプロトコルに基づいてクラス マップの一致基準を設定します。
ステップ 8	**exit** 例： `Device(config-cmap)# exit`	クラス マップ コンフィギュレーション モードを終了して、グローバル コンフィギュレーション モードに戻ります。
ステップ 9	**policy-map type inspect** *policy-map-name* 例： `Device(config)# policy-map type inspect private-internet-policy`	検査タイプ ポリシー マップを作成し、ポリシー マップ コンフィギュレーション モードを開始します。
ステップ 10	**class type inspect** {*class-map-name* | **class-default**} 例： `Device(config-pmap)# class type inspect internet-traffic-class`	アクションを実行する対象のトラフィック クラスを指定し、ポリシー マップ クラス コンフィギュレーション モードを開始します。
ステップ 11	**inspect** *parameter-map-name* 例： `Device(config-pmap-c)# inspect pmap-fw`	ステートフル パケット インスペクションをイネーブルにします。
ステップ 12	**exit** 例： `Device(config-pmap-c)# exit`	ポリシー マップ クラス コンフィギュレーション モードを終了して、ポリシー マップ コンフィギュレーション モードに戻ります。
ステップ 13	**class** {*class-map-name* | **class-default**} 例： `Device(config-pmap)# class class-default`	ポリシーを設定または変更できるようデフォルト クラスを指定します。
ステップ 14	**end** 例： `Device(config-pmap)# end`	ポリシー マップ コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

レイヤ7アプリケーション プロトコル インスペクションを有効にするためのゾーンの設定

手順の概要

1. **enable**
2. **configure terminal**
3. **zone security** {**default** | *security-zone*}
4. **exit**
5. **zone security** {**default** | *security-zone*}
6. **exit**
7. **zone-pair security** *zone-pair* **source** *source-zone* **destination** *destination-zone*
8. **service-policy type inspect** *policy-map-name*
9. **exit**
10. **interface** *type number*
11. **zone-member security** *security-zone*
12. **exit**
13. **interface** *type number*
14. **zone-member security** *security-zone*
15. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**zone security** {**default** | *security-zone*} 例： `Device(config)# zone security private`	インターフェイスを割り当てることができるセキュリティ ゾーンを作成し、セキュリティ ゾーン コンフィギュレーション モードを開始します。 • 送信元ゾーンと宛先ゾーンという、ゾーン ペアを作成するための 2 つのセキュリティ ゾーンが必要です。
ステップ 4	**exit** 例： `Device(config-sec-zone)# exit`	セキュリティ ゾーン コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードに戻ります。

	コマンドまたはアクション	目的
ステップ 5	**zone security** {**default** | *security-zone*} 例： `Device(config)# zone security internet`	インターフェイスを割り当てることができるセキュリティ ゾーンを作成し、セキュリティ ゾーン コンフィギュレーション モードを開始します。
ステップ 6	**exit** 例： `Device(config-sec-zone)# exit`	セキュリティ ゾーン コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードに戻ります。
ステップ 7	**zone-pair security** *zone-pair* **source** *source-zone* **destination** *destination-zone* 例： `Device(config)# zone-pair security private-internet source private destination internet`	ゾーン ペアを作成し、セキュリティ ゾーンペア コンフィギュレーション モードを開始します。
ステップ 8	**service-policy type inspect** *policy-map-name* 例： `Device(config-sec-zone-pair)# service-policy type inspect private-internet-policy`	ファイアウォール ポリシー マップを宛先ゾーン ペアに付加します。 • ゾーンのペア間でポリシーが設定されない場合、トラフィックはデフォルトでドロップされます。
ステップ 9	**exit** 例： `Device(config-sec-zone-pair)# exit`	セキュリティ ゾーン ペア コンフィギュレーション モードを終了し、グローバルコンフィギュレーション モードに戻ります。
ステップ 10	**interface** *type number* 例： `Device(config)# interface gigabitethernet 0/0/0`	インターフェイスを設定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 11	**zone-member security** *security-zone* 例： `Device(config-if)# zone-member security private`	インターフェイスを指定したセキュリティ ゾーンに割り当てます。 • インターフェイスをセキュリティ ゾーンのメンバーにした場合、そのインターフェイスを通して送受信されるすべてのトラフィックは、デフォルトでドロップされます（ただしデバイス宛のトラフィックとデバイス発のトラフィックを除く）。トラフィックがインターフェイス通過するには、ゾーンをポリシーの適用先のゾーンペアの一部にする必要があります。ポリシーがトラフィックを許可すると、トラフィックはそのインターフェイスを通過できます。

	コマンドまたはアクション	目的
ステップ 12	**exit** 例： `Device(config-if)# exit`	インターフェイス設定モードを終了し、グローバル設定モードに戻ります。
ステップ 13	**interface** *type number* 例： `Device(config)# interface gigabitethernet 0/2/2`	インターフェイスを設定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 14	**zone-member security** *security-zone* 例： `Device(config-if)# zone-member security internet`	インターフェイスを指定したセキュリティ ゾーンに割り当てます。
ステップ 15	**end** 例： `Device(config-if)# end`	インターフェイス コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

ゾーンベース ポリシー ファイアウォールでの ALG と AIC の有効化の設定例

例：ファイアウォールでのレイヤ7アプリケーション プロトコル インスペクションの有効化

次に、**parameter-map type inspect** コマンドを設定した後に、レイヤ 7 アプリケーション プロトコル インスペクションを有効にする例を示します。**parameter-map type inspect-global** コマンドを設定した後でも、アプリケーション インスペクションを有効にすることができます。

いつでも **parameter-map type inspect** コマンドまたは **parameter-map type inspect-global** コマンドのいずれかのみを設定できます。

```
Device# configure terminal
Device(config)# parameter-map type inspect pmap-fw
Device(config-profile)# application-inspect msrpc
Device(config-profile)# exit
Device(config)# class-map type inspect match-any internet-traffic-class
Device(config-cmap)# match protocol msrpc
Device(config-cmap)# exit
Device(config)# policy-map type inspect private-internet-policy
Device(config-pmap)# class type inspect internet-traffic-class
Device(config-pmap-c)# inspect pmap-fw
Device(config-pmap-c)# exit
```

```
Device(config-pmap)# class class-default
Device(config-pmap)# end
```

例：レイヤ7アプリケーションプロトコルインスペクションを有効化するゾーンの設定

```
Device# configure terminal
Device(config)# zone security private
Device(config-sec-zone)# exit
Device(config)# zone security internet
Device(config-sec-zone)# exit
Device(config)# zone-pair security private-internet source private destination internet
Device(config-sec-zone-pair)# service-policy type inspect private-internet-policy
Device(config-sec-zone-pair)# exit
Device(config)# interface gigabitethernet 0/0/0
Device(config-if)# zone-member security private
Device(config-if)# exit
Device(config)# interface gigabitethernet 0/2/2
Device(config-if)# zone-member security internet
Device(config-if)# end
```

ゾーンベース ポリシー ファイアウォールでの ALG と AIC の有効化に関する追加情報

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『Cisco IOS Master Command List, All Releases』
ファイアウォール コマンド	• 『Cisco IOS Security Command Reference: Commands A to C』 • 『Cisco IOS Security Command Reference: Commands D to L』 • 『Cisco IOS Security Command Reference: Commands M to R』 • 『Cisco IOS Security Command Reference: Commands S to Z』

シスコのテクニカル サポート

説明	リンク
シスコのサポート Web サイトでは、シスコの製品やテクノロジーに関するトラブルシューティングにお役立ていただけるように、マニュアルやツールをはじめとする豊富なオンライン リソースを提供しています。 お使いの製品のセキュリティ情報や技術情報を入手するために、Cisco Notification Service（Field Notice からアクセス）、Cisco Technical Services Newsletter、Really Simple Syndication（RSS）フィードなどの各種サービスに加入できます。 シスコのサポート Web サイトのツールにアクセスする際は、Cisco.com のユーザ ID およびパスワードが必要です。	http://www.cisco.com/support

ゾーンベース ポリシー ファイアウォールでの ALG と AIC の有効化に関する機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *199* : ゾーンベース ポリシー ファイアウォールでの *ALG* と *AIC* の有効化に関する機能情報

機能名	リリース	機能情報
ゾーンベース ポリシー ファイアウォールでの ALG と AIC の有効化	Cisco IOS XE リリース 3.11S	ゾーンベース ポリシー ファイアウォールでは、アプリケーション レベル ゲートウェイ（ALG）およびアプリケーション インスペクションおよびコントロール（AIC）と、レイヤ 7 アプリケーション プロトコル インスペクションがサポートされています。レイヤ 7 アプリケーション プロトコル インスペクションは、プロトコル動作の確認と、セキュリティ モジュールを通過する不要なまたは悪意のあるトラフィックの識別を容易にします。 ゾーンベース ポリシー ファイアウォールでの ALG と AIC の有効化機能が導入される前は、レイヤ 7 プロトコル インスペクションが ALG/AI C 設定とともに自動的に有効になりました。この機能を使用すると、no application-inspect コマンドを使用して、レイヤ 7 インスペクションを有効または無効にすることができます。 Cisco IOS XE リリース 3.11S では、この機能が Cisco ASR 1000 シリーズ アグリゲーション サービス ルータ、Cisco 4400 シリーズ サービス統合型ルータ、およびシスコ クラウド サービス ルータ 1000V で導入されました。 次のコマンドが導入または変更されました。**application-inspect**、**show parameter-map type inspect**、および **show platform software firewall**。

第 147 章

ファイアウォール TCP SYN Cookie の設定

ファイアウォール TCP SYN Cookie 機能は、TCP SYN フラッディング攻撃からファイアウォールを保護します。TCP SYN フラッディング攻撃は、サービス妨害（DoS）攻撃の一種です。通常、TCP 同期（SYN）パケットは、ファイアウォールの背後にある対象のエンド ホストまたは一定範囲のサブネット アドレスに送信されます。これらの TCP SYN パケットによって、送信元 IP アドレスがスプーフィングされます。スプーフィング攻撃とは、個人またはプログラムが、データを改ざんして不正な優位性を獲得し、別のものになりすますことです。TCP SYN フラッディングは、ファイアウォールまたはエンドホスト上のすべてのリソースを占有し、そのために正当なトラフィックに対する DoS が発生します。ファイアウォールおよびファイアウォール背後のエンド ホストでの TCP SYN フラッディングを防ぐには、ファイアウォール TCP SYN Cookie 機能を設定する必要があります。

ファイアウォール TCP SYN Cookie の設定に関する制約事項

- デフォルトのゾーンはゾーン タイプのパラメータ マップをサポートしていないため、デフォルトのゾーンのファイアウォール TCP SYN Cookie 機能を設定することはできません。
- ファイアウォール TCP SYN Cookie 機能は、サブスクライバ単位のファイアウォールをサポートしていません。

ファイアウォール TCP SYN Cookie の設定について

TCP SYN フラッド攻撃

ファイアウォール TCP SYN Cookie 機能は、DoS 攻撃の一種である TCP SYN フラッディング攻撃からファイアウォールを保護するソフトウェアを実装します。

SYN フラッディング攻撃は、ハッカーがサーバに膨大な数の接続要求をフラッドすることによって発生します。これらのメッセージには到達不能の返信アドレスが含まれているため、接続を確立できません。未解決のオープン接続の数が増え、最終的にはサーバで処理しきれなくなり、有効な要求へのサービスが拒否されるようになるため、正当なユーザの Web サイトへの接続、電子メールのアクセス、FTP サービスの使用などが妨げられます。

SYN フラッド攻撃は、次の 2 つのタイプに分類されます。

- ホスト フラッド：SYN フラッド パケットが単一のホストに送信され、そのホスト上のすべてのリソースを使用することが意図されます。
- ファイアウォールセッションテーブルフラッド：SYNフラッドパケットはファイアウォールの背後のアドレスの範囲に送信され、ファイアウォール上のセッションテーブルリソースを枯渇させ、その結果、リソースの拒否がファイアウォールを通過するトラフィックを正当化することが意図されます。

ファイアウォール TCP SYN Cookie 機能は、TCP 接続要求を代行受信して検証することにより、SYNフラッディング攻撃を防止するのに役立ちます。ファイアウォールは、クライアントからサーバに送信される TCP SYN パケットを代行受信します。TCP SYN Cookie がトリガーされると、設定された VPN ルーティングおよび転送（VRF）またはゾーン宛てのすべての SYN パケットに作用します。TCP SYN Cookie は宛先サーバの代わりにクライアントとの接続を確立し、クライアントの代わりにサーバとの別の接続を確立して、2 つの半接続を透過的に結び付けます。したがって、到達不能なホストからの接続試行がサーバに到達することはありません。TCP SYN Cookie は接続されている間、パケットを代行受信および転送します。

ファイアウォール TCP SYN Cookie 機能は、グローバル ルーティング ドメインと VRF ドメインのセッション テーブル SYN フラッド保護を提供します。ファイアウォールはグローバル テーブルにセッションを保存するため、TCP ハーフオープン セッションの数に制限を設定できます。TCP ハーフオープン セッションは、確立状態に達していないセッションです。VRF 対応ファイアウォールでは、各 VRF の TCP ハーフオープン セッションの数に制限を設定できます。グローバル レベルと VRF レベルの両方で、設定済みの制限に達すると、TCP SYN Cookie はより多くのセッションを作成する前に、ハーフオープンセッションの送信元を確認します。

ファイアウォール TCP SYN Cookie の設定方法

ファイアウォール ホスト保護の設定

ホストのすべてのリソースを引き継ぐために、TCP SYN パケットが単一のホストに送信されます。ホスト保護は、送信元ゾーンに関してのみ設定可能です。宛先ゾーン設定で保護を設定しても、TCP SYN 攻撃から宛先ゾーンが保護されるわけではありません。

ファイアウォール ホスト保護を設定するには、次の作業を実行します。

（注） **show** コマンドは任意の順序で指定できます。

手順の概要

1. **enable**
2. **configure terminal**
3. **parameter-map type inspect-zone** *zone-pmap-name*
4. **tcp syn-flood rate per-destination** *maximum-rate*
5. **max-destination** *limit*
6. **exit**
7. **zone security** *zone-name*
8. **protection** *parameter-map-name*
9. **exit**
10. **show parameter-map type inspect-zone** *zone-pmap-name*
11. **show zone security**
12. **show policy-firewall stats zone** *zone-name*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 3	**parameter-map type inspect-zone** *zone-pmap-name* 例： `Router(config)# parameter-map type inspect-zone zone-pmap`	ゾーン検査タイプ パラメータ マップを設定し、プロファイル コンフィギュレーション モードを開始します。
ステップ 4	**tcp syn-flood rate per-destination** *maximum-rate* 例： `Router(config-profile)# tcp syn-flood rate per-destination 400`	各宛先アドレスの 1 秒あたりの SYN フラッド パケット数を設定します。 • 特定の宛先アドレスに送信される SYN パケットのレートが、宛先ごとの制限を超えた場合、ファイアウォールは宛先アドレスにルーティングされる SYN パケットの SYN Cookie 処理を開始します。
ステップ 5	**max-destination** *limit* 例： `Router(config-profile)# max-destination 10000`	ファイアウォールがゾーンで追跡できる宛先の最大数を設定します。 • *limit* 引数を使って設定された制限を最大宛先が超えた場合、ファイアウォールはSYNパケットをドロップします。
ステップ 6	**exit** 例： `Router(config-profile)# exit`	プロファイル コンフィギュレーション モードを終了して、グローバル コンフィギュレーション モードを開始します。
ステップ 7	**zone security** *zone-name* 例： `Router(config)# zone security secure-zone`	セキュリティ ゾーンを設定し、セキュリティ ゾーン コンフィギュレーション モードを開始します。
ステップ 8	**protection** *parameter-map-name* 例： `Router(config-sec-zone)# protection zone-pmap`	パラメータ マップを使用して指定のゾーンに関する保護を設定します。
ステップ 9	**exit** 例： `Router(config-sec-zone)# exit`	セキュリティ ゾーン コンフィギュレーションを終了し、特権 EXEC モードを開始します。
ステップ 10	**show parameter-map type inspect-zone** *zone-pmap-name* 例：	（任意）ゾーン検査タイプ パラメータ マップの詳細を表示します。

	コマンドまたはアクション	目的
	`Router# show parameter-map type inspect-zone zone-pmap`	
ステップ 11	**show zone security** 例： `Router# show zone security`	（任意）ゾーン セキュリティ情報を表示します。
ステップ 12	**show policy-firewall stats zone** *zone-name* 例： `Router# show policy-firewall stats zone secure-zone`	（任意）パケット制限を超えた、SYN Cookie によって処理された SYN パケットの数を表示します。

ファイアウォール セッション テーブル保護の設定

ファイアウォール上のセッションテーブルリソースを使い果たすことで、そのファイアウォールを通過する正当なトラフィックに対するサービスを拒否することを目的として、TCP SYN パケットがファイアウォール背後の一定範囲のアドレスに送信されます。グローバル ルーティング ドメインまたは VRF ドメインにファイアウォール セッション テーブル保護を設定できます。

グローバル ルーティング ドメインでのファイアウォール セッション テーブル保護の設定

グローバル ルーティング ドメインにファイアウォール セッション テーブル保護を設定するには、次の作業を実行します。

（注） グローバル パラメータ マップは、ルータ レベルではなく、グローバル ルーティング ドメインで有効になります。

手順の概要

1. **enable**
2. **configure terminal**
3. **parameter-map type inspect global**
4. **tcp syn-flood limit** *number*
5. **end**
6. **show policy-firewall stats vrf global**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**parameter-map type inspect global** 例： `Router(config)# parameter-map type inspect global`	グローバル パラメータ マップを設定し、プロファイル コンフィギュレーション モードを開始します。
ステップ 4	**tcp syn-flood limit** *number* 例： `Router(config-profile)# tcp syn-flood limit 500`	新しい SYN パケットの SYN Cookie 処理をトリガーする TCP ハーフ オープン セッション数を制限します。
ステップ 5	**end** 例： `Router(config-profile)# end`	プロファイル コンフィギュレーション モードを終了して、特権 EXEC モードを開始します。
ステップ 6	**show policy-firewall stats vrf global** 例： `Router# show policy-firewall stats vrf global`	（任意）グローバル VRF ファイアウォール ポリシーのステータスを表示します。 • また、存在する TCP ハーフ オープン セッションの数もコマンド出力に表示されます。

VRF ドメインでのファイアウォール セッション テーブル保護の設定

VRF ドメインにファイアウォール セッション テーブル保護を設定するには、次の作業を実行します。

（注） **show** コマンドは任意の順序で指定できます。

手順の概要

1. **enable**
2. **configure terminal**

3. **parameter-map type inspect-vrf** *vrf-pmap-name*
4. **tcp syn-flood limit** *number*
5. **exit**
6. **parameter-map type inspect global**
7. **vrf** *vrf-name* **inspect** *parameter-map-name*
8. **end**
9. **show parameter-map type inspect-vrf**
10. **show policy-firewall stats vrf** *vrf-name*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**parameter-map type inspect-vrf** *vrf-pmap-name* 例： `Router(config)# parameter-map type inspect-vrf vrf-pmap`	VRF 検査タイプ パラメータ マップを設定し、プロファイル コンフィギュレーション モードを開始します。
ステップ 4	**tcp syn-flood limit** *number* 例： `Router(config-profile)# tcp syn-flood limit 200`	新しい SYN パケットの SYN Cookie 処理をトリガーする TCP ハーフ オープン セッション数を制限します。
ステップ 5	**exit** 例： `Router(config-profile)# exit`	プロファイル コンフィギュレーション モードを終了して、グローバル コンフィギュレーション モードを開始します。
ステップ 6	**parameter-map type inspect global** 例： `Router(config)# parameter-map type inspect global`	VRF 検査タイプ パラメータ マップを VRF にバインドし、プロファイルコンフィギュレーションモードを開始します。
ステップ 7	**vrf** *vrf-name* **inspect** *parameter-map-name* 例： `Router(config-profile)# vrf vrf1 inspect vrf-pmap`	パラメータ マップを VRF にバインドします。

	コマンドまたはアクション	目的
ステップ 8	**end** 例： `Router(config-profile)# end`	プロファイル コンフィギュレーション モードを終了して、特権 EXEC モードを開始します。
ステップ 9	**show parameter-map type inspect-vrf** 例： `Router# show parameter-map type inspect-vrf`	（任意）VRF 検査タイプ パラメータ マップに関する情報を表示します。
ステップ 10	**show policy-firewall stats vrf** *vrf-name* 例： `Router# show policy-firewall stats vrf vrf-pmap`	（任意）VRF ファイアウォール ポリシーのステータスを表示します。 • また、存在する TCP ハーフ オープン セッションの数もコマンド出力に表示されます。

ファイアウォール TCP SYN Cookie の設定例

ファイアウォール ホスト保護の設定例

次に、ファイアウォール ホスト保護を設定する例を示します。

```
Router(config)# parameter-map type inspect-zone zone-pmap
Router(config-profile)# tcp syn-flood rate per-destination 400
Router(config-profile)# max-destination 10000
Router(config-profile)# exit
Router(config)# zone security secure-zone
Router(config-sec-zone)# protection zone-pmap
```

ファイアウォール セッション テーブル保護の設定例

グローバル パラメータ マップ

次に、グローバル ルーティング ドメインのファイアウォール セッション テーブル保護を設定する例を示します。

```
Router# configure terminal
Router(config)# parameter-map type inspect global
Router(config-profile)# tcp syn-flood limit 500
Router(config-profile)# end
```

検査 VRF タイプ パラメータ マップ

次に、VRF ドメインのファイアウォール セッション テーブル保護を設定する例を示します。

```
Router# configure terminal
Router(config)# parameter-map type inspect-vrf vrf-pmap
Router(config-profile)# tcp syn-flood limit 200
Router(config-profile)# exit
Router(config)# parameter-map type inspect global
Router(config-profile)# vrf vrf1 inspect vrf-pmap
Router(config-profile)# end
```

ファイアウォール TCP SYN Cookie に関する追加情報

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『Cisco IOS Master Command List, All Releases』
セキュリティ コマンド	• 『Security Command Reference: Commands A to C』 • 『Security Command Reference: Commands D to L』 • 『Security Command Reference: Commands M to R』 • 『Security Command Reference: Commands S to Z』

シスコのテクニカル サポート

説明	リンク
右の URL にアクセスして、シスコのテクニカル サポートを最大限に活用してください。これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

ファイアウォール TCP SYN Cookie の設定に関する機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *200 :* ファイアウォール *TCP SYN Cookie* の設定に関する機能情報

機能名	リリース	機能情報
ファイアウォール TCP SYN Cookie	Cisco IOS XE リリース 3.3S	ファイアウォール TCP SYN Cookie 機能は、TCP SYN フラッディング攻撃からファイアウォールを保護します。TCP SYN フラッディング攻撃は DoS 攻撃の一種です。通常は、TCP SYN パケットはファイアウォールの背後のターゲット エンド ホストまたはサブネット アドレスの範囲に送信されます。これらの TCP SYN パケットによって、送信元 IP アドレスがスプーフィングされます。スプーフィング攻撃とは、個人またはプログラムが、データを改ざんして不正な優位性を獲得し、別のものになりすますことです。TCP SYN フラッディングは、ファイアウォールまたはエンド ホスト上のリソースを使い果たすことにより、正当なトラフィックに対する DoS を引き起こすことができます。ファイアウォールおよびファイアウォール背後のエンド ホストでの TCP SYN フラッディングを防ぐには、ファイアウォール TCP SYN Cookie 機能を設定する必要があります。 次のコマンドが導入または変更されました。**parameter-map type inspect-vrf**、**parameter-map type inspect-zone**、**parameter-map type inspect global**、**show policy-firewall stats**、**tcp syn-flood rate per-destination**、**tcp syn-flood limit**。

第 148 章

ACL のオブジェクト グループ

ACL のオブジェクト グループ機能を使用して、ユーザ、デバイス、またはプロトコルをグループに分類し、これらのグループをアクセス コントロール リスト（ACL）に適用してアクセス コントロール ポリシーを作成することができます。この機能により、従来の ACL で使用される個々の IP アドレス、プロトコル、ポートではなく、オブジェクト グループを使用できるようになります。この機能では、複数のアクセス コントロール エントリ（ACE）を使用できます。それぞれの ACE を使用してユーザのグループ全体にサーバやサービスのグループに対するアクセスを許可したり、アクセスを拒否したりできるため、ACL のサイズが削減されて管理が容易になります。

このモジュールでは、ゾーンベース ポリシー ファイアウォールでのオブジェクト グループ ACL の概要と、ゾーンベース ファイアウォールを設定する方法を説明します。

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報および警告については、「Bug Search Tool」およびご使用のプラットフォームおよびソフトウェア リリースのリリース ノートを参照してください。このモジュールで説明される機能に関する情報、および各機能がサポートされるリリースの一覧については、機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

ACL のオブジェクト グループに関する制約事項

以下の制限が、ゾーンベース ファイアウォール上の ACL 用オブジェクト グループ機能に適用されます。

- IPv6 はサポートされていません。
- 動的およびユーザ単位のアクセス コントロール リスト（ACL）はサポートされません。
- ACL 内で使用されている場合は、オブジェクト グループを削除したり、オブジェクト グループを空にしたりすることができません。
- オブジェクトグループを使用する ACL ステートメントは、処理のために RP に送信されるパケットでは無視されます。
- オブジェクト グループは IP 拡張 ACL でのみサポートされます。

ACL のオブジェクト グループに関する情報

ACL のオブジェクト グループの概要

大規模なネットワークでは、アクセス コントロール リスト（ACL）の行数が大量（数百行）になり、特に ACL が頻繁に変更される場合は ACL の設定および管理が困難になります。オブジェクト グループベースの ACL は小規模で読みやすく、簡単に設定および管理できます。オブジェクト グループベースの ACL により、Cisco IOS ルータの大規模なユーザ アクセス環境でのスタティック ACL の導入が容易になります。オブジェクト グループはポリシーの作成を簡素化することから（たとえば、グループ A にグループ A サービスへのアクセスを許可するなど）、ゾーンベース ファイアウォールにはオブジェクト グループによるメリットが得られます。

従来型のアクセス コントロール エントリ（ACE）を設定し、複数の ACE が同じ ACL 内のオブジェクト グループを参照するように設定できます。オブジェクト グループベースの ACL は、Quality of Service（QoS）一致基準、ゾーンベース ポリシー ファイアウォール、Dynamic Host Configuration Protocol（DHCP）、およびその他の拡張 ACL を使用する機能で使用できます。

さらに、マルチキャスト トラフィックでオブジェクト グループベースの ACL を使用することもできます。多数のインバウンドおよびアウトバウンド パケットがある場合、オブジェクト グループベースの ACL を使用すると、従来型の ACL を使用する場合よりパフォーマンスが向上します。また、大規模な構成では、この機能によりアドレスとプロトコルのペアごとに個別の ACE を定義する必要がなくなるため、NVRAM に必要なストレージを削減できます。

ゾーンベース ファイアウォールとオブジェクト グループの統合

ゾーンベース ファイアウォールでは特定のトラフィックにポリシーを適用するために、オブジェクト グループ アクセス コントロール リスト（ACL）を使用します。オブジェクト グルー

プ ACL を定義し、その ACL をゾーンベース ファイアウォール ポリシーに関連付けて、ゾーン ペアにポリシーを適用してトラフィックを検査します。

Cisco IOS XE リリース 3.12S の場合、ファイアウォールでサポートされるのは拡張オブジェクト グループ ACL のみです。

ファイアウォールで設定されたオブジェクト グループには、次の機能が有効です。

- スタティックおよびダイナミック ネットワーク アドレス変換（NAT）
- サービス NAT（**ip nat service** コマンドで設定された標準外の FTP ポート番号をサポートする NAT）
- FTP アプリケーション層ゲートウェイ（ALG）
- Session Initiation Protocol（SIP）ALG

クラスマップには、**match access-group** コマンドを使用して最大 64 のマッチングステートメントを設定できます。

ネットワーク オブジェクト グループで許可されるオブジェクト

ネットワーク オブジェクト グループは、次のいずれかのオブジェクトのグループです。

- IPv6 アドレス
- ホスト IPv6 アドレス
- その他のネットワーク オブジェクト グループ
- サブネット

サービス オブジェクト グループで許可されるオブジェクト

サービス オブジェクト グループは、次のいずれかのオブジェクトのグループです。

- 送信元および宛先プロトコル ポート（Telnet や Simple Network Management Protocol（SNMP）など）
- Internet Control Message Protocol（ICMP）タイプ（エコー、エコー応答、到達不能など）
- トップレベル プロトコル（Encapsulating Security Payload（ESP）、TCP、UDP など）
- その他のサービス オブジェクト グループ

オブジェクト グループに基づく ACL

従来のアクセス コントロール リスト（ACL）を使用または参照する機能はすべて、オブジェクト グループ ベースの ACL と互換性があり、従来の ACL の機能インタラクションはオブジェクト グループ ベース ACL と同じです。この機能により、オブジェクト グループ ベースの ACL をサポートできるように従来の ACL が拡張され、新しいキーワードと、送信元アドレス、宛先アドレス、送信元ポート、および宛先ポートが追加されます。

オブジェクト グループ メンバーシップ リストでは、（オブジェクト グループを削除および再定義せずに）オブジェクトを動的に追加、削除、または変更できます。また、オブジェクト グループ メンバーシップ リストでは、オブジェクト グループを使用する ACL アクセス コントロール エントリ（ACE）を再定義せずに、オブジェクトを追加、削除、または変更できます。グループにオブジェクトを追加してから、グループからオブジェクトを削除することで、ACL をインターフェイスに再適用せずに、オブジェクト グループ ベースの ACL 内で変更が正しく機能することを確認できます。

ソース グループのみ、宛先グループのみ、またはソース グループと宛先グループの両方を使用して、オブジェクト グループ ベースの ACL を複数回設定できます。

ACL 内またはクラス ベース ポリシー言語（CPL）ポリシー内で使用されているオブジェクト グループは削除できません。

オブジェクト グループ ACL のガイドライン

- オブジェクト グループには、固有の名前が必要となります。例として、「Engineering」という名前のネットワーク オブジェクト グループと「Engineering」という名前のサービス オブジェクト グループを作成するとします。この場合、少なくとも 1 つのオブジェクト グループ名に識別子（またはタグ）を追加して、その名前を固有のものにする必要があります。たとえば、「Engineering-admins」と「Engineering-hosts」という名前を使用すると、オブジェクト グループの名前を固有のものにして識別しやすくすることができます。
- 既存のオブジェクト グループに、さらにオブジェクトを追加することができます。オブジェクト グループを追加した後、同じグループ名で必要に応じてさらにオブジェクトを追加できます。既存のオブジェクトを再入力する必要はありません。オブジェクトグループを削除するまで以前の設定がそのまま保持されます。
- さまざまなオブジェクトをグループ化することができます。たとえば、ホスト、プロトコル、サービスなどのオブジェクトがグループ化され、同じグループ名で設定できます。ネットワーク オブジェクトは、ネットワーク オブジェクト グループでのみ定義し、サービス オブジェクトはサービス グループでのみ定義できます。
- **object-group** コマンドでグループを定義した後に任意のセキュリティ アプライアンス コマンドを使用すると、そのコマンドはそのグループの各項目に適用されます。この機能を使用すると、コンフィギュレーションのサイズを大幅に削減できます。
- ZBF 検査のクラスマップに関連付けられている ACL にオブジェクトグループが含まれている場合、ACL にエントリを追加したり、ACL からエントリを削除したりすると、アクセスリスト コンフィギュレーション プロンプトを終了した後にのみ変更が有効になります。

ACL のオブジェクト グループの設定方法

ACL のオブジェクト グループを設定するには、最初に 1 つ以上のオブジェクト グループを作成します。作成するオブジェクトグループは、ネットワーク オブジェクト グループ（ホスト

アドレスやネットワークアドレスなどのオブジェクトが含まれるグループ）またはサービス オブジェクト グループ（ポート番号に **lt**、**eq**、**gt**、**neq**、**range** などの演算子を使用するグループ）を任意に組み合わせることができます。オブジェクトグループを作成した後、それらのグループにポリシー（**permit** または **deny** など）を適用するアクセス コントロール エントリ（ACE）を作成します。

ネットワーク オブジェクト グループの作成

単一のオブジェクト（単一の IP アドレス、ホスト名、別のネットワーク オブジェクト グループ、またはサブネットなど）または複数のオブジェクトを含むネットワーク オブジェクト グループには、オブジェクトのアクセス制御ポリシーを作成するための、ネットワーク オブジェクト グループ ベース ACL が関連付けられています。

ネットワーク オブジェクト グループを作成するには、次の作業を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **object-group network** *object-group-name*
4. **description** *description-text*
5. **host** {*host-address* | *host-name*}
6. *network-address* {*/nn* | *network-mask*}
7. **group-object** *nested-object-group-name*
8. オブジェクト グループのベースとなるオブジェクトを指定するまで、手順を繰り返します。
9. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**object-group network** *object-group-name* 例： `Device(config)# object-group network my-network-object-group`	オブジェクト グループ名を定義し、ネットワーク オブジェクト グループ コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 4	**description** *description-text* 例： `Device(config-network-group)# description test engineers`	（オプション）オブジェクト グループの説明を指定します。 • 最大 200 文字を使用できます。
ステップ 5	**host** {*host-address* | *host-name*} 例： `Device(config-network-group)# host 209.165.200.237`	（オプション）ホストの IP アドレスまたは名前を指定します。 • ホストアドレスを指定する場合、IPv4 アドレスを使用する必要があります。
ステップ 6	*network-address* {*/nn* | *network-mask*} 例： `Device(config-network-group)# 209.165.200.225 255.255.255.224`	（オプション）サブネット オブジェクトを指定します。 • ネットワーク アドレスには IPv4 アドレスを指定する必要があります。デフォルトのネットワーク マスクは 255.255.255.255 です。
ステップ 7	**group-object** *nested-object-group-name* 例： `Device(config-network-group)# group-object my-nested-object-group`	（オプション）現在の（親）オブジェクト グループに含めるネストされた（子）オブジェクト グループを指定します。 • 子オブジェクト グループのタイプは親のタイプと一致している必要があります（たとえば、ネットワーク オブジェクト グループを作成する場合、子として別のネットワーク オブジェクト グループを指定する必要があります）。 • グループ オブジェクト内で重複するオブジェクトの使用は、オブジェクト グループのネストによってのみ可能です。たとえば、オブジェクト 1 がグループ A とグループ B の両方に含まれる場合、A と B の両方を含むグループ C を定義できます。ただし、グループ階層の循環を引き起こすグループ オブジェクトを含めることはできません（たとえば、グループ A をグループ B に含め、次にグループ B をグループ A に含めることはできません）。 • ネストされたオブジェクト グループのレベルの数は無制限に使用できます（ただし、最大 2 つのレベルを推奨します）。
ステップ 8	オブジェクト グループのベースとなるオブジェクトを指定するまで、手順を繰り返します。	—

	コマンドまたはアクション	目的
ステップ 9	**end** 例： `Device(config-network-group)# end`	ネットワーク オブジェクト グループ コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

サービス オブジェクト グループの作成

TCP または UDP ポートまたはポート範囲を指定するにはサービス オブジェクト グループを使用します。サービス オブジェクト グループがアクセス コントロール リスト（ACL）に関連付けられると、このサービス オブジェクト グループ ベースの ACL はポートへのアクセスを制御できます。

手順の概要

1. **enable**
2. **configure terminal**
3. **object-group service** *object-group-name*
4. **description** *description-text*
5. *protocol*
6. {**tcp** | **udp** | **tcp-udp**} [**source** {{[**eq**] | **lt** | **gt**} *port1* | **range** *port1 port2*}] [{[**eq**] | **lt** | **gt**} *port1* | **range** *port1 port2*]
7. **icmp** *icmp-type*
8. **group-object** *nested-object-group-name*
9. 手順を繰り返して、オブジェクト グループのベースとなるオブジェクトを指定します。
10. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**object-group service** *object-group-name* 例： `Device(config)# object-group service my-service-object-group`	オブジェクト グループ名を定義し、サービス オブジェクト グループ コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 4	**description** *description-text* 例： `Device(config-service-group)# description test engineers`	（オプション）オブジェクト グループの説明を指定します。 • 最大 200 文字を使用できます。
ステップ 5	*protocol* 例： `Device(config-service-group)# ahp`	（オプション）IP プロトコルの番号または名前を指定します。
ステップ 6	{**tcp** | **udp** | **tcp-udp**} [**source** {{[**eq**] | **lt** | **gt**} *port1* | **range** *port1 port2*}] [{[**eq**] | **lt** | **gt**} *port1* | **range** *port1 port2*] 例： `Device(config-service-group)# tcp-udp range 2000 2005`	（オプション）TCP、UDP、または両方を指定します。
ステップ 7	**icmp** *icmp-type* 例： `Device(config-service-group)# icmp conversion-error`	（オプション）Internet Control Message Protocol（ICMP）タイプの 10 進数または名前を指定します。
ステップ 8	**group-object** *nested-object-group-name* 例： `Device(config-service-group)# group-object my-nested-object-group`	（オプション）現在の（親）オブジェクト グループに含めるネストされた（子）オブジェクト グループを指定します。 • 子オブジェクト グループのタイプは親のタイプと一致している必要があります（たとえば、ネットワーク オブジェクト グループを作成する場合、子として別のネットワーク オブジェクト グループを指定する必要があります）。 • グループ オブジェクト内で重複するオブジェクトの使用は、オブジェクト グループのネストによってのみ可能です。たとえば、オブジェクト 1 がグループ A とグループ B の両方に含まれる場合、A と B の両方を含むグループ C を定義できます。ただし、グループ階層の循環を引き起こすグループ オブジェクトを含めることはできません（たとえば、グループ A をグループ B に含め、次にグループ B をグループ A に含めることはできません）。

	コマンドまたはアクション	目的
		• ネストされたオブジェクト グループのレベルの数は無制限に使用できます（ただし、最大2つのレベルを推奨します）。
ステップ 9	手順を繰り返して、オブジェクト グループのベースとなるオブジェクトを指定します。	—
ステップ 10	**end** 例： `Device(config-service-group)# end`	サービス オブジェクト グループ コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

オブジェクト グループ ベース ACL の作成

オブジェクト グループ ベースのアクセス コントロール リスト（ACL）を作成する場合、1 つ以上のオブジェクト グループを参照する ACL を設定します。従来の ACE と同様に、同じアクセス ポリシーを 1 つまたは複数のインターフェイスと関連付けることができます。

同じオブジェクト グループ ベース ACL 内のオブジェクト グループを参照する、複数のアクセス コントロール エントリ（ACE）を定義できます。また、複数の ACE で特定のオブジェクト グループを再利用できます。

オブジェクト グループ ベース ACL を作成するには、次の作業を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **ip access-list extended** *access-list-name*
4. **remark** *remark*
5. **deny** *protocol source* [*source-wildcard*] *destination* [*destination-wildcard*] [**option** *option-name*] [**precedence** *precedence*] [**tos** *tos*] [**established**] [**log** | **log-input**] [**time-range** *time-range-name*] [**fragments**]
6. **remark** *remark*
7. **permit** *protocol source* [*source-wildcard*] *destination* [*destination-wildcard*] [**option** *option-name*] [**precedence** *precedence*] [**tos** *tos*] [**established**] [**log** | **log-input**] [**time-range** *time-range-name*] [**fragments**]
8. 手順を繰り返して、アクセス リストのベースとなるフィールドと値を指定します。
9. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例：	特権 EXEC モードを有効にします。

	コマンドまたはアクション	目的
	`Device> enable`	• パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ip access-list extended** *access-list-name* 例： `Device(config)# ip access-list extended nomarketing`	名前を使用して拡張 IP アクセス リストを定義し、拡張アクセス リスト コンフィギュレーション モードを開始します。
ステップ 4	**remark** *remark* 例： `Device(config-ext-nacl)# remark protect server by denying access from the Marketing network`	（任意）設定されたアクセス リスト エントリに関するコメントを追加します。 • 注釈はアクセス リスト エントリの前または後に指定できます。 • この例では、注釈によって、後続のエントリがインターフェイスに対する Marketing ネットワーク アクセスを拒否することをネットワーク管理者に示します。

ステップ 5	**deny** *protocol source* [*source-wildcard*] *destination* [*destination-wildcard*] [**option** *option-name*] [**precedence** *precedence*] [**tos** *tos*] [**established**] [**log** | **log-input**] [**time-range** *time-range-name*] [**fragments**]
	例：
	`Device(config-ext-nacl)# deny ip 209.165.200.244 255.255.255.224 host 209.165.200.245 log`
	`Example based on object-group:`
	`Router(config)#object-group network my_network_object_group`
	`Router(config-network-group)#209.165.200.224 255.255.255.224`
	`Router(config-network-group)#exit`
	`Router(config)#object-group network my_other_network_object_group`
	`Router(config-network-group)#host 209.165.200.245`
	`Router(config-network-group)#exit`
	`Router(config)#ip access-list extended nomarketing`
	`Router(config-ext-nacl)#deny ip object-group my_network_object_group object-group my_other_network_object_group log`
		（任意）ステートメントに指定されたすべての条件に一致するすべてのパケットを拒否します。
		• 必要に応じて、**object-group** *service-object-group-name* キーワードおよび引数を、*protocol* の代わりに使用します。argument
		• 必要に応じて、**object-group** *source-network-object-group-name* キーワードおよび引数を、*source source-wildcard* 引数の代わりに使用します。
		• 必要に応じて、**object-group** *destination-network-object-group-name* キーワードおよび引数を、*destination destination-wildcard* 引数の代わりに使用します。
		• *source-wildcard* または *destination-wildcard* を省略すると、0.0.0.0 のワイルドカードマスクが想定され、それぞれ送信元アドレスまたは宛先アドレスの全ビットへの一致を意味します。

	コマンドまたはアクション	目的
		• 必要に応じて、*source source-wildcard* または *destination destination-wildcard* の代わりに、キーワード **any** を使用して、アドレスと 0.0.0.0 255.255.255.255 のワイルドカードを指定します。 • 必要に応じて、**host** *source* キーワードおよび引数を使用して送信元と *source* 0.0.0.0 の送信元ワイルドカードを示すか、**host** *destination* キーワードおよび引数を使用して宛先と *destination* 0.0.0.0 の宛先ワイルドカードを示します。 • この例では、すべての送信元のパケットは、宛先ネットワーク 209.165.200.244 へのアクセスが拒否されます。アクセス リストによって許可または拒否されるパケットに関するロギング メッセージは、**logging facility** コマンドに設定された設備に送信されます（たとえば、コンソール、端末、syslog）。つまり、パケットがアクセス リストに一致する場合は常に、パケットに関する情報を提供するロギング メッセージが設定された設備に送信されます。コンソールにロギングするメッセージのレベルは、**logging console** コマンドで制御します。 •
ステップ 6	**remark** *remark* **例**： `Device(config-ext-nacl)# remark allow TCP from any source to any destination`	（任意）設定されたアクセス リスト エントリに関するコメントを追加します。 • 注釈はアクセス リスト エントリの前または後に指定できます。
ステップ 7	**permit** *protocol source* [*source-wildcard*] *destination* [*destination-wildcard*] [**option** *option-name*] [**precedence** *precedence*] [**tos** *tos*] [**established**] [**log** | **log-input**] [**time-range** *time-range-name*] [**fragments**] **例**： `Device(config-ext-nacl)# permit tcp any any`	ステートメントに指定されたすべての条件に一致するすべてのパケットを許可します。 • 各アクセス リストには、少なくとも 1 つの permit ステートメントが必要です。 • 必要に応じて、**object-group** *service-object-group-name* キーワードおよび引数を、*protocol* の代わりに使用します。 • 必要に応じて、**object-group** *source-network-object-group-name* キーワードおよび引数を、*source source-wildcard* の代わりに使用します。

	コマンドまたはアクション	目的
		• 必要に応じて、**object-group** *destination-network-object-group-name* キーワードおよび引数を、*destination destination-wildcard* の代わりに使用します。 • *source-wildcard* または *destination-wildcard* を省略すると、0.0.0.0 のワイルドカードマスクが想定され、それぞれ送信元アドレスまたは宛先アドレスの全ビットへの一致を意味します。 • 必要に応じて、*source source-wildcard* または *destination destination-wildcard* の代わりに、キーワード **any** を使用して、アドレスと 0.0.0.0 255.255.255.255 のワイルドカードを指定します。 • この例では、任意の送信元から任意の宛先への TCP パケットが許可されています。 • **log-input** キーワードを使用して、ロギング出力に入力インターフェイス、送信元 MAC アドレス、または仮想回線を含めます。
ステップ 8	手順を繰り返して、アクセス リストのベースとなるフィールドと値を指定します。	明示的に許可されていないすべての送信元は、アクセス リストの末尾にある暗黙的な **deny** ステートメントで拒否されます。
ステップ 9	**end** 例： `Device(config-ext-nacl)# end`	拡張アクセス リスト コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

オブジェクト グループのクラス マップとポリシー マップの設定

手順の概要

1. **enable**
2. **configure terminal**
3. **class-map type inspect match-all** *class-map-name*
4. **match access-group name** *access-list-name*
5. **exit**
6. **policy-map type inspect** *policy-map-name*
7. **class type inspect** *class-map-name*
8. **pass**
9. **exit**

10. **class class-default**
11. **drop**
12. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**class-map type inspect match-all** *class-map-name* 例： `Device(config)# class-map type inspect match-all ogacl-cmap`	レイヤ 3 およびレイヤ 4 の検査タイプ クラス マップを作成し、クラスマップ コンフィギュレーション モードを開始します。
ステップ 4	**match access-group name** *access-list-name* 例： `Device(config-cmap)# match access-group name my-ogacl-policy`	指定された ACL に基づいて、クラス マップの一致基準を設定します。
ステップ 5	**exit** 例： `Device(config-cmap)# exit`	クラス マップ コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードに戻ります。
ステップ 6	**policy-map type inspect** *policy-map-name* 例： `Device(config)# policy-map type inspect ogacl-pmap`	検査タイプ ポリシーマップを作成して、ポリシーマップ コンフィギュレーション モードを開始します。
ステップ 7	**class type inspect** *class-map-name* 例： `Device(config-pmap)# class type inspect ogacl-cmap`	アクションを実行する対象のトラフィック クラスを指定し、ポリシー マップ クラス コンフィギュレーション モードを開始します。
ステップ 8	**pass** 例： `Device(config-pmap-c)# pass`	検査なしでパケットをデバイスに送信できるようにします。
ステップ 9	**exit** 例： `Device(config-pmap-c)# exit`	ポリシー マップ クラス コンフィギュレーション モードを終了し、ポリシーマップコンフィギュレーション モードに戻ります。

	コマンドまたはアクション	目的
ステップ 10	**class class-default** 例： `Device(config-pmap)# class class-default`	ポリシーを設定または変更するデフォルト クラスを指定し、ポリシー マップ クラス コンフィギュレーション モードを開始します。
ステップ 11	**drop** 例： `Device(config-pmap-c)# drop`	デバイスに送信されるパケットをドロップします。
ステップ 12	**end** 例： `Device(config-pmap-c)# end`	ポリシー マップ クラス コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

オブジェクト グループのゾーンの設定

手順の概要

1. **enable**
2. **configure terminal**
3. **zone security** *zone-name*
4. **exit**
5. **zone security** *zone-name*
6. **exit**
7. **interface** *type number*
8. **zone-member security** *zone-name*
9. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 3	**zone security** *zone-name* 例： `Device(config)# zone security outside`	セキュリティ ゾーンを作成し、セキュリティ ゾーン コンフィギュレーション モードを開始します。 • 送信元ゾーンと宛先ゾーンという、ゾーン ペアを作成するための 2 つのセキュリティ ゾーンが必要です。
ステップ 4	**exit** 例： `Device(config-sec-zone)# exit`	セキュリティ ゾーン コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードに戻ります。
ステップ 5	**zone security** *zone-name* 例： `Device(config)# zone security inside`	セキュリティ ゾーンを作成し、セキュリティ ゾーン コンフィギュレーション モードを開始します。 • 送信元ゾーンと宛先ゾーンという、ゾーン ペアを作成するための 2 つのセキュリティ ゾーンが必要です。
ステップ 6	**exit** 例： `Device(config-sec-zone)# exit`	セキュリティ ゾーン コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードに戻ります。
ステップ 7	**interface** *type number* 例： `Device(config)# interface gigabitethernet 0/1/1`	インターフェイスを設定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 8	**zone-member security** *zone-name* 例： `Device(config-if)# zone-member security inside`	インターフェイスをセキュリティ ゾーンにアタッチします。
ステップ 9	**end** 例： `Device(config-if)# end`	インターフェイス コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードに戻ります。

オブジェクト グループのゾーン ペアへのポリシー マップの適用

手順の概要

1. **enable**
2. **configure terminal**
3. **zone-pair security** *zone-pair-name* **source** {*zone-name* | **default** | **self**} **destination** {*zone-name* | **default** | **self**}
4. **service-policy type inspect** *policy-map-name*
5. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**zone-pair security** *zone-pair-name* **source** {*zone-name* | **default** | **self**} **destination** {*zone-name* | **default** | **self**} 例： `Device(config)# zone-pair security out-to-in source outside destination inside`	ゾーン ペアを作成し、セキュリティ ゾーンペア コンフィギュレーション モードを開始します。
ステップ 4	**service-policy type inspect** *policy-map-name* 例： `Device(conf-sec-zone-pair)# service-policy type inspect ogacl-pmap`	ファイアウォール ポリシー マップをセキュリティ ゾーン ペアにアタッチします。
ステップ 5	**end** 例： `Device(config-sec-zone-pair)# end`	セキュリティ ゾーン ペア コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードに戻ります。

ACL のオブジェクト グループの確認

手順の概要

1. **enable**
2. **show object-group** [*object-group-name*]
3. **show ip access-list** [*access-list-name*]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。

	コマンドまたはアクション	目的
ステップ 2	**show object-group** [*object-group-name*] 例： `Device# show object-group my-object-group`	名前付きまたは番号付きオブジェクト グループ（名前が入力されていない場合はすべてのオブジェクト グループ）の設定を表示します。
ステップ 3	**show ip access-list** [*access-list-name*] 例： `Device# show ip access-list my-ogacl-policy`	名前付きまたは番号付きアクセス リストまたはオブジェクト グループ ベース ACL（名前が入力されていない場合はすべてのアクセス リストおよびオブジェクト グループ ベース ACL）の内容を表示します。

ACL 用オブジェクト グループの設定例

例：IPv6 ネットワーク オブジェクト グループの作成

次に、v6-network ognet1 という名前の IPv6 ネットワーク オブジェクト グループを作成する例を示します。

```
Device> enable
Device# configure terminal
Device(config)# object-group v6-network ognet1
Device(config-v6-network-group)# 1:1:2::0/32
Device(config-v6-network-group)# host AB:233::23D5
Device(config-v6-network-group)# exit
```

次に、1つのホスト、1つのサブネット、および既存のオブジェクトグループ（子）をオブジェクトとして含む、v6-network ognet2 という名前のネットワーク オブジェクト グループを作成する例を示します。

```
Device> enable
Device# configure terminal
Device(config)# object-group network v6-network ognet2
Device(config-v6network-group)# 1:2:3::4/36
Device(config-v6network-group)# host AABB::CCDD
Device(config-v6network-group)# group-object ognet1
Device(config-v6network-group)# exit
```

例：IPv6 サービス オブジェクト グループの作成

次に、複数の ICMP、TCP、UDP、および TCP-UDP プロトコルをオブジェクトとして含む、v6-service ogserv1 という名前のサービス オブジェクト グループを作成する例を示します。

```
Device> enable
Device# configure terminal
```

```
Device(config)# object-group service v6-service ogserv1
Device(config-v6service-group)# icmp unreachable
Device(config-v6service-group)# tcp smtp
Device(config-v6service-group)# tcp telnet
Device(config-v6service-group)# tcp source range 3000 4000 telnet
Device(config-v6service-group)# pcp
Device(config-v6service-group)# udp domain
Device(config-v6service-group)# hph
Device(config-v6service-group)# exit
```

例：IPv6 オブジェクトグループベースの ACL の作成

次に、パケットを許可する IPv6 オブジェクトグループベース ACL を作成する例を示します。

```
Device> enable
Device# configure terminal
Device(config)# ipv6 access-list ogacl1
Device(config-ipv6-acl)# permit object-group ogserv1 5:6:7::5/56 object-group ognet1
Device(config-ipv6-acl)# deny ip object-group ognet2 object-group ognet3
Device(config-ipv6-acl)# permit ipv6 any any
Device(config-ipv6-acl)# exit
```

例：オブジェクト グループのクラス マップとポリシー マップの設定

```
Device# configure terminal
Device(config)# class-map type inspect match-all ogacl-cmap
Device(config-cmap)# match access-group name my-ogacl-policy
Device(config-cmap)# exit
Device(config)# policy-map type inspect ogacl-pmap
Device(config-pmap)# class type inspect ogacl-cmap
Device(config-pmap-c)# pass
Device(config-pmap-c)# exit
Device(config-pmap)# class class-default
Device(config-pmap-c)# drop
Device(config-pmap-c)# end
```

例：オブジェクト グループのゾーンの設定

```
Device# configure terminal
Device(config)# zone security outside
Device(config-sec-zone)# exit
Device(config)# zone security inside
Device(config-sec-zone)# exit
Device(config)# zone-pair security out-to-in source outside destination inside
Device(conf-sec-zone-pair)# exit
Device(config)# interface gigabitethernet 0/1/1
Device(config-if)# zone-member security inside
Device(config-if)# exit
Device(config)# interface gigabitethernet 0/1/0
Device(config-if)# zone-member security outside
```

```
Device(config-if)# end
```

例：オブジェクト グループのゾーン ペアへのポリシー マップの適用

```
Device# configure terminal
Device(config)# zone-pair security out-to-in source outside destination inside
Device(config-sec-zone-pair)# service-policy type inspect ogacl-pmap
Device(config-sec-zone-pair)# end
```

例：ACL 用 IPv6 オブジェクトグループの確認

次に、すべてのオブジェクト グループを表示する例を示します。

```
Device# show object-group

V6-Network object group ognet1
1:1:2::/32
host AB:233::23D5
V6-Network object group ognet2
1:2:3::4/36
host AABB::CCDD
group-object ognet1
V6-Network object group ognet3
host 1::1
host 1::2
host 1::3
V6-Service object group ogserv1
icmp unreachable
tcp source range 3000 4000 eq telnet
pcp
hbh
```

次に、IPv6 オブジェクトグループベース ACL に関する情報を表示する例を示します。

```
Device# show ipv6 access-list
IPv6 access list ogacl1
      permit object-group ogserv1 5:6:7::/56 object-group ognet1 sequence 10
      deny ipv6 object-group ognet2 object-group ognet3 sequence 20
      permit ipv6 any any sequence 30
```

ACL 用オブジェクト グループに関する追加情報

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『Cisco IOS Master Command List, All Releases』

関連項目	マニュアル タイトル
セキュリティ コマンド	• 『Cisco IOS Security Command Reference: Commands A to C』[英語] • 『Cisco IOS Security Command Reference: Commands D to L』[英語] • 『Cisco IOS Security Command Reference: Commands M to R』[英語] • 『Cisco IOS Security Command Reference: Commands S to Z』[英語]
ACL 設定ガイド	『セキュリティコンフィギュレーションガイド』の「アクセスコントロールリスト」

シスコのテクニカル サポート

説明	リンク
右の URL にアクセスして、シスコのテクニカル サポートを最大限に活用してください。これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

ACL 用 IPv6 オブジェクトグループに関する機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *201 : ACL* 用オブジェクト グループに関する機能情報

機能名	リリース	機能情報
ACL の IPv6 オブジェクトグループ	Cisco IOS XE リリース 16.11.1	ACL 用 IPv6 オブジェクトグループ機能を使用すれば、ユーザー、デバイス、またはプロトコルをグループに分類して、それらをアクセス制御リスト（ACL）に適用し、そのグループ用のアクセス制御ポリシーを作成することができます。この機能により、従来の ACL で使用される個々の IP アドレス、プロトコル、ポートではなく、オブジェクトグループを使用できるようになります。この機能は、複数のアクセスコントロール エントリ（ACE）を許可しますが、各 ACE を使用して、ユーザーのグループ全体に対してサーバーまたはサービスのグループへのアクセスを許可または禁止できます。

第 149 章

Cisco ファイアウォール SIP 機能拡張 ALG

Cisco XE ファイアウォールの強化された Session Initiation Protocol（SIP）インスペクションには、基本的な SIP 検査機能（SIP パケット インスペクションとピンホールのオープン）に加え、プロトコル準拠機能とアプリケーションセキュリティ機能があります。これらの機能拡張によって、SIP トラフィックおよび機能に適用するポリシーとセキュリティ チェックを制御し、不要なメッセージやユーザを除外できます。

Cisco IOS XE ソフトウェアで追加の SIP 機能を開発することで、Cisco Call Manage、Cisco Call Manager Express、および Cisco IP-IP Gateway ベースの音声/ビデオ システムのサポートが改善されます。また、アプリケーション レイヤ ゲートウェイ（ALG）SIP の機能拡張では、RFC 3261 とその拡張もサポートされています。

Cisco ファイアウォール SIP 拡張機能 ALG の前提条件

システムが Cisco IOS XE リリース 2.4 以降のリリースを実行している必要があります。

Cisco ファイアウォール SIP 拡張機能 ALG に関する制約事項

DNS 名前解決

SIP メソッドでは、IP アドレスを直接指定する代わりにドメイン ネーム システム（DNS）名を使用できますが、この機能は現在 DNS 名をサポートしていません。

Cisco ASR 1000 シリーズ ルータ

この機能は、Cisco ASR 1000 シリーズ ルータ上のアプリケーション インスペクションおよびコントロール（AIC）をサポートせずに実装されました。Cisco IOS XE リリース 2.4 では、次コマンドのみがサポートされています。**class-map type inspect**、**class type inspect**、**match protocol**、および **policy-map type inspect**。

Cisco ISR 4000 シリーズ ルータ

Cisco IOS XE Fuji 16.7.1 リリースは、Transport Layer Security（TLS）または Secure Real-time Transport Protocol（SRTP）をサポートしていません。

Cisco ファイアウォール SIP 拡張機能 ALG について

SIP の概要

Session Initiation Protocol（SIP）は、1 人または複数の参加者とのセッションを作成、変更、および終了するためのアプリケーション層コントロール（シグナリング）プロトコルです。SIP セッションには、インターネット電話の通話、マルチメディアの配布、マルチメディア会議などがあります。SIP は HTTP のような要求/応答トランザクション モデルに基づいています。各トランザクションは、サーバで特定のメソッドまたは関数を呼び出す 1 つの要求と 1 つ以上の応答で構成されます。

セッションの作成に使用される SIP の招待は、互換性のあるメディア タイプのセットに参加者が同意できるセッション記述を伝送しています。SIP は、プロキシ サーバと呼ばれる要素を利用して、ユーザの所在地への要求のルーティング、サービスのためのユーザ認証および認可、プロバイダーのコールルーティング ポリシーの実装、およびユーザへの機能提供を行っています。また、SIP には、プロキシ サーバから使用できるように、ユーザの所在地をアップロードできる登録機能があります。SIP は複数のトランスポート プロトコルを基礎として実行されます。

SIP 用ファイアウォールの機能の説明

SIP 用ファイアウォールのサポート機能を使用すると、SIP シグナリング要求は、ゲートウェイ間の直接伝送によって、または複数のプロキシを介して、宛先ゲートウェイまたは電話に送信できます。最初の要求後に、Record-Route ヘッダー フィールドを使用しない場合、後続の要求は、Contact ヘッダー フィールドに指定されている宛先ゲートウェイ アドレスに直接伝送できます。そのため、ファイアウォールは、周囲のすべてのプロキシとゲートウェイを認識し、次の機能を使用できます。

- SIP シグナリング応答は、SIP シグナリング要求と同じパスを伝送できます。
- 後続のシグナリング要求は、エンドポイント（宛先ゲートウェイ）に直接伝送できます。
- メディア エンドポイントは、相互にデータを交換できます。

SIP UDP および TCP のサポート

RFC 3261 は最新の SIP の RFC であり、RFC 2543 の置き換えです。この機能は、シグナリングに SIP UDP と TCP 形式をサポートします。

SIP インスペクション

ここでは、Cisco ファイアウォール - SIP ALG 拡張機能でサポートされる展開シナリオについて説明します。

SIP 電話と CCM 間の Cisco IOS XE ファイアウォール

Cisco IOS XE ファイアウォールは、Cisco Call Manager または Cisco Call Manager Express と SIP 電話の間にあります。SIP 電話はファイアウォールを介して Cisco Call Manager または Cisco Call Manager Express に登録され、SIP 電話とのすべての SIP コールはファイアウォールを通過します。

SIP ゲートウェイ間の Cisco IOS XE ファイアウォール

Cisco IOS XE ファイアウォールは、2 つの SIP ゲートウェイ（Cisco Call Manager、Cisco Call Manager Express、または SIP プロキシ）の間にあります。電話は SIP ゲートウェイに直接登録されます。ファイアウォールから SIP セッションまたはトラフィックを認識するのは、異なる SIP ゲートウェイに登録された電話間で SIP コールが存在する場合のみです。シナリオによっては、IP-IP ゲートウェイをファイアウォールと同じデバイスに設定することもできます。このシナリオでは、SIP ゲートウェイ間のすべてのコールは IP-IP ゲートウェイで終端します。

ローカルの Cisco Call Manager Express とリモートの Cisco Call Manager Express/Cisco Call Manager を使用する Cisco IOS XE ファイアウォール

Cisco IOS XE ファイアウォールは、2 つの SIP ゲートウェイ（Cisco Call Manager、Cisco Call Manager Express、または SIP プロキシ）の間にあります。ゲートウェイの 1 つは、ファイアウォールと同じデバイスで設定されます。このゲートウェイに登録されているすべての電話は、ファイアウォールによってローカルで検査されます。また、2 つのゲートウェイ間に SIP コールがある場合、ファイアウォールによってその SIP セッションも検査されます。このシナリオでは、ファイアウォールの一方では SIP 電話がローカルで検査され、もう一方では SIP ゲートウェイが検査されます。

ローカルの Cisco Call Manager Express を使用する Cisco IOS XE ファイアウォール

Cisco IOS XE ファイアウォールと Cisco Call Manager Express は、同じデバイスで設定されます。Cisco Call Manager Express に登録されているすべての電話は、ファイアウォールによってローカルで検査されます。また、登録されている任意の電話間で行われる SIP コールも、Cisco IOS XE ファイアウォールによって検査されます。

ALG--SIP Over TCP の拡張機能

SIP が UDP を介して転送されると、すべての SIP メッセージが 1 つの UDP データグラムで送信されます。ただし、SIP が TCP を介して転送されると、1 つの TCP セグメントに複数の SIP メッセージが含まれることがあります。また、いずれかの TCP セグメント内の最後の SIP メッセージが部分的なメッセージである可能性があります。Cisco IOS XE リリース 3.5S 以前では、受信した 1 つの TCP セグメント内に複数の SIP メッセージがある場合、SIP ALG は最初のメッセージだけを解析します。解析されないデータは 1 つの不完全な SIP メッセージと見なされ、vTCP に戻されます。次の TCP セグメントを受信すると、vTCP は未処理データをそのセグメントの前に置き、それらを SIP ALG に渡すため、vTCP でバッファする必要があるデータが増えていきます。

Cisco IOS XE リリース 3.5S では、ALG--SIP over TCP 機能拡張機能により、SIP ALG は 1 つの TCP セグメント内の複数の SIP メッセージを処理できます。TCP セグメントを受信すると、このセグメント内のすべての完全な SIP メッセージは、1 つずつ解析されます。最終的に不完全なメッセージがある場合、その部分だけが vTCP に戻されます。

Cisco ファイアウォール SIP 拡張機能 ALG の設定方法

SIP インスペクションの有効化

手順の概要

1. **enable**
2. **configure terminal**
3. **class-map type inspect match-any** *class-map-name*
4. **match protocol** *protocol-name*
5. **exit**
6. **policy-map type inspect** *policy-map-name*
7. **class type inspect** *class-map-name*
8. **inspect**
9. **exit**
10. **class class-default**
11. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。

	コマンドまたはアクション	目的
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**class-map type inspect match-any** *class-map-name* 例： `Device(config)# class-map type inspect match-any sip-class1`	検査タイプ クラス マップを作成し、クラス マップ コンフィギュレーション モードを開始します。
ステップ 4	**match protocol** *protocol-name* 例： `Device(config-cmap)# match protocol sip`	名前付きプロトコルに基づいてクラス マップの一致基準を設定します。
ステップ 5	**exit** 例： `Device(config-cmap)# exit`	クラスマップ コンフィギュレーション モードを終了します。
ステップ 6	**policy-map type inspect** *policy-map-name* 例： `Device(config)# policy-map type inspect sip-policy`	検査タイプ ポリシー マップを作成し、ポリシー マップ コンフィギュレーション モードを開始します。
ステップ 7	**class type inspect** *class-map-name* 例： `Device(config-pmap)# class type inspect sip-class1`	アクションを実行するクラスを指定し、ポリシー マップ クラス コンフィギュレーション モードを開始します。
ステップ 8	**inspect** 例： `Device(config-pmap-c)# inspect`	ステートフル パケット インスペクションをイネーブルにします。
ステップ 9	**exit** 例： `Device(config-pmap-c)# exit`	ポリシー マップ クラス コンフィギュレーション モードを終了し、ポリシーマップコンフィギュレーション モードに戻ります。
ステップ 10	**class class-default** 例： `Device(config-pmap)# class class-default`	これらのポリシー マップ設定が事前に定義したデフォルト クラスに適用されることを指定します。 • 設定済みクラス マップの一致基準のいずれともトラフィックが一致しない場合、事前に定義されたデフォルト クラスに誘導されます。
ステップ 11	**end** 例：	ポリシー マップ コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

	コマンドまたはアクション	目的
	`Device(config-pmap)# end`	

トラブルシューティングのヒント

SIP 対応のファイアウォール設定の問題を解決するには、次のコマンドを使用できます。

- **clear zone-pair**
- **debug cce**
- **debug policy-map type inspect**
- **show policy-map type inspect zone-pair**
- **show zone-pair security**

ゾーン ペアの設定と SIP ポリシー マップのアタッチ

手順の概要

1. **enable**
2. **configure terminal**
3. **zone security** {*zone-name* | **default**}
4. **exit**
5. **zone security** {*zone-name* | **default**}
6. **exit**
7. **zone-pair security** *zone-pair-name* [**source** {*source-zone-name* | **self** | **default**} **destination** [*destination-zone-name* | **self** | **default**]]
8. **service-policy type inspect** *policy-map-name*
9. **exit**
10. **interface** *type number*
11. **zone-member security** *zone-name*
12. **exit**
13. **interface** *type number*
14. **zone-member security** *zone-name*
15. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。

	コマンドまたはアクション	目的
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**zone security** {*zone-name* | **default**} 例： `Device(config)# zone security zone1`	インターフェイスを割り当てることができるセキュリティ ゾーンを作成し、セキュリティ ゾーン コンフィギュレーション モードを開始します。
ステップ 4	**exit** 例： `Device(config-sec-zone)# exit`	セキュリティ ゾーン コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードに戻ります。
ステップ 5	**zone security** {*zone-name* | **default**} 例： `Device(config)# zone security zone2`	インターフェイスを割り当てることができるセキュリティ ゾーンを作成し、セキュリティ ゾーン コンフィギュレーション モードを開始します。
ステップ 6	**exit** 例： `Device(config-sec-zone)# exit`	セキュリティ ゾーン コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードに戻ります。
ステップ 7	**zone-pair security** *zone-pair-name* [**source** {*source-zone-name* | **self** | **default**} **destination** [*destination-zone-name* | **self** | **default**]] 例： `Device(config)# zone-pair security in-out source zone1 destination zone2`	ゾーン ペアを作成し、セキュリティ ゾーン ペア コンフィギュレーション モードに戻ります。 （注） ポリシーを適用するには、ゾーン ペアを設定する必要があります。
ステップ 8	**service-policy type inspect** *policy-map-name* 例： `Device(config-sec-zone-pair)# service-policy type inspect sip-policy`	ファイアウォール ポリシー マップを宛先ゾーン ペアに付加します。 （注） ゾーンのペア間でポリシーが設定されない場合、トラフィックはデフォルトでドロップされます。
ステップ 9	**exit** 例： `Device(config-sec-zone-pair)# exit`	セキュリティ ゾーン ペア コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードに戻ります。
ステップ 10	**interface** *type number* 例： `Device(config)# interface gigabitethernet 0/0/0`	インターフェイスを設定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 11	**zone-member security** *zone-name* 例：	インターフェイスを指定したセキュリティ ゾーンに割り当てます。

	コマンドまたはアクション	目的
	`Device(config-if)# zone-member security zone1`	（注） インターフェイスをセキュリティ ゾーンのメンバーにした場合、そのインターフェイスを通して送受信されるすべてのトラフィックは、デフォルトでドロップされます（ただしデバイス宛のトラフィックとデバイス発のトラフィックを除く）。トラフィックがインターフェイス通過するには、ゾーンをポリシーの適用先のゾーン ペアの一部にする必要があります。ポリシーがトラフィックを許可すると、トラフィックはそのインターフェイスを通過できます。
ステップ 12	**exit** 例： `Device(config-if)# exit`	インターフェイス設定モードを終了し、グローバル設定モードに戻ります。
ステップ 13	**interface** *type number* 例： `Device(config)# interface gigabitethernet 0/1/1`	インターフェイスを設定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 14	**zone-member security** *zone-name* 例： `Device(config-if)# zone-member security zone2`	インターフェイスを指定したセキュリティ ゾーンに割り当てます。
ステップ 15	**end** 例： `Device(config-if)# end`	インターフェイス コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

シスコ ファイアウォール SIP 拡張機能：ALG の設定例

例：SIP インスペクションの有効化

```
class-map type inspect match-any sip-class1
 match protocol sip
!
policy-map type inspect sip-policy
 class type inspect sip-class1
  inspect
!
class class-default
```

例：ゾーン ペアの設定と SIP ポリシー マップのアタッチ

```
zone security zone1
!
zone security zone2
!
zone-pair security in-out source zone1 destination zone2
 service-policy type inspect sip-policy
!
interface gigabitethernet 0/0/0
 zone security zone1
!
interface gigabitethernet 0/1/1
 zone security zone2
```

シスコ ファイアウォール SIP 拡張機能：ALG に関する追加情報

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『Cisco IOS Master Command List, All Releases』
ファイアウォール コマンド	• 『Cisco IOS Security Command Reference: Commands A to C』 • 『Cisco IOS Security Command Reference: Commands D to L』 • 『Cisco IOS Security Command Reference: Commands M to R』 • 『Cisco IOS Security Command Reference: Commands S to Z』
追加の SIP 情報	『Guide to Cisco Systems VoIP Infrastructure Solution for SIP』
vTCP のサポート	*vTCP for ALG* サポート

標準および RFC

標準/RFC	タイトル
RFC 3261	『SIP: Session Initiation Protocol』

シスコのテクニカル サポート

説明	リンク
右の URL にアクセスして、シスコのテクニカル サポートを最大限に活用してください。これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

Cisco ファイアウォール SIP 拡張機能：ALG に関する機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *202 : Cisco* ファイアウォール *SIP* 拡張機能：*ALG* に関する機能情報

機能名	リリース	機能情報
ALG--SIP over TCP の拡張機能	Cisco IOS XE リリース 3.5S	ALG--SIP over TCP 拡張機能は、SIP ALG で 1 つの TCP セグメント内の複数の SIP メッセージを処理できるようにします。TCP セグメントを受信すると、このセグメント内のすべての完全な SIP メッセージは、1 つずつ解析されます。最終的に不完全なメッセージがある場合、その部分だけが vTCP に戻されます。

機能名	リリース	機能情報
Cisco ファイアウォール--SIP ALG 拡張機能	Cisco IOS XE リリース 2.4	Cisco ファイアウォール--SIP ALG 拡張機能は、Cisco ASR 1000 シリーズ ルータ上の Cisco IOS XE ソフトウェアのファイアウォール機能セットに含まれる音声セキュリティ機能を拡張します。 Cisco ASR 1000 シリーズ ルータでは、次のコマンドはレイヤ 7（アプリケーション固有）シンタックスをサポートせずに実装されました。**class type inspect, class-map type inspect**、**match protocol**、**policy-map type inspect**。
T.38 Fax Relay 用のファイアウォール --SIP ALG 拡張機能	Cisco IOS XE リリース 2.4.1	T.38 Fax Relay 用のファイアウォール--SIP ALG 拡張機能は、Cisco ASR 1000 シリーズ ルータ上の Cisco IOS XE ソフトウェアのファイアウォール機能セットに含まれる機能を拡張します。 この機能は、SIP ALG で、Cisco ASR 1000 シリーズ ルータ上のファイアウォールを通過する T.38 Fax Relay over IP をサポートできるようにします。

第 150 章

ファイアウォールと NAT に対する MSRPC ALG サポート

ファイアウォールおよび NAT 対応の MSRPC ALG サポート機能により、ファイアウォールにおける Microsoft（MS）リモート プロシージャ コール（RPC）アプリケーション レベル ゲートウェイ（ALG）のサポート、およびネットワーク アドレス変換（NAT）のサポートが提供されます。MSRPC ALG は、MSRPC プロトコルのディープ パケット インスペクション（DPI）を実行します。MSRPC ALG はプロビジョニング システムと連動して、ネットワーク管理者が MSRPC パケットで検索可能な一致基準を定義するマッチング フィルタを設定できるようにします。

MSRPC ALG はさらに、Virtual Transport Control Protocol（vTCP）機能もサポートします。vTCP 機能は、TCP セグメンテーションを適切に処理し、Cisco IOS Zone-Based ファイアウォール、ネットワーク アドレス変換（NAT）、およびその他のアプリケーションでセグメントを解析するための各種 ALG プロトコルに対応するフレームワークを提供します。

ファイアウォールと NAT に対する MSRPC ALG サポートに関する前提条件

- パケットに Microsoft（MS）リモート プロシージャ コール（RPC）アプリケーション レベル ゲートウェイ（ALG）を適用する前に、Cisco IOS XE ファイアウォールとネットワーク アドレス変換（NAT）を有効にする必要があります。

（注） トラフィックが Cisco IOS XE ファイアウォールと NAT のどちらかまたはその両方によって TCP ポート 135 に送信される場合は、MSRPC ALG が自動的に有効になります。

ファイアウォールと NAT に対する MSRPC ALG サポートに関する制約事項

- TCP ベースの MSRPC のみがサポートされます。
- **allow** コマンドと **reset** コマンドを同時に設定することはできません。
- DPI のために **match protocol msrpc** コマンドを設定する必要があります。
- 宛先ポート 135 に到達したトラフィックのみがサポートされます。この設定はコンフィギュレーションで変更できます。

ファイアウォールと NAT に対する MSRPC ALG サポートに関する情報

アプリケーション レベル ゲートウェイ

アプリケーション レベル ゲートウェイ（ALG）は、アプリケーション レイヤ ゲートウェイとも呼ばれ、アプリケーションパケットのペイロード内の IP アドレス情報を変換するアプリケーションです。ALG は、アプリケーション レイヤ プロトコルを解釈し、ファイアウォールおよびネットワーク アドレス変換（NAT）アクションを実行するために使用されます。これらのアクションは、ファイアウォールおよび NAT の設定に応じて次の 1 つまたは複数のアクションになります。

- クライアント アプリケーションが、ダイナミック TCP または UDP ポートを使用してサーバ アプリケーションと通信できるようにします。
- アプリケーション固有のコマンドを認識し、これらのコマンドに対するきめ細かいセキュリティ制御を提供します。
- データ交換を行う 2 つのホスト間の複数のデータ ストリームまたはデータ セッションを同期します。
- アプリケーション ペイロードで使用できるネットワーク層アドレス情報を変換します。

ファイアウォールがピンホールを開き、アプリケーション レイヤ データストリームの送信元 IP アドレスおよび宛先 IP アドレスを伝送しない TCP または UDP トラフィックに対する変換

サービスをNATが実行します。IPアドレス情報を埋め込む特定のプロトコルまたはアプリケーションにはALGのサポートが必要です。

MSRPC

MSRPCとは、開発者が一連のアプリケーションとサービスをサーバおよび企業にパブリッシュするために使用するフレームワークのことです。RPCはプロセス間通信技術であり、クライアントとサーバ ソフトウェアがネットワーク経由で通信することを可能にします。MSRPC はアプリケーション層プロトコルで、多岐にわたる Microsoft アプリケーションで使用されています。MSRPCは、多種多様なトランスポートプロトコルでコネクション型（CO）およびコネクションレス型（CL）の両方の分散コンピューティング環境（DCE）RPC モードをサポートしています。MSRPC のすべてのサービスは、プライマリ接続と呼ばれる初期セッションを確立します。MSRPC の一部のサービスは、1024 ～ 65535 のポート範囲を宛先ポートとするセカンダリ セッションを確立します。

ファイアウォールと NAT が有効にされる時点で MSRPC を機能させるには、MSRPC パケットのインスペクションに加え、ALG がダイナミック ファイアウォール セッションの確立や NAT 後のパケット コンテンツの修正などの MSRPC 固有の問題を処理する必要があります。

MSRPCプロトコルインスペクションを適用することで、ほとんどのMSRPCサービスがサポートされ、レイヤ 7 ポリシー フィルタの必要がなくなります。

ファイアウォールでの MSRPC ALG

MSRPCプロトコルを検査するようにファイアウォールを設定すると、MSRPC ALG が MSRPC メッセージの解析を開始します。次の表に、ファイアウォールおよびNAT機能のMSRPC ALGでサポートされるプロトコル データ ユニット（PDU）のタイプを記載します。

表 *203 :* サポートされる *PDU* タイプ

PDU	番号	タイプ	説明
REQUEST	0	コール	コール要求を開始します。
RESPONSE	2	コール	コール要求に応答します。
FAULT	3	コール	RPC ランタイム、RPC スタブ、またはRPC 固有の例外を示します。
BIND	11	アソシエーション	本文データのプレゼンテーションネゴシエーションを開始します。
BIND_ACK	12	アソシエーション	バインド要求を受け入れます。
BIND_NAK	13	アソシエーション	アソシエーション要求を拒否します。

PDU	番号	タイプ	説明
ALTER_CONTEXT	14	アソシエーション	別のインターフェイスやバージョンの追加プレゼンテーション ネゴシエーションを要求するか、新しいセキュリティ コンテキストのネゴシエーションを要求するか、あるいはその両方を要求します。
ALTER_CONTEXT_RESP	15	アソシエーション	ALTER_CONTEXT PDU に応答します。有効な値は accept または deny です。
SHUTDOWN	17	コール	接続を終了して関連するリソースを解放するようクライアントに要求します。
CO_CANCEL	18	コール	接続をキャンセルするか、孤立させます。このメッセージは、クライアントでキャンセル失敗が発生すると送信されます。
ORPHANED	19	コール	進行中の要求およびまだ完全に送信されていない要求を中止するか、進行中の（おそらく長い）応答を中断します。

NAT での MSRPC ALG

NAT は MSRPC パケットを受信すると MSRPC ALG を呼び出し、MSRPC ALG によってパケットのペイロードが解析されて、組み込み IP アドレスを変換するためのトークンが形成されます。このトークンが NAT に渡されて、NAT 設定に応じてアドレスまたはポートに変換されます。変換後のアドレスは、MSRPC ALG によってパケットのペイロードに書き込まれます。

ファイアウォールと NAT の両方が設定されている場合、NAT は ALG を最初に呼び出します。

MSRPC ステートフル パーサー

MSRPC ステート マシンまたはパーサーは、MSRPC ALG の中枢部です。MSRPC ステートフル パーサーにより、ファイアウォールまたは NAT（どちらの機能がパーサーを最初に呼び出したかによります）内のすべてのステートフル情報が保持されます。パーサーは、MSRPC プロトコル パケットの DPI を実行します。つまり、プロトコルへの準拠性をチェックし、順序が正しくないコマンドや形式の誤ったパケットを検出します。パケットが解析されると、ステート マシンが各種のデータを記録して、NAT およびファイアウォール インスペクション用に正しいトークン情報を取り込みます。

ファイアウォールと NAT に対する MSRPC ALG サポートの設定方法

（注） NAT が有効になっている場合は、デフォルトで、MSRPC ALG が自動的に有効になります。NAT のみの設定では MSRPC ALG を明示的に有効にする必要はありません。NAT 上で MSRPC ALG を無効にするには、**no ip nat service msrpc** コマンドを使用できます。

レイヤ 4 MSRPC クラス マップおよびポリシー マップの設定

手順の概要

1. **enable**
2. **configure terminal**
3. **class-map type inspect match-any** *class-map-name*
4. **match protocol** *protocol-name*
5. **exit**
6. **policy-map type inspect** *policy-map-name*
7. **class type inspect** *class-map-name*
8. **inspect**
9. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**class-map type inspect match-any** *class-map-name* 例： `Router(config)# class-map type inspect match-any msrpc-cmap`	トラフィック クラスの検査タイプ クラス マップを作成し、QoS クラスマップ コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 4	**match protocol** *protocol-name* 例： `Router(config-cmap)# match protocol msrpc`	指定されたプロトコルを基づくクラスマップの一致基準を設定します。 • 検査タイプ クラス マップでは Cisco IOS XE ステートフル パケット インスペクションがサポートするプロトコルだけを一致基準として使用できます。
ステップ 5	**exit** 例： `Router(config-cmap)# exit`	QoS クラス マップ コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードを開始します。
ステップ 6	**policy-map type inspect** *policy-map-name* 例： `Router(config)# policy-map type inspect msrpc-pmap`	レイヤ 3 またはレイヤ 4 の検査タイプ ポリシー マップを作成し、QoS ポリシーマップ コンフィギュレーション モードを開始します。
ステップ 7	**class type inspect** *class-map-name* 例： `Router(config-pmap)# class type inspect msrpc-class-map`	アクションの実行対象となるトラフィック（クラス）を指定し、QoS ポリシーマップ クラス コンフィギュレーション モードを開始します。
ステップ 8	**inspect** 例： `Router(config-pmap-c)# inspect`	Cisco IOS XE ステートフル パケット インスペクションをイネーブルにします。
ステップ 9	**end** 例： `Router(config-pmap-c)# end`	QoS ポリシーマップ クラス コンフィギュレーション モードを終了し、特権 EXEC モードを開始します。

ゾーン ペアの設定および MSRPC ポリシー マップのアタッチ

手順の概要

1. **enable**
2. **configure terminal**
3. **zone security** *security-zone-name*
4. **exit**
5. **zone security** *security-zone-name*
6. **exit**

7. **zone-pair security** *zone-pair-name* [**source** *source-zone* **destination** [*destination-zone*]]
8. **service-policy type inspect** *policy-map-name*
9. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Rotuer# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**zone security** *security-zone-name* 例： `Router(config)# zone security in-zone`	インターフェイスを割り当てることができるセキュリティ ゾーンを作成し、セキュリティ ゾーン コンフィギュレーション モードを開始します。
ステップ 4	**exit** 例： `Router(config-sec-zone)# exit`	セキュリティ ゾーン コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードを開始します。
ステップ 5	**zone security** *security-zone-name* 例： `Router(config)# zone security out-zone`	インターフェイスを割り当てることができるセキュリティ ゾーンを作成し、セキュリティ ゾーン コンフィギュレーション モードを開始します。
ステップ 6	**exit** 例： `Router(config-sec-zone)# exit`	セキュリティ ゾーン コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードを開始します。
ステップ 7	**zone-pair security** *zone-pair-name* [**source** *source-zone* **destination** [*destination-zone*]] 例： `Router(config)# zone-pair security in-out source in-zone destination out-zone`	ゾーン ペアを作成し、セキュリティ ゾーンペア コンフィギュレーション モードを開始します。 （注） ポリシーを適用するには、ゾーン ペアを設定する必要があります。

	コマンドまたはアクション	目的
ステップ 8	**service-policy type inspect** *policy-map-name* 例： `Router(config-sec-zone-pair)# service-policy type inspect msrpc-pmap`	ファイアウォール ポリシー マップを宛先ゾーン ペアに付加します。 （注） ゾーンのペア間でポリシーが設定されない場合、トラフィックはデフォルトでドロップされます。
ステップ 9	**end** 例： `Router(config-sec-zone-pair)# end`	セキュリティ ゾーン ペア コンフィギュレーション モードを終了して、特権 EXEC モードを開始します。

MSRPC ALG の vTCP サポートの有効化

手順の概要

1. **enable**
2. **configure terminal**
3. **alg vtcp service msrpc**
4. **exit**
5. **set platform hardware qfp active feature alg msrpc tolerance on**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**alg vtcp service msrpc** 例： `Rotuer(config)# alg vtcp service msrpc`	MSRPC ALG の vTCP 機能を有効にします。 （注） デフォルトで、MSRPC ALG は vTCP をサポートします。
ステップ 4	**exit** 例： `Rotuer(config)# exit`	グローバル コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

	コマンドまたはアクション	目的
ステップ 5	**set platform hardware qfp active feature alg msrpc tolerance on** 例： `Rotuer# set platform hardware qfp active feature alg msrpc tolerance on`	MSRPC 不明メッセージの許容を有効にします。 （注） デフォルトでは、許容はオフになっています。

MSRPC ALG の vTCP サポートの無効化

手順の概要

1. **enable**
2. **configure terminal**
3. **no alg vtcp service msrpc**
4. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**no alg vtcp service msrpc** 例： `Rotuer(config)# no alg vtcp service msrpc`	MSRPC ALG の vTCP 機能を無効にします。
ステップ 4	**end** 例： `Rotuer(config)# end`	グローバル コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

ファイアウォールと NAT に対する MSRPC ALG サポートの設定例

例：レイヤ 4 MSRPC クラス マップとポリシー マップの設定

```
Router# configure terminal
Router(config)# class-map type inspect match-any msrpc-cmap
Router(config-cmap)# match protocol msrpc
Router(config-cmap)# exit
Router(config)# policy-map type inspect msrpc-pmap
Router(config-pmap)# class type inspect msrpc-cmap
Router(config-pmap-c)# inspect
Router(config-pmap-c)# end
```

例：ゾーン ペアの設定と MSRPC ポリシー マップのアタッチ

```
Router# configure terminal
Router(config)# zone security in-zone
Router(config-sec-zone)# exit
Router(config)# zone security out-zone
Router(config-sec-zone)# exit
Router(config)# zone-pair security in-out source in-zone destination out-zone
Router(config-sec-zone-pair)# service-policy type inspect msrpc-pmap
Router(config-sec-zone-pair)# end
```

例：MSRPC ALG に対する vTCP サポートの有効化

```
Router# configure terminal
Router(config)# alg vtcp service msrpc
Router(config)# end
```

例：MSRPC ALG に対する vTCP サポートの無効化

```
Router# configure terminal
Router(config)# no alg vtcp service msrpc
Router(config)# end
```

ファイアウォールと NAT に対する MSRPC ALG サポートに関する機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *204* : ファイアウォールと *NAT* に対する *MSRPC ALG* サポートに関する機能情報

機能名	リリース	機能情報
ファイアウォールと NAT に対する MSRPC ALG サポート	Cisco IOS XE リリース 3.5S	ファイアウォールと NAT に対する MSRPC ALG サポート機能は、ファイアウォールと NAT における MSRPC ALG のサポートを提供します。MSRPC ALG は、MSRPC プロトコルのディープ パケット インスペクションを提供します。MSRPC ALG は、プロビジョニング システムと連動して、ネットワーク管理者が MSRPC パケットで検索可能な一致基準を定義する一致フィルタを設定できるようにします。 次のコマンドが導入または変更されました。**ip nat service msrpc**、**match protocol msrpc**。

機能名	リリース	機能情報
ゾーンベース ファイアウォールと NAT に対する MSRPC ALG インスペクション強化	Cisco IOS XE リリース 3.14S	ゾーンベース ファイアウォールと NAT に対する MSRPC ALG インスペクション強化機能は、Cisco ファイアウォール、ネットワーク アドレス変換（NAT）、およびその他のアプリケーションで、さまざまなALGプロトコルが適切にTCP セグメンテーションを処理しセグメントを解析するためのフレームワークを提供する Virtual Transport Control Protocol（vTCP）機能をサポートします。 次のコマンドが導入されました：**alg vtcp service msrpc**

第 151 章

ファイアウォールと NAT に対する Sun RPC ALG サポート

ファイアウォールおよび NAT 対応の Sun RPC ALG のサポート機能により、ファイアウォールおよびネットワーク アドレス変換（NAT）における Sun Microsystems（Sun）リモート プロシージャ コール（RPC）アプリケーション レベル ゲートウェイ（ALG）のサポートが追加されます。Sun RPC は、リモート サーバ プログラム内の関数をクライアント プログラムが呼び出すことができるようにするアプリケーション層プロトコルです。このモジュールでは、Sun RPC ALG を設定する方法について説明します。

ファイアウォールおよび NAT の Sun RPC ALG サポートに関する制約事項

- レイヤ 4 またはレイヤ 7 クラス マップのインスペクション アクションを設定した場合、ポート マッパー プロトコルのウェルノウン ポート（111）に一致するパケットはレイヤ 7 のインスペクションなしでファイアウォールを通過します。レイヤ 7 のインスペクションがない場合、ファイアウォール ピンホールはトラフィック フロー用に開放されず、Sun リモート プロシージャ コール（RPC）がファイアウォールによってブロックされます。回避策として、Sun RPC プログラム番号に対応する **match program-number** コマンドを設定します。
- ポート マッパー プロトコル バージョン 2 のみがサポートされます。他のバージョンはサポートされません。
- RPC バージョン 2 のみサポートされます。

ファイアウォールおよび NAT の Sun RPC ALG サポートについて

アプリケーション レベル ゲートウェイ

アプリケーション レベル ゲートウェイ（ALG）は、アプリケーション レイヤ ゲートウェイとも呼ばれ、アプリケーションパケットのペイロード内のIPアドレス情報を変換するアプリケーションです。ALG は、アプリケーション レイヤ プロトコルを解釈し、ファイアウォールおよびネットワーク アドレス変換（NAT）アクションを実行するために使用されます。これらのアクションは、ファイアウォールおよび NAT の設定に応じて次の 1 つまたは複数のアクションになります。

- クライアント アプリケーションが、ダイナミック TCP または UDP ポートを使用してサーバ アプリケーションと通信できるようにします。
- アプリケーション固有のコマンドを認識し、これらのコマンドに対するきめ細かいセキュリティ制御を提供します。
- データ交換を行う 2 つのホスト間の複数のデータ ストリームまたはデータ セッションを同期します。
- アプリケーション ペイロードで使用できるネットワーク層アドレス情報を変換します。

ファイアウォールがピンホールを開き、アプリケーション レイヤ データストリームの送信元 IP アドレスおよび宛先 IP アドレスを伝送しない TCP または UDP トラフィックに対する変換サービスを NAT が実行します。IP アドレス情報を埋め込む特定のプロトコルまたはアプリケーションには ALG のサポートが必要です。

Sun RPC

Sun リモート プロシージャ コール（RPC）アプリケーション レベル ゲートウェイ（ALG）は、Sun RPC プロトコルのディープ パケット インスペクションを実行します。Sun RPC ALG は、管理者が一致フィルタを設定できるプロビジョニング システムと連動します。一致フィルタはそれぞれ、Sun RPC パケット内で検索される一致基準を定義し、それにより、基準に一致するパケットのみ許可されます。

RPC では、クライアント プログラムは、サーバ プログラム内のプロシージャを呼び出します。RPC ライブラリは、プロシージャ引数をネットワーク メッセージ内にパッケージ化し、そのメッセージをサーバに送信します。次にサーバは、RPC ライブラリを使用して、ネットワーク メッセージからプロシージャ引数を取り出し、指定されたサーバ プロシージャを呼び出します。サーバ プロシージャが RPC に戻ると、戻り値がネットワーク メッセージ内にパッケージ化され、クライアントに送り返されます。

Sun RPC プロトコルの詳細については、RFC 1057、『*RPC: Remote Procedure Call Protocol Specification Version 2*』を参照してください。

ファイアウォール向けの Sun RPC ALG のサポート

ポリシーおよびクラス マップを使用して作成されるゾーンベース ファイアウォールを使用して Sun RPC ALG を設定できます。レイヤ 7 クラス マップを使用することで、ネットワーク管理者は一致フィルタを設定できます。フィルタはSun RPCパケット内で検索されるプログラム番号を指定します。Sun RPC レイヤ 7 ポリシーマップは、**service-policy** コマンドを使用するレイヤ 4 ポリシーマップの子ポリシーとして設定します。

レイヤ 7 ファイアウォール ポリシーを設定しないで Sun RPC レイヤ 4 クラス マップを設定すると、Sun RPC トラフィックにより戻されるトラフィックはファイアウォールを通過しますが、セッションはレイヤ 7 で検査されません。セッションが検査されないため、後続の RPC コールはファイアウォールによってブロックされます。Sun RPC レイヤ 4 クラス マップおよびレイヤ 7 ポリシーを設定すると、レイヤ 7 インスペクションが使用できるようになります。空のレイヤ7ファイアウォールポリシー、つまり、一致フィルタが設定されていないポリシーを設定できます。

NAT 向けの Sun RPC ALG のサポート

デフォルトでは、ネットワーク アドレス変換（NAT）が有効な場合、Sun RPC ALG は自動的に有効になります。NAT で Sun RPC ALG を無効にするには、**no ip nat service alg** コマンドを使用します。

ファイアウォールおよび NAT の Sun RPC ALG サポートの設定方法

ファイアウォールおよびNAT が有効にされている場合に Sun RPC を動作させるには、ALG で Sun RPC パケットを検査する必要があります。また ALG では、ダイナミック ファイアウォール セッションの確立や NAT 変換後のパケット コンテンツの修正など、Sun RPC 固有の問題も処理します。

Sun RPC ALG 用のファイアウォールの設定

Sun RPC プロトコルの検査アクションを設定している場合（つまり、レイヤ 4 クラスマップで **match protocol sunrpc** コマンドを指定している場合）は、レイヤ 7 Sun リモートプロシージャコール（RPC）ポリシーマップを設定する必要があります。

セキュリティ ゾーンと検査ルールの両方を同じインターフェイス上で設定しないことを推奨します。これは、このような設定は機能しない場合があるためです。

Sun RPC ALG 対応のファイアウォールを設定するには、次の作業を実行します。

ファイアウォール ポリシー用のレイヤ 4 クラス マップの設定

ネットワーク トラフィックを分類するためのレイヤ 4 クラス マップを設定するには、この作業を実行します。**class-map type inspect** コマンドで **match-all** キーワードを指定すると、クラスマップ内の（プログラム番号として指定された）すべてのSunリモートプロシージャコール

（RPC）レイヤ 7 フィルタに Sun RPC トラフィックがマッチします。**class-map type inspect** で **match-any** キーワードを指定すると、クラスマップ内の（プログラム番号として指定された）少なくとも 1 つの Sun RPC レイヤ 7 フィルタに Sun RPC トラフィックがマッチする必要があります。

レイヤ 4 クラスマップを設定するには、**class-map type inspect {match-any | match-all}** *classm-map-name* コマンドを使用します。

手順の概要

1. **enable**
2. **configure terminal**
3. **class-map type inspect** {**match-any** | **match-all**} *class-map-name*
4. **match protocol** *protocol-name*
5. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**class-map type inspect** {**match-any** | **match-all**} *class-map-name* 例： `Device(config)# class-map type inspect match-any sunrpc-l4-cmap`	レイヤ 4 検査タイプ クラス マップを作成し、QoS クラスマップ コンフィギュレーション モードを開始します。
ステップ 4	**match protocol** *protocol-name* 例： `Device(config-cmap)# match protocol sunrpc`	指定されたプロトコルに基づき、クラスマップの一致基準を設定します。
ステップ 5	**end** 例： `Device(config-cmap)# end`	QoS クラスマップ コンフィギュレーション モードを終了し、特権 EXEC モードを開始します。

ファイアウォール ポリシー用のレイヤ 7 クラス マップの設定

ネットワーク トラフィックを分類するためのレイヤ 7 クラス マップを設定するには、この作業を実行します。この設定により、Sun RPC を使用する mount（100005）、ネットワーク ファイル システム（NFS）（100003）などのプログラムが使用可能になります。100005 および

100003 は Sun RPC プログラムの番号です。デフォルトでは、Sun RPC ALG はすべてのプログラムをブロックします。

Sun RPC プログラムおよびプログラム番号の詳細については、RFC 1057、『*RPC: Remote Procedure Call Protocol Specification Version 2*』を参照してください。

レイヤ 7 クラスマップを設定するには、**class-map type inspect** *protocol-name* コマンドを使用します。

手順の概要

1. **enable**
2. **configure terminal**
3. **class-map type inspect** *protocol-name* {**match-any** | **match-all**} *class-map-name*
4. **match program-number** *program-number*
5. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**class-map type inspect** *protocol-name* {**match-any** | **match-all**} *class-map-name* 例： `Device(config)# class-map type inspect sunrpc match-any sunrpc-l7-cmap`	レイヤ 7（アプリケーション固有）検査タイプ クラスマップを作成し、QoS クラスマップ コンフィギュレーション モードを開始します。
ステップ 4	**match program-number** *program-number* 例： `Device(config-cmap)# match program-number 100005`	許可する RPC プロトコル プログラム番号を一致基準として指定します。
ステップ 5	**end** 例： `Device(config-cmap)# end`	QoS クラスマップ コンフィギュレーション モードを終了し、特権 EXEC モードを開始します。

Sun RPC ファイアウォール ポリシー マップの設定

Sun リモート プロシージャ コール（RPC）ファイアウォール ポリシーマップを設定するには、この作業を実行します。ポリシー マップを使用して、レイヤ 7 ファイアウォール ポリシーのクラス マップで定義する Sun RPC レイヤ 7 クラスごとにパケット転送を許可します。

手順の概要

1. **enable**
2. **configure terminal**
3. **policy-map type inspect** *protocol-name policy-map-name*
4. **class type inspect** *protocol-name class-map-name*
5. **allow**
6. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**policy-map type inspect** *protocol-name policy-map-name* 例： `Device(config)# policy-map type inspect sunrpc sunrpc-l7-pmap`	レイヤ 7（プロトコル固有）検査タイプ ポリシーマップを作成し、QoS ポリシーマップ コンフィギュレーション モードを開始します。
ステップ 4	**class type inspect** *protocol-name class-map-name* 例： `Device(config-pmap)# class type inspect sunrpc sunrpc-l7-cmap`	アクションの実行対象となるトラフィック クラスを指定し、QoS ポリシー マップ クラス コンフィギュレーション モードを開始します。
ステップ 5	**allow** 例： `Device(config-pmap-c)# allow`	パケット転送を許可します。
ステップ 6	**end** 例： `Device(config-pmap-c)# end`	QoS ポリシー マップ クラス コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

レイヤ 7 ポリシー マップをレイヤ 4 ポリシー マップにアタッチする

手順の概要

1. **enable**
2. **configure terminal**
3. **policy-map type inspect** *policy-map-name*
4. **class** {*class-map-name* | **class-default**}
5. **inspect** [*parameter-map-name*]
6. **service-policy** *protocol-name policy-map-name*
7. **exit**
8. **class class-default**
9. **drop**
10. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**policy-map type inspect** *policy-map-name* 例： `Device(config)# policy-map type inspect sunrpc-l4-pmap`	レイヤ 4 検査タイプ ポリシーマップを作成し、QoS ポリシーマップ コンフィギュレーション モードを開始します。
ステップ 4	**class** {*class-map-name*	**class-default**} 例： `Device(config-pmap)# class sunrpc-l4-cmap`	アクションを実行する対象（クラス）を関連付け、QoS ポリシー マップ クラス コンフィギュレーション モードを開始します。
ステップ 5	**inspect** [*parameter-map-name*] 例： `Device(config-pmap-c)# inspect`	ステートフル パケット インスペクションをイネーブルにします。
ステップ 6	**service-policy** *protocol-name policy-map-name* 例： `Device(config-pmap-c)# service-policy sunrpc sunrpc-l7-pmap`	レイヤ 7 ポリシー マップをトップレベルのレイヤ 4 ポリシー マップにアタッチします。

	コマンドまたはアクション	目的
ステップ 7	**exit** 例： `Device(config-pmap-c)# exit`	QoS ポリシー マップ クラス コンフィギュレーション モードを終了し、QoS ポリシー マップ コンフィギュレーション モードに戻ります。
ステップ 8	**class class-default** 例： `Device(config-pmap)# class class-default`	ポリシーを設定する前にデフォルト クラス（一般的にクラスデフォルト クラスと呼ばれます）を指定し、QoS ポリシー マップ クラス コンフィギュレーション モードを開始します。
ステップ 9	**drop** 例： `Device(config-pmap-c)# drop`	特定のクラスに属するパケットを廃棄するトラフィック クラスを設定します。
ステップ 10	**end** 例： `Device(config-pmap-c)# end`	QoS ポリシー マップ クラス コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

セキュリティ ゾーンとゾーン ペアの作成、およびゾーン ペアへのポリシー マップの付加

ゾーン ペアを作成するには、2 つのセキュリティ ゾーンが必要です。ただし、1 つのセキュリティ ゾーンのみ作成でき、もう 1 つのセキュリティ ゾーンはシステム定義のセキュリティ ゾーンにすることができます。システム定義のセキュリティゾーンまたはセルフゾーンを作成するには、**self** キーワードを指定した **zone-pair security** コマンドを設定します。

（注） セルフ ゾーンを選択する場合、検査アクションは設定できません。

このタスクの内容は以下のとおりです。

- セキュリティ ゾーンを作成します。
- ゾーン ペアを定義します。
- セキュリティ ゾーンにインターフェイスを割り当てます。
- ポリシー マップをゾーン ペアに付加します。

手順の概要

1. **enable**
2. **configure terminal**
3. **zone security** {*zone-name* | **default**}
4. **exit**
5. **zone security** {*zone-name* | **default**}

6. **exit**
7. **zone-pair security** *zone-pair-name* **source** *source-zone-name* **destination** *destination-zone-name*
8. **service-policy type inspect** *policy-map-name*
9. **exit**
10. **interface** *type number*
11. **ip address** *ip-address mask* [**secondary** [**vrf** *vrf-name*]]
12. **zone-member security** *zone-name*
13. **exit**
14. **interface** *type number*
15. **ip address** *ip-address mask* [**secondary** [**vrf** *vrf-name*]]
16. **zone-member security** *zone-name*
17. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**zone security** {*zone-name* | **default**} 例： `Device(config)# zone security z-client`	セキュリティ ゾーンを作成し、セキュリティ ゾーン コンフィギュレーション モードを開始します。 • 設定では送信元ゾーンと宛先ゾーンという、ゾーン ペアを作成するための 2 つのセキュリティ ゾーンが必要です。 • ゾーン ペアでは、デフォルト ゾーンまたはセルフ ゾーンを送信元ゾーンまたは宛先ゾーンとして使用できます。
ステップ 4	**exit** 例： `Device(config-sec-zone)# exit`	セキュリティ ゾーン コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードに戻ります。
ステップ 5	**zone security** {*zone-name* | **default**} 例： `Device(config)# zone security z-server`	セキュリティ ゾーンを作成し、セキュリティ ゾーン コンフィギュレーション モードを開始します。 • 設定では送信元ゾーンと宛先ゾーンという、ゾーン ペアを作成するための 2 つのセキュリティ ゾーンが必要です。

	コマンドまたはアクション	目的
		• ゾーン ペアでは、デフォルト ゾーンを送信元ゾーンまたは宛先ゾーンとして使用できます。
ステップ 6	**exit** 例： `Device(config-sec-zone)# exit`	セキュリティ ゾーン コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードに戻ります。
ステップ 7	**zone-pair security** *zone-pair-name* **source** *source-zone-name* **destination** *destination-zone-name* 例： `Device(config)# zone-pair security clt2srv source z-client destination z-server`	ゾーン ペアを作成し、セキュリティ ゾーンペア コンフィギュレーション モードを開始します。
ステップ 8	**service-policy type inspect** *policy-map-name* 例： `Device(config-sec-zone-pair)# service-policy type inspect sunrpc-l4-pmap`	ファイアウォール ポリシー マップをゾーン ペアに付加します。
ステップ 9	**exit** 例： `Device(config-sec-zone-pair)# exit`	セキュリティ ゾーン ペア コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードに戻ります。
ステップ 10	**interface** *type number* 例： `Device(config)# interface gigabitethernet 2/0/0`	インターフェイス タイプを設定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 11	**ip address** *ip-address mask* [**secondary** [**vrf** *vrf-name*]] 例： `Device(config-if)# ip address 192.168.6.5 255.255.255.0`	インターフェイスに対するプライマリ IP アドレスまたはセカンダリ IP アドレスを設定します。
ステップ 12	**zone-member security** *zone-name* 例： `Device(config-if)# zone-member security z-client`	インターフェイスをセキュリティ ゾーンにアタッチします。
ステップ 13	**exit** 例： `Device(config-if)# exit`	インターフェイス設定モードを終了し、グローバル設定モードに戻ります。
ステップ 14	**interface** *type number* 例： `Device(config)# interface gigabitethernet 2/1/1`	インターフェイス タイプを設定し、インターフェイス コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 15	**ip address** *ip-address mask* [**secondary** [**vrf** *vrf-name*]] 例： `Device(config-if)# ip address 192.168.6.1 255.255.255.0`	インターフェイスに対するプライマリ IP アドレスまたはセカンダリ IP アドレスを設定します。
ステップ 16	**zone-member security** *zone-name* 例： `Device(config-if)# zone-member security z-server`	インターフェイスをセキュリティ ゾーンにアタッチします。
ステップ 17	**end** 例： `Device(config-if)# end`	インターフェイス コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

ファイアウォールと NAT に対する Sun RPC ALG サポートの設定例

例：ファイアウォール ポリシー用のレイヤ 4 クラス マップの設定

```
Device# configure terminal
Device(config)# class-map type inspect match-any sunrpc-l4-cmap
Device(config-cmap)# match protocol sunrpc
Device(config-cmap)# end
```

例：ファイアウォール ポリシー用のレイヤ 7 クラス マップの設定

```
Device# configure terminal
Device(config)# class-map type inspect sunrpc match-any sunrpc-l7-cmap
Device(config-cmap)# match program-number 100005
Device(config-cmap)# end
```

例：Sun RPC ファイアウォール ポリシー マップの設定

```
Device# configure terminal
Device(config)# policy-map type inspect sunrpc sunrpc-l7-pmap
Device(config-pmap)# class type inspect sunrpc sunrpc-l7-cmap
Device(config-pmap-c)# allow
Device(config-pmap-c)# end
```

例：レイヤ 4 ポリシー マップへのレイヤ 7 ポリシー マップのアタッチ

```
Device# configure terminal
Device(config)# policy-map type inspect sunrpcl4-pmap
Device(config-pmap)# class sunrpcl4-cmap
Device(config-pmap-c)# inspect
Device(config-pmap-c)# service-policy sunrpc sunrpc-l7-pmap
Device(config-pmap-c)# exit
Device(config-pmap)# class class-default
Device(config-pmap-c)# drop
Device(config-pmap-c)# end
```

例：セキュリティ ゾーンとゾーン ペアの作成とゾーン ペアへのポリシー マップのアタッチ

```
Device# configure terminal
Device(config)# zone security z-client
Device(config-sec-zone)# exit
Device(config)# zone security z-server
Device(config-sec-zone)# exit
Device(config)# zone-pair security clt2srv source z-client destination z-server
Device(config-sec-zone-pair)# service-policy type inspect sunrpc-l4-pmap
Device(config-sec-zone-pair)# exit
Device(config)# interface gigabitethernet 2/0/0
Device(config-if)# ip address 192.168.6.5 255.255.255.0
Device(config-if)# zone-member security z-client
Device(config-if)# exit
Device(config)# interface gigabitethernet 2/1/1
Device(config-if)# ip address 192.168.6.1 255.255.255.0
Device(config-if)# zone-member security z-server
Device(config-if)# end
```

例：Sun RPC ALG 用のファイアウォールの設定

Sun リモート プロシージャ コール（RPC）アプリケーション レベル ゲートウェイ（ALG）サポート用のファイアウォール設定の例を以下に示します。

```
class-map type inspect sunrpc match-any sunrpc-l7-cmap
 match program-number 100005
!
class-map type inspect match-any sunrpc-l4-cmap
 match protocol sunrpc
!
!
policy-map type inspect sunrpc sunrpc-l7-pmap
 class type inspect sunrpc sunrpc-l7-cmap
  allow
!
!
policy-map type inspect sunrpc-l4-pmap
 class type inspect sunrpc-l4-cmap
  inspect
  service-policy sunrpc sunrpc-l7-pmap
```

```
!
 class class-default
  drop
!
!
zone security z-client
!
zone security z-server
!
zone-pair security clt2srv source z-client destination z-server
 service-policy type inspect sunrpc-l4-pmap
!
interface GigabitEthernet 2/0/0
 ip address 192.168.10.1 255.255.255.0
 zone-member security z-client
!
interface GigabitEthernet 2/1/1
 ip address 192.168.23.1 255.255.255.0
 zone-member security z-server
!
```

ファイアウォールと NAT に対する Sun RPC ALG サポートに関する追加情報

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『Master Command List, All Releases』
IP アドレッシング コマンド	『IP Addressing Services Command Reference』
セキュリティ コマンド	• 『Security Command Reference: Commands A to C』 • 『Security Command Reference: Commands D to L』 • 『Security Command Reference: Commands M to R』 • 『Security Command Reference: Commands S to Z』

標準および RFC

標準/RFC	タイトル
RFC 1057	『*RPC: Remote Procedure Call Protocol Specification Version 2*』

シスコのテクニカル サポート

説明	リンク
右の URL にアクセスして、シスコのテクニカル サポートを最大限に活用してください。これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

ファイアウォールと NAT に対する Sun RPC ALG サポートに関する機能情報

表 *205 :* ファイアウォールと *NAT* に対する *Sun RPC ALG* サポートに関する機能情報

機能名	リリース	機能情報
ファイアウォールと NAT に対する Sun RPC ALG サポート	Cisco IOS XE リリース 3.2S	ファイアウォールと NAT に対する Sun RPC ALG サポート機能は、ファイアウォールと NAT に Sun RPC ALG のサポートを追加します。 次のコマンドが導入または変更されました。**match protocol**。

第 152 章

ゾーンベース ファイアウォール ALG および AIC 条件付きデバッグおよびパケット トレースのサポート

ゾーンベース ファイアウォール ALG および AIC 条件付きデバッグおよびパケット トレースの機能は、アプリケーション レイヤ ゲートウェイ（ALG）とアプリケーション検査および制御（AIC）の次の機能をサポートしています。

- パケット トレース
- 条件付きデバッグ
- デバッグ ログ

ゾーンベース ファイアウォール ALG および AIC 条件付きデバッグおよびパケット トレースのサポートに関する情報

パケット トレース

パケット トレースを有効にすると、ルータ スループットへの影響を最小限に抑えて、指定のパケット フローのコントロール プレーン ポリシング（CPP）統計情報を生成できます。また、

フロー内の各パケットのパスもトレースされるため、入力インターフェイス、使用された機能、出力パスを判別する上で役立ちます。

アプリケーション層ゲートウェイ（ALG）が統計情報を生成し、パケットの移動パスのログを保持します。

条件付きデバッグ

送信元アドレスまたは宛先アドレスからの特定の接続が失敗するという一般的なアプリケーション レイヤ ゲートウェイ（ALG）対応シナリオでは、デバッグを実行すると、ALG を経由するすべてのトラフィックに関するメッセージのリストが表示されます。条件付きデバッグを有効にすると、指定された接続に関連するデバッグ メッセージがコンソールに表示されます。この機能が導入されるまでは、デバッグにより、ALG を通過するすべてのトラフィックに関する多数のメッセージが表示されました。

デバッグ ログ

次のシビラティ（重大度）が追加されました。

1. Error：エラーおよびファイアウォール パケット ドロップの条件。

   例：

   - パケットを送信できない。
   - ALG エラー状態

2. Warning：警告デバッグ メッセージ。
3. Info：イベントに関する情報。

   例：

   - ポリシー設定、不正なパケット、またはハードコーディングされている制限としきい値が原因で発生したパケット ドロップ。
   - ステート マシン遷移
   - ALG チェック ステータス
   - パケット パスおよびパケット ドロップのステータス。

4. Verbose：すべてのログ メッセージ。

   例：

   - データ構造
   - イベントの詳細

（注） ALG-AIC 機能デバッグ フラグとシビラティ（重大度）はどちらも設定する必要があります。シビラティ（重大度）だけが設定され、ALG-AIC機能デバッグ フラグが設定されていないと、デバッグ ログが無効になります。ALG-AIC 機能デバッグ フラグだけが設定されている場合、Info レベル（デフォルトのシビラティ（重大度））がログに記録されます。

ゾーンベース ファイアウォール ALG および AIC 条件付きデバッグおよびパケット トレースのサポートに関する追加情報

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『Cisco IOS Master Command List, All Releases』
ファイアウォール コマンド	• 『Cisco IOS Security Command Reference: Commands A to C』 • 『Cisco IOS Security Command Reference: Commands D to L』 [英語] • 『Cisco IOS Security Command Reference: Commands M to R』 [英語] • 『Cisco IOS Security Command Reference: Commands S to Z』 [英語]

シスコのテクニカル サポート

説明	リンク
シスコのサポート Web サイトでは、シスコの製品やテクノロジーに関するトラブルシューティングにお役立ていただけるように、マニュアルやツールをはじめとする豊富なオンライン リソースを提供しています。 お使いの製品のセキュリティ情報や技術情報を入手するために、Cisco Notification Service（Field Notice からアクセス）、Cisco Technical Services Newsletter、Really Simple Syndication（RSS）フィードなどの各種サービスに加入できます。 シスコのサポート Web サイトのツールにアクセスする際は、Cisco.com のユーザ ID およびパスワードが必要です。	http://www.cisco.com/support

ゾーンベース ファイアウォール ALG および AIC 条件付きデバッグおよびパケット トレースのサポートに関する機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *206*：ゾーンベース ファイアウォール *ALG* および *AIC* 条件付きデバッグおよびパケット トレースのサポートに関する機能情報

機能名	リリース	機能情報
ゾーンベース ファイアウォール ALG および AIC 条件付きデバッグおよびパケット トレースのサポート	Cisco IOS XE 3.13S	この機能は、次の機能をサポートしています。 • パケット トレース • 条件付きデバッグ • デバッグ ログ

第 153 章

ファイアウォールと NAT に対するハイ アベイラビリティ サポートを使用した ALG - H.323 vTCP

ファイアウォールおよび NAT 対応のハイ アベイラビリティ サポートを備えた ALG—H.323 vTCP 機能により、H.323 アプリケーション レベル ゲートウェイ（ALG）が拡張され、単一 H.323 メッセージではない TCP セグメントをサポートします。仮想 TCP（vTCP）は TCP セグメント リアセンブルをサポートします。この機能の導入前は、H.323 ALG は TCP セグメントが完全な H.323 メッセージである場合にだけ TCP セグメントを処理していました。TCP セグメントに複数のメッセージが含まれていた場合は、H.323 ALG が TCP セグメントを無視し、そのパケットは処理されずに転送されていました。

このモジュールでは、ファイアウォールおよび NAT 対応のハイ アベイラビリティ（HA）サポートを備えた ALG—H.323 vTCP を設定する方法について説明します。

ファイアウォールと NAT に対するハイ アベイラビリティ サポートを使用した ALG - H.323 vTCP に関する制約事項

- 着信 TCP セグメントが完全な H.323 メッセージでない場合は、H.323 ALG がその TCP セグメントをバッファリングしメッセージの残りの部分を待機します。バッファリングされたデータは、ハイ アベイラビリティ（HA）用のスタンバイ デバイスに同期されません。
- vTCP がデータのバッファリングを開始した時点で、H.323 ALG のパフォーマンスに影響する可能性があります。

ファイアウォールと NAT に対するハイ アベイラビリティ サポートを使用した ALG - H.323 vTCP に関する情報

アプリケーション レベル ゲートウェイ

アプリケーション レベル ゲートウェイ（ALG）は、アプリケーション レイヤ ゲートウェイとも呼ばれ、アプリケーション パケットのペイロード内の IP アドレス情報を変換するアプリケーションです。ALG は、アプリケーション レイヤ プロトコルを解釈し、ファイアウォールおよびネットワーク アドレス変換（NAT）アクションを実行するために使用されます。これらのアクションは、ファイアウォールおよび NAT の設定に応じて次の 1 つまたは複数のアクションになります。

- クライアント アプリケーションが、ダイナミック TCP または UDP ポートを使用してサーバ アプリケーションと通信できるようにします。
- アプリケーション固有のコマンドを認識し、これらのコマンドに対するきめ細かいセキュリティ制御を提供します。
- データ交換を行う 2 つのホスト間の複数のデータ ストリームまたはデータ セッションを同期します。
- アプリケーション ペイロードで使用できるネットワーク層アドレス情報を変換します。

ファイアウォールがピンホールを開き、アプリケーション レイヤ データストリームの送信元 IP アドレスおよび宛先 IP アドレスを伝送しない TCP または UDP トラフィックに対する変換サービスを NAT が実行します。IP アドレス情報を埋め込む特定のプロトコルまたはアプリケーションには ALG のサポートが必要です。

基本 H.323 ALG サポート

H.323は、パケットベース ネットワーク経由でのマルチメディア送信用の一連のネットワーク要素およびプロトコルを定義する ITU-T が公開している推奨事項です。H.323 は、マルチメディアの送信で使用されるさまざまなネットワーク要素を定義します。

現在、ほとんどの H.323 実装ではシグナリング用の転送メカニズムとして TCP が利用されていますが、H.323 バージョン 2 では基本 UDP トランスポートが有効になります。

- H.323 端末：この要素は、別の H.323 端末またはゲートウェイとの双方向通信を行うネットワークのエンドポイントです。
- H.323 ゲートウェイ：この要素は、H.323 端末と H.323 をサポートしないその他の端末との間のプロトコル変換を行います。
- H.323 ゲートキーパー：この要素は、アドレス変換、ネットワーク アクセス コントロール、帯域幅管理といったサービスを提供し、H.323 端末およびゲートウェイで構成されます。

次のコア プロトコルが H.323 仕様で規定されています。

- H.225：このプロトコルは、任意の 2 つの H.323 エンティティ間で通信を確立するために使用されるコール シグナリング方式を規定します。
- H.225 Registration, Admission, and Status（RAS）：このプロトコルは、アドレス解決およびアドミッション制御サービスのために、H.323 エンドポイントとゲートウェイによって使用されます。
- H.245：このプロトコルは、マルチメディア通信機能の交換と、オーディオ、ビデオ、およびデータ用の論理チャネルの開閉のために使用されます。

H.323 仕様では上記のプロトコルの他に、さまざまな IETF プロトコル（Real-time Transport Protocol（RTP）プロトコルや、オーディオ（G.711、G.729 など）およびビデオ（H.261、H.263、および H.264）コーデックなど）の使用についても規定しています。

NAT では、パケット ペイロード内の埋め込み IP アドレスおよびポート番号の変換や、制御チャネルからの新規接続/セッション情報の取得といった、レイヤ 7 プロトコル固有のサービスを処理するために、さまざまな ALG を必要とします。H.323 ALG は、H.323 メッセージに対してこれらの特定サービスを実行します。

vTCP for ALG サポートの概要

レイヤ 7 プロトコルが TCP を使用してデータ転送を行う際は、アプリケーションの設計、最大セグメント サイズ（MSS）、TCP ウィンドウ サイズなどのさまざまな理由によって TCP ペイロードがセグメント化される場合があります。ファイアウォールと NAT がサポートするアプリケーション レベル ゲートウェイ（ALG）には、パケット インスペクションで TCP フラグメントを認識する機能がありません。vTCP が、ALG を使用して TCP セグメントを認識し、TCP ペイロードを解析する汎用フレームワークになります。

vTCP は、組み込みデータを書き直すために TCP ペイロード全体を必要とする NAT や Session Initiation Protocol（SIP）などのアプリケーションに役立ちます。ファイアウォールでは vTCP を使用して、ALG がパケット間でのデータ分割をサポートできるようにします。

ファイアウォールまたは NAT ALG を設定すると、vTCP 機能が有効になります。

vTCP は、現在のところ、Real Time Streaming Protocol（RTSP）および DNS ALG をサポートしています。

TCP 確認応答と確実な送信

vTCP は 2 つの TCP ホストの間に存在するため、TCP セグメントをもう一方のホストに送信する前に一時的に保存するためのバッファ スペースが必要です。vTCP はホスト間の適切なデータ伝送を保証します。vTCP は伝送するデータがさらに必要な場合は、送信側ホストに TCP 確認応答（ACK）を送信します。また、TCP フローの最初から受信側ホストが送信する ACK をトラッキングして、確認応答されたデータを詳細にモニタします。

vTCP は、TCP セグメントを再構成します。着信セグメントの IP ヘッダーおよび TCP ヘッダー情報は、確実に送信されるように vTCP バッファに保存されます。

NAT 対応アプリケーションの場合、vTCP は発信セグメントの長さにマイナーな変更を加えることができます。vTCP は最後のセグメントのデータ長を大きくするか、新しいセグメントを作成して、追加のデータを伝送することができます。新しく作成されたセグメントの IP ヘッダーまたは TCP ヘッダーは、オリジナルの着信セグメントから派生したものです。IP ヘッダーの合計の長さと TCP ヘッダーのシーケンス番号は、必要に応じて調整されます。

NAT ALG とファイアウォール ALG を使用した vTCP

ALG は、NAT およびファイアウォールのサブコンポーネントです。NAT とファイアウォールのいずれにも、ダイナミックに ALG を連結させるためのフレームワークがあります。ファイアウォールがレイヤ 7 インスペクションを実行する場合または NAT がレイヤ 7 フィックスアップを実行する場合は、ALG によって登録されたパーサー機能が呼び出され、ALG がパケット インスペクションを引き継ぎます。vTCP は、NAT またはファイアウォールとこれらのアプリケーションを使用する ALG を仲介します。つまり、パケットは、まず、vTCP で処理されてから、ALG に渡されます。vTCP は、TCP 接続内の両方向で TCP セグメントを再構築します。

ALG の概要：高可用性をサポートする H.323 vTCP

ファイアウォールおよび NAT の高可用性をサポートする ALG/H.323 vTCP 機能は、単一の H.323 メッセージではない TCP セグメントをサポートするように H.323 アプリケーション レベル ゲートウェイ（ALG）を拡張します。H.323 ALG が vTCP と結合されると、ファイアウォールと NAT は vTCP を使用して H.323 ALG と対話するようになります。vTCP ではバッファ内のデータをスタンバイ デバイスに同期できないため、vTCP がデータのバッファリングを開始すると高可用性（HA）機能が影響を受けます。vTCP がデータをバッファリングしているときにスタンバイ デバイスへのスイッチオーバーが発生すると、バッファ内のデータがスタンバイ デバイスに同期されていないために接続がリセットされる可能性があります。vTCP がバッファ内のデータを確認応答した後は、そのデータは失われ、接続がリセットされます。ファイア

ウォールと NAT は HA を確保するためにスタンバイ デバイスにデータを同期しますが、vTCP がスタンバイ デバイスに同期するのは現在の接続のステータスだけなので、エラーが発生すると接続がリセットされます。

ファイアウォールと NAT に対するハイ アベイラビリティ サポートを使用した ALG - H.323 vTCP の設定方法

ALG の設定：ファイアウォール用のハイ アベイラビリティ サポートを備えた H.323 vTCP

手順の概要

1. **enable**
2. **configure terminal**
3. **class-map type inspect match-any** *class-map-name*
4. **match protocol** *protocol-name*
5. **match protocol** *protocol-name*
6. **exit**
7. **policy-map type inspect** *policy-map-name*
8. **class type inspect** *class-map-name*
9. **inspect**
10. **exit**
11. **class class-default**
12. **exit**
13. **zone security** *zone-name*
14. **exit**
15. **zone-pair security** *zone-pair-name* **source** *source-zone* **destination** *destination-zone*
16. **service-policy type inspect** *policy-map-name*
17. **exit**
18. **interface** *type number*
19. **zone member security** *zone-name*
20. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします • パスワードを入力します（要求された場合）。

	コマンドまたはアクション	目的
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**class-map type inspect match-any** *class-map-name* 例： `Device(config)# class-map type inspect match-any h.323-class`	検査タイプ クラス マップを作成し、QoS クラス マップ コンフィギュレーション モードを開始します。
ステップ 4	**match protocol** *protocol-name* 例： `Device(config-cmap)# match protocol h323`	指定されたプロトコルを基づいて、クラス マップの一致基準を設定します。
ステップ 5	**match protocol** *protocol-name* 例： `Device(config-cmap)# match protocol h323ras`	指定されたプロトコルを基づいて、クラス マップの一致基準を設定します。
ステップ 6	**exit** 例： `Device(config-cmap)# exit`	QoS クラス マップ コンフィギュレーション モードを終了し、グローバルコンフィギュレーションモードを開始します。
ステップ 7	**policy-map type inspect** *policy-map-name* 例： `Device(config)# policy-map type inspect h.323-policy`	検査タイプ ポリシー マップを作成し、QoS ポリシー マップ コンフィギュレーション モードを開始します。
ステップ 8	**class type inspect** *class-map-name* 例： `Device(config-pmap)# class type inspect h.323-class`	アクションを実行するクラスを指定し、QoS ポリシーマップ クラス コンフィギュレーション モードを開始します。
ステップ 9	**inspect** 例： `Device(config-pmap-c)# inspect`	ステートフル パケット インスペクションをイネーブルにします。
ステップ 10	**exit** 例： `Device(config-pmap-c)# exit`	QoS ポリシー マップ クラス コンフィギュレーション モードを終了し、ポリシー マップ コンフィギュレーション モードを開始します。
ステップ 11	**class class-default** 例： `Device(config-pmap)# class class-default`	ポリシー マップ設定を、事前に定義したデフォルト クラスに適用します。 • 設定済みクラス マップの一致基準のいずれともトラフィックが一致しない場合、事前に定義されたデフォルト クラスに誘導されます。

	コマンドまたはアクション	目的
ステップ 12	**exit** 例： `Device(config)# exit`	QoS ポリシー マップ コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードを開始します。
ステップ 13	**zone security** *zone-name* 例： `Device(config)# zone security inside`	インターフェイスを割り当てることができるセキュリティ ゾーンを作成し、セキュリティ ゾーン コンフィギュレーション モードを開始します。 • ゾーン ペアを作成するには2つのセキュリティ ゾーン（送信元ゾーンと宛先ゾーン）が設定に含まれる必要があります。 • ゾーン ペアでは、送信元ゾーンまたは宛先ゾーンとしてデフォルト ゾーンを使用できます。
ステップ 14	**exit** 例： `Device(config-sec-zone)# exit`	セキュリティ ゾーン コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードを開始します。
ステップ 15	**zone-pair security** *zone-pair-name* **source** *source-zone* **destination** *destination-zone* 例： `Device(config)# zone-pair security inside-outside source inside destination outside`	セキュリティ ゾーンのペアを作成して、セキュリティ ゾーン コンフィギュレーション モードを開始します。 • ポリシーを適用するには、ゾーン ペアを設定する必要があります。
ステップ 16	**service-policy type inspect** *policy-map-name* 例： `Device(config-sec-zone-pair)# service-policy type inspect h.323-policy`	ファイアウォール ポリシー マップを宛先ゾーン ペアに付加します。 • ゾーンのペア間でポリシーが設定されない場合、トラフィックはデフォルトでドロップされます。
ステップ 17	**exit** 例： `Device(config-sec-zone-pair)# exit`	セキュリティ ゾーンペア コンフィギュレーション モードを終了し、グローバルコンフィギュレーション モードを開始します。
ステップ 18	**interface** *type number* 例： `Device(config)# interface gigabitethernet 0/0/1`	インターフェイスを設定し、インターフェイス コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 19	**zone member security** *zone-name* 例： `Device(config-if)# zone member security inside`	インターフェイスを指定したセキュリティ ゾーンに割り当てます。 • インターフェイスをセキュリティ ゾーンのメンバーにした場合、方向に関係なくインターフェイスを通過するすべてのトラフィック（ルータ宛のトラフィックまたはルータ発信のトラフィックを除く）は、デフォルトでドロップされます。トラフィックがインターフェイス通過するには、ゾーンをポリシーの適用先のゾーン ペアの一部にする必要があります。ポリシーがトラフィックを許可すると、トラフィックはそのインターフェイスを通過できます。
ステップ 20	**end** 例： `Device(config-if)# end`	インターフェイス コンフィギュレーション モードを終了し、特権 EXEC モードを開始します。

ファイアウォールおよび NAT 対応のハイ アベイラビリティ サポートを備えた ALG—H.323 vTCP の設定例

例：ファイアウォールに対するハイ アベイラビリティ サポートを使用した ALG - H.323 vTCP の設定

```
Device# configure terminal
Device(config)# class-map type inspect h.323-class
Device(config-cmap)# match protocol h323
Device(config-cmap)# match protocol h323ras
Device(config-cmap)# exit
Device(config)# policy-map type inspect h323-policy
Device(config-pmap)# class type inspect h323
Device(config-pmap-c)# inspect
Device(config-pmap-c)# exit
Device(config-pmap)# class class-default
Device(config-pmap)# exit
Device(config)# zone security inside
Device(config-sec-zone)# exit
Device(config)# zone security outside
Device(config-sec-zone)# exit
Device(config)# zone-pair security inside-outside source inside destination outside
Device(config-sec-zone-pair)# service-policy type inspect h.323-policy
Device(config-sec-zone-pair)# exit
Device(config)# interface gigabitethernet 0/0/1
```

```
Device(config-if)# zone-member security inside
Device(config-if)# exit
Device(config)# interface gigabitethernet 0/1/1
Device(config-if)# zone-member security outside
Device(config-if)# end
```

ファイアウォールおよび NAT 対応のハイ アベイラビリティ サポートを備えた ALG-H.323 vTCP に関する追加情報

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『Master Commands List, All Releases』
ファイアウォール コマンド	• 『Security Command Reference: Commands A to C』 • 『Security Command Reference: Commands D to L』 • 『Security Command Reference: Commands M to R』 • 『Security Command Reference: Commands S to Z』
NAT コマンド	『IP Addressing Services Command Reference』

シスコのテクニカル サポート

説明	リンク
右の URL にアクセスして、シスコのテクニカル サポートを最大限に活用してください。これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

ファイアウォールと NAT に対するハイ アベイラビリティ サポートを使用した ALG - H.323 vTCP に関する機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *207 :* ファイアウォールと *NAT* に対するハイ アベイラビリティ サポートを使用した *ALG - H.323 vTCP* に関する機能情報

機能名	リリース	機能情報
ファイアウォールと NAT に対するハイ アベイラビリティ サポートを使用した ALG - H.323 vTCP	Cisco IOS XE リリース 3.7S	ファイアウォールと NAT に対するハイ アベイラビリティ サポートを使用した ALG - H.323 vTCP 機能は、単一の H.323 メッセージではない TCP セグメントをサポートするように H.323 ALG を拡張します。vTCP はセグメントの再構成をサポートします。この機能が導入される前は、H.323 メッセージが完全な場合にのみ、H.323 ALG が TCP セグメントを処理していました。TCP セグメントに複数のメッセージが含まれていた場合は、H.323 ALG が TCP セグメントを無視し、そのパケットは処理されずに転送されていました。

第 154 章

NAT とファイアウォールの SIP ALG 強化

NAT およびファイアウォール向けの SIP ALG ハードニング機能は、ネットワーク アドレス変換（NAT）とファイアウォールの既存の Session Initiation Protocol（SIP）アプリケーション レベル ゲートウェイ（ALG）サポートに対して、より優れたメモリ管理と RFC 準拠性を提供します。この機能は次の点で強化されています。

- すべての SIP レイヤ 7 データ用のローカル データベースの管理
- Via ヘッダーの処理
- 追加 SIP メソッドの記録に関するサポート
- 暫定応答確認（PRACK）コール フローのサポート
- Record-Route ヘッダーのサポート

上記の機能強化はデフォルトで使用できます。NAT やファイアウォールでの追加設定は必要ありません。

このモジュールでは、SIP ALG の機能拡張について説明し、SIP に対する NAT およびファイアウォールのサポートを有効にする方法について説明します。

NAT とファイアウォールの SIP ALG 強化に関する制約事項

- Session Initiation Protocol（SIP）アプリケーション レベル ゲートウェイ（ALG）は、セキュリティ機能を提供しません。

- SIP ALG はコール ID に基づいてローカル データベースを管理します。2 台のクライアントからコール ID が同じ 2 つのコールが送られ、コール ID が重複するという、異常ケースが発生する場合もあるかもしれません。

NAT とファイアウォールの SIP ALG 強化に関する情報

SIP の概要

Session Initiation Protocol（SIP）は、1 人または複数の参加者とのセッションを作成、変更、および終了するためのアプリケーション層コントロール（シグナリング）プロトコルです。SIP セッションには、インターネット電話の通話、マルチメディアの配布、マルチメディア会議などがあります。SIP は HTTP のような要求/応答トランザクション モデルに基づいています。各トランザクションは、サーバで特定のメソッドまたは関数を呼び出す 1 つの要求と 1 つ以上の応答で構成されます。

セッションの作成に使用される SIP の招待は、互換性のあるメディア タイプのセットに参加者が同意できるセッション記述を伝送しています。SIP は、プロキシ サーバと呼ばれる要素を利用して、ユーザの所在地への要求のルーティング、サービスのためのユーザ認証および認可、プロバイダーのコールルーティング ポリシーの実装、およびユーザへの機能提供を行っています。また、SIP には、プロキシ サーバから使用できるように、ユーザの所在地をアップロードできる登録機能があります。SIP は複数のトランスポート プロトコルを基礎として実行されます。

アプリケーション レベル ゲートウェイ

アプリケーション レベル ゲートウェイ（ALG）は、アプリケーション レイヤ ゲートウェイとも呼ばれ、アプリケーション パケットのペイロード内の IP アドレス情報を変換するアプリケーションです。ALG は、アプリケーション レイヤ プロトコルを解釈し、ファイアウォールおよびネットワーク アドレス変換（NAT）アクションを実行するために使用されます。これらのアクションは、ファイアウォールおよび NAT の設定に応じて次の 1 つまたは複数のアクションになります。

- クライアント アプリケーションが、ダイナミック TCP または UDP ポートを使用してサーバ アプリケーションと通信できるようにします。
- アプリケーション固有のコマンドを認識し、これらのコマンドに対するきめ細かいセキュリティ制御を提供します。
- データ交換を行う 2 つのホスト間の複数のデータ ストリームまたはデータ セッションを同期します。
- アプリケーション ペイロードで使用できるネットワーク層アドレス情報を変換します。

ファイアウォールがピンホールを開き、アプリケーション レイヤ データストリームの送信元 IP アドレスおよび宛先 IP アドレスを伝送しない TCP または UDP トラフィックに対する変換

サービスをNATが実行します。IPアドレス情報を埋め込む特定のプロトコルまたはアプリケーションにはALGのサポートが必要です。

SIP ALG ローカル データベース管理

Session Initiation Protocol（SIP）トランクは、サービス プロバイダーへの IP PBX の直接接続で、SIP を使用して IP ネットワークを経由します。SIP トランクでは、多数の同時コールを実現できます。コール セットアップ プロセスの間に、すべてのコールはコール確立のために同じ制御チャネルを使用します。複数のコールが、コールセットアップ用に同じ制御チャネルを使用します。同じ制御チャネルが複数のコールで使用されると、制御チャネルセッションに保存されたステートフル情報の信頼性が低くなります。SIP ステートフル情報は、メディア データを送信するクライアントおよびサーバ エンドポイントで使用される IP アドレスやポート番号などのメディア チャネル情報で構成されています。メディア チャネル情報は、ファイアウォールおよびNATに対して、それぞれのデータ チャネルのファイアウォール ピンホールとネットワーク アドレス変換（NAT）ドアを作成するために使用されます。複数のコールがコール セットアップ用に同じ制御チャネルを使用するため、メディア データの複数のセットが存在します。

SIP トランクでは、複数のコールが同じファイアウォールおよびNAT セッションを共有します。NAT およびファイアウォールは、SIP パケットの 5 つのタプル（送信元アドレス、宛先アドレス、発信元ポート、宛先ポート、およびプロトコル）を使用して、SIP セッションを識別および管理します。5 つのタプルを使用してコールを識別および照合する従来の方法は、SIP トランキングを完全にはサポートしないため、レイヤ7データのメモリ リークやコール照合の問題が発生することがよくあります。

他のアプリケーション レベル ゲートウェイ（ALG）とは対照的に、SIP ALG はローカル データベースを使用して、通常の SIP コールおよび SIP トランクに埋め込まれた SIP コールに含まれるすべてのメディア関連の情報を保存することで、SIP レイヤ 7 データを管理します。SIP ALG は、SIP メッセージに含まれるコール ID ヘッダー フィールドを使用してローカル データベース内で一致するコールを検索し、コールを管理および終了します。コール ID ヘッダー フィールドは、同じ SIP ダイアログに属するメッセージを識別するダイアログ識別子です。

SIP ALG は、コール ID を使用してローカル データベース内を検索し、メモリ リソースを管理します。SIP ALG がデータベースからレイヤ7データ レコードを解放できない特定の状況で、リソースの管理と解放にセッション タイマーが使用され、データベース内に停止したコール レコードが存在しないようにします。

（注） すべてのレイヤ7データはローカルデータベースを使用したSIP ALGにより管理されるので、SIP ALG は SIP レイヤ 7 データを解放するためにファイアウォールおよびNAT に応答しません。SIP ALG はデータを自ら解放します。**clear** コマンドを使用して、すべての NAT 変換およびファイアウォールセッションをクリアした場合、ローカルデータベース内の SIP レイヤ 7 データは解放されません。

SIP ALG Via ヘッダーのサポート

Session Initiation Protocol (SIP) INVITE 要求には、Via ヘッダー フィールドが含まれます。Via ヘッダー フィールドは、SIP 要求によって採用される転送パスを示します。Via ヘッダーには、後続の SIP 応答のリターン パスに関する情報も含まれます。その中には応答メッセージが送信される IP アドレスとポートが含まれます。

SIP ALG は、確認応答（ACK）メッセージを除き、受信した SIP 要求の Via ヘッダー フィールド内の最初の値に基づいて、ファイアウォール ピンホールまたはネットワーク アドレス変換（NAT）ドアを作成します。最初の Via ヘッダーにポート番号情報がない場合、ポート番号は 5060 であるとみなされます。

SIP ALG メソッド ロギングのサポート

NAT およびファイアウォール向けの SIP ALG ハードニング機能は、Session Initiation Protocol（SIP）アプリケーション レベル ゲートウェイ（ALG）の統計情報で次のメソッドの詳細なロギングをサポートします。

- PUBLISH
- OPTIONS
- 1XX（100、180、183 を除く）
- 2XX（200 を除く）

SIP ALG 統計情報に記録される既存の SIP メソッドには ACK、BYE、CANCEL、INFO、INVITE、MESSAGE、NOTIFY、REFER、REGISTER、SUBSCRIBE、および 1XX-6XX があります。

SIP ALG PRACK コール フローのサポート

Session Initiation Protocol（SIP）は、最終と暫定という 2 つのタイプの応答を定義します。最終応答は、要求処理の結果を知らせるもので、確実に送信されます。一方で暫定応答は、要求処理の進行状況に関する情報を提供しますが、確実には送信されません。

暫定応答確認（PRACK）は、暫定応答の確認応答（ACK）システムを提供する SIP メソッドです。PRACK を使用すると、SIP エンドポイント間の SIP の暫定応答を確実に交換できます。SIP の信頼性の高い暫定応答は、メディア情報が交換され、リソース予約がコールの接続前に実行できるようにします。

SIP は、接続ネゴシエーション中、Session Description Protocol（SDP）の接続、メディア、および属性のフィールドを使用します。SIP アプリケーション レベル ゲートウェイ（ALG）は、PRACK メッセージ内の SDP 情報をサポートします。メディア情報が PRACK メッセージ内に存在する場合、SIP ALG はメディア情報を取得して処理します。SIP ALG はまた、後続のメディア ストリームのメディア チャネルの作成を処理します。SIP ALG は PRACK メッセージ内の SDP 情報に基づいてファイアウォール ピンホールおよび NAT ドアを作成します。

SIP ALG Record-Route ヘッダーのサポート

Record-Route ヘッダー フィールドは、Session Initiation Protocol（SIP）プロキシによって SIP 要求に追加され、SIP ダイアログ内の将来の要求がプロキシを介してルーティングされることを強制します。その後、ダイアログ内で送信されるメッセージはすべての SIP プロキシを通過し、Record-Route ヘッダー フィールドが SIP 要求に追加されます。Record-Route ヘッダー フィールドには、プロキシを識別する、グローバルに到達可能な Uniform Resource Identifier（URI）が含まれます。

SIP アプリケーション レベル ゲートウェイ（ALG）は、Contact ヘッダーを解析し、Contact ヘッダー内の IP アドレスとポート番号を使用して、ファイアウォール ピンホールとネットワーク アドレス変換（NAT）ドアを作成します。さらに、SIP ALG は、プロキシを経由してルーティングされる将来のメッセージ用のファイアウォール ピンホールと NAT ドアを作成するために、Record-Route ヘッダーの解析をサポートします。

NAT とファイアウォールに対する SIP ALG 強化の設定方法

SIP の NAT サポートの有効化

SIP の NAT サポートは、デフォルトでポート 5060 でイネーブルになっています。この機能が無効になっている場合、SIP の NAT サポートを再びイネーブルにするには、次の作業を実行します。SIP の NAT サポートを無効にするには、**no ip nat service sip** コマンドを使用します。

手順の概要

1. **enable**
2. **configure terminal**
3. **ip nat service sip** {**tcp** | **udp**} **port** *port-number*
4. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 3	**ip nat service sip** {**tcp** | **udp**} **port** *port-number* 例： `Device(config)# ip nat service sip tcp port 5060`	SIP の NAT サポートを有効にします。
ステップ 4	**end** 例： `Device(config)# end`	グローバル コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

SIP インスペクションの有効化

手順の概要

1. **enable**
2. **configure terminal**
3. **class-map type inspect match-any** *class-map-name*
4. **match protocol** *protocol-name*
5. **exit**
6. **policy-map type inspect** *policy-map-name*
7. **class type inspect** *class-map-name*
8. **inspect**
9. **exit**
10. **class class-default**
11. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**class-map type inspect match-any** *class-map-name* 例： `Device(config)# class-map type inspect match-any sip-class1`	検査タイプ クラス マップを作成し、クラス マップ コンフィギュレーション モードを開始します。
ステップ 4	**match protocol** *protocol-name* 例：	名前付きプロトコルに基づいてクラス マップの一致基準を設定します。

	コマンドまたはアクション	目的
	`Device(config-cmap)# match protocol sip`	
ステップ 5	**exit** 例： `Device(config-cmap)# exit`	クラスマップ コンフィギュレーション モードを終了します。
ステップ 6	**policy-map type inspect** *policy-map-name* 例： `Device(config)# policy-map type inspect sip-policy`	検査タイプ ポリシー マップを作成し、ポリシー マップ コンフィギュレーション モードを開始します。
ステップ 7	**class type inspect** *class-map-name* 例： `Device(config-pmap)# class type inspect sip-class1`	アクションを実行するクラスを指定し、ポリシー マップ クラス コンフィギュレーション モードを開始します。
ステップ 8	**inspect** 例： `Device(config-pmap-c)# inspect`	ステートフル パケット インスペクションをイネーブルにします。
ステップ 9	**exit** 例： `Device(config-pmap-c)# exit`	ポリシー マップ クラス コンフィギュレーション モードを終了し、ポリシーマップ コンフィギュレーション モードに戻ります。
ステップ 10	**class class-default** 例： `Device(config-pmap)# class class-default`	これらのポリシー マップ設定が事前に定義したデフォルト クラスに適用されることを指定します。 • 設定済みクラス マップの一致基準のいずれともトラフィックが一致しない場合、事前に定義されたデフォルト クラスに誘導されます。
ステップ 11	**end** 例： `Device(config-pmap)# end`	ポリシー マップ コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

ゾーン ペアの設定と SIP ポリシー マップのアタッチ

手順の概要

1. **enable**
2. **configure terminal**
3. **zone security** {*zone-name* | **default**}
4. **exit**
5. **zone security** {*zone-name* | **default**}

6. **exit**
7. **zone-pair security** *zone-pair-name* [**source** {*source-zone-name* | **self** | **default**} **destination** [*destination-zone-name* | **self** | **default**]]
8. **service-policy type inspect** *policy-map-name*
9. **exit**
10. **interface** *type number*
11. **zone-member security** *zone-name*
12. **exit**
13. **interface** *type number*
14. **zone-member security** *zone-name*
15. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**zone security** {*zone-name* | **default**} 例： `Device(config)# zone security zone1`	インターフェイスを割り当てることができるセキュリティ ゾーンを作成し、セキュリティ ゾーン コンフィギュレーション モードを開始します。
ステップ 4	**exit** 例： `Device(config-sec-zone)# exit`	セキュリティ ゾーン コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードに戻ります。
ステップ 5	**zone security** {*zone-name* | **default**} 例： `Device(config)# zone security zone2`	インターフェイスを割り当てることができるセキュリティ ゾーンを作成し、セキュリティ ゾーン コンフィギュレーション モードを開始します。
ステップ 6	**exit** 例： `Device(config-sec-zone)# exit`	セキュリティ ゾーン コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードに戻ります。
ステップ 7	**zone-pair security** *zone-pair-name* [**source** {*source-zone-name* | **self** | **default**} **destination** [*destination-zone-name* | **self** | **default**]] 例： `Device(config)# zone-pair security in-out source zone1 destination zone2`	ゾーン ペアを作成し、セキュリティ ゾーン ペア コンフィギュレーション モードに戻ります。 （注） ポリシーを適用するには、ゾーン ペアを設定する必要があります。

	コマンドまたはアクション	目的
ステップ 8	**service-policy type inspect** *policy-map-name* 例： `Device(config-sec-zone-pair)# service-policy type inspect sip-policy`	ファイアウォール ポリシー マップを宛先ゾーン ペアに付加します。 （注） ゾーンのペア間でポリシーが設定されない場合、トラフィックはデフォルトでドロップされます。
ステップ 9	**exit** 例： `Device(config-sec-zone-pair)# exit`	セキュリティ ゾーン ペア コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードに戻ります。
ステップ 10	**interface** *type number* 例： `Device(config)# interface gigabitethernet 0/0/0`	インターフェイスを設定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 11	**zone-member security** *zone-name* 例： `Device(config-if)# zone-member security zone1`	インターフェイスを指定したセキュリティ ゾーンに割り当てます。 （注） インターフェイスをセキュリティ ゾーンのメンバーにした場合、そのインターフェイスを通して送受信されるすべてのトラフィックは、デフォルトでドロップされます（ただしデバイス宛のトラフィックとデバイス発のトラフィックを除く）。トラフィックがインターフェイス通過するには、ゾーンをポリシーの適用先のゾーン ペアの一部にする必要があります。ポリシーがトラフィックを許可すると、トラフィックはそのインターフェイスを通過できます。
ステップ 12	**exit** 例： `Device(config-if)# exit`	インターフェイス設定モードを終了し、グローバル設定モードに戻ります。
ステップ 13	**interface** *type number* 例： `Device(config)# interface gigabitethernet 0/1/1`	インターフェイスを設定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 14	**zone-member security** *zone-name* 例： `Device(config-if)# zone-member security zone2`	インターフェイスを指定したセキュリティ ゾーンに割り当てます。

	コマンドまたはアクション	目的
ステップ 15	**end** 例： `Device(config-if)# end`	インターフェイス コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

NAT とファイアウォールに対する SIP ALG 強化の設定例

例：SIP サポート用の NAT の有効化

```
Device> enable
Device# configure terminal
Device(config)# ip nat service sip tcp port 5060
Device(config)# end
```

例：SIP インスペクションの有効化

```
class-map type inspect match-any sip-class1
 match protocol sip
!
policy-map type inspect sip-policy
 class type inspect sip-class1
  inspect
!
class class-default
```

例：ゾーン ペアの設定と SIP ポリシー マップのアタッチ

```
zone security zone1
!
zone security zone2
!
zone-pair security in-out source zone1 destination zone2
 service-policy type inspect sip-policy
!
interface gigabitethernet 0/0/0
 zone security zone1
!
interface gigabitethernet 0/1/1
 zone security zone2
```

NAT とファイアウォールの SIP ALG 強化に関する追加情報

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『Cisco IOS Master Command List, All Releases』
NAT 設定	『*IP Addressing: NAT Configuration Guide*』
ファイアウォールの設定	『セキュリティ設定ガイド：ゾーンベース ポリシー ファイアウォール』
NAT コマンド	『Cisco IOS IP Addressing Services Command Reference』
ファイアウォール コマンド	• 『Cisco IOS Security Command Reference: Commands A to C』 • 『Cisco IOS Security Command Reference: Commands D to L』 • 『Cisco IOS Security Command Reference: Commands M to R』 • 『Cisco IOS Security Command Reference: Commands S to Z』

標準および RFC

標準/RFC	タイトル
RFC 3261	『*SIP: Session Initiation Protocol*』

シスコのテクニカル サポート

説明	リンク
右の URL にアクセスして、シスコのテクニカル サポートを最大限に活用してください。これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

NAT とファイアウォールの SIP ALG 強化に関する機能情報

表 *208 : NAT* とファイアウォールの *SIP ALG* 強化に関する機能情報

機能名	リリース	機能情報
NAT とファイアウォールの SIP ALG 強化	Cisco IOS XE リリース 3.8S	NAT とファイアウォールの SIP ALG 強化機能は、既存の NAT とファイアウォールの SIP ALG サポートでより適切なメモリ管理と RFC 準拠を可能にします。

第 155 章

DoS 攻撃に対する SIP ALG レジリエンス

DoS 攻撃に対する SIP ALG レジリエンス機能は、Session Initiation Protocol（SIP）アプリケーション レイヤ ゲートウェイ（ALG）へのサービス妨害（DoS）攻撃に対する保護を提供します。この機能は、DoS 攻撃を防ぐために、設定可能なロック制限、動的ブラックリスト、および設定可能なタイマーをサポートします。

このモジュールでは、機能と SIP アプリケーション レイヤ ゲートウェイ（ALG）に対する DoS 保護の設定方法を説明します。ネットワーク アドレス変換およびゾーンベース ポリシー ファイアウォールは、この機能をサポートしています。

DoS 攻撃に対する SIP ALG レジリエンスに関する情報

DoS 攻撃に対する SIP ALG レジリエンスの概要

DoS 攻撃に対する SIP ALG レジリエンス機能は、Session Initiation Protocol（SIP）アプリケーション レイヤ ゲートウェイ（ALG）へのサービス妨害（DoS）攻撃に対する保護を提供します。この機能は、DoS 攻撃を防ぐために、設定可能なロック制限、動的ブラックリスト、および設定可能なタイマーをサポートします。この機能はネットワーク アドレス変換（NAT）およびゾーンベース ポリシー ファイアウォールによってサポートされています。

SIP は、IP データ ネットワーク上の参加者の間でリアルタイム セッションをセットアップ、変更、および終了するための、アプリケーション レベル シグナリング プロトコルです。SIP セッションには、インターネット電話の通話、マルチメディアの配布、マルチメディア会議などがあります。SIP DoS 攻撃は、ネットワークに対する大きな脅威です。

SIP DoS 攻撃のタイプを次に示します。

- SIP 登録フラッディング：登録フラッドは、多数の VoIP デバイスが同時にネットワークに登録を試みると発生します。登録メッセージの量がデバイスの容量を超過すると、一部

のメッセージは失われます。こうしたデバイスは再び登録を試行するため、輻輳が増加します。このようなネットワークの輻輳により、ユーザは一定の期間ネットワークにアクセスできない可能性があります。

- SIP INVITE フラッディング：INVITE フラッディングは、多数の INVITE メッセージがサーバに送信され、それらのメッセージのすべてをサーバが対応できなくなると発生します。攻撃レートが非常に高くなると、サーバのメモリが枯渇します。
- SIP 破損認証およびセッション攻撃：この攻撃は、攻撃者がダイジェスト認証を使用して有効なユーザの ID を推定するときに発生します。認証サーバが攻撃者の身元を確認しようとすると、検証は無視され、攻撃者は別のセッション ID を使用して新しい要求を開始します。これらの攻撃は、サーバのメモリを消費します。

SIP ALG 動的ブラックリスト

サービス妨害（DoS）攻撃の一般的な方法の 1 つは、ターゲット ネットワークを外部通信要求で飽和させ、ネットワークが正当なトラフィックに応答できなくすることです。この問題を解決するために、SIP ALG の DoS 攻撃レジリエンス機能は、設定可能なブロックリストを使用します。ブロックリストは、特定の権限、サービス、またはアクセスが拒否されているエンティティのリストです。動的ブラックリストはデフォルトで無効になっています。宛先アドレスに対する要求が、設定されたブロックリストの定義済みトリガーの基準を超えると、Session Initiation Protocol（SIP）アプリケーション レイヤ ゲートウェイ（ALG）は、これらのパケットをドロップします。

次の異常な SIP セッションパターンは、動的ブロックリストによって監視されます。

- 設定された期間内に、送信元が宛先に複数の要求を送信し、宛先から 2xx 以外（RFC 3261 に従って、200 から 299 までのステータス コードを持つすべての応答は「2xx 応答」です）の最終応答を受信する場合。
- 設定された期間に、送信元が宛先に複数の要求を送信し、宛先からまったく応答を受信しない場合。

SIP ALG ロック制限

ネットワーク アドレス変換（NAT）とファイアウォールは、どちらも Session Initiation Protocol（SIP）アプリケーション レイヤ ゲートウェイ（ALG）を使用して SIP メッセージを解析し、トークンからセッションを作成します。セッション状態を維持するために、SIP ALG はコール単位のデータ構造とレイヤ 7 データを使用して、セッションの開始時に割り当てられセッションの解除時に解放されるコール関連情報を保存します。SIP ALG がコールの終了を示すメッセージを受信しない場合、ネットワーク リソースはコール用に保持されます。

レイヤ 7 データはスレッド間で共有されるため、データにアクセスするためにロックが必要です。サービス妨害（DoS）攻撃や分散型 DoS 攻撃の発生時は、同じロックを取得するために多くのスレッドが待機するため、CPU 使用率が高くなり、システムが不安定になります。システムが不安定になることを防ぐために、ロックを待機できるスレッドの数を抑制するように制限が追加されています。SIP セッションは、要求/応答モードで確立されます。1 つの SIP コールに対して同時 SIP メッセージの数が多すぎる場合、ロック制限を超えたパケットはドロップされます。

SIP ALG タイマー

あるタイプの DoS 攻撃は、Session Initiation Protocol（SIP）サーバのリソースを枯渇させるために、SIP コールの終わりを示しません。こうしたタイプの DoS 攻撃を防ぐために、保護タイマーが追加されました。

SIP ALG の DoS 攻撃に対するレジリエンス機能は、次のタイマーを使用します。

- 応答される SIP コールの最大長を制御する、コール継続時間タイマー。
- 応答されない SIP コールの最大長を制御する、コール進行時間タイマー。

設定された最大時間を超えると、SIP アプリケーション レイヤ ゲートウェイ（ALG）は、このコールのリソースを解放し、このコールに関連する将来のメッセージは、SIP ALG によって適切に解析されないことがあります。

DoS 攻撃に対する SIP ALG レジリエンスの設定方法

DoS 攻撃に対する SIP ALG レジリエンスの設定

ネットワーク アドレス変換（NAT）およびゾーン ベース ポリシー ファイアウォールによって使用される Session Initiation Protocol（SIP）アプリケーション レイヤ ゲートウェイ（ALG）用のサービス妨害（DoS）防止パラメータを設定できます。

手順の概要

1. **enable**
2. **configure terminal**
3. **alg sip processor session max-backlog** *concurrent-processor-usage*
4. **alg sip processor global max-backlog** *concurrent-processor-usage*
5. **alg sip blacklist trigger-period** *trigger-period* **trigger-size** *minimum-events* **destination** *ip-address*
6. **alg sip blacklist trigger-period** *trigger-period* **trigger-size** *minimum-events* **block-time** *block-time* [**destination** *ip-address*]
7. **alg sip timer call-proceeding-timeout** 時刻
8. **alg sip timer max-call-duration** 秒
9. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。

	コマンドまたはアクション	目的
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**alg sip processor session max-backlog** *concurrent-processor-usage* 例： `Device(config)# alg sip processor session max-backlog 5`	共有リソースを待機するバックログ メッセージ数に対するセッションごとの制限を設定します。
ステップ 4	**alg sip processor global max-backlog** *concurrent-processor-usage* 例： `Device(config)# alg sip processor global max-backlog 5`	すべての SIP セッションで共有リソースを待機するバックログ メッセージの最大数を設定します。
ステップ 5	**alg sip blacklist trigger-period** *trigger-period* **trigger-size** *minimum-events* **destination** *ip-address* 例： `Device(config)# alg sip blacklist trigger-period 90 trigger-size 30 destination 10.1.1.1`	指定した宛先 IP アドレスに関するダイナミック SIP ALG ブラックリスト基準を設定します。
ステップ 6	**alg sip blacklist trigger-period** *trigger-period* **trigger-size** *minimum-events* **block-time** *block-time* [**destination** *ip-address*] 例： `Device(config)# alg sip blacklist trigger-period 90 trigger-size 30 block-time 30`	設定済みの制限を超えた場合に送信元からのパケットがブロックされる期間（秒単位）を設定します。
ステップ 7	**alg sip timer call-proceeding-timeout** 時刻 例： `Device(config)# alg sip timer call-proceeding-timeout 35`	応答を受信しない SIP コールを終了するための最大時間（秒単位）で設定します。
ステップ 8	**alg sip timer max-call-duration** 秒 例： `Device(config)# alg sip timer max-call-duration 90`	正常な SIP コールの最大コール期間（秒単位）を設定します。
ステップ 9	**end** 例： `Device(config)# end`	グローバル コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

DoS 攻撃に対する SIP ALG レジリエンスの確認

機能のトラブルシューティングには、次のコマンドを使用します。

手順の概要

1. **enable**
2. **show alg sip**
3. **show platform hardware qfp** {**active** | **standby**} **feature alg statistics sip**
4. **show platform hardware qfp** {**active** | **standby**} **feature alg statistics sip dbl**
5. **show platform hardware qfp** {**active** | **standby**} **feature alg statistics sip dblcfg**
6. **show platform hardware qfp** {**active** | **standby**} **feature alg statistics sip processor**
7. **show platform hardware qfp** {**active** | **standby**} **feature alg statistics sip timer**
8. **debug alg** {**all** | **info** | **trace** | **warn**}

手順の詳細

ステップ 1 enable

例：

```
Device> enable
```

特権 EXEC モードを有効にします。

- パスワードを入力します（要求された場合）。

ステップ 2 show alg sip

Session Initiation Protocol（SIP）アプリケーション レイヤ ゲートウェイ（ALG）の情報を表示します。

例：

```
Device# show alg sip

sip timer configuration
   Type                      Seconds
   max-call-duration         380
   call-proceeding-timeout   620

sip processor configuration
   Type           Backlog number
   session         14
   global          189

sip blacklist configuration
   dst-addr         trig-period(ms)    trig-size     block-time(sec)
   10.0.0.0             60                 30              2000
   10.1.1.1             20                 30              30
   192.0.2.115          1000               5               30
   198.51.100.34        20                 30              388
```

ステップ 3 show platform hardware qfp {active | standby} feature alg statistics sip

Cisco Quantum Flow Processor（QFP）の SIP ALG 固有の統計情報を表示します。

例：

```
Device# show platform hardware qfp active feature alg statistics sip

Events
...
Cr dbl entry:                10   Del dbl entry:                 10
Cr dbl cfg entry:             8   Del dbl cfg entry:              4
start dbl trig tmr:          10   restart dbl trig tmr:        1014
stop dbl trig tmr:           10   dbl trig timeout:            1014
start dbl blk tmr:            0   restart dbl blk tmr:            0
stop dbl blk tmr:             0   dbl blk tmr timeout:            0
start dbl idle tmr:          10   restart dbl idle tmr:         361
stop dbl idle tmr:            1   dbl idle tmr timeout:           9

DoS Errors
Dbl Retmem Failed:            0    Dbl Malloc Failed:             0
DblCfg Retm Failed:           0    DblCfg Malloc Failed:          0
Session wlock ovflw:          0    Global wlock ovflw:            0
Blacklisted:                561
```

ステップ 4 **show platform hardware qfp {active | standby} feature alg statistics sip dbl**

すべての SIP ブロックリストデータに関する概要情報を表示します。

例：

```
Device# show platform hardware qfp active feature alg statistics sip dbl

SIP dbl pool used chunk entries number: 1

 entry_id          src_addr         dst_addr         remaining_time(sec)
 a4a051e0a4a1ebd   10.74.30.189     10.74.5.30                25
```

ステップ 5 **show platform hardware qfp {active | standby} feature alg statistics sip dblcfg**

すべての SIP ブロックリストの設定が表示されます。

例：

```
Device# show platform hardware qfp active feature alg statistics sip dblcfg

SIP dbl cfg pool used chunk entries number: 4
 dst_addr        trig_period(ms)    trig_size    block_time(sec)
 10.1.1.1              20              30             30
 10.74.5.30            1000             5             30
 192.0.2.2             60              30           2000
 198.51.100.115        20              30            388
```

ステップ 6 **show platform hardware qfp {active | standby} feature alg statistics sip processor**

SIP プロセッサの設定を表示します。

例：

```
Device# show platform hardware qfp active feature alg statistics sip processor

Session:     14        Global:    189

Current global wlock count:      0
```

ステップ 7 **show platform hardware qfp** {**active** | **standby**} **feature alg statistics sip timer**

SIP タイマーの設定を表示します。

例：

```
Device# show platform hardware qfp active feature alg statistics sip timer

call-proceeding:    620      call-duration:    380
```

ステップ 8 **debug alg** {**all** | **info** | **trace** | **warn**}

例：

```
Device# debug alg warn
```

ALG 警告メッセージのロギングをイネーブルにします。

DoS 攻撃に対する SIP ALG レジリエンスの設定例

例：DoS 攻撃に対する SIP ALG レジリエンスの設定

```
Device# configure terminal
Device(config)# alg sip processor session max-backlog 5
Device(config)# alg sip processor global max-backlog 5
Device(config)# alg sip blacklist trigger-period 90 trigger-size 30 destination 10.1.1.1
Device(config)# alg sip blacklist trigger-period 90 trigger-size 30 block-time 30
Device(config)# alg sip timer call-proceeding-timeout 35
Device(config)# alg sip timer max-call-duration 90
Device(config)# end
```

DoS 攻撃に対する SIP ALG レジリエンスに関する追加情報

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『Cisco IOS Master Command List, All Releases』

関連項目	マニュアル タイトル
ファイアウォール コマンド	• 『Cisco IOS Security Command Reference: Commands A to C』 • 『Cisco IOS Security Command Reference: Commands D to L』 • 『Cisco IOS Security Command Reference: Commands M to R』 • 『Cisco IOS Security Command Reference: Commands S to Z』
NAT コマンド	『IP Addressing Services Command References』

標準および RFC

標準/RFC	タイトル
RFC 4028	『*Session Timers in the Session Initiation Protocol (SIP)*』

MIB

MB	MIB のリンク
	選択したプラットフォーム、Cisco IOS リリース、およびフィーチャ セットに関する MIB を探してダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

シスコのテクニカル サポート

説明	リンク
シスコのサポート Web サイトでは、シスコの製品やテクノロジーに関するトラブルシューティングにお役立ていただけるように、マニュアルやツールをはじめとする豊富なオンライン リソースを提供しています。 お使いの製品のセキュリティ情報や技術情報を入手するために、Cisco Notification Service（Field Notice からアクセス）、Cisco Technical Services Newsletter、Really Simple Syndication（RSS）フィードなどの各種サービスに加入できます。 シスコのサポート Web サイトのツールにアクセスする際は、Cisco.com のユーザ ID およびパスワードが必要です。	http://www.cisco.com/support

第 XIII 部

「Security for VPNs with IPsec」

第 156 章

IPsec を使用した VPN のセキュリティの設定

この部分では、基本的な IP VPN を設定する方法について説明します。IPsec は、IETF によって開発されたオープン規格のフレームワークです。インターネットなどの保護されていないネットワークを介して機密情報を伝達する場合にセキュリティを提供します。IPsec はネットワーク層で機能し、Cisco ルータなどの参加している IPsec 装置（「ピア」）間の IP パケットを保護および認証します。

（注） セキュリティに対する脅威は、脅威からの保護に役立つ暗号化技術と同様に絶え間なく変化しています。シスコの暗号化に関する最新の推奨事項の詳細は、『Next Generation Encryption』（NGE）ホワイトペーパーを参照してください。

IPsec を使用した VPN のセキュリティの設定に関する前提条件

IKE の設定

インターネット キー エクスチェンジ（IKE）は、「*Configuring Internet Key Exchange for IPsec VPNs*」の手順に従って設定する必要があります。

（注） IKE を使用しない場合でも、「*Configuring Internet Key Exchange for IPsec VPNs*」の手順に従って、IKE をディセーブルにする必要があります。

アクセス リストが IPsec と互換性があるか確認する

IKE は UDP ポート 500 を使用します。IPsec Encapsulating Security Payload（ESP）プロトコルと認証ヘッダー（AH）プロトコルは、それぞれ、プロトコル番号 50 と 51 を使用します。プロトコル 50、51、および UDP ポート 500 からのトラフィックが IPsec によって使用されるインターフェイスでブロックされないように、アクセス リストが設定されていることを確認します。場合によっては、これらのトラフィックを明示的に許可する文をアクセス リストに追加する必要があります。

IPsec を使用した VPN のセキュリティの設定に関する制約事項

Cisco IPsec ポリシー マップ MIB

MIB OID オブジェクトは、IPsec セッションが起動中にしか表示されません。

不連続アクセス制御リスト

不連続マスクを持つアクセス制御リスト（ACL）を使用する暗号マップはサポートされません。

物理インターフェイスと暗号マップ

物理インターフェイスがトンネル保護インターフェイスの送信元インターフェイスである場合、物理インターフェイスの暗号マップはサポートされません。

NAT の設定

ネットワークアドレス変換（NAT）を使用する場合は、IPsec が適切に動作するように、スタティック NAT を設定する必要があります。一般に、ルータが IPsec カプセル化を実行する前に、NAT が発生する必要があります。つまり、IPsec はグローバル アドレスと連動している必要があります。

ユニキャスト IP データグラム アプリケーションのみ

IPsec は、ユニキャスト IP データグラムにのみ適用できます。IPsec のワーキング グループがまだグループ キー配布の問題に対処していないため、IPsec は現在マルチキャストまたはブロードキャスト IP データグラムを処理しません。

サポートされないインターフェイス タイプ

- 暗号 VPN は、ブリッジ ドメイン インターフェイス（BDI）上でサポートされません。
- 暗号マップは、トンネルインターフェイスとポートチャネルインターフェイス上でサポートされません。例外として、GDOIの暗号マップは、トンネルインターフェイス上でサポートされます。
- 暗号マップは、ループバック インターフェイス上ではサポートされません。
- トンネルでトランスポートプロファイルが有効になっている場合、トンネル送信元インターフェイス上では暗号マップはサポートされません。
- 暗号マップは、MFR のトンネルインターフェイス上ではサポートされません。
- 暗号マップは、VLAN インターフェイス上ではサポートされません。
- GetVPN 暗号マップは、ポートチャネル インターフェイス上でサポートされます。

IPsec を使用した VPN のセキュリティの設定に関する情報

Supported Standards

シスコでは、この機能を使用して次の規格を実装しています。

- IPsec：IPsec は、参加しているピア間のデータ機密性、データ整合性、およびデータ認証を提供するオープン スタンダードのフレームワークです。IPsecは、これらのセキュリティ サービスを IP レイヤで提供します。IPsec は、IKE を使用して、ローカル ポリシーに基づいてプロトコルおよびアルゴリズムのネゴシエーションを処理し、IPsec で使用される暗号キーと認証キーを生成します。IPsec は、1 組のホスト間、1 組のセキュリティ ゲートウェイ間、またはセキュリティ ゲートウェイとホスト間で 1 つ以上のデータ フローを保護するために使用できます。

（注） IPsec という用語は、IPsec データ サービスのプロトコル全体およびIKEセキュリティ プロトコルを表す場合に使用されることがあります。また、データ サービスだけを表す場合にも使用されることがあります。

- IKE（IKEv1 と IKEv2）：Oakley キー交換や SKEME キー交換を Internet Security Association and Key Management Protocol（ISAKMP）フレームワーク内部に実装したハイブリッド プロトコルです。IKE は他のプロトコルで使用されますが、その初期実装は IPsec プロトコルで使用されます。IKE は、IPSec ピアを認証し、IPSec セキュリティ アソシエーションをネゴシエーションし、IPSec キーを確立します。

（注） Cisco IOS XE Bengaluru 17.6.x 以降、脆弱な暗号化アルゴリズムを設定すると警告が生成されますが、警告は無視しても問題はなく、アルゴリズムの動作には影響しません。次の例では、脆弱な暗号アルゴリズムに関する警告メッセージを表示します。

```
Device(config-ikev2-proposal)# group 5
%Warning: weaker dh-group is deprecated
```

次の表に、すべての脆弱なアルゴリズムを示します。

IKEv1	IKEv2	IPSec
DH_GROUP_768_MODP/Group 1	DH_GROUP_768_MODP/Group 1	ah-md5-hmac
DH_GROUP_1024_MODP/Group 2	DH_GROUP_1024_MODP/Group 2	ah-sha-hmac
DH_GROUP_1536_MODP/Group 5	DH_GROUP_1536_MODP/Group 5	esp-des
DES	DES	esp-3des
3DES	3DES	esp-sha-hmac
MD5	MD5	esp-gmac
DH_GROUP_2048_256_MODP/Group 24	DH_GROUP_2048_256_MODP/Group 24	esp-md5-hmac
		esp-null

IPsec のために実装されているコンポーネント テクノロジーには、次のものがあります。

（注） Cisco IOS XE 17.11.1a 以降、セキュリティ強化と弱い暗号の廃止の一環として、DES、3DES、MD5、および Diffie-Hellman（DH）グループ 1、2、5 を設定するオプションは廃止され、サポートされなくなりました。代わりに、AES、SHA、および DH グループ 14 以上を使用してください。さらに、esp-gmac トランスフォームも廃止されました。

弱い暗号を引き続き使用する場合は、**crypto engine compliance shield disable** コマンドを使用してデバイスで CSDL コンプライアンスを無効にし、再起動してください。

- AES：Advanced Encryption Standard（AES）。暗号アルゴリズムの 1 つで、重要ではあるが機密扱いではない情報を保護します。AES は、IPsec および IKE 用のプライバシー変換であり、DES に代わる規格として開発されました。AES は DES よりも安全度の高い設計となっています。AES ではキーのサイズが従来より大きく、侵入者がメッセージを解読するには、あらゆるキーを試してみるしか方法がありません。AES のキーは可変長であり、アルゴリズムは 128 ビット キー（デフォルト）、192 ビット キー、または 256 ビット キーを指定できます。
- DES：データ暗号規格（DES）。パケット データの暗号化に使用されるアルゴリズムです。シスコ ソフトウェアは、必須の 56 ビット DES-CBC with Explicit IV を実装していま

す。Cipher Block Chaining（CBC）では、暗号化の開始に初期ベクター（IV）が必要です。IV は IPSec パケットに明示的に指定されます。下位互換性を確保するために、Cisco IOS IPsec は ESP DES-CBC の RFC 1829 バージョンも実装します。

また、Cisco IOS は、特定のプラットフォームで使用可能なソフトウェア バージョンに応じて、Triple DES（168 ビット）暗号化も実装します。Triple DES（3DES）は推奨されていません。

（注） 強力な暗号化を使用する Cisco IOS イメージ（56 ビット データ暗号化フィーチャ セットを含むがこれに限定されない）は、米国輸出規制の対象となり、配布が制限されます。米国以外の国でインストールされるイメージには、輸出許可が必要です。米国政府の規制により、お客様の注文が拒否されたり、納入が遅れたりすることがあります。詳細については、営業担当者または販売業者、あるいは export@cisco.com までお問い合わせください。

- SHA-2 および SHA-1 ファミリ（HMAC バリアント）：セキュア ハッシュ アルゴリズム（SHA）の 1 および 2。SHA-1 および SHA-2 は、パケット データの認証および IKE プロトコルの整合性確認メカニズムの検証に使用されるハッシュ アルゴリズムです。HMAC は、追加レベルのハッシュを提供するバリアントです。SHA-2 ファミリには、SHA-256 ビットのハッシュ アルゴリズムと SHA-384 ビットのハッシュ アルゴリズムが加わっています。この機能は Suite-B の要件に含まれています。Suite-B は、IKE および IPSec で使用するための暗号化アルゴリズムの 4 つのユーザ インターフェイス スイートで構成され、RFC 4869 に記述されています。各スイートは、暗号化アルゴリズム、デジタル署名アルゴリズム、キー合意アルゴリズム、ハッシュまたはメッセージ ダイジェスト アルゴリズムで構成されています。Cisco IOS での Suite-B サポートに関する詳細については、「Configuring Security for VPNs with IPsec」機能モジュールを参照してください。
- Diffie-Hellman：公開キー暗号法プロトコルの 1 つで、2 者間に、セキュアでない通信チャネルによる共有秘密を確立できます。Diffie-Hellman は、IKE 内でセッション キーを確立するために使用されます。これは、768 ビット（デフォルト）、1024 ビット、1536 ビット、2048 ビット、3072 ビット、および 4096 ビット DH グループをサポートします。また、256 ビット サブグループを含む 2048 ビット DH グループと、256 ビットと 384 ビットの Elliptic Curve DH（ECDH）もサポートします。2048 ビット以上の DH キー交換または ECDH キー交換の使用をお勧めします。
- MD5（ハッシュ ベースのメッセージ認証コード（HMAC）バリアント）：メッセージ ダイジェスト アルゴリズム 5（MD5）はハッシュ アルゴリズムです。HMAC はデータの認証に使用されるキー付きハッシュ バリアントです。

シスコ ソフトウェアに実装された IPsec は、さらに次の規格をサポートします。

- AH：認証ヘッダー。データ認証と、オプションとしてアンチ リプレイ サービスを提供するセキュリティ プロトコルです。AH は、保護対象のデータ（完全 IP データグラム）に埋め込まれます。
- ESP：Encapsulating Security Payload。データ プライバシー サービスと、オプションとしてデータ認証およびアンチ リプレイ サービスを提供するセキュリティ プロトコルです。ESP は保護対象のデータをカプセル化します。

サポートされるカプセル化

IPsec は、フレーム リレー、ハイ レベル データ リンク制御（HDLC）、および PPP のシリアル カプセル化と連動します。

また、IPsec は、Generic Routing Encapsulation（GRE）、IPinIP レイヤ 3、データリンクスイッチング +（DLSw+）、および Source Route Bridging（SRB）トンネリングプロトコルとも連動します。ただし、マルチポイントトンネルはサポートされません。他のレイヤ 3 のトンネリング プロトコルと IPSec の併用はサポートされない場合があります。

IPsec 機能の概要

IPSec は、次のネットワーク セキュリティ サービスを提供します。（一般に、ローカルセキュリティ ポリシーにより、これらのサービスを 1 つ以上使用するよう指示されます）。

- データ機密性：ネットワークにパケットを伝送する前に IPSec 送信側がパケットを暗号化できます。
- データ整合性：IPSec 受信者は、IPSec 送信者から送信されたパケットを認証し、伝送中にデータが変更されていないかを確認できます。
- データ送信元認証：IPsec 受信者は、送信された IPsec パケットの送信元を認証できます。このサービスは、データ整合性サービスに依存します。
- アンチ リプレイ：IPsec 受信者は、再送されたパケットを検出し、拒否できます。

IPsec は、2 つのピア（2 台のルータなど）間にセキュア トンネルを確立します。機密性が高く、セキュア トンネルを介して送信する必要があるパケットを定義し、セキュア トンネルの特性を指定することによって、機密性の高いパケットを保護するために使用するパラメータを定義します。IPsec ピアが機密パケットを認識すると、ピアは適切なセキュア トンネルを設定し、このトンネルを介してリモート ピアにパケットを送信します（この章で使用するトンネルという用語は、IPsec をトンネル モードで使用することではありません）。

正確には、このトンネルは、2 つの IPsec ピア間に確立されるセキュリティ アソシエーション（SA）のセットです。SA は、機密パケットに適用するプロトコルおよびアルゴリズムを定義し、2 つのピアが使用するキー関連情報を指定します。SA は単方向で、セキュリティ プロトコル（AH または ESP）ごとに確立されます。

2 つのピア間に複数の IPsec トンネルを設定し、トンネルごとに個別の SA のセットを使用することにより、さまざまなデータ ストリームを保護できます。たとえば、一部のデータ ストリームは認証だけが必要で、他のデータ ストリームは暗号化と認証の両方が必要な場合があります。

IKEv1 トランスフォーム セット

インターネット キー エクスチェンジ バージョン 1（IKEv1）トランスフォーム セットは、セキュリティ プロトコルとアルゴリズムの特定の組み合わせを表します。IPsec SA のネゴシエーション中に、ピアは、特定のトランスフォーム セットを使用して特定のデータ フローを保護することに合意します。

IKEv2 トランスフォーム セット

インターネット キー エクスチェンジ バージョン 2（IKEv2）プロポーザルは、IKE_SA_INIT 交換の一部としての IKEv2 SA のネゴシエーションで使用されるトランスフォームのセットです。IKEv2 プロポーザルは、少なくとも 1 つの暗号化アルゴリズム、整合性アルゴリズム、および Diffie-Hellman（DH）グループが設定されている場合にのみ、完全であるとみなされます。プロポーザルが設定されておらず、IKEv2 ポリシーに接続されていない場合、ネゴシエーションではデフォルトのプロポーザルが使用されます。デフォルトのプロポーザルは、次のような通常使用されるアルゴリズムのコレクションです。

```
encryption aes-cbc-128 3des
integrity sha1 md5
group 5 2
```

crypto ikev2 proposal コマンドは **crypto isakmp policy priority** コマンドに似ていますが、IKEv2 プロポーザルには次のような違いがあります。

- IKEv2 プロポーザルを使用すると、各トランスフォーム タイプに対して 1 つ以上のトランスフォームを設定できます。
- IKEv2 プロポーザルには関連付けられた優先順位はありません。

（注） ネゴシエーションで IKEv2 プロポーザルを使用するには、それらを IKEv2 ポリシーにアタッチする必要があります。プロポーザルが設定されていない場合、デフォルトの IKEv2 プロポーザルとデフォルトの IKEv2 ポリシーが使用されます。

トランスフォーム セット：セキュリティ プロトコルとアルゴリズムの組み合わせ

トランスフォーム セットの概要

（注） h-md5-hmac、esp-md5-hmac、esp-des、または esp-3des の使用は推奨されていません。代わりに、ah-sha-hmac、esp-sha-hmac、または esp-aes を使用する必要があります。最新のシスコの暗号化に関する推奨事項については、『Next Generation Encryption』（NGE）ホワイト ペーパーを参照してください。

トランスフォーム セットは、特定のセキュリティ プロトコルとアルゴリズムを組み合わせたものです。IPsec SA のネゴシエーション中に、ピアは、特定のトランスフォーム セットを使用して特定のデータ フローを保護することに合意します。

IKE との IPSec セキュリティ アソシエーション ネゴシエーションで、ピアは両方のピア用の同じトランスフォーム セットを探します。同一のトランスフォーム セットが検出された場合、そのトランスフォーム セットが選択され、両方のピアの IPsec SA の一部として、保護するト

ラフィックに適用されます。（手動で確立した SA は、ピアとネゴシエーションしないため、両方に同じトランスフォーム セットを指定する必要があります）。

次の表に、許可されるトランスフォームの組み合わせを示します。

表 *209* : 許可されるトランスフォームの組み合わせ

トランスフォーム タイプ	トランスフォーム	説明
AH Transform（*1* つ選択）	**ah-md5-hmac**	MD5（メッセージ ダイジェスト 5）（HMAC バリアント）認証アルゴリズムを使用する AH。（非推奨）。
	ah-sha-hmac	SHA（セキュア ハッシュ アルゴリズム）（HMAC バリアント）認証アルゴリズムを使用する AH。
ESP Encryption Transform（*1* つ選択）	**esp-aes**	128 ビット Advanced Encryption Standard（AES）暗号化アルゴリズムを使用する ESP。
	esp-aes 192	192 ビット AES 暗号化アルゴリズムを使用する ESP。
	esp-aes 256	256 ビット AES 暗号化アルゴリズムを使用する ESP。
	esp-des	56 ビットのデータ暗号規格（DES）暗号化アルゴリズムを使用する ESP。（非推奨）。
esp-3des	168 ビット DES 暗号化アルゴリズム（3DES、トリプル DES とも呼ばれる）を使用する ESP。（非推奨）。	
ESP Authentication Transform（*1* つ選択）	**esp-md5-hmac**	MD5（HMAC バリアント）認証アルゴリズムを使用する ESP。（非推奨）。
	esp-sha-hmac	SHA（HMAC バリアント）認証アルゴリズムを使用する ESP。

（注） セキュリティに対する脅威は、脅威からの保護に役立つ暗号化技術と同様に絶え間なく変化しています。最新のシスコの暗号化に関する推奨事項については、『Next Generation Encryption』（NGE）ホワイト ペーパーを参照してください。

IKE および IPsec 暗号化アルゴリズムのための Cisco IOS Suite-B のサポート

Suite-B には次の暗号化アルゴリズムがあります。

- Suite-B-GCM-128：ESP 整合性保護、機密性、および RFC 4106 で規定されている 128 ビット AES using Galois and Counter Mode（AES-GCM）を使用する IPsec 暗号化アルゴリズムを提供します。ESP の整合性の保護と暗号化の両方が必要な場合にはこのスイートを使用する必要があります。
- Suite-B-GCM-256：RFC 4106 で規定されている 256 ビット AES-GCM を使用して、ESP 整合性保護と機密性を提供します。ESP の整合性の保護と暗号化の両方が必要な場合にはこのスイートを使用する必要があります。
- Suite-B-GMAC-128：RFC 4543 で規定されている 128 ビット AES-Galois Message Authentication Code（GMAC）を使用して、ESP 整合性保護を提供しますが、機密性は提供しません。このスイートは、ESP の暗号化が不要である場合のみに使用する必要があります。
- Suite-B-GMAC-256：RFC 4543 で規定されている 256 ビット AES-GMAC を使用して、ESP 整合性保護を提供しますが、機密性は提供しません。このスイートは、ESP の暗号化が不要である場合のみに使用する必要があります。

IPSec 暗号化アルゴリズムは、暗号化が必要な場合に AES-GCM を使用し、暗号化が不要な場合のメッセージの整合性には AES-GMAC を使用します。

IKE ネゴシエーションでは、AES 暗号ブロック連鎖（CBC）モードを使用して暗号化を行い、RFC 4634 に定義されている SHA-256 および SHA-384 ハッシュ アルゴリズムを含む Secure Hash Algorithm（SHA）-2 ファミリを使用してハッシュ機能を実行します。キー交換には RFC 4753 に定義されている Elliptic Curves（ECP）を使用した Diffie-Hellman が使用され、認証を行うには RFC 4754 に定義されている楕円曲線デジタル署名アルゴリズム（ECDSA）が使用されます。

Suite-B の要件

IKE および IPsec を使用する場合、Suite-B によって次のソフトウェア暗号エンジンに要件が課せられます。

- HMAC-SHA256 と HMAC-SHA384 は疑似ランダム関数として使用されます。また、IKE プロトコル内の整合性チェックが使用されます。必要に応じて、HMAC-SHA512 を使用することもできます。

- 楕円曲線グループ 19（256 ビットの ECP 曲線）および 20（384 ビットの ECP 曲線）は、IKE で Diffie-Hellman グループとして使用されます。必要に応じて、グループ 21（521 ビットの ECP 曲線）を使用できます。
- X.509 証明書内の署名操作で、楕円曲線デジタル署名アルゴリズム（ECDSA）（256 ビットおよび 384 ビットの曲線）が使用されます。
- ESP（128 ビットおよび 256 ビットのキー）には、GCM（16 バイトの ICV）および GMAC が使用されます。必要に応じて、192 ビットのキーを使用することもできます。
- ECDSA 署名を使用した X.509 証明書の確認に対する Public Key Infrastructure（PKI）サポートを使用する必要があります。
- ECDSA 署名を使用して証明書要求を生成する場合、および発行された証明書を IOS にインポートする場合に、PKI を使用する必要があります。
- 認証方式として ECDSA signature（ECDSA-sig）を使用できるようにする場合に、IKEv2 を使用する必要があります。

Suite-B の設定情報の入手先

Suite-B の設定のサポートについては、次のマニュアルで説明されています。

- SHA-2 ファミリ（HMAC バリアント）および Elliptic Curve（EC）キー ペアの設定の詳細については、「*Configuring Internet Key Exchange for IPsec VPNs*」機能モジュールを参照してください。
- 整合性アルゴリズム タイプのトランスフォームの設定の詳細については、「*Configuring Internet Key Exchange Version 2 (IKEv2) and FlexVPN Site-to-Site*」機能モジュールの「Configuring the IKEv2 Proposal」を参照してください。
- ECDSA-sig を IKEv2 の認証方式として設定する場合の詳細については、「*Configuring Internet Key Exchange Version 2 (IKEv2) and FlexVPN Site-to-Site*」機能モジュールの「Configuring IKEv2 Profile (Basic)」を参照してください。
- IPsec SA ネゴシエーション用の Elliptic Curve Diffie-Hellman（ECDH）サポートの設定の詳細については、「*Configuring Internet Key Exchange for IPsec VPNs*」および「*Configuring Internet Key Exchange Version 2 and FlexVPN*」機能モジュールを参照してください。

PKI の証明書登録での Suite-B のサポートの詳細については、「*Configuring Certificate Enrollment for a PKI*」機能モジュールを参照してください。

IPsec VPN の設定方法

クリプト アクセス リストの作成

手順の概要

1. **enable**
2. **configure terminal**
3. 次のいずれかを実行します。
   - **access-list** *access-list-number* {**deny** | **permit**} *protocol source source-wildcard destination destination-wildcard* [**log**]
   - **ip access-list extended** *name*
4. 作成するクリプト アクセス リストごとにステップ 3 を繰り返します。

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。

ステップ 3	次のいずれかを実行します。
	• **access-list** *access-list-number* {**deny** | **permit**} *protocol source source-wildcard destination destination-wildcard* [**log**]
	• **ip access-list extended** *name*
	例：
	`Device(config)# access-list 100 permit ip 10.0.68.0 0.0.0.255 10.1.1.0 0.0.0.255`
	例：
	`Device(config)# ip access-list extended vpn-tunnel`
		保護する IP パケットを判別する条件を指定します。
		• 番号または名前によって指定された IP アクセスリストを使用して、条件を指定します。**access-list** コマンドでは、番号付き拡張アクセスリストを指定し、**ip access-list extended** コマンドでは、名前付きアクセスリストを指定します。
		• これらの条件に一致するトラフィックに対して暗号化をイネーブルまたはディセーブルにします。
		ヒント　IPsec で使用できるように "mirror image" クリプトアクセスリストを設定することを推奨します。また、**any** キーワードを使用することは推奨しません。

	コマンドまたはアクション	目的
ステップ 4	作成するクリプト アクセス リストごとにステップ 3 を繰り返します。	—

次の作業

クリプトアクセスリストを1つ以上作成したら、トランスフォームセットをIKEv1およびIKEv2プロポーザルのトランスフォームセットの設定（2168ページ）の手順に従って定義する必要があります。

次に、クリプトマップセットを設定してインターフェイスに適用するときに、クリプトアクセスリストを特定のインターフェイスに関連付ける必要があります。（クリプト マップ セットの作成（2173ページ）およびインターフェイスへのクリプトマップセットの適用（2184ページ）の指示に従ってください）。

IKEv1 および IKEv2 プロポーザルのトランスフォーム セットの設定

この作業は、IKEv1 および IKEv2 プロポーザルとの IPsec SA のネゴシエーション時に IPsec ピアが使用するトランスフォーム セットを定義するために実行します。

機能制限

SEAL 暗号化を指定する場合は、次の制約事項に注意してください。

- ルータと他のピアがハードウェア IPsec 暗号化を備えていないこと。
- ルータおよび他のピアが IPsec をサポートすること。
- ルータおよび他のピアが k9 サブシステムをサポートすること。
- SEAL 暗号化はシスコ製の装置だけで使用可能。したがって、相互運用性はありません。
- IKEv1 と異なり、認証方式と SA ライフタイムは IKEv2 ではネゴシエーション可能ではありません。そのため、これらのパラメータを IKEv2 プロポーザルで設定することはできません。

IKEv1 のトランスフォーム セットの設定

手順の概要

1. **enable**
2. **configure terminal**
3. **crypto ipsec transform-set** *transform-set-name transform1* [*transform2* [*transform3*]]
4. **mode** [**tunnel** | **transport**]
5. **end**
6. **clear crypto sa** [**peer** {*ip-address* | *peer-name*} | **sa map** *map-name* | **sa entry** *destination-address protocol spi*]

7. **show crypto ipsec transform-set** [**tag** *transform-set-name*]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**crypto ipsec transform-set** *transform-set-name transform1* [*transform2* [*transform3*]] 例： `Device(config)# crypto ipsec transform-set aesset esp-aes 256 esp-sha-hmac`	トランスフォームセットを定義し、暗号化トランスフォーム コンフィギュレーション モードを開始します。 • transform 引数に使用できるエントリを定義する複合ルールがあります。これらルールについては、**crypto ipsec transform-set** コマンドのコマンド解説で説明します。また、「トランスフォームセットの概要」の表に、許可されるトランスフォームの組み合わせのリストを示します。
ステップ 4	**mode** [**tunnel** | **transport**] 例： `Device(cfg-crypto-tran)# mode transport`	（任意）トランスフォームセットに関連付けられたモードを変更します。 • このモード設定は、送信元アドレスと宛先アドレスが IPsec ピア アドレスであるトラフィックだけに適用され、その他すべてのトラフィックに対しては無視されます。（他のトラフィックはすべてトンネル モードです）。
ステップ 5	**end** 例： `Device(cfg-crypto-tran)# end`	暗号トランスフォーム コンフィギュレーション モードを終了し、特権 EXEC モードを開始します。
ステップ 6	**clear crypto sa** [**peer** {*ip-address* | *peer-name*} | **sa map** *map-name* | **sa entry** *destination-address protocol spi*] 例： `Device# clear crypto sa`	（任意）既存の IPsec SA を消去して、その後確立された SA でトランスフォーム セットへの変更が有効になるようにします。 手動で確立した SA は、すぐに再確立されます。 • パラメータを指定せずに **clear crypto sa** コマンドを使用すると、SA データベースの内容が完全に消去されるので、アクティブなセキュリティセッションが消去されます。

	コマンドまたはアクション	目的
		• SA データベースのサブセットだけを消去するには、**peer**、**map**、または **entry** キーワードも指定します。
ステップ 7	**show crypto ipsec transform-set** [**tag** *transform-set-name*] 例： `Device# show crypto ipsec transform-set`	（任意）設定済みのトランスフォームセットを表示します。

次の作業

トランスフォーム セットを定義したら、「クリプト マップ セットの作成」の手順に従ってクリプト マップを作成する必要があります。

IKEv2 のトランスフォーム セットの設定

手順の概要

1. **enable**
2. **configure terminal**
3. **crypto ikev2 proposal** *proposal-name*
4. **encryption** *transform1* [*transform2*] ...
5. **integrity** *transform1* [*transform2*] ...
6. **group** *transform1* [*transform2*] ...
7. **end**
8. **show crypto ikev2 proposal**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**crypto ikev2 proposal** *proposal-name* 例： `Device(config)# crypto ikev2 proposal proposal-1`	プロポーザルの名前を指定し、暗号 IKEv2 プロポーザル コンフィギュレーション モードを開始します。 • IKEv2 ポリシーでは、プロポーザル名を使用してプロポーザルが参照されます。

	コマンドまたはアクション	目的
ステップ 4	**encryption** *transform1* [*transform2*] ... 例： `Device(config-ikev2-proposal)# encryption aes-cbc-128`	（任意）次の暗号化タイプのトランスフォームを 1 つ以上指定します。 • AES-CBC 128：128 ビット AES-CBC • AES-CBC 192：192 ビット AES-CBC • AES-CBC 256：256 ビット AES-CBC • 3DES：168 ビット DES（非推奨。AES が推奨されている暗号化アルゴリズムです）。
ステップ 5	**integrity** *transform1* [*transform2*] ... 例： `Device(config-ikev2-proposal)# integrity sha1`	（任意）次の整合性タイプのトランスフォームを 1 つ以上指定します。 • **sha256** キーワードは、ハッシュ アルゴリズムとして SHA-2 ファミリ 256 ビット（HMAC バリアント）を指定します。 • **sha384** キーワードは、ハッシュ アルゴリズムとして SHA-2 ファミリ 384 ビット（HMAC バリアント）を指定します。 • **sha512** キーワードは、ハッシュアルゴリズムとして SHA-2 ファミリ 512 ビット（HMAC バリアント）を指定します。 • **sha1** キーワードは、ハッシュアルゴリズムとして SHA-1（HMAC バリアント）を指定します。 • **md5** キーワードは、ハッシュアルゴリズムとして MD5（HMAC バリアント）を指定します。（非推奨。SHA-1 が推奨されている代替品です）。
ステップ 6	**group** *transform1* [*transform2*] ... 例： `Device(config-ikev2-proposal)# group 14`	（任意）使用可能な DH グループ タイプのトランスフォームを 1 つ以上指定します。 • **1**：768 ビット DH（非推奨） • **2**：1024 ビット DH（非推奨） • **5**：1536 ビット DH（非推奨） • **14**：2048 ビット DH グループを指定します。 • **15**：3072 ビット DH グループを指定します。 • **16**：4096 ビット DH グループを指定します。

	コマンドまたはアクション	目的
		• **19**：256 ビット Elliptic Curve DH（ECDH）グループを指定します。 • **20**：384 ビット ECDH グループを指定します。 • **24**：2048 ビット DH/DSA グループを指定します。
ステップ 7	**end** 例： `Device(config-ikev2-proposal)# end`	暗号 IKEv2 プロポーザル コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。
ステップ 8	**show crypto ikev2 proposal** 例： `Device# show crypto ikev2 proposal`	（任意）各 IKEv2 プロポーザルのパラメータを表示します。

IKEv2 のトランスフォーム セットの例

次の例では、プロポーザルの設定方法を示しています。

各トランスフォーム タイプに対して 1 つのトランスフォームがある IKEv2 プロポーザル

```
Device(config)# crypto ikev2 proposal proposal-1
Device(config-ikev2-proposal)# encryption aes-cbc-128
Device(config-ikev2-proposal)# integrity sha1
Device(config-ikev2-proposal)# group 14
```

各トランスフォーム タイプに対して複数のトランスフォームがある IKEv2 プロポーザル

```
crypto ikev2 proposal proposal-2
encryption aes-cbc-128 aes-cbc-192
integrity sha1 sha256
group 14 15
```

トランスフォームの組み合わせのリストについては、「Configuring Security for VPNs with IPsec」を参照してください。

発信側と応答側の IKEv2 プロポーザル

発信側のプロポーザルは次のとおりです。

```
Device(config)# crypto ikev2 proposal proposal-1
Device(config-ikev2-proposal)# encryption aes-cbc-128 aes-cbc-196
Device(config-ikev2-proposal)# integrity sha1 sha256
Device(config-ikev2-proposal)# group 14 16
```

応答側のプロポーザルは次のとおりです。

```
Device(config)# crypto ikev2 proposal proposal-2
```

```
Device(config-ikev2-proposal)# encryption aes-cbc-196 aes-cbc-128
Device(config-ikev2-proposal)# integrity sha256 sha1
Device(config-ikev2-proposal)# group 16 14
```

このシナリオでは、発信側のアルゴリズムの選択が優先されます。選択されたアルゴリズムは次のとおりです。

```
encryption aes-cbc-128
integrity sha1
group 14
```

次の作業

トランスフォーム セットを定義したら、「クリプト マップ セットの作成」の手順に従ってクリプト マップを作成する必要があります。

クリプト マップ セットの作成

スタティック クリプト マップの作成

IKE を使用して SA が確立されると、IPsec ピアは、新しいセキュリティ アソシエーションに使用する設定をネゴシエートできます。つまり、クリプト マップ エントリ内でリスト（許容されるトランスフォームのリストなど）を指定できます。

このタスクは、IKE を使用して SA を確立するクリプト マップ エントリを作成するために実行します。IPv6 クリプトマップエントリを作成するには、**crypto map** コマンドで **ipv6** キーワードを使用する必要があります。IPv4 クリプトマップでは、**ipv6** キーワードなしで **crypto map** コマンドを使用します。

（注） セキュリティに対する脅威は、脅威からの保護に役立つ暗号化技術と同様に絶え間なく変化しています。最新のシスコの暗号化に関する推奨事項については、『Next Generation Encryption』（NGE）ホワイト ペーパーを参照してください。

手順の概要

1. **enable**
2. **configure terminal**
3. **crypto map** [**ipv6**] *map-name seq-num* [**ipsec-isakmp**]
4. **match address** *access-list-id*
5. **set peer** {*hostname* | *ip-address*}
6. **crypto ipsec security-association dummy** {**pps** *rate* | **seconds** *seconds*}
7. **set transform-set** *transform-set-name1* [*transform-set-name2...transform-set-name6*]
8. **set security-association lifetime** {**seconds** *seconds* | **kilobytes** *kilobytes* | **kilobytes disable**}
9. **set security-association level per-host**
10. **set pfs** [**group1** | **group14** | **group15** | **group16** | **group19** | **group2** | **group20** | **group24** | **group5**]
11. **end**

12. **show crypto map** [**interface** *interface* | **tag** *map-name*]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**crypto map** [**ipv6**] *map-name seq-num* [**ipsec-isakmp**] 例： `Device(config)# crypto map static-map 1 ipsec-isakmp`	クリプト マップ エントリを作成または変更し、クリプト マップ コンフィギュレーション モードを開始します。 • IPv4 クリプトマップでは、**ipv6** キーワードなしでコマンドを使用します。
ステップ 4	**match address** *access-list-id* 例： `Device(config-crypto-m)# match address vpn-tunnel`	拡張アクセス リストに名前を付けます。 • このアクセス リストは、このクリプト マップ エントリに照らして、IPsec で保護する必要のあるトラフィックと IPsec セキュリティで保護する必要のないトラフィックを判別します。
ステップ 5	**set peer** {*hostname* | *ip-address*} 例： `Device(config-crypto-m)# set-peer 192.168.101.1`	リモート IPsec ピアを指定します。これは、IPsec 保護されたトラフィックの転送先となるピアです。 • 複数のリモート ピアに対して、同じ作業を繰り返します。
ステップ 6	**crypto ipsec security-association dummy** {**pps** *rate* | **seconds** *seconds*} 例： `Device(config-crypto-m)# set security-association dummy seconds 5`	ダミー パケットの生成を有効にします。これらのダミー パケットは、クリプト マップ内で作成されたすべてのフローに対して生成されます。
ステップ 7	**set transform-set** *transform-set-name1* [*transform-set-name2...transform-set-name6*] 例： `Device(config-crypto-m)# set transform-set aesset`	このクリプト マップ エントリで許可するトランスフォーム セットを指定します。 • 複数のトランスフォーム セットをプライオリティ順（最高のプライオリティのものが最初）に列挙します。

	コマンドまたはアクション	目的
ステップ 8	**set security-association lifetime** {**seconds** *seconds* | **kilobytes** *kilobytes* | **kilobytes disable**} 例： `Device (config-crypto-m)# set security-association lifetime seconds 2700`	（任意）クリプト マップ エントリの SA ライフタイムを指定します。 • デフォルトでは、クリプト マップの SA はグローバル ライフタイムに従ってネゴシエーションされ、これはディセーブルにできます。
ステップ 9	**set security-association level per-host** 例： `Device(config-crypto-m)# set security-association level per-host`	（任意）送信元と宛先ホストのペアごとに、個別の SA を確立するよう指定します。 • デフォルトで、1 つの IPsec「トンネル」を使用して、複数の送信元ホストと複数の宛先ホストのトラフィックを伝送できます。 **注意** 特定のサブネット間の複数のストリームによって急速にリソースが消費される可能性があるので、このコマンドは注意して使用してください。
ステップ 10	**set pfs** [**group1** | **group14** | **group15** | **group16** | **group19** | **group2** | **group20** | **group24** | **group5**] 例： `Device(config-crypto-m)# set pfs group14`	（任意）IPsec がこのクリプト マップ エントリの新しい SA を要求するときに Password Forward Secrecy（PFS）を要求するか、IPsec ピアから受信する要求に PFS を含めるように要求するかを指定します。 • グループ 1 は、768 ビット Diffie-Hellman（DH）識別子を指定します（デフォルト）。（非推奨）。 • グループ 2 は、1024 ビット DH 識別子を指定します。（非推奨）。 • グループ 5 は、1536 ビット DH 識別子を指定します。（非推奨） • グループ 14 は、2048 ビット DH 識別子を指定します。 • グループ 15 は、3072 ビット DH 識別子を指定します。 • グループ 16 は、4096 ビット DH 識別子を指定します。 • グループ 19 は、256 ビット Elliptic Curve DH（ECDH）識別子を指定します。 • グループ 20 は、384 ビット ECDH 識別子を指定します。

	コマンドまたはアクション	目的
		• グループ 24 は、2048 ビット DH/DSA 識別子を指定します。 • デフォルトでは、PFS は要求されません。このコマンドでグループが指定されなかった場合は、グループ 1 がデフォルトとして使用されます。
ステップ 11	**end** 例： `Device(config-crypto-m)# end`	クリプト マップ コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。
ステップ 12	**show crypto map** [**interface** *interface* | **tag** *map-name*] 例： `Device# show crypto map`	クリプト マップ コンフィギュレーションを表示します。

トラブルシューティングのヒント

特定の設定変更は、それ以後の SA をネゴシエーションする場合にだけ有効になります。新しい設定をすぐに有効にする場合は、既存の SA が変更後の設定で再確立されるように、これらの SA を消去する必要があります。ルータが活発に IPsec トラフィックを処理する場合は、設定変更によって影響を受ける SA データベースの一部だけを消去します（つまり、所定のクリプト マップ セットで確立されている SA だけを消去します）。大規模な変更を行う場合や、ルータが他の IPsec トラフィックをほとんど処理しない場合を除いて、SA データベースを完全に消去しないでください。

IPsec SA をクリアするには、**clear crypto sa** コマンドと適切なパラメータを使用してください。（パラメータをすべて省略すると、SA データベースが完全に消去され、アクティブなセキュリティ セッションも消去されてしまいます）。

次の作業

スタティック クリプトマップを正常に作成したら、IPsec トラフィック フローが通過する各インターフェイスにクリプト マップ セットを適用する必要があります。この作業を完了するには、インターフェイスへのクリプトマップセットの適用（2184ページ）を参照してください。

ダイナミック クリプト マップの作成

ダイナミック クリプト マップ エントリにより、IPsec SA を確立できるトラフィックを制限するクリプト アクセス リストを指定します。トラフィックのフィルタリング中、アクセス リストを指定しないダイナミック クリプトマップエントリは、無視されます。ダイナミック クリプトマップエントリに空のアクセスリストが含まれていると、トラフィックが廃棄されます。クリプト マップ セットにダイナミック クリプト マップ エントリが 1 つしかない場合、クリプト マップ セットは許容範囲内のトランスフォーム セットを指定する必要があります。

このタスクは、SA の確立に IKE を使用するダイナミック クリプト マップ エントリを作成するために実行します。

（注） IPv6 アドレスは、ダイナミック クリプト マップではサポートされません。

（注） セキュリティに対する脅威は、脅威からの保護に役立つ暗号化技術と同様に絶え間なく変化しています。最新のシスコの暗号化に関する推奨事項については、『Next Generation Encryption』（NGE）ホワイト ペーパーを参照してください。

手順の概要

1. **enable**
2. **configure terminal**
3. **crypto dynamic-map** *dynamic-map-name dynamic-seq-num*
4. **set transform-set** *transform-set-name1* [*transform-set-name2...transform-set-name6*]
5. **match address** *access-list-id*
6. **set peer** {*hostname* | *ip-address*}
7. **set security-association lifetime** {**seconds** *seconds* | **kilobytes** *kilobytes* | **kilobytes disable**}
8. **set pfs** [**group1** | **group14** | **group15** | **group16** | **group19** | **group2** | **group20** | **group24** | **group5**]
9. **exit**
10. **exit**
11. **show crypto dynamic-map** [**tag** *map-name*]
12. **configure terminal**
13. **crypto map** *map-name seq-num* **ipsec-isakmp dynamic** *dynamic-map-name* [**discover**]
14. **exit**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**crypto dynamic-map** *dynamic-map-name dynamic-seq-num* 例： `Device(config)# crypto dynamic-map test-map 1`	ダイナミック クリプト マップ エントリを作成し、クリプト マップ コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 4	**set transform-set** *transform-set-name1* [*transform-set-name2...transform-set-name6*] 例： `Device(config-crypto-m)# set transform-set aesset`	このクリプト マップ エントリで許可するトランスフォーム セットを指定します。 • 複数のトランスフォーム セットをプライオリティ順（最高のプライオリティのものが最初）に列挙します。これは、ダイナミック クリプト マップ エントリで必要とされる唯一の設定文です。
ステップ 5	**match address** *access-list-id* 例： `Device(config-crypto-m)# match address 101`	（任意）拡張アクセス リストのリスト番号またはリスト名を指定します。 • このアクセス リストは、このクリプト マップ エントリに照らして、IPsec で保護する必要があるトラフィックと、IPsec セキュリティで保護しないトラフィックを決定します。 （注） ダイナミック クリプトマップでは、アクセス リストの使用は任意ですが、使用することを強く推奨します。 • アクセスリストが設定されている場合、IPsec ピアによって提示されるデータフロー ID は、このクリプトアクセスリストの **permit** ステートメントの範囲内である必要があります。 • アクセス リストが設定されていない場合、デバイスは、IPsec ピアが提示したデータ フロー ID を受け入れます。ただし、アクセス リストが設定されていても指定されたアクセス リストが存在しない、あるいは空である場合、デバイスはすべてのパケットを廃棄します。これは、アクセス リストを指定する必要のあるスタティック クリプト マップと同様です。 • アクセスリストはネゴシエーションだけでなくパケットフィルタリングでも使用されるため、**any** キーワードをアクセスリストで使用する場合には注意が必要です。 • 一致アドレスを設定する必要があります。設定しない場合、パケットがクリアテキスト（暗号解除されて）で送信されるため、動作が不安定になり、TED をイネーブルにできません。

	コマンドまたはアクション	目的
ステップ 6	**set peer** {*hostname* | *ip-address*} 例： `Device(config-crypto-m)# set peer 192.168.101.1`	（任意）リモート IPsec ピアを指定します。リモート ピアが複数ある場合、このステップを繰り返します。 （注） ダイナミック クリプト マップ エントリでは、これを設定することはまれです。ダイナミック クリプト マップ エントリは、多くの場合、未知のリモート ピアで使用されます。
ステップ 7	**set security-association lifetime** {**seconds** *seconds* | **kilobytes** *kilobytes* | **kilobytes disable**} 例： `Device(config-crypto-m)# set security-association lifetime seconds 7200`	（任意）IP セキュリティ SA をネゴシエーションするときに使用されるグローバル ライフタイム値を上書きします（特定のクリプト マップ エントリの場合）。 （注） 高帯域幅環境でのキーの再生成時にパケット損失が発生する可能性を最小限にするには、大量のライフタイム有効期限によってトリガーされるキーの再生成要求をディセーブルにできます。
ステップ 8	**set pfs** [**group1** | **group14** | **group15** | **group16** | **group19** | **group2** | **group20** | **group24** | **group5**] 例： `Device(config-crypto-m)# set pfs group14`	（任意）IPsec がこのクリプト マップ エントリの新しい SA を要求した場合、PFS を要求するように、または IPsec ピアから受信する要求に PFS が含まれることを要求するように指定します。 • グループ 1 は、768 ビット Diffie-Hellman（DH）識別子を指定します（デフォルト）。（非推奨）。 • グループ 2 は、1024 ビット DH 識別子を指定します。（非推奨）。 • グループ 5 は、1536 ビット DH 識別子を指定します。（非推奨） • グループ 14 は、2048 ビット DH 識別子を指定します。 • グループ 15 は、3072 ビット DH 識別子を指定します。 • グループ 16 は、4096 ビット DH 識別子を指定します。 • グループ 19 は、256 ビット Elliptic Curve DH（ECDH）識別子を指定します。

	コマンドまたはアクション	目的
		• グループ 20 は、384 ビット ECDH 識別子を指定します。 • グループ 24 は、2048 ビット DH/DSA 識別子を指定します。 • デフォルトでは、PFS は要求されません。このコマンドでグループが指定されなかった場合は、**group1** がデフォルトとして使用されます。
ステップ 9	**exit** 例： `Device(config-crypto-m)# exit`	クリプト マップ コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードに戻ります。
ステップ 10	**exit** 例： `Device(config)# exit`	グローバル コンフィギュレーション モードを終了します。
ステップ 11	**show crypto dynamic-map** [**tag** *map-name*] 例： `Device# show crypto dynamic-map`	（任意）ダイナミック クリプト マップに関する情報を表示します。
ステップ 12	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 13	**crypto map** *map-name seq-num* **ipsec-isakmp dynamic** *dynamic-map-name* [**discover**] 例： `Device(config)# crypto map static-map 1 ipsec-isakmp dynamic test-map discover`	（任意）クリプト マップ セットにダイナミック クリプト マップを追加します。 • クリプト マップ セット内のプライオリティの最も低いエントリに、ダイナミック マップを参照するクリプト マップ エントリを設定する必要があります。 （注） TED を有効にするには、**discover** キーワードを入力する必要があります。
ステップ 14	**exit** 例： `Device(config)# exit`	グローバル コンフィギュレーション モードを終了します。

トラブルシューティングのヒント

特定の設定変更は、それ以後の SA をネゴシエーションする場合にだけ有効になります。新しい設定をすぐに有効にする場合は、既存の SA が変更後の設定で再確立されるように、これらの SA を消去する必要があります。ルータが活発に IPsec トラフィックを処理する場合は、設定変更によって影響を受ける SA データベースの一部だけを消去します（つまり、所定のクリプト マップ セットで確立されている SA だけを消去します）。大規模な変更を行う場合や、ルータが最小の IPsec トラフィックを処理している場合を除いて、SA データベース全体のクリアを予約しないでください。

IPsec SA をクリアするには、**clear crypto sa** コマンドと適切なパラメータを使用してください。（パラメータをすべて省略すると、SA データベースが完全に消去され、アクティブなセキュリティ セッションも消去されてしまいます）。

次の作業

クリプトマップセットを正常に作成したら、IPsec トラフィック フローが通過する各インターフェイスにクリプトマップセットを適用する必要があります。この作業を完了するには、「インターフェイスへのクリプト マップ セットの適用 （2184 ページ） 」を参照してください。

手動による SA を確立するためのクリプト マップ エントリの作成

このタスクは、クリプト マップ エントリを作成して手動 SA を確立するため（つまり、SA の確立に IKE が使用されない場合）に実行します。IPv6 クリプトマップエントリを作成するには、**crypto map** コマンドで **ipv6** キーワードを使用する必要があります。IPv4 クリプトマップでは、**ipv6** キーワードなしで **crypto map** コマンドを使用します。

手順の概要

1. **enable**
2. **configure terminal**
3. **crypto map** [**ipv6**] *map-name seq-num* [**ipsec-manual**]
4. **match address** *access-list-id*
5. **set peer** {*hostname* | *ip-address*}
6. **set transform-set** *transform-set-name*
7. 次のいずれかを実行します。
   - **set session-key inbound ah** *spi hex-key-string*
   - **set session-key outbound ah** *spi hex-key-string*
8. 次のいずれかを実行します。
   - **set session-key inbound esp** *spi* **cipher** *hex-key-string* [**authenticator** *hex-key-string*]
   - **set session-key outbound esp** *spi* **cipher** *hex-key-string* [**authenticator** *hex-key-string*]
9. **exit**
10. **exit**
11. **show crypto map** [**interface** *interface* | **tag** *map-name*]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**crypto map** [**ipv6**] *map-name seq-num* [**ipsec-manual**] 例： `Device(config)# crypto map mymap 10 ipsec-manual`	作成または変更するクリプト マップ エントリを指定して、クリプト マップ コンフィギュレーション モードを開始します。 • IPv4 クリプトマップでは、**ipv6** キーワードなしで **crypto map** コマンドを使用します。
ステップ 4	**match address** *access-list-id* 例： `Device(config-crypto-m)# match address 102`	このクリプトマップエントリに照らして、IPsec で保護するトラフィックと、IPsec で保護しないトラフィックを決定する IPsec アクセス リストに名前を付けます • IKE を使用しない場合、アクセスリストは **permit** エントリを 1 つだけ指定できます。
ステップ 5	**set peer** {*hostname* | *ip-address*} 例： `Device(config-crypto-m)# set peer 10.0.0.5`	リモート IPsec ピアを指定します。これは、IPsec 保護されたトラフィックの転送先となるピアです • IKE を使用しない場合、ピアを 1 つだけ指定できます。
ステップ 6	**set transform-set** *transform-set-name* 例： `Device(config-crypto-m)# set transform-set someset`	使用するトランスフォーム セットを指定します。 • これは、リモート ピアの対応するクリプトマップ エントリで指定したトランスフォーム セットと同じである必要があります。 （注） IKE を使用しない場合、トランスフォーム セットを 1 つだけ指定できます。
ステップ 7	次のいずれかを実行します。 • **set session-key inbound ah** *spi hex-key-string* • **set session-key outbound ah** *spi hex-key-string* 例：	指定されたトランスフォーム セットに AH プロトコルが含まれている場合、保護対象の着信および発信トラフィックに適用する AH セキュリティ パラメータ インデックス（SPI）およびキーを設定します

	コマンドまたはアクション	目的

	`Device(config-crypto-m)# set session-key inbound ah 256 9876543210987654987654321098765 4`
	例：
	`Device(config-crypto-m)# set session-key outbound ah 256 fedcbafedcbafedcfedcbafedcbafedc`
		• 保護するトラフィックに使用する AH セキュリティ アソシエーションを手動で指定します。

ステップ 8	次のいずれかを実行します。
	• **set session-key inbound esp** *spi* **cipher** *hex-key-string* [**authenticator** *hex-key-string*]
	• **set session-key outbound esp** *spi* **cipher** *hex-key-string* [**authenticator** *hex-key-string*]
	例：
	`Device(config-crypto-m)# set session-key inbound esp 256 cipher 0123456789012345`
	例：
	`Device(config-crypto-m)# set session-key outbound esp 256 cipher abcdefabcdefabcd`
		指定されたトランスフォーム セットに ESP プロトコルが含まれている場合、保護対象の着信および発信トラフィックに適用する Encapsulating Security Payload（ESP）セキュリティ パラメータ インデックス（SPI）およびキーを設定します。
		または
		トランスフォーム セットに ESP 暗号化アルゴリズムが含まれている場合は、暗号キーを指定します。トランスフォーム セットに ESP 認証アルゴリズムが含まれている場合は、認証キーを指定します。
		• 保護するトラフィックに使用する ESP セキュリティ アソシエーションを手動で指定します。

ステップ 9	**exit** 例： `Device(config-crypto-m)# exit`	クリプト マップ コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードに戻ります。
ステップ 10	**exit** 例： `Device(config)# exit`	グローバル コンフィギュレーション モードを終了します。
ステップ 11	**show crypto map** [**interface** *interface* | **tag** *map-name*] 例： `Device# show crypto map`	クリプト マップ コンフィギュレーションを表示します。

トラブルシューティングのヒント

手動で確立された SA の場合、変更を有効にするために SA を消去し、再初期化する必要があります。IPsec SA をクリアするには、**clear crypto sa** コマンドと適切なパラメータを使用してください。（パラメータをすべて省略すると、SA データベース全体がクリアされ、アクティブなセキュリティ セッションもクリアされてしまいます）。

次の作業

クリプトマップセットを正常に作成したら、IPsec トラフィック フローが通過する各インターフェイスにクリプトマップセットを適用する必要があります。この作業を完了するには、「インターフェイスへのクリプト マップ セットの適用 （2184 ページ） 」を参照してください。

インターフェイスへのクリプト マップ セットの適用

クリプトマップセットは、IPsec トラフィックが通過する各インターフェイスに適用する必要があります。インターフェイスにクリプト マップ セットを適用すると、デバイスに対して、トラフィックをクリプトマップで保護する代わりに、インターフェイスのトラフィックをクリプトマップセットに対して評価し、接続中またはセキュリティ アソシエーション ネゴシエーション中に指定されたポリシーを使用するように指示されます。

インターフェイスにクリプト マップを適用するには、次の作業を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **interface** *type/number*
4. **crypto map** *map-name*
5. **exit**
6. **crypto map** *map-name* **local-address** *interface-id*
7. **exit**
8. **show crypto map** [**interface** *interface*]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface** *type/number* 例： `Device(config)# interface FastEthernet 0/0`	インターフェイスを設定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	**crypto map** *map-name* 例： `Device(config-if)# crypto map mymap`	インターフェイスに対してクリプト マップ セットを適用します。
ステップ 5	**exit** 例： `Device(config-if)# exit`	インターフェイス コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードに戻ります。

	コマンドまたはアクション	目的
ステップ 6	**crypto map** *map-name* **local-address** *interface-id* 例： `Device(config)# crypto map mymap local-address loopback0`	（任意）冗長インターフェイスが同じローカルアイデンティティを使用して、同じクリプトマップを共有できるようにします。
ステップ 7	**exit** 例： `Device(config)# exit`	（任意）グローバル コンフィギュレーション モードを終了します。
ステップ 8	**show crypto map** [**interface** *interface*] 例： `Device# show crypto map`	（任意）クリプト マップ コンフィギュレーションを表示します。

IPsec VPN の設定例

例：AES ベースのスタティック暗号マップの設定

この例は、スタティック クリプト マップを設定し、暗号化方式として AES を定義する方法を示しています。

```
crypto isakmp policy 10
 encryption aes 256
 authentication pre-share
 group 14
 lifetime 180
crypto isakmp key cisco123 address 10.0.110.1
!
!
crypto ipsec transform-set aesset esp-aes 256 esp-sha-hmac
 mode transport
!
crypto map aesmap 10 ipsec-isakmp
 set peer 10.0.110.1
 set transform-set aesset
 match address 120
!
!
!
voice call carrier capacity active
!
!
mta receive maximum-recipients 0
!
!
interface FastEthernet0/0
 ip address 10.0.110.2 255.255.255.0
 ip nat outside
 no ip route-cache
 no ip mroute-cache
 duplex auto
```

```
 speed auto
 crypto map aesmap
!
interface Serial0/0
 no ip address
 shutdown
!
interface FastEthernet0/1
 ip address 10.0.110.1 255.255.255.0
 ip nat inside
 no ip route-cache
 no ip mroute-cache
 duplex auto
 speed auto
!
ip nat inside source list 110 interface FastEthernet0/0 overload
ip classless
ip route 0.0.0.0 0.0.0.0 10.5.1.1
ip route 10.0.110.0 255.255.255.0 FastEthernet0/0
ip route 172.18.124.0 255.255.255.0 10.5.1.1
ip route 172.18.125.3 255.255.255.255 10.5.1.1
ip http server
!
!
access-list 110 deny   ip 10.0.110.0 0.0.0.255 10.0.110.0 0.0.0.255
access-list 110 permit ip 10.0.110.0 0.0.0.255 any
access-list 120 permit ip 10.0.110.0 0.0.0.255 10.0.110.0 0.0.0.255
!
```

IPsec を使用した VPN のセキュリティの設定に関する追加のリファレンス

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『Cisco IOS Master Commands List, All Releases』
IKE、IPsec、および PKI のコンフィギュレーション コマンド	• 『Cisco IOS Security Command Reference Commands A to C』 • 『Cisco IOS Security Command Reference Commands D to L』 • 『Cisco IOS Security Command Reference Commands M to R』 • 『Cisco IOS Security Command Reference Commands S to Z』
IKE 設定	「*Configuring Internet Key Exchange for IPsec VPNs*」

関連項目	マニュアル タイトル
Suite-B SHA-2 ファミリ（HMAC バリアント）および Elliptic Curve（EC）キー ペアの設定	「*Configuring Internet Key Exchange for IPsec VPNs*」
Suite-B 整合性アルゴリズム タイプのトランスフォームの設定	「*Configuring Internet Key Exchange Version 2 (IKEv2)*」
IKEv2 用の Suite-B の Elliptic Curve Digital Signature Algorithm（ECDSA）signature（ECDSA-sig）認証方式の設定	「*Configuring Internet Key Exchange Version 2 (IKEv2)*」
IPsec SA ネゴシエーションでの Suite-B の Elliptic Curve Diffie-Hellman（ECDH）のサポート	• 「*Configuring Internet Key Exchange for IPsec VPNs*」 • 「*Configuring Internet Key Exchange Version 2 (IKEv2) and FlexVPN Site-to-Site*」
PKI の証明書登録のための Suite-B サポート	「*PKI* の証明書登録の設定」
推奨される暗号化アルゴリズム	『Next Generation Encryption』

標準

標準	タイトル
なし	—

MIB

MIB	MIB のリンク
• CISCO-IPSEC-FLOW-MONITOR-MIB • CISCO-IPSEC-MIB • CISCO-IPSEC-POLICY-MAP-MIB	選択したプラットフォーム、Cisco IOS ソフトウェア リリース、およびフィーチャセットの MIB を検索してダウンロードする場合は、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

RFC

RFC	タイトル
RFC 2401	『*Security Architecture for the Internet Protocol*』

RFC	タイトル
RFC 2402	『*IP Authentication Header*』
RFC 2403	『*The Use of HMAC-MD5-96 within ESP and AH*』
RFC 2404	『*The Use of HMAC-SHA-1-96 within ESP and AH*』
RFC 2405	『*The ESP DES-CBC Cipher Algorithm With Explicit IV*』
RFC 2406	『*IP Encapsulating Security Payload (ESP)*』
RFC 2407	『*The Internet IP Security Domain of Interpretation for ISAKMP*』
RFC 2408	『*Internet Security Association and Key Management Protocol (ISAKMP)*』

シスコのテクニカル サポート

説明	リンク
右の URL にアクセスして、シスコのテクニカル サポートを最大限に活用してください。これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

IPsec を使用した VPN のセキュリティの設定に関する機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *210 : IPsec VPN* のセキュリティ設定に関する機能情報

機能名	ソフトウェア リリース	機能情報
Advanced Encryption Standard		この機能により、新しい暗号化規格 AES に対するサポートが追加されます。AES は、DES の後継として開発された IPsec および IKE のプライバシー トランスフォームです。 この機能により、次のコマンドが変更されました。**crypto ipsec transform-set**、**encryption (IKE policy)**、**show crypto ipsec transform-set**、**show crypto isakmp policy**。
IOS ソフトウェア暗号での Suite-B のサポート		Suite-B には、IKE と IPSec で使用するための暗号化アルゴリズムの 4 つのユーザ インターフェイス スイートのサポートが追加されています。これは RFC 4869 に記述されています。各スイートは、暗号化アルゴリズム、デジタル署名アルゴリズム、キー合意アルゴリズム、ハッシュまたはメッセージ ダイジェスト アルゴリズムで構成されています。 この機能により、**crypto ipsec transform-set** コマンドが変更されました。

（注） GetVPN 暗号マップは、IOS XE 16.9.1 以降のポートチャネル インターフェイスでサポートされています。

用語集

anti-replay：受信者が再送攻撃から自身を保護するために、古いパケットまたは重複するパケットを拒否できるセキュリティサービス。IPSec は、データ認証とシーケンス番号を組み合わせて使用することにより、このオプション サービスを提供します。Cisco IOS XE IPsec は、手動で確立された SA（IKE ではなく、設定によって確立された SA）を除いて、データ認証サービスを実行するときは必ずこのサービスを提供します。

data authentication：データの整合性および発信元の検証。データ認証は、整合性だけを意味する場合と、整合性と認証の両方の概念を意味する場合があります（ただし、データ発信元認証はデータの整合性に依存します）。

data confidentiality：保護されたデータが第三者に読み取られないようにするセキュリティサービス。

data flow：送信元アドレスまたはマスク、宛先アドレスまたはマスク、IP 次プロトコルフィールド、送信元および宛先ポートの組み合わせによって識別されるトラフィックの集まり。プロ

トコルフィールドおよびポートフィールドには **any** の値が含まれます。IPSec 保護はデータ フローに適用されます。

IKE：Internet Key Exchange（インターネット キー エクスチェンジ）。IKE は、共有セキュリティ ポリシーを確立し、キーを必要とするサービス（IPSec など）のキーを認証します。IPSec トラフィックが通過する前に、各ルータ、ファイアウォール、およびホストはそのピアの ID を検証する必要があります。それには、事前共有キーを両ホストに手動で入力するか、CA サービスを使用します。

IPsec：IP Security（IP セキュリティ）。参加ピア間でのデータの機密性、整合性、および認証を提供するオープン スタンダードの枠組みです。IPSec は、このようなセキュリティ サービスを IP レイヤで提供します。IPSec は IKE を使用して、プロトコルやアルゴリズムのネゴシエーションをローカル ポリシーに基づいて処理し、IPSec で使用される暗号キーや認証キーを生成します。IPSec では、一対のホスト間、一対のセキュリティ ゲートウェイ間、または一対のセキュリティ ゲートウェイとホストの間で 1 つ以上のデータ フローを保護できます。

peer：ここで使用する「ピア」とは、IPsec に参加するルータまたはその他のデバイスです。

PFS：Perfect Forward Secrecy。これは、導き出される共有秘密値に関連する暗号特性です。PFS を使用すると、1 つのキーが損なわれても、これ以降のキーは前のキーの取得元から取得されないため、前および以降のキーには影響しません。

SA：Security Association（セキュリティ アソシエーション）。2 つ以上のエンティティが、特定のデータ フローにおいて安全に通信するために、特定のセキュリティ プロトコル（AH または ESP）と関連してセキュリティ サービスを使用する方法を記述します。トラフィックを保護するために、トランス フォームと共有秘密キーが使用されます。

SPI：Security Parameter Index（セキュリティ パラメータ インデックス）。これは、宛先 IP アドレスおよびセキュリティ プロトコルを組み合わせて、特定の SA を一意に識別する番号です。IKE を使用しない場合、SPI は、手動で各セキュリティ アソシエーションに指定されます。

transform：データ認証、データ機密性、およびデータ圧縮を実現するためにデータフローで実行される処理のリスト。たとえば、トランスフォームには、HMAC MD5 認証アルゴリズムを使用する ESP プロトコル、56 ビット DES 暗号規格アルゴリズムを使用する AH プロトコルおよび HMAC-SHA 認証アルゴリズムを使用する ESP プロトコルなどがあります。

tunnel：ここで使用する「トンネル」とは、2つのピア間（2台のルータなど）の安全な通信パスです。トンネル モードで IPsec を使用することではありません。

第 157 章

IPSec 仮想トンネル インターフェイス

IPsec 仮想トンネル インターフェイス（VTI）では、IPsec トンネルを終了するためのルーティング可能なインターフェイス タイプと、オーバーレイ ネットワークを形成するためにサイト間の保護を定義する簡単な手段が提供されます。IPsec VTI によって、リモート リンクを保護するための IPsec の設定が簡素化され、マルチキャストがサポートされ、さらには、ネットワーク管理およびロード バランシングが簡単に実現できるようになります。

（注） セキュリティに対する脅威は、脅威からの保護に役立つ暗号化技術と同様に絶え間なく変化しています。シスコの暗号化に関する最新の推奨事項の詳細は、『Next Generation Encryption』（NGE）ホワイトペーパーを参照してください。

IPsec 仮想トンネル インターフェイスの制約事項

フラグメンテーション

フラグメンテーションは、IPsec トンネルではサポートされていません。ホストの MTU を小さく設定してパケットフラグメントを回避することや、任意のデバイスでパケットをフラグメント化することを選択できます。

IPsec トランスフォーム セット

IPsec トランスフォーム セットを設定できるのは、トンネル モードでだけです。

IKE セキュリティ アソシエーション

インターネット キー交換（IKE）セキュリティ アソシエーション（SA）は VTI にバインドされています。

IPsec SA トラフィック セレクタ

スタティック VTI では、VTI インターフェイスに接続している単一の IPsec SA だけがサポートされます。IPsec SA のトラフィック セレクタは常に "IP any any" です。

デフォルトでは、スタティック VTI（SVTI）は、仮想トンネルインターフェイスに接続された 1 つの IPsec SA のみをサポートします。IPsec SA のトラフィックセレクタは常に "IP any any" です。

IPv4 パケット

この機能は、IPv4 パケットをカプセル化するように設定された SVTI をサポートしますが、IPv4 パケットで IPv6 パケットを伝送したり、IPv6 パケットで IPv4 パケットを伝送したりすることはできません。

tunnel protection

IPsec IPv4 モードで **tunnel mode ipsec ipv4** コマンドを使用する場合は、**shared** キーワードを設定しないでください。

traceroute

VTI での暗号化オフロードを使用したトレースルート機能はサポートされていません。

VxLAN GPE トンネルインターフェイス

VxLAN GPE トンネルインターフェイスは、IPsec VTI と同じ送信元インターフェイスを使用できません。

IPsec 仮想トンネル インターフェイスに関する情報

IPsec VTI の使用により、リモートアクセスの保護を提供する必要がある場合の設定プロセスが簡素化され、カプセル化に Generic Routing Encapsulation（GRE）またはレイヤ 2 トンネリングプロトコル（L2TP）トンネルを使用する代替手段が提供されます。IPsec VTI を使用するメリットは、設定において物理インターフェイスに対する IPsec セッションのスタティックマッピングが必要ないことです。IPsec トンネル エンドポイントは実際（仮想）のインターフェイスに関連付けられます。トンネルエンドポイントにはルーティング可能なインターフェイスがあるので、多くの共通インターフェイス機能を IPsec トンネルに適用できます。

IPsec VTI によって、複数パスの場合のように、物理インターフェイス上における IP ユニキャストおよびマルチキャストの両方の暗号化トラフィックの送受信の柔軟性が高まります。トラフィックは、トンネルインターフェイスから転送されるときに暗号化され、トンネルインターフェイスに転送されると復号化されます。また、IP ルーティング テーブルによって管理され

ます。IP ルーティングを使用してトラフィックをトンネル インターフェイスに転送すると、IPsec VPN 設定が簡単になります。DVTI は他のすべての実際のインターフェイスと同様に機能するため、トンネルがアクティブになるとすぐに Quality of Service（QoS）、ファイアウォール、およびその他のセキュリティ サービスを適用できます。

IPSec VTI に関する詳細については、次の各項を参照してください。

IPsec 仮想トンネル インターフェイスを使用するメリット

IPsec VTI によって、機能を適用できる仮想インターフェイスを設定できます。暗号化されていないテキスト パケットの機能は VTI 上で設定されます。暗号化されたパケットの機能は物理外部インターフェイス上で適用されます。IPsec VTI を使用すると、ネットワーク アドレス変換（NAT）、ACL、QoS などの各種機能のアプリケーションを分離して、それらを暗号化されていないテキストまたは暗号化されたテキスト、あるいはその両方に適用できます。

スタティック VTI（SVTI）と DVTI という 2 つのタイプの VTI インターフェイスが存在します。

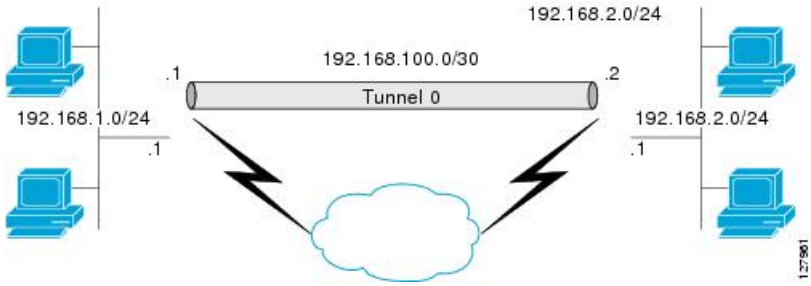
スタティック仮想トンネル インターフェイス

SVTI 設定は、トンネルによって 2 つのサイト間の常にオンであるアクセスが提供される、サイト間接続用に使用できます。

さらに、複数の Cisco IOS ソフトウェア機能を、トンネル インターフェイス上、およびトンネルインターフェイスの物理出力インターフェイス上で直接設定できます。この直接設定によって、ユーザは、暗号化前または暗号化後のパスにおける機能のアプリケーションを確実に管理できます。

次の図に、SVTI の使用方法を示します。

図 *76 : IPsec SVTI*



IPsec VTI によって、ネイティブの IPsec トンネリングがサポートされ、物理インターフェイスのプロパティの大部分が示されます。

SVTI のマルチ SA サポート

デフォルトでは、SVTI のトラフィックセレクタは「any any」に設定されます。その結果、「any any」トラフィックセレクタに対応する SVTI に単一の IPSec SA が接続されます。

Cisco IOS XE Gibraltar 16.12.1 以降では、アクセス制御リスト（ACL）を定義して SVTI に関連付けることで、デフォルトで定義されている「any any」プロキシではなく特定の送信元プロキシと宛先プロキシの間のトラフィックを選択できます。非 any-any トラフィックセレクタごとに IPsec SA が作成されるため、複数の SA が SVTI に接続されます。

この機能は、トンネルモードでの IPSec カプセル化による IPv4 および IPv6 トラフィック保護をサポートしています。この機能は IKEv1 と IKEv2 の両方をサポートしています。

制約事項

- この機能は、共有されたトンネル保護ではサポートされません。
- この機能は、IPSec 混合モードではサポートされません。
- トンネルの両端の SVTI に関連付けられたトラフィックセレクタには、一致する送信元プロキシと宛先プロキシが必要です。トンネルを形成する SVTI のいずれかでトラフィックセレクタを絞り込まないでください。

ACL の特性と SVTI IPSec SA への影響

- SVTI に関連付けられた ACL に「any any」プロキシを含めないでください。「any any」トラフィックセレクタについては、SVTI のデフォルト動作を使用してください（ACL を SVTI に関連付けないでください）。
- SVTI に関連付けられた ACL は **permit** ステートメントのみをサポートしているので、**deny** ステートメントを含めないでください。
- SVTI に関連付けられた ACL の実行時変更はサポートされていません。ACL の ACE を追加または変更する前にトンネルをシャットダウンしてください。
- SVTI への ACL の関連付けを解除すると、既存の IPSec SA が削除され、「IP any any」のデフォルト トラフィック セレクタに関する新しい IPSec SA が形成されます。
- SVTI に関連付けるアクセス制御エントリ（ACE）は 100 までにすることをお勧めします。また、さまざまなトンネルインターフェイスに関連付けられたすべての ACL で使用される ACE の合計が 2000 を超えないようにすることをお勧めします。

逆ルート注入

マルチ SA の SVTI の場合は、IPSec プロファイルで逆ルート注入（RRI）を設定できます。

拡張 ACL または ACE オプション（プロトコル、ポート番号、DHCP など）を使用する場合は、RRI を使用しないでください。ルーティングにはルートマップなどの他の手段を使用してください。

（注） 距離とタグによる RRI 機能は、まだサポートされていません。

SVTI に対するデュアルスタックのサポート

SVTI デュアルスタック機能により、IPv4 を介してトンネリングされる単一の IPsec セキュリティ アソシエーション（SA）を使用して IPv4 トラフィックと IPv6 トラフィックの両方を伝送することが可能になります。IOS XE リリース 17.9 以降では、トンネルインターフェイスの入力側がサードパーティの IPsec クライアントで設定されている場合、ACL の特定のサブネットがサポートされます。また、サードパーティの IPsec クライアントの設定に基づいて、特定のトラフィックセレクタで応答されます。この場合、IPsec は、non-any non-any プロキシ設定をサポートし、トンネルインターフェイスで IPv4 または IPv6 タイプのトラフィックを伝送することを許可します。この機能は、IKEv2 でのみサポートされます。

制約事項

- トンネルモードの設定は、デュアルオーバーレイモードでトンネルインターフェイスを使用する場合に、IPsec プロファイルでのみ許可されます。
- Cisco IOS XE では、ACL フィルタリング インフラストラクチャは、デバイスでローカルに生成されたトラフィックでは機能しません。
- IPsec SA のキー再生成には、一連の同じトラフィックセレクタを使用する必要があります。キー再生成プロセス中にトラフィックセレクタを変更することはできず、変更すると、キー再生成要求はメッセージ *TS_UNACCEPTABLE* をともなって拒否されます。
- IKEv2 レベルでは、最大 16 のトラフィックセレクタが受け入れられます。
- デュアルスタック トンネル インターフェイスの ACL は、サポートされていません。このインターフェイスで設定されている ACL は、デュアルスタック ACL によって上書きされます。

ダイナミック仮想トンネル インターフェイス

DVTI によって、リモートアクセス VPN 用接続のセキュリティ保護とスケーラビリティが向上します。DVTI テクノロジーは、ダイナミック クリプトマップとトンネルを確立するためのダイナミック ハブアンドスポーク方式にとって代わるものです。

（注） IKEv1 または IKEv2 を使用して DVTI を設定できます。レガシー クリプト マップ ベースの設定は、IKEv1 を使用した DVTI しかサポートしません。IKEv2 を使用した DVTI 設定は FlexVPN でのみサポートされます。

DVTI は、サーバと、リモート設定の両方に対して使用可能です。トンネルにより、各 VPN セッションに対して、仮想アクセスインターフェイスがオンデマンドで個別に提供されます。仮想アクセス インターフェイス設定は、仮想テンプレート設定からコピーされます。このコピーには、IPsec 設定と、QoS、NetFlow、ACL といった、仮想テンプレートインターフェイス上で設定されたすべての Cisco IOS ソフトウェア機能が含まれています。

DVTI は、他の現実のインターフェイスと同様に機能するため、トンネルがアクティブになった直後に、QoS、ファイアウォール、またはその他のセキュリティ サービスを適用できます。QoS 機能を使用して、ネットワーク上の各種アプリケーションのパフォーマンスを向上させることが可能です。Cisco IOS ソフトウェア内で提供される各種 QoS 機能の組み合わせを使用して、音声、ビデオ、またはデータ アプリケーションをサポートできます。

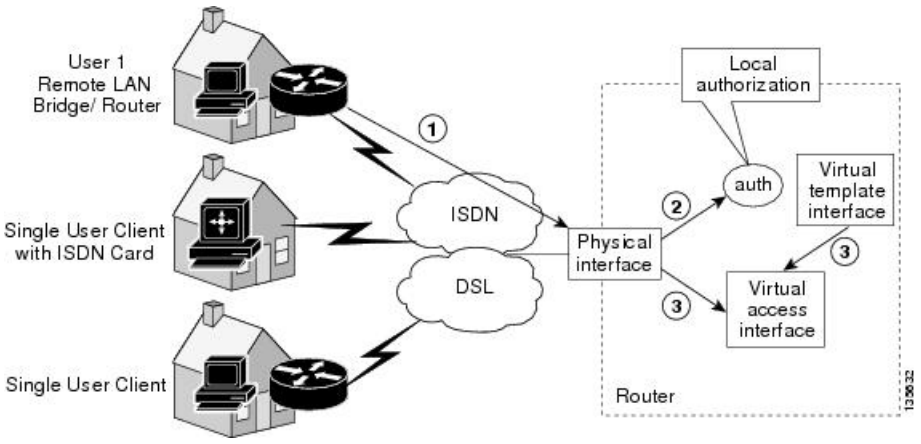
DVTI によって、IP アドレスを効率的に使用できるようになり、また、セキュアな接続を実現できます。DVTI によって、動的にダウンロード可能な、グループごとおよびユーザーごとのポリシーを RADIUS サーバー上で設定できます。グループ単位またはユーザ単位の定義は、拡張認証（Xauth）User または Unity グループを使用して作成することも、証明書から抽出することもできます。DVTI は、標準ベースです。そのため、複数のベンダー環境における相互運用性がサポートされます。IPsec DVTI を使用すれば、リモート アクセス VPN 用のセキュリティ保護が強化された接続を作成できます。また、Cisco Architecture for Voice, Video, and Integrated Data（AVVID）と組み合わせて、IP ネットワーク経由で集約された音声、ビデオ、およびデータを転送できます。DVTI は VPN ルーティングおよび転送（VRF）対応 IPsec の導入を容易にします。VRF は、インターフェイス上で設定されます。

DVTI には、ルータ上での最小限の設定が必要です。単一の仮想テンプレートを設定およびコピーできます。

DVTI によって、IPsec セッション用のインターフェイスが作成され、ダイナミック IPsec VTI の動的なインスタンス化および管理のための仮想テンプレート インフラストラクチャが使用されます。仮想テンプレート インフラストラクチャは、ダイナミック仮想アクセス トンネル インターフェイスを作成するために拡張されます。DVTI は、ハブアンドスポーク設定で使用されます。単一の DVTI で複数のスタティック VTI をサポートできます。

次の図に、DVTI 認証パスを示します。

図 *77 : ダイナミック IPsec VTI*



上の図の認証は、次のパスに従います。

1. ユーザ 1 がルータを呼び出します。
2. ルータ 1 によって ユーザ 1 が認証されます。

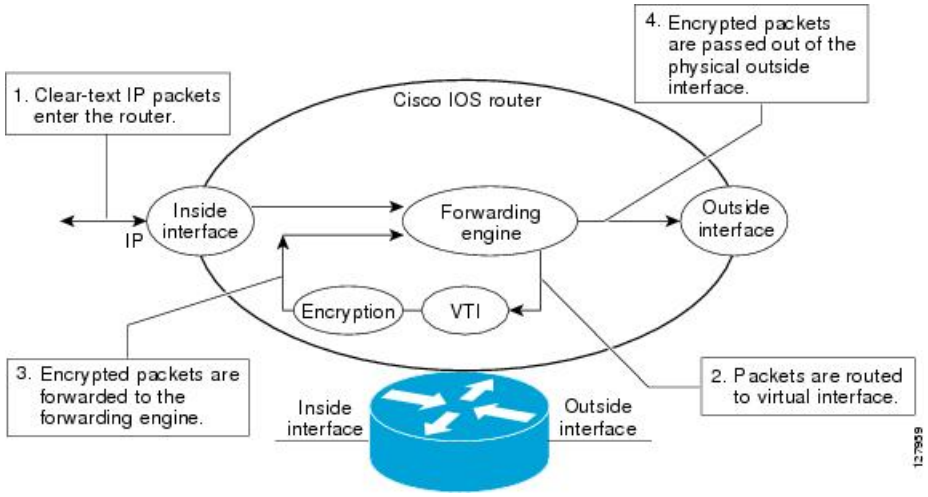
3. IPsec によって、仮想テンプレート インターフェイスから仮想アクセス インターフェイスがコピーされます。

IPsec 仮想トンネル インターフェイスを使用したトラフィックの暗号化

IPsec VTI が設定されると、暗号化がトンネル内で実行されます。トラフィックがトンネル インターフェイスに転送されると、そのトラフィックが暗号化されます。トラフィックの転送は、IP ルーティング テーブルによって処理され、ダイナミックまたはスタティック ルーティングを使用してトラフィックを SVTI にルーティングできます。DVTI では、逆ルート注入が使用されるので、ルーティングの設定がさらに簡単になっています。IP ルーティングを使用してトラフィックを暗号化に転送すると、IPsec VPN 設定が簡単になります。さらに、IPsec 仮想トンネルを使用すれば、IPsec によってマルチキャスト トラフィックを暗号化できます。

次の図に、IPsec トンネルへの IPsec パケット フローを示します。

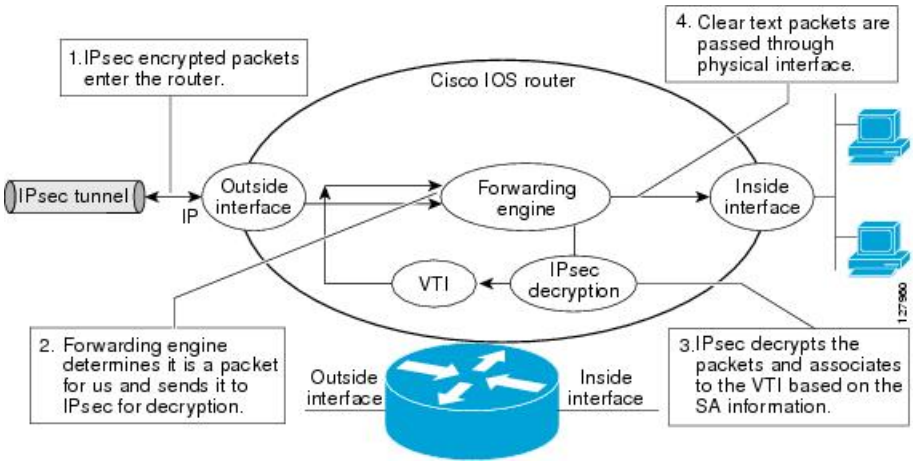
図 *78 : IPsec* トンネルへのパケット フロー



パケットが内部インターフェイスに到着すると、転送エンジンによってパケットが VTI にスイッチングされ、そこで暗号化されます。暗号化されたパケットは転送エンジンに戻され、そこで外部インターフェイスを介してスイッチングされます。

次の図に、IPsec トンネルからのパケット フローを示します。

図 *79 : IPsec* トンネルからのパケット フロー



ダイナミック仮想トンネル インターフェイスのライフ サイクル

IPsec プロファイルによって、DVTI のポリシーが定義されます。ダイナミック インターフェイスが、IKE フェーズ 1 および IKE フェーズ 1.5 の終了時に作成されます。ピアに対する IPsec セッションが終了すると、インターフェイスが削除されます。ピアに対する IKE と IPsec SA の両方が削除されると、IPsec セッションが終了します。

IPsec 仮想トンネル インターフェイスを使用したルーティング

VTI はルーティング可能なインターフェイスなので、暗号化プロセスにおけるルーティングの役割は重要です。トラフィックは、VTI の外に転送される場合にだけ暗号化され、VTI に到着するトラフィックは、適宜、復号化およびルーティングされます。VTI を利用すれば、実際のインターフェイスをトンネルエンドポイントとして使用することによって、暗号化トンネルを確立できます。インターフェイスにルーティングしたり、QoS、ファイアウォール、ネットワーク アドレス変換（NAT）、Netflow 統計情報などのサービスを必要に応じて他のインターフェイスに適用したりできます。インターフェイスをモニタして、それにルーティングできます。このインターフェイスは他の Cisco IOS インターフェイスと同様のメリットを提供します。

FlexVPN 混合モードのサポート

FlexVPN 混合モード機能は、IPsec IPv6 トランスポート経由の IPv4 トラフィックの伝送をサポートします。これは、IPsec スタック上でのデュアル スタックのサポートにつながる第 1 段階です。この実装は、IPv4 トラフィックと IPv6 トラフィックの両方に対する単一の IPSec セキュリティ アソシエーション（SA）ペアの使用をサポートしません。

この機能は、IKEv2 とダイナミック VTI を使用したリモート アクセス VPN に対してのみサポートされます。

FlexVPN 混合モード機能は、Cisco IOS XE Everest 16.4.1 からの IPsec IPv4 トランスポート経由の IPv6 トラフィック伝送をサポートします。

IPsec での自動トンネル モードのサポート

複数ベンダー シナリオで VPN ヘッドエンドを設定する場合は、ピアまたはレスポンダの技術的な詳細を認識しておく必要があります。たとえば、一部のデバイスは IPsec トンネルを使用しているが、他のデバイスは Generic Routing Encapsulation（GRE）または IPsec トンネルを使用している場合やトンネルが IPv4 または IPv6 の場合があります。最後のケースでは、インターネット キー エクスチェンジ（IKE）プロファイルと仮想テンプレートを設定する必要があります。

トンネル モード自動選択機能は、設定を容易にし、レスポンダの詳細の入手を支援します。この機能は、IKE プロファイルから仮想アクセス インターフェイスが作成されるとすぐに、トンネリング プロトコル（GRE または IPsec）とトランスポート プロトコル（IPv4 または IPv6）を自動的に仮想テンプレートに適用します。この機能は、Cisco AnyConnect VPN Client や Microsoft Windows7 Client などのマルチベンダー リモート アクセスを集約しているデュアル スタック ハブ上で役に立ちます。

（注） トンネル モード自動選択機能は、レスポンダの設定のみを容易にします。トンネルはイニシエータに対して静的に設定する必要があります。

VTI に対する IPSec 混合モードのサポート

IPSec 混合モード機能は、IPsec IPv6 トランスポート経由の IPv4 トラフィックの伝送をサポートします。これは、IPsec スタック上でのデュアル スタックのサポートにつながる第 1 段階です。この実装は、IPv4 トラフィックと IPv6 トラフィックの両方に対する単一の IPSec セキュリティ アソシエーション（SA）ペアの使用をサポートしません。

この機能は、SVTI、DVTI、IKEv1、および IKEv2 でサポートされます。

IPsec 仮想トンネル インターフェイスの設定方法

スタティック IPsec 仮想トンネル インターフェイスの設定

始める前に

IPsec プロファイルのトンネル保護を設定する前に、トンネルインターフェイスをシャットダウンする必要があります。設定後、トンネルインターフェイスを手動で有効にしてください。

手順の概要

1. **enable**
2. **configure terminal**
3. **crypto IPsec profile** *profile-name*

4. **set transform-set** *transform-set-name* [*transform-set-name2...transform-set-name6*]
5. **exit**
6. **interface** *type number*
7. **ip address** *address mask*
8. **tunnel mode ipsec ipv4**
9. **tunnel source** *interface-type interface-number*
10. **tunnel destination** *ip-address*
11. **tunnel protection IPsec profile** *profile-name*
12. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**crypto IPsec profile** *profile-name* 例： `Device(config)# crypto IPsec profile PROF`	2 つの IPsec デバイス間の IPsec 暗号化に使用される IPsec パラメータを定義して、IPsec プロファイル コンフィギュレーション モードを開始します。
ステップ 4	**set transform-set** *transform-set-name* [*transform-set-name2...transform-set-name6*] 例： `Device(ipsec-profile)# set transform-set tset`	使用可能なトランスフォームセットを指定します。
ステップ 5	**exit** 例： `Device(ipsec-profile)# exit`	IPsecプロファイル コンフィギュレーション モードを終了して、グローバル コンフィギュレーション モードを開始します。
ステップ 6	**interface** *type number* 例： `Device(config)# interface tunnel 0`	トンネルが設定されるインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 7	**ip address** *address mask* 例：	IP アドレスおよびマスクを指定します。

	コマンドまたはアクション	目的
	`Device(config-if)# ip address 10.1.1.1 255.255.255.0`	
ステップ 8	**tunnel mode ipsec ipv4** 例： `Device(config-if)# tunnel mode ipsec ipv4`	トンネルのモードを定義します。
ステップ 9	**tunnel source** *interface-type interface-number* 例： `Device(config-if)# tunnel source loopback 0`	トンネルの送信元をループバック インターフェイスとして指定します。* （注） * 仮想テンプレートを使用してトンネルモード自動選択機能を設定する場合は、interface virtual-template number type tunnel コマンドでトンネル送信元とトンネルモードを省略します。トンネル送信元とトンネルモードが指定されている場合、IPv6 トランスポートを使用するクライアントは接続に失敗します。
ステップ 10	**tunnel destination** *ip-address* 例： `Device(config-if)# tunnel destination 172.16.1.1`	トンネルの宛先の IP アドレスを指定します。
ステップ 11	**tunnel protection IPsec profile** *profile-name* 例： `Device(config-if)# tunnel protection IPsec profile PROF`	トンネル インターフェイスを IPsec プロファイルに関連付けます。
ステップ 12	**end** 例： `Device(config-if)# end`	インターフェイス コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

IPsec 仮想トンネルインターフェイスを介した BGP の設定

必要に応じて、2つのルータの仮想トンネルインターフェイスを介してBGPを設定するには、次の作業を実行します。

始める前に

スタティック IPsec 仮想トンネル インターフェイスの設定 （2199 ページ） の手順を実行します。

手順の概要

1. **router bgp** *autonomous-system-number*
2. **neighbor** *ip-address* **remote-as** *autonomous-system-number*
3. **network** *network-ip-address* **mask** *subnet-mask*
4. **exit**
5. 2 番目のルータで次のコマンドを入力します。
6. **router bgp** *autonomous-system-number*
7. **neighbor** *ip-address* **remote-as** *autonomous-system-number*
8. **network** *network-ip-address* **mask** *subnet-mask*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**router bgp** *autonomous-system-number* 例： `Device(config)# router bgp 65510`	ルータ コンフィギュレーションモードを開始して、BGP ルーティング プロセスを作成します。 *autonomous-system-number*：他の BGP ルータに対するルータを指定し、同時に渡されるルーティング情報のタギングをする自律システムの番号。番号の範囲は 1 ～ 65535 です。 この例では、この手順の最初のルータは「65510」として識別されます。
ステップ 2	**neighbor** *ip-address* **remote-as** *autonomous-system-number* 例： `Device(config-router)# neighbor 10.1.1.2 remote-as 65511`	*ip-address*：隣接ルータのトンネルインターフェイスの IP アドレス。 *autonomous-system-number*：2 番目のルータのルータを識別する自律システムの番号。番号の範囲は 1 ～ 65535 です。
ステップ 3	**network** *network-ip-address* **mask** *subnet-mask* 例： `Device(config-router)# network 2.2.2.0 mask 255.255.255.0`	*network-ip-address*：BGP でアドバタイズされるネットワークの IP アドレス。たとえば、ループバック インターフェイスの IP アドレスです。 *subnet-mask*：BGP でアドバタイズされるネットワークのサブネットマスク。 （注） BGP ネットワークコマンドの network および mask は、BGP に取り込まれて BGP ネイバーにアドバタイズされるように、ルーティングテーブルにすでに存在するルートと正確に一致する必要があります。これは、network ステートメントがインターフェイス ネットワークを「カバーする」だけで、インターフェイスからマスクを使用してネットワークを取得する EIGRP、OSPF とは異なります。

	コマンドまたはアクション	目的
ステップ 4	**exit** 例： `Device(config-router)# exit`	ルータ コンフィギュレーション モードを終了します。
ステップ 5	2 番目のルータで次のコマンドを入力します。	
ステップ 6	**router bgp** *autonomous-system-number* 例： `Device(config)# router bgp 65511`	ルータ コンフィギュレーション モードを開始して、BGP ルーティング プロセスを作成します。 *autonomous-system-number*：他の BGP ルータに対するルータを指定し、同時に渡されるルーティング情報のタギングをする自律システムの番号。番号の範囲は 1 ～ 65535 です。 この例では、この手順の 2 番目のルータは「65511」として識別されます。
ステップ 7	**neighbor** *ip-address* **remote-as** *autonomous-system-number* 例： `Device(config-router)# neighbor 10.1.1.1 remote-as 65510`	*ip-address*：隣接ルータのトンネルインターフェイスの IP アドレス。
ステップ 8	**network** *network-ip-address* **mask** *subnet-mask* 例： `Device(config-router)# network 1.1.1.0 mask 255.255.255.0`	*network-ip-address*：BGP でアドバタイズされるネットワークの IP アドレス。たとえば、ループバック インターフェイスの IP アドレスです。 *subnet-mask*：BGP でアドバタイズされるネットワークのサブネットマスク。 （注） 正確なネットワーク IP アドレスおよびサブネットマスクを使用してください。

ダイナミック IPsec 仮想トンネル インターフェイスの設定

手順の概要

1. **enable**
2. **configure terminal**
3. **crypto ipsec profile** *profile-name*
4. **set transform-set** *transform-set-name* [*transform-set-name2...transform-set-name6*]
5. **exit**
6. **interface virtual-template** *number* **type tunnel**
7. **tunnel mode ipsec ipv4**
8. **tunnel protection IPsec profile** *profile-name*

9. **exit**
10. **crypto isakamp profile** *profile-name*
11. **match identity address** *ip-address mask*
12. **virtual template** *template-number*
13. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**crypto ipsec profile** *profile-name* 例： `Device(config)# crypto ipsec profile PROF`	2 つの IPsec デバイス間の IPsec 暗号化に使用される IPsec パラメータを定義して、IPsec プロファイル コンフィギュレーション モードを開始します。
ステップ 4	**set transform-set** *transform-set-name* [*transform-set-name2...transform-set-name6*] 例： `Device(ipsec-profile)# set transform-set tset`	クリプト マップ エントリで使用可能なトランスフォーム セットを指定します。
ステップ 5	**exit** 例： `Device(ipsec-profile)# exit`	IPsec プロファイル コンフィギュレーション モードを終了して、グローバル コンフィギュレーション モードを開始します。
ステップ 6	**interface virtual-template** *number* **type tunnel** 例： `Device(config)# interface virtual-template 2 type tunnel`	仮想テンプレート トンネル インターフェイスを定義し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 7	**tunnel mode ipsec ipv4** 例： `Device(config-if)# tunnel mode ipsec ipv4`	トンネルのモードを定義します。
ステップ 8	**tunnel protection IPsec profile** *profile-name* 例： `Device(config-if)# tunnel protection ipsec profile PROF`	トンネル インターフェイスを IPsec プロファイルに関連付けます。

	コマンドまたはアクション	目的
ステップ 9	**exit** 例： `Device(config-if)# exit`	インターフェイス コンフィギュレーション モードを終了します。
ステップ 10	**crypto isakamp profile** *profile-name* 例： `Device(config)# crypto isakamp profile profile1`	仮想テンプレートに使用される ISAKAMP プロファイルを定義します。
ステップ 11	**match identity address** *ip-address mask* 例： `Device(conf-isa-prof)# match identity address 10.1.1.0 255.255.255.0`	ISAKMP プロファイルからの ID を照合して、isakmp-profile コンフィギュレーション モードを開始します。
ステップ 12	**virtual template** *template-number* 例： `Device(config)# virtual-template 1`	ISAKAMP プロファイルにアタッチされた仮想テンプレートを指定します。
ステップ 13	**end** 例： `Device(config)# end`	グローバル コンフィギュレーション モードを終了し、特権 EXEC モードを開始します。

IKEv1 を使用したダイナミック仮想トンネル インターフェイスのマルチ SA サポートの設定

（注） セキュリティに対する脅威は、脅威からの保護に役立つ暗号化技術と同様に絶え間なく変化しています。最新のシスコの暗号化に関する推奨事項については、『Next Generation Encryption』（NGE）ホワイト ペーパーを参照してください。

手順の概要

1. **enable**
2. **configure terminal**
3. **ip vrf** *vrf-name*
4. **rd** *route-distinguisher*
5. **exit**
6. **crypto keyring** *keyring-name*
7. **pre-shared-key** *address* **key** *key*
8. **exit**
9. **crypto isakmp profile** *profile-name*
10. **keyring** *keyring-name*

11. **match identity** *address mask*
12. **virtual-template** *template-number*
13. **exit**
14. **crypto ipsec transform-set** *transform-set-name transform1* [*transform2*] [*transform3*]
15. **exit**
16. **crypto ipsec profile** *name*
17. **set security-policy limit** *maximum-limit*
18. **set transform-set** *transform-set-name* [*transform-set-name2 .... transform-set-name6*]
19. **exit**
20. **interface virtual-template** *number type tunnel*
21. **ip vrf forwarding** *vrf-name*
22. **ip unnumbered** *type number*
23. **tunnel mode ipsec ipv4**
24. **tunnel protection profile ipsec** *profile-name*
25. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ip vrf** *vrf-name* 例： `Device(config)# ip vrf VRF-100-1`	VRFインスタンスを定義し、VRFコンフィギュレーション モードを開始します。
ステップ 4	**rd** *route-distinguisher* 例： `Device(config-vrf)# rd 100:21`	VRF のルーティング テーブルと転送テーブルを作成します。
ステップ 5	**exit** 例： `Device(config-vrf)# exit`	VRF コンフィギュレーション モードを終了して、グローバル コンフィギュレーション モードを開始します。
ステップ 6	**crypto keyring** *keyring-name* 例： `Device(config)# crypto keyring cisco-100-1`	暗号キーリングを定義し、キーリング コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 7	**pre-shared-key** *address* **key** *key* 例： `Device(config-keyring)# pre-shared-key address 10.1.1.1 key cisco-100-1`	インターネット キー エクスチェンジ（IKE）認証に使用する事前共有キーを定義します。
ステップ 8	**exit** 例： `Device(config-keyring)# exit`	キーリング コンフィギュレーション モードを終了して、グローバル コンフィギュレーション モードを開始します。
ステップ 9	**crypto isakmp profile** *profile-name* 例： `Device(config)# crypto isakmp profile cisco-isakmp-profile-100-1`	ISAKMP プロファイルを定義し、ISAKMP コンフィギュレーション モードを開始します。
ステップ 10	**keyring** *keyring-name* 例： `Device(conf-isa-prof)# keyring cisco-100-1`	ISAKMP モードでキーリングを設定します。
ステップ 11	**match identity** *address mask* 例： `Device(conf-isa-prof)# match identity address 10.1.1.0 255.255.255.0`	ISAKMP プロファイルからの ID を照合します。
ステップ 12	**virtual-template** *template-number* 例： `Device(conf-isa-prof)# virtual-template 101`	仮想アクセス インターフェイスの複製に使用される仮想テンプレートを指定します。
ステップ 13	**exit** 例： `Device(conf-isa-prof)# exit`	ISAKMP プロファイル コンフィギュレーション モードを終了して、グローバル コンフィギュレーション モードを開始します。
ステップ 14	**crypto ipsec transform-set** *transform-set-name transform1* [*transform2*] [*transform3*] 例： `Device(config)# crypto ipsec transform-set cisco esp-aes esp-sha-hmac`	トランスフォーム セットを定義し、暗号トランスフォーム コンフィギュレーション モードを開始します。
ステップ 15	**exit** 例： `Device(conf-crypto-trans)# exit`	クリプト トランスフォーム コンフィギュレーションモードを終了して、グローバルコンフィギュレーション モードを開始します。
ステップ 16	**crypto ipsec profile** *name* 例： `Device(config)# crypto ipsec profile cisco-ipsec-profile-101`	2 つの IPsec デバイス間の IPsec 暗号化に使用される IPsec パラメータを定義して、IPsec プロファイル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 17	**set security-policy limit** *maximum-limit* 例： `Device(ipsec-profile)# set security-policy limit 3`	仮想アクセス インターフェイスごとに作成可能なフロー数の上限を定義します。
ステップ 18	**set transform-set** *transform-set-name* [*transform-set-name2 .... transform-set-name6*] 例： `Device(ipsec-profile)# set transform-set cisco`	クリプト マップ エントリで使用されるトランスフォーム セットを指定します。
ステップ 19	**exit** 例： `Device(ipsec-profile)# exit`	IPsec プロファイル コンフィギュレーション モードを終了して、グローバル コンフィギュレーション モードを開始します。
ステップ 20	**interface virtual-template** *number type tunnel* 例： `Device(config)# interface virtual-template 101 type tunnel`	インターフェイスを設定可能な仮想テンプレート インターフェイスを作成し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 21	**ip vrf forwarding** *vrf-name* 例： `Device(config-if)# ip vrf forwarding VRF-100-1`	VRF インスタンスと仮想テンプレート インターフェイスを関連付けます。
ステップ 22	**ip unnumbered** *type number* 例： `Device(config-if)# ip unnumbered GigabitEthernet 0.0`	明示的な IP アドレスをインターフェイスに割り当てずにインターフェイス上の IP 処理をイネーブルにします。
ステップ 23	**tunnel mode ipsec ipv4** 例： `Device(config-if)# tunnel mode ipsec ipv4`	トンネルのモードを定義します。
ステップ 24	**tunnel protection profile ipsec** *profile-name* 例： `Device(config-if)# tunnel protection ipsec profile PROF`	トンネル インターフェイスを IPsec プロファイルに関連付けます。
ステップ 25	**end** 例： `Device(config-if)# end`	インターフェイス コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

SVTI に対する IPsec 混合モードのサポートの設定

手順の概要

1. **enable**
2. **configure terminal**
3. **crypto IPsec profile** *profile-name*
4. **set transform-set** *transform-set-name* [*transform-set-name2...transform-set-name6*]
5. **exit**
6. **interface** *type number*
7. **ip address** *address mask*
8. 次のいずれかを実行します。
   - **tunnel mode ipsec ipv4 v6-overlay**
   - **tunnel mode ipsec ipv6 v4-overlay**
9. **tunnel source** *interface-type interface-type*
10. **tunnel destination** *ip-address*
11. **tunnel protection IPsec profile** *profile-name*
12. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**crypto IPsec profile** *profile-name* 例： `Device(config)# crypto IPsec profile PROF`	2 つの IPsec デバイス間の IPsec 暗号化に使用される IPsec パラメータを定義して、IPsec プロファイル コンフィギュレーション モードを開始します。
ステップ 4	**set transform-set** *transform-set-name* [*transform-set-name2...transform-set-name6*] 例： `Device(ipsec-profile)# set transform-set tset`	クリプト マップ エントリで使用可能なトランスフォーム セットを指定します。

	コマンドまたはアクション	目的
ステップ 5	**exit** 例： `Device(ipsec-profile)# exit`	IPsecプロファイル コンフィギュレーション モードを終了して、グローバル コンフィギュレーション モードを開始します。
ステップ 6	**interface** *type number* 例： `Device(config)# interface tunnel 0`	トンネルが設定されるインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 7	**ip address** *address mask* 例： `Device(config-if)# ip address 10.1.1.1 255.255.255.0`	IP アドレスおよびマスクを指定します。
ステップ 8	次のいずれかを実行します。 • **tunnel mode ipsec ipv4 v6-overlay** • **tunnel mode ipsec ipv6 v4-overlay** 例： `Device(config-if)# tunnel mode ipsec ipv4 v6-overlay`	トンネルのモードを定義します。
ステップ 9	**tunnel source** *interface-type interface-type* 例： `Device(config-if)# tunnel source loopback 0`	トンネルの送信元をループバック インターフェイスとして指定します。
ステップ 10	**tunnel destination** *ip-address* 例： `Device(config-if)# tunnel destination 172.16.1.1`	トンネルの宛先の IP アドレスを指定します。
ステップ 11	**tunnel protection IPsec profile** *profile-name* 例： `Device(config-if)# tunnel protection IPsec profile PROF`	トンネルインターフェイスをIPsecプロファイルに関連付けます。
ステップ 12	**end** 例： `Device(config-if)# end`	インターフェイス コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

ダイナミック VTI に対する IPsec 混合モードのサポートの設定

手順の概要

1. **enable**
2. **configure terminal**
3. **crypto ipsec profile** *profile-name*
4. **set mixed mode**
5. **set transform-set** *transform-set-name* [*transform-set-name2...transform-set-name6*]
6. **exit**
7. **interface virtual-template** *number* **type tunnel**
8. **tunnel mode ipsec ipv4**
9. **tunnel protection IPsec profile** *profile-name*
10. **exit**
11. **crypto isakamp profile** *profile-name*
12. **match identity address** *ip-address mask*
13. **virtual template** *template-number*
14. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**crypto ipsec profile** *profile-name* 例： `Device(config)# crypto ipsec profile PROF`	2 つの IPsec デバイス間の IPsec 暗号化に使用される IPsec パラメータを定義して、IPsec プロファイル コンフィギュレーション モードを開始します。
ステップ 4	**set mixed mode** 例： `Device(config)# set mixed mode`	2 つの IPsec デバイス間の IPsec 暗号化に使用される IPsec パラメータを定義して、IPsec プロファイル コンフィギュレーション モードを開始します。
ステップ 5	**set transform-set** *transform-set-name* [*transform-set-name2...transform-set-name6*] 例： `Device(ipsec-profile)# set transform-set tset`	クリプト マップ エントリで使用可能なトランスフォーム セットを指定します。

	コマンドまたはアクション	目的
ステップ 6	**exit** 例： `Device(ipsec-profile)# exit`	IPsecプロファイル コンフィギュレーション モードを終了して、グローバル コンフィギュレーション モードを開始します。
ステップ 7	**interface virtual-template** *number* **type tunnel** 例： `Device(config)# interface virtual-template 2 type tunnel`	仮想テンプレート トンネル インターフェイスを定義し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 8	**tunnel mode ipsec ipv4** 例： `Device(config-if)# tunnel mode ipsec ipv4`	トンネルのモードを定義します。
ステップ 9	**tunnel protection IPsec profile** *profile-name* 例： `Device(config-if)# tunnel protection ipsec profile PROF`	トンネルインターフェイスをIPsecプロファイルに関連付けます。
ステップ 10	**exit** 例： `Device(config-if)# exit`	インターフェイス コンフィギュレーション モードを終了します。
ステップ 11	**crypto isakamp profile** *profile-name* 例： `Device(config)# crypto isakamp profile profile1`	仮想テンプレートに使用されるISAKAMPプロファイルを定義します。
ステップ 12	**match identity address** *ip-address mask* 例： `Device(conf-isa-prof)# match identity address 10.1.1.0 255.255.255.0`	ISAKMP プロファイルからの ID を照合して、isakmp-profile コンフィギュレーション モードを開始します。
ステップ 13	**virtual template** *template-number* 例： `Device(config)# virtual-template 1`	ISAKAMPプロファイルにアタッチされた仮想テンプレートを指定します。
ステップ 14	**end** 例： `Device(config)# end`	グローバル コンフィギュレーション モードを終了し、特権 EXEC モードを開始します。

スタティック IPsec 仮想トンネルインターフェイスのマルチ SA サポートの設定

ステップ 1 **enable**

例：

```
Device> enable
```

特権 EXEC モードを有効にします。パスワードを入力します（要求された場合）。

ステップ 2 **configure terminal**

例：

```
Device# configure terminal
```

グローバル コンフィギュレーション モードを開始します。

ステップ 3 **crypto IPsec profile** *profile-name*

例：

```
Device(config)# crypto IPsec profile PROF
```

2 つの IPsec デバイス間の IPsec 暗号化に使用される IPsec パラメータを定義して、IPsec プロファイル コンフィギュレーション モードを開始します。

ステップ 4 **set transform-set** *transform-set-name* [*transform-set-name2...transform-set-name6*]

例：

```
Device(ipsec-profile)# set transform-set tset
```

使用可能なトランスフォームセットを指定します。

ステップ 5 **exit**

例：

```
Device(ipsec-profile)# exit
```

IPsec プロファイル コンフィギュレーション モードを終了して、グローバル コンフィギュレーション モードを開始します。

ステップ 6 **interface** *type number*

例：

```
Device(config)# interface tunnel 0
```

トンネルが設定されるインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。

ステップ 7 **ip address** *address mask*

例：

```
Device(config-if)# ip address 10.1.1.1 255.255.255.0
```

IP アドレスおよびマスクを指定します。

ステップ 8 **tunnel mode ipsec** {**ipv4** | **ipv6**}

例：

```
Device(config-if)# tunnel mode ipsec ipv4
```

トンネルのモードを定義します。

ステップ 9 **tunnel source** *interface-type interface-number*

例：

```
Device(config-if)# tunnel source loopback 0
```

トンネルの送信元をループバック インターフェイスとして指定します。

ステップ 10 **tunnel destination** *ip-address*

例：

```
Device(config-if)# tunnel destination 172.16.1.1
```

トンネルの宛先の IP アドレスを指定します。

ステップ 11 **tunnel protection ipsec policy** {**ipv4** | **ipv6**} *acl*

例：

```
Device(config-if)# tunnel protection ipsec policy ipv4 ipsec-acl1
```

ACL を SVTI に関連付けて、非 any-any トラフィックセレクタを定義します。

ステップ 12 **tunnel protection ipsec profile** *profile-name*

例：

```
Device(config-if)# tunnel protection IPsec profile PROF
```

トンネル インターフェイスを IPsec プロファイルに関連付けます。

ステップ 13 **exit**

例：

```
Device(config-if)# exit
```

インターフェイス コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードに入ります。

ステップ 14 **ip access-list extended** *name* または **ipv6 access-list** *name*

例：

IPv4：

```
Device(config)# ip access-list extended ipsec-acl1
```

IPv6：

```
Device(config)# ipv6 access-list ipsec-acl1
```

名前を使用して拡張IPアクセス リストを定義し、拡張名前付きアクセス リストのコンフィギュレーション モードを開始します。

ステップ 15 **permit** *protocol source* [*source-wildcard*] *destination* [*destination-wildcard*] [**option** *option-name*]

例：

```
Device(config-ext-nacl)# permit ip 30.0.1.0 0.0.0.255 10.0.1.0 0.0.0.255
```

ステートメントに指定されたすべての条件に一致するトラフィックを許可します。

送信元プロキシと宛先プロキシの両方にキーワード**any**をワイルドカードとして使用しないでください。「any any」トラフィックセレクタの場合は、ACL が関連付けられていないデフォルトの SVTI を使用します。

deny ステートメントは使用しないでください。

ステップ 16 **end**

例：

```
Device(config-ext-nacl)# end
```

標準の名前付きアクセス リスト コンフィギュレーション モードを終了し、特権 EXEC モードを開始します。

デュアルオーバーレイとしてのトンネルモードの設定

トンネルモードをデュアルオーバーレイとして設定するには、次の手順を実行します。

ステップ 1 **enable**

例：

```
Device> enable
```

特権 EXEC モードを有効にします。パスワードを入力します（要求された場合）。

ステップ 2 **configure terminal**

例：

```
Device# configure terminal
```

グローバル コンフィギュレーション モードを開始します。

ステップ 3 **interface tunnel** *type number*

例：

```
Device(config)# interface tunnel 1
```

トンネルインターフェイスおよび番号を指定し、インターフェイス コンフィギュレーション モードを開始します。

ステップ 4 **ipv6 enable**

例：

```
Device(config-if)# ipv6 enable
```

明示的なIPv6アドレスが設定されていないインターフェイスにおけるIPv6処理をイネーブルにします。

ステップ5 **tunnel source** { **ipv4-address | interface-type | interface-number**}

例：

```
Device(config-if)# tunnel source Gigabitethernet 1
```

送信元 IPv6 アドレスまたは送信元インターフェイス タイプおよびトンネル インターフェイスの番号を指定します。インターフェイスのタイプと番号が指定されている場合、そのインターフェイスはIPv6アドレスを使用して設定する必要があります。

ステップ6 **tunnel mode ipsec dual-overlay**

例：

```
Device(config-if)# tunnel mode ipsec dual-overlay
```

デュアルオーバーレイ トンネルを指定します。**tunnel mode ipsec dual-overlay** コマンドは、トンネルのカプセル化プロトコルを指定します。

ステップ7 **tunnel destination ip address** *address mask*

例：

```
Device(config-if)# tunnel destination 89.89.89.1 255.255.255.255.0
```

トンネル インターフェイスの宛先 IPv6 アドレスを指定します。

ステップ8 **tunnel protection ipsec profile** *ipserc profile-name*

例：

```
Device(config-if)# tunnel protection IPsec profile ipsecprof
```

トンネルインターフェイスをIPsecプロファイルに関連付けます。*name*引数には、IPsecプロファイルの名前を指定します。この値は、**crypto IPsec profile** *name* コマンドで指定した *name* と一致する必要があります。

ステップ9 **exit**

例：

```
Device(config-if)# exit
```

インターフェイス コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードに入ります。

ステップ10 **end**

例：

```
Device(config-if)# end
```

インターフェイス コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

IPsec 仮想トンネル インターフェイスの設定例

例：IPsec を使用したスタティック仮想トンネル インターフェイス

次の設定例では、ピア間の認証用に事前共有キーが使用されています。VPN トラフィックは、暗号化のために IPsec VTI に転送されてから、物理インターフェイスに送信されます。サブネット 10 のトンネルでは、IPsec ポリシーに関してパケットがチェックされ、IPsec 暗号化のために暗号エンジン（CE）に渡されます。次の図に、IPSec VTI 設定を示しています。

図 *80 : IPsec* を使用した *VTI*

ルータのコンフィギュレーション

```
version 12.3
service timestamps debug datetime
service timestamps log datetime
hostname 7200-3
no aaa new-model
ip subnet-zero
ip cef
controller ISA 6/1
!
crypto isakmp policy 1
encr aes
authentication pre-share
group 14
crypto isakmp key Cisco12345 address 0.0.0.0 0.0.0.0
crypto ipsec transform-set T1 esp-aes esp-sha-hmac
crypto ipsec profile P1
set transform-set T1
!
interface Tunnel0
 ip address 10.0.51.203 255.255.255.0

 load-interval 30
 tunnel source 10.0.149.203
 tunnel destination 10.0.149.217
 tunnel mode IPsec ipv4
 tunnel protection IPsec profile P1
!

 ip address 10.0.149.203 255.255.255.0
 duplex full
!

 ip address 10.0.35.203 255.255.255.0
 duplex full
!
ip classless
ip route 10.0.36.0 255.255.255.0 Tunnel0
line con 0
line aux 0
line vty 0 4
end
```

ルータのコンフィギュレーション

```
version 12.3
hostname c1750-17
no aaa new-model
ip subnet-zero
ip cef
crypto isakmp policy 1
encr aes
authentication pre-share
group 14
crypto isakmp key Cisco12345 address 0.0.0.0 0.0.0.0
crypto ipsec transform-set T1 esp-aes esp-sha-hmac
crypto ipsec profile P1
set transform-set T1
!
interface Tunnel0
 ip address 10.0.51.217 255.255.255.0

 tunnel source 10.0.149.217
 tunnel destination 10.0.149.203
 tunnel mode ipsec ipv4
 tunnel protection ipsec profile P1
!
interface
 ip address 10.0.149.217 255.255.255.0
 speed 100
 full-duplex
!
interface
 ip address 10.0.36.217 255.255.255.0
 load-interval 30
 full-duplex
!
ip classless
ip route 10.0.35.0 255.255.255.0 Tunnel0
line con 0
line aux 0
line vty 0 4
end
```

例：IPsec スタティック仮想トンネル インターフェイスの結果の確認

ここでは、設定が正しく動作しているか確認するうえで利用可能な情報を示します。次の出力では、Tunnel 0 およびライン プロトコルが「up」状態です。ライン プロトコルが「down」状態の場合、セッションは非アクティブです。

IPsec スタティック仮想トンネル インターフェイスの確認

```
Router# show interface tunnel 0

Tunnel0 is up, line protocol is up
Hardware is Tunnel
Internet address is 10.0.51.203/24
MTU 1514 bytes, BW 9 Kbit, DLY 500000 usec,
reliability 255/255, txload 103/255, rxload 110/255
Encapsulation TUNNEL, loopback not set
Keepalive not set
Tunnel source 10.0.149.203, destination 10.0.149.217
Tunnel protocol/transport ipsec/ip, key disabled, sequencing disabled
```

```
Tunnel TTL 255
Checksumming of packets disabled, fast tunneling enabled
Tunnel transmit bandwidth 8000 (kbps)
Tunnel receive bandwidth 8000 (kbps)
Tunnel protection via IPsec (profile "P1")
Last input never, output never, output hang never
Last clearing of "show interface" counters never
Input queue: 1/75/0/0 (size/max/drops/flushes); Total output drops: 0
Queueing strategy: fifo
Output queue: 0/0 (size/max)
30 second input rate 13000 bits/sec, 34 packets/sec
30 second output rate 36000 bits/sec, 34 packets/sec
191320 packets input, 30129126 bytes, 0 no buffer
Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
59968 packets output, 15369696 bytes, 0 underruns
0 output errors, 0 collisions, 0 interface resets
0 output buffer failures, 0 output buffers swapped out

Router# show crypto session

Crypto session current status
Interface: Tunnel0
Session status: UP-ACTIVE
Peer: 10.0.149.217 port 500
IKE SA: local 10.0.149.203/500 remote 10.0.149.217/500 Active
IPsec FLOW: permit ip 0.0.0.0/0.0.0.0 0.0.0.0/0.0.0.0
Active SAs: 4,
Router# show ip route

Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2
i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
ia - IS-IS inter area, * - candidate default, U - per-user static route
o - ODR, P - periodic downloaded static route
Gateway of last resort is not set
10.0.0.0/8 is variably subnetted, 4 subnets, 2 masks
C 10.0.35.0/24 is directly connected, Ethernet3/3
S 10.0.36.0/24 is directly connected, Tunnel0
C 10.0.51.0/24 is directly connected, Tunnel0
C 10.0.149.0/24 is directly connected, Ethernet3/0
```

例：VRF 認識スタティック仮想トンネル インターフェイス

VRF をスタティック VTI の例に追加するには、次の例で示すように、**ipvrf** コマンドおよび **ip vrf forwarding** コマンドを設定に含めます。

C8000 ルータ設定

```
hostname c8000
.
.
ip vrf sample-vti1
 rd 1:1
 route-target export 1:1
 route-target import 1:1
!
.
```

```
.
interface Tunnel0
 ip vrf forwarding sample-vti1
 ip address 10.0.51.217 255.255.255.0
 tunnel source 10.0.149.217
 tunnel destination 10.0.149.203
 tunnel mode ipsec ipv4
 tunnel protection ipsec profile P1
.
.
!
end
```

例：QoS を使用したスタティック仮想トンネル インターフェイス

トンネルインターフェイスの下に**service-policy** ステートメントを指定することによって、QoS ポリシーをトンネルエンドポイントに適用できます。次に、トンネルインターフェイスからトラフィックをポリシングする例を示します。

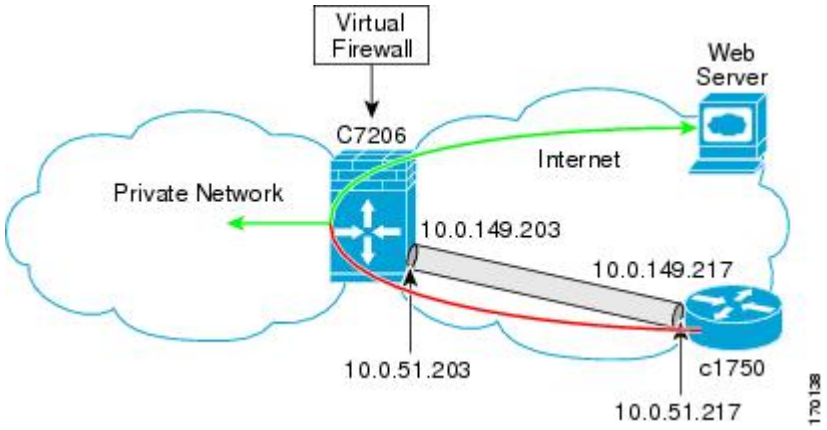
C8000 ルータ設定

```
hostname c8000
.
.
class-map match-all VTI
 match any
!
policy-map VTI
  class VTI
  police cir 2000000
    conform-action transmit
    exceed-action drop
!
.
.
interface Tunnel0
 ip address 10.0.51.217 255.255.255.0
 tunnel source 10.0.149.217
 tunnel destination 10.0.149.203
 tunnel mode ipsec ipv4
 tunnel protection ipsec profile P1
 service-policy output VTI
!
.
.
!
end
```

例：仮想ファイアウォールを使用したスタティック仮想トンネルインターフェイス

仮想ファイアウォールを SVTI トンネルに適用することによって、スポークからのトラフィックを、ハブを通過させてインターネットに送信できます。次の図に、企業ファイアウォールによって本質的に保護されているスポークを使用した SVTI を示します。

図 *81* : 仮想ファイアウォールを使用したスタティック *VTI*



SVTI の基本設定は、仮想ファイアウォール定義を含むように変更されています。

C8000 ルータ設定

```
hostname c8000
.
.
ip inspect max-incomplete high 1000000
ip inspect max-incomplete low 800000
ip inspect one-minute high 1000000
ip inspect one-minute low 800000
ip inspect tcp synwait-time 60
ip inspect tcp max-incomplete host 100000 block-time 2
ip inspect name IOSFW1 tcp timeout 300
ip inspect name IOSFW1 udp
!
.
.
interface GigabitEthernet0/1
 description Internet Connection
 ip address 172.18.143.246 255.255.255.0
 ip access-group 100 in
 ip nat outside
!
interface Tunnel0
 ip address 10.0.51.217 255.255.255.0
 ip nat inside
 ip inspect IOSFW1 in
 tunnel source 10.0.149.217
 tunnel destination 10.0.149.203
 tunnel mode ipsec ipv4
 tunnel protection ipsec profile P1
!
ip classless
ip route 0.0.0.0 0.0.0.0 172.18.143.1
!
ip nat translation timeout 120
ip nat translation finrst-timeout 2
ip nat translation max-entries 300000
ip nat pool test1 10.2.100.1 10.2.100.50 netmask 255.255.255.0
ip nat inside source list 110 pool test1 vrf test-vti1 overload
!
access-list 100 permit esp any any
```

```
access-list 100 permit udp any eq isakmp any
access-list 100 permit udp any eq non500-isakmp any
access-list 100 permit icmp any any
access-list 110 deny   esp any any
access-list 110 deny   udp any eq isakmp any
access-list 110 permit ip any any
access-list 110 deny   udp any eq non500-isakmp any
!
end
```

例：ダイナミック仮想トンネル インターフェイス Easy VPN サーバ

次に、DVTI Easy VPN サーバを使用する例を示します。このサーバは、IPsec リモート アクセス アグリゲータになります。クライアントは、Cisco VPN Client を実行しているホーム ユーザにすることも、Easy VPN クライアントとして設定された Cisco IOS ルータにすることもできます。

C8000 ルータ設定

```
hostname c8000
!
aaa new-model
aaa authentication login local_list local
aaa authorization network local_list local
aaa session-id common
!
ip subnet-zero
ip cef
!
username cisco password 0 cisco123
!
controller ISA 1/1
!
crypto isakmp policy 1
 encr aes
 authentication pre-share
 group 14
!
crypto isakmp client configuration group group1
 key cisco123
 pool group1pool
 save-password
!
crypto isakmp profile vpn1-ra
   match identity group group1
   client authentication list local_list
   isakmp authorization list local_list
   client configuration address respond
   virtual-template 1
!
crypto ipsec transform-set VTI-TS esp-aes esp-sha-hmac
!
crypto ipsec profile test-vti1
 set transform-set VTI-TS
!
interface GigabitEthernet0/1
 description Internet Connection
 ip address 172.18.143.246 255.255.255.0
!
```

```
interface GigabitEthernet0/2
 description Internal Network
 ip address 10.2.1.1 255.255.255.0
!
interface Virtual-Template1 type tunnel
 ip unnumbered GigabitEthernet0/1
 ip virtual-reassembly
 tunnel mode ipsec ipv4
 tunnel protection ipsec profile test-vti1
!
ip local pool group1pool 192.168.1.1 192.168.1.4
ip classless
ip route 0.0.0.0 0.0.0.0 172.18.143.1
!
end
```

例：ダイナミック仮想トンネル インターフェイス Easy VPN サーバの結果の確認

次に、DVTI が、Easy VPN サーバ用に設定されている例を示します。

```
Router# show running-config interface Virtual-Access2

Building configuration...
Current configuration : 250 bytes
!
interface Virtual-Access2
 ip unnumbered GigabitEthernet0/1
 ip virtual-reassembly
 tunnel source 172.18.143.246
 tunnel destination 172.18.143.208
 tunnel mode ipsec ipv4
 tunnel protection ipsec profile test-vti1
 no tunnel protection ipsec initiate
end
Router# show ip route

Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route
Gateway of last resort is 10.2.1.10 to network 0.0.0.0
     172.18.0.0/24 is subnetted, 1 subnets
C       172.18.143.0 is directly connected, GigabitEthernet0/1
     192.168.1.0/32 is subnetted, 1 subnets
S       192.168.1.1 [1/0] via 0.0.0.0, Virtual-Access2
     10.0.0.0/24 is subnetted, 1 subnets
C       10.2.1.0 is directly connected, GigabitEthernet0/2
S*   0.0.0.0/0 [1/0] via 172.18.143.1
```

例：VRF が仮想テンプレートに基づいて設定された場合のダイナミック VTI を使用した VRF 認識 IPsec

次に、仮想テンプレートに基づいて DVTI を利用するように VRF 認識 IPsec を設定する例を示します。

```
hostname c8000
!
ip vrf VRF-100-1
  rd 1:1
!
ip vrf VRF-100-2
  rd 1:1
!
!
!
crypto keyring cisco-100-1
  pre-shared-key address 10.1.1.1 key cisco-100-1
crypto keyring cisco-100-2
  pre-shared-key address 10.1.2.1 key cisco-100-2
crypto isakmp profile cisco-isakmp-profile-100-1
  keyring cisco-100-1
  match identity address 10.1.1.0 255.255.255.0
  virtual-template 101
crypto isakmp profile cisco-isakmp-profile-100-2
  keyring cisco-100-2
  match identity address 10.1.2.0 255.255.255.0
  virtual-template 102
!
!
crypto ipsec transform-set cisco esp-aes esp-sha-hmac
!
crypto ipsec profile cisco-ipsec-profile-101
  set security-policy limit 3
  set transform-set cisco
!
crypto ipsec profile cisco-ipsec-profile-102
  set security-policy limit 5
  set transform-set Cisco
!
interface Virtual-Template101 type tunnel
  ip vrf forwarding VRF-100-1
  ip unnumbered Ethernet 0/0
  tunnel mode ipsec ipv4
  tunnel protection ipsec profile cisco-ipsec-profile-101
!
interface Virtual-Template102 type tunnel
  ip vrf forwarding VRF-100-2
  ip unnumbered Ethernet 0/0
  tunnel mode ipsec ipv4
  tunnel protection ipsec profile cisco-ipsec-profile-102
!
```

例：VRF が仮想テンプレートと IPsec プロファイル内のゲートウェイ オプションに基づいて設定された場合のダイナミック VTI を使用した VRF 認識 IPsec

次に、VRF が仮想テンプレートと IPsec プロファイル内のゲートウェイ オプションに基づいて設定されている場合に、DVTI を利用するように VRF 認識 IPsec を設定する例を示します。

```
hostname c8000
!
ip vrf VRF-100-1
 rd 1:1
!
ip vrf VRF-100-2
 rd 1:1
!
!
!
crypto keyring cisco-100-1
 pre-shared-key address 10.1.1.1 key cisco-100-1
crypto keyring cisco-100-2
 pre-shared-key address 10.1.2.1 key cisco-100-2
crypto isakmp profile cisco-isakmp-profile-100-1
 keyring cisco-100-1
 match identity address 10.1.1.0 255.255.255.0
 virtual-template 101
crypto isakmp profile cisco-isakmp-profile-100-2
 keyring cisco-100-2
 match identity address 10.1.2.0 255.255.255.0
 virtual-template 102
!
!
crypto ipsec transform-set cisco esp-3des esp-sha-hmac
!
crypto ipsec profile cisco-ipsec-profile-101
 set security-policy limit 3
 set transform-set cisco
 set reverse-route gateway 172.16.0.1
!
crypto ipsec profile cisco-ipsec-profile-102
 set security-policy limit 5
 set transform-set cisco
 set reverse-route gateway 172.16.0.1
!
interface Virtual-Template101 type tunnel
 ip vrf forwarding VRF-100-1
 ip unnumbered Ethernet 0/0
 tunnel mode ipsec ipv4
 tunnel protection ipsec profile cisco-ipsec-profile-101
!
interface Virtual-Template102 type tunnel
 ip vrf forwarding VRF-100-2
 ip unnumbered Ethernet 0/0
 tunnel mode ipsec ipv4
 tunnel protection ipsec profile cisco-ipsec-profile-102
!
```

例：VRF が ISAKMP プロファイルに基づいて設定された場合のダイナミック VTI を使用した VRF 認識 IPsec

```
hostname c8000
!
ip vrf VRF-100-1
  rd 1:1
!
ip vrf VRF-100-2
  rd 1:1
```

```
!
crypto keyring cisco-100-1
  pre-shared-key address 10.1.1.1 key cisco-100-1
crypto keyring cisco-100-2
  pre-shared-key address 10.1.2.1 key cisco-100-2
crypto isakmp profile cisco-isakmp-profile-100-1
  vrf VRF-100-1
  keyring cisco-100-1
  match identity address 10.1.1.0 255.255.255.0
  virtual-template 1
crypto isakmp profile cisco-isakmp-profile-100-2
  vrf VRF-100-2
  keyring cisco-100-2
  match identity address 10.1.2.0 255.255.255.0
  virtual-template 1
!
!
crypto ipsec transform-set cisco esp-aes esp-sha-hmac
crypto ipsec profile cisco-ipsec-profile
  set security-policy limit 3
  set transform-set cisco
!
!
!
interface Virtual-Template 1 type tunnel
  ip unnumbered ethernet 0/0
  tunnel mode ipsec ipv4
  tunnel protection ipsec profile cisco-ipsec-profile
!
!
```

例：VRF が ISAKMP プロファイルと IPsec プロファイル内のゲートウェイ オプションに基づいて設定された場合のダイナミック VTI を使用した VRF 認識 IPsec

次に、VRF が ISAKMP プロファイルと IPsec プロファイル内のゲートウェイ オプションに基づいて設定されている場合に、DVTI を利用するように VRF 認識 IPsec を設定する例を示します。

```
hostname C8000 server
!
ip vrf VRF-100-1
 rd 1:1
!
ip vrf VRF-100-2
 rd 1:1
!
crypto keyring cisco-100-1
 pre-shared-key address 10.1.1.1 key cisco-100-1
crypto keyring cisco-100-2
 pre-shared-key address 10.1.2.1 key cisco-100-2
crypto isakmp profile cisco-isakmp-profile-100-1
 vrf VRF-100-1
 keyring cisco-100-1
 match identity address 10.1.1.0 255.255.255.0
```

```
 virtual-template 1
crypto isakmp profile cisco-isakmp-profile-100-2
 vrf VRF-100-2
 keyring cisco-100-2
 match identity address 10.1.2.0 255.255.255.0
 virtual-template 1
!
!
crypto ipsec transform-set cisco esp-3des esp-sha-hmac
crypto ipsec profile cisco-ipsec-profile
 set security-policy limit 3
 set transform-set cisco
 set reverse-route gateway 172.16.0.1
!
!
!
interface Virtual-Template1 type tunnel
 ip unnumbered Ethernet 0/0
 tunnel mode ipsec ipv4
 tunnel protection ipsec profile cisco-ipsec-profile
!
!
```

例：VRF が仮想テンプレートと ISAKMP プロファイルの両方に基づいて設定された場合のダイナミック VTI を使用した VRF 認識 IPsec

（注） ISAKMPプロファイルと仮想テンプレートに基づいて別々のVRFが設定されている場合は、仮想テンプレートに基づいて設定されたVRFが優先されます。この設定は推奨されません。

次に、VRF が仮想テンプレートと ISAKMP プロファイルの両方に基づいて設定されている場合に、DVTI を利用するように VRF 認識 IPsec を設定する例を示します。

```
hostname C8000 server
.
.
.
ip vrf test-vti2
 rd 1:2
 route-target export 1:1
 route-target import 1:1
!
.
.
.
ip vrf test-vti1
 rd 1:1
 route-target export 1:1
 route-target import 1:1
!
.
.
.
crypto isakmp profile cisco-isakmp-profile
```

```
 vrf test-vti2
 keyring key
 match identity address 10.1.1.0 255.255.255.0
!
.
.
.
interface Virtual-Template1 type tunnel
 ip vrf forwarding test-vti1
 ip unnumbered Loopback 0
 ip virtual-reassembly
 tunnel mode ipsec ipv4
 tunnel protection ipsec profile test-vti1
!
.
.
.
end
```

例：仮想ファイアウォールを使用したダイナミック仮想トンネルインターフェイス

DVTI Easy VPN サーバは、仮想ファイアウォールの背後に設定できます。Behind-the-firewall 設定を使用すれば、ユーザはネットワークに入れますが、ネットワーク ファイアウォールは不正アクセスから保護されます。仮想ファイアウォールでは、コンテキスト ベースのアクセス コントロール（CBAC）と、インターネットインターフェイスおよび仮想テンプレートに対して適用される NAT が使用されます。

```
hostname c8000
.
.
ip inspect max-incomplete high 1000000
ip inspect max-incomplete low 800000
ip inspect one-minute high 1000000
ip inspect one-minute low 800000
ip inspect tcp synwait-time 60
ip inspect tcp max-incomplete host 100000 block-time 2
ip inspect name IOSFW1 tcp timeout 300
ip inspect name IOSFW1 udp
!
.
.
interface GigabitEthernet0/1
 description Internet Connection
 ip address 172.18.143.246 255.255.255.0
 ip access-group 100 in
 ip nat outside
!
interface GigabitEthernet0/2
 description Internal Network
 ip address 10.2.1.1 255.255.255.0
!
interface Virtual-Template1 type tunnel
 ip unnumbered Loopback0
 ip nat inside
 ip inspect IOSFW1 in
 tunnel mode ipsec ipv4
 tunnel protection ipsec profile test-vti1
```

```
!
ip classless
ip route 0.0.0.0 0.0.0.0 172.18.143.1
!
ip nat translation timeout 120
ip nat translation finrst-timeout 2
ip nat translation max-entries 300000
ip nat pool test1 10.2.100.1 10.2.100.50 netmask 255.255.255.0
ip nat inside source list 110 pool test1 vrf test-vti1 overload
!
access-list 100 permit esp any any
access-list 100 permit udp any eq isakmp any
access-list 100 permit udp any eq non500-isakmp any
access-list 100 permit icmp any any
access-list 110 deny   esp any any
access-list 110 deny   udp any eq isakmp any
access-list 110 permit ip any any
access-list 110 deny   udp any eq non500-isakmp any
!
end
```

例：QoS を使用したダイナミック仮想トンネル インターフェイス

サービス ポリシーを仮想テンプレートに適用することによって、QoS を DVTI トンネルに追加できます。テンプレートを複製して仮想アクセスインターフェイスを作成した場合は、サービス ポリシーが仮想アクセス インターフェイスにも適用されます。次に、QoS が追加された DVTI 基本設定の例を示します。

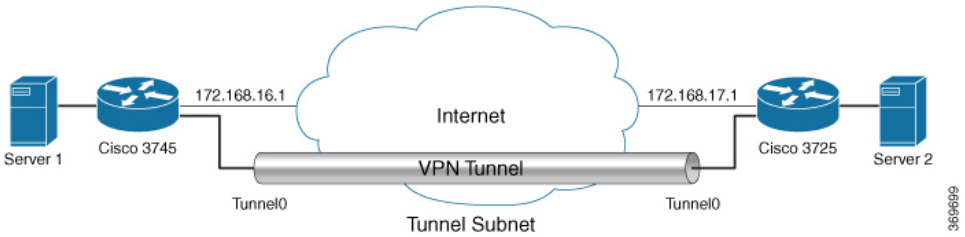
```
hostname c8000
.
.
class-map match-all VTI
 match any
!
policy-map VTI
  class VTI
  police cir 2000000
    conform-action transmit
    exceed-action drop
!
.
.
interface Virtual-Template1 type tunnel
 ip vrf forwarding test-vti1
 ip unnumbered Loopback0
 ip virtual-reassembly
 tunnel mode ipsec ipv4
 tunnel protection ipsec profile test-vti1
 service-policy output VTI
!
.
.
!
end
```

例：複数の IPsec SA を使用したスタティック仮想トンネルインターフェイス

次の例では、SVTI を使用して Cisco 3745 と Cisco 3725 の 2 つのルータの間で IPSec トンネルを確立します。この設定では、非 any-any トラフィックセレクタを使用し、複数の IPSec SA の形成を有効にします。

IPv4 トンネルモードのルータでの設定例：

次の図は、設定の参照トポロジを示しています。



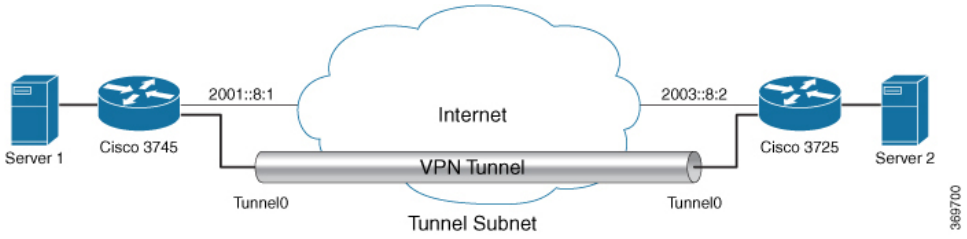
Cisco 3745 ルータの設定例は、次のとおりです。

```
crypto isakmp policy 1
 authentication pre-share
 group 2
!
crypto isakmp policy 5
 encr 3des
 authentication pre-share
 group 2
crypto isakmp key example address 172.168.17.1
!
!
crypto ipsec transform-set svti1 esp-3des esp-sha-hmac
 mode tunnel
!
!
crypto ipsec profile ipsec_prof
 set transform-set svti1
!
!
!
interface Loopback0
 ip address 30.0.0.1 255.255.255.0
!
interface Loopback1
 ip address 50.0.0.1 255.255.255.0
!
interface Tunnel0
 ip address 11.1.1.2 255.255.255.0
 tunnel source Ethernet0/0
 tunnel mode ipsec ipv4
 tunnel destination 172.168.17.1
 tunnel protection ipsec policy ipv4 ipsec_acl1
 tunnel protection ipsec profile ipsec_prof
!
interface Ethernet0/0
 ip address 172.168.16.1 255.255.255.0
!
```

```
!
ip access-list extended ipsec_acl1
permit ip 30.0.0.0 0.0.0.255 40.0.0.0 0.0.0.255
permit ip 50.0.0.0 0.0.0.255 60.0.0.0 0.0.0.255
```

IPv6 トンネルモードのルータでの設定例：

次の図は、設定の参照トポロジを示しています。



Cisco 3745 ルータの設定例は、次のとおりです。

```
crypto isakmp policy 1
 authentication pre-share
 group 2
!
crypto isakmp policy 5
 encr 3des
 authentication pre-share
 group 2
crypto isakmp key example address ipv6 2003::8:2/112
!
!
crypto ipsec transform-set svti1 esp-3des esp-sha-hmac
 mode tunnel
!
!
crypto ipsec profile ipsec_prof
 set transform-set svti1
!
!
!
interface Loopback0
 ipv6 address 2005::10:1/112
 ipv6 enable
!
interface Loopback1
 ipv6 address 2005::15:1/112
 ipv6 enable
!
interface Loopback2
 ipv6 address 2005::20:1/112
 ipv6 enable
!
interface Tunnel0
 ip address 11.1.1.2 255.255.255.0
 ipv6 address 400::10:1/112
 ipv6 enable
 tunnel source Ethernet0/0
 tunnel mode ipsec ipv6
 tunnel destination 2003::8:2
 tunnel protection ipsec policy ipv6 ipsec_acl2
 tunnel protection ipsec profile ipsec_prof
!
```

```
interface Ethernet0/0
 ipv6 address 2001::8:1/112
 ipv6 enable
!
!
ipv6 access-list ipsec_acl2
sequence 10 permit ipv6 host 2005::10:1 host 2005::11:1
sequence 20 permit ipv6 host 2005::15:1 host 2005::16:1
sequence 30 permit ipv6 host 2005::20:1 host 2005::21:1
```

例：デュアルオーバーレイとしてのトンネルモードの設定

次に、トンネルモードをデュアルオーバーレイとして設定する例を示します。

```
Device# configure terminal
Router(config)# interface tunnel 1
Router(config-if)# ipv6 enable
Router(config-if)# tunnel source ethernet 0/0
Router(config-if)# tunnel mode ipsec dual-overlay
Router(config-if)# tunnel destination 89.89.89.1 255.255.255.255.0
Device(config-if)# tunnel protection IPsec profile ipsecprof
```

デュアルオーバーレイとしてのトンネルモードの設定の確認

次のコマンドを使用して、設定をトラブルシューティングします。

- **show crypto session [detail]**
- **show crypto ipsec sa**
- **show crypto map**
- **show crypto socket**
- **show crypto ikev2 session [detail]**

```
Device# show crypto map
Crypto Map: "Tunnel0-head-0" IKEv2 profile: prof

Crypto Map IPv4 "Tunnel0-head-0" 65536 ipsec-isakmp
 IKEv2 Profile: prof
 Profile name: prof
 Security association lifetime: 4608000 kilobytes/120 seconds
 Dualstack (Y/N): N

 Responder-Only (Y/N): N
 PFS (Y/N): N
 Mixed-mode : Disabled
 Transform sets={
  default:  { esp-aes esp-sha-hmac  } ,
 }

Crypto Map IPv4 "Tunnel0-head-0" 65537 ipsec-isakmp
 Map is a PROFILE INSTANCE.
 Peer = 10.10.10.2
 IKEv2 Profile: prof
 Extended IP access list
     access-list  permit ip any any
 Current peer: 10.10.10.2
 Security association lifetime: 4608000 kilobytes/120 seconds
       Dualstack (Y/N): Y
```

```
        TRUE  ident (addr/mask/prot/port): {LOCAL -> REMOTE}
              0.0.0.0/0.0.0.0/0/0 -> 0.0.0.0/0.0.0.0/0/0
              ::/0.0.0.0/0/0 -> ::/0/0/0
 Responder-Only (Y/N): N
 PFS (Y/N): N
 Mixed-mode : Disabled
 Transform sets={
  default:  { esp-aes esp-sha-hmac  } ,
 }
 Always create SAs
 Interfaces using crypto map Tunnel0-head-0:
  Tunnel0
```

```
Device# show  crypto ipsec sa

interface: Tunnel0
    Crypto map tag: Tunnel0-head-0, local addr 10.10.10.1

   protected vrf: (none)
   local  ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
   remote ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
    TRUE  ident (addr/mask/prot/port): {LOCAL -> REMOTE}
              0.0.0.0/0.0.0.0/0/0 -> 0.0.0.0/0.0.0.0/0/0
              ::/0.0.0.0/0/0 -> ::/0/0/0
   current_peer 10.10.10.2 port 500
     PERMIT, flags={origin_is_acl,}
    #pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
    #pkts decaps: 0, #pkts decrypt: 0, #pkts verify: 0
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0
    #pkts not decompressed: 0, #pkts decompress failed: 0
    #send errors 0, #recv errors 0

     local crypto endpt.: 10.10.10.1, remote crypto endpt.: 10.10.10.2
     plaintext mtu 1438, path mtu 1500, ip mtu 1500, ip mtu idb Ethernet0/0
     current outbound spi: 0x4776A36B(1198957419)
     PFS (Y/N): N, DH group: none

     inbound esp sas:
      spi: 0xA97EDEE7(2843664103)
        transform: esp-aes esp-sha-hmac ,
        in use settings ={Tunnel, }
       conn id: 4, flow_id: 4, sibling_flags FFFFFFFF80000040, crypto map: Tunnel0-head-0

         sa timing: remaining key lifetime (k/sec): (4377587/76)
        IV size: 16 bytes
        replay detection support: Y
        Status: ACTIVE(ACTIVE)

     inbound ah sas:

     inbound pcp sas:

     outbound esp sas:
      spi: 0x4776A36B(1198957419)
        transform: esp-aes esp-sha-hmac ,
        in use settings ={Tunnel, }
       conn id: 3, flow_id: 3, sibling_flags FFFFFFFF80000040, crypto map: Tunnel0-head-0

         sa timing: remaining key lifetime (k/sec): (4377587/76)
        IV size: 16 bytes
        replay detection support: Y
        Status: ACTIVE(ACTIVE)
```

```
     outbound ah sas:

     outbound pcp sas:
Device# show crypto socket

Number of Crypto Socket connections 1

   Tu0 Peers (local/remote): 10.10.10.1/10.10.10.2
       Local Ident  (addr/mask/port/prot): (0.0.0.0/0.0.0.0/0/0)
       Remote Ident (addr/mask/port/prot): (0.0.0.0/0.0.0.0/0/0)
        TRUE  ident (addr/mask/prot/port): {LOCAL -> REMOTE}
             0.0.0.0/0.0.0.0/0/0 -> 0.0.0.0/0.0.0.0/0/0
             ::/0.0.0.0/0/0 -> ::/0/0/0
       IPSec Profile: "prof"
       Socket State: Open
       Client: "TUNNEL SEC" (Client State: Active)
Crypto Sockets in Listen state:
Client: "TUNNEL SEC" Profile: "prof" Map-name: "Tunnel0-head-0"

Device# show cry ikev2 session
 IPv4 Crypto IKEv2 Session

Session-id:1, Status:UP-ACTIVE, IKE count:1, CHILD count:1

Tunnel-id Local                 Remote                fvrf/ivrf            Status
1         10.10.10.1/500        10.10.10.2/500        none/none            READY
      Encr: AES-CBC, keysize: 256, PRF: SHA512, Hash: SHA512, DH Grp:19, Auth sign: PSK,
 Auth verify: PSK
      Life/Active Time: 86400/145 sec
      CE id: 1001, Session-id: 1
      Local spi: 25A0B173944015D3       Remote spi: 9F0C7677425670E1
Child sa:
          local selector  0.0.0.0/0 - 255.255.255.255/65535
          local selector  ::/0 - FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF/65535
          remote selector 0.0.0.0/0 - 255.255.255.255/65535
          remote selector ::/0 - FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF/65535
          ESP spi in/out: 0xA97EDEE7/0x4776A36B

 IPv6 Crypto IKEv2 Session

Device# show crypto session
Crypto session current status

Interface: Tunnel0
Profile: prof
Session status: UP-ACTIVE
Peer: 10.10.10.2 port 500
  Session ID: 1
  IKEv2 SA: local 10.10.10.1/500 remote 10.10.10.2/500 Active
  IPSEC FLOW: permit ip   0.0.0.0/0.0.0.0 0.0.0.0/0.0.0.0
  TRUE IDENT (addr/mask/prot/port): {LOCAL -> REMOTE}
             0.0.0.0/0.0.0.0/0/0 -> 0.0.0.0/0.0.0.0/0/0
             ::/0.0.0.0/0/0 -> ::/0/0/0
        Active SAs: 2, origin: crypto map
```

IPsec 仮想トンネル インターフェイスに関する追加のリファレンス

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『Cisco IOS Master Command List, All Releases』
セキュリティ コマンド	• 『Cisco IOS Security Command Reference Commands A to C』 • 『Cisco IOS Security Command Reference Commands D to L』 • 『Cisco IOS Security Command Reference Commands M to R』 • 『Cisco IOS Security Command Reference Commands S to Z』
IPsec の設定	『*Configuring Security for VPNs with IPsec*』
QoS の設定	『*Cisco IOS Quality of Service Solutions Configuration Guide*』
EasyVPN の設定	• 「*Cisco Easy VPN Remote*」 • 「*Easy VPN Server*」
推奨される暗号化アルゴリズム	『Next Generation Encryption』

標準および RFC

標準/RFC	タイトル
RFC 2401	『*Security Architecture for the Internet Protocol*』
RFC 2408	『*Internet Security Association and Key Management Protocol*』
RFC 2409	『*The Internet Key Exchange (IKE)*』

シスコのテクニカル サポート

説明	リンク
右の URL にアクセスして、シスコのテクニカル サポートを最大限に活用してください。これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

IPsec 仮想トンネル インターフェイスに関する機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *211 : IPsec* 仮想トンネル インターフェイスに関する機能情報

機能名	リリース	機能の設定情報
ダイナミック IPsec VTI	12.3(7)T 12.3(14)T	ダイナミック VTI によって IP アドレスの使用が効率的になり、セキュアな接続が提供されます。ダイナミック VTI によって、動的にダウンロード可能な、グループごとおよびユーザごとのポリシーを RADIUS サーバ上で設定できます。IPsec ダイナミック VTI を使用すれば、リモート アクセス VPN 用の高度にセキュアな接続を構築することができます。ダイナミック VTI によって、VRF 認識 IPsec の導入が簡単になります。 次のコマンドが導入または変更されました。 **crypto isakmp profile, interface virtual-template, show vtemplate, tunnel mode, virtual-template.**
FlexVPN 混合モードのサポート	15.4(2)T Cisco IOS XE Release 3.10S	FlexVPN 混合モード機能は、IPsec IPv6 トランスポート経由の IPv4 トラフィックの伝送をサポートします。これは、IPsec スタック上でのデュアルスタックのサポートにつながる第 1 段階です。この実装は、IPv4 トラフィックと IPv6 トラフィックの両方に対する単一の IPSec セキュリティ アソシエーション（SA）ペアの使用をサポートしません。 この機能は、IKEv2 とダイナミック VTI を使用したリモートアクセス VPN に対してのみサポートされます。

機能名	リリース	機能の設定情報
ダイナミック VTI に対するマルチ SA	15.2(1)T Cisco IOS XE Release 3.2S	DVTIは、イニシエータから提案された複数のIPsecセレクタを受け入れることができます。 次のコマンドが導入または変更されました。 **set security-policy limit, set reverse-route.**
スタティック IPsec VTI	12.2(33)SRA 12.2(33)SXH 12.3(7)T 12.3(14)T Cisco IOS XE Release 2.1	IPsec VTI では、IPsec トンネルを終端するためのルーティング可能なインターフェイス タイプと、オーバーレイ ネットワークを形成するためにサイト間の保護を定義する簡単な手段が提供されます。IPsec VTI によって、リモート リンクを保護するためのIPsecの設定が簡素化され、マルチキャストがサポートされ、さらには、ネットワーク管理およびロード バランシングが簡単に実現できるようになります。
トンネル モード自動選択	15.4(2)T Cisco IOS XE リリース 3.12S	トンネル モード自動選択機能は、設定を容易にし、レスポンダの詳細の入手を支援します。この機能は、IKEプロファイルから仮想アクセス インターフェイスが作成されるとすぐに、トンネリング プロトコル（GREまたはIPsec）とトランスポート プロトコル（IPv4 または IPv6）を自動的に仮想テンプレートに適用します。 次のコマンドが導入または変更されました： **virtual-template**

機能名	リリース	機能の設定情報
FlexVPN 混合モード v4 経由 v6 トランスポート	Cisco IOS XE Everest 16.4.1	FlexVPN 混合モード v4 経由 v6 トランスポート機能は、IPsec IPv4 トランスポート経由の IPv6 トラフィックの伝送をサポートします。この実装は、IPv4 トラフィックと IPv6 トラフィックの両方に対する単一の IPSec セキュリティ アソシエーション（SA）ペアの使用をサポートしません。
Cisco 以外のデバイスでの IPsec デュアルスタックのサポート	Cisco IOS XE Cupertino 17.9.x	この機能により、IPv4 を介してトンネリングされる単一の IPsec セキュリティ アソシエーション（SA）を使用して IPv4 トラフィックと IPv6 トラフィックの両方を伝送することが可能になります。IOS XE リリース 17.9.1a 以降、シスコでは、トンネルインターフェイスの入力側がサードパーティの IPsec クライアントで設定されている場合、アクセス制御リストの特定のサブネットをサポートしています。SVTI シングル セキュリティ アソシエーションデュアル スタック機能の導入により、Business-to-Business（B2B）サービスやその他の IoT ビジネスを効率的に管理できるようになりました。

第 158 章

Session Initiation Protocol トリガー VPN

Session Initiation Protocol トリガー VPN（SIP トリガー VPN または VPN SIP）は、サービス プロバイダーが提供するサービスで、Session Initiation Protocol（SIP）を使用して、オンデマンド メディアやピア間のアプリケーション共有に必要な VPN が設定されます。VPN SIP 機能は、2 つの SIP ユーザ エージェントが相互の IP アドレスを解決し、自己署名証明書、サードパーティ証明書、または事前共有キーのフィンガープリントを安全に交換して、IPsec ベース VPN の確立に同意するプロセスを定義します（訳注：NTT東日本及び西日本の提供する「ひかり電話データコネクト」サービスに接続するための機能です）。

サービス プロバイダーは、銀行の ATM や支店など、SIP ベースのサービスを必要とする顧客に VPN SIP サービスを提供します。この VPN SIP サービスは、バックアップ ネットワーク機能の ISDN 接続に代わるものです。プライマリのブロードバンド サービス リンクがダウンした場合、これらの銀行の ATM や支店は VPN SIP サービスを介して中央ヘッドエンドまたはデータ センターに接続します。

サービス プロバイダーの SIP サーバは、VPN SIP サービスの調整に加えて、サービスの使用時間を基にしたサービス料金の請求にも使用されます。

VPN SIP の機能情報

表 *212 : VPN SIP* の機能情報

機能名	リリース	機能情報
Session Initiation Protocol トリガー VPN		VPN SIP は、サービス プロバイダーが提供するサービスで、Session Initiation Protocol（SIP）を使用して、オンデマンド メディアやピア間のアプリケーション共有に必要な VPN が設定されます。 次のコマンドが導入されました：**nat force-encap, show vpn-sip session, show vpn-sip sip, show vpn-sip registration-status, vpn-sip local-number, vpn-sip logging, vpn-sip tunnel source**

VPN SIP の情報

VPN SIP ソリューションのコンポーネント

VPN SIP は、IPSec 静的仮想トンネル インターフェイス（SVTI）を使用します。IPSec SVTI は、IPSec セキュリティ アソシエーション（SA）がトンネル インターフェイスと SVTI ピア間でまったく確立されていない場合でも、アクティブ（UP）な状態のままになります。

VPN SIP ソリューションの 3 つのコンポーネントを次に示します。

- SIP
- VPN SIP
- 暗号（IP Security（IPsec）、インターネットキーエクスチェンジ（IKE）、トンネル保護（TP）、暗号内の Public Key Infrastructure（PKI）モジュール）

Session Initiation Protocol

SIP は、IKE セッションを開始するための名前解決メカニズムとして使用されます。VPN SIP は、SIP サービスを使用して、固定 IP アドレスを持たないホーム ルータまたはスモール ビジネス ルータに VPN 接続を確立します。この接続は、自己署名証明書か事前共有キーを使用し

て実現されます。SIP は、Session Description Protocol（SDP）オファー/アンサー モデルでのメディア セッションに必要な IKE の使用をネゴシエートします。

SIP は静的に設定されています。リモート SIP 番号それぞれに対して、1 つのトンネル インターフェイスを設定する必要があります。

SIP は、VPN SIP サービスの使用料を SIP 番号に基づいて顧客に請求する課金機能もサービス プロバイダーに提供します。SIP 番号に基づく請求は、サービス プロバイダー ネットワーク内で発生するものであり、Cisco VPN SIP ルータのようなエンド デバイスとは無関係です。

VPN SIP のソリューション

VPN SIP は、SIP モジュールと暗号モジュールを連携し、両者の間を抽象化する中央ブロックです。

SIP 番号の背後にあるリモート ネットワークへ向けられたトラフィックがトンネル インターフェイスにルーティングされると、そのピアには IPSEC SA が設定されていないため、IPSec コントロール プレーンはパケット スイッチング パスからのトリガーを受け取ります。このトンネルは VPN SIP 用に設定されているため、IPsec コントロール プレーンは VPN SIP にトリガーを渡します。

（注） その SIP 番号のリモート ネットワークの静的ルートは、このトンネル インターフェイスを指すように設定される必要があります。

VPN SIP サービスがトリガーされると、SIP は SIP 電話番号のペアを使用してコールを設定します。SIP は VPN SIP に着信コールの詳細も渡し、ローカルの自己署名証明書または事前共有キーのローカル アドレスとフィンガープリント情報を使用して、IKE メディア セッションをネゴシエートします。SIP は VPN SIP にリモート アドレスとフィンガープリント情報も渡します。

VPN SIP サービスはトンネル ステータスの更新をリッスンし、SIP を呼び出して、SIP セッションを切断します。VPN SIP サービスは、現在のアクティブなセッションを表示する手段も提供します。

機能一覧

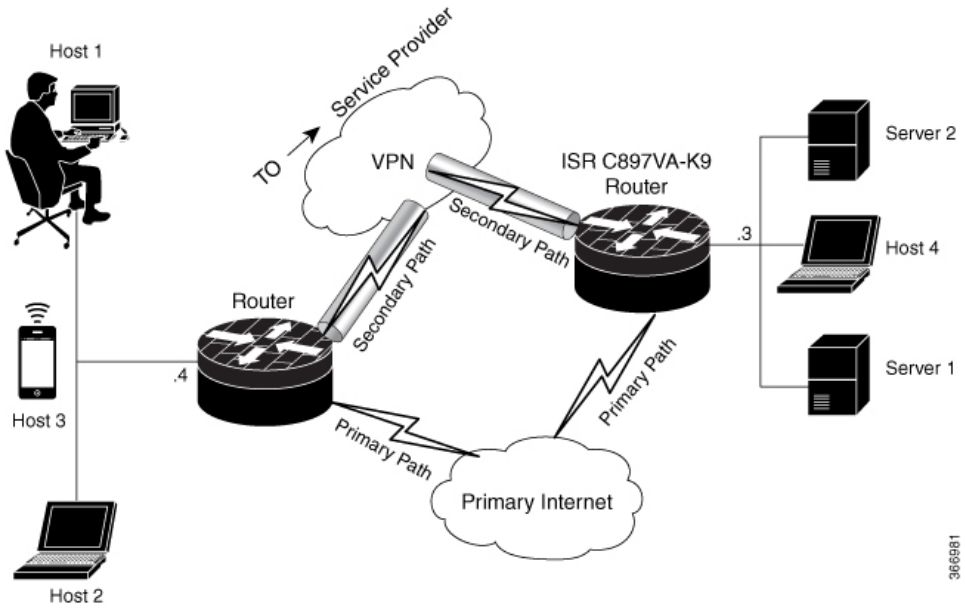
次に、VPN SIP 機能の概略を示します。

- IP SLA は、ルート トラッキングを使用してプライマリ リンクをモニタリングします。プライマリ リンクが失敗すると、IP SLA はこの障害を検出します。
- プライマリ パスが失敗すると、IP SLA はルーターに設定されているメトリックがさらに高いルートにデフォルト ルートを切り替えます。
- 関連するトラフィックがセカンダリ リンクを使用してフローを試みると、SIP は SIP サーバに招待メッセージを送信し、VPN ピア情報を取得します。

- ルータは VPN ピア情報（IP アドレス、ローカル SIP 番号とリモート SIP 番号、IKE ポート、およびフィンガープリント）を受け取って、VPN SIP トンネルを確立します。
- プライマリ パスが復帰すると、IP SLA はプライマリ パスを検出し、ルートが元のパスに戻ります。アイドル タイマーの有効期限が切れると、IPSec は破棄され、SIP コールは切断されます。

次に、VPN SIP ソリューションのトポロジを示します。

図 *82 : VPN SIP* のトポロジ



SIP コール フロー

SIP コール フローは、ローカル ピアでの開始とリモート ピアでのコールの受信に分かれます。

SIP コールの開始

データ プレーン内の SVTI インターフェイスにパケットがルーティングされると、そのアドレスを解決するためにピア SIP 番号に対して SIP コールを発呼する必要があります。これにより、VPN トンネルがアクティブになります。

- ローカル認証タイプが PSK の場合、IKEv2 はピア SIP 番号と一致するキーを検索します。IKEv2 キーリングは、各 SIP ピアの SIP 番号として id_key_id 型（文字列）で設定する必要があります。IKEv2 は検索されたキーのフィンガープリントを計算し、VPN SIP に渡します。
- ローカル認証タイプが自己署名証明書やサード パーティ証明書の場合、IKEv2 は IKEv2 プロファイルに設定されているローカルの証明書のフィンガープリントを計算し、VPN SIP に渡します。

VPN SIP モジュールは、ピアに SIP コールを設定するために SIP と対話します。コールが成功すると、VPN SIP は解決された IP アドレスを SVTI のトンネル接続先として設定し、SVTI に対して VPN トンネルを開始するように要求します。

（注） ワイルドカード キーが必要な場合は、IKEv2 プロファイルで、authentication local pre-share key コマンドと authentication remote pre-share key コマンドを使用します。

リモート ピアでの SIP コールの受信

ピアから SIP コールを受信すると、さまざまな暗号モジュールが以下のように相関して動作します。

- トンネル保護は、VPN SIP モジュールによるトンネルの宛先アドレスの設定に協力します。
- IKEv2 は、ローカル認証タイプ（PSK または PKI）とローカル フィンガープリントを VPN SIP モジュールに返します。ローカル認証タイプが PSK の場合、IKEv2 は対応する SIP 番号と一致するキーを検索します。

（注） IKEv2 は SIP 番号によってのみピアを識別できます。

ピア間で SIP コール ネゴシエーションが行われている間に、各ピアは SDP 上で交換される一意のローカル IKEv2 ポート番号を選択する必要があります。セッションごとに異なるポート番号をサポートするため、VPN SIP モジュールは IP ポート アドレス変換（PAT）をプログラムにより自動的に設定します。PAT は、IKEv2 ポート（4500）と、SDP 上で交換されるポート番号との変換を担います。変換には、セカンダリ リンク上に IP NAT が設定され、ループバック インターフェイスが VPN SIP トンネルの送信元として設定される必要があります。変換の有効期間は、VPN SIP セッションの有効期間で決まります。

SDP オファーとアンサー

RFC 6193 で定義されている、SIP コールでネゴシエートされる SDP オファーとアンサーの例を次に示します。

```
offer SDP
      ...
      m=application 50001 udp ike-esp-udpencap
      c=IN IP4 10.6.6.49
      a=ike-setup:active
      a=fingerprint:SHA-1 \
      b=AS:512
      4A:AD:B9:B1:3F:82:18:3B:54:02:12:DF:3E:5D:49:6B:19:E5:7C:AB
      ...

   answer SDP
      ...
      m=application 50002 udp ike-esp-udpencap
      c=IN IP4 10.6.6.50
```

```
a=ike-setup:passive
a=fingerprint:SHA-1 \
b=AS:512
D2:9F:6F:1E:CD:D3:09:E8:70:65:1A:51:7C:9D:30:4F:21:E4:4A:8E
```

SDP ネゴシエーションの一環として、両方のピアが「b=AS :number」という SDP 属性を使用し、VPN SIP セッションの最大帯域幅のレートをネゴシエートします。SDP に表示されるピア双方の帯域幅が異なる場合、小さい方の値が最大帯域幅として使用される必要があります。「b=AS :number」SDP 属性がオファーかアンサーに含まれていない場合、SIP コールは正常に設定されていません。

ネゴシエートされた最大帯域幅は、プログラムによって設定される出力方向の QoS ポリシーを介して SVTI トンネル インターフェイスに適用されます。静的に設定されたポリシーが既に存在する場合は、プログラムによって設定される QoS ポリシーは適用されず、セッションは失敗します。

SIP コールが完了し、ピアのアドレスが解決されると、VPN SIP は SVTI のトンネル接続先を設定し、トンネルを開始する要求を送信します。

IKEv2 ネゴシエーション

次に、IKEv2 セキュリティ セッション（SA）ネゴシエーションのプロセスを示します。

- セッションの開始前に、IKEv2 は VPN SIP を使用して、そのセッションが VPN SIP セッションであるかどうかを確認します。
- セッションが VPN SIP セッションで、ローカル認証タイプが PSK の場合、IKEv2 はピアの IP アドレスの代わりにピアの SIP 番号を使用して、PSK キー ペアを検索します。
- 自己署名証明書を検証する場合、IKEv2 はその証明書が自己署名されたものかを確認して、証明書を検証します。
  - IKEv2 プロトコルの一部である既存の AUTH ペイロード検証に加えて、IKEv2 は受信した証明書または検索された PSK のハッシュを計算して、IKEv2 が VPN SIP モジュールからクエリする SIP ネゴシエーションのフィンガープリントと比較します。フィンガープリントが一致する場合のみ、IKEv2 はピアの認証が有効であると見なします。一致しない場合、IKEv2 はそのピアが認証に失敗したことを宣言し、VPN セッションを終了します。

VPN SIP ソリューションは、バックアップ VPN でトラフィックをルーティングする必要がなくなったことを、IPSEC アイドル タイマーに基づいて検出します。トラフィックがない時にセッションが切断されるようにするには、IPSec プロファイルにアイドル時間を設定する必要があります。推奨設定は 120 秒です。

VPN SIP と SIP は、連係して SIP コールを切断します。

IPsec アイドル時間の有効期限が切れると、VPN SIP モジュールは IPsec トンネルをダウンするように IKEv2 に通知します。VPN SIP は、SIP モジュールに対して、IKEv2 からの確認を待機せずに SIP コールを切断するように要求します。

SIP コールの切断をピアから受信すると、VPN SIP モジュールは IPsec トンネルをダウンするように IKEv2 に通知し、SIP に対して SIP コールの切断を許可します。

VPN SIP の前提条件

- セキュリティ K9 ライセンスをルータで有効にする必要があります。
- ルータには最低 1 GB のメモリが必要です。
- SIP ユーザ エージェントの SIP 登録要求が成功するには、VPN SIP ルータが SIP レジストラを使用できる必要があります。
- DHCP サーバは、SIP サーバ アドレスを取得するためにオプション 120 と 125 をサポートする必要があります。SIP サーバ アドレスは、SIP セッションの登録と確立に必要になります。
- プライマリ パスがダウンしたときにバックアップ WAN パスが使用される ようにするには、ルーティングを適切に設定しておく必要があります。
- トンネル インターフェイスの最大伝送ユニット（MTU）は、セカンダリ WAN インターフェイスの MTU よりも小さくなければなりません。
- IKEv2 認証に自己署名証明書やサード パーティ証明書を使用する場合は、IP 層のフラグメンテーションを避けるために、VPN SIP ルータに IKEv2 フラグメンテーションを設定します。
- NAT SIP ALG は無効にする必要があります。
- 発信者ID通知サービス（訳注：「ナンバー・ディスプレイ」）が該当の加入者契約において、ネットワーク側で設定されている必要があります。

VPN SIP の制約事項

- VPN SIP と CUBE/SIP ゲートウェイを同一デバイス上で設定することはできません。CUBE ライセンスがデバイス上でアクティブな場合、CUBE のみが有効になります。
- トランスポートとメディア（SIP 登録、SIP シグナリング、および IPv4 トランスポートを介して暗号化された IPv4 パケットの IPv4 トランスポート）では、IPv4 のみがサポートされています。
- NAT の背後にあるピア デバイスを使用した SIP シグナリングはサポートされていません（ICE および STUN はサポートされていません）。
- SIP ネゴシエーションは、グローバル VRF でのみサポートされています。
- プライベート アドレスの割り当て、設定モード交換（CP ペイロード）、ルート交換などのリモート アクセス VPN 機能はサポートされていません。

- VPN SIP セッションでのルーティング プロトコルはサポートされていません。
- Rivest-Shamir-Addleman（RSA）サーバ自己署名証明書のみがサポートされています。
- 認証、認可、およびアカウンティング（AAA）を使用した事前共有キーの検索機能は、サポートされていません。
- IPSec アイドル タイマーは、ipsec-profile コマンドを使用して IPSec プロファイルごとに設定します。アイドル時間は、特定の IPSec プロファイルを使用するすべての VPN SIP セッションで同じです。
- IPSLA のモニタリングに使用されるトラック オブジェクトは、Cisco IOS ソフトウェアで最大 1000 オブジェクトまでに制限されています。1 つのトラック オブジェクトを使用して 1 台のピア ルーターを追跡する場合、1 台の IOS デバイスが処理できる VPN SIP セッションの最大数は、トラック オブジェクトの最大数で決まります。
- Cisco IOS ソフトウェアでは、ローカル SIP 番号は 1 つのみサポートされています。
- 静的に設定されたポリシーが既に存在する場合は、プログラムによって設定される QoS ポリシーは適用されず、セッションは失敗します。SVTI インターフェイス上に静的に設定された QoS ポリシーは、すべて削除してください。
- シスコ以外のベンダーによって実装された VPN SIP との相互運用性は、サポートされていません。
- VPN-SIP トンネルに付加されたポリシーマップに含まれるクラスポリシーについては、プライオリティキューイングとクラスベース重み付け均等化キューイング（CBWFQ）のみがサポートされます。
- CBWFQ の設定でサポートされているのは、`bandwidth percent` *`percent`* コマンドのみです。VPN-SIP セッションの帯域幅はピアルータとのネゴシエーションによって変わるため、`bandwidth` *`bandwidth`* コマンドはサポートされていません。
- VPN-SIP の設定は IPv6 ではサポートされていません。
- VPN-SIP の設定は、自律モードでのみサポートされます。
- 参照、フォークなどの複雑な SIP コールシナリオは、VPN-SIP の設定ではサポートされていません。

VPN SIP の設定方法

VPN SIP の設定

VPN SIP を設定する手順は次のとおりです。

1. サードパーティ証明書、自己署名証明書、または事前共有キーを使用してトンネル認証を設定します。

1. 証明書を使用するトンネル認証

   顧客のネットワーク内にある証明機関（CA）サーバから証明書を取得するためのトラストポイントを設定します。これはトンネル認証で必要です。次の設定を使用します。

```
peer1(config)# crypto pki trustpoint CA
 enrollment url http://10.45.18.132/
 serial-number none
 subject-name CN=peer2
 revocation-check crl
 rsakeypair peer2

peer2(config)# crypto pki authenticate CA
Certificate has the following attributes:
       Fingerprint MD5: F38A9B4C 2D80490C F8E7581B BABE7CBD
      Fingerprint SHA1: 4907CC36 B1957258 5DFE23B2 649E7DDA 99BDB7C3
% Do you accept this certificate? [yes/no]: yes
Trustpoint CA certificate accepted.

peer2(config)#crypto pki enroll CA
%
% Start certificate enrollment ..
% Create a challenge password. You will need to verbally provide this
   password to the CA Administrator in order to revoke your certificate.
   For security reasons your password will not be saved in the configuration.
   Please make a note of it.
Password:
Re-enter password:
% The subject name in the certificate will include: CN=peer2
% The subject name in the certificate will include: peer2
% Include an IP address in the subject name? [no]:
Request certificate from CA? [yes/no]: yes
% Certificate request sent to Certificate Authority
% The 'show crypto pki certificate verbose CA' command will show the fingerprint.
Certificate map for Trustpoint
crypto pki certificate map data 1
issuer-name co cn = orange
```

2. 自己署名証明書を使用するトンネル認証

   自己署名証明書を使用して認証を行う場合、そのデバイス上に自己署名証明書を生成する PKI トラストポイントを設定します。次の設定を使用します。

```
peer4(config)#crypto pki trustpoint Self
    enrollment selfsigned
    revocation-check none
    rsakeypair myRSA
    exit
crypto pki enroll Self

Do you want to continue generating a new Self Signed Certificate? [yes/no]: yes
% Include the router serial number in the subject name? [yes/no]: yes
% Include an IP address in the subject name? [no]: no
Generate Self Signed Router Certificate? [yes/no]: yes

Router Self Signed Certificate successfully created
```

3. 事前共有キーを使用してトンネル認証を設定します。

```
crypto ikev2 keyring keys
peer peer1
```

```
identity key-id 1234
pre-shared-key key123
```

2. 1. 証明書の IKEv2 プロファイルを設定します。

```
crypto ikev2 profile IPROF
match certificate data
identity local key-id 5678
authentication remote rsa-sig
authentication local rsa-sig
keyring local keys
pki trustpoint self
nat force-encap
```

2. 事前共有キーの IKEv2 プロファイルを設定します。

```
crypto ikev2 profile IPROF
match identity remote any
identity local key-id 5678
authentication remote pre-share
authentication local pre-share
keyring local keys
nat force-encap
```

（注） IKEv2 SA を設定するには、両方のピアで **nat force-encap** コマンドを設定する必要があります。UDP のカプセル化が SDP でネゴシエートされるので、IKEv2 はポート 4500 で開始し続行される必要があります。

3. IPsec プロファイルを設定します。

```
crypto ipsec profile IPROF
set security-association idle-time 2000
```

4. LAN 側インタ フェースを設定します。

```
interface Vlan101
         ip address 10.3.3.3 255.255.255.0
         no shutdown
!
     interface GigabitEthernet2
         switchport access vlan 101
         no ip address
```

5. ループバック インターフェイスを設定します。

   ループバック インターフェイスは、セカンダリ VPN トンネルの送信元インターフェイスとして使用されます。

```
interface loopback 1
    ip address 10.11.1.1 255.0.0.0
    ip nat inside
```

6. セカンダリ インターフェイスを設定します。

（注） セカンダリ インターフェイスは、IP アドレス、SIP サーバ アドレス、およびベンダー固有の情報を DHCP 経由で受信するように設定する必要があります。

```
interface GigabitEthernet8
     ip dhcp client request sip-server-address
     ip dhcp client request vendor-identifying-specific
     ip address dhcp
    ip nat outside
```

7. トンネル インターフェイスを設定します。

```
interface Tunnel1
     ip address 10.3.2.1 255.255.255.255
     load-interval 30
     tunnel source Loopback1
     tunnel mode ipsec ipv4
     tunnel destination dynamic
     tunnel protection ipsec profile IPROF ikev2-profile IPROF
     vpn-sip local-number 5678 remote-number 1234 bandwidth 1000
```

vpn-sip local-number *local-number* **remote-number** *remote-number* **bandwidth** *bw-number* コマンドを使用して、SVTI インターフェイスに VPN-SIP を設定します。帯域幅とは、このピアとネゴシエートされる必要のある最大データ伝送速度のことで、ネゴシエートされた値がトンネル インターフェイスに設定されます。使用できる値は 64 Kbps、128 Kbps、256 Kbps、512 Kbps、および 1000 Kbps です。

VPN SIP 用に SVTI を設定した後で、トンネル モード、トンネルの接続先、トンネルの送信元、およびトンネル保護を変更することはできません。モード、送信元、接続先、またはトンネル保護を変更するには、その SVTI インターフェイスから VPN SIP 設定を削除する必要があります。

8. 接続先ネットワークにスタティックルートを追加します。

メトリックが高いセカンダリ ルートを追加します。

```
ip route 192.168.10.0 255.255.255.0 Tunnel0 track 1
ip route 192.168.10.0 255.255.255.0 Tunnel1 254
```

9. IP SLA を設定します。

```
ip sla 1
         icmp-echo 10.11.11.1
         threshold 500
         timeout 500
         frequency 2
        ip sla schedule 1 life forever start-time now
```

10. ルート トラッキングを設定します。

```
track 1 ip sla 1 reachability
```

11. VPN SIP を有効化します。

```
vpn-sip enable
vpn-sip local-number 5678 address ipv4 GigabitEthernet8
vpn-sip tunnel source Loopback1
vpn-sip logging
```

VPN SIP を設定するには、ローカルの SIP 番号とローカル アドレスを設定する必要があります。**vpn-sip local-number** *SIP-number* **address ipv4** *WAN-interface-name* コマンドを使用して、SIP コールに使用するローカル SIP 番号と、関連づけられた IPv4 アドレスを設定します。

（注） IPv4 アドレスのみ設定できます。暗号モジュールはデュアル スタックをサポートしていません。

- バックアップ WAN インターフェイスのアドレスは、DHCP 割り当てに基づいて変わることがあります。

プライマリ WAN インタ フェースが機能している場合、VPN SIP トンネルの接続先はバックアップ WAN インターフェイスに設定され、トンネル インターフェイスが有効になります。トラフィックがトンネルインターフェイスにルーティングされる場合、接続先は SIP ネゴシエーションの SDP から学習されるピアの IP アドレスに設定されます。プライマリ WAN インターフェイスが失敗した場合、バック ルートがアクティブ化されていれば、パケットはバックアップを介して sVTI にルーティングされます。

（注） ループバック インターフェイスのアドレスにはルーティング不可能な未使用のアドレスを使用し、そのループバック インターフェイスは他のいかなる目的にも使用しないようにお勧めします。ループバック インターフェイスを設定すると、VPN SIP はこのインターフェイスに対するすべての更新プログラムをリッスンし、それらをブロックします。**vpn-sip logging** コマンドにより、セッションの開始、終了、障害発生などのイベントに関する VPN-SIP モジュールのシステムロギングが有効になります。

ローカル ルータの VPN SIP の確認

登録スターテスの確認

```
Peer1# show vpn-sip registration-status
 SIP registration of local number 0388881001 : registered 10.6.6.50
```

SIP レジストラの確認

```
Peer1#show vpn-sip sip registrar

Line          destination      expires(sec)  contact   transport     call-id
=============================================================================================
0388881001    example.com         2359        10.6.6.50  UDP
3176F988-9EAA11E7-8002AFA0-8EF41435
```

VPN SIP ステータスの確認

```
Peer1#show vpn-sip session detail
VPN-SIP session current status
```

```
Interface: Tunnel1
   Session status: SESSION_UP (I)
   Uptime        : 00:00:42
   Remote number : 0388881001 =====> This is the Remote Router's SIP number
   Local number  : 0388882001 =====> Local router's SIP number
   Remote address:port: 10.6.6.49:50002
   Local address:port : 10.6.6.50:50001
   Crypto conn handle: 0x8000017D
   SIP Handle        : 0x800000C7
   SIP callID        : 1554
   Configured/Negotiated bandwidth: 64/64 kbps
```

暗号化セッションの確認

```
Peer1# show crypto session detail
Crypto session current status
Code: C - IKE Configuration mode, D - Dead Peer Detection
K - Keepalives, N - NAT-traversal, T - cTCP encapsulation
X - IKE Extended Authentication, F - IKE Fragmentation
R - IKE Auto Reconnect, U - IKE Dynamic Route Update
S - SIP Vpn-sip

Interface: Tunnel1
Profile: IPROF
Uptime: 00:03:53
Session status: UP-ACTIVE
Peer: 10.6.6.49 port 4500 fvrf: (none) ivrf: (none)
      Phase1_id: 10.6.6.49
      Desc: (none)
  Session ID: 43
  IKEv2 SA: local 10.11.1.1/4500 remote 10.6.6.49/50002 Active
          Capabilities:S connid:1 lifetime:23:56:07 ====> Capabilities:S indicates this
 is a  SIP VPN_SIP Session
  IPSEC FLOW: permit ip 0.0.0.0/0.0.0.0 0.0.0.0/0.0.0.0
        Active SAs: 2, origin: crypto map
        Inbound:  #pkts dec'ed 6 drop 0 life (KB/Sec) 4222536/3366
        Outbound: #pkts enc'ed 4 drop 0 life (KB/Sec) 4222537/3366
```

IP NAT 変換の確認

```
Peer1#sh ip nat translations
Pro Inside global      Inside local       Outside local      Outside global
udp 2.2.2.2:4500       10.6.6.50:50001    10.6.6.49:50002    10.6.6.49:50002
```

DHCP SIP 設定の確認

```
Peer9#show vpn-sip sip dhcp
SIP DHCP Info

SIP-DHCP interface:  GigabitEthernet8

SIP server address:
Domain name:         dns:example.com
```

VPN SIP の設定例

認証用自己署名証明書の使用

認証用の自己署名証明書を使用して VPN SIP を設定する例を次に示します。VPN SIP では、イニシエータとレスポンダのロールに違いはありません。ピア ノード上の設定は、変更されたローカルの SIP 番号と同一になります。

```
// Self-signed certificate
crypto pki trustpoint selfCert
  rsakeypair myRSA
  enrollment selfsigned
  revocation-check none
!
crypto ikev2 profile vpn-sip-profile
 match identity remote any
 authentication local rsa-sig
 authentication remote rsa-sig
 pki trustpoint selfCert // Use same self-signed trustpoint for sign and verify
 nat force-encap
!
crypto ipsec profile vpn-sip-ipsec
 set security-association idle-time 120
!
vpn-sip enable
vpn-sip local-number 0388883001 address ipv4 GigabitEthernet1
vpn-sip tunnel source Loopback11
vpn-sip logging
!
// one tunnel per peer - configuration is for peer with a SIP-number of 0388884001
int tunnel0
 ip unnumbered loopback 0
 tunnel source loopback11
 tunnel mode ipsec ipv4
 tunnel destination dynamic
 tunnel protection ipsec profile vpn-sip-ipsec ikev2-profile vpn-sip-profile
 vpn-sip local-number 0388883001 remote-number 0388884001 bandwidth 1000
!
// ip unnumbered of tunnel interfaces
int loopback 0
  ip address 10.21.1.1 255.255.255.255
!
int loopback11
ip address 10.9.9.9 255.255.255.255
ip nat inside
!
// one tunnel per peer - this is for peer with SIP-number 0388885001
int tunnel1
 ip unnumbered loopback 0
 tunnel source loopback11
 tunnel mode ipsec ipv4
 tunnel destination dynamic
 tunnel protection ipsec profile vpn-sip-ipsec ikev2-profile iprof
 vpn-sip sip-local 0388883001 sip-remote 0388885001 bandwidth 1000
!
interface GigabitEthernet8
 ip dhcp client request sip-server-address
 ip dhcp client request vendor-identifying-specific
 ip address dhcp
```

```
ip nat outside


// backup routes configured with higher AD so that these routes will be activated only
when primary path goes down. AD need to be chosen to be greater than that of primary
route.
ip route 10.0.0.0 255.0.0.0 tunnel 0 250
ip route 10.1.0.0 255.0.0.0 tunnel 0 250
ip route 10.2.0.0 255.0.0.0 tunnel 0 250
ip route 10.3.0.0 255.0.0.0 tunnel 0 250
```

VPN SIP の DHCP の設定

ホームゲートウェイ配下での接続

Cisco IOS XE リリース 17.11.1a から、ホームゲートウェイ（HGW）の背後に VPN-SIP 対応ルータをインストールできます。このインストールでは、HGW は、固定電話番号の代わりに Dynamic Host Configuration Protocol（DHCP）を介してトンネルインターフェイスに内線番号を割り当てます。これにより、ネットワーク上のデータと音声を集約できます。これは、アナログデータとデジタルデータの両方で同じ物理加入者回線を共有する必要があるシナリオで役立ちます。

さらに、HGW のネットワーク仕様に準拠するために、VPN-SIP の DHCP には、vendor-class-data DHCP オプションを介して、HGW ネットワークへ接続する WAN 側インターフェイスの MAC アドレスが必要です。この設定では、デバイスは DHCP 要求の vendor-class-data オプションを介して、自身の WAN インターフェイスの MAC アドレスをホームゲートウェイネットワークに通知します。

サポートされている PID とファームウェア

次の表は、テストされた HGW の PID とファームウェアバージョンを示しています。シスコは、お客様の拠点に設置されている HGW または HGW の操作についてはサポートを提供していません。（訳注：ホームゲートウェイはNTTの資産としてお客様宅内に設置されるものであるためです）この機能を使用する前に、環境を確認することをお勧めします。

HGW PID	ファームウェア バージョン
RT-400NE	8.06
RT-400MI	09.00.0015
RT-400KI	08.00.0040
RT-500MI	08.00.0004
RT-500KI	08.00.0020
RX-600MI	01.00.0001
RX-600KI	01.00.0001

HGW PID	ファームウェア バージョン
OG410Xi	2.32
OG410Xa	2.32

ホームゲートウェイ配下での接続

DHCP ローカル番号を設定すると、デバイスは DHCP 応答を受信するまで SIP 登録を遅延させます。デバイスは、DHCP サーバーが内線番号を提供することを想定しています。この内線番号は、SIP サーバーへの登録に使用されます。登録が成功し、デバイスが SIP サーバーとのセッションを開始すると、200 OK 応答を通じて、内線番号、外線番号、およびその他の使用可能な番号を受信します。

（注） 外線番号は、ルータをグローバルに識別する番号です。この外線番号は、データ接続を確立するためにも必要です。

DHCP 拡張により、データ接続には SIP シグナリングチャンネルと IPsec データ接続の 2 つのチャンネルがあります。データパケットにトンネル保護が必要な場合、SIP コールが開始されます。

VPN-SIP の DHCP を設定するには、次の手順を実行します。

DHCP クライアントの有効化

手順の概要

1. **enable**
2. **configure terminal**
3. **interface type number**
4. **ip dhcp client request sip-server-address**
5. **ip dhcp client request vendor-identifying-specific**
6. **ip address dhcp**
7. **ip dhcp client vendor-class mac-address**
8. **ip nat outside**
9. **exit**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。プロンプトが表示されたらパスワードを入力します。

	コマンドまたはアクション	目的
ステップ 2	**configure terminal** 例： `Router# configure terminal`	グローバル設定モードを開始します。
ステップ 3	**interface type number** 例： `Router(config)# interface gigabitethernet 0/0`	インターフェイスタイプを設定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	**ip dhcp client request sip-server-address** 例： `Router(config-if)# ip dhcp client request sip-server-address`	DHCP サーバーに SIP サーバーアドレスを要求するように DHCP クライアントを設定します。
ステップ 5	**ip dhcp client request vendor-identifying-specific** 例： `Router(config-if)# ip dhcp client request vendor-identifying-specific`	DHCP サーバーにベンダー固有の情報を要求するように DHCP クライアントを設定します。
ステップ 6	**ip address dhcp** 例： `Router(config-if)# ip address dhcp`	インターフェイス上で DHCP から IP アドレスを取得します。
ステップ 7	**ip dhcp client vendor-class mac-address** 例： `Router(config-if)# ip dhcp client vendor-class mac-address`	HGW の DHCP 仕様に準拠します。
ステップ 8	**ip nat outside** 例： `Router(config-if)# ip nat outside`	外部ネットワークにインターフェイスを接続します。
ステップ 9	**exit** 例： `Router(config-if)# end`	インターフェイス コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

DHCP クライアントを有効にする設定例

次に、DHCP クライアントを有効にするためのサンプルコードを示します。

```
interface GigabitEthernet 0/0/0
 ip dhcp client request sip-server-address
 ip dhcp client request vendor-identifying-specific
 ip address dhcp
 ip dhcp client vendor-class mac-address
 ip nat outside
```

トンネリング認証の設定

サードパーティ証明書、自己署名証明書、または事前共有キー（PSK）を使用してトンネル認証を設定できます。トンネル認証を設定するには、次のいずれかのタスクを実行します。

証明書を使用したトンネル認証の設定

顧客のネットワーク内にある証明機関（CA）サーバから証明書を取得するためのトラストポイントを設定します。これはトンネル認証で必要です。

手順の概要

1. **enable**
2. **configure terminal**
3. **crypto pki trustpoint** name
4. **enrollment url** `url`
5. **serial-number**
6. **subject-name** `[subject-name]`
7. **revocation-check crl**
8. **rsakeypair**
9. **crypto pki authenticate CA**
10. **crypto pki enroll CA** `name`
11. **exit**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードを有効にします。プロンプトが表示されたらパスワードを入力します。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	グローバル設定モードを開始します。
ステップ 3	**crypto pki trustpoint** name 例： `Router(config)# crypto pki trustpoint CA`	トラストポイントおよび設定された名前を指定して、CA トラストポイントコンフィギュレーションモードを開始します。
ステップ 4	**enrollment url** `url` 例： `Router(ca-trustpoint)# enrollment url http://10.45.18.132/`	ルータが証明書要求を送信する CA の URL を指定します。

	コマンドまたはアクション	目的
ステップ 5	**serial-number** 例： `Router(ca-trustpoint)# serial-number`	**none** キーワードを指定した場合を除き、証明書要求でルータのシリアル番号を指定します。 証明書要求にシリアル番号を含めない場合は、**none** キーワードを使用します。
ステップ 6	**subject-name [subject-name]** 例： `Router(ca-trustpoint)# subject-name CN=peer2`	証明書要求で使用される要求された情報カテゴリ名を指定します。情報カテゴリ名が指定されていない場合は、デフォルトの情報カテゴリ名である完全修飾ドメイン名（FQDN）が使用されます。
ステップ 7	**revocation-check crl** 例： `Router(ca-trustpoint)# revocation-check crl`	証明書失効リスト（CRL）メカニズムを使用して証明書の有効性を確認します。
ステップ 8	**rsakeypair** 例： `Router (ca-trustoint)# rsakeypair peer2`	トラストポイントのキーペアを提供します。
ステップ 9	**crypto pki authenticate CA** 例： `Router(config)# crypto pki authenticate CA`	CA の公開キーが含まれている CA の自己署名証明書を取得して、CA をルータに対して認証します。
ステップ 10	**crypto pki enroll CA name** 例： `Router(config)# crypto pki enroll CA`	証明書要求を生成し、コピーして証明書サーバーに貼り付けるために要求を表示します。 証明書要求にルータの FQDN および IP アドレスを含めるかどうかなどの登録情報を求められます。コンソール端末に証明書要求を表示するかについても選択できます。
ステップ 11	**exit** 例： `Router(config-if)# exit`	インターフェイス コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

例：証明書を使用したトンネル認証の設定

これは、証明書を使用してトンネル認証を設定するためのサンプルコードです。

```
peer1(config)# crypto pki trustpoint CA
 enrollment url http://10.45.18.132/
 serial-number none
 subject-name CN=peer2
 revocation-check crl
 rsakeypair peer2

peer2(config)# crypto pki authenticate CA
Certificate has the following attributes:
```

```
Fingerprint MD5: F38A9B4C 2D80490C F8E7581B BABE7CBD
Fingerprint SHA1: 4907CC36 B1957258 5DFE23B2 649E7DDA 99BDB7C3
% Do you accept this certificate? [yes/no]: yes
Trustpoint CA certificate accepted.

peer2(config)#crypto pki enroll CA
% Start certificate enrollment ..
% Create a challenge password. You will need to verbally provide this password to the
CA Administrator in order to revoke your certificate.
For security reasons your password will not be saved in the configuration. Please make
a note of it.
Password:
Re-enter password:
% The subject name in the certificate will include: CN=peer2
% The subject name in the certificate will include: peer2
% Include an IP address in the subject name? [no]:
Request certificate from CA? [yes/no]: yes
% Certificate request sent to Certificate Authority
% The 'show crypto pki certificate verbose CA' command will show the fingerprint.
Certificate map for Trustpoint
crypto pki certificate map data 1
issuer-name co cn = orange
```

自己署名証明書を使用したトンネル認証の設定

自己署名証明書を使用してトンネル認証を設定するには、**crypto pki trustpoint self** コマンドを実行します。このコマンドにより、デバイスで自己署名証明書を生成するためのPKIトラストポイントを設定できます。

```
Router(config)# crypto pki trustpoint self
enrollment self signed
revocation-check none
rsakeypair myRSA
exit

crypto pki enroll self
Do you want to continue generating a new Self Signed Certificate? [yes/no]: yes
% Include the router serial number in the subject name? [yes/no]: yes
% Include an IP address in the subject name? [no]: no
Generate Self Signed Router Certificate? [yes/no]: yes
Router Self Signed Certificate successfully created
```

事前共有キーを使用したトンネル認証の設定

手順の概要

1. **enable**
2. **configure terminal**
3. **crypto ikev2 keyring keyring-name**
4. **peer name**
5. **address {ipv4-address [mask] | ipv6-addressprefix}**
6. **identity {address { ipv4-address | ipv6-address} | fqdn name | email email-id | key-id key-id}**
7. **pre-shared-key {local| remote} {0| 6| line}**
8. **exit**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードを有効にします。プロンプトが表示されたらパスワードを入力します。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	グローバル設定モードを開始します。
ステップ 3	**crypto ikev2 keyring keyring-name** 例： `Router(config)# crypto ikev2 keyring kyr1`	IKEv2 キーリングを定義し、IKEv2 キーリング コンフィギュレーション モードを開始します。
ステップ 4	**peer name** 例： `Router(config-ikev2-keyring)# peer peer1`	ピアまたはピアグループを定義し、IKEv2 キーリング コンフィギュレーション モードを開始します。
ステップ 5	**address {ipv4-address [mask] | ipv6-addressprefix}** 例： `Router(config-ikev2-keyring-peer)# address 10.0.0.1 255.255.255.0`	IP アドレスまたはピアの範囲を指定します。この IP アドレスが IKE エンドポイント アドレスであり、ID アドレスとは別個のものです。
ステップ 6	**identity {address { ipv4-address | ipv6-address} | fqdn name | email email-id | key-id key-id}** 例： `Router(config-ikev2-keyring-peer)# identity key-id 1234`	次の ID を使用して IKEv2 ピアを特定します。 • 電子メール • [FQDN] • IPv4 アドレス • キー ID ID は IKEv2 レスポンダ上のキー ルックアップにしか使用できません。
ステップ 7	**pre-shared-key {local| remote} {0| 6| line}** 例： `Router(config-ikev2-keyring-peer)# pre-shared-key key123`	ピアの PSK を指定します。**local** キーワードまたは **remote** キーワードを入力し、非対称 PSK を指定します。デフォルトでは、PSK は対称です。
ステップ 8	**exit** 例： `Router(config-ikev2-keyring-peer)# end`	キーリング ピア コンフィギュレーション モードを終了して、コンフィギュレーション モードに戻ります。

例：事前共有キーを使用したトンネル認証の設定

これは、事前共有キーを使用してトンネル認証を設定するためのサンプルコードです

```
crypto ikev2 keyring keys
 peer p1
 identity key-id 0388881001
 pre-shared-key cisco
 !
 peer p2
 identity key-id 0388882002
 pre-shared-key cisco
!
crypto ikev2 keyring HUB-KEY
peer SPOKES
address 0.0.0.0 0.0.0.0
pre-shared-key cisco
```

証明書の IKEv2 プロファイルの設定

IKEv2 プロファイルの証明書を設定するには、**crypto ikev2 profile IPROF** コマンドを実行します。次に、証明書の IKEv2 プロファイルを設定するためのサンプルコードを示します。

```
Router(config)# crypto ikev2 profile IPROF-psk
 match identity remote any
 identity local key-id dhcp
 authentication remote pre-share
 authentication local pre-share
 keyring local keys
 nat force-encap
```

IPsec プロファイルの設定

IPSec プロファイルを設定するには、**crypto ipsec profile IPROF** コマンドを実行します。次に、IPSec プロファイルを設定するためのサンプルコードを示します。

```
Router(config)# crypto ipsec profile IPROF
 set security-association idle-time 300
```

VPN SIP を有効化します。

VPN-SIP 機能を有効にするには、**vpn-sip enable** コマンドを実行します。次に、VPN-SIP を有効にするサンプルコードを示します。

```
Router(config)# vpn-sip enable
vpn-sip local-number dhcp address ipv4 GigabitEthernet0/0/0
vpn-sip tunnel source Loopback1
```

LAN 側インターフェイスの設定

LAN 側のインターフェースを設定するには、**interface VLAN <interface>** コマンドを実行します。次に、LAN 側インターフェイスを設定するためのサンプルコードを示します。

```
Router(config)# interface GigabitEthernet2
ip address 192.0.2.3 255.255.255.0
no shutdown
```

ループバック インターフェイスの設定

ループバック インターフェイスを設定するには、**interface loopback <number>** コマンドを実行します。次に、ループバック インターフェイスを設定するためのサンプルコードを示します。

```
Router(config)# interface Loopback1
 ip address 10.255.255.3 255.255.255.0
 ip nat inside
```

トンネルインターフェイスの設定

手順の概要

1. **enable**
2. **configure terminal**
3. **interface tunnel** *number*
4. **tunnel source** {*ip-address* | *interface-type number*}
5. **tunnel destination**
6. **tunnel protection IPsec profile** *name*
7. **vpn-sip local-number dhcp remote-number bandwidth**
8. **exit**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードを有効にします。プロンプトが表示されたらパスワードを入力します。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	グローバル設定モードを開始します。
ステップ 3	**interface tunnel** *number* 例： `Router(config)# interface tunnel1`	トンネルインターフェイスを設定し、インターフェイス コンフィギュレーション モードを開始します。*number* 引数には、作成または設定するトンネル インターフェイスの数を指定します。作成可能なトンネル インターフェイスの数に制限はありません。
ステップ 4	**tunnel source** {*ip-address* | *interface-type number*} 例：	トンネルインターフェイスの送信元 IP アドレスまたは送信元インターフェイスタイプ番号を設定します。この手順では、**tunnel protection IPsec profile** コ

	コマンドまたはアクション	目的
	`Router(config-if)# ip address 12.12.12.12 255.255.255.255` `tunnel source Loopback1`	マンドも使用するため、トンネル送信元として、IPアドレスではなくインターフェイスを指定する必要があります。
ステップ 5	**tunnel destination** 例： `Router(config-if)# tunnel destination destination dynamic`	トンネルの宛先を指定します。
ステップ 6	**tunnel protection IPsec profile** *name* 例： `Router(config-if)# tunnel protection ipsec profile IPROF ikev2-profile IPROF-psk`	トンネル インターフェイスを IPsec プロファイルに関連付けます。*name* 引数には、IPsec プロファイルの名前を指定します。この値は、**crypto IPsec profile** <*name*> コマンドで指定した値と同じである必要があります。
ステップ 7	**vpn-sip local-number dhcp remote-number bandwidth** 例： `Router(config-if)# vpn-sip local-number dhcp remote-number 0388881001 bandwidth 1000`	VPN-SIP のインターフェイスを設定します。帯域幅とは、このピアとネゴシエートされる必要のある最大データ伝送速度のことで、ネゴシエートされた値がトンネルインターフェイスに設定されます。使用できる値は、64 kbps、128 kbps、256 kbps、512 kbps、および 1000 kbps です。 （注） VPN SIP 用にインターフェイスを設定した後で、トンネルモード、トンネルの接続先、トンネルの送信元、およびトンネル保護を変更することはできません。モード、送信元、接続先、またはトンネル保護を変更するには、そのインターフェイスから VPN SIP 設定を削除する必要があります。
ステップ 8	**exit** 例： `Router(config-if)# exit`	インターフェイス コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

例：トンネルインターフェイスの設定

これは、トンネルインターフェイスを設定するためのサンプルコードです。

```
Router(config)# interface Tunnel1
 ip address 10.12.12.12 255.255.255.255
 tunnel source Loopback1
 tunnel mode ipsec ipv4
 tunnel destination dynamic
 tunnel protection ipsec profile IPROF ikev2-profile IPROF-psk
 vpn-sip local-number dhcp remote-number 0388881001 bandwidth 1000
!
```

```
interface Tunnel10
 ip address 10.20.20.21 255.255.255.255
 tunnel source Loopback1
 tunnel mode ipsec ipv4
 tunnel destination dynamic
 tunnel protection ipsec profile IPROF ikev2-profile IPROF-psk
 vpn-sip local-number dhcp remote-number 0388882002 bandwidth 100
```

VPN-SIP での DHCP 設定の確認

次の show コマンドの出力は、VPN-SIP の DHCP が HGW の背後にある Cisco IOS XE ルータで正常に設定されているかどうかを確認する方法を示しています。

```
Router_behind_HGW# show vpn-sip sip dhcp
SIP DHCP Info
SIP-DHCP interface:  GigabitEthernet 0/0/0
SIP server address:  ipv4:192.168.1.1
Domain name:         dns:ntt-east.ne.jp

Router_behind_HGW# show vpn-sip registration-status
  SIP registration of local number dhcp : registered 192.168.1.200
  Local dynamic number via dhcp[3], via SIP[0398765432]

Router_behind_HGW# show vpn-sip sip registrar
Line          destination      expires(sec)  contact
transport     call-id
============================================================
3             ntt-east.ne.jp   2439          192.168.1.20
UDP           FFFFFFFFCCE6C415-5D8611ED-FFFFFFFF810AE9D4-FFFFFFFFD

Router_behind_HGW# show vpn-sip session detail
VPN-SIP session current status
Interface: Tunnel0
    Session status: SESSION_UP (I)
    Uptime        : 00:00:37
    Remote number : 0387654321
    Local number  : dhcp
    Remote address:port: aaa.bbb.ccc.ddd:27129
    Local address:port : 192.168.1.200:50026
    Crypto conn handle: 0x4000003D
    SIP Handle        : 0x4000001B
    SIP callID        : 301
    Configured/Negotiated bandwidth: 256/256 kbps
    Applied service policy:

Router_behind_HGW# show crypto session
Crypto session current status
Interface: Tunnel0
Profile: IPROF
Session status: UP-ACTIVE
Peer: aaa.bbb.ccc.ddd port 27129
   Session ID: 26
   IKEv2 SA: local 10.255.255.1/4500 remote aaa.bbb.ccc.ddd/27129 Active
   IPSEC FLOW: permit ip   0.0.0.0/0.0.0.0 0.0.0.0/0.0.0.0
   Active SAs: 2, origin: crypto map

Router_behind_HGW# show crypto ikev2 sa
  IPv4 Crypto IKEv2  SA

Tunnel-id Local                 Remote                fvrf/ivrf
   Status
1         10.255.255.1/4500     aaa.bbb.ccc.ddd/27129  none/none
    READY
       Encr: AES-CBC, keysize: 256, PRF: SHA512, Hash: SHA512, DH
```

```
       Grp:19, Auth sign: PSK, Auth verify: PSK
       Life/Active Time: 86400/86 sec
       CE id: 1022, Session-id: 22
       Local spi: 59E8EED28441BC32
       Remote spi: B5487716A19873BE
       IPv6 Crypto IKEv2  SA

Router_behind_HGW# show crypto ipsec sa

interface: Tunnel0
Crypto map tag: Tunnel0-head-0, local addr 10.255.255.1
protected vrf: (none)
local  ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
remote ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
current_peer aaa.bbb.ccc.ddd port 27129
PERMIT, flags={origin_is_acl,}
     #pkts encaps: 4, #pkts encrypt: 4, #pkts digest: 4
     #pkts decaps: 4, #pkts decrypt: 4, #pkts verify: 4
     #pkts compressed: 0, #pkts decompressed: 0
     #pkts not compressed: 0, #pkts compr. failed: 0
     #pkts not decompressed: 0, #pkts decompress failed: 0
     #send errors 0, #recv errors 0

local crypto endpt.: 10.255.255.1, remote crypto endpt.:
aaa.bbb.ccc.ddd
plaintext mtu 1422, path mtu 1500, ip mtu 1500, ip mtu idb
GigabitEthernet0/0/0
current outbound spi: 0xE0F51D37(3774160183)
PFS (Y/N): N, DH group: none

inbound esp sas:
      spi: 0x493D896(76798102)
      transform: esp-aes esp-sha-hmac ,
      in use settings ={Tunnel UDP-Encaps, }
      conn id: 2044, flow_id: ESG:44, sibling_flags FFFFFFFF80004048,
crypto map: Tunnel0-head-0, initiator : True
       sa timing: remaining key lifetime (k/sec): (4607999/3509)
       IV size: 16 bytes
       replay detection support: Y
       Status: ACTIVE(ACTIVE)

      inbound ah sas:

      inbound pcp sas:

      outbound esp sas:
       spi: 0xE0F51D37(3774160183)
         transform: esp-aes esp-sha-hmac ,
         in use settings ={Tunnel UDP-Encaps, }
         conn id: 2043, flow_id: ESG:43, sibling_flags FFFFFFFF80004048,
crypto map: Tunnel0-head-0, initiator : True
         sa timing: remaining key lifetime (k/sec): (4607999/3509)
         IV size: 16 bytes
         replay detection support: Y
         Status: ACTIVE(ACTIVE)
      outbound ah sas:
      outbound pcp sas:


Router_behind_HGW# show ip nat translations
Pro  Inside global         Inside local          Outside local
Outside global
udp  192.168.1.200:50269   10.255.255.1:4500     aaa.bbb.ccc.ddd:23060
aaa.bbb.ccc.ddd:23060
Total number of translations: 1
```

VPN SIP のトラブルシューティング

show コマンドの出力にトンネル インターフェイスを表示する

症状

Show VPN-SIP セッションにトンネルインタ フェースの情報が表示されません。次の例では、トンネル インターフェイスである tunnel1 の情報が表示されていません。

```
Peer5-F#show vpn-sip session
VPN-SIP session current status

Interface: Tunnel2
   Session status: READY_TO_CONNECT
   Remote number : 0334563333
   Local number  : 0623458888
   Remote address:port: 0.0.0.0:0
   Local address:port : 192.30.18.22:0

Interface: Tunnel3
   Session status: READY_TO_CONNECT
   Remote number : 0323452222
   Local number  : 0623458888
   Remote address:port: 0.0.0.0:0
   Local address:port : 192.30.18.22:0

Interface: Tunnel4
   Session status: READY_TO_CONNECT
   Remote number : 0612349999
   Local number  : 0623458888
   Remote address:port: 0.0.0.0:0
   Local address:port : 192.30.18.22:0

Interface: Tunnel6
   Session status: READY_TO_CONNECT
   Remote number : 0634567777
   Local number  : 0623458888
   Remote address:port: 0.0.0.0:0
   Local address:port : 172.30.18.22:0
```

考えられる原因

そのトンネル インターフェイスに VPN SIP が設定されていません。

```
Peer5-F#sh run int tun1
Building configuration...

Current configuration : 201 bytes
!
interface Tunnel1
 ip address 10.5.5.5 255.0.0.0
 tunnel source Loopback11
 tunnel mode ipsec ipv4
 tunnel destination dynamic
 tunnel protection ipsec profile test-prof ikev2-profile test
end
```

推奨処置

そのトンネル インターフェイスに VPN SIP を設定します。

```
:

Peer5-F#show running interface tunnel 1
Building configuration...

Current configuration : 278 bytes
!
interface Tunnel1
 ip address 10.5.5.5 255.255.255.255
 tunnel source Loopback11
 tunnel mode ipsec ipv4
 tunnel destination dynamic
 tunnel protection ipsec profile test-prof ikev2-profile test
 vpn-sip local-number 0623458888 remote-number 0312341111 bandwidth 1000
end
```

次に、上記のシナリオを実行した出力を示します。

```
Peer5-F#show vpn-sip session detail
VPN-SIP session current status

Interface: Tunnel1
   Session status: READY_TO_CONNECT
   Remote number : 0312341111
   Local number  : 0623458888
   Remote address:port: 0.0.0.0:0
   Local address:port : 172.30.18.22:0

   Crypto conn handle: 0x8000002C
   SIP Handle        : 0x0
   SIP callID        : --
   Configured/Negotiated bandwidth: 1000/0 kbps

Interface: Tunnel2
   Session status: READY_TO_CONNECT
   Remote number : 0334563333
   Local number  : 0623458888
   Remote address:port: 0.0.0.0:0
   Local address:port : 172.30.18.22:0
   Crypto conn handle: 0x80000012
   SIP Handle        : 0x0
   SIP callID        : --
   Configured/Negotiated bandwidth: 512/0 kbps

Interface: Tunnel3
   Session status: READY_TO_CONNECT
   Remote number : 0323452222
   Local number  : 0623458888
   Remote address:port: 0.0.0.0:0
   Local address:port : 172.30.18.22:0
   Crypto conn handle: 0x80000031
   SIP Handle        : 0x0
   SIP callID        : --
   Configured/Negotiated bandwidth: 512/0 kbps

Interface: Tunnel4
   Session status: READY_TO_CONNECT
   Remote number : 0612349999
   Local number  : 0623458888
   Remote address:port: 0.0.0.0:0
   Local address:port : 172.30.18.22:0
   Crypto conn handle: 0x8000002F
   SIP Handle        : 0x0
   SIP callID        : --
```

```
   Configured/Negotiated bandwidth: 1000/0 kbps

Interface: Tunnel6
   Session status: READY_TO_CONNECT
   Remote number : 0634567777
   Local number  : 0623458888
   Remote address:port: 0.0.0.0:0
   Local address:port : 172.30.18.22:0
   Crypto conn handle: 0x80000026
   SIP Handle        : 0x0
   SIP callID        : --
   Configured/Negotiated bandwidth: 1000/0 kbps
```

SIP 登録ステータスのトラブルシューティング

症状

SIP 登録ステータスが登録されていません。

```
Peer5#show vpn-sip sip registrar
Line          destination      expires(sec)  contact
transport     call-id
============================================================

Peer5-F#show vpn-sip registration-status

 SIP registration of local number 0623458888 : not registered
```

考えられる原因

その WAN インターフェイスに IP アドレスが設定されていません。

```
Peer5#show ip interface brief
Interface                  IP-Address      OK? Method Status                Protocol
GigabitEthernet0/0         unassigned      YES unset  down                  down
GigabitEthernet0/1         unassigned      YES unset  up                    up
GigabitEthernet0/2         unassigned      YES unset  down                  down
GigabitEthernet0/3         unassigned      YES unset  down                  down
GigabitEthernet0/4         unassigned      YES unset  up                    up
GigabitEthernet0/5         10.5.5.5        YES manual up                    up
Vlan1                      10.45.1.5        YES NVRAM  up                    up
NVI0                       10.1.1.1         YES unset  up                    up
Loopback1                  10.1.1.1         YES NVRAM  up                    up
Loopback5                  10.5.5.5        YES NVRAM  administratively down down
Loopback11                 10.11.11.11     YES NVRAM  up                    up
Tunnel1                    10.5.5.5         YES NVRAM  up                    down
Tunnel2                    10.2.2.2         YES NVRAM  up                    down
Tunnel3                    10.3.3.3         YES NVRAM  up                    down
Tunnel4                    10.4.4.4         YES NVRAM  up                    down
Tunnel6                    10.8.8.8         YES NVRAM  up                    down

Peer5-F#show run interface gigabitEthernet 0/4
Building configuration...

Current configuration : 213 bytes
!
interface GigabitEthernet0/4
 ip dhcp client request sip-server-address
 ip dhcp client request vendor-identifying-specific
 no ip address           ====> no IP address
 ip nat outside
 ip virtual-reassembly in
 duplex auto
```

```
 speed auto
end
```

推奨処置

ip address dhcp コマンドを使用してインターフェイスの IP アドレスを設定する。

```
Peer5-F#show running-config interface gigabitEthernet 0/4
Building configuration...

Current configuration : 215 bytes
!
interface GigabitEthernet0/4
 ip dhcp client request sip-server-address
 ip dhcp client request vendor-identifying-specific
 ip address dhcp         ====> configure IP address DHCP
 ip nat outside
 ip virtual-reassembly in
 duplex auto
 speed auto
end


Peer5-F#show ip interface brief
Interface                  IP-Address      OK? Method Status                Protocol
GigabitEthernet0/0         unassigned      YES unset  down                  down
GigabitEthernet0/1         unassigned      YES unset  up                    up
GigabitEthernet0/2         unassigned      YES unset  down                  down
GigabitEthernet0/3         unassigned      YES unset  down                  down
GigabitEthernet0/4         172.30.18.22    YES DHCP   up                    up
GigabitEthernet0/5         10.5.5.5        YES manual up                    up
Vlan1                      10.45.1.5        YES NVRAM  up                    up
NVI0                       10.1.1.1         YES unset  up                    up
Loopback1                  10.1.1.1         YES NVRAM  up                    up
Loopback5                  10.5.5.5        YES NVRAM  administratively down down
Loopback11                 10.11.11.11     YES NVRAM  up                    up
Tunnel1                    10.6.5.5         YES NVRAM  up                    down
Tunnel2                    10.2.2.2         YES NVRAM  up                    down
Tunnel3                    10.3.3.3         YES NVRAM  up                    down
Tunnel4                    10.4.4.4         YES NVRAM  up                    down
Tunnel6                    10.8.8.8         YES NVRAM  up                    down

Peer5-F#show vpn-sip sip registrar
Line          destination      expires(sec)  contact
transport     call-id
============================================================
0623458888    example.com   2863          172.30.18.22
UDP           1E83ECF0-AF0611E7-802B8FCF-594EB9E7@122.50.18.22

Peer5-F#show vpn-sip registration-status

 SIP registration of local number 0623458888 : registered 172.30.18.22
```

Negotiating IKE 状態でのセッション停止

症状

Negotiating IKE 状態で VPN SIP セッションが停止します。

```
Peer5#show vpn-sip session remote-number 0612349999 detail
VPN-SIP session current status

Interface: Tunnel4
```

```
   Session status: NEGOTIATING_IKE (R)
   Uptime        : 00:00:58
   Remote number : 0612349999
   Local number  : 0623458888
   Remote address:port: 172.30.168.3:24825
   Local address:port : 172.30.18.22:50012
   Crypto conn handle: 0x8000002E
   SIP Handle        : 0x8000000C
   SIP callID        : 16
   Configured/Negotiated bandwidth: 1000/1000 kbps
```

考えられる原因

IKEv2 関連の設定が不適切です。

次の例では、キーリングで設定されているキー ID が、リモート ピアの SIP 番号と一致していません。

```
Peer5-F#show running-config interface tunnel 4
Building configuration...

Current configuration : 276 bytes
!
interface Tunnel4
 ip address 10.4.4.4 255.0.0.0
 tunnel source Loopback11
 tunnel mode ipsec ipv4
 tunnel destination dynamic
 tunnel protection ipsec profile test-prof ikev2-profile test
 VPN-SIP local-number 0623458888 remote-number 0612349999 bandwidth 1000  ====> Remote
number mentioned here doesn’t match the remote number in the keyring
end

IKEv2 Keyring configs:
!
crypto ikev2 keyring keys
 peer peer1
  identity key-id 0312341111
  pre-shared-key psk1
 !
 peer abc
  identity key-id 0345674444
  pre-shared-key psk1
 !
 peer peer2
  identity key-id 0334563333
  pre-shared-key psk10337101690
 !
 peer peer6
  identity key-id 0634567777
  pre-shared-key cisco123
 !
 peer peer3
  identity key-id 0323452222
  pre-shared-key cisco123
 !
 peer peer4
  identity key-id 0645676666
  pre-shared-key psk1
 !
 peer NONID
  identity fqdn example.com
  pre-shared-key psk1
 !
```

```
!
!
crypto ikev2 profile test
 match identity remote any
 identity local key-id 0623458888
 authentication remote pre-share
 authentication local pre-share
 keyring local keys
 dpd 10 6 periodic
 nat force-encap
```

推奨処置

キーリングの設定を修正します。

```
rypto ikev2 keyring keys
 peer peer1
  identity key-id 0312341111
  pre-shared-key psk1
 !
 peer abc
  identity key-id 0345674444
  pre-shared-key psk1
 !
 peer peer2
  identity key-id 0334563333
  pre-shared-key psk1
 !
 peer peer6
  identity key-id 0634567777
  pre-shared-key psk1
 !
 peer peer3
  identity key-id 0323452222
  pre-shared-key psk1
 !
 peer peer4
  identity key-id 0612349999
  pre-shared-key psk1
 !
 peer NONID
  identity fqdn example.com
  pre-shared-key psk1
 !
!
!
crypto ikev2 profile test
 match identity remote any
 identity local key-id 0623458888
 authentication remote pre-share
 authentication local pre-share
 keyring local keys
 dpd 10 6 periodic
 nat force-encap
!

Peer5-F#show vpn-sip session remote-number  0612349999 detail
VPN-SIP session current status

Interface: Tunnel4
   Session status: SESSION_UP (R)
   Uptime        : 00:02:04
   Remote number : 0612349999
   Local number  : 0623458888
   Remote address:port: 172.30.168.3:24845
```

```
Local address:port : 172.30.18.22:50020
Crypto conn handle: 0x8000004E
SIP Handle         : 0x80000014
SIP callID         : 24
Configured/Negotiated bandwidth: 1000/1000 kbps
```

セッション開始のトラブルシューティング

症状

セッションが開始せず、Negotiating IKE 状態で停止します。

考えられる原因

大きな PKI 証明書が IKE 認証メッセージに含まれている状況で、IKE パケットがフラグメンテーションを起こしています。

推奨処置

ルータに IKEv2 フラグメンテーションを設定します。

debug コマンド

次のデバッグ コマンドを VPN SIP 設定のデバッグに使用できます。

表 *213 :* デバッグ コマンド

コマンド名	説明
debug vpn-sip event	VPN SIP を使用した SVTI 登録、SIP 登録、コールセットアップなどのデバッグ メッセージを出力します。
debug vpn-sip errors	初期化、登録、コール セットアップなどの最中にエラーが発生した場合にのみ、エラーメッセージを出力します。
debug vpn-sip sip all	すべての SIP デバッグ トレースを有効化します。
debug vpn-sip sip calls	SIP SPI コールのデバッグ トレースを有効化します。
debug vpn-sip sip dhcp	SIP DHCP デバッグ トレースを有効化します。
debug vpn-sip sip error	SIP エラーのデバッグ トレースを有効化します。
debug vpn-sip sip events	SIP イベントのデバッグ トレースを有効化します。
debug vpn-sip sip feature	機能レベルでのデバッグを有効化します。

コマンド名	説明
debug vpn-sip sip function	SIP機能のデバッグ トレースを有効化します。
debug vpn-sip sip info	SIP情報のデバッグ トレースを有効化します。
debug vpn-sip sip level	情報レベルでのデバッグを有効化します。
debug vpn-sip sip media	SIP メディアのデバッグ トレースを有効化します。
debug vpn-sip sip messages	SIP SPI メッセージのデバッグ トレースを有効化します。
debug vpn-sip sip non-call	コール コンテキスト以外のトレース（OPTIONS、SUBSCRIBE など）を有効化します。
debug vpn-sip sip preauth	SIP 事前認証のデバッグ トレースを有効化します。
debug vpn-sip sip states	SIP SPI状態のデバッグ トレースを有効化します。
debug vpn-sip sip translate	SIP変換のデバッグ トレースを有効化します。
debug vpn-sip sip transport	SIP トランスポートのデバッグ トレースを有効化します。
debug vpn-sip sip verbose	デバッグ モードを有効化します。

VPN SIP に関する追加情報

標準および RFC

標準/RFC	タイトル
RFC 6193（制約事項付き）	セッション記述プロトコル（SDP）におけるIKEのメディア記述

第 159 章

失効したピア証明書の暗号セッションの削除

CRL ダウンロード時の失効したピア証明書の暗号セッションの削除機能は、新しい CRL のダウンロード中に証明書が失効していることが判明した場合にピアとのアクティブな暗号セッションを削除します。

失効したピア証明書の暗号セッションの削除に関する制約事項

- 失効チェックがオフで、この機能が有効になっている場合は、IKE データベースにセッション番号が入力されません。show 出力に、削除されたセッションに関する情報が表示されません。
- この機能を（デバイス上のアクティブ セッションで）頻繁に有効化/無効化するのはお勧めできません。
- 同じ発行者名（CA サーバ）の CRL を頻繁にダウンロードする（30 分間隔）のはお勧めできません。
- CRL キャッシュを有効にする必要があります。CRL キャッシングをトラストポイントベースのプリフェッチに対して無効にすることはできません。ただし、CRL キャッシングを URL ベースのプリフェッチに対して無効にすることはできます。

- IKE 上の自動登録の場合は、セッションが次の IKE キー再生成まで削除されませんが、IKEv2 の場合は、トンネルを手動でクリアするか、証明書が失効するまで待つ必要があります。
- IKE が "issuer-name" と "SN" のデータベースを生成し、PKI から証明書の失効に関する通知を受け取ると、IKE がその PKI 通知を処理します。

失効したピア証明書の暗号セッションの削除に関する情報

暗号セッションの削除方法

1. 証明書認証経由でネゴシエートする場合は、ピアが CERT ペイロードをデバイスに送信し、デバイスが各証明書を解析してシリアル番号と発行者名に関する情報を保存します。この情報は、対応する CA サーバによって発行されたシリアル番号のリストを形成し、PKI に渡され、失効がチェックされます。
2. revocation-check crl コマンドがトラストポイント用に設定されている場合は、PKI が IKE に失効チェックの結果を伝達するため、IKE は不要なピア認定情報を保存せずに済みます。
3. CRL のダウンロードが成功すると、PKI が IKE に "issuer-name" を含む通知を送信します。CRL の署名と内容が検証されます。CRL の内容に変更がなければ、PKI は IKE に通知しません。
4. PKI が IKE に発行者名を通知すると、IKE は発行者名に関するシリアル番号のリストを作成して、そのリストを PKI に渡し、リスト内のシリアル番号が失効しているかどうかが検証されます。
5. PKI は IKE から渡されたシリアル番号のリストに対して失効チェックを実行し、ダウンロードした CRL に照らしてそのリストをチェックします。失効したシリアル番号のリストが IKE に返されます。
6. 失効したシリアル番号のリストを含む通知を PKI から受信すると、IKE はそのようなシリアル番号に関連付けられたセッションを特定して削除します。

失効したピア証明書の暗号セッションの削除のイネーブル化方法

暗号セッションの削除の有効化

このタスクは、失効した証明書の暗号セッションの削除を有効にするために実行します。

手順の概要

1. **enable**
2. **clear crypto session**
3. **configure terminal**
4. 次のいずれかを実行します。
   - **crypto isakmp disconnect-revoked-peers**
   - **crypto ikev2 disconnect-revoked-peers**
5. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**clear crypto session** 例： `Device# clear crypto session`	（任意）IPSec暗号セッション、IKE、およびセキュリティ アソシエーションを削除します。 （注） このコマンドは、以前確立したセッションの機能を有効にするために使用します。そうでない場合は、機能が新しいセッションでのみ有効になります。
ステップ 3	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。

ステップ 4	次のいずれかを実行します。
	• **crypto isakmp disconnect-revoked-peers**
	• **crypto ikev2 disconnect-revoked-peers**
	例：
	`Device(config)# crypto isakmp disconnect-revoked-peers`
	例：
	`Device(config)# crypto ikev2 disconnect-revoked-peers`
		証明書が失効したピアとの IKE または IKEv2 暗号セッションを切断します。
		このコマンドを有効にするには、既存のセッションを再接続します。

ステップ 5	**end** 例： `Device(config)# exit`	グローバル コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

失効したピア証明書の暗号セッションの削除機能の確認

このタスクは、暗号セッションの削除機能が show 出力に表示されるかどうかを確認するために実行します。

手順の概要

1. **enable**
2. **show crypto isakmp peers**
3. **show crypto ikev2 session detail**

手順の詳細

ステップ 1 **enable**

例：

```
Device> enable
```

特権 EXEC モードを有効にします。

- パスワードを入力します（要求された場合）。

ステップ 2 **show crypto isakmp peers**

例：

```
Device# show crypto isakmp peers
```

Internet Security Association and Key Management Protocol（ISAKMP）ピアの説明を表示します。

ステップ 3 **show crypto ikev2 session detail**

例：

```
Device# show crypto ikev2 session detail
```

アクティブなインターネット キー エクスチェンジ バージョン 2（IKEv2）セッションのステータスを表示します。

失効したピア証明書の暗号セッションを削除する設定例

例：IKE セッションの暗号セッションの削除のイネーブル化

```
Device> enable
Device# clear crypto session
Device# configure terminal
Device(config)# crypto isakmp disconnect-revoked-peers
Device# show crypto isakmp peers
```

```
Peer: 150.1.1.2 Port: 500 Local: 150.1.1.1
 Phase1 id: 150.1.1.2
 Disconnect Revoked Peer: Enabled
```

例：IKEv2 セッションの暗号セッションの削除のイネーブル化

```
Device> enable
Device# clear crypto session
Device# configure terminal
Device(config)# crypto ikev2 disconnect-revoked-peers
Device# show crypto ikev2 session detail

Session-id:1, Status:UP-ACTIVE, IKE count:1, CHILD count:1
Tunnel-id   Local          Remote           fvrf/ivrf          Status
1           10.0.0.1/500    10.0.0.2/500      (none)/(none)      READY
      Encr: 3DES, Hash: SHA96, DH Grp:2, Auth: PSK
      Life/Remaining/Active Time: 86400/86157/248 sec
      CE id: 0, Session-id: 1, MIB-id: 1
      Status Description: Negotiation done
      Local spi: 750CBE827434A245       Remote spi: 4353FEDBABEBF24C
      Local id:          10.0.0.1        Remote id:          10.0.0.2
      Local req mess id:    0           Remote req mess id: 0
      Local next mess id:    0          Remote next mess id: 2
      Local req queued:    0            Remote req queued: 0
      Local window:    5                 Remote window: 5
      DPD configured for 0 seconds
      NAT-T is not detected
      Disconnect Revoked Peer: Enabled
Child sa: local selector  10.0.0.1/0 - 10.0.0.1/65535
          remote selector 10.0.0.2/0 - 10.0.0.2/65535
          ESP spi in/out: 0x9360A95/0x6C340600
          CPI in/out: 0x9FE5/0xC776
          AH spi in/out: 0x0/0x0
          Encr: AES CBC, keysize: 128, esp_hmac: SHA96
          ah_hmac: Unknown - 0, comp: IPCOMP_LZS, mode tunnel
```

失効したピアの暗号セッションの削除に関する追加のリファレンス

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『*Cisco IOS Master Commands List, All Releases*』

関連項目	マニュアル タイトル
セキュリティ コマンド	• 『*Cisco IOS Security Command Reference: Commands A to C*』 • 『*Cisco IOS Security Command Reference: Commands D to L*』 • 『*Cisco IOS Security Command Reference: Commands M to R*』 • 『*Cisco IOS Security Command Reference: Commands S to Z*』
IKE の設定	「*Configuring Internet Key Exchange for IPsec VPNs*」
IKEv2 の設定	『*Configuring Internet Key Exchange Version 2 and FlexVPN Site-to-Site*』
推奨される暗号化アルゴリズム	『*Next Generation Encryption*』

シスコのテクニカル サポート

説明	リンク
右の URL にアクセスして、シスコのテクニカル サポートを最大限に活用してください。これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

失効したピア証明書の暗号セッションの削除に関する機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *214 :* 失効したピア証明書の暗号セッションの削除に関する機能情報

機能名	リリース	機能情報
CRL ダウンロード時の失効したピア証明書の暗号セッションの削除		CRL ダウンロード時の失効したピア証明書の暗号セッションの削除機能は、新しい CRL のダウンロード中に証明書が失効していることが判明した場合にピアとのアクティブな暗号セッションを削除します。 次のコマンドが導入または変更されました。**crypto ikev2 disconnect-revoked-peers**、**crypto isakmp disconnect-revoked-peers**、**show crypto isakmp peers**、**show crypto ikev2 session detail**

第 160 章

暗号条件付きデバッグ サポート

暗号条件付きデバッグサポート機能では、新しいdebugコマンドが導入され、これらのコマンドにより、ユーザは、ピアIPアドレス、暗号エンジンの接続ID、セキュリティパラメータインデックス（SPI）などの事前に定義された暗号条件に基づいてIPセキュリティ（IPSec）トンネルをデバッグできます。特定のIPsec処理に限定してデバッグメッセージを表示し、デバッグ出力の量を減らすことにより、多数のトンネルを使用するルータを効率的にトラブルシューティングできます。

暗号条件付きデバッグ サポートの前提条件

暗号条件付きデバッグ サポートの制約事項

-
- 条件付きデバッグは、特定のピアまたは機能に関連するインターネットキー交換（IKE）およびIPSecの問題をトラブルシューティングする際に役立ちますが、デバッグ条件が多すぎると、そのデバッグ条件を定義およびチェックできない場合があります。デバッグ条件値を保管するために空き領域が余分に必要となるため、CPUの処理オーバーヘッドが増加し、メモリ使用量も増加します。したがって、大量のトラフィックを処理するルータで暗号条件付きデバッグをイネーブルにする場合は、注意が必要です。

暗号条件付きデバッグ サポートに関する情報

サポートされる条件タイプ

新しい暗号条件付きデバッグ CLI（**debug crypto condition**、 **debug crypto condition unmatched**、**and show crypto debug-condition**）を使用すれば、条件（フィルタ値）を指定して、指定した条件に関連するデバッグメッセージだけを生成して表示することができます。次の表に、サポートされる条件タイプを示します。

（注） **ipv4** または **ipv6** キーワードを指定した **debug crypto condition peer** コマンドは、ハードウェアプラットフォーム固有のデバッグ出力を提供できます。残りの条件フィルタは、プラットフォーム固有のデバッグ出力を提供しません。

表 *215 :* 暗号デバッグ *CLI* でサポートされる条件タイプ

条件タイプ（キーワード）	説明
connid [21]	1 ～ 32766 の整数。現在の IPSec 処理で、この値が暗号エンジンのあるインターフェイスへの接続 ID として使用されている場合、関連するデバッグ メッセージが表示されます。
FVRF	バーチャル プライベート ネットワーク（VPN）ルーティング/転送（VRF）インスタンスの名前を表す文字列。この VRF インスタンスが、現在の IPSec 処理で、前面扉 VRF（FVRF）として使用されている場合、関連するデバッグ メッセージが表示されます。
ikev2	IKEv2 プロファイルの名前文字列。IKEv2 プロファイル名が指定された場合は、関連するデバッグ メッセージが表示されます。
isakmp	ISAKMP プロファイルの名前文字列。ISAKMP プロファイル名が指定された場合は、関連するデバッグ メッセージが表示されます。
IVRF	VRF インスタンスの名前を表す文字列。この VRF インスタンスが、現在の IPSec 処理で、内部 VRF（IVRF）として使用されている場合、関連するデバッグ メッセージが表示されます。
local	IPv4 または IPv6 ローカル アドレスの名前文字列。
peer group	Unity グループ名を表す文字列。このグループ名をピアがアイデンティティとして使用している場合、関連するデバッグ メッセージが表示されます。

条件タイプ（キーワード）	説明
peer hostname	完全修飾ドメイン名（FQDN）を表す文字列。この文字列をピアがアイデンティティとして使用している場合、関連するデバッグ メッセージが示されます（たとえば、ピアがこの FQDN 文字列を使用して IKE Xauth をイネーブルにする場合）。
peer ipv4 または peer ipv6	単一の IP アドレス。現在の IPSec 処理が、このピアの IP アドレスに関係している場合、関連するデバッグ メッセージが表示されます。
peer subnet	ピアの IP アドレスの範囲を指定するサブネットおよびサブネットマスク。現在の IPSec ピアの IP アドレスが、指定したサブネット範囲に属する場合、関連するデバッグ メッセージが表示されます。
peer username	ユーザ名を表す文字列。このユーザ名をピアがアイデンティティとして使用している場合、関連するデバッグメッセージが示されます（たとえば、ピアがこのユーザ名を使用して IKE 拡張認証（Xauth）をイネーブルにする場合）。
session	暗号セッションに関する情報を提供します。
SPI	32 ビットの符号なし整数。現在の IPSec 処理がこの値を SPI として使用する場合、関連するデバッグ メッセージが表示されます。
unmatched	コンテキスト情報が使用できない場合にデバッグ メッセージを提供します。

[21] IPSec connid、flowid、または SPI をデバッグ条件として使用する場合、関連する IPSec フローに関するデバッグメッセージが生成されます。IPSec フローには、connid、flowid、および SPI が 2 つ（インバウンドとアウトバウンド）ずつ含まれています。各 2 つの connid、flowid、および SPI は、IPSec フローのデバッグ メッセージをトリガーするデバッグ条件として使用できます。

暗号条件付きデバッグ サポートのイネーブル化方法

暗号条件付きデバッグ メッセージのイネーブル化

パフォーマンス上の考慮事項

- 暗号条件付きデバッギングをイネーブルにする前に、使用するデバッグ条件タイプ（デバッグ フィルタとしても知られる）および値を決める必要があります。デバッグ メッセージの量は、定義する条件数によって異なります。

（注） 多数のデバッグ条件を指定すると、CPUサイクルが消費され、ルータのパフォーマンスに悪影響を及ぼすことがあります。

- ルータによって条件付きデバッグが実行されるのは、最低 1 つのグローバル crypto debug コマンド（**debug crypto isakmp**、**debug crypto ipsec**、および **debug crypto engine**）がイネーブルに設定されている場合に限られます。この要件により、条件付きデバッグを使用していないときは、ルータのパフォーマンスに影響が出ないようになっています。

暗号条件付きデバッグのディセーブル化

暗号条件付きデバッグをディセーブルにするには、発行済みのグローバルな暗号デバッグ CLI を事前にディセーブルにする必要があります。その後で、条件付デバッグをディセーブルにできます。

（注） **reset** キーワードを使用すると、設定されたすべての条件を同時にディセーブルにできます。

手順の概要

1. **enable**
2. **debug crypto condition** [**connid** *integer* **engine-id** *integer*] [**flowid** *integer***engine-id** *integer*] [**fvrf** *string*] [**ivrf** *string*] [**peer** [**group** *string*] [**hostname** *string*] [**ipv4** *ipaddress*] [**subnet** *subnet mask*] [**username** *string*]] [**spi** *integer*] [**reset**]
3. **show crypto debug-condition** {[**peer**] [**connid**] [**spi**] [**fvrf**] [**ivrf**] [**unmatched**]}
4. **debug crypto isakmp**
5. **debug crypto ipsec**
6. **debug crypto engine**
7. **debug crypto condition unmatched** [**isakmp** | **ipsec** | **engine**]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**debug crypto condition** [**connid** *integer* **engine-id** *integer*] [**flowid** *integer***engine-id** *integer*] [**fvrf** *string*] [**ivrf** *string*] [**peer** [**group** *string*] [**hostname** *string*] [**ipv4** *ipaddress*] [**subnet** *subnet mask*] [**username** *string*]] [**spi** *integer*] [**reset**] 例：	条件付きデバッグ フィルタを定義します。

	コマンドまたはアクション	目的
	`Router# debug crypto condition connid 2000 engine-id 1`	
ステップ 3	**show crypto debug-condition** {[**peer**] [**connid**] [**spi**] [**fvrf**] [**ivrf**] [**unmatched**]} 例： `Router# show crypto debug-condition spi`	ルータ上ですでにイネーブルに設定されている暗号デバッグ条件を表示します。
ステップ 4	**debug crypto isakmp** 例： `Router# debug crypto isakmp`	グローバル IKE デバッグをイネーブルにします。
ステップ 5	**debug crypto ipsec** 例： `Router# debug crypto ipsec`	グローバル IPSec デバッグをイネーブルにします。
ステップ 6	**debug crypto engine** 例： `Router# debug crypto engine`	グローバル暗号エンジン デバッグをイネーブルにします。
ステップ 7	**debug crypto condition unmatched** [**isakmp** | **ipsec** | **engine**] 例： `Router# debug crypto condition unmatched ipsec`	（任意）デバッグ条件をチェックするためのコンテキスト情報がない場合、デバッグ条件付き暗号メッセージを表示します。 オプションのキーワードを指定しない場合は、暗号関連のすべての情報が表示されます。

暗号エラー デバッグ メッセージのイネーブル化

暗号エラー デバッグ フィルタリングをイネーブルにするには、次の作業を実行する必要があります。

デバッグ暗号エラー CLI

debug crypto error コマンドを有効にすると、エラーに関連するデバッグメッセージだけが表示されます。これにより、IKEネゴシエーションなどの暗号処理がシステム内で失敗した理由を簡単に判別できます。

（注） このコマンドをイネーブルにする場合は、グローバル暗号 debug コマンドがイネーブルに設定されていないことを確認してください。設定されていると、グローバル コマンドによってエラー関連のデバッグ メッセージが上書きされます。

手順の概要

1. **enable**
2. **debug crypto isakmp** | **ipsec** | **engine**} **error**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**debug crypto isakmp**	**ipsec**	**engine**} **error** 例： `Router# debug crypto ipsec error`	暗号エリアに関するエラー デバッグ メッセージだけをイネーブルにします。

暗号条件付きデバッグ CLI の設定例

暗号条件付きデバッグのイネーブル化の例

次の例では、ピアの IP アドレスが 10.1.1.1、10.1.1.2、または 10.1.1.3 で、暗号エンジン 0 の接続 ID に 2000 が使用されている場合のデバッグ メッセージの表示例を示します。また、この例では、グローバルデバッグ暗号 CLI をイネーブルする方法と、**show crypto debug-condition** コマンドをイネーブルにして条件付きの設定を確認する方法も示します。

```
Router#
debug crypto condition connid 2000 engine-id 1
Router#
debug crypto condition peer ipv4 10.1.1.1
Router#
debug crypto condition peer ipv4 10.1.1.2
Router#
debug crypto condition peer ipv4 10.1.1.3
Router#
debug crypto condition unmatched
! Verify crypto conditional settings.
Router#
show crypto debug-condition
Crypto conditional debug currently is turned ON
```

```
IKE debug context unmatched flag:ON
IPsec debug context unmatched flag:ON
Crypto Engine debug context unmatched flag:ON
IKE peer IP address filters:
10.1.1.1  10.1.1.2   10.1.1.3
Connection-id filters:[connid:engine_id]2000:1,
! Enable global crypto CLIs to start conditional debugging.
Router#
debug crypto isakmp
Router#
debug crypto ipsec
Router#
debug crypto engine
```

暗号条件付きデバッグのディセーブル化の例

次の例では、すべての暗号条件付き設定をディセーブルにし、またこれらの設定がディセーブルになったことを確認する方法を示します。

```
Router#
debug crypto condition reset
! Verify that all crypto conditional settings have been disabled.
Router#
show crypto debug-condition
Crypto conditional debug currently is turned OFF
IKE debug context unmatched flag:OFF
IPsec debug context unmatched flag:OFF
Crypto Engine debug context unmatched flag:OFF
```

その他の参考資料

ここでは、暗号条件付きデバッグ サポート機能に関する関連資料について説明します。

関連資料

関連項目	マニュアル タイトル
IPSec および IKE 設定作業	『*Cisco IOS XE Security Configuration Guide: Secure Connectivity*』の「Internet Key Exchange for IPsec VPNs」の章
IPSec および IKE コマンド	『*Cisco IOS Security Command Reference*』

標準

標準	タイトル
なし	--

MIB

MIB	MIB のリンク
なし	選択したプラットフォーム、Cisco IOS XE リリース、およびフィーチャ セットの MIB を検索してダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

RFC

RFC	タイトル
なし	--

シスコのテクニカル サポート

説明	リンク
シスコのサポート Web サイトでは、シスコの製品やテクノロジーに関するトラブルシューティングにお役立ていただけるように、マニュアルやツールをはじめとする豊富なオンライン リソースを提供しています。 お使いの製品のセキュリティ情報や技術情報を入手するために、Cisco Notification Service（Field Notice からアクセス）、Cisco Technical Services Newsletter、Really Simple Syndication（RSS）フィードなどの各種サービスに加入できます。 シスコのサポート Web サイトのツールにアクセスする際は、Cisco.com のユーザ ID およびパスワードが必要です。	http://www.cisco.com/en/US/support/index.html

暗号条件付きデバッグ サポートに関する機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

第 161 章

IPv4 GRE トンネル保護経由の IPv6

IPv4 GRE トンネル保護経由の IPv6 機能は、IPv6 ユニキャスト トラフィックと IPv6 マルチキャスト トラフィックの両方が保護された Generic Routing Encapsulation（GRE）を通過できるようにします。

IPv4 GRE トンネル保護経由の IPv6 の前提条件

- この機能を有効にするには、IPv4 GRE トンネル上で IPsec トンネル保護を設定する必要があります。
- IPv6 マルチキャストを有効にするには、IPv6 マルチキャスト ルーティングを設定する必要があります。

IPv4 GRE トンネル保護経由の IPv6 の制約事項

IPv4 GRE トンネル保護経由の IPv6 機能は、IPv4 ポイントツーポイント GRE トンネル保護経由の IPv6 をサポートしますが、IPv4 mGRE トンネル保護経由の IPv6 はサポートしません。

IPv4 GRE トンネル保護経由の IPv6 に関する情報

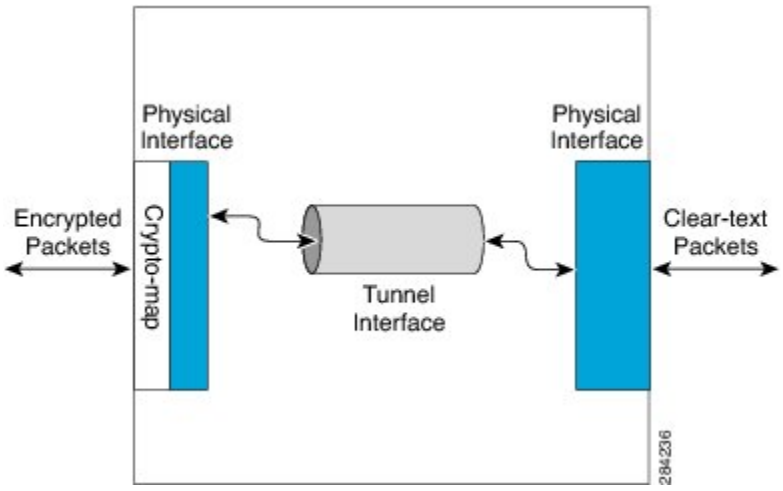
IPsec を使用した GRE トンネル

Generic Routing Encapsulation（GRE）トンネルは、ときどき、IPSec と組み合わせて使用されます。これは、IPSec が IPv6 マルチキャスト パケットをサポートしていないためです。これにより、ダイナミック ルーティング プロトコルが IPSec VPN ネットワーク経由で正しく機能しません。GRE トンネルは IPv6 マルチキャストをサポートしているため、ダイナミック ルーティング プロトコルを GRE トンネル経由で実行できます。ダイナミック ルーティング プロトコルが GRE トンネル経由で設定されている場合は、IPSec を使用して GRE IPv6 マルチキャスト パケットを暗号化できます。

IPSec は、クリプト マップまたはトンネル保護を使用して GRE パケットを暗号化できます。いずれの方法でも、GRE カプセル化の設定後に、IPSec 暗号化を実行するように指定されます。クリプト マップを使用している場合は、暗号化が GRE トンネル パケット用のアウトバウンド物理インターフェイスに適用されます。トンネル保護を使用している場合は、暗号化が GRE トンネル インターフェイス上で設定されます。

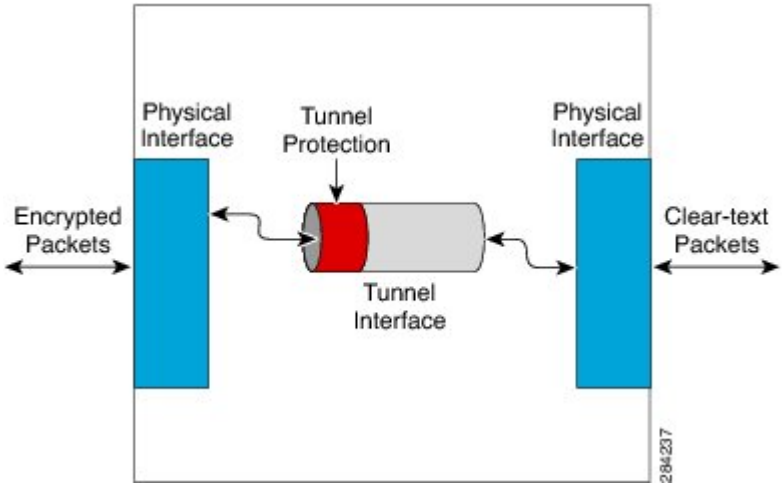
次の図に、物理インターフェイス上でクリプトマップを使用して、GRE トンネルインターフェイス経由でルータに入る暗号化されたパケットを示します。パケットは、復号化およびカプセル化解除されてから、クリア テキストとして IP 宛先に送られます。

図 *83 :* クリプト マップを使用した *IPv4 GRE* トンネル暗号化経由の *IPv6* の設定



次の図に、GRE トンネル インターフェイス上で tunnel protection コマンドを使用した暗号化を示します。暗号化されたパケットは、トンネルインターフェイス経由でルータに入り、復号化およびカプセル化解除されてから、クリア テキストとして宛先に送られます。

図 *84 :* トンネル保護を使用した *IPv4 GRE* トンネル暗号化経由の *IPv6* の設定



クリプトマップ方式を使用した場合とトンネル保護方式を使用した場合の重要な違いを以下に示します。

- IPSec クリプト マップは、物理インターフェイスに関連付けられ、パケットが物理インターフェイスを通して転送されるときにチェックされます。この時点で、パケットはすでに GRE トンネル内でカプセル化されています。
- トンネル保護は、暗号化機能を GRE トンネルに関連付け、パケットが GRE カプセル化されてから物理インターフェイスに転送されるまでの間にチェックされます。

IPv4 GRE トンネル保護経由の IPv6 の設定方法

クリプト マップを使用した IPv4 GRE 暗号化経由の IPv6 の設定

手順の概要

1. **enable**
2. **configure terminal**
3. **ipv6 multicast-routing**
4. **ipv6 unicast-routing**
5. **interface** *type number*
6. **ipv6 address** {**ipv6-address**/*prefix-length* | **prefix-name** *sub-bits*/*prefix-length*}
7. **tunnel mode** {**aurp** | **cayman** | **dvmrp** | **eon** | **gre** | **gre multipoint** | **gre ip** | **gre ipv6** | **ipip** [**decapsulate-any**] | **ipsec ipv4** | **iptalk** | **ipv6** | **ipsec ipv6** | **mpls** | **nos** | **rbscp**}
8. **tunnel source** {**ip-address** | **ipv6-address** | *interface-typeinterface-number*}
9. **tunnel destination** {*hostname* | *ip-address* | *ipv6-address*}
10. **exit**
11. **crypto isakmp policy** *priority*

12. **authentication** {**rsa-sig** | **rsa-encr** | **pre-share**}
13. **hash** {**sha** | **md5**}
14. **group** {**1** | **2** | **5**}
15. **encryption** {**des** | **3des** | **aes 192** | **aes 256**}
16. **exit**
17. **crypto isakmp key** *enc-type-digit keystring* {**address** *peer-address* [*mask*] | **ipv6** {*ipv6-address*/*ipv6-prefix*} | **hostname** *hostname*} [**no-xauth**]
18. **crypto ipsec transform-set** *transform-set-name transform1* [*transform2*] [*transform3*] [*transform4*]
19. **access-list** *access-list-number* [**dynamic** *dynamic-name* [**timeout** *minutes*]] {**deny** | **permit**} *protocol source source-wildcard destination destination-wildcard* [**precedence** *precedence*] [**tos** *tos*] [**time-range** *time-range-name*] [**fragments**] [**log** [*word*] | **log-input** [*word*]]
20. **crypto map** [**ipv6**] *map-name seq-num* [**ipsec-isakmp** [**dynamic** *dynamic-map-name* | **discover** | **profile** *profile-name*]]
21. **set peer** {*hostname* [**dynamic**] [**default**] | *ip-address* [**default**]}
22. **set transform-set** *transform-set-name* [*transform-set-name2...transform-set-name6*]
23. **match address** [*access-list-id* | *name*]
24. **exit**
25. **interface** *type number*
26. **crypto map** *map-name* [**redundancy** *standby-group-name* [**stateful**]]
27. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ipv6 multicast-routing** 例： `Router(config)# ipv6 multicast-routing`	ルータのすべての IPv6 対応インターフェイス上で Protocol Independent Multicast（PIM）とマルチキャスト リスナー検出（MLD）を使用したマルチキャスト ルーティングを有効にして、マルチキャスト転送を有効にします。 • このコマンドは、IPv6 マルチキャストを使用している場合にのみ有効にします。IPv6 ユニキャストを使用している場合は、このコマンドを有効にしないようにする必要があります。
ステップ 4	**ipv6 unicast-routing** 例：	IPv6 ユニキャスト データグラムの転送を有効にします。

	コマンドまたはアクション	目的
	`Router(config)# ipv6 unicast-routing`	
ステップ 5	**interface** *type number* 例： `Router(config)# interface tunnel 10`	トンネル インターフェイスおよび番号を指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 6	**ipv6 address** {**ipv6-address**/*prefix-length* | **prefix-name** *sub-bits*/*prefix-length*} 例： `Router(config-if)# ipv6 address 0:0:0:7272::72/64`	IPv6 の一般的なプレフィックスに基づいて IPv6 アドレスを設定し、インターフェイスにおける IPv6 処理をイネーブルにします。
ステップ 7	**tunnel mode** {**aurp** | **cayman** | **dvmrp** | **eon** | **gre** | **gre multipoint** | **gre ip** | **gre ipv6** | **ipip** [**decapsulate-any**] | **ipsec ipv4** | **iptalk** | **ipv6** | **ipsec ipv6** | **mpls** | **nos** | **rbscp**} 例： `Router(config-if)# tunnel mode gre ip`	トンネル インターフェイスのカプセル化モードを設定します。
ステップ 8	**tunnel source** {**ip-address** | **ipv6-address** | *interface-typeinterface-number*} 例： `Router(config-if)# tunnel source ethernet0`	トンネル インターフェイスの送信元アドレスを設定します。
ステップ 9	**tunnel destination** {*hostname* | *ip-address* | *ipv6-address*} 例： `Router(config-if)# tunnel destination 172.16.0.12`	トンネル インターフェイスの宛先を指定します。
ステップ 10	**exit** 例： `Router(config-if)# exit`	インターフェイス コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードに戻ります。
ステップ 11	**crypto isakmp policy** *priority* 例： `Router(config)# crypto isakmp policy 15`	インターネット キー エクスチェンジ（IKE）ポリシーを定義して、ISAKMP ポリシー コンフィギュレーション モードを開始します。 • ポリシー番号 1 は、最もプライオリティが高いポリシーを示します。*priority* 引数値が低いほど、優先順位が高くなります。
ステップ 12	**authentication** {**rsa-sig** | **rsa-encr** | **pre-share**} 例： `Router(config-isakmp-policy)# authentication pre-share`	IKE ポリシー内の認証方式を指定します。 • **rsa-sig** キーワードと **rsa-encr** キーワードは IPv6 でサポートされません。
ステップ 13	**hash** {**sha** | **md5**} 例：	IKE ポリシー内のハッシュ アルゴリズムを指定します。

	コマンドまたはアクション	目的
	`Router(config-isakmp-policy)# hash md5`	
ステップ 14	**group** {**1** | **2** | **5**} 例： `Router(config-isakmp-policy)# group 2`	IKE ポリシー内部での D-H グループの識別番号を指定します。
ステップ 15	**encryption** {**des** | **3des** | **aes 192** | **aes 256**} 例： `Router(config-isakmp-policy)# encryption 3des`	IKE ポリシー内の暗号化アルゴリズムを指定します。
ステップ 16	**exit** 例： `Router(config-isakmp-policy)# exit`	ISAKMP ポリシー コンフィギュレーション モードを終了して、グローバル コンフィギュレーション モードを開始します。
ステップ 17	**crypto isakmp key** *enc-type-digit keystring* {**address** *peer-address* [*mask*] | **ipv6** {*ipv6-address/ipv6-prefix*} | **hostname** *hostname*} [**no-xauth**] 例： `Router(config)# crypto isakmp key cisco-10 address 172.16.0.12 255.240.0.0`	事前共有認証キーを設定します。
ステップ 18	**crypto ipsec transform-set** *transform-set-name transform1* [*transform2*] [*transform3*] [*transform4*] 例： `Router(config)# crypto ipsec transform-set myset0 ah-sha-hmac esp-3des`	トランスフォーム セットを定義します。
ステップ 19	**access-list** *access-list-number* [**dynamic** *dynamic-name* [**timeout** *minutes*]] {**deny** | **permit**} *protocol source source-wildcard destination destination-wildcard* [**precedence** *precedence*] [**tos** *tos*] [**time-range** *time-range-name*] [**fragments**] [**log** [*word*] | **log-input** [*word*]] 例： `Router(config)# access-list 110 permit gre host 192.168.0.16 host 172.16.0.12`	拡張 IP アクセス リストを定義します。
ステップ 20	**crypto map** [**ipv6**] *map-name seq-num* [**ipsec-isakmp** [**dynamic** *dynamic-map-name* | **discover** | **profile** *profile-name*]] 例： `Router(config)# crypto map mymap 10 ipsec-isakmp`	新しいクリプト マップ エントリまたはプロファイルを作成し、クリプトマップコンフィギュレーション モードを開始します。
ステップ 21	**set peer** {*hostname* [**dynamic**] [**default**] | *ip-address* [**default**]} 例：	クリプト マップ エントリ内の IP Security（IPsec）ピアを指定します。

	コマンドまたはアクション	目的
	`Router(config-crypto-map)# set peer 10.0.0.1`	
ステップ 22	**set transform-set** *transform-set-name* [*transform-set-name2...transform-set-name6*] 例： `Router(config-crypto-map)# set transform-set myset0`	クリプト マップ エントリで使用可能なトランスフォーム セットを指定します。
ステップ 23	**match address** [*access-list-id* | *name*] 例： `Router(config-crypto-map)# match address 102`	クリプト マップ エントリの拡張アクセス リストを指定します。
ステップ 24	**exit** 例： `Router(config-crypto-map)# exit`	クリプト マップ コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードに戻ります。
ステップ 25	**interface** *type number* 例： `Router(config)# interface ethernet 1`	インターフェイスと番号を指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 26	**crypto map** *map-name* [**redundancy** *standby-group-name* [**stateful**]] 例： `Router(config-if)# crypto map mymap`	定義済みのクリプト マップ セットをアウトバウンド インターフェイスに適用します。
ステップ 27	**end** 例： `Router(config-if)# end`	インターフェイス コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

トンネル保護を使用した IPv4 GRE 暗号化経由の IPv6 の設定

手順の概要

1. **enable**
2. **configure terminal**
3. **ipv6 multicast-routing**
4. **ipv6 unicast-routing**
5. **crypto isakmp policy** *priority*
6. **authentication** {**rsa-sig** | **rsa-encr** | **pre-share**}
7. **hash** {**sha** | **md5**}
8. **group** {**1** | **2** | **5**}
9. **encryption**{**des** |**3des** |**aes** |**aes 192** |**aes 256**}
10. **exit**

11. **crypto isakmp key** *enc-type-digit keystring* {**address** *peer-address* [*mask*] | **ipv6** {*ipv6-address*/*ipv6-prefix*} | **hostname** *hostname*} [**no-xauth**]
12. **crypto ipsec transform-set** *transform-set-name transform1* [*transform2*] [*transform3*] [*transform4*]
13. **crypto ipsec profile** *profile-name*
14. **set transform-set** *transform-set-name* [*transform-set-name2...transform-set-name6*]
15. **exit**
16. **interface** *type number*
17. **ipv6 address** {*ipv6-address / prefix-length* | *prefix-name sub-bits*/*prefix-length*}
18. **tunnel mode** {**aurp** | **cayman** | **dvmrp** | **eon** | **gre** | **gre multipoint** | **gre ip** | **gre ipv6** | **ipip**[**decapsulate-any**] | **ipsec ipv4** | **iptalk** | **ipv6** | **ipsec ipv6** | **mpls** | **nos** | **rbscp**}
19. **tunnel source** {*ip-address* | *ipv6-address* | *interface-type interface-number*}
20. **tunnel destination** {*hostname* | *ip-address* | *ipv6-address*}
21. **tunnel protection ipsec profile** *name* [**shared**]
22. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ipv6 multicast-routing** 例： `Router(config)# ipv6 multicast-routing`	ルータのすべての IPv6 対応インターフェイス上で Protocol Independent Multicast（PIM）とマルチキャスト リスナー検出（MLD）を使用したマルチキャスト ルーティングを有効にして、マルチキャスト転送を有効にします。 • このコマンドは、IPv6 マルチキャストを使用している場合にのみ有効にします。IPv6 ユニキャストを使用している場合は、このコマンドを有効にする必要はありません。
ステップ 4	**ipv6 unicast-routing** 例： `Router(config)# ipv6 unicast-routing`	IPv6 ユニキャスト データグラムの転送を有効にします。
ステップ 5	**crypto isakmp policy** *priority* 例：	IKE ポリシーを定義し、ISAKMP ポリシー コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
	`Router(config)# crypto isakmp policy 15`	ポリシー番号1は、最もプライオリティが高いポリシーを示します。*priority* 引数値が低いほど、優先順位が高くなります。
ステップ 6	**authentication** {**rsa-sig** | **rsa-encr** | **pre-share**} 例： `Router(config-isakmp-policy)# authentication pre-share`	インターネット キー エクスチェンジ（IKE）ポリシー内の認証方式を指定します。 • **rsa-sig** キーワードと **rsa-encr** キーワードは IPv6 でサポートされません。
ステップ 7	**hash** {**sha** | **md5**} 例： `Router(config-isakmp-policy)# hash md5`	IKE ポリシー内のハッシュ アルゴリズムを指定します。
ステップ 8	**group** {**1** | **2** | **5**} 例： `Router(config-isakmp-policy)# group 2`	IKE ポリシー内部での D-H グループの識別番号を指定します。
ステップ 9	**encryption**{**des** |**3des** |**aes** |**aes 192** |**aes 256**} 例： `Router(config-isakmp-policy)# encryption 3des`	IKE ポリシー内の暗号化アルゴリズムを指定します。
ステップ 10	**exit** 例： `Router(config-isakmp-policy)# exit`	ISAKMP ポリシー コンフィギュレーション モードを終了します。続いて、グローバル コンフィギュレーション モードに戻ります。
ステップ 11	**crypto isakmp key** *enc-type-digit keystring* {**address** *peer-address* [*mask*] | **ipv6** {*ipv6-address/ipv6-prefix*} | **hostname** *hostname*} [**no-xauth**] 例： `Router(config)# crypto isakmp key cisco-10 address 172.16.0.12 255.240.0.0`	事前共有認証キーを設定します。
ステップ 12	**crypto ipsec transform-set** *transform-set-name transform1* [*transform2*] [*transform3*] [*transform4*] 例： `Router(config)# crypto ipsec transform-set myset0 ah-sha-hmac esp-3des`	トランスフォーム セットを定義し、ルータを暗号化トランスフォーム コンフィギュレーション モードにします。
ステップ 13	**crypto ipsec profile** *profile-name* 例： `Router(config)# crypto ipsec profile ipsecprof`	2 つの IPsec ルータ間の IPsec 暗号化に使用される IPsec パラメータを定義して、IPsec プロファイル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 14	**set transform-set** *transform-set-name* [*transform-set-name2...transform-set-name6*] 例： `Router(ipsec-profile)# set transform-set myset0`	クリプト マップ エントリで使用可能なトランスフォーム セットを指定します。
ステップ 15	**exit** 例： `Router(ipsec-profile)# exit`	IPsec プロファイル コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードに戻ります。
ステップ 16	**interface** *type number* 例： `Router(config)# interface tunnel 1`	トンネル インターフェイスおよび番号を指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 17	**ipv6 address** {*ipv6-address / prefix-length* | *prefix-name sub-bits*/*prefix-length*} 例： `Router(config-if)# ipv6 address 3ffe:b00:c18:1::3/127`	インターフェイスに割り当てられている IPv6 ネットワークを指定し、インターフェイスで IPv6 処理をイネーブルにします。
ステップ 18	**tunnel mode** {**aurp** | **cayman** | **dvmrp** | **eon** | **gre** | **gre multipoint** | **gre ip** | **gre ipv6** | **ipip**[**decapsulate-any**] | **ipsec ipv4** | **iptalk** | **ipv6** | **ipsec ipv6** | **mpls** | **nos** | **rbscp**} 例： `Router(config-if)# tunnel mode gre ip`	GRE IPv6 トンネルを指定します。
ステップ 19	**tunnel source** {*ip-address* | *ipv6-address* | *interface-type interface-number*} 例： `Router(config-if)# tunnel source 10.0.0.1`	トンネル インターフェイスの送信元アドレスまたは送信元インターフェイス タイプと番号を指定します。
ステップ 20	**tunnel destination** {*hostname* | *ip-address* | *ipv6-address*} 例： `Router(config-if)# tunnel destination 172.16.0.12`	トンネル インターフェイスの宛先アドレスまたはホスト名を指定します。
ステップ 21	**tunnel protection ipsec profile** *name* [**shared**] 例： `Router(config-if)# tunnel protection ipsec profile ipsecprof`	トンネルインターフェイスを IPsec プロファイルに関連付けます。 • *name* 引数には、IPsec プロファイルの名前を指定します。この値は、**crypto IPsec profile** *name* コマンドで指定した *name* と一致する必要があります。 • **shared** キーワードを指定すると、同じトンネル送信元 IP を設定した複数のトンネル イン

	コマンドまたはアクション	目的
		ターフェイス間で IPsec セッションを共有できるようになります。 （注） IPsec プロファイルのトンネル保護を変更する場合は、まずトンネルインターフェイスをシャットダウンする必要があります。変更が成功したら、トンネル設定を手動でオンにする必要があります。
ステップ 22	**end** 例： `Router(config-if)# end`	インターフェイス コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

IPv4 GRE トンネル保護経由の IPv6 の設定例

クリプト マップを使用した IPv4 GRE 暗号化経由の IPv6 の設定例

```
Router> enable
Router# configure terminal
Router(config)# ipv6 multicast-routing
Router(config)# ipv6 unicast-routing
Router(config)# interface tunnel 10
Router(config-if)# ipv6 address my-prefix 0:0:0:7272::72/64
Router(config-if)# tunnel mode gre ip
Router(config-if)# tunnel source ethernet0
Router(config-if)# tunnel destination 172.16.0.12
Router(config-if)# exit
Router(config)# crypto isakmp policy 15
Router(config-isakmp-policy)# authentication pre-share
Router(config-isakmp-policy)# hash md5
Router(config-isakmp-policy)# group 2
Router(config-isakmp-policy)# encryption 3des
Router(config-isakmp-policy)# exit
Router(config)# crypto isakmp key cisco-10 address 172.16.0.12 255.240.0.0
Router(config)# crypto ipsec transform-set myset0 ah-sha-hmac esp-3des
Router(config)# access-list 110 permit gre host 192.168.0.16 host 172.16.0.12
Router(config)# crypto map mymap 10 ipsec-isakmp
Router(config-crypto-map)# set peer 10.0.0.1
Router(config-crypto-map)# set transform-set myset0
Router(config-crypto-map)# match address 102
Router(config-crypto-map)# exit
Router(config)# interface ethernet1
Router(config-if)# crypto map mymap
Router(config-if)# end
```

トンネル保護を使用した IPv4 GRE 暗号化経由の IPv6 の設定例

次に、IPv4 GRE トンネル上で IPsec トンネル保護を設定する例を示します。IPv6 マルチキャスト ルーティングは、**ipv6 multicast-routing** コマンドを使用して有効にします。

```
Router> enable
Router# configure terminal
Router(config)# ipv6 multicast-routing
Router(config)# ipv6 unicast-routing
Router(config)# crypto isakmp policy 15
Router(config-isakmp-policy)# authentication pre-share
Router(config-isakmp-policy)# hash md5
Router(config-isakmp-policy)# group 2
Router(config-isakmp-policy)# encryption 3des
Router(config-isakmp-policy)# exit
Router(config)# crypto isakmp key cisco-10 address 172.16.0.12 255.240.0.0
Router(config)# crypto ipsec transform-set myset0 ah-sha-hmac esp-3des
Router(config)# crypto ipsec profile ipsecprof
Router(ipsec-profile)# set transform-set myset0
Router(ipsec-profile)# exit
Router(config)# interface tunnel 1
Router(config-if)# ipv6 address 3ffe:b00:c18:1::3/127
Router(config-if)# tunnel mode gre ip
Router(config-if)# tunnel source 10.0.0.1
Router(config-if)# tunnel destination 172.16.0.12
Router(config-if)# tunnel protection ipsec profile ipsecprof
Router(config-if)# end
```

その他の参考資料

関連資料

関連項目	マニュアル タイトル
IPv6 マルチキャスト ルーティング	『IPv6 Implementation Guide』
Cisco IOS コマンド	『*Cisco IOS Master Commands List, All Releases*』
セキュリティ コマンド：コマンド構文の詳細、コマンド モード、コマンド履歴、デフォルト設定、使用上の注意事項、および例	• 『*Cisco IOS Security Command Reference Commands A to C*』 • 『*Cisco IOS Security Command Reference Commands D to L*』 • 『*Cisco IOS Security Command Reference Commands M to R*』 • 『*Cisco IOS Security Command Reference Commands S to Z*』

シスコのテクニカル サポート

説明	リンク
右の URL にアクセスして、シスコのテクニカル サポートを最大限に活用してください。これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

IPv4 GRE トンネル保護経由の IPv6 に関する機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

第 162 章

RFC 430x IPsec サポート

RFC 430x IPsec サポートには、RFC 4301 で規定されているインターネット キー エクスチェンジ（IKE）と IPsec の動作を実装する機能（RFC 430x IPsec サポート フェーズ 1 およびフェーズ 2）が含まれます。

RFC 430x IPsec サポートに関する情報

RFC 430x IPsec サポート フェーズ 1

RFC 430x IPsec サポートフェーズ 1 機能は、RFC 4301 で規定されているインターネット キー エクスチェンジ（IKE）と IPsec の動作を実装します。

RFC 4301 は IPsec に準拠したシステムの基本アーキテクチャを規定しています。RFC 4301 には、IPv4 と IPv6 の両方の環境で、IP レイヤのトラフィックに一連のセキュリティ サービスを提供する方法が記載されています。RFC 430x IPsec サポート フェーズ 1 機能は、Cisco IOS ソフトウェア上の次の RFC 4301 実装をサポートします。

- **Security association (SA) lifetime**：IPSec とインターネット キー エクスチェンジ（IKE）またはインターネット キー エクスチェンジ バージョン 2（IKEv2）間のセキュリティ アソシエーションのライフタイムは認証証明書のライフタイムを超えないようにする必要があります。
- **OPAQUE selectors**：OPAQUE は、対応するセレクタフィールドが検証に使用できないことを示します。IKEv2 が OPAQUE セレクタに遭遇すると、IKEv2 はスキップして、OPAQUE セレクタを処理せず、ポリシー検証のために次のセレクタに移動します。
- **Explicit Congestion Notification (ECN) support**：ECN は、IPsec パケットの復号時に伝播されるため、パケットの送信元と宛先がネットワーク内で発生した輻輳を認識することが保証されます。

- **Fragment processing**：ピアは、同じトンネル内で初期フラグメントと非初期フラグメントを送信しないようにする必要があります。初期フラグメントと非初期フラグメントを伝送するためのトンネル モード SA と非初期フラグメント用のトンネル モード SA を分ける必要があります。IPsec ピアは、バイパス トラフィックに適合するために、パケットの破棄とステートフル フラグメント チェックをサポートする必要があります。
- **Do not fragment-(DF) bit processing**：DF ビット処理は、SA 単位で設定する必要があります。
- **Dummy packet generation support**：トラフィックが IPsec SA トンネル経由で流れている場合に IPsec SA 経由でダミーパケットを送信してパケットをカプセル化できる必要があります。

RFC 430x IPsec サポート フェーズ 2

RFC 430x IPsec サポート フェーズ 2 機能は、Cisco IOS ソフトウェア上の Internet Control Message Protocol（ICMP）パケットの暗号化と復号化の RFC 4301 実装をサポートします。

ICMP エラーが発生すると、ICMP エラー メッセージが送信されます。たとえば、ホストが到達不能の場合は、中間デバイスが ICMP 要求の発信元にホストが到達不能であることを示すメッセージを送信します。ICMP エラー メッセージが IPsec 暗号化ポリシーに届いた場合は、既存の SA と一致するように分類されない可能性があります。そのため、パケットは ICMP エラーメッセージ内のデータに基づいて分類されます。このデータには、元の ICMP メッセージの送信元アドレスと宛先アドレスが含まれています。SA が ICMP エラー メッセージ内のアドレスに基づいて検出された場合は、その SA が使用されます。SA が存在しない場合は、ポリシーで許可されていれば、SA が作成されます。復号化では、有効な SA が見つからない場合に、ICMP エラー メッセージ内のデータに基づいて復号化後チェックが実行されます。

ICMP エラーメッセージの暗号化と復号は、**show crypto ipsec sa** コマンドの出力に表示される暗号化カウンタと復号カウンタを通して確認できます。

RFC 430x IPsec サポートの設定方法

RFC 430x IPsec サポートのグローバル設定

このタスクは、RFC 4301 実装をグローバルに設定するために実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **crypto ipsec security-association dummy** {**pps** *rate* | **seconds** *seconds*}
4. **crypto ipsec security-association ecn** {**discard** | **propogate**}
5. **exit**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**crypto ipsec security-association dummy** {**pps** *rate* | **seconds** *seconds*} 例： `Device(config)# crypto ipsec security-association dummy seconds 5`	IPSec トラフィック フロー内のダミー パケットの生成と送信を可能にします。
ステップ 4	**crypto ipsec security-association ecn** {**discard** | **propogate**} 例： `Device(config)# crypto ipsec security-association ecn discard`	IPSec トラフィック フロー内の明示的輻輳通知（ECN）設定を可能にします。
ステップ 5	**exit** 例： `Device(config-crypto-map)# exit`	グローバル コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

クリプト マップ単位の RFC 430x IPsec サポートの設定

このタスクは、RFC 4301 実装をクリプト マップ単位で設定するために実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **crypto map** *map-name seq-num* **ipsec-isakmp**
4. **set ipsec security-association dfbit** {**clear** | **copy** | **set**}
5. **set ipsec security-association dummy** {**pps** *rate* | **seconds** *seconds*}
6. **set ipsec security-association ecn** {**discard** | **propogate**}
7. **end**
8. **show crypto map ipsec sa**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**crypto map** *map-name seq-num* **ipsec-isakmp** 例： `Device(config)# crypto map cmap 1 ipsec-isakmp`	作成または変更するクリプト マップ エントリを指定して、クリプト マップ コンフィギュレーション モードを開始します。
ステップ 4	**set ipsec security-association dfbit** {**clear** | **copy** | **set**} 例： `Device(config-crypto-map)# set ipsec security-association dfbit set`	クリプトマップ内の IPSec トラフィック フローのセキュリティ アソシエーション（SA）単位の Do not Fragment（DF）ビット処理を有効にします。
ステップ 5	**set ipsec security-association dummy** {**pps** *rate* | **seconds** *seconds*} 例： `Device(config-crypto-map)# set ipsec security-association dummy seconds 5`	クリプトマップ内の IPSec トラフィック フロー用のダミー パケットの生成と送信を有効にします。
ステップ 6	**set ipsec security-association ecn** {**discard** | **propogate**} 例： `Device(config-crypto-map)# set ipsec security-association ecn propogate`	クリプトマップ内の IPSec トラフィック フロー用の SA 単位の明示的輻輳通知（ECN）設定を有効にします。
ステップ 7	**end** 例： `Device(config-crypto-map)# end`	クリプト マップ コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。
ステップ 8	**show crypto map ipsec sa** 例： `Device# show crypto map ipsec sa`	IPsec SA によって使用される設定を表示します。

例

次に、**show crypto map ipsec sa** コマンドの出力例を示します。

```
Device# show crypto map ipsec sa

interface: Tunnel0
 Crypto map tag: Tunnel0-head-0, local addr 3FFE:2002::32F7:DFF:FE54:7FD1
```

```
protected vrf: (none)
local ident (addr/mask/prot/port): (3FFE:2002::32F7:DFF:FE54:7FD1/128/47/0)
remote ident (addr/mask/prot/port): (3FFE:2002::C671:FEFF:FE88:EB82/128/47/0)
current_peer 3FFE:2002::C671:FEFF:FE88:EB82 port 500
 PERMIT, flags={origin_is_acl,}
#pkts encaps: 36, #pkts encrypt: 36, #pkts digest: 36
#pkts decaps: 28, #pkts decrypt: 28, #pkts verify: 28
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 0, #pkts compr. failed: 0
#pkts not decompressed: 0, #pkts decompress failed: 0
#send errors 0, #recv errors 0
#send dummy packets 852600, #recv dummy packets 424905

local crypto endpt.: 3FFE:2002::32F7:DFF:FE54:7FD1,
remote crypto endpt.: 3FFE:2002::C671:FEFF:FE88:EB82
plaintext mtu 1430, path mtu 1500, ipv6 mtu 1500, ipv6 mtu idb GigabitEthernet0/0/1
current outbound spi: 0xE963D1EC(3915633132)
PFS (Y/N): N, DH group: none
Dummy packet: Initializing

inbound esp sas:
spi: 0xF4E01B9A(4108327834)
 transform: esp-3des esp-md5-hmac,
 in use settings ={Tunnel, }
 conn id: 2053, flow_id: ESG:53, sibling_flags FFFFFFFF80000049, crypto map: Tunnel0-head-0

 sa timing: remaining key lifetime (k/sec): (4608000/2343)
 IV size: 8 bytes
 replay detection support: Y
 Status: ACTIVE(ACTIVE)

inbound ah sas:

inbound pcp sas:

outbound esp sas:
spi: 0xE963D1EC(3915633132)
 transform: esp-3des esp-md5-hmac,
 in use settings ={Tunnel, }
 conn id: 2054, flow_id: ESG:54, sibling_flags FFFFFFFF80000049, crypto map: Tunnel0-head-0

 sa timing: remaining key lifetime (k/sec): (4608000/2343)
 IV size: 8 bytes
 replay detection support: Y
 Status: ACTIVE(ACTIVE)

outbound ah sas:

outbound pcp sas:
```

RFC 430x IPsec サポートの設定例

例：RFC 430x IPsec サポートのグローバル設定

次に、RFC 430x IPsec サポートをグローバルに設定する例を示します。

```
Device> enable
Device# configure terminal
```

```
Device(config)# crypto ipsec security-association dummy seconds 15
Device(config)# crypto ipsec security-association ecn propogate
Device(config-crypto-map)# exit
```

例：クリプト マップ単位の RFC 430x IPsec サポートの設定

次に、RFC 430x IPsec サポートをクリプト マップ単位で設定する例を示します。

```
Device> enable
Device# configure terminal
Device(config)# crypto map cmap 1 ipsec-isakmp
Device(config-crypto-map)# set security-association copy
Device(config-crypto-map)# set security-association dummy seconds 15
Device(config-crypto-map)# set security-association ecn propogate
Device(config-crypto-map)# end
Device# show crypto map ipsec sa

interface: Tunnel0
 Crypto map tag: Tunnel0-head-0, local addr 3FFE:2002::32F7:DFF:FE54:7FD1
protected vrf: (none)
local ident (addr/mask/prot/port): (3FFE:2002::32F7:DFF:FE54:7FD1/128/47/0)
remote ident (addr/mask/prot/port): (3FFE:2002::C671:FEFF:FE88:EB82/128/47/0)
current_peer 3FFE:2002::C671:FEFF:FE88:EB82 port 500
 PERMIT, flags={origin_is_acl,}
#pkts encaps: 36, #pkts encrypt: 36, #pkts digest: 36
#pkts decaps: 28, #pkts decrypt: 28, #pkts verify: 28
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 0, #pkts compr. failed: 0
#pkts not decompressed: 0, #pkts decompress failed: 0
#send errors 0, #recv errors 0
#send dummy packets 852600, #recv dummy packets 424905

local crypto endpt.: 3FFE:2002::32F7:DFF:FE54:7FD1,
remote crypto endpt.: 3FFE:2002::C671:FEFF:FE88:EB82
plaintext mtu 1430, path mtu 1500, ipv6 mtu 1500, ipv6 mtu idb GigabitEthernet0/0/1
current outbound spi: 0xE963D1EC(3915633132)
PFS (Y/N): N, DH group: none
Dummy packet: Initializing

inbound esp sas:
spi: 0xF4E01B9A(4108327834)
 transform: esp-3des esp-md5-hmac,
 in use settings ={Tunnel, }
 conn id: 2053, flow_id: ESG:53, sibling_flags FFFFFFFF80000049, crypto map: Tunnel0-head-0

 sa timing: remaining key lifetime (k/sec): (4608000/2343)
 IV size: 8 bytes
 replay detection support: Y
 Status: ACTIVE(ACTIVE)

inbound ah sas:

inbound pcp sas:

outbound esp sas:
spi: 0xE963D1EC(3915633132)
 transform: esp-3des esp-md5-hmac,
 in use settings ={Tunnel, }
 conn id: 2054, flow_id: ESG:54, sibling_flags FFFFFFFF80000049, crypto map: Tunnel0-head-0

 sa timing: remaining key lifetime (k/sec): (4608000/2343)
```

```
 IV size: 8 bytes
 replay detection support: Y
 Status: ACTIVE(ACTIVE)

outbound ah sas:

outbound pcp sas:
```

RFC 430x IPsec サポートに関する追加のリファレンス

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『Cisco IOS Master Command List, All Releases』
セキュリティ コマンド	• 『Cisco IOS Security Command Reference Commands A to C』 • 『Cisco IOS Security Command Reference Commands D to L』 • 『Cisco IOS Security Command Reference Commands M to R』 • 『Cisco IOS Security Command Reference Commands S to Z』
IKEv2 の設定	
推奨される暗号化アルゴリズム	『Next Generation Encryption』

標準および RFC

標準/RFC	タイトル
RFC 4301	『*Security Architecture for the Internet Protocol*』

シスコのテクニカル サポート

説明	リンク
右の URL にアクセスして、シスコのテクニカル サポートを最大限に活用してください。これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

RFC 430x IPsec サポートに関する機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *216 : RFC430x IPsec* サポートに関する機能情報

機能名	リリース	機能情報
RFC430x IPsec サポート フェーズ 1		RFC 430x IPsec サポートフェーズ 1 機能は、RFC 4301 で規定されているインターネット キー エクスチェンジ（IKE）と IPsec の動作を実装します。 次のコマンドが導入または変更されました。 **crypto ipsec security-association dummy, crypto ipsec security-association ecn, set ipsec security-association dfbit, set ipsec security-association dummy, set ipsec security-association ecn, show crypto map ipsec sa.**
RFC430x IPsec サポート フェーズ 2		RFC 430x IPsec サポートフェーズ 1 機能は、RFC 4301 で規定されているインターネット キー エクスチェンジ（IKE）と IPsec の動作を実装します。 この機能に関して変更または更新されたコマンドはありません。

第 XIV 部

統合脅威防御

第 163 章

Cisco Firepower Threat Defense for ISR

Cisco Firepower Threat Defense は、シスコの主要なネットワーク セキュリティ オプションです。ファイアウォール機能、モニタリング、アラート、侵入検知システム（IDS）などの総合的なセキュリティ機能を提供します。

ここでは、Cisco サービス統合型ルータ（ISR）で IDS を設定および導入する方法について説明します。

Cisco Firepower Threat Defense for ISR に関する制限事項

- マルチキャストトラフィックは検査されません。
- IPv6 トラフィックはエクスポートできません。

Cisco Firepower Threat Defense for ISR 関する情報

Cisco FirePOWER Threat Defense for ISR の概要

Cisco Firepower Threat Defense は、パケットフローの検査を強化する優れたセキュリティソリューションです。

Cisco Firepower Threat Defense ソリューションは、次の 2 つのエンティティで構成されています。

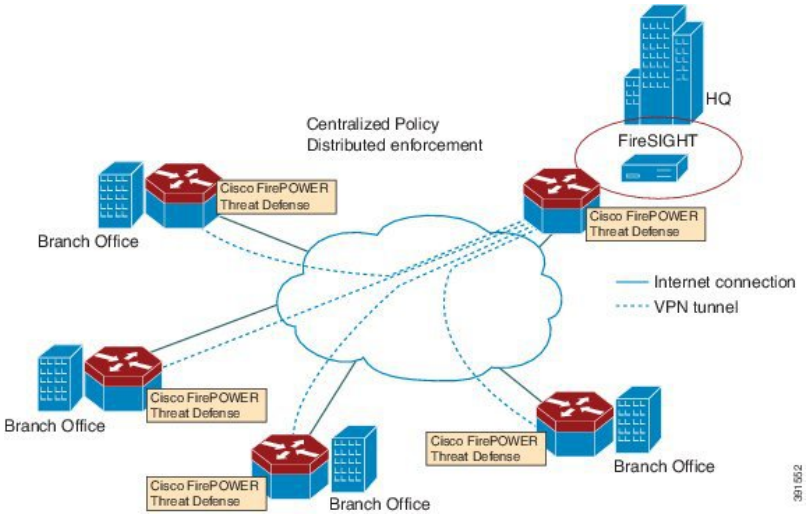
- Cisco FireSIGHT：ネットワーク内の任意の場所で実行できる一元化されたポリシーおよびレポートエンティティ。Cisco FireSIGHT は、Cisco FireSIGHT アプライアンスまたはサーバクラスマシンに仮想インストールしたもののいずれかになります。
- 仮想 Firepower センサー：ポリシーを実装し、イベントと統計情報を防御センターに送り返すセキュリティエンティティ。Firepower センサーは、Cisco 統合型コンピューティングシステム（UCS：Unified Computing System）E シリーズブレードでホストされます。FireSIGHT とセンサーの両方が仮想パッケージとして配布されます。

UCS E シリーズブレードは、第 2 世代（G2）Cisco サービス統合型ルータ（ISR）および Cisco ISR 4000 シリーズサービス統合型ルータ内に収容されている汎用ブレードサーバです。これらのブレードを、オペレーティングシステムのベアメタルとして、またはハイパーバイザの仮想マシンとして導入できます。ルータを UCS E シリーズブレードに接続する内部インターフェイスが 2 つあります。ISR G2 では、Slot0 は周辺機器相互接続エキスプレス（PCIe：Peripheral Component Interconnet Express）の内部インターフェイスであり、UCS E シリーズのスロット 1 はバックプレーン マルチ ギガビット ファブリック（MGF：Multi Gigabit Fabric）に接続されたスイッチドインターフェイスです。Cisco ISR 4000 シリーズルータでは、両方の内部インターフェイスが MGF に接続されます。

ハイパーバイザが UCS E シリーズブレードにインストールされ、Cisco Firepower Threat Defense が仮想マシンとして実行されます。Cisco Firepower Threat Defense の OVA ファイルは、ハイパーバイザ オペレーティング システムを使用して UCS E シリーズブレードに直接インストールされます。Cisco Firepower Threat Defense は、ルータとの追加の通信を行うことなく、匿名のインラインデバイスとして動作します。トラフィックは、入力物理インターフェイスから UCS E シリーズブレードで実行される Cisco Firepower Threat Defense に転送されます。

次の図は、Cisco Firepower Threat Defense の導入の概要を示しています。この図では、センサーと FireSIGHT の間のトラフィックの流れが制御接続となっています。パケットは、ルータの転送ルールを使用し、これらの接続を介してルーティングされます。

図 *85 : Cisco FirePOWER Threat Defense* の導入概要



デフォルトでは、仮想 Cisco Firepower センサーには 3 つのインターフェイスがあり、1 つは管理用、残りの 2 つはトラフィック分析用です。これらのインターフェイスは、UCS E シリーズのインターフェイスにマッピングする必要があります。

UCS ベースのホスティング

Cisco 統合型コンピューティングシステム（UCS）E シリーズブレードは、アプリケーションをホストするための汎用サーバブレードを提供します。このブレードは通常、VMware ESXi ハイパーバイザを実行し、他の VMWare 導入と同様に vSphere を介して管理されます。

Firepower センサーが Cisco UCS E シリーズブレードでホストされている場合は、Cisco Firepower Threat Defense に接続されている Cisco IOS インターフェイスを指定する必要があります。UCS E シリーズブレード内で実行されているアプリケーションは Cisco IOS との互換性が低いため、アプライアンスに接続されているインターフェイスを特定するには、インターフェイスのマッピングを実行する必要があります。Cisco UCS E シリーズブレードに接続するインターフェイスは、ブリッジ ドメイン インターフェイス（BDI）です。

次の Cisco UCS E シリーズブレードは、Firepower センサーのホスティングに対応しています。

- UCS-E 120S
- UCS-E 140D
- UCS-E 140S
- UCS-E 160D
- UCS-E 180D

Cisco Firepower Threat Defense における IDS パケットフロー

Cisco Firepower Threat Defense は、侵入検知システム（IDS）に対応しています。IDS モードでは、トラフィックがセンサーにコピーされ、脅威が分析されます。IDS モードではポリシーを適用できません。違反を検出して報告できます。IDS モードでは、トラフィックはインターフェイスから複製され、Cisco UCS E シリーズブレードで実行される Cisco Firepower Threat Defense にリダイレクトされます。

IDS はトラフィックをコピーし、脅威を検出するためそのトラフィックを分析します。次のいずれかの基準に基づいて、Firepower センサーにパケットを複製する **utd** コマンドを有効にします。

- グローバル検査が有効である場合、ルータを通過するすべてのパケットがセンサーに複製されます。
- インターフェイス単位の検査が有効である場合、入力または出力インターフェイスで検査の **utd** コマンドが有効になっている場合にのみ、パケットが複製されます。

IDS モードでパケット検査を有効にしたインターフェイスを表示するには、**show platform software utd interfaces** コマンドを使用します。パケットの複製は、最初の出力機能の 1 つとして実行されます。

通常のパケット処理では、パケットに適用される機能は、デバイスの設定によって決定される順序付けられたシーケンスを形成します。通常、これらの機能は入力機能または出力機能としてグループ化され、ルーティング機能はこの 2 つの機能の境界を示しています。IDS パケットの複製は、最初の出力機能の1つとして実行されるため、入力機能がパケットをドロップした場合、そのパケットは IDS エンジンへ複製されません。

Firepower センサーのインターフェイス

Firepower センサーの仮想アプライアンスには、トラフィック分析用の 2 つのインターフェイスと FireSIGHT への管理接続用の 1 つのインターフェイスという 3 つのネットワークインターフェイスがあります。2つのトラフィック対応インターフェイスは、設定で2つの仮想インターフェイス「ブリッジ ドメイン インターフェイス（BDI： Bridge Domain Interface）」として表されます。

トラフィックの分析には2つのインターフェイスを使用できますが、侵入検知システム（IDS）には 1 つのトラフィック対応インターフェイスのみ使用できます。

Firepower センサーは管理ネットワークに接続され、LAN セグメント上の別のホストとして表示されます。

（注） 仮想環境で VLAN トラフィックを監視するには、無差別ポートの VLAN ID を 4095 に設定します。

Cisco FirePOWER Threat Defense の相互運用性

Cisco Firepower Threat Defense は、侵入検知システム（IDS）に対応しています。IDS モードでは、選択したトラフィックが分析のために Firepower センサーにコピーされます。

Cisco Firepower Threat Defense は、次の機能と相互運用します。

- ゾーンベースのファイアウォール：アプリケーション レイヤ ゲートウェイ（ALG：Application Layer Gateways）、アプリケーション検査および制御（AIC：Application Inspection and Control）、およびゾーン間で設定されたポリシー
- ネットワークアドレス変換（NAT：Network Address Translation）

（注） Cisco Firepower Threat Defense は、外部グローバルアドレスについて Firepower Threat Defense に通知するメカニズムがないため、外部アドレス変換に対応していません。ただし、外部インターフェイスでアドレス変換を有効にできます。侵入防止システム（IPS）は、常に内部アドレスを使用して、入力インターフェイスの NAT の後、および出力インターフェイスの NAT の前で呼び出されます。

- 暗号
- インテリジェント WAN（IWAN：Intelligent WAN）
- カーネルベースの仮想マシンのワイドエリア アプリケーション サービス（kWAAS：Kernel-based Virtual Machine Wide-Area Application Service）

Cisco Firepower Threat Defense のハードウェアおよびソフトウェア要件

Cisco Firepower Threat Defense ソリューションを実行するには、次のハードウェアが必要です。

- Cisco Firepower センサー（バージョン 5.4）
- Cisco サービス統合型ルータ（ISR）4000 シリーズルータ
- Cisco 統合型コンピューティングシステム（UCS）E シリーズブレード
- Cisco FireSIGHT

Cisco Firepower Threat Defense ソリューションを実行するには、次のソフトウェアが必要です。

- UCS-E ハイパーバイザ
- ESXi 5.0.0、5.1.0、5.5.0
- Cisco Firepower センサー（バージョン Cisco IOS XE リリース 3.14S 以降）
- Cisco FireSIGHT（バージョン 5.2、5.3、5.4）。FireSIGHT は現在のバージョンのみに対応し、直前のバージョンのみとの下位互換性があります。Cisco Firepower センサーのバージョンが 5.4 の場合は、FireSIGHT のバージョン 5.4 または 5.3 を使用する必要があります。

Cisco Firepower Threat Defense ライセンスの取得

Cisco ISR 4000 シリーズサービス統合型ルータには、Cisco Firepower Threat Defense を有効にするためのセキュリティ K9 ライセンスとアプリケーションエクスペリエンス（AppX）ライセンスが必要です。

```
Technology Package License Information:
------------------------------------------------------------------
Technology    Technology-package           Technology-package
              Current       Type           Next reboot
------------------------------------------------------------------
appx             appxk9           EvalRightToUse   appxk9
uc               uck9             EvalRightToUse   uck9
security         securityk9       EvalRightToUse   securityk9
ipbase           ipbasek9         Permanent        ipbasek9
```

Cisco Firepower Threat Defense for ISR の導入方法

Cisco Firepower Threat Defense の侵入検知システム（IDS）を導入するには、次のタスクを実行します。

1. Firepower センサーのパッケージを入手します。

2. VMWare VSphere などのハイパーバイザを使用して Firepower センサーのパッケージをインストールします。
3. トラフィックリダイレクションのルータインターフェイスを設定します。
   - Cisco ISR 4000 シリーズルータのブリッジドメインインターフェイス（BDI）の設定。
   - Cisco ISR 第 2 世代ルータの VLAN 設定。
4. Firepower センサーをブートストラップします。
5. Cisco FireSIGHT でポリシーを設定します。
   - ポリシーは FireSIGHT GUI を使用して設定します。
6. 検査を有効にします。

Firepower センサーパッケージの入手

統合型コンピューティングシステム（UCS）E シリーズブレードに Firepower センサーを導入するために、OVA ファイルをダウンロードして保存します。OVA は仮想マシンの圧縮された「インストール可能な」バージョンを含む、オープン仮想アーカイブ（Open Virtualization Archive）です。https://support.sourcefire.com/sections/1/sub_sections/51#5-2-virtual-appliances から OVA ファイルをダウンロードします。

Firepower センサー OVA ファイルのインストール

VMWare VSphere などのハイパーバイザを使用して、UCS E シリーズブレードに Firepower センサー OVA をインストールします。

UCS E シリーズブレードへの Firepower センサーの取り付け

ここでは、Cisco ISR 4000 シリーズサービス統合型ルータにインストールされている統合型コンピューティングシステム（UCS）E シリーズブレードに Firepower センサーを取り付ける方法について説明します。

1. UCS E シリーズカードを取り付けます。
2. **show platform** コマンドを使用して、カードが動作していることを確認します。
3. Cisco 統合型管理コントローラ（CIMC：Cisco Integrated Management Controller）のポートを設定します。

   CIMC GUI は、E シリーズサーバの Web ベースの管理インターフェイスです。CIMC GUI を起動して、次の最小要件を満たしている任意のリモートホストからサーバを管理できます。

   - Java 1.6 以降
   - HTTP または HTTPS に対応
   - Adobe Flash Player 10 以降

   CIMC は、管理（management）という名前のポートで実行されます。次に、管理ポートを IP アドレスでブートストラップする例を示します。

```
ucse subslot 1/0
  imc access-port dedicated
  imc ip-address 10.66.152.158 255.255.255.0
!
```

デフォルトのログインとパスワード（それぞれ admin と password）を使用して、ブラウザから CIMC に接続します。設定例では、ブラウザのアドレスは https://10.66.152.158 です。

4. ESXi をインストールします。

   Cisco UCS E シリーズブレードの ESXi イメージを https://my.vmware.com/web/vmware/details?downloadGroup=CISCO-ESXI-5.1.0-GA-25SEP2012&productId=284 からダウンロードします。

5. VMWare VSphere を使用してCisco UCS E シリーズブレードに Firepower センサーをインストールします。
6. トラフィックリダイレクトを設定します。詳細については、「Cisco UCS E シリーズブレードでのトラフィックリダイレクトの設定」の項を参照してください。
7. VMWare vSwitch を設定します。ISR 4000 シリーズルータの仮想マシン ネットワーク インターフェイス カード（VMNIC：Virtual Machine Network Interface Card）のマッピングは次のとおりです。

   - VMNIC0：ルータバックプレーンの UCS E シリーズのインターフェイス x/0/0 にマッピング
   - VMNIC1：ルータバックプレーンのUCS E シリーズのインターフェイス x/0/1 にマッピング
   - VMNIC2：UCS E シリーズのフロントプレーン GigabitEthernet 2 インターフェイスにマッピング
   - VMNIC3：UCS E シリーズのフロントプレーン GigabitEthernet 3 インターフェイスにマッピング

（注） VMNIC3 は、UCS E シリーズ 140D、160Dm、および 180D でのみ使用できます。

UCS E シリーズ 120S および 140S には、3 つのネットワークアダプタと 1 つの管理ポートがあります。UCS E シリーズ140D、160Dm、および 180D には 4 つのネットワークアダプタがあります。

Cisco UCS E シリーズブレードにおけるトラフィックのリダイレクトの設定

手順の概要

1. **enable**
2. **configure terminal**

3. **interface** *type number*
4. **no ip address**
5. **no negotiation auto**
6. **switchport mode trunk**
7. **no mop enabled**
8. **no mop sysid**
9. **service instance** *service-instance-number ethernet*
10. **encapsulation dot1q** *vlan-id*
11. **rewrite ingress tag pop** {**1** | **2**} **symmetric**
12. **bridge domain** *bridge-ID*
13. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface** *type number* 例： `Router(config)# interface ucse 1/0/0`	インターフェイスを設定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	**no ip address** 例： `Router(config-if)# no ip address`	インターフェイス上で IP アドレスを削除するか、IP 処理を無効にします。
ステップ 5	**no negotiation auto** 例： `Router(config-if)# no negotiation auto`	インターフェイス上で速度、デュプレックスモード、およびフロー制御のアドバタイズメントを無効にします。
ステップ 6	**switchport mode trunk** 例： `Router(config-if)# switchport mode trunk`	トランキング VLAN レイヤ 2 インターフェイスを指定します。
ステップ 7	**no mop enabled** 例： `Router(config-if)# no mop enabled`	インターフェイス上でメンテナンス オペレーション プロトコル（MOP：Maintenance Operation Protocol）を無効にします。
ステップ 8	**no mop sysid** 例：	インターフェイスからの定期的な MOP システム識別メッセージの送信を無効にします。

	コマンドまたはアクション	目的
	`Router(config-if)# no mop sysid`	
ステップ 9	**service instance** *service-instance-number ethernet* 例： `Router(config-if)# service instance 10 ethernet`	インターフェイスでイーサネット サービス インスタンスを設定し、イーサネット サービス インスタンスの設定モードに入ります。
ステップ 10	**encapsulation dot1q** *vlan-id* 例： `Router(config-if-srv)# encapsulation dot1q 10`	インターフェイスの 802.1Q フレーム入力を適切なサービス インスタンスにマップするための一致基準を定義します。
ステップ 11	**rewrite ingress tag pop** {**1** | **2**} **symmetric** 例： `Router(config-if-srv)# rewrite ingress tag pop 1 symmetric`	サービス インスタンスに入るフレームで実行されるカプセル化調整を指定します。
ステップ 12	**bridge domain** *bridge-ID* 例： `Router(config-if-srv)# bridge domain 10`	サービス インスタンスまたは MAC トンネルをブリッジ ドメイン インスタンスにバインドします。
ステップ 13	**end** 例： `Router(config-if)# end`	イーサネット サービス インスタンスの設定モードを終了し、特権 EXEC 設定モードに戻ります。

Firepower センサーのブートストラップ

Firepower センサーは手動で設定する必要があります。FireSIGHT と通信するように Firepower センサーを設定するには、次のタスクを実行します。詳細については、https://support.sourcefire.com/sections/10 を参照してください。

Cisco 統合型コンピューティングシステム（UCS）E シリーズブレードで実行されているセンサーは、VSphere を介して Firepower センサーの仮想マシンのコンソールにログインすることによってブートストラップされます。

（注） Firepowerセンサーは、ブートストラップする前にインストールして導入する必要があります。

手順の概要

1. ログインするためのデフォルトのユーザ名とパスワードを入力します。
2. **configure network ipv4 manual** *ip-address network-mask default-gateway*
3. **configure network dns servers** *dns-server*
4. **configure network dns searchdomains** *domain-name*
5. **configure manager add** *dc-hostname registration-key*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	ログインするためのデフォルトのユーザ名とパスワードを入力します。	センサーを設定する場合、デフォルトのユーザ名とパスワードはそれぞれ admin と Sourcefire となります。 • Firepowerセンサーに初めてログインした後は、管理者パスワードを変更する必要があります。
ステップ 2	**configure network ipv4 manual** *ip-address network-mask default-gateway* 例： `Device# configure network ipv4 manual 10.66.152.137 255.255.255.0 10.66.152.1`	ネットワーク接続を設定します。
ステップ 3	**configure network dns servers** *dns-server* 例： `Device# configure network dns servers 192.10.26.10`	ドメインネームシステム（DNS：Domain Name System）サーバを設定します。
ステップ 4	**configure network dns searchdomains** *domain-name* 例： `Device# configure network dns searchdomains cisco.com`	DNS 検索ドメインを設定します。
ステップ 5	**configure manager add** *dc-hostname registration-key* 例： `Device# configure manager sourcefire-dc.cisco.com cisco-sf`	センサーを FireSIGHT に関連付けます。 • *registration key*は、ユーザが FireSIGHT にセンサーを登録するために後で使用する文字列です。

例

次は、Firepower センサーの設定済みのネットワーク設定を表示する **show network** コマンドからの出力例です。

```
Device# show network

-----------------------------------------------------
IPv4
Configuration             : manual
Address                   : 10.66.152.137
Netmask                   : 255.255.255.0
Gateway                   : 10.66.152.1
MAC Address               : 44:03:A7:43:05:AD
Management port           : 8305
-----------------------------------------------------
IPv6
Configuration             : disabled
Management port           : 8305
```

```
-----------------------------------------------------
```

次は、設定済みの DNS 設定を表示する **show dns** コマンドからの出力例です。

```
Device# show dns

search cisco.com
nameserver 192.10.26.10
```

次は、設定済みの管理設定を表示する **show managers** コマンドからの出力例です。

```
Device# show managers

Host                        : sourcefire-dc.cisco.com
Registration Key            : cisco-sf
Registration                : pending
RPC Status                  :
```

IDS 検査のグローバルな有効化

要件に基づいて、グローバルレベルまたはインターフェイスレベルで侵入検知システム（IDS）の検査を設定できます。

専用の管理インターフェイスでは IDS 検査を有効にできません。

手順の概要

1. **enable**
2. **configure terminal**
3. **utd enable**
4. **utd engine advanced**
5. **threat detection**
6. **exit**
7. **utd**
8. **all-interfaces**
9. **engine advanced**
10. **fail close**
11. **rate** *pps-rate*
12. **redirect-interface** *interface interface-number*
13. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。

	コマンドまたはアクション	目的
ステップ 2	**configure terminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**utd enable** 例： `Router(config)# utd enable`	統合脅威防御の設定モードに入ります。
ステップ 4	**utd engine advanced** 例： `Router(config)# utd engine advanced`	統合脅威防御（UTD）の拡張エンジンを設定し、UTD の拡張エンジンの設定に入ります。 モードで使用します。
ステップ 5	**threat detection** 例： `Router(config-utd-eng-adv)# threat detection`	脅威検知または侵入防止システム（IPS）を Snort エンジンの動作モードとして設定します。
ステップ 6	**exit** 例： `Router(config-if)# exit`	インターフェイス設定モードを終了し、グローバル設定モードに戻ります。
ステップ 7	**utd** 例： `Router(config)# utd`	統合脅威防御の設定モードに入ります。
ステップ 8	**all-interfaces** 例： `Router(config-utd)# all-interfaces`	デバイスのすべてのレイヤ3インターフェイスで UTD を設定します。
ステップ 9	**engine advanced** 例： `outer(config-utd)# engine advanced`	統合脅威防御（UTD）の拡張エンジンを設定し、UTD の拡張エンジンの設定に入ります。
ステップ 10	**fail close** 例： `Device(config-engine-std)# fail close`	（オプション）UTD エンジンに障害が発生した場合に行うアクションを定義します。デフォルトのオプションはフェールオープンです。フェールクローズオプションは、UTD エンジンに障害が発生した場合にすべての IPS または IDS トラフィックをドロップします。フェールオープンオプションを使用すると、UTD エンジンに障害が発生した場合にすべての IPS または IDS トラフィックを許可します。

	コマンドまたはアクション	目的
ステップ 11	**rate** *pps-rate* 例： `Device(config-engine-std)# rate 2000000`	（オプション）センサーにプッシュする pps レートを指定します。指定できる範囲は 1000 ～ 4000000 です。
ステップ 12	**redirect-interface** *interface interface-number* 例： `Router(config-utd)# redirect-interface BDI 10`	インターフェイスで IDS のトラフィックリダイレクトを設定します。
ステップ 13	**end** 例： `Router(config-utd)# end`	統合脅威防御の設定モードを終了し、特権 EXEC モードに戻ります。

インターフェイスごとの IDS 検査の有効化

要件に基づいて、グローバルレベルまたはインターフェイスレベルで侵入検知システム（IDS）の検査を設定できます。

専用の管理インターフェイスでは IDS 検査を有効にできません。

手順の概要

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **utd enable**
5. **exit**
6. IDS 検査を必要とするすべてのインターフェイスで、手順 3 ー 5 を繰り返します。管理インターフェイスで検査を設定しないでください。
7. **utd engine advanced**
8. **threat detection**
9. **utd**
10. **engine advanced**
11. **fail close**
12. **rate** *range*
13. **redirect interface** *type number*
14. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。

	コマンドまたはアクション	目的
ステップ 2	**configure terminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface** *type number* 例： `Router(config)# interface gigabitethernet 0/1/1`	インターフェイスを設定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	**utd enable** 例： `Router(config-if)# utd enable`	インターフェイスで侵入検知を有効にします。
ステップ 5	**exit** 例： `Router(config-if)# exit`	インターフェイス設定モードを終了し、グローバル設定モードに戻ります。
ステップ 6	IDS 検査を必要とするすべてのインターフェイスで、手順3ー5を繰り返します。管理インターフェイスで検査を設定しないでください。	-
ステップ 7	**utd engine advanced** 例： `Router(config)# utd engine advanced`	統合脅威防御（UTD）の拡張エンジンを設定し、UTD の拡張エンジンの設定に入ります。 モードで使用します。
ステップ 8	**threat detection** 例： `Router(config-utd-eng-adv)# threat detection`	脅威検知または侵入防止システム（IPS）を Snort エンジンの動作モードとして設定します。
ステップ 9	**utd** 例： `Router(config)# utd`	統合脅威防御の設定モードに入ります。
ステップ 10	**engine advanced** 例： `outer(config-utd)# engine advanced`	統合脅威防御（UTD）の拡張エンジンを設定し、UTD の拡張エンジンの設定に入ります。
ステップ 11	**fail close** 例： `Device(config-engine-std)# fail close`	（オプション）UTD エンジンに障害が発生した場合に行うアクションを定義します。デフォルトのオプションはフェールオープンです。フェールクローズオプションは、UTD エンジンに障害が発生した場合にすべての IPS または IDS トラフィックをドロップします。フェールオープンオプションを使用すると、UTD エンジンに障害が発生した場合にすべての IPS または IDS トラフィックを許可します。

	コマンドまたはアクション	目的
ステップ 12	**rate** *range* 例： `Device(config-engine-std)# rate 1000`	（オプション）センサーにプッシュする pps レートを指定します。指定できる範囲は 1000 ～ 4000000 です。
ステップ 13	**redirect interface** *type number* 例： `Router(config-utd)# redirect interface BDI 10`	インターフェイスで IDS のトラフィックリダイレクトを設定します。
ステップ 14	**end** 例： `Router(config-utd)# end`	統合脅威防御の設定モードを終了し、特権 EXEC モードに戻ります。

ISR での Cisco Firepower Threat Defense の設定例

例：Cisco UCS E シリーズブレードでのトラフィックリダイレクトの設定

次に、トラフィックリダイレクトの入力および出力インターフェイスを設定する例を示します。

```
Router# configure terminal
Router(config)# interface ucse 1/0/0
Router(config-if)# no ip address
Router(config-if)# no negotiation auto
Router(config-if)# switchport mode trunk
Router(config-if)# no mop enabled
Router(config-if)# no mop sysid
Router(config-if)# exit
Router(config)# interface ucse 1/0/1
Router(config-if)# no ip address
Router(config-if)# no negotiation auto
Router(config-if)# switchport mode trunk
Router(config-if)# no mop enabled
Router(config-if)# no mop sysid
Router(config-if)# service instance 10 ethernet
Router(config-if-srv)# encapsulation dot1q 10
Router(config-if-srv)# rewrite ingress tag pop 1 symmetric
Router(config-if-srv)# bridge domain 10
Router(config-if-srv)# exit
Router(config-if)# exit
Router(config)# interface BDI 10
Router(config-if)# no shutdown
Router(config-if)# ip address 10.1.1.1 255.255.255.0
Router(config-if-srv)# end
```

例：Firepower センサーのブートストラップ

次に、Firepower Threat Defense センサーをブートストラップする例を示します。

```
Sourcefire3D login: admin
Password: Sourcefire
Last login: Tue Nov 12 11:15:03 UTC 2013 on tty1

Copyright 2001-2013, Sourcefire, Inc. All rights reserved. Sourcefire is
a registered trademark of Sourcefire, Inc. All other trademarks are
property of their respective owners.

Sourcefire Linux OS v5.2.0 (build 135)
Sourcefire Virtual Device 64bit v5.2.0 (build 838)

> configure password
Enter current password:
Enter new password:
Confirm new password:

> configure network ipv4 manual 10.66.152.137 255.255.255.0 10.66.152.1
Setting IPv4 network configuration.
ADDRCONF(NETDEV_UP): eth0: link is not ready
e1000: eth0: e1000_phy_read_status: Error reading PHY register
e1000: eth0: e1000_watchdog_task: NIC Link is Up
1000 Mbps Full Duplex, Flow Control: None
ADDRCONF(NETDEV_CHANGE): eth0: link becomes ready

Network settings changed.

> configure network dns servers 192.10.26.10

> configure network dns searchdomains cisco.com

configure manager add sourcefire-dc.cisco.com cisco-sf
Manager successfully configured.
```

例：IDS 検査のグローバルな有効化

```
Router# configure terminal
Router(config)# utd enable
Router(config-utd)# utd engine advanced
Router(config-utd-adv)# threat detection
Router(config-utd-adv)# exit
Router(config)# utd
Router(config-utd)# all-interfaces
Router(config-utd)# engine advanced
Router(config-utd)# fail close
Router(config-utd)# rate 1000
Router(config-utd)# redirect-interface BDI 10
Router(config-utd)# end
```

例：インターフェイスごとの IDS 検査の有効化

```
Device# configure terminal
Device(config)# interface gigabitethernet 0/1/1
Device(config-if)# utd enable
Router(config-utd)# utd engine advanced
Router(config-utd-adv)# threat detection
Router(config-utd-adv)# exit
Router(config)# utd
Router(config-utd)# engine advanced
Router(config-utd)# fail close
Router(config-utd)# rate 1000
Router(config-utd)# redirect-interface BDI 10
Router(config-utd)# end
```

IDS 検査の確認とモニタリング

次のコマンドを使用して、侵入検知システム（IDS）の導入を確認およびモニタします。

手順の概要

1. **enable**
2. **debug platform condition feature utd controlplane**
3. **debug platform condition feature utd dataplane submode**
4. **show platform hardware qfp active utd** {**config** | **status** [**all**] [**clear**] [**drop**] [**general**]}

手順の詳細

ステップ 1 enable

特権 EXEC モードを有効にします。

- パスワードを入力します（要求された場合）。

例：

```
Router> enable
```

ステップ 2 debug platform condition feature utd controlplane

IDS 設定およびステータス情報のデバッグを有効にします。

例：

```
Router# debug platform condition feature utd controlplane

network RF:
  network-rf idb-sync-history events debugging is on
IOSXE Conditional Debug Configs:

Conditional Debug Global State: Stop

Feature      Type           Submode       Level
```

```
------------|-------------|------------------------------
UTD           controlplane                info

IOSXE Packet Tracing Configs:

Packet Infra debugs:

Ip Address                                                Port
-------------------------------------------------------|----------
```

ステップ 3 **debug platform condition feature utd dataplane submode**

IDS パケットフロー情報のデバッグを有効にします。

例：

```
Router# debug platform  condition feature utd dataplane submode

network RF:
  network-rf idb-sync-history events debugging is on
IOSXE Conditional Debug Configs:

Conditional Debug Global State: Stop

Feature      Type            Submode                    Level
-----------|-------------|---------------------|----------
UTD           controlplane                             info
UTD           dataplane     fia proxy punt             info

IOSXE Packet Tracing Configs:

Packet Infra debugs:

Ip Address                                                Port
-------------------------------------------------------|----------
```

ステップ 4 **show platform hardware qfp active utd** {**config** | **status** [**all**] [**clear**] [**drop**] [**general**]}

Cisco クォンタムフロープロセッサ（QFP：Quantum Flow Processor）の IDS 検査に関する情報を表示します。

例：

```
Router# show platform hardware qfp active utd config

Global flags: 0x40004
Num divert interfaces: 1
Divert UIDBs: 65521 0
FIB information
[0][0] 0x309e3c30
[0][1] 0x0
[1][0] 0x309e4040
[1][1] 0x0
```

Cisco Firepower Threat Defense for ISR に関するその他の参考資料

関連資料

関連項目	マニュアル タイトル
IOS コマンド	『Cisco IOS Master Command List, All Releases』[英語]
セキュリティ コマンド	• 『Cisco IOS Security Command Reference: Commands A to C』[英語] • 『Cisco IOS Security Command Reference: Commands D to L』[英語] • 『Cisco IOS Security Command Reference: Commands M to R』[英語] • 『Cisco IOS Security Command Reference: Commands S to Z』[英語]
UCS E シリーズ サーバ	http://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/e/2-0/gs/guide/b_2_0_Ge

シスコのテクニカル サポート

説明	リンク
シスコのサポート Web サイトでは、シスコの製品やテクノロジーに関するトラブルシューティングにお役立ていただけるように、マニュアルやツールをはじめとする豊富なオンライン リソースを提供しています。 お使いの製品のセキュリティ情報や技術情報を入手するために、Cisco Notification Service（Field Notice からアクセス）、Cisco Technical Services Newsletter、Really Simple Syndication（RSS）フィードなどの各種サービスに加入できます。 シスコのサポート Web サイトのツールにアクセスする際は、Cisco.com のユーザ ID およびパスワードが必要です。	http://www.cisco.com/support

Cisco FirePOWER Threat Defense for ISR の機能に関する情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *217 : Cisco FirePOWER Threat Defense for ISR* の機能に関する情報

機能名	リリース	機能情報

第 164 章

Snort IPS

Snort IPS 機能は、Cisco 4000 シリーズサービス統合型ルータおよび Cisco クラウドサービスルータ 1000v シリーズのブランチオフィスで侵入防止システム（IPS）または侵入検知システム（IDS）を実現します。この機能は、オープンソースの Snort ソリューションを使用して IPS と IDS を有効にします。Snort IPS 機能は、Cisco IOS XE リリース 3.16.1S、3.17S、およびそれ以降のリリースで使用できます。

（注） 仮想ルーティングおよび転送（VRF）機能は、Cisco IOS XE Denali リリース16.3.1 以降のリリースの Snort IPS 設定に対応しています。

ここでは、その機能および動作の仕組みについて説明します。

Snort IPS の制約事項

Snort IPS 機能には、次のような制約事項が適用されます。

- Cisco 4000 シリーズ ISR でブーストライセンスを有効にした場合、Snort IPS の仮想サービスコンテナを設定できません。
- ゾーンベース型ファイアウォールの SYN クッキー機能と互換性がありません。

- ネットワークアドレス変換 64（NAT64）には対応しません。
- オープンソースの Snort での SNMP ポーリングには、SnortSnmp プラグインが必要となります。SnortSnmp プラグインが UTD にインストールされていないため、Snort IPS は SNMP ポーリング機能または MIB に対応しません。
- **IOS syslog はレートが制限されているため、Snort によって生成されたすべてのアラートが IOS Syslog で表示されない場合があります。ただし、外部ログサーバにエクスポートする場合は、すべての Syslog メッセージを表示できます。**

Snort IPS に関する情報

Snort IPS の概要

Snort IPS 機能は、Cisco 4000 シリーズサービス統合型ルータおよび Cisco クラウドサービスルータ 1000v シリーズのブランチオフィスで侵入防止システム（IPS）または侵入検知システム（IDS）を実現します。この機能は、Snort エンジンを使用して IPS および IDS 機能を実現します。

Snort は、リアルタイムでトラフィック分析を行い、IP ネットワークで脅威が検出されたときにアラートを生成するオープンソースのネットワーク IPS です。また、プロトコル分析、コンテンツ検索またはマッチングを実行し、バッファオーバーフロー、ステルスポートスキャンなどのさまざまな攻撃やプローブを検出することもできます。Snort エンジンは、Cisco 4000 シリーズサービス統合型ルータおよび Cisco クラウドサービスルータ 1000v シリーズで仮想コンテナサービスとして実行されます。

Snort IPS 機能は、IPS または IDS 機能を提供するネットワーク侵入検知および防止モードで動作します。ネットワーク侵入検知および防止モードでは、Snort は次のアクションを実行します。

- ネットワークトラフィックをモニタし、定義されたルールセットに照らしあわせて分析します。
- 攻撃の分類を行います。
- 一致したルールに照らしあわせてアクションを呼び出します。

要件に応じて、IPS または IDS モードで Snort を有効にできます。IDS モードでは、Snort はトラフィックを検査し、アラートを報告しますが、攻撃を防ぐためのアクションは実行しません。IPS モードでは、侵入検知に加えて、攻撃を防ぐためのアクションを実行します。

Snort IPS はトラフィックをモニタし、イベントを外部ログサーバまたは IOS syslog に報告します。IOS syslog へのロギングを有効にすると、ログメッセージが大量に発生する可能性があるため、パフォーマンスに影響する場合があります。Snort ログに対応する外部のサードパーティ製のモニタリングツールを、ログの収集と分析に使用できます。

Snort IPS 署名パッケージ

UTD OVA は、ルータのセキュリティライセンスに含まれています。デフォルトでは、ルータにはコミュニティ署名パッケージのみがロードされています。サブスクリプションには次の 2 つのタイプがあります。

- コミュニティ署名パッケージ
- サブスクライバベースの署名パッケージ

コミュニティ署名パッケージのルールセットは、脅威に対する限定的な防御を提供します。サブスクライバベースの署名パッケージのルールセットは、脅威に対する最良の防御を提供します。これには、エクスプロイトの前のカバレッジが含まれているため、セキュリティインシデントまたは新しい脅威のプロアクティブな検出に応じて、更新された署名に最速でアクセスできます。このサブスクリプションはシスコによって完全にサポートされており、パッケージは Cisco.com でアップデートされます。サブスクライバベースの署名パッケージは、ソフトウェアのダウンロードページからダウンロードできます。

ユーザがソフトウェアのダウンロードページから署名パッケージを手動でダウンロードする場合、パッケージのバージョンが Snort エンジンのバージョンと同じであることを確認する必要があります。たとえば、Snort エンジンのバージョンが 2982 の場合、ユーザは同じバージョンの署名パッケージをダウンロードする必要があります。バージョンが一致しないと、署名パッケージのアップデートは拒否され、失敗します。

（注） 署名パッケージがアップデートされると、データプレーンのフェールオープンまたはフェールクローズ設定に応じて、エンジンが再起動され、トラフィックが短時間中断されるか、もしくは検知がバイパスされます。

署名更新でサポートされる Cisco IOS XE のリリースおよび UTD パッケージの最小バージョン

次の表 1 に、Cisco IOS XE の最小リリースと、2020 年 1 月以降の署名パッケージのアップデートに対応する各 UTD パッケージのバージョンを示します。表に示されているものより前の Cisco IOS XE のリリースおよび各 UTD パッケージのバージョンには対応していません。表に記載されているものよりも新しい Cisco IOS XE のリリースおよび各 UTD パッケージのバージョンには、最初のリリースから対応しています。

表 *218 : UTD* 署名パッケージのアップデート対応バージョンのマトリックス

Cisco IOS XE リリース	UTD パッケージのバージョン
16.6.7	1.0.10_SV29111_XE_16_6
16.9.4	1.0.4_SV29111_XE_16_9

Cisco IOS XE リリース	UTD パッケージのバージョン
16.10.2	1.0.9_SV2.9.11.1_XE16.10

（注） UTD がオーバーサブスクライブされると、脅威防御チャネルの状態が緑と赤の間で変化します。UTD データプレーンは、フェールクローズが設定されている場合はそれ以降のすべてのパケットをドロップするか、フェールクローズが設定されていない場合は検査されてないパケットを転送します（デフォルト）。UTD サービスプレーンがオーバーサブスクリプションから回復すると、緑色のステータスで UTD データプレーンに応答します。

Snort IPS ソリューション

Snort IPS ソリューションは、次のエンティティで構成されています。

- Snort センサー：トラフィックをモニタして、設定されたセキュリティポリシー（署名、統計情報、プロトコル分析など）に基づいて異常を検出し、アラートサーバまたはレポートサーバにアラートメッセージを送信します。Snort センサーは、仮想コンテナサービスとしてルータに導入されます。
- 署名ストア：定期的に更新される Cisco 署名パッケージをホストします。これらの署名パッケージは、定期的にもしくはオンデマンドで Snort センサーにダウンロードされます。検証済みの署名パッケージは Cisco.com に掲載されます。設定に基づいて、署名パッケージを Cisco.com またはローカルサーバからダウンロードできます。

  次のドメインは、次の cisco.com から署名パッケージをダウンロードするプロセスにおいてルータによってアクセスされます。

  - api.cisco.com
  - apx.cisco.com
  - cloudsso.cisco.com
  - cloudsso-test.cisco.com
  - cloudsso-test3.cisco.com
  - cloudsso-test4.cisco.com
  - cloudsso-test5.cisco.com
  - cloudsso-test6.cisco.com
  - cloudsso.cisco.com
  - download-ssc.cisco.com
  - dl.cisco.com
  - resolver1.opendns.com
  - resolver2.opendns.com

（注） 署名パッケージを保持するためにローカルサーバから署名パッケージをダウンロードする場合は、HTTP のみに対応します。

Snort センサーが署名パッケージを取得するには、Cisco.com の認証情報を使用して、署名パッケージを Cisco.com からローカルサーバに手動でダウンロードする必要があります。

URL が IP アドレスとして指定されていない場合、Snort コンテナは（ルータに設定された DNS サーバ上で）ドメイン名ルックアップを実行して、Cisco.com によるまたはローカルサーバ上の自動署名更新の場所を解決します 。

- アラートまたはレポートサーバ：Snort センサーからアラートイベントを受信します。Snort センサーによって生成されたアラートイベントは、IOS syslog または外部 syslog サーバ、もしくは IOS syslog と外部 syslog サーバの両方に送信できます。Snort IPS ソリューションに付属している外部ログサーバはありません。
- 管理：Snort IPS ソリューションを管理します。管理は、IOS CLI を使用して設定します。Snort センサーには直接アクセスできず、すべての設定は IOS CLI を使用してのみ行えます。

Snort 仮想サービスインターフェイスの概要

Snort センサーは、ルータ上でサービスとして動作します。サービスコンテナは、仮想テクノロジーを使用して、アプリケーション用の Cisco デバイスにホスティング環境を提供します。

Snort トラフィック検査は、インターフェイス単位で、または対応しているすべてのインターフェイスでグローバルに有効にできます。検査対象のトラフィックは Snort センサーに転送され、再度投入されます。侵入検知システム（IDS）では、識別された脅威がログイベントとして報告され、許可されます。ただし、侵入防止システム（IPS）では、ログイベントとともに攻撃を防ぐためのアクションが実行されます。

Snort センサーには 2 つの VirtualPortGroup インターフェイスが必要です。最初の VirtualPortGroup インターフェイスは管理トラフィックに使用され、2 つ目は転送プレーンと Snort 仮想コンテナサービス間のデータトラフィックに使用されます。これらの VirtualPortGroup インターフェイスには、ゲスト IP アドレスを設定する必要があります。管理 VirtualPortGroup インターフェイスに割り当てられた IP サブネットは、署名サーバおよびアラート / 報告サーバと通信できる必要があります。

2 つ目の VirtualPortGroup インターフェイスの IP サブネットは、このインターフェイス上のトラフィックがルータ内部にあるため、カスタマーネットワーク上でルーティング可能であってはなりません。内部サブネットを外部に公開することはセキュリティ上のリスクとなります。2 つ目の VirtualPortGroup サブネットには 192.0.2.0/30 の IP アドレス範囲を使用することをお勧めします。192.0.2.0/24 のサブネットを使用することは、RFC 3330 で定義されています。

管理トラフィック用の **virtual-service** コマンドを使って管理インターフェイスを使用することもできます。管理インターフェイスを設定する場合、2 つの VirtualPortGroup インターフェイ

スが必要となります。ただし、最初の VirtualPortGroup インターフェイスには **guest ip address** を設定しないでください。

仮想サービスが実行されているルータと同じ管理ネットワークで、Snort 仮想コンテナサービスの IP アドレスを割り当てることができます。この設定は、syslog またはアップデートサーバが管理ネットワーク上にあり、他のインターフェイスからアクセスできない場合に役立ちます。

仮想サービスのリソースプロファイル

Snort IPS 仮想サービスは、低、中、高という 3 つのリソースプロファイルに対応しています。これらのプロファイルは、仮想サービスの実行に必要な CPU およびメモリリソースを表示します。これらのリソースプロファイルの 1 つを設定できます。リソースプロファイルの設定は任意です。プロファイルを設定しない場合、仮想サービスはデフォルトのリソースプロファイルでアクティブ化されます。次の表に、Cisco 4000 シリーズ ISR および Cisco クラウドサービスルータ 1000v シリーズのリソースプロファイルの詳細を示します。

プラットフォーム	プロファイル	仮想サービスのリソース要件		プラットフォーム要件
		システム CPU	メモリ	
Cisco 4321 ISR	デフォルト	50%	最小：1 GB（RAM） 最小：750 MB（ディスクまたはフラッシュ）	最小：8 GB（RAM） 最小：8 GB（ディスクまたはフラッシュ）
Cisco 4331 ISR	低（デフォルト）	25%	最小：1 GB（RAM） 最小：750 MB（ディスクまたはフラッシュ）	最小：8 GB（RAM） 最小：8 GB（ディスクまたはフラッシュ）
	中	50%	最小：2 GB（RAM） 最小：1 GB（ディスクまたはフラッシュ）	最小：8 GB（RAM） 最小：8 GB（ディスクまたはフラッシュ）
	高	75%	最小：4 GB（RAM） 最小：2 GB（ディスクまたはフラッシュ）	最小：8 GB（RAM） 最小：8 GB（ディスクまたはフラッシュ）

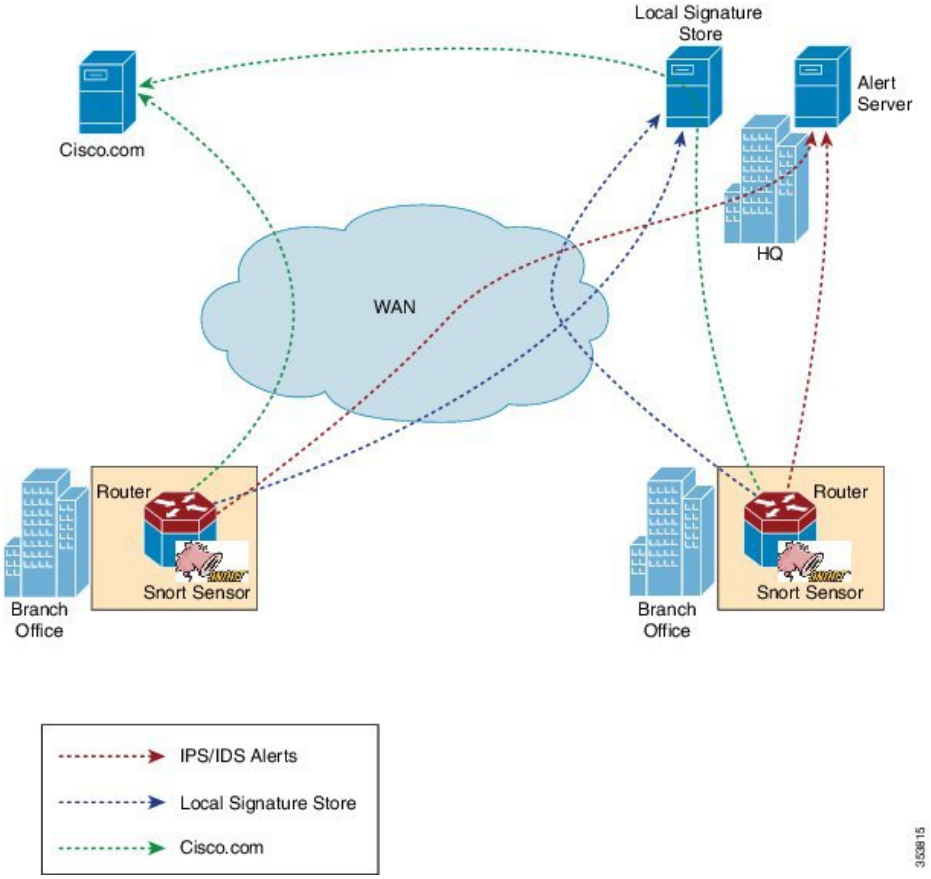
プラットフォーム	プロファイル	仮想サービスのリソース要件		プラットフォーム要件
		システム CPU	メモリ	
Cisco 4351 ISR	低（デフォルト）	25%	最小：1 GB（RAM） 最小：750 MB（ディスクまたはフラッシュ）	最小：8 GB（RAM） 最小：8 GB（ディスクまたはフラッシュ）
	中	50%	最小：2 GB（RAM） 最小：1 GB（ディスクまたはフラッシュ）	最小：8 GB（RAM） 最小：8 GB（ディスクまたはフラッシュ）
	高	75%	最小：4 GB（RAM） 最小：2 GB（ディスクまたはフラッシュ）	最小：8 GB（RAM） 最小：8 GB（ディスクまたはフラッシュ）
Cisco 4431 ISR	低（デフォルト）	25%	最小：1 GB（RAM） 最小：750 MB（ディスクまたはフラッシュ）	最小：8 GB（RAM） 最小：8 GB（ディスクまたはフラッシュ）
	中	50%	最小：2 GB（RAM） 最小：1 GB（ディスクまたはフラッシュ）	最小：8 GB（RAM） 最小：8 GB（ディスクまたはフラッシュ）
	高	75%	最小：4 GB（RAM） 最小：2 GB（ディスクまたはフラッシュ）	最小：12 GB（RAM） 最小：12 GB（ディスクまたはフラッシュ）

プラットフォーム	プロファイル	仮想サービスのリソース要件		プラットフォーム要件
		システム CPU	メモリ	
Cisco 4451 ISR	低（デフォルト）	25%	最小：1 GB（RAM） 最小：750 MB（ディスクまたはフラッシュ）	最小：8 GB（RAM） 最小：8 GB（ディスクまたはフラッシュ）
	中	50%	最小：2 GB（RAM） 最小：1 GB（ディスクまたはフラッシュ）	最小：8 GB（RAM） 最小：8 GB（ディスクまたはフラッシュ）
	高	75%	最小：4 GB（RAM） 最小：2 GB（ディスクまたはフラッシュ）	最小：12 GB（RAM） 最小：12 GB（ディスクまたはフラッシュ）
Cisco CSR 1000V	低（デフォルト）	25%	最小：1 GB（RAM） 最小：750 MB（ディスクまたはフラッシュ）	最小：8 GB（RAM） 最小：8 GB（ディスクまたはフラッシュ）
	中	50%	最小：2 GB（RAM） 最小：1 GB（ディスクまたはフラッシュ）	最小：8 GB（RAM） 最小：8 GB（ディスクまたはフラッシュ）
	高	75%	最小：3 GB（RAM） 最小：2 GB（ディスクまたはフラッシュ）	最小：12 GB（RAM） 最小：12 GB（ディスクまたはフラッシュ）

Snort IPS の導入

次の図は、Snort IPS の導入概要を示しています。

図 *86 : Snort IPS* の展開概要



次の手順では、Snort IPS ソリューションの導入について説明します。

- Snort OVA ファイルを Cisco ルータにコピー、インストール、アクティブ化する。
- 署名パッケージを、Cisco.com または設定済みのローカルサーバから Cisco ルータにダウンロードする。
- ネットワーク侵入検知またはネットワーク防御機能を設定する。
- アラートおよびレポートサーバを、Snort センサーからアラートを受信するように設定する。

Snort IPS の導入方法

対応しているデバイスに Snort IPS を導入するには、次のタスクを実行します。

1. デバイスをプロビジョニングします。

   Snort IPS 機能をインストールするデバイスを特定します。

2. ライセンスを取得します。

Snort IPS 機能は、サービスを有効にするためにセキュリティライセンスを必要とするセキュリティパッケージでのみ使用できます。この機能は、Cisco IOS XE リリース 3.16.1S、3.17S、およびそれ以降のリリースで使用できます。

（注） ライセンスの取得については、シスコ サポートにお問い合わせください。

3. Snort OVA ファイルをインストールします。
4. VirtualPortGroup のインターフェイスおよび仮想サービスを設定します。
5. Snort 仮想コンテナサービスをアクティブにします。
6. Snort IPS または IDS のモードとポリシーを設定します。
7. 外部アラートおよびログサーバまたは IOS syslog、あるいはその両方へのイベントのレポートを設定します。
8. 署名の更新方法を設定します。
9. 署名を更新します。
10. IPS をグローバルに、または必要なインターフェイスで有効にします。

Snort OVA ファイルのインストール

OVA ファイルは、仮想マシンの圧縮された「インストール可能な」バージョンを含むオープン仮想アーカイブ（Open Virtualization Archive）です。Snort IPS は仮想コンテナサービスとして使用できます。この OVA ファイルをルータにダウンロードし、**virtual-service install** CLI を使用してサービスをインストールする必要があります。

サービス OVA ファイルは、ルータにインストールされている Cisco IOS XE リリースイメージには付属していません。ただし、OVA ファイルはルータのフラッシュに事前にインストールされている場合があります。

セキュリティライセンスが付属した Cisco IOS XE イメージを使用する必要があります。OVA ファイルのインストール中に、セキュリティライセンスがチェックされ、ライセンスが存在しない場合はエラーが報告されます。

手順の概要

1. **enable**
2. **virtual-service install name** *virtual-service-name* **package** *file-url* **media** *file-system*
3. **show virtual-service list**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。

	コマンドまたはアクション	目的
ステップ 2	**virtual-service install name** *virtual-service-name* **package** *file-url* **media** *file-system* 例： `Device# virtual-service install name UTDIPS package harddisk:utd-ips-v102.ova media harddisk:`	デバイスの仮想サービスコンテナにアプリケーションをインストールします。 • 名前の長さは 20 文字です。ハイフン（-）は有効な文字ではありません。 • インストールする OVA パッケージの完全パスを指定する必要があります。 （注） OVA のインストールは、ハードディスクとブートフラッシュの両方で行えますが、OVA をインストールするのに推奨されるファイルシステムはハードディスクです。
ステップ 3	**show virtual-service list** 例： `Device# show virtual-service list`	仮想サービスコンテナにインストールされているすべてのアプリケーションのインストールのステータスを表示します。

VirtualPortGroup のインターフェイスおよび仮想サービスの設定

2 つの VirtualPortGroup インターフェイスと両方のインターフェイスのゲスト IP アドレスを設定する必要があります。ただし、 **vnic management GigabitEthernet0** コマンドを使用して管理インターフェイスを設定する場合は、最初の VirtualPortGroup インターフェイスのゲスト IP アドレスを設定しないでください。

（注） データトラフィック用の VirtualPortGroup インターフェイスは、プライベートまたはルーティング不可の IP アドレスを使用する必要があります。このインターフェイスには、IP アドレスの範囲として 192.0.2.0 / 30を 使用することを推奨します。

（注） Cisco IOS ソフトウェアイメージを XE 3.x バージョンから XE 16.2.1 に、または XE 16.2.1 から XE 3.x バージョンに変更する前に、デバイス上の仮想サービスごとに **virtual-service uninstall name [name]** コマンドを使用して仮想サービスをアンインストールします。仮想サービスの 1 つが ISR-WAAS サービスであり、**service waas enable** コマンドを使用してインストールされている場合は、**service waas disable** コマンドを使用します。

Cisco IOS ソフトウェアイメージの新しいバージョンでデバイスをアップグレードした後、仮想サービスを再インストールします。ISR-WAAS の場合は **service wass enable** コマンドを使用し、その他の仮想サービスの場合は **virtual-service install name [name] package [.ova file]** コマンドを使用します。

手順の概要

1. **enable**
2. **configure terminal**
3. **interface** *VirtualPortGroup number*
4. **ip address** *ip-address mask*
5. **exit**
6. **interface** *type number*
7. **ip address** *ip-address mask*
8. **exit**
9. **virtual-service** *name*
10. **profile** *profile-name*
11. **vnic gateway VirtualPortGroup** *interface-number*
12. **guest ip address** *ip-address*
13. **exit**
14. **vnic gateway VirtualPortGroup** *interface-number*
15. **guest ip address** *ip-address*
16. **exit**
17. **vnic management GigabitEthernet0**
18. **guest ip address** *ip-address*
19. **exit**
20. **activate**
21. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface** *VirtualPortGroup number* 例： `Device(config)# interface VirtualPortGroup 0`	インターフェイスを設定し、インターフェイス設定モードを開始します。 • VirtualPortGroup インターフェイスを設定します。このインターフェイスは、管理インターフェイスの GigabitEthernet0 が使用されていない場合に管理トラフィックに対して使用されます。
ステップ 4	**ip address** *ip-address mask* 例：	インターフェイスのプライマリ IP アドレスを設定します。このインターフェイスは、署名アップデー

	コマンドまたはアクション	目的
	`Device(config-if)# ip address 10.1.1.1 255.255.255.252`	トサーバおよび外部ログサーバにルーティング可能である必要があります。
ステップ 5	**exit** 例： `Device(config-if)# exit`	インターフェイス設定モードを終了し、グローバル設定モードに戻ります。
ステップ 6	**interface** *type number* 例： `Device(config)# interface VirtualPortGroup 1`	インターフェイスを設定し、インターフェイス コンフィギュレーション モードを開始します。 • VirtualPortGroup インターフェイスを設定します。 • このインターフェイスは、データトラフィックに使用されます。
ステップ 7	**ip address** *ip-address mask* 例： `Device(config-if)# ip address 192.0.2.1 255.255.255.252`	インターフェイスのプライマリ IP アドレスを設定します。 • この IP アドレスは、外部ネットワークに対してルーティング不能である必要があります。 • IP アドレスは、推奨される 192.0.2.0/30 のサブネットから割り当てられます。
ステップ 8	**exit** 例： `Device(config-if)# exit`	インターフェイス コンフィギュレーション モードを終了し、グローバルコンフィギュレーションモードに戻ります。
ステップ 9	**virtual-service** *name* 例： `Device(config)# virtual-service UTDIPS`	仮想コンテナサービスを設定し、仮想サービス設定モードに入ります。 • *name* 引数は、仮想コンテナサービスを識別するために使用される論理名です。

ステップ 10	**profile** *profile-name*
	例：
	`Device(config-virt-serv)#profile high`
	例：
	`Device(config-virt-serv)#profile multi-tenancy`
		（オプション）リソースプロファイルを設定します。リソースプロファイルを設定しない場合、仮想サービスはデフォルトのリソースプロファイルを使用してアクティブ化されます。オプションは、low、medium、high、および multi-tenancy です。（マルチテナントモードの場合（Cisco CSR 1000v のみ）、`profile multi-tenancy` コマンドを設定する必要があります。

ステップ 11	**vnic gateway VirtualPortGroup** *interface-number* 例： `Device(config-virt-serv)# vnic gateway VirtualPortGroup 0`	仮想コンテナサービスの仮想ネットワーク インターフェイス カード（vNIC）のゲートウェイ インターフェイスを作成し、vNIC ゲートウェイ インターフェイスを仮想ポートグループにマッピングして、仮想サービスの vNIC 設定モードに入ります。

	コマンドまたはアクション	目的
		• このコマンドで参照されるインターフェイスは、手順3で設定したインターフェイスである必要があります。このコマンドは、管理目的で使用されるインターフェイスをマッピングします。
ステップ 12	**guest ip address** *ip-address* 例： `Device(config-virt-serv-vnic)# guest ip address 10.1.1.2`	（オプション）vNIC ゲートウェイ インターフェイスのゲスト vNIC アドレスを設定します。 • （注） 手順 17 で指定した **vnic management gigabitethernet0** コマンドが設定されていない場合にのみこのコマンドを設定します。
ステップ 13	**exit** 例： `Device(config-virt-serv-vnic)# exit`	仮想サービスの vNIC 設定モードを終了し、仮想サービス設定モードに戻ります。
ステップ 14	**vnic gateway VirtualPortGroup** *interface-number* 例： `Device(config-virt-serv)# vnic gateway VirtualPortGroup 1`	仮想コンテナサービスの vNIC ゲートウェイ インターフェイスを作成し、vNIC ゲートウェイ インターフェイスを仮想ポートグループにマッピングして、仮想サービスの vNIC 設定モードに入ります。 • このコマンドで参照されるインターフェイスは、手順6で設定したインターフェイスである必要があります。このコマンドは、Snortがユーザトラフィックのモニタリングに使用する仮想コンテナサービスのインターフェイスをマッピングします。
ステップ 15	**guest ip address** *ip-address* 例： `Device(config-virt-serv-vnic)# guest ip address 192.0.2.2`	vNIC ゲートウェイ インターフェイスのゲスト vNIC アドレスを設定します。
ステップ 16	**exit** 例： `Device(config-virt-serv-vnic)# exit`	仮想サービスの vNIC 設定モードを終了し、仮想サービス設定モードに戻ります。
ステップ 17	**vnic management GigabitEthernet0** 例： `Device(config-virt-serv)# vnic management GigabitEthernet0`	（オプション）GigabitEthernet インターフェイスを vNIC 管理インターフェイスとして設定します。 • 管理インターフェイスは、VirtualPortGroup インターフェイスまたはGibugitEthernet0インターフェイスである必要があります。

	コマンドまたはアクション	目的
		• **vnic management GigabitEthernet0** コマンドを設定しない場合は、手順 12 で指定した **guest ip address** コマンドを設定する必要があります。
ステップ 18	**guest ip address** *ip-address* 例： `Device(config-virt-serv-vnic)# guest ip address 209.165.201.1`	（オプション）vNIC 管理インターフェイスのゲスト vNIC アドレスを設定します。このアドレスは、管理インターフェイスおよび GigabitEthernet0 設定と同じサブネット内にある必要があります。
ステップ 19	**exit** 例： `Device(config-virt-serv-vnic)# exit`	仮想サービスの vNIC 設定モードを終了し、仮想サービス設定モードに戻ります。
ステップ 20	**activate** 例： `Device(config-virt-serv)# activate`	仮想コンテナサービスにインストールされたアプリケーションをアクティブにします。
ステップ 21	**end** 例： `Device(config-virt-serv)# end`	仮想サービス設定モードを終了し、特権 EXEC モードに戻ります。

Snort IPS のグローバル設定

要件に基づいて、侵入防止システム（IPS）または侵入検知システム（IDS）の検査をグローバルレベルまたはインターフェイスで設定します。このタスクを実行して、デバイス上で IPS をグローバルに設定します。

（注） グローバルという用語は、対応しているすべてのインターフェイスで実行されている Snort IPS を意味します。

手順の概要

1. **enable**
2. **configure terminal**
3. **utd threat-inspection whitelist**
4. **generator id** *generator-id* **signature id** *signature-id* [**comment** *description*]
5. **exit**
6. **utd engine standard**
7. **logging** {**host** *hostname* | **syslog**}
8. **threat-inspection**

9. **threat** {**detection** | **protection** }
10. **policy** {**balanced** | **connectivity** | **security**}
11. **whitelist**
12. **signature update occur-at** {**daily** | **monthly** *day-of-month* | **weekly** *day-of-week*} *hour minute*
13. **signature update server** {**cisco** | **url** *url* } [**username** *username* [**password** *password*]]
14. **logging level** {**alert** | **crit** | **debug** | **emerg** | **err** | **info** | **notice** | **warning**}
15. **exit**
16. **utd**
17. **redirect interface virtualPortGroup** *interface-number*
18. **all-interfaces**
19. **engine standard**
20. **fail close**
21. **exit**
22. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル設定モードを開始します。
ステップ 3	**utd threat-inspection whitelist** 例： `Device(config)# utd threat-inspection whitelist`	（オプション）UTD 許可リストの設定モードを有効にします。
ステップ 4	**generator id** *generator-id* **signature id** *signature-id* [**comment** *description*] 例： `Device(config-utd-whitelist)# generator id 24 signature id 24245 comment traffic from branchoffice1`	署名 ID を許可リストに表示するように設定します。 • 署名 IDは、抑制する必要があるアラートからコピーできます。 • 複数の署名 ID を設定できます。 • 許可リストに追加する必要がある署名 ID ごとに、この手順を繰り返します。
ステップ 5	**exit** 例： `Device(config-utd-whitelist)# exit`	UTD 許可リストの設定モードを終了して、グローバル設定モードに戻ります。

	コマンドまたはアクション	目的
ステップ 6	**utd engine standard** 例： `Device(config)# utd engine standard`	統合脅威防御（UTD）標準エンジンを設定し、UTD 標準エンジンの設定モードに入ります。
ステップ 7	**logging** {**host** *hostname* | **syslog**} 例： `Device(config-utd-eng-std)# logging host syslog.yourcompany.com`	サーバへの緊急メッセージのロギングを有効にします。
ステップ 8	**threat-inspection** 例： `Device(config-utd-eng-std)# threat-inspection`	Snort エンジンの脅威検知を設定します。
ステップ 9	**threat** {**detection** | **protection** } 例： `Device(config-utd-eng-std-insp)# threat protection`	脅威検知または侵入防止システム（IPS）を Snort エンジンの動作モードとして設定します。 • デフォルトは**detection**です。 • 侵入検知システム（IDS）を設定するには、**detection** キーワードを設定します。
ステップ 10	**policy** {**balanced** | **connectivity** | **security**} 例： `Device(config-utd-eng-std-insp)# policy security`	Snort エンジンのセキュリティポリシーを設定します。 • デフォルトのポリシーオプションは **balanced** です。
ステップ 11	**whitelist** 例： `Device(config-utd-eng-std-insp)# whitelist`	（オプション）UTD エンジンで許可リストを有効にします。
ステップ 12	**signature update occur-at** {**daily** | **monthly** *day-of-month* | **weekly** *day-of-week*} *hour minute* 例： `Device(config-utd-eng-std-insp)# signature update occur-at daily 0 0`	署名の更新間隔パラメータを設定します。この設定をすることで、午前0時に署名の更新がトリガーされます。
ステップ 13	**signature update server** {**cisco** | **url** *url* } [**username** *username* [**password** *password*]] 例： `Device(config-utd-eng-std-insp)# signature update server cisco username abcd password cisco123`	署名更新サーバのパラメータを設定します。サーバの詳細で署名更新パラメータを指定する必要があります。署名の更新にCisco.comを使用する場合は、ユーザ名とパスワードを入力する必要があります。署名の更新にローカルサーバを使用する場合は、サーバ設定に基づいてユーザ名とパスワードを指定できます。

	コマンドまたはアクション	目的
ステップ 14	**logging level** {**alert** | **crit** | **debug** | **emerg** | **err** | **info** | **notice** | **warning**} 例： `Device(config-utd-eng-std-insp)# logging level emerg`	ログレベルを有効にします。
ステップ 15	**exit** 例： `Device(config-utd-eng-std-insp)# exit`	UTD標準エンジンの設定モードを終了して、グローバル設定モードに戻ります。
ステップ 16	**utd** 例： `Device(config)# utd`	統合脅威防御（UTD）を有効にし、UTD 設定モードに入ります。
ステップ 17	**redirect interface virtualPortGroup** *interface-number* 例： `Device(config-utd)# redirect interface virtualPortGroup 1`	（オプション）VirtualPortGroup インターフェイスにリダイレクトします。これはデータ トラフィック インターフェイスです。このインターフェイスを設定しない場合、インターフェイスは自動検出されます。
ステップ 18	**all-interfaces** 例： `Device(config-utd)# all-interfaces`	デバイスのすべてのレイヤ 3 インターフェイスで UTD を設定します。
ステップ 19	**engine standard** 例： `Device(config-utd)# engine standard`	統合脅威防御（UTD）エンジンを設定し、標準エンジンの設定モードに入ります。
ステップ 20	**fail close** 例： `Device(config-engine-std)# fail close`	（オプション）UTD エンジンに障害が発生した場合に行うアクションを定義します。デフォルトのオプションはフェールオープンです。フェールクローズオプションは、UTD エンジンに障害が発生した場合にすべての IPS または IDS トラフィックをドロップします。フェールオープンオプションを使用すると、UTD エンジンに障害が発生した場合にすべての IPS または IDS トラフィックを許可します。
ステップ 21	**exit** 例： `Device(config-eng-std)# exit`	標準エンジンの設定モードを終了して、グローバル設定モードに戻ります。
ステップ 22	**end** 例： `Device(config-utd)# end`	UTD 設定モードを終了して、グローバル設定モードに戻ります。

Snort IDS 検知のグローバル設定

要件に基づいて、侵入防止システム（IPS）または侵入検知システム（IDS）検査をグローバルレベルまたはインターフェイスレベルで設定します。インターフェイスごとにIDSを設定するには、次のタスクを実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **utd enable**
5. **exit**
6. 検査が必要なすべてのインターフェイスで、手順 3 ー 5 を繰り返します。
7. **utd threat-inspection whitelist**
8. **generator id** *generator-id* **signature id** *signature-id* [**comment** *description*]
9. **exit**
10. **utd engine standard**
11. **logging** {**host** *hostname* | **syslog**}
12. **threat-inspection**
13. **threat** {**detection** | **protection** }
14. **policy** {**balanced** | **connectivity** | **security**}
15. **whitelist**
16. **signature update occur-at** {**daily** | **monthly** *day-of-month* | **weekly** *day-of-week*} *hour minute*
17. **signature update server** {**cisco** | **url** *url*} [**username** *username* [**password** *password*]]
18. **logging level** {**alert** | **crit** | **debug** | **emerg** | **err** | **info** | **notice** | **warning**}
19. **exit**
20. **utd**
21. **redirect interface virtualPortGroup** *interface-number*
22. **engine standard**
23. **fail close**
24. **exit**
25. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 3	**interface** *type number* 例： `Device(config)# interface gigabitethernet 0/0/0`	インターフェイスを設定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	**utd enable** 例： `Device(config-if)# utd enable`	統合脅威防御（UTD）を有効にします。
ステップ 5	**exit** 例： `Device(config-if)# exit`	インターフェイス設定モードを終了し、グローバル設定モードに戻ります。
ステップ 6	検査が必要なすべてのインターフェイスで、手順 3 ー 5 を繰り返します。	–
ステップ 7	**utd threat-inspection whitelist** 例： `Device(config)# utd threat-inspection whitelist`	（オプション）UTD 許可リストの設定モードを有効にします。
ステップ 8	**generator id** *generator-id* **signature id** *signature-id* [**comment** *description*] 例： `Device(config-utd-whitelist)# generator id 24 signature id 24245 comment traffic from branchoffice1`	署名 ID を許可リストで表示するように設定します。 • 署名 IDは、抑制する必要があるアラートからコピーできます。 • 複数の署名 ID を設定できます。 • 許可リストに表示する必要がある署名 ID ごとに、この手順を繰り返します。
ステップ 9	**exit** 例： `Device(config-utd-whitelist)# exit`	UTD 許可リストの設定モードを終了して、グローバル設定モードに戻ります。
ステップ 10	**utd engine standard** 例： `Device(config)# utd engine standard`	統合脅威防御（UTD）標準エンジンを設定し、UTD 標準エンジンの設定モードに入ります。
ステップ 11	**logging** {**host** *hostname* | **syslog**} 例： `Device(config-utd-eng-std)# logging syslog`	IOSd syslog への重要なメッセージのロギングを有効にします。
ステップ 12	**threat-inspection** 例： `Device(config-utd-eng-std)# threat-inspection`	Snort エンジンの脅威検知を設定します。

	コマンドまたはアクション	目的
ステップ 13	**threat** {**detection** | **protection** } 例： `Device(config-utd-eng-std-insp)# threat detection`	脅威防止または侵入検知システム（IDS）を Snort センサーの動作モードとして設定します。 • 侵入防止システム（IPS）を設定するには、**protection** キーワードを設定します。
ステップ 14	**policy** {**balanced** | **connectivity** | **security**} 例： `Device(config-utd-eng-std-insp)# policy balanced`	Snort センサーのセキュリティポリシーを設定します。
ステップ 15	**whitelist** 例： `Device(config-utd-eng-std-insp)# whitelist`	（オプション）トラフィックの許可リストを有効にします。
ステップ 16	**signature update occur-at** {**daily** | **monthly** *day-of-month* | **weekly** *day-of-week*} *hour minute* 例： `Device(config-utd-eng-std-insp)# signature update occur-at daily 0 0`	署名の更新間隔パラメータを設定します。この設定をすることで、午前0時に署名の更新がトリガーされます。
ステップ 17	**signature update server** {**cisco** | **url** *url*} [**username** *username* [**password** *password*]] 例： `Device(config-utd-eng-std-insp)# signature update server cisco username abcd password cisco123`	署名更新サーバのパラメータを設定します。サーバの詳細で署名更新パラメータを指定する必要があります。署名の更新にCisco.comを使用する場合は、ユーザ名とパスワードを入力する必要があります。署名の更新にローカルサーバを使用する場合は、サーバ設定に基づいてユーザ名とパスワードを指定できます。
ステップ 18	**logging level** {**alert** | **crit** | **debug** | **emerg** | **err** | **info** | **notice** | **warning**} 例： `Device(config-utd-eng-std-insp)# logging level crit`	ログレベルを有効にします。
ステップ 19	**exit** 例： `Device(config-utd-eng-std-insp)# exit`	UTD標準エンジンの設定モードを終了して、グローバル設定モードに戻ります。
ステップ 20	**utd** 例： `Device(config)# utd`	統合脅威防御（UTD）を有効にし、UTD 設定モードに入ります。
ステップ 21	**redirect interface virtualPortGroup** *interface-number* 例：	（オプション）VirtualPortGroup インターフェイスにリダイレクトします。これはデータ トラフィック インターフェイスです。このインターフェイス

	コマンドまたはアクション	目的
	`Device(config-utd)# redirect interface virtualPortGroup 1`	を設定しない場合、インターフェイスは自動検出されます。
ステップ 22	**engine standard** 例： `Device(config-utd)# engine standard`	統合脅威防御（UTD）エンジンを設定し、標準エンジンの設定モードに入ります。
ステップ 23	**fail close** 例： `Device(config-engine-std)# fail close`	（オプション）UTD エンジンに障害が発生した場合に行うアクションを定義します。デフォルトのオプションはフェールオープンです。フェールクローズオプションは、UTD エンジンに障害が発生した場合にすべての IPS または IDS トラフィックをドロップします。フェールオープンオプションを使用すると、UTD エンジンに障害が発生した場合にすべての IPS または IDS トラフィックを許可します。
ステップ 24	**exit** 例： `Device(config-eng-std)# exit`	標準エンジンの設定モードを終了して、グローバル設定モードに戻ります。
ステップ 25	**end** 例： `Device(config-utd)# end`	設定モードを終了し、EXEC モードに戻ります。

アクティブな署名のリストの表示

アクティブな署名は、Snort IDS または IPS に脅威に対するアクションを実行するように指示するものです。トラフィックがアクティブな署名のいずれかと一致した場合、Snort コンテナは IDS モードでアラートをトリガーし、IPS モードでトラフィックをドロップします。

utd threat-inspection signature active-list write-to bootflash: file nameコマンドは、アクティブな署名のリストと、アクティブな署名、ドロップ署名、およびアラート署名の合計数のサマリーを表示します。

コンテナの正常性をモニタリングするための Quality of Service（QoS）ポリシーの設定

コンテナの正常性をモニタリングする正常性プローブが高いトラフィックレートで影響を受けないように、Quality of Service（QoS）ポリシーを設定することをお勧めします。

手順の概要

1. **ip access-list extended** {acl-name | acl-number}

2. sequence-number permit protocol source *source-wildcard destination destination-wildcard* [precedence] [tos *tos* tos] [log] [time-range*time-range-name*] [fragments]
3. **exit**
4. class-map { [type inspect match-all] | [match-any] } *class-map-name*
5. match access-group { *access-group* | name *access-group-name*}
6. **exit**
7. policy-map *policy-map-name*
8. class {*class-name* | class-default
9. priority level *level*
10. **exit**
11. **interface** *type number*
12. service-policy [history | {output} *policy-map-name* | type control *control-policy-name*]
13. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**ip access-list extended** {acl-name | acl-number} 例： `Device(config)# ip access-list extended health_probes_accesslist`	拡張 ACL コンフィギュレーション モードを有効にします。CLI は拡張 ACL コンフィギュレーション モードを開始します。このモードでは、後続のすべてのコマンドが現在の拡張アクセスリストに適用されます。
ステップ 2	sequence-number permit protocol source *source-wildcard destination destination-wildcard* [precedence] [tos *tos* tos] [log] [time-range*time-range-name*] [fragments] 例： `Device(config-ext-nacl)# 10 permit udp any eq 3367 any eq 3367`	名前付き IP アクセス リスト モードで permit ステートメントを指定します。このアクセスリストでは、**permit** ステートメントを最初に使用していますが、必要なステートメントの順序に応じて、**deny** ステートメントが最初に使用される可能性もあります。
ステップ 3	**exit** 例： `Device(config-ext-nacl)# exit`	拡張 ACL コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードに戻ります。
ステップ 4	class-map { [type inspect match-all] | [match-any] } *class-map-name* 例： `Device(config)# class-map match-all health_probes_cmap`	作成するクラス マップの名前を指定し、QoS クラス マップ コンフィギュレーション モードを開始します。
ステップ 5	match access-group { *access-group* | name *access-group-name*} 例： `Device(config-cmap)# match access-group name health_probes_accesslist`	すべてのパケットに対して適切に一致する基準となる、クラスマップの一致基準を設定します。

	コマンドまたはアクション	目的
ステップ 6	**exit** 例： `Device(config-cmap)# exit`	クラス マップ コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードに戻ります。
ステップ 7	policy-map *policy-map-name* 例： `Device(config)# policy-map health_probes_pmap`	サービス ポリシーを指定するために 1 つ以上のインターフェイスに適用可能なポリシー マップを作成または修正し、QoS ポリシーマップ コンフィギュレーション モードを開始します。
ステップ 8	class {*class-name* | class-default 例： `Device(config-pmap)# class health_probes_cmap`	クラスのポリシーを設定する前に、ポリシーの作成/変更対象となるクラスの名前を指定するか、（一般に class-default クラスと呼ばれる）デフォルト クラスを指定してから、ポリシーマップ コンフィギュレーション モードを開始します。
ステップ 9	priority level *level* 例： `Device(config-pmap)# priority level 1`	指定されたプライオリティ レベルでトラフィック クラスにプライオリティを割り当てます。 • プライオリティ クラスに割り当てられた優先順位の値を入力します。有効な値は、1（高優先順位）または2（低優先順位）です。デフォルトは 1 です。
ステップ 10	**exit** 例： `Device(config-pmap)# exit`	ポリシーマップ コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードに戻ります。
ステップ 11	**interface** *type number* 例： `Device(config)# interface VirtualPortGroup 1`	インターフェイスを設定し、インターフェイス コンフィギュレーション モードを開始します。 • VirtualPortGroup インターフェイスを設定します。 • このインターフェイスは、データトラフィックに使用されます。
ステップ 12	service-policy [history | {output} *policy-map-name* | type control *control-policy-name*] 例： `Device(config-if)# service-policy output health_probes_pmap`	ポリシー マップをクラスに結合します。適用されるサービス ポリシー マップ（**policy-map** コマンドを使用して作成）の名前。名前には最大 40 文字までの英数字を指定できます。
ステップ 13	**end** 例： `Device(config-if)# end`	インターフェイス コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

Snort IPS の設定例

例：VirtualPortGroup インターフェイスおよび仮想サービスの設定

```
Device# configure terminal
Device(config)# interface VirtualPortGroup 0
Device(config-if)# ip address 10.1.1.1 255.255.255.252
Device(config-if)# exit
Device(config)# interface VirtualPortGroup 1
Device(config-if)# ip address 192.0.2.1 255.255.255.252
Device(config-if)# exit
Device(config)# virtual-service UTDIPS
Device(config-virt-serv)# vnic gateway VirtualPortGroup 0
Device(config-virt-serv-vnic)# exit
Device(config-virt-serv)# vnic gateway VirtualPortGroup 1
Device(config-virt-serv-vnic)# guest ip address 192.0.2.2
Device(config-virt-serv-vnic)# exit
Device(config-virt-serv)# vnic management GigabitEthernet0
Device(config-virt-serv-vnic)# guest ip address 209.165.201.1
Device(config-virt-serv-vnic)# exit
Device(config-virt-serv)# activate
Device(config-virt-serv-vnic)# end
```

例：異なるリソースプロファイルの設定

```
Device# configure terminal
Device(config)# virtual-service UTDIPS
Device(config-virt-serv)# no activate
Device(config-virt-serv)# end
Device# virtual-service uninstall name UTDIPS
Device# configure terminal
Device(config)# virtual-service UTDIPS
Device(config-virt-serv)# profile medium
Device(config-virt-serv)# end
Device# virtual-service install name UTDIPS package:utd.ova
Device# configure terminal
Device(config)# virtual-service UTDIPS
Device(config-virt-serv)# activate
Device(config-virt-serv)# end
```

例：Snort IPS のグローバル設定

次に、デバイス上で侵入防止システム（IPS）をグローバルに設定する例を示します。

```
Device# configure terminal
Device(config)# utd engine standard
Device(config-utd-eng-std)# threat-inspection
Device(config-utd-eng-std-insp)# threat protection
Device(config-utd-eng-std-insp)# policy security
```

```
Device(config-utd-eng-std)# exit
Device(config)# utd
Device(config-utd)# all-interfaces
Device(config-utd)# engine standard
Device(config-utd-whitelist)# end
Device#
```

例：インターフェイスごとの Snort IPS 検査の設定

次に、インターフェイスごとに Snort 侵入検知システム（IDS）を設定する例を示します。

```
Device# configure terminal
Device(config)# utd engine standard
Device(config-utd-eng-std)# threat-inspection
Device(config-utd-eng-std-insp)# threat detection
Device(config-utd-eng-std-insp)# policy security
Device(config-utd-eng-std)# exit
Device(config)# utd
Device(config-utd)# engine standard
Device(config-eng-std)# exit
Device(config)# interface gigabitethernet 0/0/0
Device(config-if)# utd enable
Device(config-if)# exit
```

例：インバウンドインターフェイスとアウトバウンドインターフェイスの両方での VRF を使用した UTD の設定

```
Device# configure terminal
Device(config)# vrf definition VRF1
Device(config-vrf)# rd 100:1
Device(config-vrf)# route-target export 100:1
Device(config-vrf)# route-target import 100:1
Device(config-vrf)# route-target import 100:2
!
Device(config-vrf)# address-family ipv4
Device(config-vrf-af)# exit
!
Device(config-vrf)# address-family ipv6
Device(config-vrf-af)# exit
!
Device(config-vrf-af)# vrf definition VRF2
Device(config-vrf)# rd 100:2
Device(config-vrf)# route-target export 100:2
Device(config-vrf)# route-target import 100:2
Device(config-vrf)# route-target import 100:1
!
Device(config-vrf)# address-family ipv4
Device(config-vrf-af)# exit
!
Device(config-vrf)# address-family ipv6
Device(config-vrf-af)# exit
!
Device(config-vrf)# interface VirtualPortGroup0
Device(config-if)# ip address 192.0.2.1 255.255.255.252
```

```
Device(config-if)# no mop enabled
Device(config-if)# no mop sysid
!
Device(config-if)# interface VirtualPortGroup1
Device(config-if)# ip address 192.0.2.5 255.255.255.252
Device(config-if)# no mop enabled
Device(config-if)# no mop sysid
!
Device(config-if)# interface GigabitEthernet0/0/2
Device(config-if)# vrf forwarding VRF1
Device(config-if-vrf)# ip address 192.1.1.5 255.255.255.0
Device(config-if-vrf)# ipv6 address A000::1/64
!
Device(config-if)# interface GigabitEthernet0/0/3
Device(config-if)# vrf forwarding VRF2
Device(config-if-vrf)# ip address 192.1.1.5 255.255.255.0
Device(config-if-vrf)# ipv6 address B000::1/64
!
Device(config-if-vrf)# router bgp 100
Device(config-if-vrf)# bgp log-neighbor-changes
!
Device(config-vrf)# address-family ipv4 vrf VRF1
Device(config-vrf-af)# redistribute connected
Device(config-vrf-af)# redistribute static
Device(config-vrf-af)# exit
!
Device(config-vrf)# address-family ipv6 vrf VRF1
Device(config-vrf-af)# redistribute connected
Device(config-vrf-af)# redistribute static
Device(config-vrf-af)# exit
!
Device(config-vrf)# address-family ipv4 vrf VRF2
Device(config-vrf-af)# redistribute connected
Device(config-vrf-af)# redistribute static
Device(config-vrf-af)# exit
!
Device(config-vrf)# address-family ipv6 vrf VRF2
Device(config-vrf-af)# redistribute connected
Device(config-vrf-af)# redistribute static
Device(config-vrf-af)# exit
!
Device(config)# utd
Device(config-utd)# all-interfaces
Device(config-utd)# engine standard
Device(config-utd)# exit

Device(config)# utd engine standard
Device(config-utd-eng-std)# logging syslog
Device(config-utd-eng-std)# threat-inspection
Device(config-utd-engstd-insp)# threat protection
Device(config-utd-engstd-insp)# policy security
Device(config-utd-engstd-insp)# exist
Device(config-utd-eng-std)# exit
!
Device(config)# virtual-service utd
Device(config-virt-serv)# profile low
Device(config-virt-serv)# vnic gateway VirtualPortGroup0
Device(config-virt-serv-vnic)# guest ip address 192.0.2.2
Device(config-virt-serv-vnic)# exit
Device(config-virt-serv)# vnic gateway VirtualPortGroup1
Device(config-virt-serv-vnic)# guest ip address 192.0.2.6
Device(config-virt-serv-vnic)# exit
Device(config-virt-serv)# activate
```

```
UTD Snort IPS Drop Log
============================
2016/06/13-14:32:09.524475 IST [**] [Instance_ID: 1] [**] Drop [**]
[1:30561:1] BLACKLIST DNS request for known malware
domain domai.ddns2.biz - Win.Trojan.Beebone [**]
[Classification: A Network Trojan was Detected]
[Priority: 1] [VRF_ID: 2] {UDP} 11.1.1.10:58016 -> 21.1.1.10:53
```

例：IOS Syslog のロギングの設定

次に、デバイスのログレベルを使用して IOS syslog のロギングを設定する例を示します。

```
Device# configure terminal
Device(config)# utd engine standard
Device(config-utd-eng-std)# logging syslog
Device(config-utd-eng-std)# threat-inspection
Device(config-utd-engstd-insp)# logging level debug
Device(config-utd-eng-std-insp)# end
Device#
```

例：中央集中型ログサーバへのロギングの設定

次の例は、中央集中型ログサーバへのロギングの設定方法を示しています。

```
Device# configure terminal
Device(config)# utd engine standard
Device(config-utd-eng-std-insp)# logging host syslog.yourcompany.com
Device(config-utd-eng-std)# threat-inspection
Device(config-utd-eng-std-insp)# logging level info
Device(config-utd-eng-std-insp)# end
Device#
```

例：Cisco サーバからの署名更新の設定

次の例は、Cisco サーバから署名の更新を設定する方法を示しています。

```
Device# configure terminal
Device(config)# utd engine standard
Device(config-utd-eng-std)# threat-inspection
Device(config-utd-eng-std-insp)# signature update server cisco username CCOuser password
 passwd123
Device(config-utd-eng-std-insp)# end
Device#
```

（注） DNS が Cisco サーバから署名をダウンロードするように設定されていることを確認します。

例：ローカルサーバからの署名更新の設定

次の例は、ローカルサーバから署名の更新を設定する方法を示しています。

```
Device# configure terminal
Device(config)# utd engine standard
Device(config-utd-eng-std)# threat-inspection
Device(config-utd-eng-std-insp)# signature update server url http://192.168.1.2/sig-1.pkg
Device(config-utd-eng-std-insp)# end
Device#
```

例：自動署名更新の設定

次の例は、サーバで自動署名更新を設定する方法を示しています。

```
Device# configure terminal
Device(config)# utd engine standard
Device(config-utd-eng-std)# threat-inspection
Device(config-utd-eng-std-insp)# signature update occur-at daily 0 0
Device(config-utd-eng-std-insp)# signature update server cisco username abcd password
cisco123
Device(config-utd-eng-std-insp)# end
Device#
```

例：手動による署名の更新の実行

次の例は、さまざまな方法で手動で署名を更新する方法を示しています。

```
Device# utd threat-inspection signature update
```

既存のサーバ設定をダウンロードするか、既存のサーバ設定を使用して設定された明示的なサーバ情報を取得します。これらのコマンドにより、次の設定を使用して手動で署名更新が実行されます。

```
Device# show utd engine standard threat-inspection signature update status

Current signature package version: 2983.4.s
Current signature package name: UTD-STD-SIGNATURE-2983-4-S.pkg
Previous signature package version: 29.0.c
----------------------------------------
Last update status: Successful
----------------------------------------
Last successful update time: Mon Aug  7 02:02:32 2017 UTC
Last successful update method: Manual
Last successful update server: cisco
Last successful update speed: 3022328 bytes in 25 secs
----------------------------------------
Last failed update time: Mon Aug  7 01:53:21 2017 UTC
Last failed update method: Manual
Last failed update server: cisco
Last failed update reason: ('Connection aborted.', gaierror(-2, 'Name or service hnot
known'))
----------------------------------------
Last attempted update time: Mon Aug  7 02:02:32 2017 UTC
Last attempted update method: Manual
```

```
Last attempted update server: cisco
----------------------------------------
Total num of updates successful: 1
Num of attempts successful: 1
Num of attempts failed: 3
Total num of attempts: 4
----------------------------------------
Next update scheduled at: None
----------------------------------------
Current status: Idle
```

```
Device# utd threat-inspection signature update server cisco username ccouser password
passwd123
```

```
Device# utd threat-inspection signature update server url http://192.168.1.2/sig-1.pkg
```

例：署名許可リストの設定

次の例は、署名の許可リストを設定する方法を示しています。

```
Device# configure terminal
Device(config)# utd threat-inspection whitelist
Device(config-utd-whitelist)# utd-whitelist)# generator id 1 signature id 23456 comment
 "traffic from client x"
Device(config-utd-whitelist)# exit
Device(config)# utd engine standard
Device(config-utd-eng-std)# threat-inspection
Device(config-utd-eng-std-insp)# whitelist
Device(config-utd-eng-std-insp)# end
Device#
```

（注） 許可リストの署名 ID が設定されると、Snort はフローがアラートやドロップなしでデバイスを通過できるようにします。

アクティブな署名の表示例

例：接続ポリシーを使用したアクティブな署名の表示

```
Device# utd threat-inspection signature active-list write-to bootflash:siglist_connectivity
Device# more bootflash:siglist_connectivity
================================================================================
Signature Package Version: 2982.1.s
Signature Ruleset: Connectivity
Total no. of active signatures: 581
Total no. of drop signatures: 452
Total no. of alert signatures: 129

For more details of each signature please go to www.snort.org/rule_docs to lookup
================================================================================
List of Active Signatures:
```

```
-------------------------
<snipped>
```

例：バランスの取れたポリシーを使用したアクティブな署名の表示

```
Device# utd threat-inspection signature active-list write-to bootflash:siglist_balanced
Device# more bootflash:siglist_balanced
================================================================================
Signature Package Version: 2982.1.s
Signature Ruleset: Balanced
Total no. of active signatures: 7884
Total no. of drop signatures: 7389
Total no. of alert signatures: 495

For more details of each signature please go to www.snort.org/rule_docs to lookup
================================================================================

List of Active Signatures:
-------------------------
<snipped>
```

例：セキュリティポリシーを使用したアクティブな署名の表示

```
Device# utd threat-inspection signature active-list write-to bootflash:siglist_security
Device# more bootflash:siglist_security
================================================================================
Signature Package Version: 2982.1.s
Signature Ruleset: Security
Total no. of active signatures: 11224
Total no. of drop signatures: 10220
Total no. of alert signatures: 1004

For more details of each signature please go to www.snort.org/rule_docs to lookup
================================================================================

List of Active Signatures:
-------------------------
<snipped>
```

統合型 Snort IPS 設定の確認

次のコマンドを使用して、設定をトラブルシューティングします。

手順の概要

1. **enable**
2. **show virtual-service list**
3. **show virtual-service detail**
4. **show service-insertion type utd service-node-group**
5. **show service-insertion type utd service-context**
6. **show utd engine standard config**
7. **show utd engine standard status**
8. **show utd engine standard threat-inspection signature update status**

9. **show utd engine standard logging events**
10. **clear utd engine standard logging events**
11. **show platform hardware qfp active feature utd config**
12. **show platform software utd global**
13. **show platform software utd interfaces**
14. **show platform hardware qfp active feature utd stats**
15. **show utd engine standard statistics daq all**

手順の詳細

ステップ 1 enable

例：

```
Device> enable
```

特権 EXEC モードを有効にします。

- パスワードを入力します（要求された場合）。

ステップ 2 show virtual-service list

仮想サービスコンテナ上のすべてのアプリケーションのインストールのステータスを表示します。

例：

```
Device# show virtual-service list

Virtual Service List:


Name                     Status              Package Name
------------------------------------------------------------------------------
UTDIPS                   Activated           utdsnort.1_0_1_SV2982_XE_16_3.20160701_131509.ova
```

ステップ 3 show virtual-service detail

デバイスの仮想サービスコンテナにインストールされているアプリケーションによって使用されるリソースを表示します。

例：

```
Device# show virtual-service detail


Device#show virtual-service detail
Virtual service UTDIPS detail
  State                : Activated
  Owner                : IOSd
  Package information
    Name               : utdsnort.1_0_1_SV2982_XE_16_3.20160701_131509.ova
    Path               : bootflash:/utdsnort.1_0_1_SV2982_XE_16_3.20160701_131509.ova
    Application
      Name             : UTD-Snort-Feature
      Installed version : 1.0.1_SV2982_XE_16_3
      Description      : Unified Threat Defense
```

```
    Signing
      Key type          : Cisco development key
      Method            : SHA-1
    Licensing
      Name              : Not Available
      Version           : Not Available

  Detailed guest status

------------------------------------------------------------------------
Process               Status            Uptime           # of restarts
------------------------------------------------------------------------
climgr                 UP         0Y 0W 0D  0: 0:35        1
logger                 UP         0Y 0W 0D  0: 0: 4        0
snort_1                UP         0Y 0W 0D  0: 0: 4        0
Network stats:
eth0: RX  packets:43, TX  packets:6
eth1: RX  packets:8, TX  packets:6

Coredump file(s): lost+found

  Activated profile name: None
  Resource reservation
    Disk                : 736 MB
    Memory              : 1024 MB
    CPU                 : 25% system CPU

  Attached devices
    Type              Name        Alias
    ---------------------------------------------
    NIC               ieobc_1     ieobc
    NIC               dp_1_0      net2
    NIC               dp_1_1      net3
    NIC               mgmt_1      mgmt
    Disk              _rootfs
    Disk              /opt/var
    Disk              /opt/var/c
    Serial/shell                  serial0
    Serial/aux                    serial1
    Serial/Syslog                 serial2
    Serial/Trace                  serial3
    Watchdog          watchdog-2

  Network interfaces
    MAC address             Attached to interface
    ------------------------------------------------------
    54:0E:00:0B:0C:02       ieobc_1
    A4:4C:11:9E:13:8D       VirtualPortGroup0
    A4:4C:11:9E:13:8C       VirtualPortGroup1
    A4:4C:11:9E:13:8B       mgmt_1

  Guest interface
  ---
  Interface: eth2
  ip address: 48.0.0.2/24
Interface: eth1
  ip address: 47.0.0.2/24

  ---

  Guest routes
  ---
  Address/Mask                        Next Hop                          Intf.
-------------------------------------------------------------------------------
```

```
0.0.0.0/0                           48.0.0.1                        eth2
0.0.0.0/0                           47.0.0.1                        eth1

  ---

  Resource admission (without profile) : passed
    Disk space    : 710MB
    Memory        : 1024MB
    CPU           : 25% system CPU
    VCPUs         : Not specified
```

ステップ 4 show service-insertion type utd service-node-group

サービスノードグループのステータスを表示します。

例：

```
Device# show service-insertion type utd service-node-group

Service Node Group name : utd_sng_1
Service Context : utd/1
Member Service Node count : 1


Service Node (SN) : 30.30.30.2
Auto discovered : No
SN belongs to SNG : utd_sng_1
Current status of SN : Alive
Time current status was reached : Tue Jul 26 11:57:48 2016

Cluster protocol VPATH version : 1
Cluster protocol incarnation number : 1
Cluster protocol last sent sequence number : 1469514497
Cluster protocol last received sequence number: 1464
Cluster protocol last received ack number : 1469514496
```

ステップ 5 show service-insertion type utd service-context

AppNav およびサービスノードビューを表示します。

例：

```
Device# show service-insertion type utd service-context

Service Context : utd/1
Cluster protocol VPATH version : 1
Time service context was enabled : Tue Jul 26 11:57:47 2016
Current FSM state : Operational
Time FSM entered current state : Tue Jul 26 11:57:58 2016
Last FSM state : Converging
Time FSM entered last state : Tue Jul 26 11:57:47 2016
Cluster operational state : Operational

Stable AppNav controller View:
30.30.30.1

Stable SN View:
30.30.30.2

Current AppNav Controller View:
30.30.30.1

Current SN View:
```

```
30.30.30.2
```

ステップ 6 show utd engine standard config

統合脅威防御（UTD）の設定を表示します。

例：

```
Device# show utd engine standard config


UTD Engine Standard Configuration:
  Operation Mode : Intrusion Prevention
  Policy         : Security

Signature Update:
  Server    : cisco
  User Name : ccouser
  Password  : YEX^SH\fhdOeEGaOBIQAIcOVLgaVGf
  Occurs-at : weekly ;  Days:0 ; Hour: 23; Minute: 50

Logging:
  Server    :   IOS Syslog; 10.104.49.223
  Level     : debug

Whitelist Signature IDs:
  28878
```

ステップ 7 show utd engine standard status

UTD エンジンのステータスを表示します。

例：

```
Device# show utd engine standard status

Profile : High
System memory :
Usage : 8.00 %
Status : Green
Number of engines : 4

Engine Running CFT flows Health Reason
======================================================
Engine(#1): Yes 0 Green None
Engine(#2): Yes 0 Green None
Engine(#3): Yes 0 Green None
Engine(#4): Yes 0 Green None
======================================================

Overall system status: Green

Signature update status:
========================
Current signature package version: 2983.4.s
Last update status: Successful
Last successful update time: Mon Aug  7 02:02:32 2017 UTC
Last failed update time: Mon Aug  7 01:53:21 2017 UTC
Last failed update reason: ('Connection aborted.', gaierror(-2, 'Name or service not known'))
Next update scheduled at: None
Current status: Idle
```

ステップ 8 **show utd engine standard threat-inspection signature update status**

署名更新プロセスのステータスを表示します。

例：

```
Device# show utd engine standard threat-inspection signature update status

Current signature package version: 2983.4.s
Current signature package name: UTD-STD-SIGNATURE-2983-4-S.pkg
Previous signature package version: 29.0.c
----------------------------------------
Last update status: Successful
----------------------------------------
Last successful update time: Mon Aug  7 02:02:32 2017 UTC
Last successful update method: Manual
Last successful update server: cisco
Last successful update speed: 3022328 bytes in 25 secs
----------------------------------------
Last failed update time: Mon Aug  7 01:53:21 2017 UTC
Last failed update method: Manual
Last failed update server: cisco
Last failed update reason: ('Connection aborted.', gaierror(-2, 'Name or service hnot known'))
----------------------------------------
Last attempted update time: Mon Aug  7 02:02:32 2017 UTC
Last attempted update method: Manual
Last attempted update server: cisco
----------------------------------------
Total num of updates successful: 1
Num of attempts successful: 1
Num of attempts failed: 3
Total num of attempts: 4
----------------------------------------
Next update scheduled at: None
----------------------------------------
Current status: Idle
```

ステップ 9 **show utd engine standard logging events**

Snort センサーからのログイベントを表示します。

例：

```
Device# show utd engine standard logging events

2016/06/13-14:32:09.524475 IST [**] [Instance_ID: 1] [**] Drop [**] [1:30561:1]
BLACKLIST DNS request for known malware domain domai.ddns2.biz -
Win.Trojan.Beebone [**] [Classification: A Network Trojan was Detected] [Priority: 1]
[VRF_ID: 2] {UDP} 11.1.1.10:58016 -> 21.1.1.10:53
2016/06/13-14:32:21.524988 IST [**] [Instance_ID: 1] [**] Drop [**] [1:30561:1]
BLACKLIST DNS request for known malware domain domai.ddns2.biz -
Win.Trojan.Beebone [**] [Classification: A Network Trojan was Detected] [Priority: 1]
[VRF_ID: 2] {UDP} a000:0:0:0:0:0:0:10:59964 -> b000:0:0:0:0:0:0:10:53
```

ステップ 10 **clear utd engine standard logging events**

例：

```
Device# clear utd engine standard logging events
```

Snort センサーからのログイベントをクリアします。

ステップ 11 **show platform hardware qfp active feature utd config**

サービスノードの正常性に関する情報を表示します。

例：

```
Device# show platform hardware qfp active feature utd config

Global configuration
NAT64: disabled
SN threads: 12
CFT inst_id 0 feat id 1 fo id 1 chunk id 8
Context Id: 0, Name: Base Security Ctx
Ctx Flags: (0x60000)
Engine: Standard
SN Redirect Mode : Fail-open, Divert
Threat-inspection: Enabled, Mode: IDS
Domain Filtering : Not Enabled
URL Filtering : Not Enabled
SN Health: Green
```

ステップ 12 show platform software utd global

UTD が有効になっているインターフェイスを表示します。

例：

```
Device# show platform software utd global

UTD Global state
Engine               : Standard
Global Inspection    : Enabled
Operational Mode     : Intrusion Prevention
Fail Policy          : Fail-open
Container techonlogy : LXC
Redirect interface   : VirtualPortGroup1
UTD interfaces
All dataplane interfaces
```

ステップ 13 show platform software utd interfaces

すべてのインターフェイスに関する情報を表示します。

例：

```
Device# show platform software utd interfaces

UTD interfaces
All dataplane interfaces
```

ステップ 14 show platform hardware qfp active feature utd stats

データプレーンの UTD 統計情報を表示します。

例：

```
Device# show platform hardware qfp active feature utd stats

Security Context:    Id:0    Name: Base Security Ctx

Summary Statistics:
Pkts entered policy feature                         pkt                  228
```

```
                                                    byt                31083

Drop Statistics:

Service Node flagged flow for dropping                                    48
Service Node not healthy                                                  62

General Statistics:

Non Diverted Pkts to/from divert interface                             32913
Inspection skipped - UTD policy not applicable                         48892
Policy already inspected                                                2226
Pkts Skipped - L2 adjacency glean                                          1
Pkts Skipped - For Us                                                     67
Pkts Skipped - New pkt from RP                                           102
Response Packet Seen                                                     891
Feature memory allocations                                               891
Feature memory free                                                      891
Feature Object Delete                                                    863

Service Node Statistics:
SN Health: Green
SN down                                                                   85
SN health green                                                           47
SN health red                                                             13

Diversion Statistics
redirect                                                                2226
encaps                                                                  2226
decaps                                                                  2298
reinject                                                                2250
decaps: Could not locate flow                                             72
Redirect failed, SN unhealthy                                             62
Service Node requested flow bypass drop                                   48
```

ステップ 15　show utd engine standard statistics daq all

サービスプレーンのデータ収集（DAQ）の統計情報を表示します。

例：

```
Device# show utd engine standard statistics daq all

IOS-XE DAQ Counters(Engine #1):
--------------------------------
Frames received                       :0
Bytes received                        :0
RX frames released                    :0
Packets after vPath decap             :0
Bytes after vPath decap               :0
Packets before vPath decap            :0
Bytes before vPath decap              :0
Frames transmitted                    :0
Bytes transmitted                     :0

Memory allocation                     :2
Memory free                           :0
Merged packet buffer allocation       :0
Merged packet buffer free             :0

VPL buffer allocation                 :0
VPL buffer free                       :0
VPL buffer expand                     :0
```

```
VPL buffer merge                        :0
VPL buffer split                        :0
VPL packet incomplete                   :0

VPL API error                           :0
CFT API error                           :0
Internal error                          :0
External error                          :0
Memory error                            :0
Timer error                             :0

Kernel frames received                  :0
Kernel frames dropped                   :0

FO cached via timer                     :0
Cached fo used                          :0
Cached fo freed                         :0
FO not found                            :0
CFT full packets                        :0


VPL Stats(Engine #1):
------------------------
```

Cisco Prime CLI テンプレートを使用した Snort IPS の導入

Cisco Prime CLI テンプレートを使用して、Snort IPS 導入をプロビジョニングすることができます。Cisco Prime CLI テンプレートを使用すると、Snort IPS 導入を容易にプロビジョニングできます。Cisco Prime CLI テンプレートを Snort IPS 導入のプロビジョニングに使用するには、次の手順を実行します。

ステップ 1 システムで実行されている IOS XE バージョンに対応する Prime テンプレートをソフトウェアのダウンロードページからダウンロードします。

ステップ 2 このファイルが圧縮されている場合は解凍します。

ステップ 3 Prime から、[Configuration] > [Templates] > [Features and Technologies] の順に選び、[CLI Templates] を選択します。

ステップ 4 [Import] をクリックします。

ステップ 5 テンプレートのインポート先フォルダを選択し、[Select Templates] をクリックして、先ほどダウンロードしたテンプレートを選択してインポートします。

次の Snort IPS CLI テンプレートを使用できます。

- Copy OVA to Device：このテンプレートを使用して、Snort IPS OVA ファイルをルータのファイルシステムにコピーします。
- Delete OVA：このテンプレートを使用して、コピーした Snort IPS OVA ファイルをルータのファイルシステムから削除します。

- Dynamic NAT：ダイナミック NAT（ネットワークアドレス変換）が環境内で設定されており、Snort IPS 管理インターフェイス IP 用に変更する必要がある NAT 変換を選択するためにアクセスリストを使用する場合は、このテンプレートを使用します。
- Dynamic NAT Cleanup：このテンプレートを使用して、Snort IPS の NAT 設定を削除します。
- Dynamic PAT：環境内でダイナミック PAT（ポートアドレス変換）が設定されており、Snort IPS 管理インターフェイスIP用に変更する必要のある PAT 変換を選択するためにアクセスリストを使用する場合は、このテンプレートを使用します。
- Dynamic NAT Cleanup：このテンプレートを使用して、Snort IPS の PAT 設定を削除します。
- IP Unnumbered：このテンプレートを使用して、Snort IPS および IP 番号なしの導入に必要な仮想サービスを設定します。
- IP Unnumbered Cleanup：このテンプレートを使用して、IP 番号なしで設定された Snort IPS 管理インターフェイスを削除します。
- Management Interface：Snort IPS 管理トラフィックのルーティングにシステム管理インターフェイス（GigabitEthernet0 など）を使用する場合は、このテンプレートを使用します。
- Management Interface Cleanup：このテンプレートを使用して、Snort IPS 管理トラフィックをルーティングするために設定されたシステム管理インターフェイス（GigabitEthernet0 など）を削除します。
- Static NAT：このテンプレートを使用して、Snort IPS および既存の静的 NAT の導入に必要な仮想サービスを設定します。
- Static NAT Cleanup：このテンプレートを使用して、静的 NAT の導入で設定された Snort IPS を削除します。
- Upgrade OVA：このテンプレートを使用して、Snort IPS の OVA ファイルをアップグレードします。

IOx コンテナへの移行

ここでは、Cisco 1000 シリーズサービス統合型ルータ（ISR）での UTD 対応を拡張するための、Cisco IOx および IOx への UTD の移行について説明します。Cisco IOx では Cisco IOS と Linux OS が組み合わされており、安全性の高いネットワークを実現します。

Cisco IOx について

Cisco IOx は、さまざまな Cisco プラットフォームにおける各種アプリケーションに統一された一貫性のあるホスティング機能を提供するアプリケーション プラットフォームです。このプラットフォームは、ネットワーキング オペレーティング システム（Cisco IOS）とオープンソースのプラットフォーム（Linux）を統合し、ネットワーク上のカスタムアプリケーションとインターフェイスを実現します。

仮想サービス コンテナはデバイスの仮想化環境です。仮想マシン（VM）、仮想サービス、またはコンテナとも呼ばれます。仮想サービス コンテナ内にアプリケーションをインストールできます。このアプリケーションは、デバイスのオペレーティング システムの仮想サービス コンテナ内で稼動します。アプリケーションは、拡張子 .ova を持つ tar ファイルである Open Virtual Application（OVA）として提供されます。OVA パッケージは、コマンドラインのインターフェイスを介してデバイスにインストールされ、有効化されます。オープンフローの Cisco プラグインは、仮想サービスコンテナ内に導入できるアプリケーションの一例です。

UTD OVA をホストするために使用される仮想サービスコンテナのインフラストラクチャは、Cisco 1100 シリーズ ISR では対応していません。現在、UTD は両方のコンテナに対応しています。ただし、OVA コンテナ機能は Cisco IOS XE Gibrafilter 16.10 のリリースでは対応していますが、それ以降のリリースでは対応していません。

仮想サービスコンテナから IOx へのアップグレード

OVA ファイルは、仮想マシンの圧縮された「インストール可能な」バージョンを含むオープン仮想アーカイブ（Open Virtualization Archive）です。Snort IPS は仮想コンテナサービスとして使用できます。この OVA ファイルをデバイスにダウンロードし、**virtual-service install** CLI を使用してサービスをインストールする必要があります。

UTD IOx インフラストラクチャの場合、IOx ベースの OVA は IOx CLI コマンドを使用してインストールします。インストールする前に、グローバル設定モードで IOx 環境を開始します。

IOx ベースの OVA は TAR ファイルと呼ばれます。セキュリティライセンスが付属した Cisco IOS XE イメージを使用する必要があります。OVA ファイルのインストール中に、セキュリティライセンスがチェックされ、ライセンスが存在しない場合はエラーが報告されます。

仮想サービスから IOx コンテナにアップグレードするには、次の手順を実行します。

ステップ 1 **no activate**

例：

```
Device# configure terminal
Device (config)# virtual-service utd
Device (config-virt-serv)# no activate
Device (config-virt-serv)# exit
Device (config)# no virtual-service utd
```

仮想マネージャベースの仮想サービスのインスタンスを非アクティブにします。

ステップ 2 **show virtual-service list**

例：

```
Device# show virtual-service list
```

仮想サービスコンテナにインストールされているすべてのアプリケーションのステータスを表示します。仮想サービスインスタンスが非アクティブになっていることを確認します。

ステップ 3 **virtual-service uninstall name** *virtual-service instance*

例：

```
Device# virtual-service uninstall name utd
```

仮想マネージャベースの仮想サービスインスタンスをアンインストールします。**show virtual-service list** コマンドを実行したときに、仮想サービスインスタンスが表示されないことを確認します。

ステップ 4 **iox**

例：

```
Device# configure terminal
Device (config)# iox
Device (config)# end
```

IOx環境をグローバル設定モードで開始します。

ステップ 5 **app-hosting install appid** *name* **package** *bootflash:<tarfile>*

例：

```
Device# app-hosting install appid UTD package bootflash:utd.tar
Device#
```

Iox ベースの OVA tar ファイルをデバイスにコピーしてインストールします。

ステップ 6 **show app-hosting list**

例：

```
Device# show app-hosting list
App id                                   State
---------------------------------------------------------
UTD                                      DEPLOYED
Device#
```

インストールのステータスを表示します。アプリケーションが展開されていることを確認します。

ステップ 7 **app-hosting activate appid** *name*

例：

```
Device# app-hosting activate appid UTD
```

デバイス上の IOx ベースの TAR ファイルをアクティブにします。

ステップ 8 **show app-hosting list**

例：

```
Device# show app-hosting list
App id                                   State
---------------------------------------------------------
UTD                                      ACTIVATED

Device#
```

アクティベーションのステータスが表示されます。アプリケーションがアクティブになっていることを確認します。

ステップ 9 **app-hosting start appid** *name*

例：

```
Device# app-hosting start appid UTD
Device# show app-hosting list | in UTD
```

IOx ベースの OVA を開始します。

ステップ 10 **show app-hosting list**

例：

```
Example:
Device# show app-hosting list
App id                                   State
---------------------------------------------------------
UTD                                      RUNNING

Device#
```

開始のステータスを表示します。アプリケーションが実行されていることを確認します。

IOx の設定例

IOx の設定例を次に示します。

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# iox
Device(config)# interface VirtualPortGroup0
Device(config-if)# no shutdown
Device(config-if)# ip address 192.0.2.1 255.255.255.252
Device(config-if)# exit
Device(config)# interface VirtualPortGroup1
Device(config-if)# no shutdown
Device(config-if)# ip address 192.0.2.5 255.255.255.252
Device(config-if)# exit
Device(config)# app-hosting appid utd
Device(config-app-hosting)# app-vnic gateway0 virtualportgroup 0 guest-interface 0
Device(config-app-hosting-gateway0)# guest-ipaddress 192.0.2.2 netmask 255.255.255.252
Device(config-app-hosting-gateway0)# exit
Device(config-app-hosting)# app-vnic gateway1 virtualportgroup 1 guest-interface 1
Device(config-app-hosting-gateway1)# guest-ipaddress 192.0.2.6 netmask 255.255.255.252
Device(config-app-hosting-gateway1)# exit
Device(config-app-hosting)# app-resource package-profile custom
Device(config-app-hosting)# start
Device(config-app-hosting)# exit
Device(config)# exit
Device#
```

Snort IPS のトラブルシューティング

トラフィックが転送されない

問題 トラフィックは転送されません。

考えられる原因 仮想サービスがアクティブになっていない可能性があります。

解決法 **show virtual-service list** コマンドを使用して、仮想サービスがアクティブになっているかどうかを確認します。次に、コマンドの出力例を示します。

```
Device# show virtual-service list

Virtual Service List:


Name Status Package Name
--------------------------------------------------------------------------------
snort Activated utdsnort.1_0_1_SV2982_XE_16_3.20160701_131509.ova
```

考えられる原因 指定されたインターフェイスでは、統合脅威防御（UTD）が有効になっていない可能性があります。

解決法 **show platform software utd global** コマンドを使用して、インターフェイスで UTD が有効になっているかどうかを確認します。

```
Device# show platform software utd global

UTD Global state
Engine               : Standard
Global Inspection    : Disabled
Operational Mode     : Intrusion Prevention
Fail Policy          : Fail-open
Container techonlogy : LXC
Redirect interface   : VirtualPortGroup1
UTD interfaces
GigabitEthernet0/0/0
```

考えられる原因 サービスノードが正常に動作していない可能性があります。

解決法 **show platform hardware qfp active feature utd config** コマンドを使用して、サービスノードの状態が緑色かどうかを確認します。

```
Device# show platform hardware qfp active feature utd config

Global configuration
NAT64: disabled
SN threads: 12
CFT inst_id 0 feat id 0 fo id 0 chunk id 4
Context Id: 0, Name: Base Security Ctx
Ctx Flags: (0x60000)
Engine: Standard
SN Redirect Mode : Fail-open, Divert
Threat-inspection: Enabled, Mode: IDS
Domain Filtering : Not Enabled
URL Filtering : Not Enabled
SN Health: Green
```

考えられる原因 Snort プロセスがアクティブになっていない可能性があります。

解決法 **show virtual-service detail** コマンドを使用して、Snortプロセス が稼働しているかどうかを確認します。

```
Device# show virtual-service detail

Virtual service UTDIPS detail
  State                : Activated
  Owner                : IOSd
  Package information
```

```
    Name                : utdsnort.1_0_1_SV2982_XE_16_3.20160701_131509.ova
    Path                : bootflash:/utdsnort.1_0_1_SV2982_XE_16_3.20160701_131509.ova
    Application
      Name              : UTD-Snort-Feature
      Installed version : 1.0.1_SV2982_XE_16_3
      Description       : Unified Threat Defense
    Signing
      Key type          : Cisco development key
      Method            : SHA-1
    Licensing
      Name              : Not Available
      Version           : Not Available

  Detailed guest status

------------------------------------------------------------------------
Process               Status            Uptime           # of restarts
------------------------------------------------------------------------
climgr                 UP         0Y 0W 0D  0: 0:35        1
logger                 UP         0Y 0W 0D  0: 0: 4        0
snort_1                UP         0Y 0W 0D  0: 0: 4        0
Network stats:
eth0: RX  packets:43, TX  packets:6
eth1: RX  packets:8, TX  packets:6

Coredump file(s): lost+found

  Activated profile name: None
  Resource reservation
    Disk                : 736 MB
    Memory              : 1024 MB
    CPU                 : 25% system CPU

  Attached devices
    Type              Name        Alias
    ---------------------------------------------
    NIC               ieobc_1     ieobc
    NIC               dp_1_0      net2
    NIC               dp_1_1      net3
    NIC               mgmt_1      mgmt
    Disk              _rootfs
    Disk              /opt/var
    Disk              /opt/var/c
    Serial/shell                  serial0
    Serial/aux                    serial1
    Serial/Syslog                 serial2
    Serial/Trace                  serial3
    Watchdog          watchdog-2

  Network interfaces
    MAC address             Attached to interface
    ------------------------------------------------------
    54:0E:00:0B:0C:02       ieobc_1
    A4:4C:11:9E:13:8D       VirtualPortGroup0
    A4:4C:11:9E:13:8C       VirtualPortGroup1
    A4:4C:11:9E:13:8B       mgmt_1

  Guest interface
  ---
  Interface: eth2
  ip address: 48.0.0.2/24
Interface: eth1
  ip address: 47.0.0.2/24
```

```
  ---

  Guest routes
  ---
  Address/Mask                            Next Hop                              Intf.
-------------------------------------------------------------------------------
0.0.0.0/0                               48.0.0.1                              eth2
0.0.0.0/0                               47.0.0.1                              eth1

  ---

  Resource admission (without profile) : passed
    Disk space    : 710MB
    Memory        : 1024MB
    CPU           : 25% system CPU
    VCPUs         : Not specified
```

考えられる原因 AppNav トンネルがアクティブになっていない可能性があります。

解決法 **show service-insertion type utd service-node-group** および **show service-insertion type utd service-context** コマンドを使用して、AppNav トンネルがアクティブになっているかどうかを確認します。

解決法 次に、**show service-insertion type utd service-node-group** コマンドの出力例を示します。

```
Device# show service-insertion type utd service-node-group

Service Node Group name : utd_sng_1
Service Context : utd/1
Member Service Node count : 1


Service Node (SN) : 30.30.30.2
Auto discovered : No
SN belongs to SNG : utd_sng_1
Current status of SN : Alive
Time current status was reached : Tue Jul 26 11:57:48 2016

Cluster protocol VPATH version : 1
Cluster protocol incarnation number : 1
Cluster protocol last sent sequence number : 1469514497
Cluster protocol last received sequence number: 1464
Cluster protocol last received ack number : 1469514496
```

解決法 次に、**show service-insertion type utd service-context** コマンドの出力例を示します。

```
Device# show service-insertion type utd service-context

Service Context : utd/1
Cluster protocol VPATH version : 1
Time service context was enabled : Tue Jul 26 11:57:47 2016
Current FSM state : Operational
Time FSM entered current state : Tue Jul 26 11:57:58 2016
Last FSM state : Converging
Time FSM entered last state : Tue Jul 26 11:57:47 2016
Cluster operational state : Operational

Stable AppNav controller View:
30.30.30.1

Stable SN View:
```

```
30.30.30.2

Current AppNav Controller View:
30.30.30.1

Current SN View:
30.30.30.2
```

考えられる原因 トラフィックのステータスのデータプレーンUTD統計情報を確認します。トラフィックが転送されない場合、転送および拒否されたパケットの数はゼロになります。数値がゼロ以外の場合、トラフィック転送が行われており、Snort センサーはデータプレーンにパケットを再送信しています。

解決法 **show platform hardware qfp active feature utd stats** コマンドを使用してトラフィックのステータスを確認します。

```
Device# show platform hardware qfp active feature utd stats

Security Context:    Id:0    Name: Base Security Ctx

Summary Statistics:
Active Connections                                                    29
TCP Connections Created                                           712910
UDP Connections Created                                               80
Pkts entered policy feature                          pkt            3537977
                                                     byt          273232057
Pkts entered divert feature                          pkt            3229148
                                                     byt          249344841
Pkts slow path                                       pkt             712990
                                                     byt           45391747
Pkts Diverted                                        pkt            3224752
                                                     byt          249103697
Pkts Re-injected                                     pkt            3224746
                                                     byt          249103373
….
```

署名の更新が機能しない

問題 Cisco ボーダレスソフトウェア配布（BSD：Borderless Software Distribution）サーバからの署名更新が機能していません。

考えられる原因 さまざまな理由により署名の更新に失敗した可能性があります。最後に署名の更新に失敗した理由を確認します。

解決法 **show utd engine standard threat-inspection signature update status** コマンドを使用して、最後に署名の更新に失敗した理由を表示します。

```
Device# show utd eng standard threat-inspection signature update status
Current signature package version: 29.0.c
Current signature package name: default
Previous signature package version: None
----------------------------------------
Last update status: Failed
----------------------------------------
Last successful update time: None
```

```
Last successful update method: None
Last successful update server: None
Last successful update speed: None
----------------------------------------
Last failed update time: Thu Jan 11 13:34:36 2018 PST
Last failed update method: Manual
Last failed update server: http://172.27.57.252/UTD-STD-SIGNATURE-2983-1-S.pkg
Last failed update reason: [Errno 113] No route to host
----------------------------------------
Last attempted update time: Thu Jan 11 13:34:36 2018 PST
Last attempted update method: Manual
Last attempted update server: http://172.27.57.252/UTD-STD-SIGNATURE-2983-1-S.pkg
----------------------------------------
Total num of updates successful: 0
Num of attempts successful: 0
Num of attempts failed: 1
Total num of attempts: 1
----------------------------------------
Next update scheduled at: None
----------------------------------------
Current status: Idle
```

考えられる原因 ドメインネームシステム（DNS）が正しく設定されていません。

解決法 **show running-config | i name-server** コマンドを使用して、ネームサーバの詳細を表示します。

```
Device#  show run | i name-server

ip name-server 10.104.49.223
```

考えられる原因 システムエラー：ユーザ名とパスワードの組み合わせの処理に失敗しました。

解決法 署名パッケージのダウンロードに正しい認証情報を使用したことを確認します。

ローカルサーバからの署名の更新が機能しない

問題 ローカルサーバからの署名の更新が機能しない。

考えられる原因 最後の失敗の理由：無効なスキーム — HTTP または HTTPS のみに対応します。

解決法 ローカルダウンロード方式として HTTP またはセキュア HTTP（HTTPS）が指定されていることを確認します。

考えられる原因 最後の失敗の理由：名前またはサービスが不明です。

解決法 ローカルサーバに指定されたホスト名または IP アドレスが正しいことを確認します。

考えられる原因 最後の失敗の理由：認証情報が入力されていません。

解決法 ローカル HTTP または HTTPS サーバの認証情報が入力されていることを確認します。

考えられる原因 最後の失敗の理由：ファイルが見つかりません。

解決法 入力した署名ファイル名または URL が正しいことを確認します。

考えられる原因 最後の失敗の理由：ダウンロードが破損しています。

解決法

- 以前の署名のダウンロード時に署名更新の再試行でエラーが発生していないかどうかを確認します。
- 正しい署名パッケージが使用可能であることを確認します。

IOSd Syslog へのロギングが機能しない

問題 IOSd syslog へのロギングが機能しない。

考えられる原因 syslog へのロギングは、統合脅威防御（UTD）の設定では設定できません。

解決法 UTD 設定を表示し、syslog へのロギングが設定されていることを確認するには、**show utd engine standard config** コマンドを使用します。

```
Device# show utd engine standard config

UTD Engine Standard Configutation:
  Operation Mode : Intrusion Prevention
  Policy         : Security

Signature Update:
  Server    : cisco
  User Name : ccouser
  Password  : YEX^SH\fhdOeEGaOBIQAIcOVLgaVGf
  Occurs-at : weekly ;  Days:0 ; Hour: 23; Minute: 50

Logging:
  Server    :   IOS Syslog; 10.104.49.223
  Level     : debug

Whitelist Signature IDs:
  28878
```

解決法 UTD エンジンのイベントログを表示するには、次の **show utd engine standard logging events** コマンドを使用します。

```
Device# show utd engine standard logging events

2016/06/13-14:32:09.524475 IST [**] [Instance_ID: 1] [**] Drop [**] [1:30561:1]
BLACKLIST DNS request for known malware domain domai.ddns2.biz -
Win.Trojan.Beebone [**] [Classification: A Network Trojan was Detected]
[Priority: 1] [VRF_ID: 2] {UDP} 11.1.1.10:58016 -> 21.1.1.10:53
2016/06/13-14:32:21.524988 IST [**] [Instance_ID: 1] [**] Drop [**] [1:30561:1]
BLACKLIST DNS request for known malware domain domai.ddns2.biz -
Win.Trojan.Beebone [**] [Classification: A Network Trojan was Detected] [Priority: 1]
[VRF_ID: 2] {UDP} a000:0:0:0:0:0:0:10:59964 -> b000:0:0:0:0:0:0:10:53
```

外部サーバへのロギングが機能しない

問題 外部サーバへのロギングが機能していません。

考えられる原因 外部サーバで Syslog が実行されていない可能性があります。

解決法 syslog サーバが外部サーバで実行されているかどうかを確認します。ステータスを表示するには、外部サーバで次のコマンドを設定します。

```
ps -eaf | grep syslog

 root 2073 1 0 Apr12 ? 00:00:02 syslogd -r -m
```

考えられる原因 統合脅威防御（UTD）の Linux コンテナ（LXC：Linux Container）と外部サーバ間の接続が失われている可能性があります。

解決法 管理インターフェイスから外部 syslog サーバへの接続を確認します。

UTD 条件付きデバッグ

条件付きデバッグは、Unified Threat Defense のマルチテナントに対応しています。条件付きデバッグの設定方法の詳細については、以下を参照してください。

http://www.cisco.com/c/en/us/td/docs/routers/asr1000/troubleshooting/guide/Tbl-shooting-xe-3s-asr-1000-book.html#task_AC969BB06B414DCBBDEF7ADD29EF8131

Snort IPS に関するその他の参考資料

関連資料

関連項目	マニュアル タイトル
IOS コマンド	『Cisco IOS Master Command List, All Releases』[英語]
セキュリティ コマンド	• 『Cisco IOS Security Command Reference: Commands A to C』[英語] • 『Cisco IOS Security Command Reference: Commands D to L』[英語] • 『Cisco IOS Security Command Reference: Commands M to R』[英語] • 『Cisco IOS Security Command Reference: Commands S to Z』[英語]

シスコのテクニカル サポート

説明	リンク
シスコのサポート Web サイトでは、シスコの製品やテクノロジーに関するトラブルシューティングにお役立ていただけるように、マニュアルやツールをはじめとする豊富なオンライン リソースを提供しています。 お使いの製品のセキュリティ情報や技術情報を入手するために、Cisco Notification Service（Field Notice からアクセス）、Cisco Technical Services Newsletter、Really Simple Syndication（RSS）フィードなどの各種サービスに加入できます。 シスコのサポート Web サイトのツールにアクセスする際は、Cisco.com のユーザ ID およびパスワードが必要です。	http://www.cisco.com/support

Snort IPS の機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *219 : Snort IPS* の機能情報

機能名	リリース	機能情報
Snort IPS	Cisco IOS XE 3.16.1S、3.17S 以降のリリース	Snort IPS 機能は、Cisco IOS XE ベースのプラットフォームのブランチオフィスにおける侵入防止システム（IPS：Intrusion Prevention System）および侵入検知システム（IDS）を有効にします。この機能は、オープンソースの Snort ソリューションを使用して IPS と IDS を有効にします。
Snort IPS での VRF 対応	Cisco IOS XE Denali 16.3.1	Snort IPS 設定で仮想フラグメンテーションの再構成（VFR：Virtual Fragmentation Reassembl）に対応。
Cisco クラウドサービスルータ 1000v シリーズで Snort IPS に対応	Cisco IOS XE Denali 16.3.1	Cisco クラウドサービスルータ 1000v シリーズは Snort IPS に対応します。

機能名	リリース	機能情報
16.4 リリースにおける UTD Snort IPS の機能拡張	Cisco IOS XE Everest 16.4.1	16.4 リリースにおける UTD Snort IPS の機能拡張には、アクティブな署名のリストを表示する機能が追加されています。
脅威検知アラートの可視性 UTD サービスの有用性の強化	Cisco IOS XE Fuji 16.8.1	この機能は、脅威検知アラートの概要を提供します。次のコマンドが導入されています。 • **show utd engine standard logging statistics threat-inspection** • **show utd engine standard logging statistics threat-inspection** *detail* 次のコマンドは、UTD サービスの有用性の強化の一環として変更されています。 • **show utd engine standard status** • **show utd engine standard threat-inspection signature update status**
IOX コンテナへの UTD（IPS および URL フィルタリング）の移行	Cisco IOS XE Gibraltar 16.10.1	UTD は、仮想サービスコンテナを OVA から IOx に移行することで、Cisco 1100 シリーズ ISR に対応します。

第 165 章

Web フィルタリング

Web フィルタリング機能を使用すると、ドメインベースまたは URL ベースのポリシーとフィルタをデバイスに設定することで、インターネット Web サイトまたはインターネットサイトへのアクセスを制御できます。ユーザは、Web アクセスを管理する Web フィルタリングプロファイルを設定できます。Web フィルタリング機能はコンテナサービスを使用して実装され、これは Snort IPS ソリューションに似ています。

Web フィルタリングでは、以下に基づいて特定のドメインまたは URL へのアクセスを許可または拒否できます。

- 許可リストおよびブロックリスト：これらは静的ルールであり、ユーザがドメインまたは URL を許可または拒否するのに役立ちます。許可リストとブロックリストの両方で同じパターンが設定されている場合、トラフィックは許可されます。
- カテゴリ：URL を、ニュース、ソーシャルメディア、教育、アダルトなどの複数のカテゴリに分類できます。要件に基づいて、ユーザは 1 つ以上のカテゴリをブロックまたは許可することができます。
- レピュテーション：各 URL にはレピュテーションスコアが関連付けられています。レピュテーションスコアの範囲は 0 ー 100 で、高リスク（レピュテーションスコア（0 ー 20）、疑わしい（0 ー 40）、中程度のリスク（0 ー 60）、低リスク（0 ー 80）、信頼できる（0 ー100）に分類されます。URL のレピュテーションスコアと設定に基づいて、URL はブロックまたは許可されます。ユーザが CLI を使用してレピュテーションのしきい値を定義すると、レピュテーションスコアがユーザ定義のしきい値よりも低いすべての URL がブロックされます。

Web フィルタリング

Web フィルタリング機能を使用すると、ドメインベースまたは URL ベースのポリシーとフィルタをデバイスに設定することで、インターネット Web サイトへのアクセスを制御できます。ドメインベースのフィルタリングでは、ユーザはドメインレベルで Web サイトまたはサーバへのアクセスを制御でき、URL ベースのフィルタリングでは、ユーザは URL レベルで Web サイトへのアクセスを制御できます。この項では、次のトピックについて取り上げます。

ドメインベースのフィルタリング

ドメインベースのフィルタリングでは、ユーザは、デバイスに設定されたドメインベースのポリシーとフィルタに基づいてアクセスを許可または拒否することで、ドメインへのアクセスを制御できます。クライアントが Cisco クラウドサービスルータ 1000V シリーズを介して DNS 要求を送信すると、DNS トラフィックはドメインベースのポリシー（許可リストまたはブロックリスト）に基づいて検査されます。許可リストまたはブロックリストにあるドメインは、設定されている場合でも URL ベースのフィルタリングの対象になりません。グレーリストのトラフィックは許可リストとブロックリストの両方に一致せず、設定されている場合は URL ベースのフィルタリングの対象となります。

許可リストフィルタを使用したドメインベースのフィルタリング

完全なドメイン（cisco.com）をフィルタリングせずに許可するには、許可リストオプションを使用します。ユーザがブラウザを使用して Web サイトにアクセスする要求を行うと、ブラウザは Web サイトの IP アドレスを取得するための DNS 要求を行います。ドメインフィルタリングは、DNS トラフィックにフィルタを適用します。Web サイトのドメイン名が許可リストのパターンのいずれかに一致する場合、ドメインフィルタリングは Web サイトのアドレスを許可リストに追加します。ブラウザが Web サイトの IP アドレスを受信し、Web サイトの IP アドレスに HTTP 要求を送信します。ドメインフィルタリングは、このトラフィックを許可されたトラフィックとして扱います。この許可されたトラフィックは、設定されていても URL ベースのフィルタリングの対象にはなりません。Snort IPS が設定されている場合、トラフィックは Snort IPS の対象となります。

ブロックリストフィルタを使用したドメインベースのフィルタリング

ユーザがドメイン全体（badsite.com）をブロックする場合は、ブロックリストオプションを使用します。ドメインフィルタリングは、DNS トラフィックにフィルタを適用します。Web サイトのドメイン名がブロックリストのパターンの 1 つと一致する場合、ドメインフィルタリングは、Web サイトの実際に解決された IP アドレスの代わりに、DNS 応答で設定されたブロックサーバの IP アドレスをエンドユーザに送信します。ブラウザは、Web サイトの IP アドレスとしてブロックサーバの IP アドレスを受信し、この IP アドレスに HTTP 要求を送信します。このトラフィックは、設定されている場合でも URL フィルタリングまたは Snort IPS の対象になりません。ブロックサーバは HTTP 要求を受信し、エンドユーザにブロックページを提供します。また、DNS 要求がブロックリストに一致すると、そのドメインへのすべてのアプリケーショントラフィックがブロックされます。

ドメインフィルタリングは、DNS 要求が FTP、Telnet などの非HTTP（S）要求である方法で行われた場合でも、すべての DNS トラフィックに適用されます。ブロックリストに追加されている非HTTP（S）トラフィック（FTP、telnetなど）もブロックサーバに転送されます。ブロックページへの対応または要求の拒否はブロックサーバの役割です。内部または外部ブロックサーバを設定できます。設定手順については、「外部ブロックサーバを使用したドメインベースの Web フィルタリングの設定 （2395 ページ）」および「ローカルブロックサーバを使用したドメインベースの Web フィルタリングの設定 （2397 ページ）」を参照してください。

ドメインフィルタリング中にトラフィックが許可リストまたはブロックリストに含まれていない場合、URL フィルタリングと Snort IPS が設定されていれば、そのトラフィックは URL フィルタリングと Snort IPS の対象となります。

ユーザは、ドメインフィルタリングの許可パターンリストとブロックパターンリストの組み合わせてフィルタを設計することを検討できます。たとえば、ユーザが許可リスト www\.foo\.com だけでなく、www\.foo\.abc や www\.foo\.xyz などのブロックリストにある他のドメインを作成する場合は、www\.foo\.com を許可リストのパターンに、www\.foo\ をブロックリストのパターンに設定します。

（注） 許可またはブロック正規表現パターンで *www* プレフィックスを使用している場合、クライアントメッセージで返されるサーバー名インジケータ（SNI）が一致しない場合に問題が発生する可能性があります。たとえば、*www./foo./com* を許可する場合、SNI は *foo.com* としてのみ返されます。正規表現による照合には *www* を含めないことをお勧めします。

URL ベースのフィルタリング

URL ベースのフィルタリングにより、ユーザは許可リスト、ブロックリスト、カテゴリ、レピュテーションの設定に基づいて特定の Web サイトへのアクセスを許可または拒否することで、インターネット Web サイトへのアクセスを制御できます。たとえば、クライアントが Cisco CSR 1000V クラウドサービスルータ経由で HTTP 要求を送信すると、HTTP トラフィックは URL フィルタリングポリシー（許可リスト、ブロックリスト、カテゴリ、レピュテーション）に基づいて検査されます。HTTP 要求がブロックリストと一致する場合、HTTP 要求はインラインブロックページ応答によってブロックされるか、URL をブロックサーバにリダイレクトします。HTTP 要求が許可リストと一致する場合、トラフィックはそれ以上の URL フィルタリング検査を行われずに許可されます。

HTTPS トラフィックの場合、インラインブロックページは表示されません。URL ベースのフィルタリングでは、ルックアップを実行する前にエンコードされた URL をデコードしません。

デバイスに許可リストおよびブロックリストの設定がない場合、URL のカテゴリとレピュテーションに基づいて、ブロックページまたは HTTP のリダイレクト URL を使用してトラフィックが許可またはブロックされます。HTTP の場合、ブロックページまたはリダイレクト URL はなく、フローはドロップされます。

ユーザがカテゴリまたはレピュテーションベースの URL フィルタリングを設定すると、URL データベースがクラウドからダウンロードされます。URL カテゴリまたはレピュテーションデータベースには IP アドレスベースの記録がいくつかあり、カテゴリまたはレピュテーショ

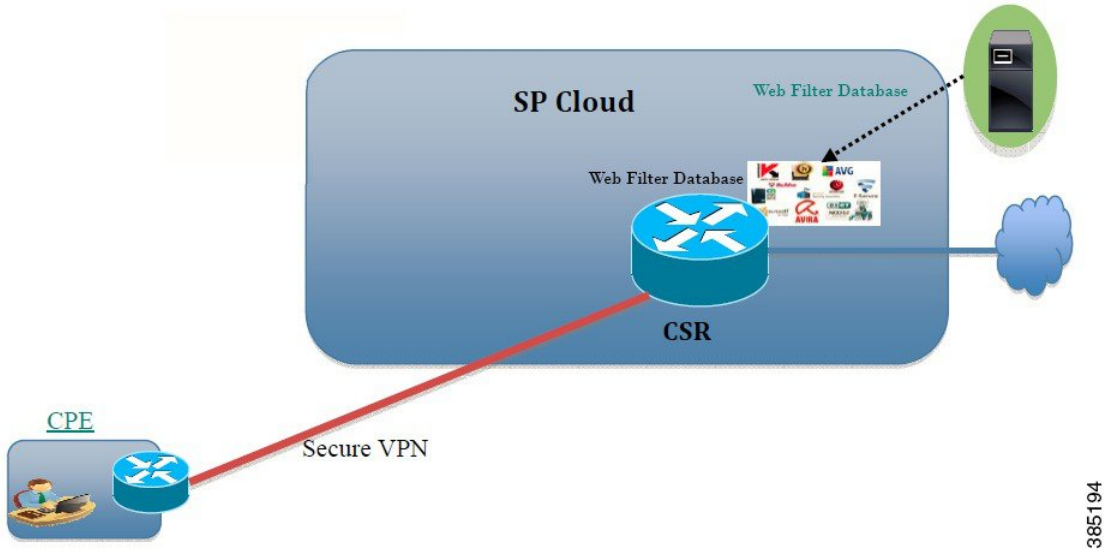
ンの検索は、URL のホスト部分にドメイン名がある場合にのみ実行されます。完全なデータベースがクラウドからダウンロードされた後、既存のデータベースに更新がある場合、差分の更新が 15 分ごとに自動的にダウンロードされます。完全なデータベースのサイズは約 440 MB で、ダウンロードしたデータベースは常にクラウドと同期する必要があります。クラウドへの接続が 24 時間以上失われると、データベースは無効になります。

デバイスがクラウドからデータベースの更新を取得しない場合、フェールオープンオプションにより、URL フィルタリング用に指定されたトラフィックがドロップされません。フェールクローズオプションを設定した場合、クラウドの接続が失われると、URL フィルタリング宛てのすべてのトラフィックがドロップされます。

（注） Web フィルタリングデータベースは、15 分ごとにクラウドから定期的に更新されます。

次の図に Web フィルタリングトポロジを示します。

図 *87 : Web* フィルタリングのネットワークトポロジ



URL フィルタリングにおける仮想サービスのリソースプロファイル

Cisco ISR 4000 シリーズサービス統合型ルータは、urlf-low プロファイルとともに urlf-medium および urlf-high リソースプロファイルに対応します。これらのプロファイルは、仮想サービスの実行に必要な CPU およびメモリリソースを表示します。

プラットフォーム	プロファイル	仮想サービスのリソース要件		プラットフォーム要件
		システム CPU	SP メモリ	
CSR1000v、ISRv	urlf-low	25%	3 GB	8 GB（RAM）
	urlf-medium	50%	4 GB	8 GB（RAM）
	urlf-high	75%	6 GB	12 GB（RAM）

クラウドルックアップ

クラウドルックアップ能は、シングルテナントモードで動作し、ローカルデータベースで使用できない URL のカテゴリとレピュテーションスコアを取得します。クラウドルックアップ機能は、デフォルトで有効になっています。

クラウドルックアップ機能は、オンボックス データベース ルックアップ機能を拡張したものです。以前は、オンボックスデータベースルックアップ機能により、オンボックスデータベースに存在せず、レピュテーションスコアが 0 の URL が許可されていました。クラウドルックアップが有効になっている場合、レピュテーションスコアと設定されたブロックしきい値に基づいて、以前に許可されていた URL がドロップされる場合があります。そのような URL を許可するには、それらを許可リストに追加する必要があります。クラウドルックアップのさまざまなURLのカテゴリおよびレピュテーションスコアを以下に説明します。

URL には次の 2 種類があります。

- 名前ベースの URL
- IP ベースの URL

クラウドルックアップ機能を有効にすると、不明な URL のカテゴリとレピュテーションスコアが次のように返されます。

名前ベースの URL

- 有効な URL：対応するカテゴリとレピュテーションスコアが受信されます。
- 不明なURL（新しいURLまたはクラウドに対して未知なURL）：カテゴリは「未分類」、レピュテーションスコアは 40
- 適切なドメイン名を持つ内部URL（例：internal.abc.com）：カテゴリとレピュテーションスコアはベースドメイン名（上記の例の abc.com）に基づきます。
- 完全に内部にある URL（例：abc.xyz）：カテゴリは「未分類」、レピュテーションスコアは 40

IP ベースの URL

- パブリックホスト型 IP：対応するカテゴリとレピュテーションスコアが受信されます。
- プライベート IP（例：10.<>. 192.168.<>）：カテゴリは「未分類」、レピュテーションスコアは 100

- 非ホスト型またはルーティング不可の IP：カテゴリは「未分類」、レピュテーションスコアは 40

クラウドルックアップのスコアは、これらの URL（不明 / 非ホスト型 / ルーティング不可 / 内部 URL）のオンボックスデータベースとは異なります。

（注） クラウドルックアップ機能は、マルチテナントモードでは使用できません。

Web フィルタリングの利点

Web フィルタリング機能を使用すると、ドメインおよび URL ベースのポリシーとフィルタを設定して、インターネットへのアクセスを制御できます。悪意のあるまたは不要な Web サイトをブロックすることで、ネットワークを保護します。Web フィルタリングは、URL ベースのフィルタリングとドメインベースのフィルタリングで構成されています。ドメインベースのフィルタリングは、ドメインレベルで Web サイトまたはサーバへのアクセスを制御し、URL ベースのフィルタリングは、URL レベルで Web サイトへのアクセスを制御します。ユーザは Web フィルタリングを使用して、個別の URL をブロックリストまたはドメイン名に追加し、その同じ URL に対して許可リストのポリシーを設定できます。ユーザは、レピュテーションまたはカテゴリに基づいて URL を許可またはブロックするようにプロビジョニングすることもできます。

Web フィルタリングの前提条件

Cisco CSR 1000V クラウドサービスルータで Web フィルタリング機能を設定する前に、次のことを確認します。

- Cisco CSR 1000V クラウドサービスルータは、Cisco IOS XE Denali 16.3 以降のソフトウェアイメージを実行します。
- Cisco CSR 1000V クラウドサービスルータには、コンテナサービスを導入するために 2 つの vCPU、8 GB のメモリ、および 2 GB の追加のディスク領域が必要となります。
- Cisco CSR 1000V クラウドサービスルータには、Web フィルタリング機能を有効にするためのセキュリティ K9 ライセンスが必要です。

Web フィルタリングの制約事項

Web フィルタリング機能には、次のような制約事項が適用されます。

- この機能は、Cisco CSR 1000V クラウドサービスルータのみに対応し、Cisco 4000 シリーズサービス統合型ルータには対応しません。

- 許可リストおよびブロックリストのパターンは正規表現のパターンのみに対応し、現在は許可リストおよびブロックリストでは 64 個のパターンに対応しています。正規表現のパターンの詳細については、「正規表現」の章を参照してください。
- ドメインフィルタリングは、IPv4 UDP 転送を使用して DNS プロトコルで解決された IPv4 ドメインのみに対応します。ドメインフィルタリングアラートは、IOS syslog にのみ送信されます。
- OpenDNS によるドメインフィルタリングには対応していません。
- 仮想ルーティングおよび転送（VRF：Virtual Routing and Forwarding）を使用した URL フィルタリングには対応していません。
- CWS によるドメインフィルタリングには対応していません。
- ドメインフィルタリングは、カテゴリとレピュテーションに対応していません。
- ローカルブロックサーバは、HTTPS ブロックページの提供には対応していません。URL フィルタがブロックページまたはリダイレクトメッセージを挿入しようとする場合、HTTPS トラフィックには対応しません。
- URL にユーザ名とパスワードがある場合、URL フィルタは許可リストおよびブロックリストのパターンと一致させる前に URL からそれらを削除することはしません。ただし、カテゴリまたはレピュテーションルックアップにはこの制限はなく、ルックアップの前に URL からユーザ名とパスワードを削除します。
- HTTPS 検査は制限されています。Web フィルタリングでは、サーバ証明書を使用して URL およびドメイン情報を取得します。完全な URL のパスを検査することはできません。
- UTD は、VRF 間シナリオにおいては WCCP および NBAR との相互運用は行いません。
- URL、ドメイン、ブロック、sourcedb の Web フィルタのプロファイル名に使用できるのは、英数字、ダッシュ、および下線のみです。
- 仮想サービスプロファイルが変更された場合、プロファイルの変更を有効にするには、仮想サービスを再インストールする必要があります。

Web フィルタリングの導入方法

対応しているデバイスに Web フィルタリングを導入するには、次のタスクを実行します。

始める前に

- **デバイスのプロビジョニング**：Web フィルタリング機能をインストールするデバイスを特定します。この機能は、Cisco CSR 1000V クラウドサービスルータに対応しています。
- **ライセンスの取得**：Web フィルタリング機能は、サービスを有効にするためにセキュリティライセンスが必要なセキュリティパッケージでのみ使用できます。ライセンスの取得については、シスコ サポートにお問い合わせください。

ステップ 1 仮想コンテナサービスをインストールしてアクティブにします。仮想コンテナサービスのインストールおよびアクティブ化の方法 （2394 ページ）

ステップ 2 外部ブロックサーバを使用してドメインベースの Web フィルタリングを設定します。外部ブロックサーバを使用したドメインベースの Web フィルタリングの設定 （2395 ページ）

ステップ 3 ローカルブロックサーバを使用してドメインベースの Web フィルタリングを設定します。ローカルブロックサーバを使用したドメインベースの Web フィルタリングの設定 （2397 ページ）

ステップ 4 ローカルブロックサーバを使用して URL ベースの Web フィルタリングを設定します。ローカルブロックサーバを使用した URL ベースの Web フィルタリングの設定 （2398 ページ）

ステップ 5 インラインブロックサーバを使用して URL ベースの Web フィルタリングを設定します。インラインブロックページを使用した URL ベースの Web フィルタリングの設定 （2401 ページ）

ステップ 6 Snort IPS または IDSを設定します。ドメインおよび URL ベースの Web フィルタリングと Snort IPS の設定 （2402 ページ）

仮想コンテナサービスのインストールおよびアクティブ化の方法

仮想コンテナサービスをインストールしてアクティブにするには、次のタスクを実行します。

ステップ 1 UTD OVA ファイルをインストールします。UTD OVA ファイルのインストール （2394 ページ）

ステップ 2 VirtualPortGroup のインターフェイスおよび仮想サービスを設定します。VirtualPortGroup のインターフェイスおよび仮想サービスの設定 （2395 ページ）

ステップ 3 Snort 仮想コンテナサービスをアクティブにします。

UTD OVA ファイルのインストール

OVA ファイルは、仮想マシンの圧縮された「インストール可能な」バージョンを含むオープン仮想アーカイブ（Open Virtualization Archive）です。この OVA ファイルをルータにダウンロードし、仮想サービスのインストール CLI を使用してサービスをインストールする必要があります。サービス OVA ファイルは、ルータにインストールされている Cisco IOS XE リリースイメージには付属していません。ただし、OVA ファイルはルータのフラッシュに事前にインストールされている場合があります。

セキュリティライセンスが付属した Cisco IOS XE イメージを使用する必要があります。OVA ファイルのインストール中に、セキュリティライセンスがチェックされ、ライセンスが存在しない場合はエラーが報告されます。

これはサンプル設定です。

```
Device> enable
Device# virtual-service install name UTDIPS package harddisk:utd-ips-v102.ova media
harddisk:
Device# show virtual-service list
```

```
Virtual Service List:
Name Status Package Name
------------------------------------------------------------------------------
snort Installed utdsnort.1_2_2_SV2982_XE_main.20160
```

VirtualPortGroup のインターフェイスおよび仮想サービスの設定

2 つの VirtualPortGroup インターフェイスと両方のインターフェイスのゲスト IP アドレスを設定する必要があります。

（注） データトラフィック用の VirtualPortGroup インターフェイスは、プライベートまたはルーティング不可の IP アドレスを使用する必要があります。このインターフェイスには、IP アドレスの範囲として 192.0.2.0 / 30を 使用することを推奨します。

これはサンプル設定です。

```
Device# configure terminal
evice(config)# interface VirtualPortGroup0
Device(config-if)# ip address 192.0.2.1 255.255.255.252
Device(config-if)# exit
Device(config)# interface VirtualPortGroup 1
Device(config-if)# ip address 192.0.2.5 255.255.255.252
Device(config-if)# exit
Device(config)# virtual-service UTDIPS

Device(config-virt-serv)# profile urlf-low (This is minimum requirement for web filtering
 to work.)

Device(config-virt-serv)# vnic gateway VirtualPortGroup 0 (The IP-address configured in
 VPG0 interface should have access to Internet over http(s).If the VPG0 interface does
not have access to Internet, the web filter database will not be updated.)
Device(config-virt-serv-vnic)# guest ip address 192.0.2.2
Device(config-virt-serv-vnic)# exit
Device(config-virt-serv)# vnic gateway VirtualPortGroup 1
Device(config-virt-serv-vnic)# guest ip address 192.0.2.6
Device(config-virt-serv-vnic)# exit
Device(config-virt-serv)# activate
Device(config-virt-serv)# end

Device# show virtual-service list
Virtual Service List:

Name                    Status             Package Name
------------------------------------------------------------------------------
snort                   Activated          utdsnort.1_2_2_SV2982_XE_main.20160
```

外部ブロックサーバを使用したドメインベースのWebフィルタリングの設定

外部ブロックサーバを使用してドメインベースの Web フィルタリングを設定するには、次の手順を実行します。

ステップ 1 仮想サービスをインストールし、アクティブにします。詳細については、VirtualPortGroup のインターフェイスおよび仮想サービスの設定 （2395 ページ）を参照してください。

ステップ 2 ブロックリストのパラメータマップを次のように設定します。

```
parameter-map type regex domainfilter_blacklist_pmap1
  pattern examplebook\.com
  pattern bitter\.com
```

ステップ 3 許可リストのパラメータマップを次のように設定します。

```
parameter-map type regex domainfilter_whitelist_pmap1
  pattern example\.com
  pattern exmaplegogle\.com
```

ステップ 4 ドメインプロファイルを設定し、ブロックリストと許可リストのパラメータマップを次のように関連付けます。

```
utd web-filter domain profile 1
 blacklist
  parameter-map regex domainfilter_blacklist_pmap1
 whitelist
  parameter-map regex domainfilter_whitelist_pmap1
```

ステップ 5 （オプション）デフォルトでは、ドメインフィルタリングアラートは有効になっていません。ドメインプロファイルでブロックリストまたは許可リスト、あるいはその両方のアラートを設定します。

```
alert {all | blacklist | whitelist}
```

ステップ 6 ドメインプロファイルで外部リダイレクトサーバを設定します。

```
redirect-server external x.x.x.x (This is the IP address that is used for serving block page when
a page is on the blocked list)
```

ステップ 7 次のドメインプロファイルを使用して UTD エンジン標準を設定します。

```
utd engine standard
 web-filter
  domain-profile 1
```

ステップ 8 エンジン標準を使用してUTDを設定し、グローバルに、または特定のインターフェイスで有効にします。

```
utd
  all-interfaces
  engine standard
```

次に、外部ブロックサーバを使用してドメインベースの Web フィルタリングを設定する例を示します。

```
parameter-map type regex domainfilter_blacklist_pmap1
  pattern examplebook\.com
  pattern bitter\.com
parameter-map type regex domainfilter_whitelist_pmap1
  pattern exmaplegogle\.com
  pattern exmaplegogle\.com
utd engine standard
  web-filter
    domain-profile 1
!
utd web-filter domain profile 1
  alert all
  blacklist
```

```
    parameter-map regex domainfilter_blacklist_pmap1
  whitelist
    parameter-map regex domainfilter_whitelist_pmap1
  redirect-server external 192.168.1.1
!
utd
  all-interfaces
  engine standard
```

ローカルブロックサーバを使用したドメインベースのWebフィルタリングの設定

ローカルブロックサーバでを使用してドメインベースの Web フィルタリングを設定するには、次の手順を実行します。

ステップ 1 仮想サービスをインストールし、アクティブにします。詳細については、VirtualPortGroup のインターフェイスおよび仮想サービスの設定 （2395 ページ）を参照してください。

ステップ 2 ループバックインターフェイスを設定するか、クライアントがアクセスできる既存のインターフェイスを使用します。

```
interface loopback 110
 ip address 10.1.1.1 255.255.255.255
exit
```

ステップ 3 ローカルブロックサーバのプロファイルを使用して UTD Web フィルタを設定します。

```
utd web-filter block local-server profile 1
 block-page-interface loopback 110
 http-ports 80
 content text "Blocked by Web-Filter"
```

ステップ 4 ブロックリストのパラメータマップを次のように設定します。

```
parameter-map type regex domainfilter_blacklist_pmap1
  pattern bitter\.com
```

ステップ 5 許可リストのパラメータマップを次のように設定します。

```
parameter-map type regex domainfilter_whitelist_pmap1
  pattern sweet\.com
```

ステップ 6 ドメインプロファイルを設定し、ブロックリストと許可リストのパラメータマップを次のように関連付けます。

```
utd web-filter domain profile1
 blacklist
  parameter-map regex domainfilter_blacklist_pmap1
 whitelist
  parameter-map regex domainfilter_whitelist_pmap1
```

ステップ 7 （オプション）デフォルトでは、ドメインフィルタリングアラートは有効になっていません。ドメインプロファイルでブロックリストまたは許可リスト、あるいはその両方のアラートを設定します。

```
alert {all |blacklist | whitelist}
```

ステップ 8 ドメインプロファイルでリダイレクトサーバをローカルブロックサーバとして設定します。

```
redirect-server local-block-server 1
```

ステップ 9 次のドメインプロファイルを使用して UTD エンジン標準を設定します。

```
utd engine standard
 web-filter
  domain-profile 1
```

ステップ 10 エンジン標準を使用して UTD を設定し、グローバルに、または特定のインターフェイスで有効にします。

```
utd
  all-interfaces
  engine standard
```

次に、ローカルブロックサーバを使用してドメインベースの Web フィルタリングを設定する例を示します。

```
interface loopback 110
  ip address 10.1.1.1 255.255.255.255
exit
parameter-map type regex domainfilter_blacklist_pmap1
  pattern bitter\.com
parameter-map type regex domainfilter_whitelist_pmap1
  pattern sweet\.com
utd engine standard
  web-filter
    domain-profile 1
!
utd web-filter block local-server profile 1
  block-page-interface Loopback110
  content text "Blocked by Web-Filter"
  http-ports 80
!
utd web-filter domain profile 1
  alert all
  blacklist
    parameter-map regex domainfilter_blacklist_pmap1
  whitelist
    parameter-map regex df_whitelist_pmap1
  redirect-server local-block-server 1
!
utd
  all-interfaces
  engine standard
```

ローカルブロックサーバを使用した URL ベースの Web フィルタリングの設定

ローカルブロックサーバを使用して URL ベースの Web フィルタリングを設定するには、次の手順を実行します。

ステップ 1 仮想サービスをインストールし、アクティブにします。詳細については、VirtualPortGroup のインターフェイスおよび仮想サービスの設定 （2395 ページ）を参照してください。

ステップ 2 ループバックインターフェイスを設定するか、クライアントがアクセスできる既存のインターフェイスを使用します。

```
interface loopback 110
 ip address 10.1.1.1 255.255.255.255
exit
```

ステップ 3 ローカルブロックサーバのプロファイルを使用して UTD Web フィルタを設定します。

```
utd web-filter block local-server profile 1
 block-page-interface loopback 110
 http-ports 80
 content text "Blocked by Web-Filter"
```

ステップ 4 ブロックリストのパラメータマップを次のように設定します。

```
parameter-map type regex urlf_blacklist_pmap1
 pattern exmplee.com/sports
```

ステップ 5 許可リストのパラメータマップを次のように設定します。

```
parameter-map type regex urlf_whitelist_pmap1
 pattern examplehoo.com/finance
```

ステップ 6 URL プロファイルを設定し、次の手順を実行します。

```
utd web-filter url profile 1
```

a) ブロックリストと許可リストのパラメータマップを関連付けます。

```
blacklist
  parameter-map regex urlf_blacklist_pmap1
whitelist
  parameter-map regex urlf_whitelist_pmap1
```

b) ローカルブロックサーバのプロファイルでブロックリスト、許可リスト、またはその両方のアラートを設定します。

```
alert {all | blacklist | whitelist}
```

c) 許可またはブロックするカテゴリを設定します。

```
categories allow
  sports
```

d) レピュテーションブロックのしきい値を設定します。

```
reputation
  block-threshold high-risk
```

e) フェールオプションを使用して URL ソースデータベースを設定します。

```
sourcedb fail close
```

f) ログレベルを設定します。デフォルトオプションはエラーです。オプションを [info] または [detail] に設定すると、パフォーマンスが次の影響を受ける可能性があります。

```
log level error
```

g) ローカルブロックサーバをブロックに設定します。

```
block local-server 1
```

ステップ 7 URL プロファイルを使用して UTD エンジン標準を設定します。

```
utd engine standard
 web-filter
   url-profile 1
```

ステップ 8 UTD エンジン標準を設定し、グローバルまたは特定のインターフェイスで UTD を有効にします。

```
utd
  all-interfaces
  engine standard
```

次に、ローカルブロックサーバを使用して URL ベースの Web フィルタリングを設定する例を示します。

```
parameter-map type regex urlf_blacklist_pmap1
 pattern examplee.com/sports
parameter-map type regex urlf_whitelist_pmap1
 pattern exmaplehoo.com/finance
!
interface loopback 110
 ip address 10.1.1.1 255.255.255.255
 exit
utd web-filter block local-server profile 1
 block-page-interface loopback 110
 http-ports 80
 content text "Blocked by Web-Filter"
utd web-filter url profile 1
 blacklist
  parameter-map regex urlf_blacklist_pmap1
 whitelist
  parameter-map regex urlf_whitelist_pmap1
 alert all
 categories allow
  sports
 reputation
  block-threshold high-risk
 sourcedb fail close
 log level error
 block local-server 1
!
utd engine standard
 web-filter
  url-profile 1
!
utd
 all-interfaces
 engine standard
```

インラインブロックページを使用したURLベースのWebフィルタリングの設定

インラインブロックページを使用して URL ベースの Web フィルタリングを設定するには、次の手順を実行します。

ステップ 1 仮想サービスをインストールし、アクティブにします。詳細については、VirtualPortGroup のインターフェイスおよび仮想サービスの設定 （2395 ページ）を参照してください。

ステップ 2 ブロックリストのパラメータマップを次のように設定します。

```
parameter-map type regex urlf_blacklist_pmap1
 pattern exmaplegogle.com/sports
```

ステップ 3 許可リストのパラメータマップを次のように設定します。

```
parameter-map type regex urlf_whitelist_pmap1
 pattern exmaplehoo.com/finance
```

ステップ 4 UTD ブロックページのプロファイルを設定します。

```
utd web-filter block page profile 1
 text "Blocked by Web-Filter URLF" (The other options are file and redirect-url)
```

ステップ 5 URL プロファイルを設定し、次の手順を実行します。

```
utd web-filter url profile 1
```

a) ブロックリストと許可リストのパラメータマップを関連付けます。

```
blacklist
  parameter-map regex urlf_blacklist_pmap1
whitelist
  parameter-map regex urlf_whitelist_pmap1
```

b) ローカルブロックサーバのプロファイルでブロックリスト、許可リスト、またはその両方のアラートを設定します。

```
alert {all | blacklist | whitelist | categories-reputation}
```

c) 許可またはブロックするカテゴリを設定します。

```
categories allow
  sports
```

d) レピュテーションブロックのしきい値を設定します。

```
reputation
  block-threshold high-risk
```

e) フェールオプションを使用して URL ソースデータベースを設定します。

```
sourcedb fail close
```

f) ログレベルを設定します。デフォルトオプションはエラーです。オプションを [info] または [detail] に設定すると、パフォーマンスが次の影響を受ける可能性があります。

```
log level error
```

g) ローカルブロックサーバをブロックに設定します。

```
block local-server 1
```

ステップ 6 URL プロファイルを使用して UTD エンジン標準を設定します。

```
utd engine standard
 web-filter
   url-profile 1
```

ステップ 7 UTD エンジン標準を設定し、グローバルまたは特定のインターフェイスで UTD を有効にします。

```
utd
  all-interfaces
  engine standard
```

次に、インラインブロックサーバを使用して URL ベースの Web フィルタリングを設定する例を示します。

```
parameter-map type regex urlf_blacklist_pmap1
  pattern exmaplegogle.com/sports
parameter-map type regex urlf_whitelist_pmap1
 pattern exmaplehoo.com/finance
!
utd web-filter block page profile 1
 text "Blocked by Web-Filter URLF"
!
utd web-filter url profile 1
 blacklist
  parameter-map regex urlf_blacklist_pmap1
 whitelist
  parameter-map regex urlf_whitelist_pmap1
 alert all
 categories allow
  sports
 reputation
  block-threshold high-risk
 sourcedb fail close
 log level error
!
utd engine standard
 web-filter
  url-profile 1
!
utd
 all-interfaces
 engine standard
```

ドメインおよび URL ベースの Web フィルタリングと Snort IPS の設定

ドメインまたは URL ベースの Web フィルタリングと Snort IPS を設定するには、次の手順を実行します。

ステップ 1 ドメインプロファイルを設定します。

```
utd web-filter domain profile 1
```

ステップ 2 URL プロファイルを設定します。

```
utd web-filter url profile 1
```

ステップ 3 UTD エンジン標準で脅威検知を設定します。

```
utd engine standard
 threat-inspection
```

ステップ 4 ドメインプロファイルと URL プロファイルを使用して、UTD エンジン標準で Web フィルタを設定します。

```
utd engine standard
 logging syslog
 threat-inspection
  threat protection
  policy security
 signature update server cisco username xxx password QhLb]Z[ifMbFgLYgR]^KLDUZ
  signature update occur-at daily 0 0
  logging level error
 web-filter
  domain-profile 1
  url-profile 1
```

ステップ 5 UTD エンジン標準を設定し、グローバルに、または特定のインターフェイスで有効にします。

```
utd
  all-interfaces
  engine standard
```

Web フィルタ設定の確認

次のコマンドを使用して、Web フィルタリングの設定を確認できます。

```
Device# show utd engine standard config

UTD Engine Standard Configuration:
  Operation Mode : Intrusion Detection
  Policy         : Balanced

  Signature Update: Not Configured

  Logging:
    Server    :  IOS Syslog
    Level     : err (Default)
    Statistics    : Disabled

  Whitelist : Disabled
  Whitelist Signature IDs:

Web-Filter      : Enabled

  Whitelist :
    www.cisco.com
  Blacklist :
    www.hotstar.com
```

```
  Categories Action : Block
  Categories :
    Fashion and Beauty

  Block Profile:
   No config present

  Reputation Block Threshold : Moderate risk
  Alerts Enabled : Blacklist
  Cloud Lookup : Enabled
  Debug level : Error
Conditional debug level : Error
```

Web フィルタリングのトラブルシューティング

ログを収集するには、**virtual-service move name "CONTAINER_NAME" log to bootflash:** コマンドを使用します。デバイスで次のコマンドを使用して、Web フィルタリング機能の有効化に関連する問題のトラブルシューティングを行うことができます。

- **debug utd engine standard all**
- **debug utd engine standard climgr**
- **debug utd engine standard daq**
- **debug utd engine standard internal**
- **debug utd engine standard onep**
- **show utd engine standard logging events**

（注） このツールは、設定された URL フィルタリングアラート/イベントの出力のみを表示します。ユーザーは、「設定例」セクションの手順に従って、この出力に表示されるイベントとアラートのタイプを設定できます。たとえば、「alert all」を設定した場合は、「ホワイトリスト」、「ブラックリスト」、およびカテゴリとレピュテーションのイベントが表示されます。「alert whitelist」のみを設定すると、「ホワイトリスト」イベントのみが表示されます。

リリース 16.8.1 では、コンテナの設定および署名の更新を適用するために、コンテナの設定エラーの回復が強化されています。強化されたエラー修復により、次のことが可能になります。

- エラーを検出して対処するための、設定をダウンロードする際の安定性の向上。
- 署名と設定の更新を同時に処理する効率的な方法。
- IOSd と CLIMGR 間の oneP 接続が失われた際の早期における検出と回復。たとえば、CLIMGR がクラッシュした場合など。
- （現在または最近の）設定ダウンロードの詳細結果の可視性の向上（デバッグを有効にする必要はありません）。

次のサイト https://www.brightcloud.com/tools/url-ip-lookup.php を使用すると、URL フィルタリング機能によって Web サイトがどのように分類されるのかを検証できます。

設定例

次に、CSR 1000V クラウドサービスルータでドメインフィルタリングを有効にする例を示します。

```
Device# configure terminal
Device(config)# parameter-map type regex wlist1
Device(config-profile)# pattern google.com
Device(config-profile)# pattern cisco.com
Device(config-profile)# exit
Device(config)# parameter-map type regex blist1
Device(config-profile)# pattern exmaplehoo.com
Device(config-profile)# pattern bing.com
Device(config-profile)# exit
Device(config)# utd web-filter block local-server profile 1
Device(config--utd-webf-blk-srvr)# content file bootflash:test.utd.file
Device(config--utd-webf-blk-srvr)# end
```

ローカルブロックサーバを動作させるには、HTTP サーバが稼働している必要があります。ip http server コマンドを使用して、ブロックサーバを設定します。show ip http server status コマンドは、サーバのステータスを有効として表示します。

```
Device# show ip http server status
HTTP server status: Enabled
HTTP server port: 80
```

例：Web フィルタのドメインプロファイルの設定

次の例は、Web フィルタのドメインプロファイルを設定する方法を示しています。

```
Device(config)# utd web-filter domain profile 1
Device(config-utd-webfltr-domain)# blacklist
Device(config-utd-webf-dmn-bl)# parameter-map regex blist1
Device(config-utd-webf-dmn-bl)# whitelist
Device(config-utd-webf-dmn-wl)# parameter-map regex wlist1
Device(config-utd-webf-dmn-wl)# exit
Device(config-utd-webfltr-domain)# alert all
Device(config-utd-webfltr-domain)# redirect-server external 1.2.3.4
Device(config-utd-webfltr-domain)# exit
```

Web フィルタの URL プロファイルの設定

次の例は、Web フィルタの URL プロファイルを設定する方法を示しています。

```
Device(config)# utd web-filter url profile 1
Device(config-utd-webfltr-url)# blacklist
Device(config-utd-webf-url-bl)# parameter-map regex blist1
Device(config-utd-webf-url-bl)# whitelist
Device(config-utd-webf-url-wl)# parameter-map regex wlist1
Device(config-utd-webf-url-wl)# exit
Device(config-utd-webfltr-url)# categories allow
Device(config-utd-webf-url-cat)# news-and-media
```

```
Device(config-utd-webf-url-cat)# search-engines
Device(config-utd-webf-url-cat)# computer-and-internet-info
Device(config-utd-webf-url-cat)# computer-and-internet-security
Device(config-utd-webf-url-cat)# financial-services
Device(config-utd-webf-url-cat)# image-and-video-search
Device(config-utd-webf-url-cat)# job-search
Device(config-utd-webf-url-cat)#exit
Device(config-utd-webfltr-url)# alert all
Device(config-utd-webfltr-url)# reputation
Device(config-utd-webf-url-rep)# block-threshold suspicious
Device(config-utd-webf-url-rep)# exit
Device(config-utd-webfltr-url)# block local-server 1
Device(config-utd-webfltr-url)# exit
```

UTD Snort IPS または IDS の許可リスト署名の設定

次の例は、署名の許可リストを設定する方法を示しています。

```
Device(config)# utd threat-inspection whitelist
Device(config-utd-whitelist)# generator id 1 signature id 1
Device(config-utd-whitelist)# generator id 1 signature id 2
Device(config-utd-whitelist)# exit
```

例：Web フィルタプロファイルの設定

次の例は、Web フィルタのプロファイルを設定する方法を示しています。

```
Device(config)# utd engine standard
Device(config-utd-eng-std)# logging server 1.2.3.4
Device(config-utd-eng-std)# threat-inspection
Device(config-utd-engstd-insp)#threat protection
Device(config-utd-engstd-insp)# policy security
Device(config-utd-engstd-insp)# logging level emerg
Device(config-utd-engstd-insp)# whitelist
Device(config-utd-engstd-insp)# web-filter
Device(config-utd-engstd-webf)# domain-profile 1
Device(config-utd-engstd-webf)# url-profile 1
Device(config-utd-engstd-webf)# exit
```

例：Web フィルタリングイベントのアラートメッセージ

次に、Web フィルタリングイベントのアラートメッセージの例を示します。

```
016/06/02-14:44:41.061501 IST [**] [Instance_ID: 1] [**] Drop [**] UTD WebFilter Blacklist
 [**] [URL: www.edition.cnn.com/2016/03/31/asia/kolkata-bridge-collapse/index.html]
[Initiator_VRF: 0] {TCP} 1.0.0.9:56608 -> 2.0.0.29:80

2016/06/02-14:48:06.636270 IST [**] [Instance_ID: 1] [**] Pass [**] UTD WebFilter Whitelist
 [**] [URL: www.ndtv.com/index.html] [Initiator_VRF: 0] {TCP} 1.0.0.9:56611 -> 2.0.0.23:80

Jun 2 14:37:57.856 IST: %IOSXE-6-PLATFORM: F0: cpp_cp: QFP:0.0 Thread:000
TS:00000618422205723793 %UTD-6-UTD_DF_BLACKLIST_MATCH: UTD WebFilter Domain Blacklist
[**] [Domain: www.cricinfo.com] [Matched Pattern: www.cricinfo.com] {UDP} 2.0.0.10:53
-> 1.0.0.9:55184

Jun 2 14:39:22.653 IST: %IOSXE-6-PLATFORM: F0: cpp_cp: QFP:0.0 Thread:000
TS:00000618507002407540 %UTD-6-UTD_DF_WHITELIST_MATCH: UTD WebFilter Domain Whitelist
```

```
[**] [Domain: www.cricinfo.com] [Matched Pattern: www.cricinfo.com] {UDP} 2.0.0.10:53
-> 1.0.0.9:55286
```

例：クラウドルックアップの設定解除

次に、Web フィルタリングでクラウドルックアップ機能を設定解除する例を示します。

```
Device(config)# utd engine standard
Device(config-utd-eng-std)# web-filter
% Please ensure urlf-<low/medium/high> virtual-service profile is configured to use the
 web-filter feature

Device(config-utd-engstd-webf)# no cloud-lookup
Device(config-utd-engstd-webf)# end
Device # exit
```

Cisco Web フィルタリングに関する追加の参考資料

関連資料

関連項目	マニュアル タイトル
IOS コマンド	『Cisco IOS Master Command List, All Releases』[英語]
セキュリティ コマンド	• 『Cisco IOS Security Command Reference: Commands A to C』[英語] • 『Cisco IOS Security Command Reference: Commands D to L』 [英語] • 『Cisco IOS Security Command Reference: Commands M to R』 [英語] • 『Cisco IOS Security Command Reference: Commands S to Z』[英語]
UCS E シリーズ サーバ	http://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/e/2-0/gs/guide/b_2_0_Ge

シスコのテクニカル サポート

説明	リンク
シスコのサポート Web サイトでは、シスコの製品やテクノロジーに関するトラブルシューティングにお役立ていただけるように、マニュアルやツールをはじめとする豊富なオンライン リソースを提供しています。 お使いの製品のセキュリティ情報や技術情報を入手するために、Cisco Notification Service（Field Notice からアクセス）、Cisco Technical Services Newsletter、Really Simple Syndication（RSS）フィードなどの各種サービスに加入できます。 シスコのサポート Web サイトのツールにアクセスする際は、Cisco.com のユーザ ID およびパスワードが必要です。	http://www.cisco.com/support

Cisco Web フィルタリングに関する機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *220 : Cisco Web* フィルタリングに関する機能情報

機能名	リリース	機能情報
Cisco Web フィルタリング	Cisco IOS XE Denali リリース 16.3.1	Web フィルタリング機能を使用すると、ドメインベースまたは URL ベースのポリシーとフィルタをデバイスに設定することで、インターネット Web サイトへのアクセスを制御できます。ユーザは Web フィルタリングのプロファイルを設定して Web アクセスを管理できます。Web フィルタリング機能はコンテナサービスを使用して実装され、これは Snort IPS ソリューションに似ています。
ISRv の UTD 機能パリティ UTD サービスの有用性の強化	Cisco IOS XE Fuji リリース 16.8.1	CSR では、シングルテナントモードとマルチテナントモードの両方でのドメインおよび URL フィルタリングに対応しています。ISRv では、シングルテナントのみに対応しています。この機能は、ENCS プラットフォームのすべてのモデルで使用できます。 UTD のエラー回復機能が強化され、IOS から一括設定のダウンロードを開始することで、コンテナが内部エラーから回復できるようになりました。 コマンド **utd web-filter** *profile name*が変更されています。
Web ルート URL フィルタリングの機能強化	Cisco IOS XE Fuji リリース 16.9.1	Web フィルタリングの URLF 仮想リソースプロファイルは、プラットフォーム CSR1000v および ISRv にのみ対応します。 URL フィルタリングは、データベースに存在しないクラウド内の URL を検索するクラウドルックアップ機能に対応しています。

第 166 章

統合脅威防御（UTD）のマルチテナントの設定

統合脅威防御（UTD）のマルチテナントは、複数のユーザに Snort IPS と Web フィルタリングを提供します。1 つの Cisco CSR 1000v インスタンスで 1 つ以上のテナントのポリシーを定義できます。各ポリシーには、脅威検知プロファイルと Web フィルタリングプロファイルを設定できます。次の項では、Unified Threat Defense のマルチテナントを設定する方法について説明します。これらの設定手順で使用されるコマンドの多くは、シングルテナントの設定で使用されるものと似ています。「Snort IPS （2335 ページ）」および「Web フィルタリング （2387 ページ）」を参照してください。

統合脅威防御（UTD）のマルチテナントに関する情報

Snort IPS および Web フィルタリングのマルチテナントを使用すると、1 つの Cisco CSR 1000v のインスタンスで 1 つ以上のテナントのポリシーを定義できます。この機能は、Cisco IOS XE Everest 16.6.1 で導入されました。

各テナントは、1 つ以上の VPN ルーティングおよび転送テーブル（VRF）を持つ VPN ルーティングおよび転送インスタンスです。統合脅威防御（UTD）のポリシーは、脅威検知プロファイルと Web フィルタリングプロファイルに関連付けられています。複数のテナントが UTD ポリシーを共有できます。

システムログには、テナントごとの統計情報の生成を可能にする VRF の名前が含まれます。

マルチテナントモードで使用する CLI コマンドは、シングルテナントモードで使用するものと似ています（Snort IPS （2335 ページ） および Web フィルタリング （2387 ページ） を参照）。マルチテナントでは、サブモードである `utd engine standard multi-tenancy` に入り、UTD ポ

リシー、Webフィルタリング、および脅威検知プロファイルを設定します。`utd engine standard multi-tenancy`のサブモードを終了すると、UTD ポリシーが適用されます。

Web フィルタリングと脅威検知（Snort IPS または IDS）の利点については、次の項で説明します。

- Web フィルタリングの利点 （2392 ページ）
- Snort 仮想サービスインターフェイスの概要 （2412 ページ）

Web フィルタリングの概要

Web フィルタリングにより、URL ベースのポリシーとフィルタを設定することで、インターネットへのアクセスを制御できます。Web フィルタリングは、悪意のあるもしくは不要な Web サイトをブロックし、ネットワークのセキュリティを強化することで、Web サイトへのアクセスの制御に役立ちます。個々の URL またはドメイン名をブロックリストに載せ、それらに対して許可リストポリシーを設定できます。レピュテーションまたはカテゴリに基づいて URL を許可またはブロックするようにプロビジョニングすることもできます。

Snort IPS の概要

Snort IPS 機能は、Cisco 4000 シリーズサービス統合型ルータおよび Cisco クラウドサービスルータ 1000v シリーズのブランチオフィスで侵入防止システム（IPS）または侵入検知システム（IDS）を実現します。この機能は、Snort エンジンを使用して IPS および IDS 機能を実現します。

Snort は、リアルタイムでトラフィック分析を行い、IP ネットワークで脅威が検出されたときにアラートを生成するオープンソースのネットワーク IPS です。また、プロトコル分析、コンテンツ検索またはマッチングを実行し、バッファオーバーフロー、ステルスポートスキャンなどのさまざまな攻撃やプローブを検出することもできます。Snort エンジンは、Cisco 4000 シリーズサービス統合型ルータおよび Cisco クラウドサービスルータ 1000v シリーズで仮想コンテナサービスとして実行されます。

Snort IPS 機能は、IPS または IDS 機能を提供するネットワーク侵入検知および防止モードで動作します。ネットワーク侵入検知および防止モードでは、Snort は次のアクションを実行します。

- ネットワークトラフィックをモニタし、定義されたルールセットに照らしあわせて分析します。
- 攻撃の分類を行います。
- 一致したルールに照らしあわせてアクションを呼び出します。

要件に応じて、IPS または IDS モードで Snort を有効にできます。IDS モードでは、Snort はトラフィックを検査し、アラートを報告しますが、攻撃を防ぐためのアクションは実行しません。IPS モードでは、侵入検知に加えて、攻撃を防ぐためのアクションを実行します。

Snort IPS はトラフィックをモニタし、イベントを外部ログサーバまたは IOS syslog に報告します。IOS syslog へのロギングを有効にすると、ログメッセージが大量に発生する可能性があるため、パフォーマンスに影響する場合があります。Snort ログに対応する外部のサードパーティ製のモニタリングツールを、ログの収集と分析に使用できます。

Snort IPS ソリューション

Snort IPS ソリューションは、次のエンティティで構成されています。

- Snort センサー：トラフィックをモニタして、設定されたセキュリティポリシー（署名、統計情報、プロトコル分析など）に基づいて異常を検出し、アラートサーバまたはレポートサーバにアラートメッセージを送信します。Snort センサーは、仮想コンテナサービスとしてルータに導入されます。
- 署名ストア：定期的に更新される Cisco 署名パッケージをホストします。これらの署名パッケージは、定期的にもしくはオンデマンドで Snort センサーにダウンロードされます。検証済みの署名パッケージは Cisco.com に掲載されます。設定に基づいて、署名パッケージを Cisco.com またはローカルサーバからダウンロードできます。

  次のドメインは、次の cisco.com から署名パッケージをダウンロードするプロセスにおいてルータによってアクセスされます。

  - api.cisco.com
  - apx.cisco.com
  - cloudsso.cisco.com
  - cloudsso-test.cisco.com
  - cloudsso-test3.cisco.com
  - cloudsso-test4.cisco.com
  - cloudsso-test5.cisco.com
  - cloudsso-test6.cisco.com
  - cloudsso.cisco.com
  - download-ssc.cisco.com
  - dl.cisco.com
  - resolver1.opendns.com
  - resolver2.opendns.com

（注） 署名パッケージを保持するためにローカルサーバから署名パッケージをダウンロードする場合は、HTTP のみに対応します。

Snort センサーが署名パッケージを取得するには、Cisco.com の認証情報を使用して、署名パッケージを Cisco.com からローカルサーバに手動でダウンロードする必要があります。

URL が IP アドレスとして指定されていない場合、Snort コンテナは（ルータに設定された DNS サーバ上で）ドメイン名ルックアップを実行して、Cisco.com によるまたはローカルサーバ上の自動署名更新の場所を解決します。

- アラートまたはレポートサーバ：Snort センサーからアラートイベントを受信します。Snort センサーによって生成されたアラートイベントは、IOS syslog または外部 syslog サーバ、もしくは IOS syslog と外部 syslog サーバの両方に送信できます。Snort IPS ソリューションに付属している外部ログサーバはありません。
- 管理：Snort IPS ソリューションを管理します。管理は、IOS CLI を使用して設定します。Snort センサーには直接アクセスできず、すべての設定は IOS CLI を使用してのみ行えます。

Snort 仮想サービスインターフェイスの概要

Snort センサーは、ルータ上でサービスとして動作します。サービスコンテナは、仮想テクノロジーを使用して、アプリケーション用の Cisco デバイスにホスティング環境を提供します。

Snort トラフィック検査は、インターフェイス単位で、または対応しているすべてのインターフェイスでグローバルに有効にできます。検査対象のトラフィックは Snort センサーに転送され、再度投入されます。侵入検知システム（IDS）では、識別された脅威がログイベントとして報告され、許可されます。ただし、侵入防止システム（IPS）では、ログイベントとともに攻撃を防ぐためのアクションが実行されます。

Snort センサーには 2 つの VirtualPortGroup インターフェイスが必要です。最初の VirtualPortGroup インターフェイスは管理トラフィックに使用され、2 つ目は転送プレーンと Snort 仮想コンテナサービス間のデータトラフィックに使用されます。これらの VirtualPortGroup インターフェイスには、ゲスト IP アドレスを設定する必要があります。管理 VirtualPortGroup インターフェイスに割り当てられた IP サブネットは、署名サーバおよびアラート / 報告サーバと通信できる必要があります。

2 つ目の VirtualPortGroup インターフェイスの IP サブネットは、このインターフェイス上のトラフィックがルータ内部にあるため、カスタマーネットワーク上でルーティング可能であってはなりません。内部サブネットを外部に公開することはセキュリティ上のリスクとなります。2 つ目の VirtualPortGroup サブネットには 192.0.2.0/30 の IP アドレス範囲を使用することをお勧めします。192.0.2.0/24 のサブネットを使用することは、RFC 3330 で定義されています。

仮想サービスが実行されているルータと同じ管理ネットワークで、Snort 仮想コンテナサービスの IP アドレスを割り当てることができます。この設定は、syslog またはアップデートサーバが管理ネットワーク上にあり、他のインターフェイスからアクセスできない場合に役立ちます。

統合脅威防御（UTD）のマルチテナントの設定に関する制約事項

-
- ドメインベースのフィルタリングには対応しません。
- 各 Cisco CSR 1000v インスタンスで最大25のテナントに対応します。
- 最大 25 のポリシーに対応します。
- Cisco CSR 1000v では、最大 50,000 の同時セッションに対応します。
-
- ブロックリストまたは許可リストのルールは、正規表現のパターンのみに対応します。現在、ブロックリストまたは許可リストのルールごとに 64 のパターンに対応しています。ただし、各テナントには複数のルールを設定できます。
- ローカルブロックサーバは、HTTPS ブロックページの提供には対応していません。URL フィルタがブロックページまたはリダイレクトメッセージを挿入しようとする場合、HTTPS トラフィックには対応しません。
- URL にユーザ名とパスワードがある場合、ブロックリストまたは許可リストのパターンと一致する前に、URL フィルタがユーザ名とパスワードを URL から削除することはしません。ただし、カテゴリまたはレピュテーションルックアップにはこの制限はなく、ルックアップの前に URL からユーザ名とパスワードを削除します。
- HTTPS 検査は制限されています。Web フィルタリングでは、サーバ証明書を使用して URL およびドメイン情報を取得します。完全な URL のパスを検査することはできません。
- UTD は、VRF 間シナリオにおいては WCCP および NBAR との相互運用は行いません。
- Snort IPS コマンドの `threat inspection profile` *`profile-name`* は、ID（番号）ではなく英数字のプロファイル名を使用します。

統合脅威防御（UTD）のマルチテナントの設定方法

対応しているデバイスに Unified Threat Defense のマルチテナント機能を導入するには、次のタスクを実行します。

始める前に

マルチテナント用に Web フィルタリングおよび脅威検知をインストールするデバイスをプロビジョニングします。この機能は現在、Cisco CSR 1000v でのみ対応しています。

ライセンスを取得します。UTD は、セキュリティパッケージを実行しているルータでのみ使用でき、サービスを有効にするにはセキュリティライセンスが必要となります。セキュリティライセンスの取得については、シスコサポートにお問い合わせください。

手順の概要

1. 仮想サービスをインストールしてアクティブにします。マルチテナント用の UTD OVA ファイルのインストール （2414 ページ）
2. VirtualPortGroup のインターフェイスおよび仮想サービスを設定します。マルチテナント用の VirtualPortGroup インターフェイスと仮想サービスの設定方法 （2415 ページ）
3. VRF を設定します。マルチテナント用の VRF の設定方法 （2418 ページ）
4. マルチテナント用の脅威検知と Web フィルタリングを設定します。マルチテナント Web フィルタリングおよび脅威検知の設定方法 （2419 ページ）

手順の詳細

ステップ 1 仮想サービスをインストールしてアクティブにします。マルチテナント用の UTD OVA ファイルのインストール （2414 ページ）

ステップ 2 VirtualPortGroup のインターフェイスおよび仮想サービスを設定します。マルチテナント用の VirtualPortGroup インターフェイスと仮想サービスの設定方法 （2415 ページ）

ステップ 3 VRF を設定します。マルチテナント用の VRF の設定方法 （2418 ページ）

ステップ 4 マルチテナント用の脅威検知と Web フィルタリングを設定します。マルチテナント Web フィルタリングおよび脅威検知の設定方法 （2419 ページ）

マルチテナント用の UTD OVA ファイルのインストール

仮想サービスの OVA ファイルは、仮想マシンの圧縮された「インストール可能な」バージョンを含むオープン仮想アーカイブファイルです。この OVA ファイルをルータにダウンロードしてから、仮想サービスをインストールする必要があります。仮想サービスの OVA ファイルは、ルータにインストールされている Cisco IOS XE リリースイメージには付属していません。OVA ファイルは、ルータのフラッシュメモリに事前にインストールされている場合があります。

OVA ファイルをインストールするには、セキュリティライセンス付きの Cisco IOS XE イメージを使用する必要があります。インストール中に、セキュリティライセンスのチェックが行われます。

仮想サービスのインストール例：

```
Device> enable
Device# virtual-service install name utd package
bootflash:utdsnort.1.0.4_SV2983_XE_16_6.20170623_174453_RELEASE.ova
Device# show virtual-service list

Name Status    Package Name
```

```
--------------------------------------------------------------------------------
utd Activated utdsnort.1.0.4_SV2983_XE_16_6.20170
```

仮想サービスのアップグレードの例：

```
Device> enable
Device# virtual-service upgrade name utd package
bootflash:utdsnort.1.0.4_SV2983_XE_16_6.20170623_174453_RELEASE.ova
Device# show virtual-service list

Name Status   Package Name
--------------------------------------------------------------------------------
utd Activated utdsnort.1.0.4_SV2983_XE_16_6.20170
```

仮想サービスのアンインストールの例：

```
Device> enable
Device# virtual-service uninstall name utd
Device# show virtual-service list

Virtual Service List:
```

マルチテナント用のVirtualPortGroupインターフェイスと仮想サービスの設定方法

この手順に示すように、マルチテナントの場合、2 つの VirtualPortGroup インターフェイスと両方のインターフェイスのゲスト IP アドレスを設定する必要があります。

（注） データトラフィック用の VirtualPortGroup インターフェイスは、プライベートまたはルーティング不可の IP アドレスを使用する必要があります。このインターフェイスには、IP アドレスの範囲として 192.0.2.0 / 30を 使用することを推奨します。

手順の概要

1. **enable**
2. **configure terminal**
3. **interface VirtualPortGroup** *interface-number*
4. **ip address** *ip-address mask*
5. **exit**
6. **interface VirtualPortGroup** *interface-number*
7. **ip address** *ip-address mask*
8. **exit**
9. **virtual-service** *name*
10. **profile multi-tenancy**
11. **vnic gateway VirtualPortGroup** *interface-number*
12. **guest ip address** *ip-address*
13. **exit**
14. **vnic gateway VirtualPortGroup** *interface-number*

15. **guest ip address** *ip-address*
16. **exit**
17. **activate**
18. **end**
19. **show virtual-service list**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface VirtualPortGroup** *interface-number* 例： `Device(config)# interface VirtualPortGroup 0`	インターフェイス設定モードに入り、VirtualPortGroup インターフェイスを設定します。このインターフェイスは、管理インターフェイスの GigabitEthernet0 が使用されていない場合に管理トラフィックに対して使用されます。
ステップ 4	**ip address** *ip-address mask* 例： `Device(config-if)# ip address 10.1.1.1 255.255.255.252`	インターフェイスのプライマリ IP アドレスを設定します。このインターフェイスは、署名アップデートサーバおよび外部ログサーバにルーティング可能である必要があります。
ステップ 5	**exit** 例： `Device(config-if)# exit`	インターフェイス設定モードを終了し、グローバル設定モードに戻ります。
ステップ 6	**interface VirtualPortGroup** *interface-number* 例： `Device(config)# interface VirtualPortGroup 1`	インターフェイスを設定し、インターフェイス設定モードを開始します。VirtualPortGroup インターフェイスを設定します。このインターフェイスは、データトラフィックに使用されます。
ステップ 7	**ip address** *ip-address mask* 例： `Device(config-if)# ip address 192.0.2.1 255.255.255.252`	インターフェイスのプライマリ IP アドレスを設定します。この IP アドレスは、外部ネットワークに対してルーティング不能である必要があります。IP アドレスは、推奨される 192.0.2.0/30 のサブネットから割り当てられます。
ステップ 8	**exit** 例： `Device(config-if)# exit`	インターフェイス コンフィギュレーション モードを終了し、グローバルコンフィギュレーションモードに戻ります。

	コマンドまたはアクション	目的
ステップ 9	**virtual-service** *name* 例： `Device(config)# virtual-service utd`	仮想コンテナサービスを設定し、仮想サービス設定モードに入ります。*name* 引数は、仮想コンテナサービスを識別するために使用される論理名です。
ステップ 10	**profile multi-tenancy** 例： `Device(config-virt-serv)#profile multi-tenancy`	リソースプロファイルを設定します。マルチテナントモードの場合（Cisco CSR 1000v のみ）、このプロファイル マルチテナント コマンドを設定する必要があります。
ステップ 11	**vnic gateway VirtualPortGroup** *interface-number* 例： `Device(config-virt-serv)# vnic gateway VirtualPortGroup 0`	仮想サービスの仮想ネットワーク インターフェイス カード（vNIC：virtual network interface card）設定モードに入ります。仮想コンテナサービス用の vNIC ゲートウェイ インターフェイスを作成し、vNIC ゲートウェイ インターフェイスを仮想ポートグループ インターフェイスにマッピングします。これは、手順3で設定したインターフェイスです。
ステップ 12	**guest ip address** *ip-address* 例： `Device(config-virt-serv-vnic)# guest ip address 10.1.1.2`	vNIC ゲートウェイ インターフェイスのゲスト vNIC アドレスを設定します。
ステップ 13	**exit** 例： `Device(config-virt-serv-vnic)# exit`	仮想サービスの vNIC 設定モードを終了し、仮想サービス設定モードに戻ります。
ステップ 14	**vnic gateway VirtualPortGroup** *interface-number* 例： `Device(config-virt-serv)# vnic gateway VirtualPortGroup 1`	仮想サービスの vNIC 設定モードに入ります。仮想コンテナサービス用の vNIC ゲートウェイ インターフェイスを設定し、インターフェイスを仮想ポートグループにマッピングします。手順6で設定されたインターフェイス（*interface-number*）は、ユーザトラフィックをモニタするために Snort エンジンによって使用されます。
ステップ 15	**guest ip address** *ip-address* 例： `Device(config-virt-serv-vnic)# guest ip address 192.0.2.2`	vNIC ゲートウェイ インターフェイスのゲスト vNIC アドレスを設定します。
ステップ 16	**exit** 例： `Device(config-virt-serv-vnic)# exit`	仮想サービスの vNIC 設定モードを終了し、仮想サービス設定モードに戻ります。
ステップ 17	**activate** 例：	仮想コンテナサービスにインストールされたアプリケーションをアクティブにします。

	コマンドまたはアクション	目的
	`Device(config-virt-serv)# activate`	
ステップ 18	**end** 例： `Device(config-virt-serv)# end`	仮想サービス設定モードを終了し、特権EXECモードに戻ります。

ステップ 19	**show virtual-service list**
	例：
	`Device# show virtual-service list`
	
	`Virtual Service List:`
	
	`Name Status Package Name`
	`----------`
	`utd Activated utdsnort.1.0.4_SV2983_XE_16_6.20170`	

マルチテナント用の VRF の設定方法

この手順では、テナントの VRF を設定するために必要な一般的な手順について説明します。この手順は後にマルチテナント Web フィルタリングおよび脅威検知の設定方法（2419 ページ）で使います。

（注） VRF 間トラフィックの場合、2 つの VRF 間を流れるトラフィックに UTD 用の入力インターフェイスと出力インターフェイスが設定されている場合、セッションを表す VRF を決定するルールが適用されます。選択した VRF の UTD ポリシーは、VRF 間トラフィックのすべてのパケットに適用されます。

手順の概要

1. **vrf definition** *vrf-name*
2. **rd** *route-distinguisher*
3. **address-family ipv4**
4. **exit address-family**
5. VRF ごとに手順 1 ～ 4 を繰り返します。

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**vrf definition** *vrf-name* 例： `Device(config)# vrf definition 100`	VRF 名を定義し、VRF 設定モードに入ります。

	コマンドまたはアクション	目的
ステップ 2	**rd** *route-distinguisher* 例： `Device(config-vrf)# rd 100:1`	ルーティングテーブルと転送テーブルを作成し、ルート識別子を「VRF 名」という名前の VRF インスタンスに関連付けます。ルータはルート識別子を使用して、パケットが属する VRF を識別します。ルート識別子は、次の 2 つのタイプのいずれかとなります。 • 自律システム関連。AS 番号 xxx および任意の番号 y：xxx:y • IP アドレス関連。IP アドレス A.B.C.D および任意の番号 y：A.B.C.D:y
ステップ 3	**address-family ipv4** 例： `Device(config-vrf)# address-family ipv4`	IP バージョン 4 アドレスを使用してルーティングセッションを設定するためのアドレスファミリ設定モードに入ります。
ステップ 4	**exit address-family** 例： `Device(config-vrf-af)# exit`	アドレスファミリ設定モードを終了します。
ステップ 5	VRF ごとに手順 1 ～ 4 を繰り返します。	

マルチテナント Web フィルタリングおよび脅威検知の設定方法

マルチテナント（複数のテナントまたは VRF）の脅威検知（IPS または IDS）および Web フィルタリングを設定するには、次の手順を実行します。

この手順では、ブロックリストと許可リストの定義を最初の手順 1 ー 5 に示します。主な設定手順（マルチテナント用の UTD 標準エンジンの設定モード）は、手順 6 以降に示しています。

（注） シングルテナント用の脅威検知と Web フィルタリングの詳細については、Snort IPS （2335 ページ） および Web フィルタリング （2387 ページ） を参照してください。

始める前に

`no utd engine standard` コマンドを使用して、既存のシングルテナントの UTD 設定を削除します。

テナントごとに VRF を事前に設定しておく必要があります（マルチテナント用の VRF の設定方法 （2418 ページ） を参照）。

手順

	コマンドまたはアクション	目的
ステップ 1	**parameter-map type regex** *blacklist-name* 例： `Device(config)# parameter-map type regex urlf-blacklist1`	ブロックリストのパラメータマップを定義します。これは、後に手順 17 で使用します。

ステップ 2	**pattern** *URL-name*
	例：
	`Device(config-profile)# pattern www\.cnn\.com`
	`Device(config-profile)# pattern www\.msnbc\.com`
		ブロックリストに登録する URL を定義します。*URL-name* 内のピリオドの前には、必ずエスケープ「\」文字を入れてください。ブロックリストに複数の URL を設定するには、この手順を繰り返します。

ステップ 3	**parameter-map type regex** *whitelist-name* 例： `Device(config-profile)# parameter-map type regex urlf-whitelist1`	許可リストのパラメータマップを定義します。これは、後に手順 20 で使用します。
ステップ 4	**pattern** *URL-name* 例： `Device(config-profile)# pattern www\.nfl\.com`	許可リストに登録する URL を定義します。ブロックリストの URL では、*URL-name* 内のピリオドの前には、必ずエスケープ「\」文字を入れてください。許可リストに複数の URL を設定するには、この手順を繰り返します。
ステップ 5	**exit** 例： `Device(config-profile)# exit`	
ステップ 6	**utd multi-tenancy** 例： `Device(config)# utd multi-tenancy`	このコマンドは、次の `utd engine standard multi-tenancy` コマンドに備えて、スイッチの役割を果たします。
ステップ 7	**utd engine standard multi-tenancy** 例： `Device(config)# utd engine standard multi-tenancy`	マルチテナント用の UTD 標準エンジンの設定モードに入ります。 （注） 後に手順 50 で UTD 標準エンジンの設定モードを終了すると、ポリシー設定が適用されます。
ステップ 8	**web-filter sourcedb** *sourcedb-number* 例： `Device(config)# web-filter sourcedb 1`	Web フィルタリングのソース DB プロファイル（*sourcedb-number* は数字）を設定します。これは、後に手順 29 で使用されます。

	コマンドまたはアクション	目的
ステップ 9	**logging level** {**alerts** | **critical** | **debugging** | **emergencies** | **errors** | **informational** | **notifications** | **warnings**} 例： `Device(config)# logging level errors`	Web フィルタリングイベントに関して報告されるシステムメッセージのレベルを設定します。指定したレベル以下のメッセージが報告されます。（各レベルには、次の表に示す数値があります） **表 *221 :* システム メッセージのシビラティ（重大度）** レベル / 説明 0：emergencies / システムが使用不可 1：alerts / 即時処理が必要 2：critical / クリティカル状態 3：errors / エラー状態 4：warnings / 警告状態 5：notifications / 正常だが注意を要する状態 6：informational / 情報メッセージだけ 7：debugging / デバッグ実行時にのみ表示
ステップ 10	**web-filter block local-server profile** *profile-id* 例： `Device(config-utd-multi-tenancy)# web-filter block local-server profile 1` コンテンツのテキストはローカルサーバによって表示されます。	Webフィルタリングのローカルブロックサーバのプロファイルを設定します。*profile-id* の値の範囲は 1 ー 255 です。 「ローカルブロックサーバを使用した URL ベースの Web フィルタリングの設定」を参照してください。 （注） マルチテナント用のコマンドを設定する場合、シングルテナントと比較して、最初の `utd` というキーワードを使用しないでください。
ステップ 11	**block-page-interface loopback** *id* 例： `Device(config-utd-mt-webf-blk-srvr)# block-page-interface loopback 110`	ループバックインターフェイスにこのプロファイルを関連付けます。このループバックインターフェイスの IP アドレスは、ブロックローカルサーバの IP アドレスとして使用されます。
ステップ 12	**content text** *display-text* 例：	ブロックされたページにアクセスした後に表示される警告テキストを指定します。

	コマンドまたはアクション	目的
	`Device(config-utd-mt-webf-blk-srvr)# content text "Blocked by Web-Filter"`	
ステップ 13	**http-ports** *port-number* 例： `Device(config-utd-mt-webf-blk-srvr)# http-ports 80`	http ポート値は、カンマで区切られたポートの文字列です。nginx HTTP サーバはこれらのポートをリッスンします。

ステップ 14	**web-filter block page profile** *profile-name*
	例：
	`Device(config-utd-multi-tenancy)# web-filter block page profile 1`
	`Device(config-utd-mt-webf-block-urc)# text "this page is blocked"`
		インラインブロックページを使用した URL ベースの Web フィルタリングの設定（2401 ページ）を参照してください。ただし、マルチテナント用にここで使用されるコマンドは、シングルテナント用に使用される `utd` キーワードを使用しません）。

ステップ 15	**web-filter url profile** *web-filter-profile-id*
	例：
	`Device(config-utd-multi-tenancy)# web-filter url profile 1`
	`Device(config-utd-mt-webfltr-url)#`
		Web フィルタリングの URL プロファイルである *web-filter-profile-id* を指定します。値は 1 ～ 255 です。このコマンドの後、ブロックリスト、許可リスト、およびカテゴリのアラートを設定できます。詳細については、「インラインブロックページを使用した URL ベースの Web フィルタリングの設定」を参照してください。
		（注） マルチテナント用のコマンドを設定する場合、シングルテナントと比較して、最初の `utd` というキーワードを使用しないでください。

ステップ 16	**blacklist** 例： `Device(config-utd-mt-webfltr-url)# blacklist`	Web フィルタリングのブロックリストの設定モードに入ります。
ステップ 17	**parameter-map regex** *blacklist-name* 例： `Device(config-utd-mt-webf-url-bl)# parameter-map regex urlf-blacklist1`	手順 1 で前に定義したブロックリストを使用して、パラメータマップの正規表現を指定します。

ステップ 18	**exit**
	例：
	`Device(config-utd-mt-webf-url-bl)# exit`
	`Device(config-utd-mt-webfltr-url)#`
		Web フィルタリングのブロックリストの設定モードを終了します。

ステップ 19	**whitelist** 例：	Web フィルタリングの許可リストの設定モードに入ります。

	コマンドまたはアクション	目的
	`Device(config-utd-mt-webfltr-url)# whitelist` `Device(config-utd-mt-webf-url-wl)#`	
ステップ 20	**parameter-map regex** *whitelist-name* 例： `Device(config-utd-mt-webf-url-wl)# parameter-map regex urlf-list1`	手順3で前に定義した許可リストを使用して、パラメータマップの正規表現を指定します。

ステップ 21	**exit**
	例：
	`Device(config-utd-mt-webf-url-wl)# exit`
	`Device(config-utd-mt-webfltr-url)#`
		Web フィルタリングの許可リストの設定モードを終了します。

ステップ 22	**exit**
	例：
	`Device(config-utd-mt-webfltr-url)# exit`
	`Device(config-utd-multi-tenancy)#`
		Web フィルタリングの URL プロファイルモードを終了します。

ステップ 23	**utd global** 例： `Device(config-utd-multi-tenancy)# utd global`	`utd global` に入力されたコマンドは、すべてのテナントまたはポリシーに適用されます。Cisco CSR 1000v インスタンスの場合のコマンド例は、`logginghost syslog` および `threat inspection` などです。

ステップ 24	**logging** {**host** *hostname* | **syslog**}
	例：
	この例では、アラートは指定されたホストのログファイルに記録されます。
	`Device(config-utd-mt-utd-global)# logging host systemlog1`
	例：
	この例では、アラートは IOS syslog に記録されます。
	`Device(config-utd-mt-utd-global)# logging syslog`
		`logging` コマンドは、syslog メッセージの送信先となるホスト名または IOS syslog を指定します。

ステップ 25	**threat inspection** 例： `Device(config-utd-mt-utd-global)# threat inspection`	グローバル脅威検知モードに入ります。
ステップ 26	**signature update server** {**cisco** | **url** *url* } [**username** *username* [**password** *password*]] 例：	署名更新サーバのパラメータを設定します。サーバの詳細で署名更新パラメータを指定する必要があります。署名の更新に www.cisco.com を使用する場合は、ユーザ名とパスワードを入力する必要がありま

	コマンドまたはアクション	目的
	`Device(config-utd-mt-utd-global-threat)# signature update server cisco username abcd password cisco123`	す。署名の更新にローカルサーバを使用する場合は、サーバ設定に基づいてユーザ名とパスワードを指定できます。ルータは、インターネットに接続することでドメイン名を解決できる必要があります。
ステップ 27	**signature update occur-at** {**daily** | **monthly** *day-of-month* | **weekly** *day-of-week*} *hour minute* 例： `Device(config-utd-mt-utd-global-threat)# signature update occur-at daily 0 0`	署名の更新間隔パラメータを設定します。この設定をすることで、午前0時に署名の更新がトリガーされます。
ステップ 28	**web-filter** 例： `Device(config-utd-mt-utd-global-threat)# web-filter`	このコマンドは、次の `sourcedb` コマンドと組み合わせて使用し、Web フィルタリングの URL ソースデータベースを指定します。
ステップ 29	**sourcedb** *sourcedb-number* 例： `Device(config-utd-mt-utd-global-threat)# sourcedb 1`	Web フィルタリングのソースデータベースを割り当てます。アクティブにできるソースデータベースは 1 つだけです。
ステップ 30	**exit** 例： `Device(config-utd-mt-utd-global-threat)# exit`	脅威検知設定モードを終了します。
ステップ 31	**exit** 例： `Device(config-utd-mt-global)# exit`	グローバル更新設定モードを終了します。
ステップ 32	**threat-inspection whitelist profile** *policy-name* 例： `Device(config-utd-multi-tenancy)# threat-inspection whitelist profile wh101`	許可リストのプロファイルを現在設定されているポリシーに関連付けます。同様のコマンドがシングルテナントで使用されますが、`utd` キーワードを使用します。
ステップ 33	**signature id** *id* 例： `Device(config-utd-mt-list)# signature id 101`	以前に脅威として特定した ID である *id* を指定します。たとえば、アラートのログファイルの ID を確認した後などです。 複数の署名 ID に対してこのコマンドを繰り返します。
ステップ 34	**exit** 例： `Device(config-utd-mt-whitelist)# exit`	許可リストの設定モードを終了します。

	コマンドまたはアクション	目的
ステップ 35	**threat-inspection profile** *profile-name* 例： `Device(config-utd-multi-tenancy)# threat-inspection profile 101`	脅威検知プロファイルを設定することで、複数のテナントにより再利用できるようになります。複数の脅威検知プロファイルを設定できます。プロファイル内では、複数の許可リストを設定できます。 `profile-name` は英数字です。
ステップ 36	**threat** {**detection** | **protection** } 例： `Device(config-utd-mt-threat)# threat protection`	Snort エンジンの動作モードとして侵入検知システム（IDS）または侵入防止システム（IPS）を指定します。 デフォルトは **threat detection** です。
ステップ 37	**policy** {**balanced** | **connectivity** | **security**} 例： `Device(config-utd-mt-threat)# policy security`	Snort エンジンのセキュリティポリシーを設定します。 • デフォルトのセキュリティポリシータイプは **balanced** です。
ステップ 38	**logging level**{**alert** | **crit** | **debug** | **emerg** | **err** | **info** | **notice** | **warning**}	次のいずれかのカテゴリのログを表示します。 • alert：アラートレベルのログを表示します（シビラティ（重大度）＝2）。 • crit：クリティカルレベルのログ（シビラティ（重大度）＝3） • debug：すべてのログ（シビラティ（重大度）＝8） • emerg：緊急レベルのログ（シビラティ（重大度）＝1） • err：エラーレベルのログ（シビラティ（重大度）＝4）デフォルト。 • info：情報レベルのログ（シビラティ（重大度）＝7） • notice：通知レベルのログ（シビラティ（重大度）＝6） • warning：警告レベルのログ（シビラティ（重大度）＝5）
ステップ 39	**whitelist profile** *profile-name* 例： `Device(config-utd-mt-threat)# whitelist profile wh101`	また、許可リストプロファイルを別の場所にある許可リストのプロファイルに対してのみ指定することもできます（上記の `threat-inspection whitelist profile` コマンド）。

	コマンドまたはアクション	目的
		（オプション）UTD エンジンで許可リストを有効にします。
ステップ 40	**exit** 例： `Device(config-utd-mt-threat)# exit`	脅威検知モードを終了します。
ステップ 41	脅威検知プロファイルを追加するには、手順 35 ー 40 を繰り返します。	
ステップ 42	**policy** *policy-name* 例： `Device(config-utd-multi-tenancy)# policy pol101`	複数のテナントに関連付けるポリシーを定義します。脅威検知（IPS）および Web フィルタリングのプロファイルがポリシーに追加されます。
ステップ 43	**vrf** [*vrf-name* | global] 例： この例では、2 つのテナント（VRF）と 2 つのポリシーの設定を示します。 `Device(config-utd-mt-policy)# vrf vrf101`	UTD ポリシーを使用する VRF（テナント）ごとに `vrf vrf-name` コマンドを繰り返し入力します。以前に定義されたこれらの VRF については、マルチテナント用の VRF の設定方法（2418 ページ） を参照してください。 または、`vrf global` を使用してグローバル（デフォルト）VRF に関連付け、インターフェイスで VRF を有効にします。
ステップ 44	**all-interfaces** 例： `Device(config-utd-mt-policy)# all-interfaces`	（オプション）VRF のすべてのインターフェイスをポリシーに関連付けます。
ステップ 45	**threat-inspection profile** *profile-name* 例： `Device(config-utd-mt-policy)# threat-inspection profile 101`	（オプション）以前に定義した脅威検知プロファイルにポリシーを関連付けます。手順 35 を参照してください。
ステップ 46	**web-filter url profile** *web-filter-profile-id* 例： `Device(config-utd-mt-policy)# web-filter url profile 1`	（オプション）以前に定義した Web フィルタリングのプロファイルにポリシーを関連付けます。手順 15 を参照してください。
ステップ 47	**fail close** 例： `Device(config-utd-mt-policy)# fail close`	（オプション）エンジン障害時に IPS または IDS パケットをドロップします。デフォルトは `fail open` です。
ステップ 48	**exit**	ポリシー設定モードを終了します。
ステップ 49	各ポリシーに対して手順 42 ー 48 を繰り返します。	

	コマンドまたはアクション	目的
ステップ 50	**exit** 例： `Device(config-utd-multi-tenancy)# exit`	`utd engine standard multi-tenancy`モードを終了します。 ポリシー設定が適用されます。これには数分かかる場合があります。この間は、`utd engine standard multi-tenancy`設定モードのコマンドはそれ以上入力できません。

ステップ 51	**exit**
	例：
	`Device(config)# exit`
	`Device#`	

ステップ 52	**show logging**
	例：
	`Device(config)# show logging`
	`..UTD MT configuration download has started`
	`..UTD MT configuration download has completed`	

ステップ 53	**interface** *sub-interface* 例： `Device(config)# interface GigabitEthernet4.101`	テナント（VRF）に使用するサブインターフェイスを指定します。
ステップ 54	**encapsulation dot1Q** *vlan-id* 例： `Device(config-if)# encapsulation dot1Q 101`	VLAN ID をサブインターフェイスに適用します。
ステップ 55	**ip vrf forwarding** *vrf-name* 例： `Device(config-if)# ip vrf forwarding vrf101`	VRF インスタンスをサブインターフェイスに関連付けます。
ステップ 56	**ip address** *ip-address subnet-mask* 例： `Device(config-if)# ip address 111.0.0.1 255.255.255.0`	VRF のサブインターフェイスの IP アドレスを指定します。
ステップ 57	**ip route** *ip-address subnet-mask sub-interface* 例： この例では、VRF のサブネット GigabitEthernet4.101 は、静的 IP アドレス 111.0.0.0 255.255.255.0 を使用してグローバル ルーティング テーブルにリンクされています。 `Device(config-if)# ip route 111.0.0.0 255.255.255.0 GigabitEthernet4.101`	（オプション）次の手順のこの `ip route` コマンドと `ip route vrf` コマンドはオプションです。VRF とグローバル ルーティング テーブル間の静的ルートを使用してルートリークを設定する場合にこれらの手順を使用できます。 これにより、VRF インターフェイスから VRF サブネットへの静的ルートが設定され、VRF サブネットにグローバル ルーティング テーブルからアクセ

	コマンドまたはアクション	目的
		スできるようになります。ルートリークの設定の詳細については、「MPLS または VPN ネットワークでのルートリーク」を参照してください。
ステップ 58	**ip route vrf** *vrf-name ip-address subnet-mask* **global** 例： `Device(config-if)# ip route vrf vrf101 0.0.0.0 0.0.0.0 5.2.1.1 global`	（オプション）この手順と前の手順は任意となります。VRF とグローバル ルーティング テーブル間の静的ルートを使用してルートリークを設定する場合は、次の手順を使用できます。ルートリークの設定の詳細については、「MPLS または VPN ネットワークでのルートリーク」を参照してください。 グローバル ルーティング テーブルへの静的 VRF のデフォルトルートを指定します。
ステップ 59	**utd enable**	（オプション）インターフェイス上で UTD を有効にします。このコマンドは、`all-interfaces` コマンドが設定されていない場合に使用できます（手順 44 内）。
ステップ 60	各テナント（VRF）のサブインターフェイスを設定するには、手順 53 ー 59 を繰り返します。	
ステップ 61	**exit**	インターフェイス設定モードを終了します。

Web フィルタリングおよび脅威検知（IPS）のプロファイルが適用されました。

設定例：統合脅威防御（UTD） のマルチテナント

この例は、2 つのテナントの UTD にマルチテナントを設定した後の一般的な実行設定を示しています。

（注） 次の例では、パラメータマップである `urlf-blacklist1` および `urlf-whitelist1` について説明します。これらのパラメータマップの設定は、例には示されていません。ブロックリストおよび承認済みリストのパラメータマップの詳細については、「インラインブロックページを使用した URL ベースの Web フィルタリングの設定」を参照してください。

```
utd multi-tenancy
utd engine standard multi-tenancy
 web-filter block page profile 1
  text "This page is blocked"
 web-filter block page profile 2
  text "This page is blocked"
 web-filter url profile 1
  alert all
  blacklist
   parameter-map regex urlf-blacklist1
  whitelist
```

```
  parameter-map regex urlf-whitelist1
 categories block
  social-network
  sports
 block page-profile 1
 log level error
web-filter url profile 2
 alert all
 blacklist
  parameter-map regex urlf-blacklist2
 categories block
  shopping
  news-and-media
  sports
  real-estate
  motor-vehicles
 block page-profile 2
 log level error
 reputation
  block-threshold low-risk
web-filter sourcedb 1
 logging level error
threat-inspection whitelist profile wh101
 signature id 101
threat-inspection profile 101
 threat protection
 policy security
 logging level debug
 whitelist profile wh101
threat-inspection profile 102
 threat detection
 policy security
 logging level debug
utd global
 logging host 172.27.58.211
 logging host 172.27.58.212
 logging host 172.27.56.97
 threat-inspection
  signature update server cisco username abc password
]RDCe[B\^KFI_LgQgCFeBEKWP^SWZMZMb]KKAAB
  signature update occur-at daily 0 0
 web-filter
  sourcedb 1
policy pol102
 vrf vrf102
 all-interfaces
 threat-inspection profile 102
 web-filter url profile 2
policy pol101
 vrf vrf101
 all-interfaces
 threat-inspection profile 101
 web-filter url profile 1
 fail close
```

統合脅威防御エンジンの標準設定の確認

次のコマンドを使用して、設定を確認します。

手順の概要

1. **enable**
2. **show utd multi-tenancy**
3. **show utd engine standard global**
4. **show utd engine standard status**
5. **show utd engine standard statistics**
6. **show utd engine standard statistics daq** [**dp** | **cp**]
7. **show utd engine standard statistics url-filtering** [**engine** | *no*]
8. **show utd engine standard statistics url-filtering vrf name** *vrf-name*
9. **show utd engine standard statistics internal**
10. **show utd engine standard logging event**
11. **show logging** | **include** CONFIG_DOWNLOAD
12. **show utd threat-inspection whitelist** [**profile** *profile-name*]
13. **show utd threat-inspection profile** *profile-name*
14. **show utd** [**policy** *profile-name*]
15. **show utd web-filter url** [**profile** *profile-name*]
16. **show utd web-filter block local-server** [**profile** *profile-name*]
17. **show utd web-filter sourcedb** [**profile** *profile-name*]
18. **show utd engine standard statistics daq dp** [**engine** *engine-num*] [**vrf** [**name** *vrf-name* | **global**]]
19. **show utd engine standard config threat-inspection whitelist** [**profile** *profile-name*]
20. **show utd engine standard config web-filter url profile** *profile-name*
21. **show utd engine standard config** [**vrf name** *vrf-name*]
22. **show utd engine standard config threat-inspection profile** *profile-name*
23. **show utd engine standard threat-inspection signature update status**
24. **show platform software qfp active feature utd config** [**vrf**[{**id** *vrf-id* | **name** *vrf-name* | **global** }]
25. **show platform software utd interfaces**
26. **show platform hardware qfp active feature utd config** [**vrf** {**id** *vrf-id* | **name** *vrf-name* | **global** }]
27. **show platform hardware qfp active feature utd stats** [**clear** | **divert** | **drop** | **general** | **summary**] [**vrf** {**id** *vrf-id* | **name** *vrf-name* | **global** }] [all] [**verbose**]
28. **show platform hardware qfp active feature utd stats summary** [**vrf name** *vrf-name* | **all**]
29. **show platform hardware qfp active feature utd stats drop all**

手順の詳細

ステップ 1 **enable**

例：

```
Device# enable
```

特権 EXEC モードを有効にします。パスワードを入力します（要求された場合）。

ステップ 2 **show utd multi-tenancy**

マルチテナントの現在のステータスを表示します。

例：

```
Device# show utd multi-tenancy
Multitenancy is enabled
```

ステップ 3 show utd engine standard global

UTD エンジン標準のグローバル設定を表示します。

例：

```
Device# show utd engine standard global
UTD Engine Standard Global: enabled
Threat-inspection: enabled
Web-filter: enabled
Logging:
```

ステップ 4 show utd engine standard status

UTD エンジンのステータスが緑色であることを確認します。

例：

```
Device# show utd eng standard status
Engine version       : 1.0.2_SV2983_XE_16_8

Profile              : Multi-tenancy
System memory        :
              Usage  : 3.50 %
              Status : Green
Number of engines    : 1

Engine        Running    CFT flows  Health     Reason
===============================================================
Engine(#1):   Yes        0          Green      None
===============================================================

Overall system status: Green

Signature update status:
========================
Current signature package version: 29.0.c
Last update status: Failed
Last successful update time: None
Last failed update time: Thu Jan 11 13:34:36 2018 PST
Last failed update reason: [Errno 113] No route to host
Next update scheduled at: None
Current status: Idle
```

ステップ 5 show utd engine standard statistics

例：

```
Device# show utd engine standard statistics
*************Engine #1*************
===============================================================================
Memory usage summary:
Total non-mmapped bytes (arena): 80125952
Bytes in mapped regions (hblkhd): 359546880
Total allocated space (uordblks): 68314032
Total free space (fordblks): 11811920
Topmost releasable block (keepcost): 112
===============================================================================
```

```
Packet I/O Totals:
Received: 49088
Analyzed: 49088 (100.000%)
Dropped: 0 ( 0.000%)
Filtered: 0 ( 0.000%)
Outstanding: 0 ( 0.000%)
Injected: 640
================================================================================
Breakdown by protocol (includes rebuilt packets):
Eth: 49394 (100.000%)

<output removed for brevity>

Total: 49394
================================================================================
Action Stats:
Alerts: 65 ( 0.132%)
Logged: 65 ( 0.132%)
Passed: 0 ( 0.000%)
```

ステップ 6　show utd engine standard statistics daq [dp | cp]

Snort DAQ 統計情報を表示します。

例：

```
Device# show utd engine standard statistics daq dp
IOS-XE DAQ Counters(Engine #1):
--------------------------------
Frames received 654101
Bytes received 549106120
RX frames released 654101
Packets after vPath decap 654101
Bytes after vPath decap 516510928
Packets before vPath encap 651686
Bytes before vPath encap 514800669
Frames transmitted 651686
Bytes transmitted 544447557

<output removed for brevity>
```

例：

```
Device# show utd engine standard statistics daq cp
IOS-XE DAQ CP Counters(Engine #1):
-----------------------------------
Packets received :16353210
Bytes received :1112018252
Packets transmitted :16353210
Bytes transmitted :1700733776
Memory allocation :16353212
Memory free :16353210
CFT API error :0
VPL API error :0
Internal error :0
External error :0
Memory error :0
Timer error :0
RX ring full 0
CFT full 0
sPath lib flow handle exhausted 0
Memory status changed to yellow :1
Memory status changed to red :0
```

```
Process restart notifications :0
```

ステップ 7 **show utd engine standard statistics url-filtering** [**engine** | *no*]

すべてのテナントのURL統計情報（ブロックリストのサイトのヒット数、許可リストのサイトのヒット数、カテゴリブロックとレピュテーションブロックによってブロックされたサイトの数を）を表示します。

例：

```
Device# show utd engine standard statistics url-filtering
UTM Preprocessor Statistics
---------------------------
URL Filter Requests Sent:               377226166       379846771       381117940
URL Filter Response Received:           377009606       379622845       380892658
Blacklist Hit Count:                    0               0               0
Whitelist Hit Count:                    0               0               0

Reputation Lookup Count:                376859139       379458008       380706804
Reputation Action Block:                0               0               0
Reputation Action Pass:                 307             280             102
Reputation Action Default Pass:         376858832       379457728       380706702
Reputation Score None:                  376858832       379457728       380706702
Reputation Score Out of Range:          0               0               0

Category Lookup Count:                  376859139       379458008       380706804
Category Action Block:                  0               0               0
Category Action Pass:                   307             280             102
Category Action Default Pass:           376858832       379457728       380706702
Category None:                          376858832       379457728       380706702


Device# show utd engine standard statistics url-filtering engine1
UTM Preprocessor Statistics
---------------------------------------------------
URL Filter Requests Sent:               377226166
URL Filter Response Received:           377009606
Blacklist Hit Count:                    0
Whitelist Hit Count:                    0

Reputation Lookup Count:                376859139
Reputation Action Block:                0
Reputation Action Pass:                 307
Reputation Action Default Pass:         376858832
Reputation Score None:                  376858832
Reputation Score Out of Range:          0

Category Lookup Count:                  376859139
Category Action Block:                  0
Category Action Pass:                   307
Category Action Default Pass:           376858832
Category None:                          376858832
```

ステップ 8 **show utd engine standard statistics url-filtering vrf name** *vrf-name*

追加パラメータの **vrf name** *vrf-name* を使用して、テナントごとの URL の統計情報を表示します。

例：

```
Device# show utd engine standard statistics url-filtering vrf name vrf101
UTM Preprocessor Statistics
```

```
--------------------------
URL Filter Requests Sent: 764
URL Filter Response Received: 764
Blacklist Hit Count: 3
Whitelist Hit Count: 44

Reputation Lookup Count: 764
Reputation Action Block: 0
Reputation Action Pass: 58
Reputation Action Default Pass: 706
Reputation Score None: 706
Reputation Score Out of Range: 0

Category Lookup Count: 764
Category Action Block: 5
Category Action Pass: 53
Category Action Default Pass: 706
Category None: 706
```

ステップ 9 show utd engine standard statistics internal

例：

```
Device# show utd engine standard statistics internal
*************Engine #1*************
===============================================================================
Memory usage summary:
Total non-mmapped bytes (arena): 80125952
Bytes in mapped regions (hblkhd): 359546880
Total allocated space (uordblks): 68314032
Total free space (fordblks): 11811920
Topmost releasable block (keepcost): 112
===============================================================================
Packet I/O Totals:
Received: 49088
Analyzed: 49088 (100.000%)
Dropped: 0 ( 0.000%)
Filtered: 0 ( 0.000%)
Outstanding: 0 ( 0.000%)
Injected: 640
===============================================================================
Breakdown by protocol (includes rebuilt packets):
Eth: 49394 (100.000%)
VLAN: 49394 (100.000%)
IP4: 49394 (100.000%)
Frag: 0 ( 0.000%)
ICMP: 5 ( 0.010%)
UDP: 2195 ( 4.444%)
TCP: 47194 ( 95.546%)

<output removed for brevity>
```

ステップ 10 show utd engine standard logging event

VRF ごとにブロックリストまたは許可リストにあるアラートと URL を含むログを表示します。

例：

```
Device# show utd engine standard logging event

2017/08/04-16:01:49.205959 UTC [**] [Instance_ID: 1] [**] Drop [**]
UTD WebFilter Category/Reputation [**] [URL: www.cricinfo.com] ** [Category: Sports]
** [Reputation: 96] [VRF: vrf101] {TCP} 23.72.180.26:80 -> 111.0.0.254:53509
```

```
2017/08/04-16:02:12.253330 UTC [**] [Instance_ID: 1] [**] Pass [**]
 UTD WebFilter Whitelist [**] [URL: www.espn.go.com/m]
[VRF: vrf101] {TCP} 111.0.0.254:53511 -> 199.181.133.61:80
```

ステップ 11 **show logging** | **include** CONFIG_DOWNLOAD

例：

```
show# logging | include CONFIG_DOWNLOAD
Aug 23 11:34:21.250 PDT: %IOSXE_UTD-4-MT_CONFIG_DOWNLOAD: UTD MT configuration download has started
Aug 23 11:54:18.496 PDT: %IOSXE_UTD-4-MT_CONFIG_DOWNLOAD: UTD MT configuration download has
completed
```

ステップ 12 **show utd threat-inspection whitelist** [**profile** *profile-name*]

すべての許可リストのプロファイルまたは特定の許可リストのプロファイルを表示します。

例：

```
Device# show utd threat-inspection whitelist
Whitelist Profile: wh101
Signature ID: 101
```

例：

```
Device# show utd threat-inspection whitelist profile wh101
Whitelist Profile: wh101
Signature ID: 101
```

ステップ 13 **show utd threat-inspection profile** *profile-name*

プロファイル名で指定された脅威検知プロファイルの詳細を表示します。

例：

```
Device# show utd threat-inspection profile 101
Threat-inspection Profile: 101
Operational Mode: Intrusion Protection
Operational Policy: Security
Logging Level: debug
Whitelist Profile: wh101
```

ステップ 14 **show utd** [**policy** *profile-name*]

すべての UTD ポリシーまたは特定の UTD ポリシーを表示します。

例：

```
Device# show utd policy pol101
Policy name: pol101
VRF name: vrf101, VRF ID: 1
Global Inspection (across above VRFs): Enabled
Threat-inspection profile: 101
Web-filter URL profile: 1
Fail Policy: Fail-open
```

ステップ 15 **show utd web-filter url** [**profile** *profile-name*]

すべての URL プロファイルまたは特定のプロファイルを表示します。

例：

```
Device# show utd web-filter url profile 1
URL Profile: 1
Alert: all
Blacklist Parameter Map Regex: urlf-blacklist1
Whitelist Parameter Map Regex: urlf-whitelist1
Block Categories:
dating
sports
Block Page Profile 1
Log level error
reputation block-threshold high-risk
```

ステップ 16 **show utd web-filter block local-server** [**profile** *profile-name*]

すべてのブロックページのプロファイルまたは特定のブロックページのプロファイルを表示します。

例：

```
Device# show utd web-filter block local-server profile 2
Block Local Server Profile: 2
Content text: "Blocked by Web-Filter"
HTTP ports: 80
```

ステップ 17 **show utd web-filter sourcedb** [**profile** *profile-name*]

すべての sourcedb プロファイルまたは特定の sourcedb プロファイルを表示します。

例：

```
Device# show utd web-filter sourcedb
SourceDB Profile: 1
database update server interval hour 0 minute 0
Fail open
Log level: error
Proxy host port 0

SourceDB Profile: 2
database update server interval hour 0 minute 0
Fail open
Log level: error
Proxy host port 0
```

例：

```
Device# show utd web-filter sourcedb profile 1
SourceDB Profile: 1
database update server interval hour 0 minute 0
Fail open
Log level: error
Proxy host port 0
```

ステップ 18 **show utd engine standard statistics daq dp** [**engine** *engine-num*] [**vrf** [**name** *vrf-name* | **global**]]

すべての VRF または特定の VRF のサービスプレーンのデータ収集（DAQ：Data Acquistion）の統計情報を表示します。

例：

次の例は、VRF vrf101 のサービスプレーンのデータ収集の統計情報を示しています。

```
Device# show utd engine standard statistics daq dp vrf name vrf101
IOS-XE DAQ Counters(Engine #1):
--------------------------------
Frames received 374509
Bytes received 303136342
RX frames released 374509
Packets after vPath decap 374509
Bytes after vPath decap 284405526
Packets before vPath encap 372883
Bytes before vPath encap 283234522
Frames transmitted 372883
Bytes transmitted 300202270

Memory allocation 781856
Memory free 749636
Memory free via timer 29420
Merged packet buffer allocation 0
Merged packet buffer free 0

VPL buffer allocation 0
VPL buffer free 0
VPL buffer expand 0
VPL buffer merge 0
VPL buffer split 0
VPL packet incomplete 0

VPL API error 0
CFT API error 0
Internal error 52
External error 0
Memory error 0
Timer error 0

Kernel frames received 373590
Kernel frames dropped 0

FO cached via timer 0
Cached fo used 0
Cached fo freed 0
FO not found 0
CFT full packets 0
```

ステップ 19 **show utd engine standard config threat-inspection whitelist** [**profile** *profile-name*]

コンテナに保存されている脅威検知許可リストのプロファイルの詳細を表示します。

例：

```
Device# show utd engine standard config threat-inspection whitelist
UTD Engine Standard Configuration:

UTD threat-inspection whitelist profile table entries:
Whitelist profile: wh101
Entries: 1
```

ステップ 20 **show utd engine standard config web-filter url profile** *profile-name*

コンテナに保存されている Web フィルタのプロファイルの詳細を表示します。

例：

```
Device# show utd engine standard config web-filter url profile 1
UTD Engine Standard Configuration:

UTD web-filter profile table entries
Web-filter URL profile: 1
Whitelist:
www.espn.com
www.nbcsports.com
www.nfl.com
Blacklist:
www.cnn.com
Categories Action: Block
Categories:
Social Network
Sports
Block Profile: 1
Redirect URL: http://172.27.56.97/vrf101.html
Reputation Block Threshold: High risk
Alerts Enabled: Whitelist, Blacklist, Categories, Reputation
Debug level: Error
Conditional debug level: Error
```

ステップ 21 **show utd engine standard config** [**vrf name** *vrf-name*]

特定の VRF に関連付けられた UTD ポリシー、脅威検知プロファイル、および Web フィルタプロファイルの詳細を表示します。

例：

```
Device# show utd engine standard config vrf name vrf101
UTD Engine Standard Configuration:

UTD VRF table entries:
VRF: vrf101 (1)
Policy: pol101
Threat Profile: 101
Webfilter Profile: 1
```

ステップ 22 **show utd engine standard config threat-inspection profile** *profile-name*

特定の脅威検知プロファイルの詳細を表示します。

例：

```
Device# show utd engine standard config threat-inspection profile 101
UTD Engine Standard Configuration:

UTD threat-inspection profile table entries:
Threat profile: 101
Mode: Intrusion Prevention
Policy: Security
Logging level: Debug
Whitelist profile: wh101

Description:
Displays the details of a threat-inspection profile stored in the container.
```

ステップ 23 **show utd engine standard threat-inspection signature update status**

現在の署名パッケージのバージョン、以前の署名パッケージのバージョン、および最後のステータス更新の出力を表示します。

例：

```
Device# show utd engine standard threat-inspection signature update status
Current signature package version: 29.0.c
Current signature package name: default
Previous signature package version: None
----------------------------------------
Last update status: Failed
----------------------------------------
Last successful update time: None
Last successful update method: None
Last successful update server: None
Last successful update speed: None
----------------------------------------
Last failed update time: Thu Jan 11 13:34:36 2018 PST
Last failed update method: Manual
Last failed update server: http://172.27.57.252/UTD-STD-SIGNATURE-2983-1-S.pkg
Last failed update reason: [Errno 113] No route to host
----------------------------------------
Last attempted update time: Thu Jan 11 13:34:36 2018 PST
Last attempted update method: Manual
Last attempted update server: http://172.27.57.252/UTD-STD-SIGNATURE-2983-1-S.pkg
----------------------------------------
Total num of updates successful: 0
Num of attempts successful: 0
Num of attempts failed: 1
Total num of attempts: 1
----------------------------------------
Next update scheduled at: None
----------------------------------------
Current status: Idle
```

ステップ 24 **show platform software qfp active feature utd config [vrf[{id** *vrf-id* | **name** *vrf-name* | **global** }]

サービスノードの統計情報を表示します。VRF情報は、マルチテナントの場合にのみ表示できます。データプレーンUTD設定を表示します。次の例では、セキュリティコンテキスト情報が強調表示されています。

例：

```
Device# Global configuration
  NAT64: disabled
  SN threads: 12
  CFT inst_id 0 feat id 0 fo id 0 chunk id 4
  Context Id: 0, Name: Base Security Ctx
   Ctx Flags: (0xf0000)
        Engine: Standard
        SN Redirect Mode : Fail-close, Divert
        Threat-inspection: Enabled, Mode: IPS
        Domain Filtering : Not Enabled
        URL Filtering    : Not Enabled
   SN Health: Green
```

ステップ 25 **show platform software utd interfaces**

例：

```
Device# show platform software utd interfaces

UTD interfaces
All dataplane interfaces
```

ステップ 26 **show platform hardware qfp active feature utd config** [**vrf** {**id** *vrf-id* | **name** *vrf-name* | **global** }]

UTD データパスの設定とステータスを表示します。

例：

```
Device# show platform hardware qfp active feature utd config vrf name vrf101
Global configuration
  NAT64: disabled
  Drop pkts: disabled
  Multi-tenancy: enabled
  Data plane initialized: yes
  SN threads: 12
  CFT inst_id 0 feat id 1 fo id 1 chunk id 8
  SN Health: Green
```

ステップ 27 **show platform hardware qfp active feature utd stats** [**clear** | **divert** | **drop** | **general** | **summary**] [**vrf** {**id** *vrf-id* | **name** *vrf-name* | **global** }] [all] [**verbose**]

ゼロのカウントを含むデータプレーン UTD 統計情報を表示します。

clear：統計情報をクリアします

divert：AppNav リダイレクト統計情報を表示します

drop：ドロップ統計情報を表示します

general：一般統計情報を表示します

summary：サマリー統計情報を表示します

verbose：Verbose 統計情報を表示します

VRF 統計情報ごとの VRF 表示：VRF 情報は、マルチテナントが有効な場合にのみ入力できます。

id：VRF ID に関連付けられた統計情報を表示します

name：指定した名前の VRF に関連付けられた統計情報を表示します

global：グローバル VRF（つまり VRF ID が 0）に関連付けられている統計情報を表示します

例：

```
Device# show platform hardware qfp active feature utd stats

Summary Statistics:
TCP Connections Created 29893
UDP Connections Created 24402
ICMP Connections Created 796
Pkts dropped pkt 258
byt 66365
Pkts entered policy feature pkt 715602
byt 562095214
Pkts entered divert feature pkt 662014
byt 516226302
Pkts slow path pkt 55091
byt 4347864
Pkts Diverted pkt 662014
byt 516226302
```

```
Pkts Re-injected pkt 659094
byt 514305557

Would-Drop Statistics:

Service Node flagged flow for dropping 258

General Statistics:
Non Diverted Pkts to/from divert interface 1022186
Inspection skipped - UTD policy not applicable 1081563

<output removed for brevity>
```

例：

ステップ 28 **show platform hardware qfp active feature utd stats summary** [**vrf name** *vrf-name* | **all**]

show platform hardware qfp active feature utd stats コマンドのサマリーオプションから取得したすべての VRF または特定の VRF に関する情報を表示します。

例：

```
Device# show platform hardware qfp active feature utd stats vrf name vrf101
Security Context: Id:1 Name: 1 : vrf101

Summary Statistics:
TCP Connections Created 18428
UDP Connections Created 13737
ICMP Connections Created 503
Pkts dropped pkt 258
byt 66365
Pkts entered policy feature pkt 407148
byt 296496913
Pkts entered divert feature pkt 383176
byt 283158966
Pkts slow path pkt 32668
byt 2571632
Pkts Diverted pkt 383176
byt 283158966
Pkts Re-injected pkt 381016
byt 281761395


<output removed for brevity>
```

ステップ 29 **show platform hardware qfp active feature utd stats drop all**

show platform コマンドのドロップオプションから取得したすべての VRF からの情報を表示します。

例：

```
Device# show platform hardware qfp active feature utd stats drop all

Would-Drop Statistics:

No diversion interface                                                  0
No egress interface                                                     0
Inspection service down                                                 0
Could not find divert interface                                         0
Could not find divert fib                                               0
UTD FIB did not contain oce_chain                                       0
Invalid IP version                                                      0
```

```
IPS not supported                                                    0
Re-inject Error                                                      0
Service Node flagged flow for dropping                            1225
Could not attach feature object                                      0
Could not allocate feature object                                    0
Error getting feature object                                         0
Policy: could not create connection                                  0
NAT64 Interface Look up Failed                                       0
Decaps: VPATH connection establishment error                         0
Decaps: VPATH could not find flow, no tuple                          0
Decaps: VPATH notification event error                               0
Decaps: Could not delete flow                                        0
Decaps: VPATH connection classification error                        0
Encaps: Error retrieving feature object                              0
Encaps: Flow not classified                                          0
Encaps: VPATH connection specification error                         0
Encaps: VPATH First packet meta-data failed                          0
Encaps: VPATH No memory for meta-data                                0
Encaps: VPATH Could not add TLV                                      0
Encaps: VPATH Could not fit TLV into memory                          0
Service Node Divert Failed                                           0
No feature object                                                    0
Service Node not healthy                                           123
Could not allocate VRF meta-data                                     0
Could not allocate debug meta-data                                   0
Packet was virtually fragmented (VFR)                                0
IPv6 Fragment                                                        0
IPv4 Fragment                                                        0
```

統合脅威防御（UTD）のマルチテナントに関するトラブルシューティング

トラフィックが転送されない

問題 トラフィックは転送されません。

考えられる原因 仮想サービスがアクティブになっていない可能性があります。

解決法 **show virtual-service list** コマンドを使用して、仮想サービスがアクティブになっているかどうかを確認します。次に、コマンドの出力例を示します。

```
Device# show virtual-service list

Virtual Service List:


Name Status Package Name
--------------------------------------------------------------------------------
snort Activated utdsnort.1_0_1_SV2982_XE_16_3.20160701_131509.ova
```

考えられる原因 指定されたインターフェイスでは、統合脅威防御（UTD）が有効になっていない可能性があります。

解決法 **show platform software utd global** コマンドを使用して、インターフェイスで UTD が有効になっているかどうかを確認します。

```
Device# show platform software utd global

UTD Global state
Engine               : Standard
Global Inspection    : Disabled
Operational Mode     : Intrusion Prevention
Fail Policy          : Fail-open
Container techonlogy : LXC
Redirect interface   : VirtualPortGroup1
UTD interfaces
GigabitEthernet0/0/0
```

考えられる原因 サービスノードが正常に動作していない可能性があります。

解決法 **show platform hardware qfp active feature utd config** コマンドを使用して、サービスノードの状態が緑色かどうかを確認します。

```
Device# show platform hardware qfp active feature utd config

Global configuration
NAT64: disabled
SN threads: 12
CFT inst_id 0 feat id 0 fo id 0 chunk id 4
Context Id: 0, Name: Base Security Ctx
Ctx Flags: (0x60000)
Engine: Standard
SN Redirect Mode : Fail-open, Divert
Threat-inspection: Enabled, Mode: IDS
Domain Filtering : Not Enabled
URL Filtering : Not Enabled
SN Health: Green
```

解決法 また、マルチテナントの場合は、**show platform hardware qfp active feature utd config vrf name** *vrf-name*コマンドを使用して、特定の VRF 関するサービスノードの正常性が緑色であるかどうかを確認できます。

```
Device# show platform hardware qfp active feature utd config vrf name vrf102
Global configuration
  NAT64: disabled
  Drop pkts: disabled
  Multi-tenancy: enabled
  Data plane initialized: yes
  SN threads: 12
  CFT inst_id 0 feat id 0 fo id 0 chunk id 4
  SN Health: Green
```

考えられる原因 Snort プロセスがアクティブになっていない可能性があります。

解決法 **show virtual-service detail** コマンドを使用して、Snortプロセス が稼働しているかどうかを確認します。

```
Device# show virtual-service detail

Virtual service UTDIPS detail
  State                : Activated
  Owner                : IOSd
  Package information
    Name               : utdsnort.1_0_1_SV2982_XE_16_3.20160701_131509.ova
    Path               : bootflash:/utdsnort.1_0_1_SV2982_XE_16_3.20160701_131509.ova
```

```
    Application
      Name              : UTD-Snort-Feature
      Installed version : 1.0.1_SV2982_XE_16_3
      Description       : Unified Threat Defense
    Signing
      Key type          : Cisco development key
      Method            : SHA-1
    Licensing
      Name              : Not Available
      Version           : Not Available

  Detailed guest status

------------------------------------------------------------------------
Process               Status            Uptime           # of restarts
------------------------------------------------------------------------
climgr                 UP         0Y 0W 0D  0: 0:35        1
logger                 UP         0Y 0W 0D  0: 0: 4        0
snort_1                UP         0Y 0W 0D  0: 0: 4        0
Network stats:
eth0: RX  packets:43, TX  packets:6
eth1: RX  packets:8, TX  packets:6

Coredump file(s): lost+found

  Activated profile name: None
  Resource reservation
    Disk                : 736 MB
    Memory              : 1024 MB
    CPU                 : 25% system CPU

  Attached devices
    Type              Name        Alias
    ---------------------------------------------
    NIC               ieobc_1     ieobc
    NIC               dp_1_0      net2
    NIC               dp_1_1      net3
    NIC               mgmt_1      mgmt
    Disk              _rootfs
    Disk              /opt/var
    Disk              /opt/var/c
    Serial/shell                  serial0
    Serial/aux                    serial1
    Serial/Syslog                 serial2
    Serial/Trace                  serial3
    Watchdog          watchdog-2

  Network interfaces
    MAC address             Attached to interface
    ------------------------------------------------------
    54:0E:00:0B:0C:02       ieobc_1
    A4:4C:11:9E:13:8D       VirtualPortGroup0
    A4:4C:11:9E:13:8C       VirtualPortGroup1
    A4:4C:11:9E:13:8B       mgmt_1

  Guest interface
  ---
  Interface: eth2
  ip address: 48.0.0.2/24
Interface: eth1
  ip address: 47.0.0.2/24

  ---
```

```
  Guest routes
  ---
  Address/Mask                            Next Hop                              Intf.
-------------------------------------------------------------------------------------
0.0.0.0/0                               48.0.0.1                             eth2
0.0.0.0/0                               47.0.0.1                             eth1

  ---

  Resource admission (without profile) : passed
    Disk space    : 710MB
    Memory        : 1024MB
    CPU           : 25% system CPU
    VCPUs         : Not specified
```

考えられる原因 AppNav トンネルがアクティブになっていない可能性があります。

解決法 **show service-insertion type utd service-node-group** および **show service-insertion type utd service-context** コマンドを使用して、AppNav トンネルがアクティブになっているかどうかを確認します。

解決法 次に、**show service-insertion type utd service-node-group** コマンドの出力例を示します。

```
Device# show service-insertion type utd service-node-group

Service Node Group name : utd_sng_1
Service Context : utd/1
Member Service Node count : 1


Service Node (SN) : 30.30.30.2
Auto discovered : No
SN belongs to SNG : utd_sng_1
Current status of SN : Alive
Time current status was reached : Tue Jul 26 11:57:48 2016

Cluster protocol VPATH version : 1
Cluster protocol incarnation number : 1
Cluster protocol last sent sequence number : 1469514497
Cluster protocol last received sequence number: 1464
Cluster protocol last received ack number : 1469514496
```

解決法 次に、**show service-insertion type utd service-context** コマンドの出力例を示します。

```
Device# show service-insertion type utd service-context

Service Context : utd/1
Cluster protocol VPATH version : 1
Time service context was enabled : Tue Jul 26 11:57:47 2016
Current FSM state : Operational
Time FSM entered current state : Tue Jul 26 11:57:58 2016
Last FSM state : Converging
Time FSM entered last state : Tue Jul 26 11:57:47 2016
Cluster operational state : Operational

Stable AppNav controller View:
30.30.30.1

Stable SN View:
30.30.30.2
```

```
Current AppNav Controller View:
30.30.30.1

Current SN View:
30.30.30.2
```

考えられる原因 トラフィックのステータスのデータプレーンUTD統計情報を確認します。トラフィックが転送されない場合、転送および拒否されたパケットの数はゼロになります。数値がゼロ以外の場合、トラフィック転送が行われており、Snort センサーはデータプレーンにパケットを再送信しています。

解決法 **show platform hardware qfp active feature utd stats** コマンドを使用してトラフィックのステータスを確認します。

```
Device# show platform hardware qfp active feature utd stats

Security Context:    Id:0    Name: Base Security Ctx

Summary Statistics:
Active Connections                                                  29
TCP Connections Created                                         712910
UDP Connections Created                                             80
Pkts entered policy feature                         pkt        3537977
                                                    byt      273232057
Pkts entered divert feature                         pkt        3229148
                                                    byt      249344841
Pkts slow path                                      pkt         712990
                                                    byt       45391747
Pkts Diverted                                       pkt        3224752
                                                    byt      249103697
Pkts Re-injected                                    pkt        3224746
                                                    byt      249103373

….
```

解決法 また、マルチテナントの場合は、**show platform hardware qfp active feature utd stats vrf name** *vrf-name*コマンドを使用して、特定の VRF に関するトラフィックのステータスを確認できます。

```
Device# show platform hardware qfp active feature utd stats vrf name vrf 101

Security Context:    Id:1    Name: 1 : vrf101

Summary Statistics:
Active Connections                                                   2
TCP Connections Created                                          34032
UDP Connections Created                                          11448
ICMP Connections Created                                            80
Pkts dropped                                        pkt           626
                                                    byt        323842
Pkts entered policy feature                         pkt        995312
                                                    byt     813163885
Pkts entered divert feature                         pkt        639349
                                                    byt     420083106
Pkts slow path                                      pkt         45560
                                                    byt       7103132
Pkts Diverted                                       pkt        638841
                                                    byt     419901335
```

```
Pkts Re-injected                                    pkt              630642
                                                    byt           412139098
….
```

署名の更新が機能しない

問題　Cisco ボーダレスソフトウェア配布（BSD：Borderless Software Distribution）サーバからの署名更新が機能していません。

考えられる原因　さまざまな理由により署名の更新に失敗した可能性があります。最後に署名の更新に失敗した理由を確認します。

解決法　**show utd engine standard threat-inspection signature update status** コマンドを使用して、最後に署名の更新に失敗した理由を表示します。

```
Device# show utd eng standard threat-inspection signature update status
Current signature package version: 29.0.c
Current signature package name: default
Previous signature package version: None
----------------------------------------
Last update status: Failed
----------------------------------------
Last successful update time: None
Last successful update method: None
Last successful update server: None
Last successful update speed: None
----------------------------------------
Last failed update time: Thu Jan 11 13:34:36 2018 PST
Last failed update method: Manual
Last failed update server: http://172.27.57.252/UTD-STD-SIGNATURE-2983-1-S.pkg
Last failed update reason: [Errno 113] No route to host
----------------------------------------
Last attempted update time: Thu Jan 11 13:34:36 2018 PST
Last attempted update method: Manual
Last attempted update server: http://172.27.57.252/UTD-STD-SIGNATURE-2983-1-S.pkg
----------------------------------------
Total num of updates successful: 0
Num of attempts successful: 0
Num of attempts failed: 1
Total num of attempts: 1
----------------------------------------
Next update scheduled at: None
----------------------------------------
Current status: Idle
```

考えられる原因　ドメインネームシステム（DNS）が正しく設定されていません。

解決法　**show running-config | i name-server** コマンドを使用して、ネームサーバの詳細を表示します。

```
Device#  show run | i name-server

ip name-server 10.104.49.223
```

考えられる原因　システムエラー：ユーザ名とパスワードの組み合わせの処理に失敗しました。

解決法 署名パッケージのダウンロードに正しい認証情報を使用したことを確認します。

ローカルサーバからの署名の更新が機能しない

問題 ローカルサーバからの署名の更新が機能しない。

考えられる原因 最後の失敗の理由：無効なスキーム — HTTP または HTTPS のみに対応します。

解決法 ローカルダウンロード方式として HTTP またはセキュア HTTP（HTTPS）が指定されていることを確認します。

考えられる原因 最後の失敗の理由：名前またはサービスが不明です。

解決法 ローカルサーバに指定されたホスト名または IP アドレスが正しいことを確認します。

考えられる原因 最後の失敗の理由：認証情報が入力されていません。

解決法 ローカル HTTP または HTTPS サーバの認証情報が入力されていることを確認します。

考えられる原因 最後の失敗の理由：ファイルが見つかりません。

解決法 入力した署名ファイル名または URL が正しいことを確認します。

考えられる原因 最後の失敗の理由：ダウンロードが破損しています。

解決法

- 以前の署名のダウンロード時に署名更新の再試行でエラーが発生していないかどうかを確認します。
- 正しい署名パッケージが使用可能であることを確認します。

IOSd Syslog へのロギングが機能しない

問題 IOSd syslog へのロギングが機能しない。

考えられる原因 syslog へのロギングは、統合脅威防御（UTD）の設定では設定できません。

解決法 UTD 設定を表示し、syslog へのロギングが設定されていることを確認するには、**show utd engine standard config** コマンドを使用します。

```
Device# show utd engine standard config

UTD Engine Standard Configutation:
  Operation Mode : Intrusion Prevention
  Policy         : Security

Signature Update:
  Server    : cisco
  User Name : ccouser
  Password  : YEX^SH\fhdOeEGaOBIQAIcOVLgaVGf
  Occurs-at : weekly ;  Days:0 ; Hour: 23; Minute: 50

Logging:
  Server    :   IOS Syslog; 10.104.49.223
  Level     : debug
```

```
Whitelist Signature IDs:
  28878
```

解決法 UTD エンジンのイベントログを表示するには、次の **show utd engine standard logging events** コマンドを使用します。

```
Device# show utd engine standard logging events

2016/06/13-14:32:09.524475 IST [**] [Instance_ID: 1] [**] Drop [**] [1:30561:1]
BLACKLIST DNS request for known malware domain domai.ddns2.biz -
Win.Trojan.Beebone [**] [Classification: A Network Trojan was Detected]
[Priority: 1] [VRF_ID: 2] {UDP} 11.1.1.10:58016 -> 21.1.1.10:53
2016/06/13-14:32:21.524988 IST [**] [Instance_ID: 1] [**] Drop [**] [1:30561:1]
BLACKLIST DNS request for known malware domain domai.ddns2.biz -
Win.Trojan.Beebone [**] [Classification: A Network Trojan was Detected] [Priority: 1]
[VRF_ID: 2] {UDP} a000:0:0:0:0:0:0:10:59964 -> b000:0:0:0:0:0:0:10:53
```

外部サーバへのロギングが機能しない

問題 外部サーバへのロギングが機能していません。

考えられる原因 外部サーバで Syslog が実行されていない可能性があります。

解決法 syslog サーバが外部サーバで実行されているかどうかを確認します。ステータスを表示するには、外部サーバで次のコマンドを設定します。

```
ps -eaf | grep syslog

 root 2073 1 0 Apr12 ? 00:00:02 syslogd -r -m
```

考えられる原因 統合脅威防御（UTD）の Linux コンテナ（LXC：Linux Container）と外部サーバ間の接続が失われている可能性があります。

解決法 管理インターフェイスから外部 syslog サーバへの接続を確認します。

UTD 条件付きデバッグ

条件付きデバッグは、Unified Threat Defense のマルチテナントに対応しています。条件付きデバッグの設定方法の詳細については、以下を参照してください。

http://www.cisco.com/c/en/us/td/docs/routers/asr1000/troubleshooting/guide/Tbl-shooting-xe-3s-asr-1000-book.html#task_AC969BB06B414DCBBDEF7ADD29EF8131

第 XV 部

Umbrella

第 167 章

Cisco Umbrella 統合

Cisco Umbrella 統合機能では、デバイスを介して DNS サーバーに送信されるドメインネームシステム（DNS）クエリを検証して、クラウドベースのセキュリティサービスを有効にすることができます。セキュリティ管理者は、完全修飾ドメイン名（FQDN）へのトラフィックを許可または拒否するポリシーを Cisco Umbrella ポータルに設定します。Cisco デバイスは、ネットワークエッジの DNS フォワーダとして機能し、DNS トラフィックを透過的にキャッチして Cisco Umbrella ポータルに DNS クエリを転送します。この機能は、Cisco IOS XE Denali 16.3 以降のリリースで使用できます。

Cisco Umbrella 統合の制限

- アプリケーションまたはホストが、DNSを使用する代わりにIPアドレスを直接使用してドメイン名をクエリしている場合、ポリシーは適用されません。

- クライアントが Web プロキシに接続すると、DNS クエリはシスコデバイスをパススルーしません。この場合、コネクタはDNS要求を一切検出できず、Web サーバーへの接続は Cisco Umbrella ポータルからのすべてのポリシーをバイパスします。
- Cisco Umbrella の統合ポリシーによって DNS クエリがブロックされると、クライアントは Cisco Umbrella ブロックページにリダイレクトされます。これらのブロックページは、HTTPS サーバによって提供され、IP アドレス範囲は Cisco Umbrella ポータルによって定義されます。
- ユーザー認証とアイデンティティは、このリリースではサポートされません。
- リダイレクトされるレコードは、タイプ A、AAAA、および TXT クエリのみです。他のタイプのクエリはコネクタをバイパスします。Cisco Umbrella Connector は、悪意のあるトラフィックに関する既知の IP アドレスのリストを保持しています。Cisco Umbrella ローミングクライアントは、これらのアドレスが宛先のパケットを検出すると、各アドレスを Cisco Umbrella クラウドに転送して、さらに検査します。
- ホストの IPv4 アドレスのみが EDNS オプションで伝達されます。
- 最大 64 のローカルドメインを設定できます。許可されるドメイン名の長さは 100 文字です。

Cisco Umbrella 統合の前提条件

Cisco Umbrella 統合機能を設定するには、次の要件を満たしている必要があります。

- Cisco Umbrella を有効にするには、デバイスにセキュリティ K9 ライセンスが必要です。
- デバイスが Cisco IOS XE Denali 16.3 以降のソフトウェアイメージを実行している必要があります。
- Cisco Umbrella サブスクリプションライセンスが利用可能である必要があります。
- デバイスがデフォルトの DNS サーバーゲートウェイとして設定されており、DNS トラフィックがその Cisco デバイスを確実に通過する必要があります。
- Cisco Umbrella サーバへのデバイス登録に使用する通信は HTTPS 経由です。HTTPS 通信を行うには、ルータにルート証明書がインストールされている必要があります。この証明書をペーストする代わりに、次のリンクから証明書を直接ダウンロードすることができます。https://cacerts.digicert.com/DigiCertGlobalRootCA.crt.pem

Cisco Umbrella Integration を使用したクラウドベースのセキュリティサービス

Cisco Umbrella Integration 機能は、デバイスを介して DNS サーバーに送信される DNS クエリを検査する、クラウドベースのセキュリティサービスを提供します。ホストがトラフィックを開始し、DNS クエリを送信すると、デバイスの Cisco Umbrella コネクタは DNS クエリを横取りして検査します。ローカルドメインへの DNS クエリの場合は、DNS パケットを変更せずにエンタープライズ ネットワーク内の DNS サーバーにクエリを転送します。外部ドメインへの DNS クエリの場合は、クエリに拡張 DNS（EDNS）レコードを追加して Cisco Umbrella リゾルバに送信します。EDNS レコードには、デバイス識別子情報、組織 ID、およびクライアント IP アドレスが含まれています。Cisco Umbrella クラウドは、この情報に基づいて、DNS クエリにさまざまなポリシーを適用します。

DNS パケットの暗号化

Cisco デバイスから Cisco Umbrella 統合サーバーに送信される DNS パケットは、パケット内の EDNS 情報にユーザー ID、内部ネットワーク IP アドレスなどの情報が含まれている場合、暗号化する必要があります。DNS 応答が DNS サーバーから戻されると、デバイスはパケットを復号してからホストに転送します。

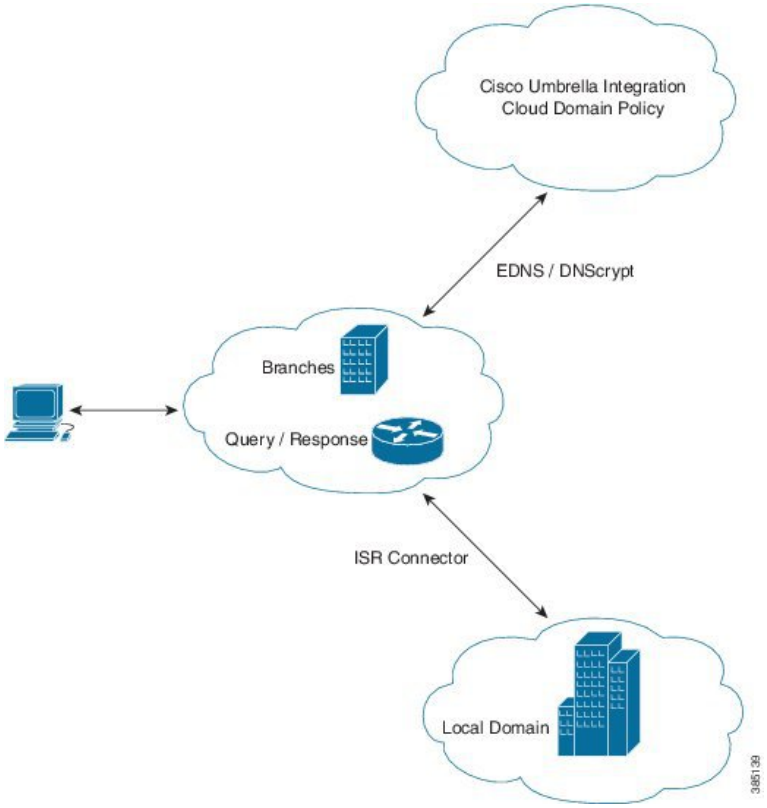
DNS パケットは、DNScrypt 機能が Cisco デバイスで有効化されている場合にのみ暗号化できます。

Cisco デバイスは次の Anycast 再帰型 Cisco Umbrella 統合サーバーを使用します。

- 208.67.222.222
- 208.67.220.220
- 2620:119:53::53
- 2620:119:35::35

次の図は、Cisco Umbrella 統合のトポロジを示します。

図 *88 : Cisco Umbrella* 統合のトポロジ



Cisco Umbrella 統合のメリット

Cisco Umbrella 統合により、DNS レベルでセキュリティとポリシーを適用できます。これにより、管理者は DNS トラフィックを分割して、目的の DNS トラフィックの一部を特定の DNS サーバ（エンタープライズ ネットワーク内にある DNS サーバ）に直接送信することができます。これにより、管理者は Cisco Umbrella 統合をバイパスできます。

Cisco Umbrella Connector の設定

Cisco Umbrella Connector を設定するには、次の手順を実行します。

- Cisco Umbrella 登録サーバーから API トークンを取得します。
- Cisco Umbrella 登録サーバとの間で HTTPS 接続を確立するために、ルート証明書を取得します。**crypto pki trustpool import terminal** コマンドを使用して、以下に示す DigiCert のルート証明書をデバイスにインポートします。

```
-----BEGIN CERTIFICATE-----
MIIDrzCCApegAwIBAgIQCDvgVpBCRrGhdWrJWZHHSjANBgkqhkiG9w0BAQUFADBh
MQswCQYDVQQGEwJVUzEVMBMGA1UEChMMRGlnaUNlcnQgSW5jMRkwFwYDVQQLExB3
```

```
d3cuZGlnaWNlcnQuY29tMSAwHgYDVQQDExdEaWdpQ2VydCBHbG9iYWwgUm9vdCBD
QTAeFw0wNjExMTAwMDAwMDBaFw0zMTExMTAwMDAwMDBaMGExCzAJBgNVBAYTAlVT
MRUwEwYDVQQKEwxEaWdpQ2VydCBJbmMxGTAXBgNVBAsTEHd3dy5kaWdpY2VydC5j
b20xIDAeBgNVBAMTF0RpZ2lDZXJ0IEdsb2JhbCBSb290IENBMIIBIjANBgkqhkiG
9w0BAQEFAAOCAQ8AMIIBCgKCAQEA4jvhEXLeqKTTo1eqUKKPC3eQyaKl7hLOllsB
CSDMAZOnTjC3U/dDxGkAV53ijSLdhwZAAIEJzs4bg7/fzTtxRuLWZscFs3YnFo97
nh6Vfe63SKMI2tavegw5BmV/Sl0fvBf4q77uKNd0f3p4mVmFaG5cIzJLv07A6Fpt
43C/dxC//AH2hdmoRBBYMql1GNXRor5H4idq9Joz+EkIYIvUX7Q6hL+hqkpMfT7P
T19sdl6gSzeRntwi5m3OFBqOasv+zbMUZBfHWymeMr/y7vrTC0LUq7dBMtoM1O/4
gdW7jVg/tRvoSSiicNoxBN33shbyTApOB6jtSj1etX+jkMOvJwIDAQABo2MwYTAO
BgNVHQ8BAf8EBAMCAYYwDwYDVR0TAQH/BAUwAwEB/zAdBgNVHQ4EFgQUA95QNVbR
TLtm8KPiGxvDl7I90VUwHwYDVR0jBBgwFoAUA95QNVbRTLtm8KPiGxvDl7I90VUw
DQYJKoZIhvcNAQEFBQADggEBAMucN6pIExIK+t1EnE9SsPTfrgT1eXkIoyQY/Esr
hMAtudXH/vTBH1jLuG2cenTnmCmrEbXjcKChzUyImZOMkXDiqw8cvpOp/2PV5Adg
06O/nVsJ8dWO41P0jmP6P6fbtGbfYmbW0W5BjfIttep3Sp+dWOIrWcBAI+0tKIJF
PnlUkiaY4IBIqDfv8NZ5YBberOgOzW6sRBc4L0na4UU+Krk2U886UAb3LujEV0ls
YSEY1QSteDwsOoBrp+uvFRTp2InBuThs4pFsiv9kuXclVzDAGySj4dzp30d8tbQk
CAUw7C29C79Fv1C5qfPrmAESrciIxpg0X40KPMbp1ZWVbd4=
-----END CERTIFICATE-----
```

- PEM インポートが正常に行われたことを確認します。証明書をインポートすると、メッセージが表示されます。

これはサンプル設定です。

```
enable
configure terminal
parameter-map type umbrella global
 token AABBA59A0BDE1485C912AFE472952641001EEECC

exit
```

Cisco Umbrella タグの登録

Cisco Umbrella タグを登録するには、次の手順を実行します。

1. 前の項で示したように Cisco Umbrella パラメータマップを設定します。
2. WAN インターフェイスで **umbrella out** を設定します。

```
interface gigabitEthernet 0/0/1
 umbrella out
```

3. LANインターフェイスで **umbrella in** を設定します。

```
interface gigabitEthernet 0/0/0.4
 umbrella in mydevice_tag
```

（注） Cisco デバイスの場合、ホスト名と umbrella タグは 49 文字以内で指定します。

4. **umbrella in mydevice_tag** コマンドを使用してタグと **umbrella in** を設定すると、デバイスによって Cisco Umbrella Integration ポータルにタグが登録されます。

5. デバイスが *api.opendns.com* を解決して登録プロセスを開始します。FQDN の解決を成功させるために、デバイスにネームサーバー（*ip name-server x.x.x.x*）とドメインルックアップ（*ip domain-lookup*）が設定されている必要があります。

（注） **umbrella in** コマンドを設定する前に、**umbrella out** コマンドを設定してください。登録は、ポート 443 が「オープン」状態にあり、既存のファイアウォールへのトラフィックのパススルーが許可される場合にのみ成功します。

Cisco デバイスをパススルーサーバーとして設定

ドメイン名を使用して、バイパスされるトラフィックを特定することができます。Cisco デバイスでは、正規表現形式でこれらのドメインを定義できます。デバイスによってキャッチされる DNS クエリが、設定済みの正規表現の 1 つにマッチすると、このクエリはバイパスされ、Cisco Umbrella クラウドにリダイレクトされずに、指定された DNS サーバーに送信されます。次の設定例は、目的のドメイン名と正規表現で regex parameter-map を定義する方法を示しています。

```
Device# configure terminal
Device(config)# parameter-map type regex dns_bypass
Device(config)# pattern www.fisco.com
Device(config)# pattern .*engineering.fisco.*

Attach the regex param-map with the openDNS global configuration as shown below:

Device(config)# parameter-map type umbrella global
Device(config-profile)# token AADDD5FF6E510B28921A20C9B98EEEFF
Device(config-profile)# local-domain dns_bypass
```

DNSCrypt、リゾルバ、および公開キー

- DNSCrypt
- リゾルバ IP
- 公開キー

上記のパラメータは、ラボで特定のテストを実行するときのみ変更することをお勧めします。これらのパラメータは今後の利用のために予約されています。これらのパラメータを変更すると、デバイスの正常な機能に影響が及ぶことがあります。

リゾルバ

次のコマンドは、DNS パケットのリダイレクションを Cisco デバイスから Cisco Umbrella クラウドに変更します。

- **resolver ipv4** *1.1.1.1*

- **resolver ipv4** *1.1.1.2*
- **resolver ipv6** *1234::1*
- **resolver ipv6** *2345::1*

この例では、すべての IPv4 DNS パケットが 1.1.1.1 または 1.1.1.2 にリダイレクトされ、IPv6 DNS パケットが 1234::1 または 2345::1 にリダイレクトされます。リゾルバのデフォルト値に戻すには、IP アドレスを削除する必要があります。リゾルバ IP アドレスを変更すると、次のメッセージが表示されます。

```
User configured would overwrite defaults
Defaults are restored when no more user configured are present
```

208.67.222.222 および **208.67.220.220** のデフォルト値を使用すると、すべての DNS パケットが Cisco Umbrella Anycast リゾルバにリダイレクトされます。デバイスは、すべてのリダイレクションに最初のデフォルトリゾルバ IP アドレスを使用します。Cisco デバイスは、3 つの連続する DNS クエリの応答を受信しない場合、別のリゾルバ IP アドレスに自動的に切り替えます。この動作は、IPv6 リゾルバ アドレスの場合も同じです。

（注） IPv6 リダイレクションは延期され、すべての IPV6 DNS パケットは Cisco Umbrella Anycast サーバーにリダイレクトされません。

公開キー

公開キーは、Cisco Umbrella Integration クラウドから DNSCrypt 証明書をダウンロードするために使用されます。この値は、**B735:1140:206F:225D:3E2B:D822:D7FD:691E:A1C3:3CC8:D666:8D0C:BE04:BFAB:CA43:FB79**（Cisco Umbrella Integration Anycast サーバーの公開キー）に事前に設定されています。public-key に変更があり、このコマンドを変更する場合、デフォルト値に戻すときは変更されたコマンドを削除する必要があります。この値を変更すると、DNSCrypt 証明書のダウンロードは失敗することがあります。

DNSCrypt

DNSCrypt を無効化するには **no dnscrypt** コマンドを使用し、DNSCrypt を再度有効化するには **dnscrypt** コマンドを使用します。

DNSCrypt を使用する場合は、DNS 要求パケットサイズが 512 バイトよりも大きくなります。これらのパケットが中間デバイスで許可されていることを確認します。そうしないと、応答が目的の受信者に到達しない可能性があります。

Cisco Umbrella Connector の設定の確認

Cisco Umbrella Connector の設定を確認するには、次のコマンドを実行します。

```
Router# show umbrella config
Umbrella Configuration
==================
   Token:  AAC1A2555C11B2B798FFF3AF27C2FB8F001CB7B2
   OrganizationID: 1882034
   Local Domain Regex parameter-map name: NONE
   DNSCrypt: Enabled
   Public-key:
B735:1140:206F:225D:3E2B:D822:D7FD:691E:A1C3:3CC8:D666:8D0C:BE04:BFAB:CA43:FB79

   UDP Timeout: 5 seconds
   Resolver address:
       1. 208.67.220.220
       2. 208.67.222.222
       3. 2620:119:53::53
       4. 2620:119:35::35
   Umbrella Interface Config:
       Number of interfaces with "opendns out" config: 1
         1. GigabitEthernet0/0/0
             Mode     :  OUT
             VRF      : global(Id: 0)
       Number of interfaces with "opendns in" config: 1
         1. GigabitEthernet0/0/1
             Mode      : IN
             Tag       : test
             Device-id : 010a6aef0b443f0f
             VRF       : global(Id: 0)

Device# show umbrella deviceid
Device registration details
Interface Name          Tag       Status   Device-id
GigabitEthernet0/0/1     guest  200 SUCCESS 010a7ba73bd216d1


Device#show umbrella dnscrypt
    DNSCrypt: Enabled
Public-key: B735:1140:206F:225D:3E2B:D822:D7FD:691E:A1C3:3CC8:D666:8D0C:BE04:BFAB:CA43:FB79
Certificate Update Status:
Last Successful Attempt : 10:55:40 UTC Apr 14 2016
Last Failed Attempt : 10:55:10 UTC Apr 14 2016
Certificate Details:
Certificate Magic : DNSC
Major Version : 0x0001
Minor Version : 0x0000
Query Magic : 0x717744506545635A
Serial Number : 1435874751
Start Time : 1435874751 (22:05:51 UTC Jul 2 2015)
End Time : 1467410751 (22:05:51 UTC Jul 1 2016)
Server Public Key :
ABA1:F000:D394:8045:672D:73E0:EAE6:F181:19D0:2A62:3791:EFAD:B04E:40B7:B6F9:C40B
Client Secret Key Hash :
BBC3:409F:5CB5:C3F3:06BD:A385:78DA:4CED:62BC:3985:1C41:BCCE:1342:DF13:B71E:F4CF
Client Public key :
ECE2:8295:2157:6797:6BE2:C563:A5A9:C5FC:C20D:ADAF:EB3C:A1A2:C09A:40AD:CAEA:FF76
NM key Hash :
F9C2:2C2C:330A:1972:D484:4DD8:8E5C:71FF:6775:53A7:0344:5484:B78D:01B1:B938:E884
```

Cisco Umbrella 統合のトラブルシューティング

次のコマンドを使用して、Cisco Umbrella 機能の有効化に関連する問題のトラブルシューティングを行うことができます。

- **debug umbrella device-registration**
- **debug umbrella config**
- **debug umbrella dnscrypt**

OS に応じて、クライアントデバイスから次の 2 つのコマンドのいずれかを実行します。

- Windows マシンのコマンドプロンプトから **nslookup -type=txt debug.umbrella.com** コマンドを実行します
- Linux マシンのターミナルウィンドウまたはシェルから **nslookup -type=txt debug.umbrella.com** コマンドを実行します

```
nslookup -type=txt debug.opendns.com 8.8.8.8
Server: 8.8.8.8
Address: 8.8.8.8#53
Non-authoritative answer:
debug.opendns.com text = "server r6.mum1"
debug.opendns.com text = "device 010A826AAABB6C3D"
debug.opendns.com text = "organization id 1892929"
debug.opendns.com text = "remoteip 171.168.1.7"
debug.opendns.com text = "flags 436 0 6040 39FF000000000000000"
debug.opendns.com text = "originid 119211936"
debug.opendns.com text = "orgid 1892929"
debug.opendns.com text = "orgflags 3"
debug.opendns.com text = "actype 0"
debug.opendns.com text = "bundle 365396"
debug.opendns.com text = "source 72.163.220.18:36914"
debug.opendns.com text = "dnscrypt enabled (713156774457306E)"
```

設定例

次に、Cisco Umbrella 統合を有効にする例を示します。

Cisco Prime CLI テンプレートを使用した Cisco Umbrella Integration の展開

Cisco Prime CLI テンプレートを使用して、Cisco Umbrella Integration 環境をプロビジョニングできます。Cisco Prime CLI テンプレートを使用すると、Cisco Umbrella Integration 環境を簡単にプロビジョニングできます。

（注） Cisco Prime CLI テンプレートは、Cisco Prime バージョン 3.1 以降でのみサポートされています。

Cisco Prime CLI テンプレートを Cisco Umbrella Integration 環境のプロビジョニングに使用するには、次の手順を実行します。

ステップ 1 システムで実行されている Cisco IOS XE バージョンに対応する Cisco Prime テンプレートをダウンロードします。

ステップ 2 このファイルが圧縮されている場合は解凍します。

ステップ 3 Cisco Prime Web UI から、[設定（Configuration）] > [テンプレート（Templates）] > [機能とテクノロジー（Features and Technologies）] を選択し、次に [CLIテンプレート（ユーザー定義）（CLI Templates (User Defined)）] を選択します。

ステップ 4 [Import] をクリックします。

ステップ 5 テンプレートのインポート先フォルダを選択し、[テンプレートを選択（Select Templates）] をクリックして、先ほどダウンロードしたテンプレートを選択します。

ステップ 6 次の Cisco Umbrella Integration テンプレートが使用可能です。

- [Cisco Umbrella（Umbrella）]：このテンプレートは、デバイスの Cisco Umbrella Connector のプロビジョニングに使用します。
- [Cisco Umbrella クリーンアップ（Umbrella Cleanup）]：このテンプレートは、Cisco Umbrella Connector の削除に使用します。

Cisco Umbrella 統合の追加情報

関連資料

関連項目	マニュアル タイトル
IOS コマンド	『Cisco IOS Master Command List, All Releases』[英語]

関連項目	マニュアル タイトル
セキュリティ コマンド	• 『Cisco IOS Security Command Reference: Commands A to C』[英語] • 『Cisco IOS Security Command Reference: Commands D to L』[英語] • 『Cisco IOS Security Command Reference: Commands M to R』[英語] • 『Cisco IOS Security Command Reference: Commands S to Z』[英語]

シスコのテクニカル サポート

説明	リンク
シスコのサポート Web サイトでは、シスコの製品やテクノロジーに関するトラブルシューティングにお役立ていただけるように、マニュアルやツールをはじめとする豊富なオンライン リソースを提供しています。 お使いの製品のセキュリティ情報や技術情報を入手するために、Cisco Notification Service（Field Notice からアクセス）、Cisco Technical Services Newsletter、Really Simple Syndication（RSS）フィードなどの各種サービスに加入できます。 シスコのサポート Web サイトのツールにアクセスする際は、Cisco.com のユーザ ID およびパスワードが必要です。	http://www.cisco.com/support

Cisco Umbrella 統合の機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *222 : Cisco Umbrella* 統合の機能情報

機能名	リリース	機能情報
Cisco Umbrella 統合	Cisco IOS XE Everest リリース 16.6.1	Cisco Umbrella 統合機能により、Cisco デバイスを介して任意の DNS サーバに送信される DNS クエリを検査する、クラウドベースのセキュリティサービスを利用できるようになります。セキュリティ管理者は、完全修飾ドメイン名（FQDN）へのトラフィックを許可または拒否するポリシーを Cisco Umbrella クラウドに設定します。この機能は、Cisco ISR でのみサポートされます。

第 XVI 部

ユーザーセキュリティ

第 168 章

Cisco IOS Login Enhancements（Login Block）

Cisco IOS Login Enhancements（Login Block）機能により、ユーザはサービス拒絶（DoS）攻撃と思われる攻撃が検出された場合、ログイン試行を自動的にブロックするオプションを設定して、ルータのセキュリティを強化できます。

この機能により導入された Login Block オプションおよび Login Delay オプションで、Telnet または SSH 仮想接続を設定できます。この機能をイネーブルにすると、接続試行の失敗が複数回検出された場合に、「待機時間」を強制して「辞書攻撃」をスローダウンし、ルーティングデバイスをサービス拒絶（DoS）攻撃攻撃から保護できます。

（注） AAA の「待機モード」機能を使用する場合は、**aaa new-model** コマンドを使用して aaa new-model を設定する必要があります。

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報および警告については、「Bug Search Tool」およびご使用のプラットフォームおよびソフトウェア リリースのリリース ノートを参照してください。このモジュールで説明される機能に関する情報、および各機能がサポートされるリリースの一覧については、機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

Cisco IOS Login Enhancements について

サービス拒絶攻撃および辞書ログイン攻撃からの保護

ユーザまたは経営幹部レベルで、デバイスを管理する目的によるルーティングデバイスへの接続は、リモート コンソール（PC など）から Telnet または SSH（セキュア シェル）を使用して最も頻繁に実行されます。ユーザのデバイスと管理デバイスとの間の通信トラフィックが暗号化されるため、SSH では、よりセキュアな接続オプションが提供されます。Login Block 機能をイネーブルにすると、Telnet 接続と SSH 接続の両方に適用されます。

この機能によって導入される自動有効化、および Login Block 機能および Quiet Period 機能のロギングは、個人が使用するとネットワーク デバイスを阻害したり、損なう可能性のある 2 つの既知の方法に特に対処したりすることで、デバイスのセキュリティをさらに強化するように設計されています。

デバイスの接続アドレスが検出され、到達可能である場合、悪意あるユーザが接続要求のフラッディングによってデバイスの通常の動作を妨げようとする可能性があります。通常のルーティング サービスを適切に処理しようとして、繰り返し行われるログイン接続試行を処理しようとしたり、デバイスがビジーになったり、正規のシステム管理者に通常のログイン サービスを提供できなくなる可能性があるため、この種の攻撃は、サービス拒絶（DoS）攻撃の試行と呼ばれます。

辞書攻撃の主な意図は、一般的な DoS 攻撃とは異なり、デバイスへの管理アクセスを実際に取得することです。辞書攻撃とは、数千、時には数百万ものユーザ名/パスワードの組み合わせでログインを試行する自動プロセスです（このタイプの攻撃は、まず最初に、有効なパスワードとして一般的な辞書で見られるあらゆる言葉が使用されるため、「辞書攻撃」と呼ばれています）。このアクセスを試行するためにスクリプトやプログラムが使用されていて、このような試みのプロファイルは通常、DoS 試行のものと同じです。短期間で複数のログインを試行します。

検出プロファイルをイネーブルにすることにより、ログイン試行の失敗が反復する場合は、以降の接続要求を拒否して対応するように、ルーティング デバイスを設定できます（ログイン ブロッキング）。このブロックには「待機時間」と呼ばれる、一定の時間を設定できます。システム管理者との関連付けが把握されているアドレスを使用してアクセス リスト（ACL）を設定し、待機時間中でも正規の接続試行を許可できます。

Login Enhancements 機能の概要

連続するログイン試行間の遅延

シスコのデバイスは、仮想接続をできる限り高速で処理して受け入れることができます。ログイン試行間に遅延を導入すると、シスコのデバイスを辞書攻撃や DoS 攻撃などの悪意あるログイン接続から保護することができます。遅延は次のいずれかの方法でイネーブルにできます。

- **auto secure** コマンドを介します。AutoSecure 機能をイネーブルにすると、デフォルトで 1 秒のログイン遅延時間が自動的に強制されます。
- **login block-for** コマンドを介します。**login delay** コマンドを発行する前に、このコマンドを入力する必要があります。**login block-for** コマンドのみを入力すると、デフォルトで 1 秒のログイン遅延時間が自動的に強制されます。
- ログイン遅延時間の強制を秒単位で指定できる新しいグローバル コンフィギュレーション モード コマンドの **login delay** を介します。

DoS 攻撃が疑われる場合のログイン シャットダウン

設定された回数の接続試行が指定期間内で失敗しても、シスコのデバイスは「待機時間」のどのような追加接続も受け付けません。（事前定義されたアクセス コントロール リスト（ACL）によって許可されたホストは待機時間から除外されます）。

待機時間を発生させる接続試行の失敗回数は、新しいグローバル コンフィギュレーション モード コマンド **login block-for** で指定できます。待機時間から除外される定義済みの ACL は、新しいグローバル コンフィギュレーション モード コマンド **login quiet-mode access-class** で指定できます。

この機能は、デフォルトではディセーブルです。AutoSecure がイネーブルの場合はイネーブルになりません。

Cisco IOS Login Enhancement の設定方法

ログイン パラメータの設定

シスコのデバイスへの DoS 攻撃の疑いを検出し、辞書攻撃による影響の緩和に役立つログイン パラメータを設定するには、ここに示す手順を実行します。

すべてのログインパラメータは、デフォルトではディセーブルです。他のログインコマンドを使用する前に、デフォルトのログイン機能を有効にする **login block-for** コマンドを発行する必要があります。**login block-for** コマンドをイネーブルにすると、次のデフォルトが強制されます。

- デフォルトの 1 秒のログイン遅延
- Telnet または SSH を通じて行われるすべてのログイン試行は、待機時間中拒否されます。つまり、**login quiet-mode access-class** コマンドが発行されるまで、ACL はログイン時間から除外されません。

手順の概要

1. **enable**
2. **configure terminal**
3. **aaa new-model**

4. **login block-for** *seconds* **attempts** *tries* **within** *seconds*
5. **login quiet-mode access-class** {*acl-name* | *acl-number*}
6. **login delay** *seconds*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**aaa new-model** 例： `Router(config)# aaa new-model`	認証、許可、およびアカウンティング（AAA）アクセス コントロール モデルをイネーブルにします。
ステップ 4	**login block-for** *seconds* **attempts** *tries* **within** *seconds* 例： `Router(config)# login block-for 100 attempts 2 within 100`	Cisco IOS XE デバイスで DoS 検出の提供に役立つログイン パラメータを設定します。 （注） このコマンドは、その他のログイン コマンドを使用する前に発行する必要があります。
ステップ 5	**login quiet-mode access-class** {*acl-name* | *acl-number*} 例： `Router(config)# login quiet-mode access-class myacl`	（任意）このコマンドはオプションですが、ルータが待機モードに切り替わるときにルータに適用される ACL を指定するように設定することを推奨します。ルータが待機モードになっている間は、すべてのログイン要求が拒否され、使用できる接続はコンソール経由の接続のみになります。 このコマンドを設定しないかぎり、デフォルトの ACL **sl_def_acl** はルータ上に作成されます。この ACL は実行コンフィギュレーションでは非表示です。デフォルトの ACL のパラメータを表示するには、**show access-list sl_def_acl** を使用します。 次に例を示します。 `Router#show access-lists sl_def_acl`

	コマンドまたはアクション	目的
		Extended IP access list sl_def_acl 10 deny tcp any any eq telnet 20 deny tcp any any eq www 30 deny tcp any any eq 22 40 permit ip any any
ステップ 6	**login delay** *seconds* 例： Router(config)# login delay 10	（任意）連続するログイン試行間の遅延を設定します。

次の作業

ルータでログインパラメータを設定した後、設定を確認する必要がある場合があります。この作業を完了するには、「ログイン パラメータの確認 （2471 ページ）」を参照してください。

ログイン パラメータの確認

ルータに適用されたログイン設定と現在のログイン ステータスを確認するには、次の作業を実行します。

手順の概要

1. **enable**
2. **show login failures**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： Router> enable	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**show login failures** 例： Router# show login	ログイン パラメータを表示します。 • **failures** ：失敗したログイン試行に関連する情報のみを表示します。

例

show login コマンドからの次のサンプル出力は、ログインパラメータが指定されていないことを確認します。

```
Router# show login
No login delay has been applied.
No Quiet-Mode access list has been configured.
All successful login is logged and generate SNMP traps.
All failed login is logged and generate SNMP traps
Router NOT enabled to watch for login Attacks
```

show login コマンドからの次のサンプル出力は、**login block-for** コマンドが発行されたことを確認します。この例で、コマンドは100秒以内に16回以上のログイン要求が失敗した場合、ログインホストを100秒ブロックするように設定されています。すでに5回のログイン要求が失敗しています。

```
Router# show login
A default login delay of 1 seconds is applied.
No Quiet-Mode access list has been configured.
All successful login is logged and generate SNMP traps.
All failed login is logged and generate SNMP traps.
Router enabled to watch for login Attacks.
If more than 15 login failures occur in 100 seconds or less, logins will be disabled for
 100 seconds.
Router presently in Watch-Mode, will remain in Watch-Mode for 95 seconds.
Present login failure count 5.
```

show login コマンドからの次のサンプル出力は、ルータが待機モードになっていることを確認します。この例で、**login block-for** コマンドは、100秒以内に3回以上のログイン要求が失敗した場合、ログインホストを100秒ブロックするように設定されています。

```
Router# show login
A default login delay of 1 seconds is applied.
No Quiet-Mode access list has been configured.
All successful login is logged and generate SNMP traps.
All failed login is logged and generate SNMP traps.
Router enabled to watch for login Attacks.
If more than 2 login failures occur in 100 seconds or less, logins will be disabled for
 100 seconds.
Router presently in Quiet-Mode, will remain in Quiet-Mode for 93 seconds.
Denying logins from all sources.
```

show login failures コマンドからの次のサンプル出力は、ルータ上で失敗したすべてのログイン試行を表示します。

```
Router# show login failures
Information about login failure's with the device
Username      Source IPAddr  lPort Count  TimeStamp
try1          10.1.1.1        23    1     21:52:49 UTC Sun Mar 9 2003
try2          10.1.1.2        23    1     21:52:52 UTC Sun Mar 9 2003
```

show login failures コマンドからの次のサンプル出力は、現在記録されている情報がないことを確認します。

```
Router# show login failures
*** No logged failed login attempts with the device.***
```

ログイン パラメータの設定例

ログイン パラメータの設定例

次に、100秒以内に15回ログイン試行が失敗した場合に100秒の待機時間に入るようにルータを設定する例を示します。待機時間中、ACL “myacl” からのホスト以外、すべてのログイン要求が拒否されます。

```
Router(config)# aaa new-model
Router(config)# login block-for 100 attempts 15 within 100
Router(config)# login quiet-mode access-class myacl
```

その他の参考資料

関連資料

関連項目	マニュアル タイトル
AutoSecure の設定	AutoSecure の機能モジュール。
セキュリティ コマンド：コマンド構文の詳細、コマンドモード、コマンド履歴、デフォルト設定、使用上のガイドライン、および例	『*Cisco IOS Security Command Reference*』
セキュアな管理/管理アクセス	「Role-Based CLI Access」機能モジュール

標準

標準	タイトル
なし。	--

MIB

MIB	MIB のリンク
なし。	選択したプラットフォーム、Cisco ソフトウェア リリース、およびフィーチャ セットの MIB を検索してダウンロードする場合は、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

RFC

RFC	タイトル
この機能によりサポートされた新規 RFC または改訂 RFC はありません。またこの機能による既存 RFC のサポートに変更はありません。	--

シスコのテクニカル サポート

説明	リンク
シスコのサポート Web サイトでは、シスコの製品やテクノロジーに関するトラブルシューティングにお役立ていただけるように、マニュアルやツールをはじめとする豊富なオンライン リソースを提供しています。 お使いの製品のセキュリティ情報や技術情報を入手するために、Cisco Notification Service（Field Notice からアクセス）、Cisco Technical Services Newsletter、Really Simple Syndication（RSS）フィードなどの各種サービスに加入できます。 シスコのサポート Web サイトのツールにアクセスする際は、Cisco.com のユーザ ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

Cisco IOS Login Enhancements（Login Block）に関する機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *223 : Cisco IOS Login Enhancements*（*Login Block*）に関する機能情報

機能名	リリース	機能の設定情報
Cisco IOS Login Enhancements	Cisco IOS XE Release 2.1	Cisco IOS Login Enhancements（Login Block）機能により、ユーザはサービス拒絶（DoS）攻撃と思われる攻撃が検出された場合、ログイン試行を自動的にブロックするオプションを設定して、ルータのセキュリティを強化できます。 この機能は、Cisco IOS XE リリース 2.1 では、Cisco ASR 1000 シリーズ サービス アグリゲーション ルータに導入されていました。 この機能により、次のコマンドが変更されました。**login block-for**、**login delay**、 **login quiet-mode access-class**、**show login**。

第 169 章

パスワード、特権、およびログインによるセキュリティ設定

Cisco IOS ベースのネットワーキング デバイスには、デバイスで実行されているオペレーティング システムだけを使用して、基本的なセキュリティを実装できる機能が複数あります。たとえば、次のような機能があります。

- ネットワーキングデバイスのステータスを変更できるコマンドと、デバイスの監視に使用されるコマンドに対するアクセスを制御する CLI セッションの複数の認可レベル
- CLI セッションにパスワードを割り当てる機能
- ユーザがユーザ名を使用してネットワーキングデバイスにログインする操作を必須にする機能
- CLI セッション用に新しい認可レベルを作成するコマンドの特権レベルを変更する機能

このモジュールは、使用しているネットワーキングデバイスについて、基本レベルのセキュリティを実装する手順です。基本レベルのセキュリティを実装するために使用できる、最もシンプルなオプションを中心に説明します。セキュリティ オプションを設定せずにネットワークにネットワーキング デバイスをインストールした場合、またはこれからネットワーキング デバイスをインストールする予定で、基本的なセキュリティを実装する方法を理解する必要がある場合、このドキュメントが役立ちます。

パスワード、特権、およびログインによるセキュリティ設定の制約事項

任意のローカルまたはリモートの認証、許可、アカウンティング（AAA）セキュリティ機能を使用するようにネットワーキングデバイスを設定しないでください。このドキュメントでは、ネットワーク デバイスでローカルで設定できる非 AAA セキュリティ機能のみを説明します。

ネットワーク デバイスでローカルで実行できる AAA セキュリティ機能の設定方法、または TACACS+ や RADIUS サーバを使用したリモート AAA セキュリティの設定方法については、『*Securing User Services Configuration Guide Library*』を参照してください。

可逆的パスワードタイプの制約事項とガイドライン

- パスワードタイプ 0 およびタイプ 7 は廃止されました。したがって、コンソール、Telnet、SSH、webUI、NETCONF への管理者ログインに使用されるパスワードタイプ 0 およびタイプ 7 は、パスワードタイプ 8 またはタイプ 9 に移行する必要があります。
- ISG および Dot1x の CHAP、EAP などのローカル認証でユーザー名とパスワードがタイプ 0 およびタイプ 7 の場合、アクションは不要です。
- イネーブルパスワードタイプ 0 およびタイプ 7 は、パスワードタイプ 8 またはタイプ 9 に移行する必要があります。

不可逆的パスワードタイプの制約事項とガイドライン

- パスワードタイプ 5 は廃止されました。パスワードタイプ 5 は、より強力なパスワードタイプ 8 またはタイプ 9 に移行する必要があります。
- ユーザー名シークレット パスワード タイプ 5 およびイネーブル シークレット パスワード タイプ 5 の場合は、タイプ 8 または 9 に移行します。
- シークレット パスワード タイプ 4 はサポートされていません。

パスワード、特権、およびログインによるセキュリティ設定について

セキュリティ スキームを作成する利点

ネットワークの優れたセキュリティ スキームの基礎は、ネットワーキング デバイスのユーザ インターフェイスを不正アクセスから保護することです。ネットワーキング デバイス上のユー

ザインターフェイスに対するアクセスを保護することで、ネットワークの安定を妨げ、ネットワーク セキュリティを危険にさらすような設定の変更を不正ユーザが行うことを回避できます。

このドキュメントで説明するCisco IOS XEの機能をさまざまな方法で組み合わせて、実際の各ネットワーク デバイスに固有のセキュリティ スキームを作成できます。次に、いくつかの設定例を示します。

- コマンドを実行可能なレベルを非管理特権レベルまで下げることで、非管理ユーザに対して、ネットワーキングデバイスで使用できる管理コマンドの一部の実行を許可できます。この処理は、次のシナリオに役立ちます。
  - ISPで、窓口のテクニカルサポートスタッフが、新規顧客の新規インターフェイスをイネーブルにするタスク、または接続がトラフィックのパスを停止した顧客の接続をリセットするタスクなどを実行できるようにする場合。その実行方法の例については、例：ユーザがインターフェイスをシャットダウンおよびイネーブル化することを可能にするデバイスの設定 （2518 ページ）を参照してください。
  - 窓口のテクニカル サポート スタッフが、ターミナル サーバから不正に接続解除されたコンソール ポート セッションをクリアする機能を実行できるようにする場合。その実行方法の例については、例：ユーザがリモート セッションをクリア可能にするデバイスの設定 （2516 ページ）を参照してください。
  - 窓口のテクニカル サポート スタッフが、ネットワーク デバイスの設定を変更ではなく表示し、ネットワークの問題を解決する機能を実行できるようにする場合。その実行方法の例については、例：ユーザが実行コンフィギュレーションを表示可能にするデバイスの設定 （2517 ページ）を参照してください。

Cisco IOS XE CLI モード

シスコ デバイスの設定を支援するために、Cisco IOS XE コマンドライン インターフェイスは、さまざまなコマンド モードに分かれています。各コマンド モードには、ルータとネットワークの動作を設定、メンテナンス、モニタリングするための独自のコマンドセットがあります。常に使用可能なコマンドは、モードによって異なります。システムプロンプト（デバイスプロンプト）で疑問符（**?**）を入力すると、各コマンドモードで使用できるコマンドのリストを取得できます。

特定のコマンドを使用すると、コマンドモードを変更できます。ユーザがモードにアクセスする標準の順序は、ユーザEXECモード、特権EXECモード、グローバル コンフィギュレーション モード、特定のコンフィギュレーション モード、コンフィギュレーション サブモード、およびコンフィギュレーション サブモードです。

（注） Cisco IOS XE ソフトウェア ベースのネットワーク デバイスのデフォルト設定で使用できるのは、ユーザEXECモード（ローカルおよびリモートCLIセッションの場合）と特権EXECモードへのアクセスを保護するパスワードを設定する操作だけです。ここでは、ユーザー名、パスワード、および**privilege**コマンドを組み合わせて他のモードへのアクセスおよびコマンドを保護することで、追加のセキュリティレベルを提供する方法について説明します。

ほとんどの EXEC モード コマンドは、現在の設定ステータスを表示する **show** コマンドまたは **more** コマンドや、カウンタやインターフェイスをクリアする **clear** コマンドのように、1 回限りのコマンドです。EXEC モードのコマンドは、ルータをリブートすると保持されません。

特権 EXEC モードから、グローバル コンフィギュレーション モードに入ることができます。このモードでは、一般的なシステム特性を設定するためのコマンドを実行できます。また、グローバル コンフィギュレーション モードを使用して特定のコンフィギュレーション モードを開始することもできます。グローバル コンフィギュレーション モードを含むコンフィギュレーション モードでは、実行コンフィギュレーションを変更できます。後で設定を保存すると、ルータをリブートしてもこれらのコマンドが保持されます。

グローバル コンフィギュレーション モードから、さまざまなプロトコル固有または機能固有のコンフィギュレーション モードを開始できます。CLI 階層では、グローバル コンフィギュレーション モードのみからこれらのコンフィギュレーション モードを開始できます。たとえば、インターフェイス コンフィギュレーション モードは、共通して使用されるコンフィギュレーション モードです。

コンフィギュレーション モードから、コンフィギュレーション サブモードを開始できます。コンフィギュレーション サブモードは、特定のコンフィギュレーション モードの範囲内で特定の機能を設定するために使用します。たとえば、この章では、インターフェイス コンフィギュレーション モードのサブモードであるサブインターフェイス コンフィギュレーション モードについて説明します。

ROM モニタ モードは、ルータが適切にブートできない場合に使用される別のモードです。システム（ルータ、スイッチ、またはアクセス サーバー）のブート時に適切なシステム イメージが見つからない場合、システムは ROM モニター モードを開始します。ROM モニター（ROMMON）モードには、起動時にブート シーケンスに割り込むことでもアクセスできます。ROMMON には使用できるセキュリティ機能がないため、このドキュメントでは説明していません。

ユーザ EXEC モード

ルータでセッションを開始するときは、通常、EXEC モードの 2 つあるアクセス レベルの 1 つであるユーザ *EXEC* モードから始めます。セキュリティのために、ユーザー EXEC モードで使用できる EXEC コマンドは制限されています。このアクセス レベルは、ルータのステータスを確認するなど、ルータの設定を変更しない作業のために予約されています。

デバイスの設定で、ユーザのログインが必須の場合、そのログインプロセスはユーザ名とパスワードが必須になります。接続が拒否されるまでにパスワードを 3 回入力できます。

ユーザ EXEC モードは、デフォルトで特権レベル 1 に設定されています。特権 EXEC モードは、デフォルトで特権レベル 15 に設定されています。ユーザ EXEC モードでネットワーキング デバイスにログインしている場合、システムは特権レベル 1 で実行されます。デフォルトで、特権レベル 1 の EXEC コマンドは、特権レベル 15 で使用できるコマンドのサブセットです。特権 EXEC モードでネットワーキング デバイスにログインしている場合、システムは特権レベル 15 で実行されます。**privilege** コマンドを使用すると、1 ～ 15 の任意の特権レベルにコマンドを移動できます。

一般に、ユーザ EXEC コマンドでは、リモート デバイスへの接続、端末回線の一時的な設定変更、基本的なテストの実行、システム情報の表示を行うことができます。

使用可能なユーザ EXEC コマンドの一覧を表示するには、次のコマンドを使用します。

コマンド	目的
`Device(config)# ?`	ユーザ EXEC モード コマンド リストを表示します

ユーザ EXEC モード プロンプトは、デバイスのホスト名と、それに続く山カッコ（>）で構成されます。次に例を示します。

```
Device>
```

setup EXEC コマンドで初期設定時に変更していなければ、通常はデフォルトのホスト名は Router です。また、ホスト名の変更には、 **hostname** グローバル コンフィギュレーション コマンドを使用します。

（注） Cisco IOS XE のドキュメントの例では、「デバイス」のデフォルト名を使用することを想定しています。さまざまなデバイス（アクセス サーバ）が異なるデフォルト名を使用できます。デバイス（ルータ、アクセスサーバー、またはスイッチ）に、**hostname** コマンドで名前が設定されている場合、デフォルトの名前の代わりにその名前がプロンプトに表示されます。

ユーザーEXEC モードで使用できるコマンドの一覧を表示するには、次の例に示すように疑問符（**?**）を入力します。

```
Device> ?

Exec commands:
 <1-99>           Session number to resume
 connect          Open a terminal connection
 disconnect       Disconnect an existing telnet session
 enable           Turn on privileged commands
 exit             Exit from Exec mode
 help             Description of the interactive help system
 lat              Open a lat connection
 lock             Lock the terminal
 login            Log in as a particular user
 logout           Exit from Exec mode and log out
 menu             Start a menu-based user interface
 mbranch          Trace multicast route for branch of tree
 mrbranch         Trace reverse multicast route to branch of tree
 mtrace           Trace multicast route to group
 name-connection  Name an existing telnet connection
 pad              Open a X.29 PAD connection
 ping             Send echo messages
 resume           Resume an active telnet connection
 show             Show running system information
 systat           Display information about terminal lines
 telnet           Open a telnet connection
 terminal         Set terminal line parameters
 tn3270           Open a tn3270 connection
```

```
trace           Trace route to destination
where           List active telnet connections
x3              Set X.3 parameters on PAD
```

コマンドの一覧は、使用しているソフトウェア機能セットおよびプラットフォームによって異なります。

（注） コマンドは、大文字、小文字、または大文字と小文字を混在させて入力できます。大文字と小文字の区別があるのはパスワードだけです。ただし、Cisco IOS XE のマニュアルの表記法では、コマンドは常に小文字になっています。

特権 EXEC モード

すべてのコマンドにアクセスするには、EXECモードの第2レベルのアクセスである特権*EXEC*モードを開始する必要があります。特権EXECモードを開始するには、通常、パスワードが必要です。特権EXECモードでは、任意のEXECコマンドを入力できます。これは、特権EXECモードが、ユーザー EXEC モード コマンドのスーパーセットであるためです。

多くの特権EXECモードコマンドは操作パラメータを設定するため、不正使用を防ぐために、特権EXECレベルアクセスをパスワードで保護する必要があります。特権EXECコマンドセットには、ユーザEXECモードに含まれているこれらのコマンドが含まれます。また、特権EXECモードでは、**configure** コマンドを使用することで各種コンフィギュレーション モードにアクセスでき、**debug** などの高度なテストコマンドも含まれています。

特権 EXEC モードは、デフォルトで特権レベル 15 に設定されています。ユーザ EXEC モードは、デフォルトで特権レベル 1 に設定されています。詳細については、ユーザ EXEC モード（2480ページ）を参照してください。特権EXECモードでネットワーキングデバイスにログインしている場合、システムは特権レベル15で実行されます。ユーザEXECモードでネットワーキングデバイスにログインしている場合、システムは特権レベル1で実行されます。デフォルトで、特権レベル15のEXECコマンドは、特権レベル1で使用できるコマンドのスーパーセットです。**privilege** コマンドを使用すると、1～15の任意の特権レベルにコマンドを移動できます。特権レベルおよび**privilege** コマンドの詳細については、Cisco IOS XE の特権レベル（2491ページ）を参照してください。

特権 EXEC モード プロンプトは、デバイスのホスト名と、それに続くポンド記号（#）で構成されます。次に例を示します。

```
Device#
```

特権 EXEC モードにアクセスするには、次のコマンドを使用します。

コマンド	目的

`Device> enable`
`Password`
`Device# exit`
`Device>`
	特権 EXEC モードをイネーブルにします。
	• 特権 EXEC モードのパスワードを選択すると、enable コマンドの発行後にパスワードの入力が求められます。
	• 特権 EXEC モードを終了するには、exit コマンドを使用します。

（注） 特権 EXEC モードは、モードの開始に、**enable** コマンドを使用するため、「イネーブルモード」とも呼ばれます。

システムでパスワードが設定されている場合、特権 EXEC モードへのアクセスが許可される前にパスワードを入力するよう求められます。パスワードは画面には表示されません。また、大文字と小文字が区別されます。イネーブル パスワードが設定されていない場合、特権 EXEC モードには、ローカル CLI セッション（コンソール ポートに接続された端末）からしかアクセスできません。

Telnet 接続など、リモート接続上のルータで特権 EXEC モードへのアクセスを試行しても、特権 EXEC モードのパスワードを設定していない場合は、**% No password set** エラーメッセージが表示されます。リモート接続の詳細については、リモート CLI セッション （2487 ページ）を参照してくださいシステム管理者は、**enable secret** または **enable password** グローバル コンフィギュレーション コマンドを使用して、特権 EXEC モードへのアクセスを制限するパスワードを設定します。特権 EXEC モードのパスワード設定の詳細については、特権 EXEC モードへのアクセスの保護 （2498 ページ） を参照してください。

ユーザ EXEC モードに戻るには、次のコマンドを使用します。

コマンド	目的
`Device# disable`	特権 EXEC モードを終了し、ユーザ EXEC モードに戻ります。

次に、特権 EXEC モードにアクセスするプロセスの例を示します。

```
Device> enable
Password:<letmein>
Device#
```

入力してもパスワードが表示されませんが、ここでは説明のために表示しています。特権 EXEC モードで使用できるコマンドの一覧を表示するには、プロンプトで **?** コマンドを発行します。次の項で説明するように、特権 EXEC モードからグローバル コンフィギュレーション モードにアクセスできます。

（注） 特権 EXEC コマンド セットには、ユーザ EXEC モードで使用できるすべてのコマンドが含まれているため、一部のコマンドはどちらのモードでも実行できます。Cisco IOS XE のドキュメントでは、ユーザ EXEC モードまたは特権 EXEC モードで入力できるコマンドは、EXEC モードコマンドと呼ばれます。ユーザまたは特権とドキュメントに特記されていない場合、どちらのモードでもそのコマンドを入力できることを示します。

グローバル コンフィギュレーション モード

「グローバル」という言葉は、システム全体に影響する特性や機能を示すために使用されています。グローバル コンフィギュレーション モードは、システムをグローバルに設定したり、インターフェイスやプロトコルなどの特定の要素を設定したりする目的で、特定のコンフィギュレーションモードを開始するために使用します。グローバルコンフィギュレーションモードを開始するには、**configure terminal** 特権 EXEC コマンドを使用します。

グローバル コンフィギュレーション モードにアクセスするには、特権 EXEC モードで次のコマンドを入力します。

コマンド	目的
`Device# configure terminal`	特権 EXEC モードで、グローバル コンフィギュレーション モードを開始します。

次に、特権 EXEC モードからグローバル コンフィギュレーション モードを開始するプロセスの例を示します。

```
Device# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Device(config)#
```

システム プロンプトが変わり、グローバル コンフィギュレーション モードに入ったことが示されることに注意してください。グローバルコンフィギュレーションモードのプロンプトは、デバイスのホスト名と、それに続く（config）およびポンド記号（#）で構成されます。特権 EXEC モードで使用できるコマンドの一覧を表示するには、プロンプトで **?** コマンドを発行します。

グローバルコンフィギュレーションモードでコマンドを入力すると、すぐに実行コンフィギュレーション ファイルが更新されます。つまり、設定に対する変更は、有効なコマンドの後で Enter キーまたは Return キーを押すたびに有効になります。ただし、これらの変更は、**copy running-config startup-config** EXEC モードコマンドを発行するまで、スタートアップ コンフィギュレーション ファイルに保存されません。この動作は、このマニュアルの後の項で詳しく説明します。

上記の例のように、コントロール（Ctrl）キーと「z」キーを同時に押すと、システムダイアログでコンフィギュレーションセッションを終了するプロンプトが表示されます。これらのキー操作で、**^Z** が画面に出力されます。実際にコンフィギュレーション セッションを終了するには、Ctrl+Z キーの組み合わせ、**end** コマンド、または Ctrl+C キーの組み合わせを使用できま

す。現在のコンフィギュレーションセッションを終了することをシステムに示すための方法としては、**end** コマンドが推奨されます。

⚠

注意 有効なコマンドを入力してから、コマンド ラインの最後で Ctrl+Z キーを使用すると、そのコマンドが実行コンフィギュレーション ファイルに追加されます。つまり、Ctrl+Z キーを使用することは、終了前に Enter（復帰）キーを押すことと同じです。このような理由から、**end** コマンドを使用してコンフィギュレーションセッションを終了するほうが安全です。また、改行信号を送信せずにコンフィギュレーション セッションを終了するには、Ctrl+C キーの組み合わせを使用できます。

また、**exit** コマンドを使用して、グローバル コンフィギュレーション モードから EXEC モードに戻ることもできますが、使用できるのはグローバル コンフィギュレーション モードだけです。Ctrl+Z キーを押すか **end** コマンドを入力することにより、どのコンフィギュレーション モードまたはコンフィギュレーション サブモードにいるかにかかわらず、常に EXEC モードに戻ることができます。

グローバル コンフィギュレーション コマンド モードを終了して特権 EXEC モードに戻るには、次のいずれかのコマンドを使用します。

コマンド	目的

`Device(config)# end`
または
`Device(config)# ^Z`
	現在のコンフィギュレーション セッションを終了して、特権 EXEC モードに戻ります。

`Device(config)# exit`	現在のコマンド モードを終了して、前のモードに戻ります。たとえば、グローバル コンフィギュレーション モードから特権 EXEC モードに戻ります。

グローバル コンフィギュレーション モードから、いくつかのプロトコル固有、プラットフォーム固有、機能固有のコンフィギュレーション モードを開始できます。

次のセクションで説明されているインターフェイス コンフィギュレーション モードは、グローバル コンフィギュレーション モードから入ることができるコンフィギュレーション モードの例です。

インターフェイス コンフィギュレーション モード

グローバル コンフィギュレーション モードから開始する特定のコンフィギュレーション モードの一例が、インターフェイス コンフィギュレーション モードです。

多くの機能は、インターフェイスごとにイネーブルになります。インターフェイス コンフィギュレーション コマンドは、イーサネット、FDDI、シリアル ポートなど、インターフェイスの動作を変更します。インターフェイス コンフィギュレーション コマンドは常に、インター

フェイスタイプを定義する **interface** グローバル コンフィギュレーション コマンドの後に指定します。

帯域幅やクロック レートなど、一般的なインターフェイス パラメータに影響があるインターフェイス コンフィギュレーション コマンドの詳細については、Release 12.2 の『*Cisco IOS Interface Configuration Guide*』を参照してください。プロトコル固有のコマンドについては、該当する Cisco IOS XE ソフトウェア コマンド リファレンスを参照してください。

インターフェイス コンフィギュレーション コマンドにアクセスし、その一覧を表示するには、次のコマンドを使用します。

コマンド	目的
`Device(config)# interface type number`	設定するインターフェイスを指定して、インターフェイス コンフィギュレーション モードを開始します。

次に、シリアル インターフェイス 0 についてユーザがインターフェイス コンフィギュレーション モードを開始する例を示します。新しいプロンプト、*hostname*（config-if）# は、インターフェイス コンフィギュレーション モードを示しています。

```
Device(config)# interface serial 0
Device(config-if)#
```

インターフェイス コンフィギュレーション モードを終了してグローバル コンフィギュレーション モードに戻るには、**exit** コマンドを入力します。

コンフィギュレーション サブモードは、他のコンフィギュレーション モード（グローバル コンフィギュレーション モード以外）から開始されるコンフィギュレーション モードです。コンフィギュレーション サブモードは、コンフィギュレーション モード内の特定の要素を設定するためにあります。コンフィギュレーション サブモードの 1 つの例は、次の項で説明するサブインターフェイス コンフィギュレーション モードです。

サブインターフェイス コンフィギュレーション モード

インターフェイス コンフィギュレーション モードから、サブインターフェイス コンフィギュレーション モードに入ることができます。サブインターフェイス コンフィギュレーション モードは、インターフェイス コンフィギュレーション モードのサブモードの 1 つです。サブインターフェイス コンフィギュレーション モードでは、1 つの物理インターフェイスに複数の仮想インターフェイス（別名サブインターフェイス）を設定できます。サブインターフェイスは、さまざまなプロトコルにとって個別の物理インターフェイスのように見えます。

サブインターフェイスの設定方法の詳細については、Cisco IOS XE ソフトウェア マニュアル セットの特定のプロトコルの該当するドキュメンテーション モジュールを参照してください。

サブインターフェイス コンフィギュレーション モードにアクセスするには、インターフェイス コンフィギュレーション モードで次のコマンドを使用します。

コマンド	目的
`Device(config-if)# interface type number`	設定する仮想インターフェイスを指定し、サブインターフェイス コンフィギュレーション モードを開始します。

次の例では、シリアル ライン 2 のサブインターフェイスで、フレーム リレー カプセル化を設定します。シリアルインターフェイス 2 のサブインターフェイス 1 であることを示すため、サブインターフェイスは「2.1」として識別されます。新しいプロンプトの *hostname*（config-subif）#は、サブインターフェイス コンフィギュレーション モードを示します。サブインターフェイスは、1 つ以上のフレーム リレー PVC をサポートするように設定できます。

```
Device(config)# interface serial 2
Device(config-if)# encapsulation frame-relay
Device(config-if)# interface serial 2.1
Device(config-subif)#
```

サブインターフェイス コンフィギュレーション モードを終了しインターフェイス コンフィギュレーション モードに戻るには、**exit** コマンドを入力します。コンフィギュレーション セッションを終了し特権 EXEC モードに戻るには、Ctrl+Z キーを押すか、**end** コマンドを入力します。

Cisco IOS XE CLI セッション

ローカル CLI セッション

ローカル CLI セッションでは、ネットワーク デバイスのコンソール ポートへの直接アクセスが要求されます。ローカル CLI セッションは、ユーザ EXEC モードで開始されます。ネットワーキング デバイスの設定とおよび管理に必要なすべてのタスクは、ローカル CLI セッションを使用して実行できます。ローカル CLI セッションを確立する最も一般的な方式は、PC 上のシリアルポートを、ネットワーキング デバイスのコンソール ポートに接続し、PC で端末エミュレーション アプリケーションを起動する方法です。必要とされるケーブルとコネクタの種類および PC 上の端末エミュレーション アプリケーションの設定は、設定しているネットワーク デバイスの種類によって異なります。ローカル CLI セッションでネットワーキング デバイスを設定する方法の詳細については、そのデバイスのマニュアルを参照してください。

リモート CLI セッション

リモート CLI セッションは、PC などのホストとネットワーク上のルータなどのネットワーク デバイス間で、Telnet やセキュア シェル（SSH）などのリモート端末アクセス アプリケーションを使用して作成されます。ローカル CLI セッションは、ユーザ EXEC モードで開始されます。ネットワーク デバイスの設定とおよび管理に必要なほとんどのタスクは、リモート CLI セッションを使用して実行できます。例外は、ROM モニタ モードのときのネットワーク デバイスとの通信や、（コンソール ポートで新しい OS イメージをアップロードすることによる、破壊されたオペレーティング システム（OS）の復元など）、コンソール ポートと直接的に通信するタスクです。

このドキュメントでは、リモート Telnet セッションのセキュリティを設定する方法について説明します。Telnet は、ネットワーキング デバイスでリモート CLI セッションにアクセスする際に最も一般的な方式です。

（注） ただし、SSH の方が Telnet よりも安全な方式です。SSH には、PC などのローカル管理デバイスと、管理しているネットワーキング デバイスとの間のセッション トラフィックを暗号化する機能があります。SSH を使用してセッション トラフィックを暗号化すると、ハッカーがトラフィックを傍受しても、トラフィックをデコードできなくなります。SSH を使用する詳細については、「Secure Shell Version 2 Support」フィーチャ モジュールを参照してください。

端末回線はローカルおよびリモート CLI セッションに使用される

シスコ ネットワーク デバイスでは、ローカルおよびリモート CLI セッションを管理するソフトウェア コンポーネントを参照するため語線を使用します。**line console 0** グローバル コンフィギュレーション コマンドを使用してライン コンフィギュレーション モードを開始し、パスワードなど、コンソール ポートのオプションを設定します。

```
Device# configure terminal
Device(config)# line console 0
Device(config-line)# password password-string
```

リモート CLI セッションでは、仮想テレタイプ（VTY）の行である回線を使用しています。**line vty** *line-number* [*ending-line-number*] グローバル コンフィギュレーション コマンドを使用してライン コンフィギュレーション モードを開始し、パスワードなど、リモート CLI セッションのオプションを設定します。

```
Device# configure terminal
Device(config)# line vty 0 4
Device(config-line)# password password-string
```

Cisco IOS XE EXEC モードへのアクセスの保護

Cisco IOS XE では、次へのアクセスを保護するパスワードを設定できます。

ユーザ EXEC モードへのアクセスの保護

ネットワーク デバイスの安全な環境の構築に向けた第一歩は、ローカルおよびリモート CLI セッションのパスワードを設定することで、ユーザ EXEC モードへのアクセスを保護することです。

ローカル CLI セッションでユーザ EXEC モードに対するアクセスを保護するには、コンソール ポートでパスワードを設定します。ローカル CLI セッションのパスワードの設定と確認（2496 ページ）を参照してください。

リモート CLI セッションでユーザ EXEC モードに対するアクセスを保護するには、仮想端末回線（VTY）でパスワードを設定します。リモート CLI セッションのパスワード設定方法の手順については、「リモート CLI セッションのパスワードの設定と確認（2493 ページ）」を参照してください。

特権 EXEC モードへのアクセスの保護

ネットワーキング デバイスのセキュア環境を作成するための第 2 段階は、特権 EXEC モードに対するアクセスをパスワードで保護することです。特権 EXEC モードに対するアクセスを保護する方式は、ローカルおよびリモートの CLI セッションと同じです。

特権 EXEC モードに対するアクセスを保護するには、そのモード用のパスワードを設定します。特権 EXEC モードを開始するコマンドが **enable** なので、このパスワードもイネーブルパスワードと呼ばれることがあります。

コマンド	目的

enable
 	
`Device> enable`
 	
`Password`
 	
`Device#`
	特権 EXEC モードを有効にします。
	• パスワードを入力します（要求された場合）。パスワードはターミナル ウィンドウに表示されません。
	• プロンプト文字列の末尾の「>」は、特権 EXEC モードにいることを示す「#」に変更されました。

Cisco IOS XE のパスワード暗号化レベル

ネットワーク デバイスで設定するパスワードの中には、プレーン テキストで設定に保存されるものもあります。これは、ディスクにコンフィギュレーション ファイルのコピーを保存すると、コンフィギュレーション ファイルを読み取ることで、ディスクへのアクセス権を持つ誰もが、パスワードがわかることを意味します。次の種類のパスワードは、デフォルトでプレーン テキストで設定に保存されます。

- ローカル CLI セッションのコンソール パスワード
- リモート CLI セッションの仮想端末回線のパスワード
- パスワードを設定するため、デフォルトの方法を使用したユーザ名のパスワード
- **enable password** *password* コマンドで設定されるときの特権 EXEC モードのパスワード
- RIPv2 と EIGRP で使用されている認証キー チェーン パスワード
- BGP ネイバーを認証するための BGP パスワード
- OSPF ネイバーの認証に使用する OSPF 認証キー
- ISIS ネイバーを認証するための ISIS パスワード

ルータの設定ファイルからのこの引用文は、クリアテキストとして保存されたパスワードと認証キーの例を示しています。

```
!
enable password O9Jb6D
!
username username1 password 0 kV9sIj3
!
key chain trees
 key 1
  key-string willow
!
interface Ethernet1/0.1
 ip address 172.16.6.1 255.255.255.0
 ip router isis
 ip rip authentication key-chain trees
 ip authentication key-chain eigrp 1 trees
 ip ospf authentication-key j7876
 no snmp trap link-status
 isis password u7865k
!
line vty 0 4
 password V9jA5M
!
```

service password-encryption コマンドを使用することで、これらのクリアテキストのパスワードをコンフィギュレーション ファイルで暗号化できます。パスワードを暗号化するのに **service password-encryption** コマンドによって使用された暗号化アルゴリズムは、公で使用可能なツールを使用して暗号化されるテキストストリングを作成するため、これは最小レベルのセキュリティにすぎないと見なされる必要があります。また、**service password-encryption** コマンドを使用後、コンフィギュレーション ファイルのどのような電子または文書でのコピーに対するアクセスも保護する必要があります。

パスワードがリモートデバイスに送信されるとき、**service password-encryption** コマンドではパスワードを暗号化しません。ネットワークに対するアクセス権があるネットワーク トラフィック アナライザを使用するユーザは、デバイス間でパケットを送信するときに、パケットからこのようなパスワードをキャプチャできます。コンフィギュレーション ファイルでのクリアテキストパスワードの暗号化の詳細については、「クリア テキスト パスワードのパスワード暗号化の設定 （2500 ページ）」を参照してください。

クリア テキスト パスワードを使用する Cisco IOS XE 機能の多くは、より安全な MD5 アルゴリズムを使用するように設定することもできます。MD5 アルゴリズムによって、暗号化がはるかに難しいコンフィギュレーション ファイル内でテキストストリングが作成されます。MD5 アルゴリズムは、リモートデバイスにパスワードを送信しません。これによって、トラフィック アナライザのユーザが、内部ネットワークのトラフィックをキャプチャしてパスワードを検出することを防ぎます。

ネットワーキング デバイスのコンフィギュレーション ファイルにパスワード文字列とともに保存されている数字によって、使用されているパスワード暗号化の種類を判断できます。下記のコンフィギュレーションの引用文での数字 5 は、イネーブル シークレット パスワードは MD5 アルゴリズムを使用して暗号化されていること示しています。

enable secret 5 1fGCS$rkYbR6.Z8xo4qCl3vghWQ0

下記の引用文での数字 7 は、**service password-encryption** コマンドによって使用された、より安全でないアルゴリズムを使用してイネーブルパスワードが暗号化されたことを示しています。

!

enable password 7 00081204

Cisco IOS XE CLI セッションのユーザ名

これらのパスワードを設定して、ユーザ EXEC モードおよび特権 EXEC モードへのアクセスを保護した後に、個々のユーザにネットワーク デバイスの CLI セッションへのアクセスを制限するためのユーザ名を設定することで、ネットワーク デバイスのセキュリティ レベルをさらに強化できます。

ネットワーキング デバイスの管理に使用するユーザ名は、次のような追加オプションを使用して変更できます。

『 *Cisco IOS Security Command Reference*』を参照してください。**username** コマンドの設定方法の詳細については、（http://www.cisco.com/en/US/docs/ios/security/command/reference/sec_book.html）を参照してください。

Cisco IOS XE の特権レベル

Cisco IOS XE ベースのネットワーク デバイスのデフォルト設定では、ユーザ EXEC モードに特権レベル 1 を、特権 EXEC に特権レベル 15 を使用します。特権レベル 1 のユーザ EXEC モードで実行できるコマンドは、特権レベル 15 の特権 EXEC モードで実行できるコマンドのサブセットです。

privilege コマンドは、1 つの特権レベルから別の特権レベルへコマンドを移動するのに使用されます。たとえば、一部の ISP では、窓口のテクニカル サポート スタッフに対して、新しい顧客の接続をアクティブ化するインターフェイスをイネーブルまたはディセーブルにする機能、およびトラフィックの送信を終了した接続を再起動する機能を許可しています。このオプションの設定方法の例については、例：ユーザがインターフェイスをシャットダウンおよびイネーブル化することを可能にするデバイスの設定 （2518 ページ）を参照してください。

privilege コマンドは、ユーザー名に特権レベルを割り当てるために使用できるため、ユーザーがこのユーザー名でログインすると、セッションは、**privilege** コマンドで指定された特権レベルで実行されます。たとえば、テクニカルサポートスタッフに対して、設定を変更することなくネットワークの問題を解決できるように、ネットワークデバイス設定を閲覧できるようにする場合、ユーザー名を作成し、特権レベル 15 を使用してユーザー名を設定し、**show running-config** コマンドを自動的に実行するように設定できます。ユーザがそのユーザ名でログインすると、実行コンフィギュレーションが自動的に表示されます。ユーザがコンフィギュレーションの最後の行を表示すると、ユーザのセッションは自動的にログアウトされます。このオプションの設定方法の例については、例：ユーザが実行コンフィギュレーションを表示可能にするデバイスの設定 （2517 ページ）を参照してください。

このようなコマンドの特権は、TACACS+ および RADIUS による AAA を使用するときにも実装できます。たとえば、TACACS+ には、ユーザ別またはグループ別にルータ コマンドの認可を制御する方法が 2 つあります。1 つ目の方法では、コマンドに特権レベルを割り当て、指定した特権レベルでユーザが認可されているかどうかについて、TACACS+ サーバを使用するルータで確認します。2 つ目の方法では、ユーザ別またはグループ別に、明示的に許可するコマンドを TACACS+ サーバに指定します。TACACS+ および RADIUS による AAA の実装の詳細については、『How to Assign Privilege Levels with TACACS+ and RADIUS』のテクニカル ノートを参照してください。

Cisco IOS XE のパスワード設定

Cisco IOS XE ソフトウェアでは、パスワードが意図したとおりに正確に入力されたことを確認するため、設定するパスワードの再入力を求めるプロンプトを採用していません。新しいパスワードおよび既存のパスワードへの変更は、パスワード コンフィギュレーション コマンド文字列の末尾に、Enter キーを入力すると、ただちに有効になります。新しいパスワードを入力し、ネットワーク デバイスのスタートアップ コンフィギュレーション ファイルに設定を保存し、特権 EXEC モードを出たときに間違えた場合、間違えたことを認識する前に、デバイスを管理できなくなっていることがわかる場合があります。

発生する可能性のある一般的な状況は次のとおりです。

- コンソール ポートでローカル CLI セッションのパスワード設定時に間違えます。
  - リモート CLI セッションでネットワーク デバイスに対するアクセスを適切に設定した場合、コンソール ポートで Telnet をして、パスワードを再設定できます。
- リモート Telnet または SSH セッションのパスワード設定時に間違えます。
  - ローカル CLI セッションでネットワーキング デバイスに対するアクセスを適切に設定した場合、端末に接続して、リモート CLI セッションのパスワードをリセットできます。
- 特権 EXEC モードでパスワード（イネーブル パスワードまたはイネーブル シークレット パスワード）を設定するときに誤入力しました。
  - 失われたパスワードの復元手順を実行する必要があります。
- ユーザ名パスワード設定するときに誤入力し、ネットワーキング デバイスからそのユーザ名を使用してログインするように求められました。
  - 別のアカウント名へのアクセス権を持っていない場合、失われたパスワード復元手順を実行する必要があります。

忘失パスワードの復元手順を実行する必要がないようにするには、ネットワーキング デバイスに対して 2 つの CLI セッションを開き、特権 EXEC モードでその一方を開いたままで、他のセッションを使用してパスワードをリセットします。2 つの CLI セッションまたは 2 種類のデバイスを実行するときに、同じデバイス（PC または端末）を使用できます。この手順には、ローカルの CLI セッションとリモート CLI セッションを使用するか、2 つのリモート CLI セッションを使用できます。パスワードの設定に使用する CLI セッションを、パスワードが適切に変更されたことを確認するために利用することもできます。最初の設定で誤入力した場合、特

権EXECモードで開いておいたもう一方のCLIセッションはパスワードを変更するときにも利用できます。

実行コンフィギュレーションで行ったパスワードの変更は、そのパスワードが適切に変更されたことを確認できるまで、スタートアップコンフィギュレーションに保存しないでください。パスワードの設定時に誤入力したことに気づき、上記のような第2のCLIセッションの手法を使用して問題を解決できなかった場合、スタートアップコンフィギュレーションに保存されている以前のパスワードに戻すように、ネットワーキング デバイスの電源を再投入します。

AES パスワード暗号化およびマスター暗号キー

強力で、反転可能な 128 ビットの高度暗号化規格（AES）パスワード暗号化（タイプ 6 暗号化ともいう）をイネーブルにすることができます。タイプ 6 暗号化の使用を開始するには、AES パスワード暗号化機能をイネーブルにし、パスワード暗号化および復号化に使用されるマスター暗号キーを設定する必要があります。AESパスワード暗号化を有効にしてマスターキーを設定すると、タイプ6パスワード暗号化を無効にしない限り、サポートされているアプリケーションの既存および新規作成されたクリアテキストパスワードがすべて、タイプ6暗号化の形式で保存されます。また、既存の弱いすべての暗号化パスワードをタイプ6暗号化パスワードに変換するようにデバイスを設定することもできます。

AESパスワード暗号化機能とマスター暗号キーが設定されている場合、タイプ0およびタイプ7 のパスワードはタイプ 6 に自動変換できます。

（注） タイプ 6 のユーザー名とパスワードには、Cisco IOS リリース 16.10.1 とのみ下位互換性があります。Cisco IOS リリース 16.10.1 より前のリリースバージョンにダウングレードすると、タイプ 6 のユーザー名とパスワードは拒否されます。自動変換後、管理者パスワードがダウングレード中に拒否されないようにするには、パスワードを移行します。

パスワード、特権、およびログインによるセキュリティの設定方法

ユーザ EXEC モードへのアクセスの保護

リモート CLI セッションのパスワードの設定と確認

このタスクを実行すると、リモートCLIセッションのパスワードが割り当てられます。このタスクを完了すると、この次にリモート CLI セッションを起動するときに、ネットワーク デバイスからパスワードの入力が求められます。

Cisco IOS XE ベースのネットワーク デバイスでは、リモート CLI セッション用に設定されたパスワードが必要になります。リモートCLIセッション用に設定されたパスワードがないデバ

イスでリモートCLIセッションを開始しようとすると、パスワードが必要で、設定されていないことを示すメッセージが表示されます。リモートCLIセッションは、リモートホストによって終了されます。

始める前に

以前にリモート CLI セッションのパスワードを設定していない場合、コンソール ポートに接続している端末、または端末エミュレーション アプリケーションを実行する PC を使用して、ローカル CLI セッションでこのタスクを実行する必要があります。

ネットワーキング デバイス上のコンソール ポートに使用される設定によって、端末、または端末エミュレーションアプリケーションを設定する必要があります。ほとんどのシスコのネットワーク デバイスのコンソール ポートには、次の設定が必要です。9600 ボー、8 データ ビット、1 ストップ ビット、パリティなし、およびフロー制御は"none"に設定します。これらの設定が端末で機能しない場合は、ネットワーク デバイスのマニュアルを参照してください。

このタスクの確認手順（手順6）を実行するには、ネットワーキングデバイスに、動作状態のインターフェイスが必要です。インターフェイスは有効な IP アドレスを持っている必要があります。

（注） 以前にリモート CLI セッションのパスワードを設定していない場合、コンソール ポートに接続している端末を使用して、ローカル CLI セッションでこのタスクを実行する必要があります。

手順の概要

1. **enable**
2. **configure terminal**
3. **line vty** *line-number* [*ending-line-number*]
4. **password** *password*
5. **end**
6. **telnet** *ip-address*
7. **exit**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例：	グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
	`Device# configure terminal`	
ステップ 3	**line vty** *line-number* [*ending-line-number*] 例： `Device(config)# line vty 0 4`	ライン コンフィギュレーション モードを開始します。
ステップ 4	**password** *password* 例： `Device(config-line)# password H7x3U8`	引数 *password* は、ライン パスワードを指定する文字列です。次の規則が *password* 引数に適用されます。 • 最初の文字を数値にはできません。 • ストリングには、80 文字以下の任意の英数字（スペースを含む）を指定できます。数字-スペース-任意の文字の形式ではパスワードを指定できません。 • パスワードは大文字と小文字が区別されます。
ステップ 5	**end** 例： `Device(config-line)# end`	現在のコンフィギュレーションモードを終了し、特権 EXEC モードに戻ります。
ステップ 6	**telnet** *ip-address* 例： `Device# telnet 172.16.1.1`	動作状態（インターフェイスがアップ、ラインプロトコルがアップ）のネットワーキングデバイスで、インターフェイスの IP アドレスを使用して、現在の CLI セッションからネットワーキング デバイスとのリモート CLI セッションを開始します。 • プロンプトが表示されたら、手順 4 で設定したパスワードを入力します。 （注） この手順は、ネットワーキング デバイス自体からネットワーキング デバイスへのリモート Telnet セッションを開始するため、再帰的 Telnet セッションの開始とも呼ばれます。
ステップ 7	**exit** 例： `Device# exit`	ネットワーキング デバイスとのリモート CLI セッション（再帰的 Telnet セッション）を終了します。

トラブルシューティングのヒント

合法的傍受ビューにアクセス可能なすべてのユーザーに関する情報を表示するには、**show users lawful-intercept** コマンドを発行します（このコマンドは、認可された合法的傍受ビュー ユーザしか使用できません）。

次の作業

ローカル CLI セッションのパスワードの設定と確認 （2496 ページ）に進みます。

ローカル CLI セッションのパスワードの設定と確認

このタスクを実行すると、コンソール ポートでのローカル CLI セッション用のパスワードが割り当てられます。このタスクを完了した後に、コンソール ポートでローカル CLI セッションを起動すると、ネットワーキング デバイスからパスワードの入力が求められます。

このタスクは、コンソールポートを使用するローカルCLIセッションまたはリモートCLIセッションで実行できます。パスワードを適切に設定したことを確認するオプションの手順を実行する場合、コンソール ポートでローカル CLI セッションを使用して、このタスクを実行する必要があります。

始める前に

ローカル CLI セッション パスワードを確認するオプションの手順を実行する場合、ローカル CLIセッションを使用してこのタスクを実行する必要があります。ネットワーク デバイスのコンソール ポートに、端末または端末エミュレーション プログラムが稼働している PC を接続する必要があります。ネットワーキング デバイス上のコンソール ポートに使用される設定によって、端末を設定する必要があります。ほとんどのシスコのネットワーク デバイスのコンソール ポートには、次の設定が必要です。9600 ボー、8 データ ビット、1 ストップ ビット、パリティなし、およびフロー制御は "none" に設定します。これらの設定が端末で機能しない場合は、ネットワーク デバイスのマニュアルを参照してください。

手順の概要

1. **enable**
2. **configure terminal**
3. **line console 0**
4. **password** *password*
5. **end**
6. **exit**
7. Enter キーを押します。

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例：	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。

	コマンドまたはアクション	目的
	`Device> enable`	
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**line console 0** 例： `Device(config)# line console 0`	ライン コンフィギュレーション モードを開始し、設定しているラインとしてコンソール ポートを選択します。
ステップ 4	**password** *password* 例： `Device(config-line)# password Ji8F5Z`	引数 *password* は、ライン パスワードを指定する文字列です。次の規則が *password* 引数に適用されます。 • 最初の文字を数値にはできません。 • ストリングには、80 文字以下の任意の英数字（スペースを含む）を指定できます。数字-スペース-任意の文字の形式ではパスワードを指定できません。 • パスワードは大文字と小文字が区別されます。
ステップ 5	**end** 例： `Device(config-line)# end`	現在のコンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。
ステップ 6	**exit** 例： `Device# exit`	特権 EXEC モードを終了します。
ステップ 7	Enter キーを押します。	（任意）コンソール ポートでローカル CLI セッションを開始します。 • プロンプトが表示されたら、ステップ 4 で設定したパスワードを入力して、適切に設定されたことを確認します。 （注） この手順を実行できるのは、このタスクの実行にローカル CLI セッションを使用している場合だけです。

トラブルシューティングのヒント

新しいパスワードを受け入れられなかったら次に何をするのかについては、パスワード、特権、およびログインによるセキュリティ設定の設定例に進みます。

次の作業

特権 EXEC モードへのアクセスの保護 （2498 ページ）に進みます。

特権 EXEC モードへのアクセスの保護

イネーブル パスワードの設定と確認

シスコは特権 EXEC モードのパスワード設定に **enable password** コマンドを使用することを推奨しなくなりました。**enable password** コマンドを使用して入力したパスワードは、ネットワークデバイスのコンフィギュレーションファイルにプレーンテキストとして保存されます。ネットワークデバイスのコンフィギュレーション ファイルに含まれる **enable password** コマンドのパスワードを暗号化するには、**service password-encryption** コマンドを使用します。ただし、**service password-encryption** コマンドで使用される暗号化レベルは、インターネットで入手できるツールを使用して復号できます。

シスコでは、**enable password** コマンドを使用する代わりに、**enable secret** コマンドを使用することを推奨します。設定したパスワードが、強力な暗号化方式で暗号化されるためです。パスワード暗号化問題の詳細については、Cisco IOS XE のパスワード暗号化レベル （2489 ページ）を参照してください。**enable secret** コマンドの設定については、イネーブル シークレット パスワードの設定と確認 （2501 ページ）を参照してください。

（注） このタスクを正常に実行するため、ネットワークデバイスでは、**enable secret** コマンドを使用してパスワードを設定しないでください。**enable secret** コマンドを使用して特権 EXEC モードのパスワードを既に設定している場合、設定されたパスワードは、このタスクで**enable password** コマンドを使用して設定するパスワードより優先されます。

enable secret コマンドと **enable** *password* コマンドに同じパスワードを使用することはできません。

手順の概要

1. **enable**
2. **configure terminal**
3. **enable password** *password*
4. **end**
5. **exit**
6. **enable**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。

ステップ 3	**enable password** *password*
	例：
	`Device(config)# enable password t6D77CdKq`
		引数 *password* は、イネーブル パスワードを指定する文字列です。次の規則が *password* 引数に適用されます。
		• 1 ～ 25 文字の大文字と小文字の英数字を含める必要があります。
		• 先頭の文字に数字は指定できません。
		• 先頭にスペースを指定できますが、無視されます。ただし、中間および末尾のスペースは認識されます。
		• パスワードを作成するときに、Ctrl+v キーの組み合わせを押してから疑問符（?）を入力すると、パスワードに疑問符を含めることができます。たとえば、abc?123 というパスワードを作成するには、次の手順を実行します。
		  • abc と入力します。
		  • Crtl-v キーを押します。
		  • ?123 と入力します。

ステップ 4	**end** 例： `Device(config)# end`	現在のコンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。
ステップ 5	**exit** 例： `Device# exit`	特権 EXEC モードを終了します。
ステップ 6	**enable** 例：	特権 EXEC モードをイネーブルにします。 • 手順 3 で設定したパスワードを入力します。

	コマンドまたはアクション	目的
	`Device> enable`	

トラブルシューティングのヒント

新しいパスワードを受け入れられなかったら、次に何をするのかについては、特権EXECモードの忘失パスワードまたは誤設定パスワードの復元セクションに進みます。

次の作業

クリアテキストパスワードのパスワード暗号化の設定（2500ページ）で説明した手順を使用して、ネットワーキング デバイスのコンフィギュレーション ファイルにクリア テキストで保存されているイネーブル パスワードを暗号化します。

クリア テキスト パスワードのパスワード暗号化の設定

Cisco IOS XEは、一部の機能について、ネットワーク デバイスのコンフィギュレーション ファイルにクリアテキストでパスワードを保存します。たとえば、ローカルおよびリモートのCLIセッションのパスワード、およびルーティングプロトコルのネイバー認証のパスワードなどです。コンフィギュレーション ファイルのアーカイブ コピーにアクセスできれば、誰でもクリア テキストで保存されているパスワードを発見できるため、クリア テキスト パスワードはセキュリティ リスクです。**service password-encryption** コマンドを使用して、ネットワークデバイスのコンフィギュレーション ファイルに含まれるクリアテキストコマンドを暗号化できます。詳細については、Cisco IOS XEのパスワード暗号化レベル（2489ページ）を参照してください。

ネットワーキング デバイスのコンフィギュレーション ファイルにクリア テキストとして保存されているパスワードについて、パスワード暗号化を設定するには、次の手順を実行します。

始める前に

このコマンドの結果を即時に確認するために、クリア テキスト パスワードを使用する機能が1つ以上、ネットワーキング デバイスに設定されている必要があります。

手順の概要

1. **enable**
2. **configure terminal**
3. **service password-encryption**
4. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ1	**enable** 例：	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。

	コマンドまたはアクション	目的
	`Device> enable`	
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**service password-encryption** 例： `Device(config)# service password-encryption`	すべてのクリア テキスト パスワード（ユーザ名パスワード、認証キー パスワード、特権コマンド パスワード、コンソールおよび仮想端末ライン アクセス パスワード、および Border Gateway Protocol ネイバーパスワード）について、パスワード暗号化をイネーブルにします。
ステップ 4	**end** 例： `Device(config)# end`	現在のコンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

イネーブル シークレット パスワードの設定と確認

シスコは、**enablenable** *password* コマンドの代わりに **enable secret** コマンドを使用して特権 EXEC モードのパスワードを設定することを推奨しています。**enable secret** コマンドで作成されたパスワードは、より安全な MD5 アルゴリズムで暗号化されます。

（注） **enable secret** コマンドと **enable** *password* コマンドに同じパスワードを使用することはできません。

手順の概要

1. **enable**
2. **configure terminal**
3. 次のいずれかの手順を実行します。
   - **enable secret** *password*
   - **enable secret 5** *previously-encrypted-password*
4. **end**
5. **exit**
6. **enable**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。

ステップ 3	次のいずれかの手順を実行します。
	• **enable secret** *password*
	• **enable secret 5** *previously-encrypted-password*
	例：
	`Device(config)# enable secret t6D77CdKq`
	例：
	`Device(config)# enable secret 5 $1$/x6H$RhnDI3yLC4GA01aJnHLQ4/`
		引数 *password* は、**enable secret** パスワードを指定する文字列です。次の規則が *password* 引数に適用されます。
		• 1 ～ 25 文字の大文字と小文字の英数字を含める必要があります。
		• 先頭の文字に数字は指定できません。
		• 先頭にスペースを指定できますが、無視されます。ただし、中間および末尾のスペースは認識されます。
		• パスワードを作成するときに、Ctrl+v キーの組み合わせを押してから疑問符（?）を入力すると、パスワードに疑問符を含めることができます。たとえば、abc?123 というパスワードを作成するには、次の手順を実行します。
		  • abc と入力します。
		  • Crtl-v キーを押します。
		  • ?123 と入力します。
		または
		前に暗号化した文字列の前に数字 5 を入力することで、以前に暗号化した特権 EXEC モードのパスワードを設定します。この方式を使用するには、**enable secret** コマンドによって以前に暗号化されたコンフィギュレーション ファイルから、パスワードの正確なコピーを入力する必要があります。

ステップ 4	**end** 例：	現在のコンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

	コマンドまたはアクション	目的
	`Device(config)# end`	
ステップ 5	**exit** 例： `Device# exit`	特権 EXEC モードを終了します。
ステップ 6	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • 手順 3 で設定したパスワードを入力します。

トラブルシューティングのヒント

新しいパスワードを受け入れられなかったら次に何をするのかについては、パスワード、特権、およびログインによるセキュリティ設定の設定例に進みます。

次の作業

ローカルおよびリモートのCLIセッションのパスワードを設定し終わり、ユーザ名や特権レベルなど、追加のセキュリティ機能を設定する場合、CLIセッションとコマンドへのアクセスを管理するセキュリティ オプションの設定 （2505 ページ）に進みます。

ユーザが実行コンフィギュレーションを表示可能にするデバイスの設定

レベル 15 より低い特権レベルで **show running-config** コマンドを使用してデバイスの実行コンフィギュレーションにアクセスするには、次の作業を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **privilege exec all level** *level command-string*
4. **file privilege** *level*
5. **privilege configure all level** *level command-string*
6. **end**
7. **show privilege**
8. **show running-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例：	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。

	コマンドまたはアクション	目的
	`Device> enable`	
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**privilege exec all level** *level command-string* 例： `Device(config)# privilege exec all level 5 show running-config`	指定されたコマンドの特権レベルを、1 つの権限レベルから別の特権レベルに変更します。
ステップ 4	**file privilege** *level* 例： `Device(config)# file privilege 5`	特権レベルのユーザが、ファイル システムを含むコマンドをデバイスで実行できるようにします。
ステップ 5	**privilege configure all level** *level command-string* 例： `Device(config)# privilege configure all level 5 logging`	特権レベルのユーザが、特定のコンフィギュレーション コマンドを表示できるようにします。たとえば、特権レベル 5 のユーザが、実行コンフィギュレーションでロギング コンフィギュレーション コマンドを表示できるようにします。
ステップ 6	**end** 例： `Device(config)# end`	グローバル コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。
ステップ 7	**show privilege** 例： `Device# show privilege`	現在の特権レベルを表示します。
ステップ 8	**show running-config** 例： `Device# show running-config`	指定された特権レベルの現在の実行コンフィギュレーションを表示します。

例

show running-config コマンドの次の出力は、実行コンフィギュレーションのロギング コンフィギュレーション コマンドを表示します。15 未満の特権レベルを持つユーザーは、**privilege configure all level** *level command-string* コマンドを設定した後、実行コンフィギュレーションを表示できます。

```
Device# show running-config

Building configuration...

Current configuration : 128 bytes
!
boot-start-marker
boot-end-marker
!
no logging queue-limit
logging buffered 10000000
no logging rate-limit
!
!
!
end
```

CLI セッションとコマンドへのアクセスを管理するセキュリティ オプションの設定

ここでは、特権EXECモードで使用できる全コマンドに対してはアクセス権が持たないユーザが、特権 EXEC モード コマンドのサブセットを使用できるように、ネットワーキング デバイスを設定するタスクについて説明します。

このようなタスクは、複数レベルのネットワーク サポート スタッフがいて、各レベルのスタッフに、異なるサブセットの特権 EXEC モード コマンドに対するアクセス権を付与したい会社に役立ちます。

このタスクでは、特権EXECモードで使用できる全コマンドに対してはアクセス権を持たないユーザは、窓口のテクニカル サポート スタッフと呼びます。

ここでは、次の手順について説明します。

窓口のテクニカル サポート スタッフ用のネットワーク デバイスの設定

このタスクでは、窓口のテクニカル サポート スタッフ ユーザ用にネットワーキング デバイスを設定する方法について説明します。通常、窓口のテクニカル サポート スタッフは、ネットワーキング デバイスの特権 EXEC モードで（特権レベル 15）使用できる全コマンドの実行は許可されていません。また、特権EXECモードに割り当てられているパスワード、またはネットワーキング デバイスに設定されている他の役割に対してアクセス権が付与されていないため、権限がないコマンドを実行できません。

privilege コマンドは、ある特権レベルのコマンドを別の特権レベルに移動するために使用されます。この操作で、ネットワークデバイスに追加レベルの管理が作成されます。このような操作は、さまざまなスキルレベルを持つ、さまざまなレベルのネットワーク サポート スタッフがいる会社の場合に必要です。

Cisco IOS XE デバイスのデフォルトの設定では、2 種類のユーザが CLI にアクセスできます。1つ目のユーザは、ユーザEXECモードだけにアクセスできるユーザです。2つ目のユーザは、特権EXECモードにアクセスできるユーザです。ユーザEXECモードへのアクセスが許可され

ているだけのユーザは、ネットワーク デバイスの設定を表示または変更したり、ネットワーク デバイスの稼働状態を変更することはできません。一方、特権EXECモードにアクセスできるユーザは、CLI に許可されているネットワーキング デバイスを変更できます。

この作業では、通常特権レベル 15 で動作する 2 つのコマンドは、特権コマンドを使用して特権レベル 7 にリセットされます。窓口のテクニカル サポート スタッフ ユーザが 2 つのコマンドを実行できるようにするためです。特権レベルをリセットする 2 つのコマンドは、**clear counters** コマンドと **reload** コマンドです。

- **clear counters** コマンドは、受信されたパケット、送信されたパケット、およびエラーなどの統計情報のために、インターフェイスのカウンタフィールドをリセットするために使用されます。窓口のテクニカル サポート スタッフ ユーザがネットワーク デバイス間で、またはネットワークに接続しているリモートユーザとの間で、インターフェイスに関する接続の問題を解決しているときに、インターフェイスの統計情報をゼロにリセットしたり、インターフェイスの統計情報カウンタの値が変化するかを見るため、一定の時間インターフェイスを監視するのに役立ちます。

- **reload** コマンドは、ネットワークデバイスのリブートシーケンスを開始するのに使用します。窓口のテクニカル サポート スタッフによる一般的な reload コマンドの使用方法の 1 つは、メンテナンス ウィンドウでネットワーク デバイスをリブートすることです。この操作によって、高い権限レベルのユーザが以前にネットワーク デバイスのファイル システムにコピーした新しいオペレーティング システムがロードされます。

窓口のテクニカル サポート ユーザー ロールの特権レベルに割り当てられている **enable secret** パスワードを知る権限を持つユーザーは、窓口のテクニカルサポートユーザーとしてそのネットワークデバイスにアクセスできます。ネットワーク デバイスのユーザ名を設定し、ユーザによるユーザ名とパスワードの把握を必須にして、新たなセキュリティ レベルを追加できます。追加レベルのセキュリティとしてユーザ名を設定する方法については、「」を参照してください。窓口のテクニカル サポート スタッフのユーザ名を必須にするデバイスの設定（2510 ページ）

（注） ネットワークデバイスでは、**aaa new-model** コマンドをイネーブルにしないでください。コンソールポートでのローカル CLI セッションの場合、またはリモート CLI セッションの場合、**login local** コマンドを設定しないでください。

（注） このタスクの手順では、わかりやすくするために、各手順に関係する構文に使用しています。これらのコマンドと併用できるその他の引数いては、お使いの Cisco IOS リリースの Cisco IOS コマンド リファレてください。

注意 コマンドの特権レベルをデフォルトにリセットする場合、**privilege** コしないでください。コンフィギュレーションが適切なデフォルト状態ます。コマンドをデフォルトの特権レベルに戻すには、**privilege** コマを使用します。たとえば、コンフィギュレーションから **privilege exe** 削除し、**reload** コマンドをデフォルトの特権レベル 15 に戻すには、コマンドを使用します。

手順の概要

1. **enable**
2. **configure terminal**
3. **enable secret level** *level password*
4. **privilege exec level** *level command-string*
5. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを開始します。プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**enable secret level** *level password* 例：	特権レベル 7 の新しいイネーブル シークレット パスワードを設定します。

	コマンドまたはアクション	目的
	`Device(config)# enable secret level 7 Zy72sKj`	
ステップ 4	**privilege exec level** *level command-string* 例： `Device(config)# privilege exec level 7 clear counters`	**clear counters** コマンドの特権レベルを、特権レベル 15 から特権レベル 7 に変更します。
ステップ 5	**end** 例： `Device(config)# end`	グローバル コンフィギュレーション モードを終了します。

窓口のテクニカル サポート スタッフ用の設定の確認

ここでは、ネットワーキング デバイスが窓口のテクニカル サポート スタッフ用に適切に設定されていることを確認するタスクについて説明します。

始める前に

次のコマンドは、このタスクのために特権レベル 7 で実行するように変更済みです。

- **clear counters**
- **reload**

手順の概要

1. **enable** *level password*
2. **show privilege**
3. **clear counters**
4. **clear ip route** *
5. **reload in time**
6. **reload cancel**
7. **disable**
8. **show privilege**

手順の詳細

ステップ 1 **enable** *level password*

level 引数に指定した特権レベルで、ネットワーキング デバイスにログインします。

例：

```
Device> enable 7 Zy72sKj
```

ステップ 2 show privilege

現在の CLI セッションの特権レベルを表示します。

例：

```
Device# show privilege

Current privilege level is 7
```

ステップ 3 clear counters

clear counters コマンドは、インターフェイスのカウンタをクリアします。このコマンドは、特権レベル 15 から特権レベル 7 に変更されました。

例：

```
Device# clear counters

Clear "show interface" counters on all interfaces [confirm]
Device#
02:41:37: %CLEAR-5-COUNTERS: Clear counter on all interfaces by console
```

ステップ 4 clear ip route *

clear コマンドの *ip route* 引数文字列は、特権レベル 15 から特権レベル 7 に変更されていないため、使用できません。

例：

```
Device# clear ip route *
                                                                  ^
% Invalid input detected at '^' marker.
```

ステップ 5 reload in time

reload コマンドによって、ネットワーキング デバイスはリブートされます。

例：

```
Device# reload in

10
Reload scheduled in 10 minutes by console
Proceed with reload? [confirm]

Device#

***
*** --- SHUTDOWN in 0:10:00 ---
***
02:59:50: %SYS-5-SCHEDULED_RELOAD: Reload requested for 23:08:30 PST Sun Mar 20
```

ステップ 6 reload cancel

reload cancel によって、以前に **reload in** *time* コマンドで設定したリロードが終了します。

例：

```
Device# reload cancel

***
*** --- SHUTDOWN ABORTED ---
***
04:34:08: %SYS-5-SCHEDULED_RELOAD_CANCELLED:  Scheduled reload cancelled at 15:38:46 PST Sun Mar 27
 2005
```

ステップ 7 disable

現在の特権レベルを終了し、特権レベル 1 に戻します。

例：

```
Device# disable
```

ステップ 8 show privilege

現在の CLI セッションの特権レベルを表示します。

例：

```
Device> show privilege

Current privilege level is 1
```

トラブルシューティングのヒント

設定が希望どおりに機能しないため、設定から privilege コマンドを削除する場合、コマンドをデフォルトの特権レベルに戻すには、**privilege** コマンドに **reset** キーワードを使用します。たとえば、コンフィギュレーションから **privilege exec level** *reload* コマンドを削除し、**reload** コマンドをデフォルトの特権レベル 15 に戻すには、**privilege exec reset** *reload* コマンドを使用します。

次の作業

窓口のテクニカルサポートスタッフがログイン名を使用することを必須にして、セキュリティレベルを追加する場合、窓口のテクニカル サポート スタッフのユーザ名を必須にするデバイスの設定 （2510 ページ）に進みます。

窓口のテクニカル サポート スタッフのユーザ名を必須にするデバイスの設定

このタスクでは、窓口のテクニカルサポートスタッフが、admin のログイン名を使用してネットワーキング デバイスにログインすることを必須にするように、ネットワーキング デバイスを設定します。このタスクで設定された admin ユーザ名には、特権レベル 7 が割り当てられています。この名前を使用してログインするユーザは、前のタスクで特権レベル 7 に再割り当て

されたコマンドを実行できます。ユーザがユーザ名 admin で正常にログインすると、CLI セッションは自動的に特権レベル 7 に入ります。

Cisco IOS XE リリース 2.3 よりも前のリリースでは、2 種類のパスワードがユーザー名に関連付けられていました。タイプ 0 は、ルータの特権モードにアクセスできるすべてのユーザーから確認できるクリアテキストパスワードです。また、タイプ 7 は、**service password encryption** コマンドで暗号化されたパスワードです。

Cisco IOS XE リリース 2.3 以降のリリースでは、**username** コマンドに新しい **secret** キーワードを使用することで、ユーザー名のパスワードに Message Digest 5（MD5）暗号化を設定できます。

始める前に

次のコマンドは、このタスクのために特権レベル 7 で実行するように変更済みです。

- **clear counters**
- **reload**

コマンドの特権レベルを変更する手順については、窓口のテクニカル サポート スタッフ用のネットワーク デバイスの設定 （2505 ページ）を参照してください。

（注） **username** コマンドの MD5 暗号化は、Cisco IOS XE リリース 2.3 よりも前の Cisco IOS ソフトウェアバージョンではサポートされません。

ネットワーキング デバイスでは、aaa-new model コマンドをイネーブルにしないでください。コンソールポートでのローカル CLI セッションの場合、またはリモート CLI セッションの場合、**login local** コマンドを設定しないでください。

（注） このタスクの手順では、わかりやすくするために、各手順に関係する
構文に使用しています。これらのコマンドと併用できるその他の引数
いては、お使いの Cisco IOS XE リリースの Cisco IOS コマンド リファ
照してください。

手順の概要

1. **enable**
2. **configure terminal**
3. **username** *username* **privilege** *level* **secret** *password*
4. **end**
5. **disable**
6. **login** *username*
7. **show privilege**
8. **clear counters**

9. **clear** *ip route* *
10. **reload in** *time*
11. **reload cancel**
12. **disable**
13. **show privilege**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを開始します。プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**username** *username* **privilege** *level* **secret** *password* 例： `Device(config)# username admin privilege 7 secret Kd65xZa`	ユーザ名を作成し、*password* テキスト ストリングに MD5 暗号化を適用します。
ステップ 4	**end** 例： `Device(config)# end`	グローバル コンフィギュレーション モードを終了します。
ステップ 5	**disable** 例： `Device# disable`	現在の特権レベルを終了し、ユーザ EXEC モードに戻します。
ステップ 6	**login** *username* 例： `Device> login admin`	ユーザにログインします。プロンプトが表示されたら、手順3で設定したユーザ名とパスワードを入力します。

ステップ 7	**show privilege**
	例：
	`Device# show privilege`
	`Current privilege level is 7`
		show privilege コマンドで、CLI セッションの特権レベルが表示されます。

	コマンドまたはアクション	目的

ステップ 8	**clear counters**
	例：
	`Device# clear counters`
	`Clear "show interface" counters on all interfaces [confirm]`
	`Device#`
	`02:41:37: %CLEAR-5-COUNTERS: Clear counter on all interfaces by console`
		clear counters コマンドでインターフェイスカウンタがクリアされます。このコマンドは、特権レベル 15 から特権レベル 7 に変更されました。

ステップ 9	**clear** *ip route* *
	例：
	`Device# clear ip route *`
	`^`
	`% Invalid input detected at '^' marker.`
		clear コマンドの *ip route* 引数文字列は、特権レベル 15 から特権レベル 7 に変更されていないため、使用できません。

ステップ 10	**reload in** *time*
	例：
	`Device# reload in`
	`10`
	`Reload scheduled in 10 minutes by console`
	`Proceed with reload? [confirm]`
	`Device#`
	`***`
	`*** --- SHUTDOWN in 0:10:00 ---`
	`***`
	`02:59:50: %SYS-5-SCHEDULED_RELOAD: Reload requested for 23:08:30 PST Sun Mar 20`
		reload コマンドによって、ネットワーキングデバイスはリブートされます。

ステップ 11	**reload cancel**
	例：
	`Device# reload cancel`
	`***`
	`*** --- SHUTDOWN ABORTED ---`
	`***`
	`04:34:08: %SYS-5-SCHEDULED_RELOAD_CANCELLED: Scheduled reload cancelled at 15:38:46 PST Sun Mar 27 2005`
		reload cancel コマンドによって、以前に **reload in** *time* コマンドで設定したリロードが終了します。

ステップ 12	**disable** 例： `Device# disable`	現在の特権レベルを終了し、ユーザ EXEC モードに戻します。

	コマンドまたはアクション	目的

ステップ 13	**show privilege**
	例：
	`Device> show privilege`
	`Current privilege level is 1`
		現在のCLIセッションの特権レベルを表示します。

ローカルセッションの忘失パスワードおよび誤設定パスワードの復元

コンソール ポートでローカル CLI セッションの忘失パスワードおよび誤設定パスワードを復元するために使用できる方式は3つあります。使用する方式は、ネットワーキングデバイスの現在の設定によって変わります。

ネットワーク デバイスがリモート CLI セッションを許可するように設定されている

ローカルCLIセッションの忘失パスワードまたは誤設定パスワードを復元する最速の方式は、ネットワーキング デバイスとリモート CLI セッションを確立し、ローカル CLI セッションのパスワードの設定と確認（2496ページ）を繰り返す方法です。この手順を実行するには、リモートCLIセッションを許可するようにネットワーキングデバイスを設定し、さらにリモートCLIセッションのパスワードを知っている必要があります。

ネットワーク デバイスがリモート CLI セッションを許可するように設定されていない

- ネットワーキング デバイスに対するリモート セッションを確立できず、誤設定したローカル CLI セッション パスワードをスタートアップ コンフィギュレーションに保存していない場合、ネットワーキング デバイスを再起動できます。ネットワーキング デバイスを再起動すると、スタートアップ コンフィギュレーション ファイルが読み込まれます。以前のローカル CLI セッション パスワードが復元されます。

注意 ネットワーキング デバイスの再起動によって、トラフィックの転送が停止されます。また、DHCP サーバ サービスなど、ネットワーキング デバイスで実行されているすべてのサービスが中断されます。必要な操作は、ネットワークのメンテナンスに割り当てられた期間中に、ネットワーキング デバイスを再起動することだけです。

リモートセッションの忘失パスワードおよび誤設定パスワードの復元

忘失または誤設定したリモート CLI セッション パスワードから復元するために使用できる方式は3つあります。使用する方式は、ネットワーキングデバイスの現在の設定によって変わります。

ネットワーク デバイスがローカル CLI セッションを許可するように設定されている

リモート CLI セッションの忘失パスワードまたは誤設定パスワードを復元する最速の方式は、ネットワーキング デバイスとローカル CLI セッションを確立し、リモート CLI セッションのパスワードの設定と確認（2493 ページ）を繰り返す方法です。この手順を実行するには、ローカル CLI セッションを許可するようにネットワーキング デバイスを設定し、さらにローカル CLI セッションのパスワードを知っている必要があります。

ネットワーク デバイスがローカル CLI セッションを許可するように設定されていない

- ネットワーキング デバイスに対するローカル CLI セッションを確立できず、誤設定したリモート CLI セッション パスワードをスタートアップ コンフィギュレーションに保存していない場合、ネットワーキング デバイスを再起動できます。ネットワーキング デバイスを再起動すると、スタートアップ コンフィギュレーション ファイルが読み込まれます。以前のリモート CLI セッション パスワードが復元されます。

⚠

注意 ネットワーキング デバイスの再起動によって、トラフィックの転送が停止されます。また、DHCP サーバ サービスなど、ネットワーキング デバイスで実行されているすべてのサービスが中断されます。必要な操作は、ネットワークのメンテナンスに割り当てられた期間中に、ネットワーキング デバイスを再起動することだけです。

特権 EXEC モードの忘失パスワードまたは誤設定パスワードの復元

忘失または誤設定した特権 EXEC モード パスワードから復元するために使用できる方式は 2 つあります。使用する方式は、ネットワーキング デバイスの現在の設定によって変わります。

誤設定された特権 EXEC モードのパスワードが保存されていない

- 誤設定した特権 EXEC モード パスワードをスタートアップ コンフィギュレーションに保存していない場合、ネットワーキング デバイスを再起動できます。ネットワーキング デバイスを再起動すると、スタートアップ コンフィギュレーション ファイルが読み込まれます。以前の特権 EXEC モード パスワードが復元されます。

⚠

注意 ネットワーキング デバイスの再起動によって、トラフィックの転送が停止されます。また、DHCP サーバ サービスなど、ネットワーキング デバイスで実行されているすべてのサービスが中断されます。必要な操作は、ネットワークのメンテナンスに割り当てられた期間中に、ネットワーキング デバイスを再起動することだけです。

パスワード、特権、およびログインによるセキュリティ設定の設定例

例：暗号化事前共有キーの設定

次に示すのは、タイプ6の事前共有キーが暗号化された場合の設定例です。この中には、ユーザに対して表示されるプロンプトやメッセージも含まれています。

```
Device(config)# password encryption aes
New key:
Confirm key:
Device (config)#

01:46:40: TYPE6_PASS: New Master key configured, encrypting the keys with
the new master key
Device (config)# exit
```

例：ユーザがリモートセッションをクリア可能にするデバイスの設定

次に、管理者以外のユーザがリモートCLIセッションの仮想端末（VTY）回線をクリアできるように、ネットワーキング デバイスを設定する例を示します。

最初の項は、この例の実行コンフィギュレーションの抜粋です。ここでは、この例を使用する方法を示します。

次の項は、実行コンフィギュレーションの抜粋です。

```
!
privilege exec level 7 clear line
!
no aaa new-model
!
!
username admin privilege 7 secret 5 $1$tmIw$1aM7sadKhWMpkVTzxNw1J.
!
privilege exec level 7 clear line
!
! the privilege exec level 7 clear command below is entered automatically
! when you enter the privilege exec level 7 clear line command above, do
! not enter it again
!
privilege exec level 7 clear
!
```

次の項では、**login**コマンドを使用して、ユーザーがadminのユーザー名を使用してネットワークデバイスにログインする場合を示します。

```
R1> login
Username: admin
Password:
```

次の項では、**show privilege** コマンドを使用して、現在の特権レベルが 7 であることを示します。

```
R1# show privilege

Current privilege level is 7
R1#
```

次の項では、**show user** コマンドを使用して、現在、2 ユーザー（admin と root）がネットワークデバイスにログインしていることを示します。

```
R1# show user

    Line       User       Host(s)              Idle       Location
*  0 con 0     admin      idle                 00:00:00
   2 vty 0     root       idle                 00:00:17 172.16.6.2
  Interface    User               Mode         Idle     Peer Address
```

次の項では、**clear line** *2* コマンドを使用して、ユーザー名 root に使用されているリモート CLI セッションを終了します。

```
R1# clear line  2

[confirm]
 [OK]
```

次の項では、**show user** コマンドを使用して、ネットワークデバイスに現在ログインしているユーザーは admin だけであることを示します。

```
R1# show user
    Line       User       Host(s)              Idle       Location
*  0 con 0     admin      idle                 00:00:00
  Interface    User               Mode         Idle     Peer Address
```

例：ユーザが実行コンフィギュレーションを表示可能にするデバイスの設定

特権レベル 15 を持つユーザ

次に、管理者以外のユーザ（特権EXECモードへのアクセスなし）が、実行コンフィギュレーションを自動的に表示できるようにネットワーキングデバイスを設定する例を示します。この例では、ユーザ名を特権レベル 15 に設定する必要があります。コンフィギュレーション ファイルの多くのコマンドは、特権レベル 15 へのアクセス権を持つユーザだけが表示できるためです。

この点を解決するには、**show running-config** コマンドの実行中、一時的に特権レベル 15 へのユーザーアクセスを許可し、コンフィギュレーションファイルの表示後に、CLIセッションを終了します。この例では、設定ファイルの表示後に、ネットワーキング デバイスが CLI セッションを自動的に終了します。その他の設定手順は必要ありません。

注意 **username** コマンドに **noescape** キーワードを含める必要があります。これは、コンフィギュレーション ファイルの表示を終了し、特権レベル 15 で実行するセッションを終了するエスケープ文字をユーザーが入力しないようにするためです。

```
!
!
username viewconf privilege 15 noescape secret 5 $1$zA9C$TDWD/Q0zwp/5xRwRqdgc/.
username viewconf autocommand show running-config
!
```

レベル 15 より低い特権レベルを持つユーザ

次の例は、レベル 15 より低い特権レベルを持つユーザが、実行コンフィギュレーションを表示可能にするネットワーク デバイスの設定方法を示しています。

```
Device> enable
Device# configure terminal
Device(config)# privilege exec all level 5 show running-config
Device(config)# file privilege 5
Device(config)# privilege configure all level 5 logging
Device(config)# end
Device# show privilege

Current privilege level is 5

Device# show running-config

Building configuration...

Current configuration : 128 bytes
!
boot-start-marker
boot-end-marker
!
no logging queue-limit
logging buffered 10000000
no logging rate-limit
!
!
!
end
```

例：ユーザがインターフェイスをシャットダウンおよびイネーブル化することを可能にするデバイスの設定

次に、管理者以外のユーザが、インターフェイスをシャットダウンおよびイネーブルにできるように、ネットワーキング デバイスを設定する例を示します。

最初の項は、この例の実行コンフィギュレーションの抜粋です。ここでは、この例を使用する方法を示します。

次の項は、実行コンフィギュレーションの抜粋です。

```
!
no aaa new-model
!
username admin privilege 7 secret 5 $1$tmIw$1aM7sadKhWMpkVTzxNw1J.
!
privilege interface all level 7 shutdown
privilege interface all level 7 no shutdown
privilege configure level 7 interface
privilege exec level 7 configure terminal
!
! the privilege exec level 7 configure command below is entered automatically
! when you enter the privilege exec level 7 configure terminal command above, do
! not enter it again
!
privilege exec level 7 configure
!
```

次の項では、**login** コマンドを使用して、ユーザーが admin のユーザー名を使用してネットワークデバイスにログインする場合を示します。

```
R1> login
Username: admin
Password:
```

次の項では、**show privilege** コマンドを使用して、現在の特権レベルが 7 であることを示します。

```
R1# show privilege
Current privilege level is 7
```

次の項では、**show user** コマンドを使用して、ネットワークデバイスに現在ログインしているユーザーは admin だけであることを示します。

```
R1# show user
    Line       User       Host(s)              Idle       Location
*  0 con 0     admin      idle                 00:00:00
  Interface    User               Mode         Idle     Peer Address
```

次の項は、admin ユーザがインターフェイスをシャットダウンおよびイネーブルにできる権限を持つことを示します。

```
R1# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)# interface ethernet 1/0
R1(config-if)# shutdown
R1(config-if)# no shutdown
R1(config-if)# exit
R1#
```

次の作業

ネットワーキングデバイスのセキュリティの基本を設定したら、次のように高度なオプションを考慮できます。

- ロールベースのCLIアクセス：ネットワークマネージャが、さまざまなレベルのテクニカルサポートスタッフに、異なるレベルのCLIコマンドのアクセスを付与する場合、ロールベースのCLIアクセス機能には、（このドキュメントで説明する）**privilege** コマンドよりも包括的なオプションセットが用意されています。
- AAA セキュリティ：多くのシスコ ネットワーク デバイスは、認証、許可、およびアカウンティング（AAA）機能を使用して、高度なレベルのセキュリティを提供しています。ネットワーキング デバイスで AAA を使用し、リモート TACACS+ または RADIUS サーバを併用することで、このドキュメントで説明しているすべてのタスクと、他のより高度なセキュリティ機能を実装できます。ネットワーク デバイスのローカルで実行できる AAA セキュリティ機能を設定する方法、またはTACACS+やRADIUSサーバを使用してリモート AAA セキュリティを設定する方法については、『*Cisco IOS XE Security Configuration Guide:Securing User Services* リリース 2』を参照してください。

その他の参考資料

ここでは、パスワードによるセキュリティの設定、およびネットワーキングデバイスでのCLIセッションのログイン ユーザ名に関連する関連資料について説明します。

関連資料

関連項目	マニュアル タイトル
CLI コマンドおよび設定情報に対するユーザ アクセスの管理	『*Cisco IOS XE Security Configuration Guide: Securing User Services*』Release 2 の「Role-Based CLI Access」
AAA セキュリティ機能	『*Cisco IOS XE Security Configuration Guide: Securing User Services*』Release 2
TACACS+ およびRADIUS での特権レベルの割り当て	『How to Assign Privilege Levels with TACACS+ and RADIUS』

標準

標準	タイトル
この機能によってサポートされる新しい RFC または変更された RFC はありません。また、この機能による既存 RFC のサポートに変更はありません。	--

MIB

MIB	MIB のリンク
この機能によってサポートされる新しい MIB または変更された MIB はありません。またこの機能による既存 MIB のサポートに変更はありません。	選択したプラットフォーム、Cisco IOS XE ソフトウェア リリース、およびフィーチャ セットの MIB の場所を検索しダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

RFC

RFC	タイトル
この機能によってサポートされる新しい RFC または変更された RFC はありません。また、この機能による既存 RFC のサポートに変更はありません。	--

シスコのテクニカル サポート

説明	リンク
シスコのサポート Web サイトでは、シスコの製品やテクノロジーに関するトラブルシューティングにお役立ていただけるように、マニュアルやツールをはじめとする豊富なオンライン リソースを提供しています。 お使いの製品のセキュリティ情報や技術情報を入手するために、Cisco Notification Service（Field Notice からアクセス）、Cisco Technical Services Newsletter、Really Simple Syndication（RSS）フィードなどの各種サービスに加入できます。 シスコのサポート Web サイトのツールにアクセスする際は、Cisco.com のユーザ ID およびパスワードが必要です。	http://www.cisco.com/en/US/support/index.html

パスワード、特権、およびログインによるセキュリティ設定に関する機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *224*：ネットワーク デバイス上の *CLI* セッションでのパスワード、特権レベル、およびログイン ユーザ名によるセキュリティ設定に関する機能情報

機能名	リリース	機能の設定情報
強化されたパスワード セキュリティ		Enhanced Password Security 機能を使用すると、ユーザ名のパスワードに MD5 暗号化を設定できます。MD5 暗号化は、暗号化されたパスワードの逆送信を不可能にする一方向ハッシュ関数であり、強力な暗号化保護を可能にします。MD5 暗号化を使用すると、クリアテキストパスワードを取得できません。MD5 で暗号化されたパスワードは、クリア テキスト パスワードを取得可能にすることを必須にするプロトコルでは使用できません。たとえば、チャレンジハンドシェーク認証プロトコル（CHAP）などのプロトコルです。

第 170 章

ロールベースの CLI アクセス

ロールベースの CLI アクセス機能を使用すれば、ネットワーク管理者はビューを定義できます。ビューは、Cisco IOS EXEC コマンドおよびコンフィギュレーション（config）モード コマンドへのアクセスを精選したり部分的に制限する、操作コマンドと設定機能のセットです。ビューで、ユーザの Cisco IOS コマンドライン インターフェイス（CLI）や設定情報へのアクセスを制限します。つまり、ビューで、使用するコマンドや表示する設定情報を定義できます。したがって、ネットワーク管理者はシスコ ネットワーキング デバイスへのアクセスを柔軟に管理できます。

ロールベースの CLI アクセスの前提条件

イメージで CLI ビューをサポートする必要があります。

ロールベースの CLI アクセスの制約事項

合法的傍受イメージの制限

CLI ビューは Cisco IOS パーサーの一部であるため、すべてのプラットフォームおよび Cisco IOS イメージの一部です。ただし、合法的傍受ビューは、合法的傍受サブシステムが組み込まれたイメージ内でしか使用できません。

許可されたビューの最大数

1 つの合法的傍受ビューを含むCLI ビューとスーパービューの設定可能な最大数は 15 です（これには、ルート ビューは含まれません）。

解析ビューのプロファイル

解析ビューのプロファイルを設定する場合、「no」コマンドまたは「default」コマンドと任意の設定コマンドの組み合わせは、スタートアップ コンフィギュレーション ファイルに保存されません。設定は受け入れられ、デバイスがリロードされるまで保持されます。スタートアップ コンフィギュレーションに保存されないコマンドの例：

- **command configure include all no**
- **command interface include all no**
- **command configure include all default**

ロールベースの CLI アクセスに関する情報

CLI ビューを使用するメリット

ユーザは特権レベルとイネーブル モード パスワードの両方を介して CLI アクセスを制御できますが、これらの機能では、ネットワーク管理者に Cisco IOS デバイスを操作するのに必要な詳細レベルが提供されません。CLI ビューは、より詳細なアクセス コントロール機能をネットワーク管理者に提供するため、Cisco IOS ソフトウェア全体のセキュリティとアカウンタビリティが向上します。

Cisco IOS Release 12.3(11)T 以降では、ネットワーク管理者が、ビューへのインターフェイスまたはインターフェイス グループを指定することもできます。そのため、指定されたインターフェイスに基づくアクセスが可能になります。

ルート ビュー

システムがルート ビューになっている場合は、レベル 15 の権限を持つユーザとして、すべてのアクセス権限が付与されます。管理者がシステムのビュー（CLI ビュー、スーパービュー、合法的傍受ビューなど）を設定する場合は、システムをルート ビューにする必要があります。

レベル 15 権限を持つユーザとルート ビュー ユーザの違いは、ルート ビュー ユーザは、新しいビューを設定したり、ビューに対してコマンドを追加または削除したりできることです。また、CLI ビューでは、ルート ビュー ユーザがそのビューに追加したコマンドにしかアクセスできません。

合法的傍受ビュー

CLI ビューと同様に、合法的傍受ビューは、特定のコマンドと設定情報へのアクセスを制限します。具体的には、合法的傍受ビューを使用すれば、ユーザは、コールとユーザに関する情報を保存する簡易ネットワーク管理プロトコル（SNMP）コマンドの特別なセットである TAP-MIB 内に保持された合法的傍受コマンドへのアクセスを保護できます。

合法的傍受ビュー内で使用可能なコマンドは、次のカテゴリのいずれかに属します。

- 他のビューまたは権限レベルでは使用不可にすべき合法的傍受コマンド
- 合法的傍受ユーザにとっては有効であるが、他のビューまたは権限レベルから除外する必要のない CLI ビュー

スーパービュー

スーパービューは、1 つ以上の CLI ビューで構成されています。このビューでは、受け入れるコマンドと表示する設定情報を定義できます。スーパービューを使用すれば、ネットワーク管理者は、複数の CLI ビューをユーザ グループに割り当てなくても、設定された CLI ビュー内のすべてのユーザをスーパービューに割り当てることができます。

スーパービューには次の特性があります。

- CLI ビューを複数のスーパービュー間で共有できます。
- スーパービューにはコマンドを設定できません。つまり、CLI ビューにコマンドを追加してから、その CLI ビューをスーパービューに追加する必要があります。
- スーパービューにログインしたユーザは、そのスーパービューに属している CLI ビューに設定されたすべてのコマンドにアクセスできます。
- スーパービューごとにパスワードが設定されます。このパスワードは、スーパービューを切り替えたり、CLI ビューからスーパービューに切り替えたりするために使用されます。
- スーパービューが削除されても、関連する CLI ビューは削除されません。

ビュー認証と新しい AAA 属性

ビュー認証は、新しい属性の **cli-view-name** を介して、外部の認証、許可、およびアカウンティング（AAA）サーバーで実行されます。

AAA 認証は特定のユーザに 1 つのビュー名のみを関連付けます。つまり、認証サーバ内の 1 人のユーザに対して 1 つのビュー名しか設定できません。

ロールベースの CLI アクセスの使用方法

CLI ビューの設定

このタスクを実行して、CLI ビューを作成し、必要に応じて、コマンドまたはインターフェイスをビューに追加します。

始める前に

ビューを作成する前に、次のタスクを実行する必要があります。

- **aaa new-model** コマンドを使用して AAA をイネーブルにします。
- システムが特権レベル 15 ではなく、ルート ビューになっていることを確認します。

手順の概要

1. **enable view**
2. **configure terminal**
3. **parser view** *view-name* [**inclusive**]
4. **secret** [**0** | **5**] *encrypted-password*
5. **commands** *parser-mode* {**exclude** | **include-exclusive** | **include**} [**all**] [**interface** *interface-name* | *command*]
6. **end**
7. **enable** [*privilege-level* | **view** *view-name*]
8. **show parser view all**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable view** 例： `Device> enable view`	ルート ビューを有効にします。 • プロンプトが表示されたら、権限レベル 15 パスワード（ルートパスワードなど）を入力します。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**parser view** *view-name* [**inclusive**] 例：	すべてのコマンドを含むビューがデフォルトで作成されます。**inclusive** キーワードオプションを選択しないと、すべてのコマンドを除くビューがデフォル

	コマンドまたはアクション	目的
	`Device(config)# parser view first inclusive` `Device(config-view)#`	トで作成されます。ビューの設定モードになります。
ステップ 4	**secret** [**0** | **5**] *encrypted-password* 例： `Device(config-view)# secret 5 secret`	CLI ビューまたはスーパービューとパスワードを関連付けます。 （注） このコマンドを発行しなければ、ビューのその他の属性が設定できません。 （注） CSCts50236 を使用すると、パスワードは削除または上書きできます。設定されたパスワードを削除するには、**no secret** コマンドを使用します。
ステップ 5	**commands** *parser-mode* {**exclude** | **include-exclusive** | **include**} [**all**] [**interface** *interface-name* | *command*] 例： `Device(config-view)# commands exec include show version`	コマンドまたはインターフェイスをビューに追加し、指定されたコマンドがあるモードを指定します。 （注） parser view プロファイルを設定するときは、次の **no** または **default** コマンドはスタートアップ コンフィギュレーションには保存されません。これらのコマンドは、デバイスがリロードされるまで使用中です。デバイスをリロードしたら、必要な結果が得られるように、これらのコマンドを再適用します。 • **commands configure include all no** • **commands interface include all no** • **commands configure include all default**
ステップ 6	**end** 例： `Device(config-view)# end`	ビューのコンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。
ステップ 7	**enable** [*privilege-level* | **view** *view-name*] 例： `Device# enable view first`	設定済みの CLI ビューにアクセスするためのパスワードを求めるプロンプトが表示され、1つのビューから別のビューへ切り替えられます。 パスワードを入力して CLI ビューにアクセスします。

	コマンドまたはアクション	目的
ステップ 8	**show parser view all** 例： `Device# show parser view all`	（任意）デバイス上で設定されるすべてのビューに関する情報を表示します。 （注） このコマンドはルートユーザーと合法的傍受ユーザーの両方に使用できますが、**all** キーワードはルートユーザーしか使用できません。ただし、**all** キーワードは、ルートビュー内のユーザーが、合法的傍受ビューやCLI ビュー内のユーザーに使用を許可するように設定できます。

トラブルシューティングのヒント

パスワードとビューを関連付ける必要があります。パスワードを関連付けずに、**commands** コマンド経由でビューにコマンドを追加しようとすると、次のようなシステムメッセージが表示されます。

```
%Password not set for view <viewname>.
```

合法的傍受ビューの設定

このタスクを実行して、ビューを初期化し、合法的傍受固有のコマンドと設定情報用に設定します

始める前に

合法的傍受ビューを初期化する前に、**privilege** コマンド経由で特権レベルが 15 に設定されていることを確認します。

（注） レベル 15 権限を持っている管理者またはユーザだけが合法的傍受ビューを初期化できます。

手順の概要

1. **enable view**
2. **configure terminal**
3. **li-view** *li-password* **user** *username* **password** *password*
4. **username lawful-intercept** [*name*] [**privilege** *privilege-level* | **view** *view-name*] **password** *password*
5. **parser view** *view-name*
6. **secret 5** *encrypted-password*
7. **name** *new-name*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable view** 例： `Device> enable view`	ルート ビューを有効にします。 • プロンプトが表示されたら、権限レベル 15 パスワード（ルートパスワードなど）を入力します。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**li-view** *li-password* **user** *username* **password** *password* 例： `Device(config)# li-view lipass user li_admin password li_adminpass`	合法的傍受ビューを初期化します。 li-view が初期化されたら、**user** *username* **password** *password* オプション経由で少なくとも 1 人のユーザーを指定する必要があります。
ステップ 4	**username lawful-intercept** [*name*] [**privilege** *privilege-level* | **view** *view-name*] **password** *password* 例： `Device(config)# username lawful-intercept li-user1 password li-user1pass`	シスコ デバイス上で合法的傍受ユーザを設定します。
ステップ 5	**parser view** *view-name* 例： `Device(config)# parser view li view name`	（任意）ビュー コンフィギュレーション モードに入ります。このモードでは、合法的傍受ビューのパスワードや名前を変更できます。
ステップ 6	**secret 5** *encrypted-password* 例： `Device(config-view)# secret 5 secret`	（任意）合法的傍受ビューの既存のパスワードを変更します。
ステップ 7	**name** *new-name* 例： `Device(config-view)# name second`	（任意）合法的傍受ビューの名前を変更します。 このコマンドが発行されなかった場合、合法的傍受ビューのデフォルト名は "li-view" になります。

トラブルシューティングのヒント

合法的傍受ビューにアクセス可能なすべてのユーザーに関する情報を表示するには、**show users lawful-intercept** コマンドを発行します（このコマンドは、認可された合法的傍受ビュー ユーザしか使用できません）。

スーパービューの設定

このタスクを実行して、スーパービューを設定し、スーパービューに少なくとも 1 つの CLI ビューを追加します。

始める前に

CLI ビューをスーパービューに追加する前に、スーパービューに追加する CLI ビューがシステム内で有効なビューであることを確認します。つまり、ビューが、**parser view** コマンド経由で正常に作成されたことを確認します。

（注） スーパービューにビューを追加するには、スーパービューに対してパスワードを設定する必要があります（**secret 5** コマンド経由）。その後で、ビュー コンフィギュレーション モードで **view** コマンドを発行して、少なくとも 1 つの CLI ビューをスーパービューに追加します。

手順の概要

1. **enable view**
2. **configure terminal**
3. **parser view** *superview-name* **superview**
4. **secret 5** *encrypted-password*
5. **view** *view-name*
6. **end**
7. **show parser view all**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable view** 例： `Device> enable view`	ルート ビューを有効にします。 • プロンプトが表示されたら、権限レベル 15 パスワード（ルート パスワードなど）を入力します。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**parser view** *superview-name* **superview** 例： `Device(config)# parser view su_view1 superview`	スーパービューを作成して、ビュー コンフィギュレーション モードに入ります。

	コマンドまたはアクション	目的
ステップ 4	**secret 5** *encrypted-password* 例： `Device(config-view)# secret 5 secret`	CLI ビューまたはスーパービューとパスワードを関連付けます。 （注） このコマンドを発行しなければ、ビューのその他の属性が設定できません。
ステップ 5	**view** *view-name* 例： `Device(config-view)# view view_three`	正常な CLI ビューをスーパービューに追加します。 特定のスーパービューに追加する各 CLI ビューに対して、このコマンドを発行します。

ステップ 6	**end**
	例：
	`Device(config-view)# end`
	`Device#`
		ビューのコンフィギュレーションモードを終了し、特権 EXEC モードに戻ります。

ステップ 7	**show parser view all** 例： `Device# show parser view`	（任意）デバイス上で設定されるすべてのビューに関する情報を表示します。 （注） このコマンドはルートユーザーと合法的傍受ユーザーの両方に使用できますが、**all** キーワードはルートユーザーしか使用できません。ただし、**all** キーワードは、ルートビュー内のユーザーが、合法的傍受ビューや CLI ビュー内のユーザーに使用を許可するように設定できます。

ビューとビュー ユーザのモニタリング

すべてのビュールート、CLI、合法的傍受、およびスーパービューに関するデバッグメッセージを表示するには、特権 EXEC モードで **debug parser view** コマンドを使用します。

ロールベースの CLI アクセスの設定例

例：CLI ビューの設定

次の例は、2 つの CLI ビュー "first" と "second" の設定方法を示しています。その後、実行コンフィギュレーションの CLI ビューを確認できます。

```
Device(config)# parser view first inclusive
Device(config-view)# secret 5 firstpass
Device(config-view)# command exec exclude show version
```

```
Device(config-view)# command exec exclude configure terminal
Device(config-view)# command exec exclude all show ip
Device(config-view)# exit
Device(config)# parser view second
Device(config-view)# secret 5 secondpass
Device(config-view)# command exec include-exclusive show ip interface
Device(config-view)# command exec include logout
Device(config-view)# exit
!
!
Device(config-view)# do show running-config | beg view

parser view first inclusive
 secret 5 $1$MCmh$QuZaU8PIMPlff9sFCZvgW/
 commands exec exclude configure terminal
 commands exec exclude configure
 commands exec exclude all show ip
 commands exec exclude show version
 commands exec exclude show
!
parser view second
 secret 5 $1$iP2M$R16BXKecMEiQesxLyqygW.
 commands exec include-exclusive show ip interface
 commands exec include show ip
 commands exec include show
 commands exec include logout
!
```

例：CLI ビューの確認

CLI ビューの "first" と "second" を設定したら、**enable view** コマンドを発行して、各ビュー内で使用可能なコマンドを確認できます。次の例は、ユーザが CLI ビューの "first" にログイン後に、どのコマンドがこのビュー内で使用可能かを示しています（**show ip** コマンドは all オプションと一緒に設定されているため、second ビュー内で **include-exclusive** キーワードを使用している **show ip interface** コマンドを除く、すべてのサブオプションのセットが表示されます）。

```
Device# enable view first
Password:
Device# ?
Exec commands:
  configure  Enter configuration mode
  enable     Turn on privileged commands
  exit       Exit from the EXEC
  show       Show running system information
Device# show ?
  ip       IP information
  parser   Display parser information
  version  System hardware and software status
Device# show ip ?

  access-lists            List IP access lists
  accounting              The active IP accounting database
  aliases                 IP alias table
  arp                     IP ARP table
  as-path-access-list     List AS path access lists
  bgp                     BGP information
  cache                   IP fast-switching route cache
  casa                    display casa information
  cef                     Cisco Express Forwarding
```

```
  community-list          List community-list
  dfp                     DFP information
  dhcp                    Show items in the DHCP database
  drp                     Director response protocol
  dvmrp                   DVMRP information
  eigrp                   IP-EIGRP show commands
  extcommunity-list       List extended-community list
  flow                    NetFlow switching
  helper-address          helper-address table
  http                    HTTP information
  igmp                    IGMP information
  irdp                    ICMP Device Discovery Protocol
.
.
.
```

例：合法的傍受ビューの設定

次の例は、合法的傍受ビューの設定方法、ビューへのユーザの追加方法、および追加されたユーザの確認方法を示しています。

```
!Initialize the LI-View.
Device(config)# li-view lipass user li_admin password li_adminpass
Device(config)# end
! Enter the LI-View; that is, check to see what commands are available within the view.
Device# enable view li-view
Password:
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# parser view li-view

Device(config-view)# ?
View commands:
  commands  Configure commands for a view
  default   Set a command to its defaults
  exit      Exit from view configuration mode
  name      New LI-View name
  no        Negate a command or set its defaults
  password  Set a password associated with CLI views
Device(config-view)#
! NOTE:LI View configurations are never shown as part of 'running-configuration'.
! Configure LI Users.
Device(config)# username lawful-intercept li-user1 password li-user1pass

Device(config)# username lawful-intercept li-user2 password li-user2pass
! Displaying LI User information.
Device# show users lawful-intercept
li_admin
li-user1
li-user2
Device#
```

（注） 合法的傍受ビューは特定のイメージに対してのみ使用でき、表示名オプションは合法的傍受ビューでのみ使用できます。

例：スーパービューの設定

次の **show running-config** コマンドのサンプル出力は、"view_one" と "view_two" がスーパービューの "su_view1" に追加され、"view_three" と "view_four" がスーパービューの "su_view2" に追加されていることを示しています。

```
Device# show running-config
!
parser view su_view1 superview
 secret 5 <encoded password>
 view view_one
 view view_two
!
parser view su_view2 superview
 secret 5 <encoded password>
 view view_three
 view view_four
!
```

ロールベースの CLI アクセスに関する追加情報

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『Cisco IOS Master Command List, All Releases』
セキュリティ コマンド	• 『Cisco IOS Security Command Reference: Commands A to C』 • 『Cisco IOS Security Command Reference: Commands D to L』 • 『Cisco IOS Security Command Reference: Commands M to R』 • 『Cisco IOS Security Command Reference: Commands S to Z』
SNMP、MIB、CLI 設定	『*Cisco IOS Network Management Configuration Guide , Release 15.0.*』
権限レベル	「パスワード、特権、およびログインによるセキュリティ設定」モジュール

シスコのテクニカル サポート

説明	リンク
右の URL にアクセスして、シスコのテクニカル サポートを最大限に活用してください。これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

ロールベースの CLI アクセスに関する機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *225* : ロールベースの *CLI* アクセスに関する機能情報

機能名	リリース	機能情報
ロールベースの CLI アクセス		ロールベースの CLI アクセス機能は、ネットワーク管理者が、CLI と設定情報に対するユーザ アクセスを制限できるようにします。 CLI ビュー機能は、インターフェイス単位レベルでユーザ アクセスを制限するように拡張されました。新しい CLI ビューは、拡張されたビュー機能をサポートするために導入されました。また、設定された CLI ビューをスーパービューにグループ分けするためのサポートが導入されました。 次のコマンドが導入または変更されました。**commands (view)**、**enable**、**li-view**、**name (view)**、**parser view , parser view superview**、**secret**、**show parser view**、**show users**、**username**、および **view**。
ロールベースの CLI 包含ビュー		ロールベースの CLI 包含ビュー機能によって、すべてのコマンドを含む標準 CLI ビューがデフォルトで有効になっています。 次のコマンドが変更されました。**parser view inclusive**。

第 171 章

セキュア ストレージについて

セキュア ストレージ機能では、重要な設定情報を暗号化して保護できます。VPN、IPSec とその他の非対称キーペア、事前共有秘密、タイプ 6 のパスワード暗号化キーおよび特定のクレデンシャルを暗号化します。インスタンス固有の暗号キーは、危険にさらされることを防ぐためにハードウェアのトラスト アンカーに保管されます。

デフォルトでは、この機能はハードウェアのトラストアンカーを備えたプラットフォームで有効です。この機能は、ハードウェアのトラストアンカーがないプラットフォームではサポートされません。

サポートされるプラットフォーム

Cisco IOS リリース 15.6(3) M1 以降、次の Cisco 880 シリーズ プラットフォームでセキュアストレージがサポートされています。

表 *226 :* セキュアストレージでサポートされるプラットフォーム： *Cisco* サービス統合型ルータ *880 PID*

C881-K9
C887VA-K9
C886VA-K9
C887VAM-K9
C886VAJ-K9
C888-K9

Cisco IOS リリース 15.6(3) M1 以降、次の Cisco 890 シリーズ プラットフォームでセキュアストレージがサポートされています。

表 *227 :* セキュアストレージでサポートされるプラットフォーム：*Cisco* サービス統合型ルータ *890 PID*

C891FW-E-K9
C891F-K9
C891FW-A-K9
C891-24X-K9

Cisco IOS リリース 15.6(3) M1 以降、次の Cisco 800M シリーズ プラットフォームでセキュアストレージがサポートされています。

表 *228 :* セキュアストレージでサポートされるプラットフォーム：*Cisco* サービス統合型ルータ *800M PID*

C841M-4X/K9
C886VA-K9
C841M-8X/K9

Cisco IOS XE リリース 16.6.1 以降、次の ISR 4000 シリーズ プラットフォームでセキュアストレージがサポートされています。

表 *229 :* セキュアストレージでサポートされるプラットフォーム：*Cisco* サービス統合型ルータ *4000 PID*

ISR4431
ISR4221
ISR4321
ISR4331
ISR4351
ISR4451-X

Cisco IOS XE リリース 16.6.1 以降、次の ASR 1000 プラットフォームでセキュアストレージがサポートされています。

表 *230 :* セキュアストレージでサポートされるプラットフォーム：*Cisco ASR 1000* シリーズ アグリゲーション サービス ルータ *PID*

ASR1000-RP3
ASR1001-X
ASR1001-HX
ASR1002-HX

Cisco IOS XE リリース 16.9.1 以降、次の Cisco 1000 シリーズ プラットフォームでセキュアストレージがサポートされています。

表 *231 :* セキュアストレージでサポートされるプラットフォーム：*Cisco 1000* シリーズ *PID*

C1101-4P
C1111-8P
C1111-4P
C1112-8P
C1113-8P
C1113-8PM
C1116-4P
C1117-4P
C1117-4PM
C1101-4PLTEP
C1111-8PLTEEA
C1111-8PLTELA
C1111-4PLTEEA
C1111-4PLTELA
C1112-8PLTEEA
C1113-8PLTEEA
C1113-8PLTELA
C1113-8PMLTEEA
C1116-4PLTEEA
C1117-4PLTEEA
C1117-4PLTELA
C1117-4PMLTEEA
C1111-8PWY
C1111-4PWX
C1112-8PWE
C1113-8PWA

C1113-8PWB
C1113-8PWE
C1116-4PWE
C1117-4PWE
C1117-4PWA
C1117-4PWZ
C1117-4PMWE
C1111-8PLTEEAWX
C1111-8PLTELAWY
C1112-8PLTEAWE
C1113-8PLTEEAWA
C1113-8PLTEEAWB
C1113-8PLTEEAWE
C1113-8PLTELAWZ
C1116-4PLTEEAWE
C1117-4PMLTEEA
C1117-4PLTEEAWE
C1117-4PLTEEAWA
C1117-4PLTELAWZ
C1117-4PMLTEEAWE
C1101-4PLTEPWX

セキュア ストレージの有効化

始める前に

デフォルトでは、この機能はプラットフォームで有効です。この手順は、無効になっているプラットフォームで使用します。

手順の概要

1. Config terminal

2. service private-config-encryption
3. do write memory

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	Config terminal 例： `router#config terminal`	コンフィギュレーション モードを開始します。
ステップ 2	service private-config-encryption 例： `router(config)# service private-config-encryption`	プラットフォームでセキュリティ ストレージ機能を有効にします。
ステップ 3	do write memory 例： `router(config)# do write memory`	private-config ファイルを暗号化し、暗号化フォーマットで保存します。

例

次に、セキュア ストレージをイネーブルにする例を示します。

```
router#config terminal
router(config)# service private-config-encryption
router(config)# do write memory
```

セキュア ストレージの無効化

始める前に

プラットフォームでセキュア ストレージ機能を無効にするには、次のタスクを実行します。

手順の概要

1. Config terminal
2. no service private-config-encryption
3. do write memory

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	Config terminal 例：	コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
	`router#config terminal`	
ステップ 2	no service private-config-encryption 例： `router(config)# no service private-config-encryption`	プラットフォームでセキュリティストレージ機能を無効にします。
ステップ 3	do write memory 例： `router(config)# do write memory`	private-config ファイルを復号し、プレーン フォーマットで保存します。

例

次に、セキュア ストレージをディセーブルにする例を示します。

```
router#config terminal
router(config)# no service private-config-encryption
router(config)# do write memory
```

暗号化のステータスの確認

暗号化のステータスを確認するには、**show parser encrypt file status** コマンドを使用します。次のコマンド出力は、機能は利用できるが、ファイルが暗号化されていないことを示します。ファイルは「プレーン テキスト」形式です。

```
router#show parser encrypt file status
Feature: Enabled
File Format: Plain Text
Encryption Version: Ver1
```

次のコマンド出力は、機能は有効で、ファイルが暗号化されていることを示します。ファイルは「暗号テキスト」形式です。

```
router#show parser encrypt file status
Feature: Enabled
File Format: Cipher Text
Encryption Version: Ver1
```

プラットフォームイメージの旧バージョンへのダウングレード

セキュア ストレージがサポートされていない旧バージョンにプラットフォーム イメージをダウングレードする場合は、サポートされているバージョンでこの機能を事前に無効にする必要があります。

旧バージョンにダウングレードする前にこの機能を無効にしないと、private-config ファイルが暗号化形式になります。ファイルが暗号化形式になっていることを示す、次の Syslog メッセージが生成されます。

```
%PARSER-4-BADCFG: Unexpected end of configuration file.
```

ファイルが「プレーン テキスト」の場合、Syslog メッセージは生成されません。

セキュアストレージの概要の機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *232 : Cisco TrustSec* の概要の機能情報

機能名	リリース	機能情報
セキュアなストレージ	Cisco IOS XE Fuji 16.9.1	セキュアなストレージのサポートが ASR および ISR プラットフォームに導入されました。

第 172 章

AutoSecure

AutoSecure 機能では、1 つの CLI コマンドによって、ネットワーク攻撃に悪用されるおそれのある一般的な IP サービスを無効にしたり、攻撃を受けたときにネットワークを防御するのに役立つ IP サービスや機能を有効にしたりできます。また、ルータのセキュリティ設定を簡素化しつつ機能を堅牢にすることができます。

AutoSecure では、「lab」や「cisco」など、ネットワークで広く使用されているありふれたパスワードが排除され、最小限必要なパスワード長が設定されることで、ルータへのセキュアなアクセスが強化されています。正常に実行できなかった回数が、設定したしきい値を超えると、syslog メッセージが生成されます。

また、ロールバックを有効にすると、AutoSecure 設定に失敗しても、ルータを前の設定状態に戻すことができます。

AutoSecure を有効にすると、システム ロギング メッセージの詳細な監査証跡によって、実行コンフィギュレーションに適用される可能性のある AutoSecure の設定変更または改ざんがキャプチャされます。

AutoSecure の制約事項

AutoSecure の設定は、実行時またはセットアップ時に行います。AutoSecure をイネーブルにした後に、関連する設定を変更した場合は、AutoSecure の設定が完全に有効にならないことがあります。

AutoSecure について

管理プレーンのセキュリティ保護

管理プレーンのセキュリティ保護は、潜在的にセキュリティ攻撃に利用される可能性がある特定のグローバルおよびインターフェイス サービスをオフにし、攻撃の脅威を軽減できるグローバル サービスをオンにすることで行います。また、セキュリティ保護されたアクセスとロギングもルータに設定できます。

⚠

注意 デバイスがネットワーク管理（NM）アプリケーションで管理されている場合、管理プレーンのセキュリティ保護によって、HTTPサーバなどのいくつかのサービスがディセーブル化され、NM アプリケーションのサポートが妨げられることがあります。

ここでは、AutoSecureがマネジメントプレーンのセキュリティ保護にどのように役立つかを説明します。

グローバル サービスのディセーブル化

この機能をイネーブルにすると（**auto secure** コマンドを介して）、次のグローバルサービスは、ユーザーにプロンプトを表示することなくルータで自動的にディセーブルになります。

- Finger：攻撃の前にシステムの情報を収集（探査）します。イネーブルになっている場合、この情報により、デバイスが攻撃に対して脆弱なままになることがあります。
- PAD：すべてのパケット アセンブラ/逆アセンブラ（PAD）コマンドと、PAD デバイスとアクセス サーバとの接続をイネーブルにします。イネーブルになっている場合、このサービスにより、デバイスが攻撃に対して脆弱なままになることがあります。
- スモール サーバ：TCP およびユーザ データグラム プロトコル（UDP）の診断ポート攻撃の原因となります。この攻撃では、送信者がルータの UDP 診断サービスに偽の要求を大量に送信し、すべての CPU リソースを使い果たします。
- BOOTP サーバ：BOOTP はセキュアではないプロトコルです。攻撃で悪用されます。
- HTTP サーバ：Secure HTTP サーバが使用されていないか、ACL を関連付けて HTTP サーバに組み込まれる認証が使用されていない場合、HTTP サーバは安全ではなく、攻撃に悪用されることがあります。（HTTP サーバをイネーブルにする必要がある場合は、適切な認証またはアクセス リストの指定を求めるメッセージが表示されます）。

（注） Cisco Configuration Professional（CCP）を使用している場合は、**ip http server** コマンドを介して手動で HTTP サーバーをイネーブルにする必要があります。

- 識別サービス：RFC 1413 で定義されている安全ではないプロトコルです。TCP ポートで ID を照会することが可能です。攻撃者は、ID サーバでユーザに関する個人的な情報にアクセスできます。
- CDP：大量の Cisco Discovery Protocol（CDP）パケットがルータに送信されると、ルータの使用可能なメモリが消費され、ルータがクラッシュすることがあります。

⚠

注意 CDP を使用してネットワーク トポロジを検出する NM アプリケーションは、検出を実行できなくなります。

- NTP：認証またはアクセス コントロールが行われないと、ネットワーク タイム プロトコル（NTP）は安全ではありません。攻撃者はこのプロトコルを使用して NTP パケットを送信し、ルータをクラッシュさせたり、過負荷状態にしたりすることが可能です。（NTP を有効にする場合は、Message Digest 5（MD5）および **ntp access-group** コマンドを使用して NTP 認証を設定する必要があります。NTP がグローバルにイネーブルになっている場合は、NTP が不要なすべてのインターフェイスでディセーブルにしてください）。
- 送信元ルーティング：デバッグ作業でのみ使用するため、それ以外のすべての場合でルーティングをディセーブルにする必要があります。そうしないと、アクセス コントロール メカニズムを通過すべきパケットが、一部のアクセス コントロール メカニズムを回避する可能性があります。

サービスのインターフェイス単位のディセーブル化

この機能をイネーブルにすると、次のインターフェイス単位のサービスが自動的にルータでディセーブルになります。

- ICMP リダイレクト：すべてのインターフェイスでディセーブルになります。このサービスは、正しく設定されたネットワークにとっては有益な機能ではなく、セキュリティ ホールを悪用するために攻撃者によって使用される可能性があります。
- ICMP 到達不能：すべてのインターフェイスでディセーブルになります。インターネット制御マネジメント プロトコル（ICMP）到達不能は、ICMP ベースのサービス拒否攻撃（DoS）の原因として知られています。
- ICMP マスク応答メッセージ：すべてのインターフェイスでディセーブルになります。ICMP マスク応答メッセージにより、攻撃者はインターネットワークの特定のサブネットワークのサブネットマスクを入手できます。
- プロキシ Arp：すべてのインターフェイスでディセーブルになります。プロキシ Arp 要求は、DoS 攻撃の原因として知られています。これは、攻撃者が何度も送信した要求に応答しようとしてルータの使用可能な帯域幅とリソースが消費されることがあるためです。
- ダイレクト ブロードキャスト：すべてのインターフェイスでディセーブルになります。DoS を生じさせるための SMURF 攻撃の原因となる可能性があります。

- メンテナンス オペレーション プロトコル（MOP）サービス：すべてのインターフェイスでディセーブルになります。

グローバル サービスのイネーブル化

AutoSecure機能をイネーブルにすると、次のグローバル サービスが自動的にルータでイネーブルになります。

- **service password-encryption** コマンド：設定でパスワードが表示されなくなります。
- **service tcp-keepalives-in** および **service tcp-keepalives-out** コマンド：異常終了したTCPセッションが確実に削除されます。

ルータへのアクセスの保護

⚠

注意 デバイスがNMアプリケーションによって管理されている場合に、ルータへのアクセスをセキュリティ保護すると、重要なサービスが無効化されたり、NMアプリケーションのサポートが妨げられたりすることがあります。

AutoSecure機能をイネーブルにすると、ルータへのアクセスをセキュリティ保護する次のオプションをユーザが使用できるようになります。

- テキスト バナーがない場合は、バナーの追加を求めるメッセージが表示されます。AutoSecure 機能には次のサンプル バナーが用意されています。

```
Authorized access only
This system is the property of ABC Enterprise
Disconnect IMMEDIATELY if you are not an authorized user!
Contact abc@xyz.com +99 876 543210 for help.
```

- ログインおよびパスワード（サポートされている場合はシークレット パスワードを推奨）は、コンソール、AUX、TTYの各回線で設定されます。**transport input** コマンドと **transport output** コマンドも、これらの回線のすべてで設定されます。（Telnetおよびセキュア シェル（SSH）のみが有効な転送方式です。）**exec-timeout** コマンドは、コンソールとAUXの各回線で10に設定されます。
- デバイスのイメージが暗号化イメージである場合、AutoSecureはルータに対するアクセスとファイル転送にSSHとセキュア コピー（SCP）をイネーブルにします。 **ip ssh** コマンドの **timeout** *seconds* および **authentication-retries** *integer* オプションは最小数に設定されます。（Telnet および FTP は、この操作の影響を受けず、引き続き動作します）。
- AutoSecure ユーザが、デバイスで簡易ネットワーク管理プロトコル（SNMP）を使用しないと指定した場合は、次のいずれかの状態になります。
  - インタラクティブ モードでは、コミュニティ ストリングの値に関係なくSNMPをディセーブルにするかどうかを尋ねるメッセージがユーザに表示されます。コミュニティ

ストリングは、パスワードと同じように機能し、ルータのエージェントへのアクセスを規制します。

- 非インタラクティブ モードでは、コミュニティ ストリングが "public" または "private" である場合に SNMP がディセーブルになります。

（注） AutoSecure がイネーブルになると、装置のモニタおよび設定のために SNMP を使用するツールは、SNMP を使用する装置との通信を行うことができなくなります。

- 認証、許可、アカウンティング（AAA）が設定されていない場合は、ローカル AAA を設定します。ユーザは、ローカルのユーザ名とそのパスワードをルータで設定するように AutoSecure から要求されます。

セキュリティ ロギング

次のロギング オプションは、AutoSecure をイネーブルにした後で使用できます。これらのオプションは、セキュリティ インシデントを特定し、顧客に対応する方法を提供します。

- すべてのデバッグ メッセージおよびログ メッセージのシーケンス番号とタイム スタンプ。このオプションは、ロギング メッセージを監査するときに役立ちます。
- ロギング メッセージはログ関連のイベントに対して生成されます。たとえば、ログイン攻撃が検出されルータが「待機モード」に入ると、「Blocking Period when Login Attack Detected」のメッセージが表示されます。（待機モードでは、ルータは Telnet、HTTP、または SSH を使用したログイン試行を許可しません）。

ログイン関連のシステム メッセージの詳細については、『Cisco IOS Release 12.3(4)T feature module Cisco IOS Login Enhancements』を参照してください。

- **logging console critical** コマンド。これにより、システムロギング（Syslog）メッセージがすべての使用可能な TTY 回線に送信され、シビラティ（重大度）に応じてメッセージが制限されます。
- **logging buffered** コマンド。これにより、ロギングメッセージが内部バッファにコピーされ、バッファに記録されるメッセージがシビラティ（重大度）に応じて制限されます。
- **logging trap debugging** コマンド。これにより、デバッグよりもシビラティ（重大度）の高いコマンドをすべてロギングサーバーに送信できます。

フォワーディング プレーンのセキュリティ保護

ルータのフォワードプレーンでの攻撃の危険を最小限にするために、AutoSecure には次の機能が用意されています。

- Cisco エクスプレス フォワーディング（CEF）：AutoSecure は、可能であれば CEF または分散 CEF（dCEF）をルータでイネーブルにします。トラフィックが新たな宛先に到着し

始めたときにキャッシュエントリを作成する必要がないため、大量のトラフィックが多数の宛先に送信される場合でも、CEFは他のモードよりも予測しやすい方法で動作します。このため、CEF 用に設定されているルータは、SYN 攻撃下において、従来のキャッシュ方法を採用しているルータと比較して高い性能を発揮します。

（注） CEF は従来のキャッシュよりもメモリを多く消費します。

- TCPインターセプト機能が使用可能な場合、この機能をルータで接続タイムアウト用に設定することができます。
- ストリクト ユニキャスト リバース パス転送（uRPF）が使用可能である場合、偽造（詐称）された送信元 IP アドレスが入ってくることによって発生する問題を軽減できるようにするために、この uRPF をルータで設定できます。uRPF は検証可能な送信元 IP アドレスが不足している IP パケットを廃棄します。
- ルータは、ファイアウォールとして使用されている場合、インターネットに繋がっているパブリック インターフェイスでコンテキストベース アクセス コントロール（CBAC）用に設定することができます。

（注） AutoSecureダイアログの冒頭では、パブリック インターフェイスのリストの指定を求めるメッセージが表示されます。

AutoSecure の設定方法

AutoSecure の設定

注意 **auto secure** コマンドでルータのセキュリティ保護を行うことはできますが、ルータが完全にセキュリティ保護されるという保証はありません。

手順の概要

1. **enable**
2. auto secure [management | forwarding] [no-interact | full] [ntp | login | ssh | firewall | tcp-intercept]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードなど、高位の権限レベルを有効にします。 パスワードを入力します（要求された場合）。

ステップ 2	auto secure [management | forwarding] [no-interact | full] [ntp | login | ssh | firewall | tcp-intercept]
	例：
	`Router#`
	`auto secure`
		セミインタラクティブ ダイアログ セッションは、**management** または **forwarding** キーワードが選択されているときに、ルータの管理またはフォワーディングプレーンのセキュリティ保護を開始します。いずれのオプションも選択しないと、ダイアログによってどちらのプレーンにも設定するよう尋ねられます。**management** キーワードが選択されると、管理プレーンだけがセキュリティ保護されます。**forwarding keyword is selected, then** の場合は、フォワーディングプレーンのみがセキュリティ保護されます。
		no-interact キーワードが選択されると、どのようなインタラクティブな設定も求められません。
		full キーワードが選択されると、デフォルトで、ユーザーはすべてのインタラクティブな質問を入力するように求められます。

強化されたルータへのセキュリティ アクセスの設定

手順の概要

1. **enable**
2. **configure terminal**
3. **enable password** {*password* | [*encryption-type*] *encrypted-password* }
4. **security authentication failure rate** *threshold-rate* **log**
5. **exit** *threshold-rate* **log**
6. **show auto secure config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードなど、高位の権限レベルを有効にします。 パスワードを入力します（要求された場合）。

	コマンドまたはアクション	目的
ステップ 2	**configure terminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**enable password** {*password* | [*encryption-type*] *encrypted-password* } 例： `Router(config)# enable password elephant`	さまざまな権限レベルへのアクセスを制御するローカル パスワードを設定します。
ステップ 4	**security authentication failure rate** *threshold-rate* **log** 例： `Router(config)# security authentication failure rate 10 log`	許容されるログイン失敗回数を設定します。 • *threshold-rate*：許容されるログイン失敗回数。 • **log**：回数がしきい値を超えた場合、Syslog認証は失敗します。
ステップ 5	**exit** *threshold-rate* **log** 例： `Router(config)# exit`	コンフィギュレーション モードを終了して、特権 EXEC モードを開始します。
ステップ 6	**show auto secure config** 例： `Router# show auto secure config`	（任意）AutoSecure の設定の過程で追加されたコンフィギュレーション コマンドをすべて表示します。

AutoSecure の設定例

AutoSecure ダイアログの例を次に示します。**auto secure** コマンドを実行すると、下記のようなダイアログが自動的に表示されます。ただし、**no-interact** キーワードを指定した場合を除きます（ディセーブルになっているサービスと、イネーブルになっている機能については、このマニュアルで前述されている「管理プレーンのセキュリティ保護 （2546ページ）」および「フォワーディング プレーンのセキュリティ保護 （2549 ページ）」を参照してください）。

```
Router# auto secure
                --- AutoSecure Configuration ---
*** AutoSecure configuration enhances the security of the router but it will not make
router absolutely secure from all security attacks ***
All the configuration done as part of AutoSecure will be shown here. For more details
of why and how this configuration is useful, and any possible side effects, please refer
 to Cisco documentation of AutoSecure.
At any prompt you may enter '?' for help.
Use ctrl-c to abort this session at any prompt.
Gathering information about the router for AutoSecure
Is this router connected to internet? [no]:y
```

```
Enter the number of interfaces facing internet [1]:
Interface                  IP-Address OK? Method Status
Protocol
FastEthernet0/1/0          10.1.1.1  YES NVRAM  up down
FastEthernet1/0/0            10.2.2.2  YES NVRAM  up down
FastEthernet1/1/0            10.0.0.1  YES NVRAM  up up
Loopback0                  unassigned YES NVRAM  up up
FastEthernet0/0/0            10.0.0.2  YES NVRAM  up down
Enter the interface name that is facing internet:FastEthernet0/0/0
Securing Management plane services..
Disabling service finger
Disabling service pad
Disabling udp & tcp small servers
Enabling service password encryption
Enabling service tcp-keepalives-in
Enabling service tcp-keepalives-out
Disabling the cdp protocol
Disabling the bootp server
Disabling the http server
Disabling the finger service
Disabling source routing
Disabling gratuitous arp
Enable secret is either not configured or is same as enable password
Enter the new enable secret:abc123
Configuring aaa local authentication
Configuring console, Aux and vty lines for
local authentication, exec-timeout, transport
Configure SSH server? [yes]:
Enter the domain-name:example.com
Configuring interface specific AutoSecure services
Disabling the following ip services on all interfaces:
 no ip redirects
 no ip proxy-arp
 no ip unreachables
 no ip directed-broadcast
 no ip mask-reply
Disabling mop on Ethernet interfaces
Securing Forwarding plane services..
Enabling CEF (it might have more memory requirements on some low end
platforms)
Enabling unicast rpf on all interfaces connected to internet
Configure CBAC Firewall feature? [yes/no]:yes
This is the configuration generated:
no service finger
no service pad
no service udp-small-servers
no service tcp-small-servers
service password-encryption
service tcp-keepalives-in
service tcp-keepalives-out
no cdp run
no ip bootp server
no ip http server
no ip finger
no ip source-route
no ip gratuitous-arps
no ip identd
security authentication failure rate 10 log
enable secret 5 $1$CZ6G$GkGOnHdNJCO3CjNHHyTUA.
aaa new-model
aaa authentication login local_auth local
line console 0
 login authentication local_auth
 exec-timeout 5 0
```

```
 transport output telnet
line aux 0
 login authentication local_auth
 exec-timeout 10 0
 transport output telnet
line vty 0 4
 login authentication local_auth
 transport input telnet
ip domain-name example.com
crypto key generate rsa general-keys modulus 1024
ip ssh time-out 60
ip ssh authentication-retries 2
line vty 0 4
 transport input ssh telnet
service timestamps debug datetime localtime show-timezone msec
service timestamps log datetime localtime show-timezone msec
logging facility local2
logging trap debugging
service sequence-numbers
logging console critical
logging buffered
interface FastEthernet0/1/0
 no ip redirects
 no ip proxy-arp
 no ip unreachables
 no ip directed-broadcast
 no ip mask-reply
 no mop enabled
interface FastEthernet1/0/0
 no ip redirects
 no ip proxy-arp
 no ip unreachables
 no ip directed-broadcast
 no ip mask-reply
 no mop enabled
interface FastEthernet1/1/0
 no ip redirects
 no ip proxy-arp
 no ip unreachables
 no ip directed-broadcast
 no ip mask-reply
 no mop enabled
interface FastEthernet0/0/0
 no ip redirects
 no ip proxy-arp
 no ip unreachables
 no ip directed-broadcast
 no ip mask-reply
 no mop enabled
ip cef
interface FastEthernet0/0/0
 ip verify unicast reverse-path
ip inspect audit-trail
ip inspect dns-timeout 7
ip inspect tcp idle-time 14400
ip inspect udp idle-time 1800
ip inspect name autosec_inspect cuseeme timeout 3600
ip inspect name autosec_inspect ftp timeout 3600
ip inspect name autosec_inspect http timeout 3600
ip inspect name autosec_inspect rcmd timeout 3600
ip inspect name autosec_inspect realaudio timeout 3600
ip inspect name autosec_inspect smtp timeout 3600
ip inspect name autosec_inspect tftp timeout 30
ip inspect name autosec_inspect udp timeout 15
```

```
ip inspect name autosec_inspect tcp timeout 3600
access-list 100 deny ip any any
interface FastEthernet0/0/0
 ip inspect autosec_inspect out
 ip access-group 100 in
!
end
Apply this configuration to running-config? [yes]:yes
Applying the config generated to running-config
The name for the keys will be:ios210.example.com
% The key modulus size is 1024 bits
% Generating 1024 bit RSA keys ...[OK]
Router#
```

その他の参考資料

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『Cisco IOS Master Commands List, All Releases』
SNMP サポートの設定	SNMP サポートの設定
セキュリティ コマンド	『*Cisco IOS Security Command Reference*』

標準

標準	タイトル
PacketCable™ コントロール ポイント検出インターフェイス仕様	『*PacketCable™ Control Point Discovery Interface Specification*』（PKT-SP-CPD-I02-061013）

MIB

MIB	MIB のリンク
• CISCO-802-TAP-MIB • CISCO-IP-TAP-MIB • CISCO-MOBILITY-TAP-MIB • CISCO-TAP2-MIB • CISCO-USER-CONNECTION-TAP-MIB	選択したプラットフォーム、Cisco ソフトウェア リリース、およびフィーチャ セットの MIB を検索してダウンロードする場合は、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

RFC

RFC	タイトル
RFC-2865	『*Remote Authentication Dial In User Service (RADIUS)*』
RFC-3576	*Dynamic Authorization Extensions to Remote Authentication Dial In User Service (RADIUS)*
RFC-3924	『*Cisco Architecture for Lawful Intercept in IP Networks*』

シスコのテクニカル サポート

説明	リンク
右の URL にアクセスして、シスコのテクニカル サポートを最大限に活用してください。これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

AutoSecure に関する機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *233 : AutoSecure* に関する機能情報

機能名	リリース	機能情報
AutoSecure の管理性	Cisco IOS XE Release 2.3	この機能は、Cisco ASR 1000 シリーズのアグリゲーション サービス ルータで導入されました。 単一のコマンドライン インターフェイス（CLI）を使用することで、AutoSecure 機能ではユーザは次の機能を実行することができます。 • ネットワーク攻撃のために不正利用される可能性のある、一般的な IP サービスをディセーブルする。 • 攻撃を受けたときにネットワークの防御を支援できる IP サービスと機能をイネーブルにする。 この機能は、ルータのセキュリティ設定を簡素化し、ルータの設定も強化します。 次のコマンドが導入または変更されました。**auto secure** および **show auto secure config**

第 173 章

Kerberos の設定

Kerberos に関する情報

Kerberos は、マサチューセッツ工科大学（MIT）が開発した秘密キーネットワーク認証プロトコルであり、暗号化と認証にデータ暗号規格（DES）暗号アルゴリズムを使用します。Kerberos は、ネットワーク リソースの要求を認証するために設計されました。Kerberos は他の秘密キーシステムと同様に、ユーザーとサービスのセキュアな検証を実行する、信頼できるサードパーティの概念に基づいています。Kerberos プロトコルでは、この信頼できるサードパーティは、キー発行局（KDC）と呼ばれます。

Kerberos の主な用途は、ユーザと、そのユーザが使用するネットワーク サービスの身元が主張どおりであることを検証することです。この検証のために、信頼できる Kerberos サーバがユーザにチケットを発行します。有効期限のあるこれらのチケットは、ユーザの認定証キャッシュに保存されており、標準のユーザ名とパスワードの認証メカニズムの代わりに使用できます。

Kerberos の認定証スキームは、「シングル ログイン」という概念を表しています。この手順では、ユーザを 1 回認証することが必要で、ユーザ クレデンシャルが有効な間は（他のパスワードの暗号化を行わずに）セキュア認証が可能になります。

Cisco IOS XE ソフトウェアは Kerberos 5 をサポートするようになりました。そのため、Kerberos 5 をすでに配置している組織の場合、ルータ上で、他のネットワーク ホスト（UNIX サーバや PC など）ですでに使用している同じ Kerberos 認証データベースを使用できます。

次のネットワーク サービスは、Cisco IOS XE ソフトウェアの Kerberos 認証機能によってサポートされています。

- Telnet
- rlogin

- rsh
- rcp

（注） Kerberos クライアント サポートのシスコの実装は、MIT のコードから派生した CyberSafe が開発したコードに基づいています。そのため、シスコの Kerberos 実装は、CyberSafe Challenger 製の市販 Kerberos サーバおよび無料配布されている MIT のサーバ コードとの完全互換性テストに成功しています。

一般的な Kerberos 関連の用語と定義を下表に示します。

表 *234 : Kerberos* の用語

用語	定義
認証	ユーザやサービスが他のサービスに対して自分自身の身元を証明する手順。たとえば、クライアントがルータに対して認証したり、ルータが他のルータに対して認証したりすることができます。
許可	ネットワークまたはルータでユーザが持っている特権、および実行できるアクションをルータが判断する手段です。
クレデンシャル	認証チケット（チケット認可チケット（TGT）、サービス クレデンシャルなど）を表す総称。Kerberos クレデンシャルで、ユーザまたはサービスの ID を検証します。ネットワーク サービスがチケットを発行した Kerberos サーバを信頼することを決定すると、ユーザとパスワードを再入力する代わりにそのチケットを使用できます。クレデンシャルの有効期限は、8 時間がデフォルトの設定です。
インスタンス	Kerberos プリンシパルの承認レベル ラベル。ほとんどの Kerberos プリンシパルは、user@REALM という形式です（たとえば、smith@EXAMPLE.COM）。Kerberos インスタンスを指定した Kerberos プリンシパルは、user/instance@REALM という形式です（たとえば、smith/admin@EXAMPLE.COM）。Kerberos インスタンスは、認証が成功した場合のユーザーの承認レベルを指定するために使用できます。Kerberos インスタンスの認可マッピングを実装および実施するのは、各ネットワーク サービスのサーバ次第です。Kerberos レルム名は、大文字で指定する必要があります。
Kerberos 対応	Kerberos 証明書の基盤をサポートするように変更されたアプリケーションおよびサービス。

用語	定義
Kerberos レルム	Kerberos サーバーに登録されたユーザー、ホスト、およびネットワーク サービスで構成されるドメイン。Kerberos サーバーを信頼して、ユーザーまたはネットワーク サービスに対する別のユーザーまたはネットワーク サービスの ID を検証します。Kerberos レルムは、常に大文字にする必要があります。
Kerberos サーバ	ネットワーク ホスト上で稼働しているデーモン。ユーザーおよびネットワーク サービスはそれぞれ Kerberos サーバーに ID を登録します。ネットワーク サービスは Kerberos サーバーにクエリーを送信して、他のネットワーク サービスの認証を得ます。
キー発行局（KDC）	ネットワーク ホストで実行される Kerberos サーバとデータベース プログラム。
プリンシパル	Kerberos ID とも呼ばれ、Kerberos サーバに基づき、ユーザが誰であるか、サービスが何であるかを表します。
サービス認定証	ネットワーク サービスのクレデンシャル。この認定証は、KDC から発行されるとき、ネットワーク サービスと KDC で共有されるパスワード、およびユーザの TGT で暗号化されます。
SRVTAB	ネットワーク サービスが KDC と共有するパスワード。ネットワーク サービスは、SRVTAB（別名 KEYTAB）を使用することにより、暗号化されたサービス証明書を認証して解読します。
チケット認可チケット（TGT）	キー発行局（KDC）が認証済みユーザに発行する認定証。TGT を受け取ったユーザーは、KDC が示した Kerberos レルム内のネットワーク サービスに対して認証を得ることができます。

Kerberos クライアントのサポート操作

ここでは、Kerberos セキュリティ システムが、セキュリティ サーバとして機能する Cisco ルータと連携する方法について説明します。（便宜上または技術的な理由から）Kerberos は多様な方法でカスタマイズできますが、ネットワーク サービスにアクセスを試みるリモート ユーザは、3 レイヤのセキュリティを通過してからネットワーク サービスにアクセスする必要があります。

境界ルータに対する認証

ここでは、リモート ユーザがネットワークにアクセスを試みるときに通過する必要があるセキュリティの第 1 レイヤについて説明します。Kerberos 認証プロセスの第 1 段階は、ユーザが境界ルータに対して自身を認証することです。次のプロセスでは、ユーザが境界ルータに対して認証する方法について説明します。

1. リモート ユーザは、会社サイトのルータに対して PPP 接続を開きます。

2. ルータは、ユーザに対してユーザ名とパスワードの入力を求めます。
3. ルータは、そのユーザに関する KDC の TGT を要求します。
4. KDC は、（他の情報も含まれますが）ユーザの ID を含む暗号化済み TGT をルータに送信します。
5. ルータは、ユーザが入力したパスワードを使用して、TGT の復号化を試行します。復号化に成功すると、リモート ユーザはルータに対して認証されます。

PPP セッションの開始、および境界ルータに対する認証に成功するリモートユーザは、ファイアウォール内にいますが、ネットワーク サービスにアクセスするには KDC に対して直接認証する必要があります。これは、KDC から発行された TGT はルータに保存され、ユーザが物理的にルータにログインしない限り、追加の認証には役立ちません。

KDC からの TGT の取得

ここでは、境界ルータに対して認証されたリモート ユーザが、KDC に対して自身を認証する方法について説明します。

リモートユーザが境界ルータに対して認証すると、そのユーザは技術的にはネットワークの一部になります。つまり、ネットワークは、そのリモートユーザとユーザのマシンまたはネットワークを含むように拡張されます。ただし、リモート ユーザーがネットワーク サービスに対するアクセス権を得るには、KDC から TGT を取得する必要があります。次のプロセスでは、リモート ユーザーが KDC に対して認証する方法について説明します。

1. リモート サイトにあるワークステーションを使用するリモート ユーザーは、KINIT プログラム（Kerberos プロトコルに付属するクライアント ソフトウェアの一部）を起動します。
2. KINIT プログラムは、ユーザの ID を検索し、KDC から TGT を要求します。
3. KDC は TGT を作成します。TGT には、ユーザーの ID、KDC の ID、および TGT の有効期限が含まれます。
4. KDC は、ユーザーのパスワードをキーとして使用して、TGT を暗号化し、その TGT をワークステーションに送信します。
5. KINIT プログラムは暗号化された TGT を受信すると、ユーザーにパスワード（KDC でそのユーザー用に定義されているパスワード）の入力を求めます。
6. ユーザーが入力したパスワードを使用して KINIT プログラムが TGT を復号化できる場合、ユーザーは KDC に対して認証され、KINIT プログラムはユーザーの認定証キャッシュに TGT を保存します。

この時点で、ユーザーは TGT を持っており、KDC と安全に通信できます。その TGT を使用して、ユーザーは他のネットワーク サービスに対して認証できます。

ネットワーク サービスに対する認証の取得

次のプロセスでは、TGT を持つリモート ユーザーが、特定の Kerberos レルム内でネットワーク サービスに対して認証する方法について説明します。ここでは、ユーザーはリモート ワークステーション（Host A）上にあり、Host B にログインしようとしているとします。

1. Host A 上のユーザーは、Host B に対して Kerberos 化アプリケーション（Telnet など）を開始します。
2. Kerberos 化アプリケーションはサービス認定証要求を構築し、KDC に送信します。サービス認定証要求には、（他の情報も含まれますが）ユーザーの ID と目的のネットワーク サービスの ID が含まれます。TGT は、サービス認定証要求を暗号化するために使用されます。
3. KDC は、Host A 上のユーザーに対して発行された TGT を使用して、サービス認定証要求を復号化しようとします。KDC がパケットを復号化できる場合、要求の発行元が Host A 上の認証済みユーザーであると確認されます。
4. KDC は、サービス認定証要求に含まれるネットワーク サービス ID を記録します。
5. KDC は、Host A 上のユーザーの代理で、適切なネットワーク サービスのサービス認定証を Host B に構築します。サービス認定証には、クライアントの ID および必要なネットワーク サービスの ID が含まれます。
6. 次に、KDC はサービス認定証の暗号化を 2 回実行します。まず、認定証に指定されたネットワーク サービスと共有する SRVTAB を使用して認定証を暗号化します。次に、ユーザー（この場合は Host A 上のユーザー）の TGT を使用して結果のパケットを暗号化します。
7. KDC は、2 回暗号化された認定証を Host A に送信します。
8. Host A は、ユーザーの TGT を使用してサービス認定証の復号化を試行します。Host A がサービス認定証を復号化できる場合、その認定証の発行元が KDC であると確認されます。
9. Host A はサービス認定証を目的のネットワーク サービスに送信します。認定証は、まだ KDC とネットワーク サービスに共有されている SRVTAB で暗号化されています。
10. ネットワーク サービスは、SRVTAB を使用してサービス認定証の復号化を試行します。
11. ネットワーク サービスが認定証を復号化できる場合、その認定証の発行元が KDC であると確認されます。ネットワーク サービスは、ユーザーから間接的に送信されたデータでも、KDC から送信された復号化できるデータであれば、常に信頼します。これは、ユーザーがまず KDC で認証されているためです。

この時点で、ユーザーは Host B のネットワーク サービスに認証されます。このプロセスは、ユーザーが Kerberos レルムのネットワーク サービスにアクセスするときは毎回繰り返されます。

Kerberos を設定する方法

通信と相互認証を行う Kerberos レルムのホストと KDC について、相互に識別する必要があります。そのために、KDC 上の Kerberos データベースにホストのエントリを追加し、KDC が生成する SRVTAB ファイルを Kerberos レルムのすべてのホストに追加します。また、KDC データベースにユーザのエントリも作成します。

ここでは、Kerberos 認証済みのサーバ クライアント システムを設定する方法について説明します。内容は次のとおりです。

このセクションは、KDC 認識された UNIX ホストで Kerberos 管理プログラムをインストールし、データベースを初期化して、Kerberos レルム名とパスワードを選択していることを前提とします。これらのタスクの実行に関する手順については、Kerberos ソフトウェアに付属のマニュアルを参照してください。

（注） KDC のホスト名または IP アドレス、KDC で照会のために監視するポート番号、およびサービスを提供する Kerberos レルムの名前を書き留めます。この情報は、ルータの設定で必要になります。

Kerberos コマンドによる KDC の設定

Kerberos レルムで KDC として動作するようにホストを設定した後は、レルムのすべてのプリンシパルの KDC データベースに対してエントリを作成する必要があります。プリンシパルは、Cisco ルータおよびホスト上のネットワーク サービスの場合、またはユーザの場合があります。

Kerberos コマンドで KDC データベースにサービスを追加するには（また、既存のデータベース情報を変更するには）、以下の項のタスクを実行します。

（注） すべての Kerberos コマンド例は、オリジナルの MIT 実装の Kerberos 5 Beta 5 に基づいています。それよりも新しいバージョンでは、やや異なるインターフェイスを使用しています。

KDC データベースへのユーザーの追加

KDC にユーザーを追加し、そのユーザーの特権インスタンスを作成するには、KDC を実行するホストのルートになるために **su** コマンドを実行します。また、kdb5_edit プログラムを使用して、特権 EXEC モードで次のコマンドを使用します。

手順の概要

1. Router# **ank***username@REALM*
2. Router# **ank***username/instance@REALM*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	Router# **ank***username@REALM*	**ank**（新しいキーを追加）コマンドを使用して、ユーザーを KDC に追加します。このコマンドを実行するとパスワードの入力が求められ、ユーザはルータに対して認証するために入力する必要があります。
ステップ 2	Router# **ank***username/instance@REALM*	**ank** コマンドを使用して、ユーザの特権インスタンスを追加します。

次のタスク

たとえば、Kerberos レルム CISCO.COM のユーザ *loki* を追加するには、次の Kerberos コマンドを入力します。

```
ank loki@CISCO.COM
```

（注） Kerberos レルム名は、大文字で指定する必要があります。

ネットワーク管理がイネーブル レベルでルータに接続できるように、特権インスタンスを作成できます。たとえば、イネーブル モードを開始するためにクリア テキスト パスワードを入力する（またセキュリティを脅かす）必要がないようにできます。

新しい特権（この場合 enable ですが、任意に指定できます）を使用して *loki* のインスタンスを追加するには、次の Kerberos コマンドを入力します。

```
ank loki/enable@CISCO.COM
```

以下の各例では、パスワードの入力が求められます。このパスワードは、ユーザ *loki* がログイン時に使用できるように、ユーザに付与する必要があります。

「Kerberos インスタンス マッピングの有効化（2571 ページ）」では、Kerberos インスタンスを多様な Cisco IOS XE 特権レベルにマッピングする方法について説明します。

KDC での SRVTAB の作成

Kerberos プロトコルを使用するために認証するすべてのルータは、SRVTAB を持っている必要があります。SRVTAB の抽出の詳細については、「*SRVTAB* の抽出」を参照してください。

KDC に SRVTAB エントリを作成するには、特権 EXEC モードで次のコマンドを使用します。

コマンド	目的
Router# **ark** *SERVICE/HOSTNAME@REALM*	**ark**（add random key）コマンドを使用して、ホストまたはルータがサポートするネットワークサービスを KDC に追加します。

たとえば、*router1* という Cisco ルータ用の Kerberos 化認証サービスを Kerberos レルム CISCO.COM に追加するには、次の Kerberos コマンドを入力します。

```
ark host/router1.cisco.com@CISCO.COM
```

すべての Kerberos 化ホスト上に、認証にこの KDC を使用するすべてのネットワーク サービスに関するエントリを作成します。

SRVTAB の抽出

SRVTAB には、（他の情報も含まれますが）KDC データベースに入力したサービス プリンシパルのパスワードまたはランダムに生成されたキーが含まれます。サービス プリンシパル キーは、そのサービスを実行するホストと共有する必要があります。そのためには、SRVTAB をファイルに保存し、Kerberos レルムにあるルータおよびすべてのホストにそのファイルをコピーします。SRVTAB エントリをファイルに保存することを、SRVTAB の抽出といいます。SRVTAB を抽出するには、特権 EXEC モードで次のコマンドを使用します。

コマンド	目的
`Router# xst router-name host`	kdb5_edit コマンド **xst** を使用して、SRVTAB エントリをファイルに書き込みます。

たとえば、host/router1.cisco.com@CISCO.COM SRVTAB をファイルに書き込むには、次の Kerberos コマンドを入力します。

```
xst router1.cisco.com@CISCO.COM host
```

quit コマンドを使用して、kdb5_edit プログラムを終了します。

Kerberos プロトコルを使用するルータの設定

Kerberos レルムの定義

ルータが、Kerberos データベースに定義されているユーザを認証するには、KDC を実行するホストのホスト名または IP アドレスと Kerberos レルムの名前を知っている必要があります。また、オプションで、ホスト名またはドメイン ネーム システム（DNS）ドメインを Kerberos レルムにマッピングする機能がルータに必要です。

特定の Kerberos レルムで、指定した KDC に対して認証するようにルータを設定するには、グローバル コンフィギュレーション モードで次のコマンドを使用します。DNS ドメイン名の先頭にはドット（.）を付ける必要があります。

手順の概要

1. Router(config)# **kerberos local-realm***kerberos-realm*
2. Router(config)# **kerberos server***kerberos-realm* {*hostname* | *ip-address* } [*port-number*]
3. Router(config)# **kerberos realm** {*dns-domain* | *host* } *kerberos-realm*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	Router(config)# **kerberos local-realm***kerberos-realm*	ルータのデフォルト レルムを定義します。
ステップ 2	Router(config)# **kerberos server***kerberos-realm* {*hostname* | *ip-address* } [*port-number*]	特定の Kerberos レルムで使用する KDC、およびオプションで KDC が監視するポート番号をルータに指定します（デフォルト値は 88 です）。
ステップ 3	Router(config)# **kerberos realm** {*dns-domain* | *host* } *kerberos-realm*	（任意）ホスト名または DNS ドメインを Kerberos レルムにマッピングします。

次のタスク

（注） KDC を実行するマシンおよびすべての Kerberos 化ホストは 5 分の期限内で通信する必要があり、通信できない場合、認証は失敗します。そのため、すべての Kerberos 化マシン（特に KDC）は、ネットワーク タイム プロトコル（NTP）を実行する必要があります。

kerberos local-realm、**kerberos realm**、および **kerberos server** コマンドは、UNIX krb.conf ファイルに相当します。下記の表は、Cisco IOS XE コンフィギュレーション コマンドから Kerberos 5 コンフィギュレーション ファイル（krb5.conf）への対応一覧です。

表 *235 : Kerberos 5* のコンフィギュレーション ファイルおよびコマンド

krb5.conf ファイル	**Cisco IOS XE のコンフィギュレーション コマンド**
[libdefaults] `default_realm = DOMAIN.COM`	（コンフィギュレーション モードで） **kerberos local-realm** *DOMAIN.COM*

[domain_realm]
 	
`.domain.com = DOMAIN.COM`
 	
`domain.com = DOMAIN.COM`
	（コンフィギュレーション モードで）
	
	kerberos realm
	.domain.com
	DOMAIN.COM
	kerberos realm
	domain.com DOMAIN.COM

[realms]
 	
`kdc = DOMAIN.PIL.COM:750`
 	
`admin_server = DOMAIN.PIL.COM`
 	
`default_domain = DOMAIN.COM`
	（コンフィギュレーション モードで）
	
	kerberos server
	DOMAIN.COM 172.65.44.2
	(*172.65.44.2*
	is the example IP address for *DOMAIN.PIL.COM*
	)

Kerberos レルムの定義例については、Kerberos レルムの定義例のモジュールを参照してください。

SRVTAB ファイルのコピー

リモートユーザが Kerberos 認定証を使用してルータに対して認証できるようにするには、ルータが KDC 秘密キーを共有する必要があります。そのためには、KDC で抽出した SRVTAB をルータにコピーする必要があります。

SRVTAB ファイルを Kerberos レルムのホストにコピーする最もセキュアな方式は、ファイルを物理メディアにコピーし、各ホストの場所に行き、そのシステムに手動でファイルをコピーすることです。ルータに物理メディア ドライバがない場合、SRVTAB ファイルをルータにコピーするには、TFTP を使用してネットワークを介して転送する必要があります。

KDC からルータに対して SRVTAB ファイルをリモート コピーするには、グローバル コンフィギュレーション モードで次のコマンドを使用します。

コマンド	目的
`Router(config)# kerberos srvtab remote {hostname | ip-address} {filename}`	KDC から SRVTAB ファイルを取得します。

SRVTAB ファイルをルータから KDC にコピーする場合、**kerberos srvtab remote** コマンドでこのファイルの情報を解析し、**kerberos srvtab entry** 形式でルータの実行コンフィギュレーションに保存します。ルータをリブートしたときに SRVTAB が使用できるようにするには（KDC から取得する必要はありません）、**write memory** コンフィギュレーション コマンドを使用し、実行コンフィギュレーション（解析した SRVTAB ファイルを含みます）を NVRAM に書き込みます。

SRVTAB ファイルのコピー例については、「SRVTAB ファイルのコピー例（2572 ページ）」を参照してください。

Kerberos 認証の指定

これまでの操作でルータの Kerberos の設定が完了しました。そのため、ルータは Kerberos を使用して認証できます。次の手順は、認証するようにルータに指示することです。AAA によって Kerberos 認証が容易になるため、**aaa authentication** コマンドを入力し、認証方式として Kerberos を指定する必要があります。詳細については、「認証の設定」の章を参照してください。

認定証転送の有効化

これまでの手順で Kerberos を設定すると、Kerberos 化ルータに対して認証されているユーザは TGT を持ち、その TGT を使用してネットワーク上のホストに対して認証できます。ただし、ユーザがホストの認証後に認定証のリストを表示しようとすると、出力には Kerberos 認定証が表示されません。

Kerberos 化された Telnet、rcp、rsh、および rlogin（適切なフラグ付き）を使用するときに、ルータからネットワーク上の Kerberos 化リモート ホストに対して認証する場合、オプションで、ユーザの TGT を転送するようにルータを設定できます。

Kerberos レルムで他のホストに接続するときにユーザーの認定証を転送するように、すべてのクライアントに強制するには、グローバル コンフィギュレーション モードで次のコマンドを使用します。

コマンド	目的
`Router(config)# kerberos credentials forward`	Kerberos 認証に成功したときに、すべてのクライアントがユーザーの認定証を転送するように強制します。

認定証の転送を有効にすると、ユーザーの TGT は、認証を受ける次のホストへ自動的に転送されます。この方法で、ユーザーは Kerberos レルム内の複数のホストに接続できます。新しい TGT を取得するたびに KINIT プログラムを実行する必要はありません。

ルータに対する Telnet セッションの開始

ネットワーク内からルータに対して Telnet セッションを開始するユーザを認証するために、Kerberos を使用するには、グローバル コンフィギュレーション モードで次のコマンドを使用します。

コマンド	目的
`Router(config)# aaa authentication login {default | list-name } krb5_telnet`	Telnet を使用してルータに接続する場合、ログイン認証を設定して Kerberos 5 Telnet 認証プロトコルを使用します。

ルータに対する Telnet セッションは認証されますが、イネーブル モードを開始するには、ユーザがクリア テキスト パスワードを入力する必要があります。後述する **kerberos instance map** コマンドを使用すると、事前に定義した特権レベルでルータに対して認証できます。

暗号化された Kerberos 対応 Telnet セッションの確立

ユーザーがセキュア Telnet セッションを開始するもう 1 つの方法は、Encrypted Kerberized Telnet を使用することです。Encrypted Kerberized Telnet を使用すると、Telnet セッションを確立する前に、ユーザーは Kerberos 認定証によって認証されます。Telnet セッションは、64-bit Cipher Feedback（CFB）による 56-bit データ暗号規格（DES）暗号を使用して暗号化されます。送受信データは暗号化され、クリア テキストではないため、着信したルータまたはアクセス サーバの整合性は制御しやすくなります。

（注） この機能を使用できるのは、56-bit 暗号化イメージを持っている場合だけです。56 ビット DES 暗号化は、米国政府の輸出管理規制の対象となります。

ルータからリモート ホストに対して、Encrypted Kerberized Telnet セッションを確立するには、EXEC コンフィギュレーション モードで次のコマンドのいずれかを使用します。

コマンド	目的

`Router(config)# connect host [port] /encrypt kerberos`
 	
または
 	
`Router(config)# telnet host [port] /encrypt kerberos`
	暗号化された Telnet セッションを確立します。

ユーザが Cisco ルータからリモート ホストに対する Telnet セッションを開始すると、ルータとリモートホストは、Kerberos 認定証を使用してユーザを認証するためにネゴシエートします。この認証に成功すると、ルータとリモートホストは、暗号化を使用するかどうかをネゴシエートします。このネゴシエーションに成功すると、着信および発信トラフィックは、64-bit CFB による 56-bit DES を使用して暗号化されます。

ユーザが、リモート ホストから Kerberos 認証用に設定された Cisco ルータに対してダイヤルインすると、Telnet セッションに暗号化を使用するかどうかについて、ホストとルータでネゴシエーションが試行されます。このネゴシエーションに成功すると、ルータは Telnet セッション中のすべての発信データを暗号化します。

暗号化のネゴシエーションに成功しなかった場合、セッションは終了し、ユーザは、暗号化された Telnet セッションの確立に失敗したというメッセージを受信します。

リモート ホストから双方向暗号化をイネーブル化する方法については、リモート ホスト デバイスのマニュアルを参照してください。

暗号化された Kerberos 対応 Telnet を使用してセキュアな Telnet セッションを開始する例については、この章で後述する「暗号化された Telnet セッションの例 （2573 ページ）」を参照してください。

必須の Kerberos 認証の有効化

セキュリティの追加レイヤとして、リモートユーザがルータに対して認証した後に、ユーザは Kerberos 化 Telnet、rlogin、rsh、および rcp だけを使用してネットワーク上の他のサービスに対して認証できます。Kerberos 認証を必須にしていない状態で Kerberos 認証に失敗すると、アプリケーションは、そのネットワーク サービスのデフォルト認証方式を使用して、ユーザーの認証を試行します。たとえば、Telnet および rlogin はパスワードの入力を求め、rsh はローカル rhost ファイルを使用して認証を試行します。

Kerberos 認証を必須にするには、グローバル コンフィギュレーション モードで次のコマンドを使用します。

コマンド	目的
`Router(config)# kerberos clients mandatory`	リモート ホストとの間で Kerberos プロトコルをネゴシエートできない場合、Telnet、rlogin、rsh、および rcp を失敗に設定します。

Kerberos インスタンス マッピングの有効化

「KDC での SRVTAB の作成（2565 ページ）」で説明したように、KDC データベースにユーザの管理インスタンスを作成することができます。**kerberos instance map** コマンドを使用すると、その管理インスタンスを Cisco IOS XE 特権レベルにマッピングできます。それによって、事前定義した特権レベルで、ユーザーはルータに対するセキュア Telnet セッションを開くことができます。イネーブルモードを開始するためにクリアテキストのパスワードを入力する必要はありません。

Kerberos インスタンスを Cisco IOS XE 特権レベルにマッピングするには、グローバル コンフィギュレーション モードで次のコマンドを使用します。

コマンド	目的
`Router(config)# kerberos instance map` *instance privilege-level*	Kerberos インスタンスを Cisco IOS XE 特権レベルにマッピングします。

KDC データベースにユーザ *loki*（たとえば、*loki/admin*）の Kerberos インスタンスがある場合、ユーザ *loki* は、loki/admin としてルータに対して Telnet セッションを開始し、特権レベル 15 で自動的に認証します。インスタンス「admin」は特権レベル 15 にマッピングされるという前提です。（ルータに対する Telnet セッションの開始 （2569 ページ）を参照してください。）

Cisco IOS XE コマンドは、 **privilege level** コマンドを使用して、さまざまな権限レベルに設定できます。

Kerberos インスタンスを Cisco IOS XE 権限レベルにマッピングした後、ユーザーがログインするたびに Kerberos インスタンスをチェックするようにルータを設定する必要があります。マッピングされた Kerberos インスタンスに基づいて、ユーザーに EXEC シェルの実行を許可するかどうかを決定するための承認を実行するには、**krb5-instance** キーワードを指定して **aaa authorization** コマンドを使用します。詳細については、「認可の設定」の章を参照してください。

Kerberos の監視とメンテナンス

現在のユーザの認定証を表示または削除するには、EXEC モードで次のコマンドを使用します。

手順の概要

1. Router# **show kerberos creds**
2. Router# **clear kerberos creds**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	Router# **show kerberos creds**	現在のユーザの認定証キャッシュに含まれる認定証を一覧表示します。
ステップ 2	Router# **clear kerberos creds**	転送済みの認定証を含め、現在のユーザの認定証キャッシュに含まれるすべての認定証を破棄します。

Kerberos 設定の例

Kerberos レルムの定義例

デフォルトの Kerberos レルムとして CISCO.COM を定義するには、次のコマンドを使用します。

```
kerberos local-realm CISCO.COM
```

CISCO.COM KDC が、ホスト 10.2.3.4 でポート番号 170 を使用して実行されていることをルータに示すには、次の Kerberos コマンドを使用します。

```
kerberos server CISCO.COM 10.2.3.4 170
```

DNS ドメイン cisco.com を Kerberos レルム CISCO.COM にマッピングするには、次のコマンドを使用します。

```
kerberos realm.cisco.com CISCO.COM
```

SRVTAB ファイルのコピー例

host123.cisco.com というホスト上の SRVTAB ファイルを、router1.cisco.com というルータにコピーするには、次のようなコマンドを使用します。

```
kerberos srvtab remote host123.cisco.com router1.cisco.com-new-srvtab
Valid Starting          Expires                 Service Principal
13-May-1996 14:59:44    13-May-1996 23:00:45    krbtgt/CISCO.COM@CISCO.COM
chet-2500# show privilege
Current privilege level is 15
chet-2500# q
Connection closed by foreign host.
chet-ss20% telnet chet-2500
Trying 172.16.0.0 ...
Connected to chet-2500.cisco.com.
Escape character is '^]'.
User Access Verification
Username: chet/restricted
Password:
```

```
chet-2500# show kerberos creds
Default Principal:  chet/restricted@CISCO.COM
Valid Starting          Expires                 Service Principal
13-May-1996 15:00:32    13-May-1996 23:01:33    krbtgt/CISCO.COM@CISCO.COM
chet-2500# show privilege
Current privilege level is 3
chet-2500# q
Connection closed by foreign host.
chet-ss20%
```

暗号化された Telnet セッションの例

ルータから「host1」というリモート ホストに対して、暗号化された Telnet セッションを確立する例を示します。

Router> **telnet host1 /encrypt kerberos**

その他の参考資料

次の項では、No Service Password-Recovery 機能の関連資料を示します。

関連資料

関連項目	マニュアル タイトル
パスワードの設定、変更および忘失パスワードの回復	「Configuring Security with Passwords, Privilege Levels and, Login Usernames for CLI Sessions on Networking Devices」機能モジュール
システム イメージのロードと再起動	「Using the Cisco IOS Integrated File System」機能モジュール
セキュリティ コマンド：コマンド構文の詳細、コマンドモード、コマンド履歴、デフォルト設定、使用上の注意事項、および例	『*Cisco IOS Security Command Reference*』
Cisco IOS コマンド	『Cisco IOS Master Commands List, All Releases』

標準

標準	タイトル
なし	--

MIB

MIB	MIB のリンク
なし	選択したプラットフォーム、Cisco IOS リリース、およびフィーチャ セットに関する MIB を探してダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

RFC

RFC	タイトル
この機能でサポートが追加または変更された RFC はありません。	--

シスコのテクニカル サポート

説明	リンク
シスコのサポート Web サイトでは、シスコの製品やテクノロジーに関するトラブルシューティングにお役立ていただけるように、マニュアルやツールをはじめとする豊富なオンライン リソースを提供しています。 お使いの製品のセキュリティ情報や技術情報を入手するために、Cisco Notification Service（Field Notice からアクセス）、Cisco Technical Services Newsletter、Really Simple Syndication（RSS）フィードなどの各種サービスに加入できます。 シスコのサポート Web サイトのツールにアクセスする際は、Cisco.com のユーザ ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

Kerberos の設定に関する機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *236 : Kerberos* の設定に関する機能情報

機能名	リリース	機能情報
暗号化された Kerberos 対応 Telnet	Cisco IOS XE Release 2.1	Encrypted Kerberized Telnet を使用すると、Telnet セッションを確立する前に、ユーザーは Kerberos 認定証によって認証されます。Telnet セッションは、64-bit Cipher Feedback（CFB）による 56-bit データ暗号規格（DES）暗号を使用して暗号化されます。送受信データは暗号化され、クリア テキストではないため、着信したルータまたはアクセス サーバの整合性は制御しやすくなります。 Cisco IOS XE Release 2.1 では、Cisco ASR 1000 シリーズ Aggregation Services Router にこの機能が実装されました。 次のコマンドが導入または変更されました。**connect** および **telnet**。
Kerberos V クライアントのサポート	Cisco IOS XE Release 2.1	Kerberos 5 のサポートでは、Kerberos 5 をすでに配置している組織は、ルータ上で、他のネットワーク ホスト（UNIX サーバや PC など）ですでに使用している同じ Kerberos 認証データベースを使用できます。 Cisco IOS XE Release 2.1 では、Cisco ASR 1000 シリーズ Aggregation Services Router にこの機能が実装されました。

第 174 章

合法的傍受アーキテクチャ

合法的傍受（LI）機能は、法執行機関（LEA）の要件を満たす際にサービス プロバイダーをサポートし、管轄または行政命令によって承認されている電子サーベイランスを提供します。サーベイランスは、エッジ ルータを通過する Voice over Internet Protocol（VoIP）またはデータ トラフィックを傍受するため、盗聴を利用して実行されます。LEA は、ターゲットのサービス プロバイダーに盗聴を要求します。サービス プロバイダーには、IP セッションを使用してその個人が送受信するデータ通信を傍受する責任があります。

このマニュアルでは、Cisco Service Independent Intercept アーキテクチャと PacketCable Lawful Intercept アーキテクチャを含む、LI アーキテクチャについて説明します。また、LI 機能の構成要素と、システムで LI 機能を設定するための手順についても説明します。

Cisco IOS XE リリース 2.5 以前は、PPP セッションはアカウンティング セッションに基づいてタップされました。回線 ID ベースのタッピングは、Cisco IOS XE リリース 2.5 で導入されました。

Cisco IOS XE リリース 2.6 では、ユーザ セッションはイーサネット（PPPoE）回線 ID タグを介する独自の PPP に基づいてタップされます。この回線 ID タグは、デバイスの PPPoE ユーザ セッションの固有のパラメータとして機能します。タップされたユーザ セッションは SNMP を使ってプロビジョニングされ、ユーザ セッションのデータ パケットおよび RADIUS 認証のデータ パケットはタップされます。

合法的傍受の前提条件

Cisco LI MIB ビューへのアクセスは、メディエーションデバイスと、ルータ上の合法的傍受について知っておく必要があるシステム管理者に制限されます。MIB にアクセスするには、ルータ上でレベル 15 のアクセス権がユーザに必要です。

メディエーション デバイスとの通信

ルータがメディエーションデバイスと通信して合法的傍受を実行するには、次の構成要件が満たされている必要があります。

- ルータとメディエーション デバイスの両方のドメイン名が、ドメイン ネーム システム（DNS）に登録されている必要があります。

DNS で、ルータの IP アドレスは、通常はルータ上の FastEthernet0/0/0 インターフェイスのアドレスです。

- メディエーション デバイスに Access Function（AF）および Access Function Provisioning Interface（AFPI）が必要です。
- メディエーション デバイスを、CISCO-TAP2-MIB ビューにアクセスできるシンプル ネットワーク管理プロトコル（SNMP）ユーザ グループに追加する必要があります。グループに追加するユーザとして、メディエーション デバイスのユーザ名を指定します。

メディエーション デバイスを CISCO-TAP2-MIB ユーザとして追加するときに、必要に応じてメディエーションデバイスの認可パスワードを指定できます。パスワードの長さは、最低 8 文字である必要があります。

合法的傍受の制約事項

一般的な制約事項

ルータで LI を設定するためのコマンドライン インターフェイス（CLI）はありません。すべてのエラー メッセージは、メディエーション デバイスに SNMP 通知として送信されます。すべての傍受は、SNMPv3 だけを使用してプロビジョニングされます。

合法的傍受では SUP HA がサポートされません。SUP スイッチオーバーの後に LI 設定を再適用する必要があります。このイベント用に SNMP トラップが生成されます。

合法的傍受 MIB

合法的傍受について知る必要があるメディエーション デバイスとユーザだけに LI MIB へのアクセスが許可されます。

Cisco LI MIB は、その機密性から、LI 機能をサポートしているソフトウェア イメージだけで使用できます。これらの MIB には、Network Management Software MIBs Support ページ（http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml）からはアクセスできません。

SNMP 通知

LI の SNMP 通知は、メディエーション デバイス上のユーザ データグラム プロトコル（UDP）ポート 161 に送信する必要があります。ポート 162（SNMP のデフォルト）ではありません。

合法的傍受に関する情報

合法的傍受の概要

LI は、司法当局（LEA）が、司法命令または行政命令の許可に従って、電子的監視を行うためのプロセスです。ますます多くの法律が採択され、規制が施行されるのに伴い、サービス プロバイダー（SP）やインターネット サービス プロバイダー（ISP）は、許可された電子監視を明示的にサポートするネットワークを実装する必要性に迫られています。LI の指令に従う必要がある SP または ISP の種類は、国によって大きく異なります。米国での LI への準拠は、Commission on Accreditation for Law Enforcement Agencies（CALEA）で規定されています。

シスコでは、LI に対し、PacketCable と Service Independent Intercept の 2 つのアーキテクチャをサポートしています。LI コンポーネントだけでは、該当する規制に準拠できません。LI コンポーネントは、SP および ISP が、LI 準拠のネットワークを構築するために使用可能なツールを提供します。

Cisco Service Independent Intercept アーキテクチャ

『Cisco Service Independent Intercept Architecture Version 3.0』では、Cisco BTS 10200 Softswitch コール エージェント バージョン 5.0 を非 PacketCable ネットワークで使用した、VoIP ネットワーク向けの LI の実装について説明しています。Packet Cable Event Message 仕様バージョン 1.5-I01 は、コール識別情報と、コールの内容に対する Cisco Tap MIB バージョン 2.0 を提供するために使用されます。

『Cisco Service Independent Intercept Architecture Version 2.0』では、Cisco BTS 10200 Softswitch コール エージェント バージョン 4.4 および 4.5 を非 PacketCable ネットワークで使用した、VoIP ネットワーク向けの LI の実装について説明しています。PacketCable ネットワークではありませんが、PacketCable Event Messages Specification バージョン I08 は、コール識別情報と、コール内容に対する Cisco Tap MIB のバージョン 1.0 またはバージョン 2.0 を提供するために引き続き使用されています。『*Cisco Service Independent Intercept Architecture Version 2.0*』では、IP アドレスとセッション ID の両方でデータを傍受するための追加機能について説明しています。これは、どちらも Cisco Tap MIB（CISCO-TAP2-MIB）のバージョン 2.0 でサポートされています。

『Cisco Service Independent Intercept Architecture Version 1.0』では、Cisco BTS 10200 Softswitch コール エージェント バージョン 3.5 および 4.1 を非 PacketCable ネットワークで使用した、VoIP

ネットワーク向けの LI の実装について説明しています。PacketCable ネットワークではありませんが、PacketCable Event Message Specification バージョン I03 は、コール識別情報と、コール内容に対する Cisco Tap MIB（CISCO-TAP-MIB）のバージョン 1.0 を提供するために引き続き使用されています。IP アドレスによる単純なデータの傍受についても説明されています。

PacketCable 合法的傍受アーキテクチャ

『*PacketCable Lawful Intercept Architecture for BTS Version 5.0*』では、PacketCable Event Messages Specification バージョン 1.5-I01 に準拠した PacketCable ネットワークで、Cisco BTS 10200 Softswitch コール エージェント バージョン 5.0 を使用した、VoIP 向けの LI の実装について説明しています。

『*PacketCable Lawful Intercept Architecture for BTS Versions 4.4 and 4.5*』では、Cisco BTS 10200 Softswitch コール エージェント バージョン 4.4 および 4.5 を、PacketCable Event Messages Specification バージョン I08 に準拠した PacketCable ネットワークで使用した、VoIP 向けの LI の実装について説明しています。

『 PacketCable Lawful Intercept Architecture for BTS Versions 3.5 and 4.1 』では、Cisco Broadband Telephony Softswitch (BTS) 10200 Softswitch コール エージェント バージョン 3.5 および 4.1 を、PacketCable Event Message Specification バージョン I03 に準拠した PacketCable ネットワークで使用した、Voice over IP（VoIP）向けの LI の実装について説明しています。

『*PacketCable Control Point Discovery Interface Specification* 』では、指定された IP アドレスのコントロールポイントを発見するために使用可能な IP ベースのプロトコルが定義されています。コントロール ポイントとは、Quality of Service（QoS）操作、LI コンテンツ タッピング操作、その他の操作を実行可能な場所です。

CISCO ASR 1000 シリーズ ルータ

Cisco ASR 1000 シリーズ アグリゲーション サービス ルータは、通常および広帯域（加入者ごと）の 2 種類の LI をサポートしています。広帯域の盗聴は、アクセス サブインターフェイスおよびトンネル インターフェイス上で実行します。通常の盗聴は、アクセス サブインターフェイス、トンネル インターフェイス、および物理インターフェイス上で実行します。内部インターフェイス上では盗聴は不要であり、実行されません。ルータは、ターゲット トラフィックが使用しているインターフェイスに基づいて、実行する盗聴の種類を決定します。

Cisco ASR 1000 シリーズ ルータ上の LI は、次の 1 つ以上のフィールドの組み合わせに基づいてトラフィックを傍受できます。

- 宛先 IP アドレスとマスク（IPv4 または IPv6 アドレス）
- 宛先ポートまたは宛先ポートの範囲
- 送信元 IP アドレスとマスク（IPv4 または IPv6 アドレス）
- 送信元ポートまたは送信元ポート範囲
- プロトコル ID

- Type of Service（TOS）
- ルータ内で *vrf-tableid* 値に変換される Virtual Routing and Forwarding（VRF）名
- 加入者（ユーザ）接続 ID

Cisco ASR 1000 シリーズ ルータ上の LI の実装は、SNMP3 を使用してプロビジョニングされ、次の機能がサポートされています。

- RADIUS セッションは傍受し、次のいずれかの方法で実行できます。
  - アクセス許可パケットを介した傍受では、セッションの開始時に傍受が開始されるようにできます。
  - CoA 要求パケットによる傍受では、ルータがセッション中に傍受を開始または停止することができます。
- 通信内容の傍受。ルータは、傍受した各パケットを複製し、パケットのコピーを UDP ヘッダーでカプセル化されたパケットに（設定された CCCid とともに）格納します。ルータは、カプセル化したパケットを LI メディエーション デバイスに送信します。複数の合法的傍受が同じデータ フローに対して設定されている場合でも、パケットの 1 つのコピーだけメディエーション デバイスに送信されます。必要に応じて、メディエーション デバイスは各 LEA に対しパケットを複製できます。
- IPv4、IPv4 マルチキャスト、IPv6、および IPv6 マルチキャストフローの傍受。

VRF 対応 LI

VRF 対応 LI は、特定のバーチャル プライベート ネットワーク（VPN）での IPv4 データの LI 盗聴をプロビジョニングする機能です。この機能により、LEA は、その VPN 内のターゲット データを合法的に傍受できます。VRF ベースの LI タップを受けるのは、その VPN 内の IPv4 データのみです。

VRF 対応の LI は、次の種類のトラフィックに対して使用できます。

- ip2ip
- ip2tag（IP から MPLS）
- tag2ip（MPLS から IP）

VPN ベースの IPv4 タップをプロビジョニングするために、LI 管理機能（メディエーション デバイスで動作します）は、CISCO-IP-TAP-MIB を使用して、ターゲットの VPN が使用している VRF テーブルの名前を特定します。VRF 名は、タップを実行するために LI をイネーブルにする VPN インターフェイスを選択するのに使用します。

ルータは、傍受するトラフィックと、傍受したパケットを送信するメディエーションデバイスを、VRF 名（および送信元および宛先アドレス、送信元および宛先ポート、およびプロトコル）に基づいて決定します。

（注） Cisco-IP-TAP-MIB を使用する場合、VRF 名がストリーム エントリで指定されていない場合、デフォルトでグローバル IP ルーティング テーブルが使用されます。

合法的傍受 MIB

Cisco LI MIB は、その機密性から、LI 機能をサポートしているソフトウェア イメージだけで使用できます。これらの MIB には、Network Management Software MIBs Support ページ（http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml）からはアクセスできません。

合法的傍受 MIB へのアクセスの制限

合法的傍受について知る必要があるメディエーション デバイスとユーザだけに LI MIB へのアクセスを許可する必要があります。これらの MIB へのアクセスを制限するには、次の作業を実行する必要があります。

1. Cisco LI MIB を含むビューを作成します。
2. このビューへの読み取りおよび書き込みアクセス権を持つ SNMP ユーザ グループを作成します。このユーザ グループに割り当てられたユーザだけが、MIB の情報にアクセスできます。
3. ユーザをシスコ LI ユーザ グループに追加し、合法的傍受に関連する MIB および情報にアクセスできるユーザを定義します。このグループのユーザとして、メディエーションデバイスを追加してください。追加しないと、ルータで合法的傍受を実行できません。

詳細は、「合法的傍受 MIB の制限付き SNMP ビューの作成」を参照してください。

（注） Cisco LI MIB ビューへのアクセスは、メディエーション デバイスと、ルータ上の合法的傍受について知っておく必要があるシステム管理者に制限されます。MIB にアクセスするには、ルータ上でレベル 15 のアクセス権がユーザに必要です。

RADIUS ベースの合法的傍受

RADIUS ベースの合法的傍受ソリューションを使用すると、傍受要求は RADIUS サーバからネットワーク アクセス サーバ（NAS ）またはレイヤ 2 トンネル プロトコル アクセス コンセントレータ（LAC）に（アクセス許可パケットまたは認可変更（CoA）要求パケットを介して）送信されるようになります。PPP または L2TP セッションとやり取りされるすべてのトラフィック データは、仲介デバイスに渡されます。RADIUS ベースの合法的傍受のもう 1 つの利点は、ソリューションの同期です。すべてのターゲット トラフィックを傍受するように、タップはアクセス許可パケットで設定されます。

傍受要求は、SNMPv3 メッセージによって仲介デバイスで開始されるため、特定の IP アドレスから送受信されるすべてのトラフィック データは仲介デバイスに渡されます。IP アドレスに基づいた傍受は、IPアドレスがセッションに割り当てられるまでセッションがタップされるのを防ぎます。

RADIUSベースの合法的傍受機能は、次のモードの合法的傍受にハイ アベイラビリティ（HA）サポートを提供します。

- 新しいセッションのアクセス許可ベースの LI
- 既存のセッションの CoA ベースの LI

RADIUSベースのLI HAは、RADIUSベースのプロビジョニングのみをサポートします。SNMPベースのプロビジョニングはサポートされません。

傍受の動作

傍受要求がアクセス許可パケット内で動作するしくみ

傍受ターゲットが接続の確立を開始するとき、アクセス要求パケットはRADIUSサーバに送信されます。RADIUS サーバは、4 つの RADIUS 属性を含むアクセス許可パケットで応答します。

NAS または LAC は値 1 の LI-Action 属性を受け取り、新しいセッションの開始時に NAS または LAC でトラフィック データを複製できるようにします。また、属性、MD IP アドレス、およびMDポート番号を通して指定された仲介デバイスに複製されたデータを転送できるようにします。

（注） NASまたはLACが新しいセッションのトラフィック データの傍受を開始することができなければ、セッションは確立されません。

アカウンティングが（**aaa accounting network** コマンドおよび **aaa accounting send stop-record authentication failure** コマンドを介して）イネーブル化されると、アカウンティング停止パケットは、Acct-Termination-Cause 属性（49）が 15 に設定されて送信される必要があります。つまり、サービスは利用できないということです。

傍受要求が CoA 要求パケット内で動作するしくみ

セッションが傍受ターゲットに対して確立された後、次のタスクに CoA 要求パケットを使用できます。

- 既存のセッションの傍受の開始。LI-Action の属性は 1 に設定されます。
- 既存のセッションの傍受の停止。LI-Action の属性は 0 に設定されます。
- ダミーの傍受要求の発行。LI-Action の属性は 2 に設定されます。NAS または LAC は、どのセッションの傍受も実行することはできません。代わりに、CoA要求パケットで指定されている Acct-Session-Id 属性値に基づいてセッションを検索します。セッションが存在す

ると、NASまたはLACはRADIUSサーバへCoAの確認応答（ACK）を送信します。セッションがなければ、NASまたはLACは「セッションが見つかりません」のエラー メッセージを発行します。

各ケースでRADIUSサーバは、特定の属性とAcct-Session-Id属性のCoA要求パケットを送信する必要があります。これらの属性はそれぞれ、パケットである必要があります。

Acct-Session-Id属性は傍受されるセッションを識別します。Acct-Session-Id属性は、アクセス要求パケットまたはアカウンティング停止パケットから取得できます。

セッションがタップされセッションが終了すると、タップが停止します。アクセス許可が開始タップを示すか、CoA要求がセッションを開始するように送信されることを示さない限り、加入者のログが戻るときにセッションは開始されません。

（注） CoA要求パケットの頻度は、10分ごとに1つの要求のレートを超えることはありません。

Service Independent Intercept（SII）

シスコでは、サービスプロバイダーカスタマーの合法的傍受のサポート要件に対応するため、Service Independent Intercept（SII）アーキテクチャを開発しました。SIIアーキテクチャは、コンテンツの傍受アクセスポイント（IAP）として機能するシスコ機器とメディエーションデバイス間に、明確に定義されたオープン インターフェイスを提供します。SIIアーキテクチャのモジュラ特性により、サービスプロバイダーは、特定のネットワーク要件と警察当局の収集機能へのインターフェイスに対する地域的な標準ベースの要件とを満たす最適なメディエーション デバイスを選択できます。

メディエーションデバイスはSNMPv3を使用してコール接続（CC）IAPを指示し、CCを複製してメディエーション デバイスにコンテンツを送信します。CC IAPは、エッジルータまたは音声のトランキング ゲートウェイのいずれか、およびエッジ ルータまたはデータのアクセスサーバのいずれかにできます。

セキュリティを強化し、SNMPv3脆弱性を緩和するには、次のタスクが必要です。

信頼できるホストへのアクセス制限（暗号化なし）

SNMPv3は、セキュリティ モデルとセキュリティ レベルの両方をサポートします。セキュリティモデルは、ユーザおよびユーザに属するグループに合わせて設定される認証方式です。セキュリティ レベルとは、セキュリティ モデル内で許可されるセキュリティのレベルです。セキュリティ モデルとセキュリティ レベルの組み合わせによって、SNMPパケットを処理するときに適用されるセキュリティ メカニズムが決定されます。

さらに、名前付きアクセス リストのSNMPサポート機能により、いくつかのSNMPコマンドに、標準の名前付きアクセス コントロール リスト（ACL）へのサポートが追加されます。

新しいSNMPグループ、またはSNMPユーザーをSNMPビューにマップするテーブルを設定するには、グローバル コンフィギュレーション モードで**snmp-server group**コマンドを使用します。

```
access-list my-list permit ip host 10.10.10.1
snmp-server group my-group v3 auth access my-list
```

この例では、**my-list** という名前のアクセス リストは 10.10.10.1 以降の SNMP トラフィックのみ許可します。次にこのアクセス リストは、**my-group** という名前の SNMP グループに適用されます。

合法的傍受をするトラフィックの暗号化および信頼できるホストへのアクセス制限

ルータ（コンテンツインターセプトアクセスポイント（IAP））と仲介デバイス（MD）間で傍受されたトラフィックを暗号化することを強く推奨します。

次のように設定する必要があります。

- ルータの暗号化およびMDの暗号化クライアント、またはトラフィックを複合化するためMD に関連付けられたルータを設定します。
- 信頼できるホストへのアクセスを制限します。
- VPN クライアントを設定します。

ルータの暗号化の設定

最初に、認証、許可、およびアカウンティング（AAA）パラメータを設定します。次に、パラメータを設定する例を示します。

```
aaa authentication login userauthen local
username <username> password 0 <password>
```

次の例は、内部データベースを使用しています。ただし、認証を実行するように、外部認証サーバを指定できます。

AAA パラメータを設定した後、Internet Security Association and Key Management Protocol（ISAKMP）ポリシーとクリプト マップを設定します。次の例では、フェーズ 1（Internet Key Exchange（IKE））の暗号化プロトコルとして事前共有キー、Diffie-Hellman（DH）グループ 2 および AES 256 を使用します。クリプト マップはダイナミック マップと呼ばれ、VPN グループはLI グループと呼ばれます。アクセス リスト 108 によって、ルータに許可されるトラフィックが定義されます（この状況で ip プールは 10.1.1.254 を介した 10.1.1.1 です）。

```
crypto isakmp policy 1
encr aes 256
authentication pre-share
group 2
!
crypto isakmp client configuration group LI-group
key <password>
dns 10.10.10.10
wins 10.10.10.20
domain cisco.com
pool ippool
acl 108
!
!
crypto ipsec transform-set myset esp-3des esp-sha-hmac
```

```
!
crypto dynamic-map dynmap 10
set transform-set myset
!
!
crypto map clientmap client authentication list userauthen
crypto map clientmap isakmp authorization list groupauthor
crypto map clientmap client configuration address respond
crypto map clientmap 10 ipsec-isakmp dynamic dynmap
!
!
interface GigabitEthernet0/3
ip address <IP address of LI-enabled router> 255.255.255.0
crypto map clientmap
!
!
ip local pool ippool 10.1.1.1 10.1.1.254
!
!
access-list 108 permit ip  10.1.1.0 0.0.0.255 host 10.0.24.4 <IP address of LI-enabled
router>
```

信頼できるホストへのアクセス制限（暗号化あり）

次の例は、VPN クライアントの IP プール（10.1.1.0/24）のみを許可する ACL の作成方法と、SNMPv3 グループへのその ACL の割り当て方法を示しています。

```
access-list my-list permit ip 10.1.1.0 0.0.0.255
snmp-server group my-group v3 auth access my-list
```

VPN クライアントの設定

```
See the
 Installing the VPN Client
 document to download and configure the Cisco VPN Client for Solaris. See the
Cisco VPN Client installation instructions
 document to download and configure the Cisco VPN Client for other operating systems.
```

合法的傍受の設定方法

ルータで合法的傍受をプロビジョニングするための直接のユーザ コマンドはありませんが、LI MIB へのアクセスの有効化、SNMP 通知の設定、LI RADIUS セッション機能のイネーブル化など、いくつかの設定作業を実行する必要があります。ここでは、必要なタスクの実行方法について説明します。

合法的傍受 MIB の制限付き SNMP ビューの作成

ユーザを作成して、シスコの合法的傍受 MIB を含む SNMP ビューに割り当てるには、ここに示す手順を実行します。

始める前に

- コマンドは、レベル 15 のアクセス権で、グローバル コンフィギュレーション モードで実行する必要があります。
- デバイスで SNMPv3 が設定されている必要があります。

手順の概要

1. **enable**
2. **configure terminal**
3. **aaa intercept**
4. **snmp-server view** *view-name MIB-name* **included**
5. **snmp-server view** *view-name MIB-name* **included**
6. **snmp-server view** *view-name MIB-name* **included**
7. **snmp-server group** *group-name* **v3 noauth read** *view-name* **write** *view-name*
8. **snmp-server user** *user-name group-name* **v3 auth md5** *auth-password*
9. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**aaa intercept** 例： `Device(config)# aaa intercept`	デバイスで合法的傍受をイネーブルにします。 • このコマンドが削除されたときに許可のないユーザが傍受を停止できないように、このコマンドを高い管理セキュリティに関連付けます。 （注） **aaa intercept** コマンドは、IP セッションを使用した盗聴の設定に必要です。
ステップ 4	**snmp-server view** *view-name MIB-name* **included** 例： `Device(config)# snmp-server view exampleView ciscoTap2MIB included`	CISCO-TAP2-MIB を含む SNMP ビューを作成します（ここで、*exampleView* は、MIB に対して作成するビューの名前です）。 • この MIB は、通常とブロードバンドの両方の合法的傍受に必要です。

	コマンドまたはアクション	目的
ステップ 5	**snmp-server view** *view-name MIB-name* **included** 例： `Device(config)# snmp-server view exampleView ciscoIpTapMIB included`	CISCO-IP-TAP-MIB を SNMP ビューに追加します。
ステップ 6	**snmp-server view** *view-name MIB-name* **included** 例： `Device(config)# snmp-server view exampleView cisco802TapMIB included`	CISCO-802-TAP-MIB を SNMP ビューに追加します。
ステップ 7	**snmp-server group** *group-name* **v3 noauth read** *view-name* **write** *view-name* 例： `Device(config)# snmp-server group exampleGroup v3 noauth read exampleView write exampleView`	LI MIB ビューにアクセス可能な SNMP ユーザ グループを作成し、グループのビューに対するアクセス権を定義します。
ステップ 8	**snmp-server user** *user-name group-name* **v3 auth md5** *auth-password* 例： `Device(config)# snmp-server user exampleUser exampleGroup v3 auth md5 examplePassword`	指定したユーザ グループにユーザを追加します。
ステップ 9	**end** 例： `Device(config)# end`	現在のコンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

次の作業

これで、メディエーション デバイスは合法的傍受 MIB にアクセスし、SNMP の **set** および **get** 要求を発行して、ルータ上で合法的傍受を設定および実行できるようになります。ルータがメディエーション デバイスに SNMP 通知を送信するよう設定する方法については、「合法的傍受のための SNMP 通知のイネーブル化」を参照してください。

合法的傍受のための SNMP 通知のイネーブル化

SNMP は、合法的傍受イベントについての通知を自動的に生成します。合法的傍受通知をメディエーション デバイスに送信するようにルータを設定するには、ここに示す手順を実行します。

始める前に

- コマンドは、レベル 15 のアクセス権で、グローバル コンフィギュレーション モードで実行する必要があります。
- ルータで SNMPv3 が設定されている必要があります。

手順の概要

1. **enable**
2. **configure terminal**
3. **snmp-server host** *ip-address* **community-string udp-port** *port notification-type*
4. **snmp-server enable traps snmp authentication linkup linkdown coldstart warmstart** *and* **snmp-server enable traps rf**
5. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**snmp-server host** *ip-address* **community-string udp-port** *port notification-type* 例： `Device(config)# snmp-server 10.2.2.1 community-string udp-port 161 udp`	メディエーション デバイスの IP アドレスと、通知要求とともに送信されるパスワードに似たコミュニティ ストリングを指定します。 • 合法的傍受では、**udp-port** は 162（SNMP のデフォルト）ではなく 161 とする必要があります。

ステップ 4	**snmp-server enable traps snmp authentication linkup linkdown coldstart warmstart** *and* **snmp-server enable traps rf**
	例：
	`Device(config)# snmp-server enable traps snmp authentication linkup linkdown coldstart warmstart`
	`Device(config)# snmp-server enable traps rf`
		RFC 1157 通知をメディエーション デバイスに送信するようにルータを設定します。
		これらの通知は、認証の失敗、リンク ステータス（アップまたはダウン）、およびルータ再起動を示します。

	コマンドまたはアクション	目的
ステップ 5	**end** 例： `Device(config)# end`	現在のコンフィギュレーションモードを終了し、特権 EXEC モードに戻ります。

SNMP 通知のディセーブル

ルータ上で SNMP 通知をディセーブルにするには、ここに示す手順を実行します。

（注） 合法的傍受通知をディセーブルにするには、SNMPv3 を使用して CISCO-TAP2-MIB オブジェクト cTap2MediationNotificationEnable を false(2) に設定します。SNMPv3 を通じて合法的傍受の通知を再度イネーブルにするには、オブジェクトに true（1）を再設定します。

手順の概要

1. **enable**
2. **configure terminal**
3. **no snmp-server enable traps**
4. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**no snmp-server enable traps** 例： `Device(config)# no snmp-server enable traps`	システムで使用可能なすべての SNMP 通知タイプをディセーブルにします。
ステップ 4	**end** 例： `Device(config)# end`	現在のコンフィギュレーションモードを終了し、特権 EXEC モードに戻ります。

RADIUS セッション傍受のイネーブル化

メディエーションデバイスまたはタップをプロビジョニングするために使用可能なユーザCLIコマンドはありません。しかし、CISCO-TAP-MIB を通じて傍受をイネーブルにするには、account-session-id 値をメディエーションデバイスが使用できるようにシステムを設定する必要があります。ルータでRADIUSセッション傍受をイネーブルにするには、ここに示す手順を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **aaa intercept**
4. **aaa authentication ppp default group radius**
5. **aaa accounting delay-start all**
6. **aaa accounting send stop-record authentication failure**
7. **aaa accounting network default start-stop group radius**
8. **radius-server attribute 44 include-in-access-req**
9. **radius-server host** *host-name*
10. **aaa server radius dynamic-author**
11. **client** *ip-address*
12. **domain** {**delimiter** *character*| **stripping [right-to-left]**}
13. **server-key** *word*
14. **port** *port-number*
15. **exit**
16. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**aaa intercept** 例： `Device(config)# aaa intercept`	ルータで合法的傍受をイネーブルにします。 • このコマンドが削除されたときに許可のないユーザが傍受を停止できないように、このコマンドを高い管理セキュリティに関連付けます。

	コマンドまたはアクション	目的
ステップ 4	**aaa authentication ppp default group radius** 例： `Device(config)# aaa authentication ppp default group radius`	ポイントツーポイントプロトコル（PPP）を実行中のシリアル インターフェイス上で使用する認証方式を指定します。 （注） このコマンドが必要なのは、タップ情報が RADIUS サーバにしかないためです。ローカルに設定した情報で認証できますが、ローカルに設定した情報ではタップを指定できません。
ステップ 5	**aaa accounting delay-start all** 例： `Device(config)# aaa accounting delay-start all`	アカウンティング開始レコードの生成を、ユーザの IP アドレスが確立されるまで遅らせます。**all** キーワードを指定することにより、遅延がすべての VRF ユーザーおよび非 VRF ユーザーに適用されます。 （注） このコマンドは、メディエーション デバイスがターゲットに割り当てられた IP アドレスを参照できるようにするために必要です。
ステップ 6	**aaa accounting send stop-record authentication failure** 例： `Device(config)# aaa accounting send stop-record authentication failure`	（任意）ログイン時またはセッションのネゴシエーション中に認証に失敗したユーザに対するアカウンティング停止レコードを生成します。 （注） 合法的傍受の動作 1 でタップが開始されない場合、停止レコードの Acct-Termination-Cause（属性 49）に 15（サービス使用不能）が設定されます。
ステップ 7	**aaa accounting network default start-stop group radius** 例： `Device(config)# aaa accounting network default start-stop group radius`	（任意）すべてのネットワーク関連のサービス要求に対するアカウンティングをイネーブルにします。 （注） このコマンドは、タップが開始されなかった理由を特定するためだけに必要です。
ステップ 8	**radius-server attribute 44 include-in-access-req** 例： `Device(config)# radius-server attribute 44 include-in-access-req`	（任意）ユーザ認証前のアクセス要求パケット（事前認証の要求を含む）中で、RADIUS 属性 44（アカウンティング セッション ID）を送信します。 （注） このコマンドは、Access-Request パケットから属性 44 を取得するために入力します。そうしない場合、属性 44 の値を特定するには、アカウンティング パケットが受信されるのを待つ必要があります。

	コマンドまたはアクション	目的
ステップ 9	**radius-server host** *host-name* 例： `Device(config)# radius-server host host1`	（任意）RADIUS サーバ ホストを指定します。
ステップ 10	**aaa server radius dynamic-author** 例： `Device(config)# aaa server radius dynamic-author`	デバイスを認証、許可、アカウンティング（AAA）サーバとして設定して外部ポリシー サーバとの通信を容易にし、ダイナミック認可ローカル サーバ コンフィギュレーション モードを開始します。 （注） セッションの開始時に常にタップが開始される場合、このコマンドはオプションです。CoA-Requests を使用して既存のセッションでタップを開始および停止する場合は、このコマンドは必須です。
ステップ 11	**client** *ip-address* 例： `Device(config-locsvr-da-radius)# client 10.0.0.2`	（任意）デバイスが CoA-Request パケットを受け付ける RADIUS クライアントを指定します。

ステップ 12	**domain** {**delimiter** *character*| **stripping [right-to-left]**}
	例：
	`Device(config-locsvr-da-radius)# domain stripping right-to-left`
	例：
	`Device(config-locsvr-da-radius)# domain delimiter @`
		（任意）RADIUSアプリケーションについてユーザ名のドメイン オプションを設定します。
		• **delimiter** キーワードで、ドメインデリミタを指定します。次のいずれかのオプションを文字引数に指定できます：**@**、**/**、**$**、**%**、\、**#**または **-**
		• **stripping** キーワードは、着信のユーザー名と、**@** ドメインデリミタの左側にある名前を比較します。
		• The **right-to-left** キーワードは、右から左方向に見て最初のデリミタで文字列を終了します。

ステップ 13	**server-key** *word* 例： `Device(config-locsvr-da-radius)# server-key samplekey`	（任意）デバイスと RADIUS クライアントの間で共有する RADIUS キーを設定します。
ステップ 14	**port** *port-number* 例：	（任意）デバイスが CoA-Request パケットを受け付ける RADIUS クライアントを指定します。

	コマンドまたはアクション	目的
	`Device(config-locsvr-da-radius)# port 1600`	
ステップ 15	**exit** 例： `Device(config-locsvr-da-radius)# exit`	ダイナミック認可ローカル サーバー コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードに戻ります。
ステップ 16	**end** 例： `Device(config)# end`	現在のコンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

回線 ID ベースのタッピングの設定

ルータのユーザ セッションのデータ パケットと RADIUS 認証のデータ パケットの回線 ID ベースのタッピングを設定するには、このセクションの手順を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **subscriber access pppoe unique-key circuit-id**
4. **end**
5. **show pppoe session all**
6. **show idmgr session key circuit-id** *circuit-id*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**subscriber access pppoe unique-key circuit-id** 例： `Device(config)#subscriber access pppoe unique-key circuit-id`	PPPoE のユーザ セッションの一意の回線 ID タグがルータでタップされるように指定します。

	コマンドまたはアクション	目的
ステップ 4	**end** 例： `Device(config)# end`	現在のコンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。
ステップ 5	**show pppoe session all** 例： `Device# show pppoe session all`	次の手順でユーザ セッションの検証に使用される、PPPoE セッションの回線 ID タグを表示します。

ステップ 6	**show idmgr session key circuit-id** *circuit-id*
	例：
	`Device# show idmgr session key circuit-id Ethernet4/0.100:PPPoE-Tag-1`
	例：
	例：
	`session-handle = AA000007`
	例：
	`aaa-unique-id = 0000000E`
	例：
	`circuit-id-tag = Ethernet4/0.100:PPPoE-Tag-1`
	例：
	`interface = nas-port:0.0.0.0:0/1/1/100`
	例：
	`authen-status = authen`
	例：
	`username = user1@cisco.com`
	例：
	`addr = 106.1.1.3`
	例：
	`session-guid = 650101020000000E`
	例：
		一意の回線 ID タグを指定して、ID Manager（IDMGR）データベースのユーザ セッション情報を確認します。

	コマンドまたはアクション	目的

	`The session hdl AA000007 in the record is valid`
	例：
	`The session hdl AA000007 in the record is valid`
	例：
	`No service record found`	

合法的傍受の設定例

例：メディエーション デバイス アクセスの合法的傍受 MIB の有効化

次に、メディエーション デバイスが合法的傍受 MIB にアクセスできるようにする例を示します。この例では、4 つの LI MIB（CISCO-TAP2-MIB、CISCO-IP-TAP-MIB、CISCO-802-TAP-MIB、CISCO-USER-CONNECTION-TAP-MIB）を含む SNMP ビュー（tapV）を作成します。また、tapV ビュー内の MIB に読み込み、書き込み、通知アクセス可能なユーザ グループも作成します。

```
aaa intercept
snmp-server view tapV ciscoTap2MIB included
snmp-server view tapV ciscoIpTapMIB included
snmp-server view tapV cisco802TapMIB included
snmp-server view tapV ciscoUserConnectionTapMIB included
snmp-server group tapGrp v3 noauth read tapV write tapV notify tapV
snmp-server user MDuser tapGrp v3 auth md5 MDpasswd
snmp-server engineID local 1234
```

例：RADIUS セッションの合法的傍受のイネーブル化

次に、イーサネットの PPP connection over Ethernet（PPPoE）リンクを使用したネットワーク アクセス サーバ（NAS）デバイスとして機能するルータ上で、RADIUS ベースの合法的傍受ソリューションを設定する例を示します。

```
aaa new-model
!
aaa intercept
!
aaa group server radius SG
server 10.0.56.17 auth-port 1645 acct-port 1646
!
aaa authentication login LOGIN group SG
aaa authentication ppp default group SG
aaa authorization network default group SG
aaa accounting send stop-record authentication failure
aaa accounting network default start-stop group SG
```

```
!
aaa server radius dynamic-author
client 10.0.56.17 server-key cisco
!
vpdn enable
!
bba-group pppoe PPPoE-TERMINATE
virtual-template 1
!
interface Loopback0
ip address 10.1.1.2 255.255.255.0
!
interface GigabitEthernet4/1/0
description To RADIUS server
ip address 10.0.56.20 255.255.255.0
duplex auto
!
interface GigabitEthernet4/1/2
description To network
ip address 10.1.1.1 255.255.255.0
duplex auto
!
interface GigabitEthernet5/0/0
description To subscriber
no ip address
!
interface GigabitEthernet5/0/0.10
encapsulation dot1q 10
protocol pppoe group PPPoE-TERMINATE
!
interface Virtual-Template1
ip unnumbered Loopback0
ppp authentication chap
!
radius-server attribute 44 include-in-access-req
radius-server attribute nas-port format d
radius-server host 10.0.56.17 auth-port 1645 acct-port 1646
radius-server key cisco
```

その他の参考資料

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『Cisco IOS Master Commands List, All Releases』
SNMP サポートの設定	*SNMP* サポートの設定
セキュリティ コマンド	『*Cisco IOS Security Command Reference*』

標準

標準	タイトル
PacketCable™ コントロール ポイント検出インターフェイス仕様	『*PacketCable™ Control Point Discovery Interface Specification*』（PKT-SP-CPD-I02-061013）

MIB

MIB	MIB のリンク
• CISCO-TAP2-MIB • CISCO-IP-TAP-MIB • CISCO-802-TAP-MIB • CISCO-USER-CONNECTION-TAP-MIB	選択したプラットフォーム、Cisco ソフトウェア リリース、およびフィーチャ セットの MIB を検索してダウンロードする場合は、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

RFC

RFC	タイトル
RFC-2865	『*Remote Authentication Dial In User Service (RADIUS)*』
RFC-3576	*Dynamic Authorization Extensions to Remote Authentication Dial In User Service (RADIUS)*
RFC-3924	『*Cisco Architecture for Lawful Intercept in IP Networks*』

シスコのテクニカル サポート

説明	リンク
右の URL にアクセスして、シスコのテクニカル サポートを最大限に活用してください。これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

合法的傍受に関する機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだ

けを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *237* : 合法的傍受に関する機能情報

機能名	リリース	機能情報
合法的傍受	Cisco IOS XE Release 2.4 Cisco IOS XE Release 3.15S	合法的傍受（LI）機能を利用すると、サービス プロバイダーは、エッジ ルータを通過する Voice-over-Internet（VoIP）トラフィックまたはデータ トラフィックを傍受できる機能を提供するという、司法当局による要求を満たすことができます。 Cisco IOS XE Release 2.4 では、Cisco ASR 1000 シリーズ Aggregation Services Router にこの機能が実装されました。 Cisco IOS XE リリース 3.15S で、Cisco ASR 1000 シリーズアグリゲーション サービス ルータのトンネル インターフェイスに合法的傍受機能が導入されました。
VRF 対応の LI（合法的傍受）	Cisco IOS XE Release 2.4	VRF 対応 LI は、特定のバーチャル プライベート ネットワーク（VPN）での IPv4 データの LI 盗聴をプロビジョニングする機能です。 Cisco IOS XE Release 2.4 では、Cisco ASR 1000 シリーズ Aggregation Services Router にこの機能が実装されました。
RADIUS ベースの合法的傍受	Cisco IOS XE Release 2.4 Cisco IOS XE Release 3.5S	合法的傍受の実装は SNMP3 を使用してプロビジョニングされ、RADIUS セッションの傍受をサポートします。 Cisco IOS XE Release 2.4 では、Cisco ASR 1000 シリーズ Aggregation Services Router にこの機能が実装されました。 Cisco IOS XE リリース 3.5 では、ハイ アベイラビリティのサポートが RADIUS ベースの合法的傍受用に追加されました。
合法的傍受の PPP セッションの回線 ID ベースのタッピング	Cisco IOS XE Release 2.5	Cisco IOS XE リリース 2.5 では、PPP セッションの回線 ID ベースのタッピングが導入されました。回線 ID ベースのタッピングは、ユーザ セッションがアクティブになった後、タップがプロビジョニングされる場合にのみ動作します。このインスタンスでは、ユーザセッションは回線 ID タグで一意に識別されることを前提としています。

機能名	リリース	機能情報
合法的傍受の回線 ID ベースのタッピング	Cisco IOS XE Release 2.6	Cisco IOS XE リリース 2.6 では、PPP セッションの回線 ID ベースのタッピングの事前プロビジョニングが導入されました。ユーザ セッションがアクティブになる前にタップがプロビジョニングされる場合、タップはユーザ セッションがアクティブになればいつでも有効になります。また、対応する RADIUS 認証とアカウンティング パケットもタップされます。このインスタンスでは、ユーザ セッションは回線 ID タグで一意に識別されることを前提としています。
非合法的傍受（Non-LI）のイメージ	Cisco IOS XE Release 3.10S	Cisco IOS XE リリース 3.10S では、この機能は Cisco ASR 1000 シリーズ アグリゲーション サービス ルータに導入されました。 非合法的傍受のイメージは、Cisco IOS XE リリース 3.10S 以降で使用可能で、合法的傍受サブシステムは含まれません。

第 175 章

IPoE セッションの LI サポート

IPoE セッションの LI サポート機能は、RFC 2866 に準拠した IP over Ethernet（IPoE）セッションへのプロビジョニングされた合法的傍受（LI）のサポートを拡張しています。このドキュメントでは、IPoE 用の RADIUS ベースの合法的傍受を説明します。合法的傍受アーキテクチャとコンポーネントの情報およびコンフィギュレーションタスクと例については、「合法的傍受アーキテクチャ」モジュールを参照してください。

IPoE セッションの LI サポートの制約事項

次の制約事項は IPoE セッションの RADIUS ベースの合法的傍受に適用されます。

- アクセス許可パケットは、LI パラメータが暗号化されるとき、RADIUS プロキシセッションに対してタップを開始するために使用することはできません。
- **aaa intercept** コマンドは、RADIUS ベースの LI に関連付けられた属性値ペア（AVP）を受け付けるように設定する必要があります。開始、停止、または非動作の認可変更（CoA）要求の頻度は、10 分あたり 1 のレートを超えることはありません。
- 異なるユーザから傍受されたトラフィックは、同じ仲介デバイス（MD）に送信されます。各 MD ごとに固有のストリーム ID（8 桁の傍受 ID の最初の 4 桁で構成される）を使用する必要があります。
- RADIUS ベースの LI を使用してキャプチャされた傍受パケットの形式には、L2 ヘッダーが含まれます。これは SNMP ベースの LI の形式とは異なります。
- フロー単位のタップは、RADIUS ベースの LI を介してはサポートされていません。SNMP ベースの LI でサポートされます。

IPoE セッションの LI サポートに関する追加情報

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『Cisco IOS Master Commands List, All Releases』
『Configuring SNMP Support』	『*Configuring SNMP Support*』
セキュリティ コマンド	『*Cisco IOS Security Command Reference*』

標準

標準	タイトル
PacketCable™ コントロール ポイント検出インターフェイス仕様	『*PacketCable™ Control Point Discovery Interface Specification*』（PKT-SP-CPD-I02-061013）

MIB

MIB	MIB のリンク
• CISCO-IP-TAP-MIB • CISCO-TAP2-MIB • CISCO-802-TAP-MIB • CISCO-USER-CONNECTION-TAP-MIB	選択したプラットフォーム、Cisco ソフトウェア リリース、およびフィーチャ セットの MIB を検索してダウンロードする場合は、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

RFC

RFC	タイトル
RFC 2866	『*RADIUS Accounting*』

シスコのテクニカル サポート

説明	リンク
シスコのサポート Web サイトでは、シスコの製品やテクノロジーに関するトラブルシューティングにお役立ていただけるように、マニュアルやツールをはじめとする豊富なオンライン リソースを提供しています。 お使いの製品のセキュリティ情報や技術情報を入手するために、Cisco Notification Service（Field Notice からアクセス）、Cisco Technical Services Newsletter、Really Simple Syndication（RSS）フィードなどの各種サービスに加入できます。 シスコのサポート Web サイトのツールにアクセスする際は、Cisco.com のユーザ ID およびパスワードが必要です。	http://www.cisco.com/support

IPoE セッションの LI サポートに関する機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *238 : IPoE* セッションの *LI* サポートに関する機能情報

機能名	リリース	機能情報
IPoE セッションの LI サポート	Cisco IOS XE Release 3.10S	RFC 2866 に従って、IPoE セッションへのプロビジョニング LI サポートを拡張します。

第 176 章

イメージ検証

イメージ検証機能を使用すると、Cisco IOS XEイメージとプロビジョニング ファイルの完全性を自動的に検証できます。そのため、ユーザは、イメージまたはプロビジョニング ファイルが偶発的な破壊から保護されていることを確認できます。破壊は、シスコによってファイルが作成される瞬間からユーザに届くまで、輸送中にいつでも起きる可能性があります。

イメージ検証の制約事項

イメージ検証は、任意のファイルに適用され実行されますが、ファイルがイメージファイルまたはプロビジョニング ファイルでない場合、イメージ検証は実行されず、「SIGNATURE-4-NOT_PRESENT」というエラーが表示されます。

（注） イメージ検証機能は、Cisco IOS XE デバイスに格納されている Cisco IOS XE ソフトウェア イメージまたはプロビジョニング ファイルの完全性を確認するためにだけに使用できます。リモート ファイル システム上のイメージや、メモリ内で実行されているイメージの完全性を確認するためは使用できません。

イメージ検証について

（注） このドキュメントでは、Cisco IOS XEイメージに関する記述は、プロビジョニング ファイルにも適用されます。

イメージ検証の利点

転送エラーやディスク破壊の結果、偶発的にイメージやプロビジョニング ファイルの完全性が破壊される場合に、ルータが自動的に検出できるようになったため、Cisco IOS XE ルータの効率は向上しています。

イメージ検証の動作

実稼働イメージは、一連の転送を経てルータのメモリにコピーされるため、イメージの完全性が転送のたびに偶発的に破壊される危険があります。Cisco.com からイメージをダウンロードするとき、ユーザはダウンロードしたイメージに対してメッセージ ダイジェスト 5（MD5）ハッシュを実行し、Cisco.com で公開されている MD5 ダイジェストが、ユーザのサーバで計算した MD5 ダイジェストと同じであることを確認できます。しかし、MD5 ダイジェストが 128 ビット長であり、検証が手動であることから、多くのユーザは MD5 ダイジェストを実行しません。イメージ検証により、ユーザーは、ダウンロードしたすべてのイメージの完全性を自動的に検証できるため、ユーザーの操作が大幅に削減されます。

イメージ検証の使用方法

イメージの完全性のグローバルな検証

file verify auto コマンドを使用すると、イメージの検証がグローバルにイネーブルになります。つまり、コピー（**copy** コマンドを使用）またはリロード（**reload** コマンドを使用）されるすべてのイメージが自動的に検証されます。**copy** コマンドと **reload** コマンドには、イメージの検証をイネーブルにする **/verify** キーワードがありますが、イメージをコピーまたはリロードするたびにキーワードを指定する必要があります。**file verify auto** コマンドを使用すると、デフォルトでイメージの検証がイネーブルになるため、イメージ検証を何度も指定する必要がなくなります。

デフォルトでイメージ検証をイネーブルにし、特定のイメージのコピーまたはリロードで検証をディセーブルにする場合は、**/noverify** キーワードは、**copy** コマンドまたは **reload** コマンドを指定することで、**file verify auto** コマンドを上書きします。

自動的なイメージ検証をイネーブルにするには、ここに示す手順を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **file verify auto**
4. **exit**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**file verify auto** 例： `Device(config)# file verify auto`	自動的なイメージ検証をイネーブルにします。
ステップ 4	**exit** 例： `Device(config)# exit`	グローバル コンフィギュレーション モードを終了します。 イメージをコピーまたはリロードする場合は、グローバル コンフィギュレーション モードを終了する必要があります。

次の作業

file verify auto コマンドを実行した後は、**/verify** キーワードを **copy** または **reload** コマンドで発行する必要はなくなります。これは、コピーまたはリロードされる各イメージが自動的に検証されるためです。

コピーしようとしているイメージの完全性の検証

copy コマンドを実行するとき、**/verify** キーワードを指定することで、コピーされるファイルの完全性を検証できます。完全性の確認に失敗した場合、コピーされたファイルは削除されます。コピーしようとしているファイルにハッシュが埋め込まれていない場合（古いイメージの場合）、コピー処理を続行するかどうかを質問されます。続行を選択すると、ファイルは正常にコピーされ、続行しないことを選択すると、コピーされたファイルが削除されます。

/verify キーワードを指定しないと、**copy** コマンドにより有効でないファイルがコピーされる可能性があります。そのため、**copy** コマンドを正常に実行した後、いつでも **verify** コマンドを実行して、ルータのストレージに格納されているファイルの完全性を確認できます。

ルータにコピーする前にイメージの完全性を確認するには、次の手順を実行します。

手順の概要

1. **enable**

2. **copy** [**/erase**] [**/verify**| **/noverify**] *source-url destination-url*
3. **verify** [**/md5** [*md5-value*]] *filesystem: file-url*]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**copy** [**/erase**] [**/verify**| **/noverify**] *source-url destination-url* 例： `Device# copy /verify tftp://10.1.1.1/cat3k_caa-universalk9.SSA.16.1.0.EFT3-1.bin flash:`	コピー元からコピー先に任意のファイルをコピーします。 • **/verify**：コピー先のファイルのシグニチャを検証します。検証に失敗すると、ファイルは削除されます。 • **/noverify**：イメージをコピーする前にコピー先ファイルのシグニチャを検証しません。 （注） **/noverify** は、多くの場合、**file verify auto** コマンドが有効になっており、コピーするすべてのイメージのシグニチャが自動的に検証される場合に使用されます。
ステップ 3	**verify** [**/md5** [*md5-value*]] *filesystem: file-url*] 例： `Device# flash: tftp://10.1.1.1/cat3k_caa-universalk9.SSA.16.1.0.EFT3-1.bin flash:`	（任意）デバイスのストレージに格納されているイメージの完全性を検証します。

リロードしようとしているイメージの完全性の検証

reload コマンドを **/verify** キーワード付きで実行することにより、システムにロードしようとしているイメージの完全性が確認されます。**/verify** キーワードを指定した場合、システムがリブートを開始する前にイメージの検証が実行されます。そのため、検証に失敗すると、イメージはロードされません。

（注） プラットフォームが異なれば、ロードするファイルの取得方法も異なるため、BOOTVAR で指定されたファイルが検証されます。ファイルが指定されていない場合、各サブシステム上の最初のファイルが検証されます。プラットフォームによっては、設定レジスタなどの変数があるため、検証されるファイルがロードされるファイルになるとは限りません。

ルータにリロードする前にイメージの完全性を確認するには、次の手順を実行します。

手順の概要

1. **enable**
2. **reload** [[**warm**] [**/verify**| **/noverify**] *text* | [**warm**] [**/verify**| **/noverify**] **in** [*hh* **:** *mm* [*text*] | [**warm**] [**/verify**| **/noverify**] **at** *hh* **:** *mm* [*month day* | *day month*] [*text*] | [**warm**] [**/verify**| **/noverify**] **cancel**]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**reload** [[**warm**] [**/verify**| **/noverify**] *text*	[**warm**] [**/verify**| **/noverify**] **in** [*hh* **:** *mm* [*text*]	[**warm**] [**/verify**| **/noverify**] **at** *hh* **:** *mm* [*month day*	*day month*] [*text*]	[**warm**] [**/verify**| **/noverify**] **cancel**] 例： `Device# reload /verify`	オペレーティング システムをリロードします。 • **/verify**：コピー先のファイルのシグニチャを検証します。検証に失敗すると、ファイルは削除されます。 • **/noverify**：イメージをリロードする前にコピー先ファイルのシグニチャを検証しません。 （注） **/noverify** は、多くの場合、**file verify auto** コマンドが有効になっており、コピーするすべてのイメージのシグニチャが自動的に検証される場合に使用されます。

イメージ検証の設定例

グローバル イメージ検証の例

次に、自動的なイメージ検証をイネーブルにする例を示します。このコマンドをイネーブルにした後、コピー（**copy** コマンドを使用）またはリロード（**reload** コマンドを使用）されるすべてのイメージに対し、イメージ検証が自動的に実行されます。

```
Device(config)# file verify auto
```

copy コマンドを使用したイメージ検証の例

次に、イメージをコピーする前にイメージ検証を指定する例を示します。

```
Device# copy /verify tftp://10.1.1.1/jdoe/c7200-js-mz disk0:
Destination filename [c7200-js-mz]?
Accessing tftp://10.1.1.1/jdoe/c7200-js-mz...
Loading jdoe/c7200-js-mz from 10.1.1.1 (via FastEthernet0/0):!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
[OK - 19879944 bytes]
19879944 bytes copied in 108.632 secs (183003 bytes/sec)
Verifying file integrity of disk0:/c7200-js-mz
.....................................................................................
.....................................................................................
.....................................................................................
.........................Done!
Embedded Hash   MD5 :CFA258948C4ECE52085DCF428A426DCD
Computed Hash       MD5 :CFA258948C4ECE52085DCF428A426DCD
CCO Hash               MD5 :44A7B9BDDD9638128C35528466318183
Signature Verified
```

reload コマンドを使用したイメージ検証の例

次に、デバイスにイメージをリロードする前にイメージ検証を指定する例を示します。

```
Device# reload /verify
Verifying file integrity of bootflash:c7200-kboot-mz.121-8a.E
%ERROR:Signature not found in file bootflash:c7200-kboot-mz.121-8a.E.
Signature not present. Proceed with verify? [confirm]
Verifying file disk0:c7200-js-mz
.....................................................................
.....................................................Done!
Embedded Hash     MD5 :CFA258948C4ECE52085DCF428A426DCD
Computed Hash      MD5 :CFA258948C4ECE52085DCF428A426DCD
CCO Hash          MD5 :44A7B9BDDD9638128C35528466318183
Signature Verified
Proceed with reload? [confirm]n
```

verify コマンドの出力例

次に、**verify** コマンドでイメージ検証を指定する例を示します。

```
Device# verify disk0:c7200-js-mz
%Filesystem does not support verify operations
Verifying file integrity of disk0:c7200-js-mz.....................................
.....................................................................Done!
Embedded Hash     MD5 :CFA258948C4ECE52085DCF428A426DCD
Computed Hash      MD5 :CFA258948C4ECE52085DCF428A426DCD
CCO Hash          MD5 :44A7B9BDDD9638128C35528466318183
```

Signature Verified

その他の参考資料

ここでは、イメージ検証機能に関する関連資料について説明します。

関連資料

関連項目	マニュアル タイトル
システム イメージのロード、メンテナンス、リブートに関する設定作業と情報	『Cisco ASR 1000 Series Aggregation Services Routers Software Configuration Guide』
システム イメージをロード、メンテナンス、リブートするためのその他のコマンド	『Cisco IOS Master Command List, All Releases』

標準

標準	タイトル
この機能でサポートされる新規の標準または変更された標準はありません。また、既存の標準のサポートは変更されていません。	--

MIB

MIB	MIB のリンク
この機能によってサポートされる新しい MIB または変更された MIB はありません。またこの機能による既存 MIB のサポートに変更はありません。	選択したプラットフォーム、Cisco IOS XE ソフトウェア リリース、およびフィーチャ セットの MIB の場所を検索しダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

RFC

RFC	タイトル
この機能によりサポートされた新規 RFC または改訂 RFC はありません。またこの機能による既存 RFC のサポートに変更はありません。	--

シスコのテクニカル サポート

説明	リンク
シスコのサポート Web サイトでは、シスコの製品やテクノロジーに関するトラブルシューティングにお役立ていただけるように、マニュアルやツールをはじめとする豊富なオンライン リソースを提供しています。 お使いの製品のセキュリティ情報や技術情報を入手するために、Cisco Notification Service（Field Notice からアクセス）、Cisco Technical Services Newsletter、Really Simple Syndication（RSS）フィードなどの各種サービスに加入できます。 シスコのサポート Web サイトのツールにアクセスする際は、Cisco.com のユーザ ID およびパスワードが必要です。	http://www.cisco.com/en/US/support/index.html

イメージ検証に関する機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *239 :* イメージ検証に関する機能情報

機能名	リリース	機能情報
イメージ検証		イメージ検証機能を使用すると、ユーザは Cisco IOS XE イメージの完全性を自動的に検証できます。 次のコマンドが導入または変更されました。**copy**、**file verify auto**、**reload**、**verify**。

第 XVII 部

IPsec データ プレーン

第 177 章

IPsec アンチリプレイウィンドウの拡張と無効化

Cisco IP セキュリティ（IPsec）認証では、暗号化されたパケットそれぞれに対して固有のシーケンス番号を割り当てることによって、暗号化されたパケットを複製する攻撃者に対するアンチリプレイ保護が提供されます。それらの番号に基づいて、デクリプタが検知したパケットを追跡します。現在、デフォルトのウィンドウ サイズは、64 パケットです。一般的にはこの数字（ウィンドウ サイズ）で十分ですが、このウィンドウ サイズを拡張する必要がある場合もあります。IPsec アンチ リプレイ ウィンドウの拡張とディセーブル化機能を使用すれば、ウィンドウ サイズを拡張でき、デクリプタによる 64 を超すパケットの追跡が可能となります。

IPsec アンチ リプレイ ウィンドウの拡張と無効化の前提条件

- この機能を設定する前に、クリプトマップまたは暗号プロファイルを作成しておく必要があります。
- IPsec アンチリプレイウィンドウの拡張とディセーブル化機能を設定するには、次の概念を理解しておく必要があります。IPsec アンチ リプレイ ウィンドウ （2616 ページ）

IPsecアンチリプレイウィンドウの拡張と無効化に関する情報

IPsec アンチ リプレイ ウィンドウ

Cisco IPsec 認証では、暗号化されたパケットそれぞれに対して固有のシーケンス番号を割り当てることによって、暗号化されたパケットを複製する攻撃者に対するアンチリプレイ保護が提供されます（セキュリティ アソシエーション（SA）アンチリプレイは、受信側がリプレイ攻撃から自身を保護するために、古いパケットまたは重複パケットを拒否できるセキュリティ サービスです）。復号機能によって、以前に認識したシーケンス番号が除外されます。エンクリプタによって、シーケンス番号が昇順で割り当てられます。すでに検出されている最も高いシーケンス番号である値 X はデクリプタによって記録されます。また、デクリプタによって、X-N+1 ～ X（N はウィンドウ サイズ）までのシーケンス番号を持つパケットが検出されているかどうかも記録されます。シーケンス番号 X-N を持つすべてのパケットが廃棄されます。現在、N は 64 に設定されているため、デクリプタによって追跡できるパケットは 64 までです。

ただし、64 パケット ウィンドウ サイズでは不十分な場合があります。たとえば、Cisco Quality of Service（QoS）によってハイプライオリティパケットにプライオリティが与えられている場合、一部のロープライオリティパケットは、それらがデクリプタに 64 パケットのリプレイウィンドウを超えて到着すると、廃棄されてしまう可能性があります。IPsec アンチ リプレイ ウィンドウの拡張とディセーブル化機能を使用すれば、ウィンドウ サイズを拡張でき、デクリプタによる 64 を超すパケットの追跡が可能となります。

アンチリプレイ ウィンドウ サイズを増やしても、スループットおよびセキュリティに影響はありません。メモリへの影響は限定的です。デクリプタ上にシーケンス番号を保管するために必要となるのは、着信 IPsec SA ごとに追加の 128 バイトだけであるためです。今後アンチリプレイに関する問題が発生しないように、最大のウィンドウ サイズである 1024 を使用することを推奨します。

IPsecアンチリプレイウィンドウの拡張と無効化機能の設定方法

IPsec アンチ リプレイ ウィンドウの拡張と無効化のグローバル設定

IPsec アンチ リプレイ ウィンドウ：拡張と無効化をグローバルに設定する（その結果、作成されるすべての SA が影響を受けます）には、次の手順を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **crypto ipsec security-association replay window-size** [*N*]
4. **crypto ipsec security-association replay disable**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**crypto ipsec security-association replay window-size** [*N*] 例： `Router (config)# crypto ipsec security-association replay window-size 256`	SA リプレイ ウィンドウのサイズをグローバルに設定します。 （注） このコマンドまたは **crypto ipsec security-association replay disable** コマンドを設定します。この 2 つのコマンドは、同時に使用できません。
ステップ 4	**crypto ipsec security-association replay disable** 例： `Router (config)# crypto ipsec security-association replay disable`	検査をグローバルにイネーブルにします。 （注） このコマンドまたは **crypto ipsec security-association replay window-size** コマンドを設定します。この2つのコマンドは、同時に使用できません。

クリプトマップ上における IPsec アンチリプレイウィンドウの拡張と無効化の設定

暗号マップ上でIPsecアンチリプレイ ウィンドウの拡張と無効化を、特定の暗号マップまたはプロファイルを使用して作成された SA に影響を与えるように設定するには、次の手順を実行します。

手順の概要

1. **enable**
2. **configure terminal**

3. **crypto map** *map-name seq-num* [**ipsec-isakmp**]
4. **set security-association replay window-size** [*N*]
5. **set security-association replay disable**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**crypto map** *map-name seq-num* [**ipsec-isakmp**] 例： `Router (config)# crypto map ETHO 17 ipsec-isakmp`	クリプト マップ コンフィギュレーション モードを開始し、動的に作成されるクリプトマップの設定のためのテンプレートを提供する暗号プロファイルを作成します。
ステップ 4	**set security-association replay window-size** [*N*] 例： `Router (crypto-map)# set security-association replay window-size 128`	特定のクリプトマップ、ダイナミック クリプトマップ、または暗号プロファイルによって指定されたポリシーを使用して作成される SA を制御します。 （注） このコマンドまたは **set security-association replay disable** コマンドを設定します。この 2 つのコマンドは、同時に使用できません。
ステップ 5	**set security-association replay disable** 例： `Router (crypto-map)# set security-association replay disable`	特定のクリプトマップ、ダイナミック クリプトマップ、または暗号プロファイルに対するリプレイ検査をディセーブルにします。 （注） このコマンドまたは **set security-association replay window-size** コマンドを設定します。この 2 つのコマンドは、同時に使用できません。

トラブルシューティングのヒント

• 受信されるパケットの数に対して十分高い数字がリプレイ ウィンドウ サイズに設定されていない場合、次のようなシステム メッセージが受信されます。

```
*Nov 17 19:27:32.279: %CRYPTO-4-PKT_REPLAY_ERR: decrypt: replay check failed connection
 id=1
```

受信されたメッセージが、アンチ リプレイ ウィンドウの範囲を超えていると判断されると、上記メッセージが生成されます。

IPsec アンチ リプレイ ウィンドウの拡張と無効化の設定例

アンチ リプレイ ウィンドウのグローバル拡張と無効化：例

次の例は、アンチ リプレイ ウィンドウ サイズがグローバルに 1024 に設定されていることを示しています。

```
version 2.1
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname VPN-Gateway1
!
boot-start-marker
boot-end-marker
!
!
clock timezone EST 0
no aaa new-model
ip subnet-zero
!
!
ip audit po max-events 100
no ftp-server write-enable
!
!
crypto isakmp policy 10
 authentication pre-share
crypto isakmp key cisco123 address 192.165.201.2 !
crypto ipsec security-association replay window-size 1024 !
crypto ipsec transform-set basic esp-des esp-md5-hmac !
crypto map mymap 10 ipsec-isakmp
 set peer 192.165.201.2
 set transform-set basic
 match address 101
!
!
interface FastEthernet0/0
 ip address 192.168.1.1 255.255.255.0
!
interface Serial1/0
 ip address 192.165.200.2 255.255.255.252  serial restart-delay 0  crypto map mymap !
ip classless
ip route 0.0.0.0 0.0.0.0 192.165.200.1
no ip http server
no ip http secure-server
```

```
!
!
access-list 101 permit ip 192.168.1.0 0.0.0.255 172.16.2.0 0.0.0.255 access-list 101
remark Crypto ACL
!
!
control-plane
!
!
line con 0
line aux 0
line vty 0 4
!
!
end
```

暗号マップまたは暗号プロファイルのアンチ リプレイ ウィンドウの拡張および無効化：例

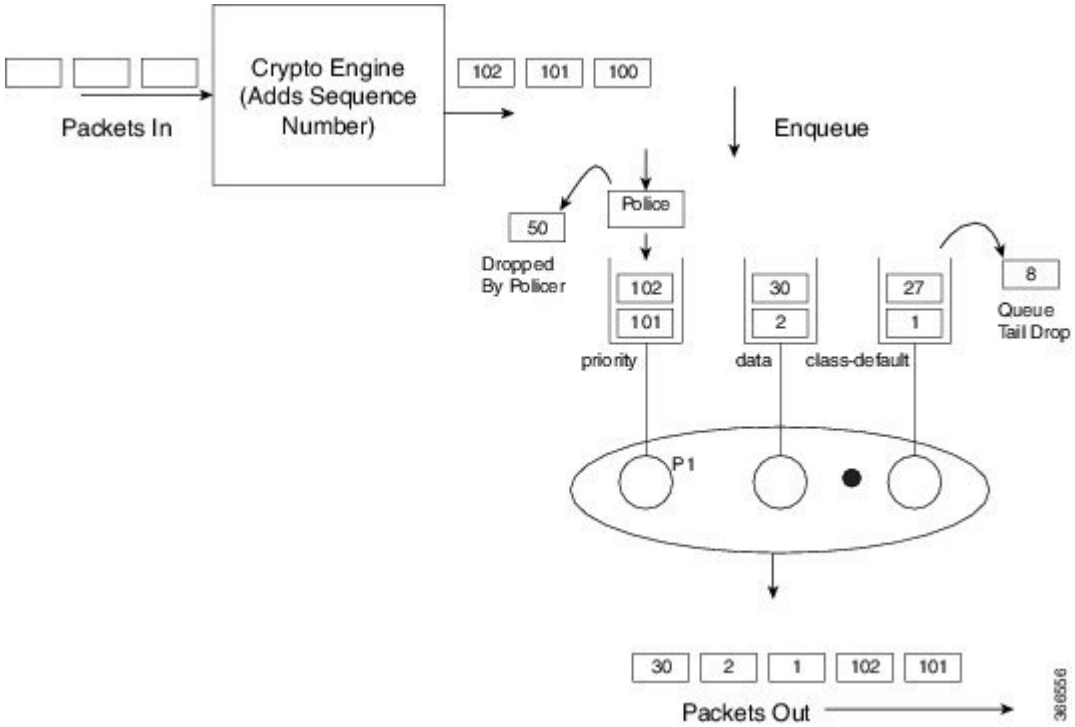
次の例では、アンチ リプレイ検査が、172.17.150.2 への IPsec 接続に関してディセーブルにされているが、172.17.150.3 および 172.17.150.4 への IPsec 接続に関してはイネーブル（および、デフォルトのウィンドウ サイズが 64）にされていることを示しています。

```
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname networkserver1
!
enable secret 5 $1$KxKv$cbqKsZtQTLJLGPN.tErFZ1 enable password ww !
ip subnet-zero
!
cns event-service server
crypto isakmp policy 1
authentication pre-share
crypto isakmp key cisco170 address 172.17.150.2 crypto isakmp key cisco180 address
172.17.150.3 crypto isakmp key cisco190 address 172.17.150.4
crypto ipsec transform-set 170cisco esp-des esp-md5-hmac crypto ipsec transform-set
180cisco esp-des esp-md5-hmac crypto ipsec transform-set 190cisco esp-des esp-md5-hmac
crypto map ETH0 17 ipsec-isakmp
 set peer 172.17.150.2
 set security-association replay disable set transform-set 170cisco match address 170
crypto map ETH0 18 ipsec-isakmp  set peer 192.168.1.3 set transform-set 180cisco match
address 180 crypto map ETH0 19 ipsec-isakmp set peer 192.168.1.4 set transform-set
190cisco match address 190 !
interface FastEthernet0
 ip address 172.17.150.1 255.255.255.0
 no ip directed-broadcast
 no ip route-cache
 no ip mroute-cache
 no mop enabled
 crypto map ETH0
!
interface Serial0
 ip address 172.16.160.1 255.255.255.0
 no ip directed-broadcast
 no ip mroute-cache
 no fair-queue
!
```

```
ip classless
ip route 172.18.170.0 255.255.255.0 172.17.150.2 ip route 172.19.180.0 255.255.255.0
172.17.150.3 ip route 172.20.190.0 255.255.255.0 172.17.150.4 no ip http server !
access-list 170 permit ip 172.16.160.0 0.0.0.255 172.18.170.0 0.0.0.255 access-list 180
 permit ip 172.16.160.0 0.0.0.255 172.19.180.0 0.0.0.255 access-list 190 permit ip
172.16.160.0 0.0.0.255 172.20.190.0 0.0.0.255 !
dialer-list 1 protocol ip permit
dialer-list 1 protocol ipx permit
!
line con 0
transport input none
line aux 0
line vty 0 4
password ww
logi
end
```

QoS のための IPsec アンチリプレイのメカニズム

QoS メカニズム（暗号化デバイスの出力インターフェイスまたはパス内の他のネットワーク要素上）、ロードバランシング メカニズム、またはルーティング/パス選択メカニズム（異なるパスを介して異なるフローを送信する）が使用される IP ネットワークでは、パケットの順序が変更されるのは通常のことです。

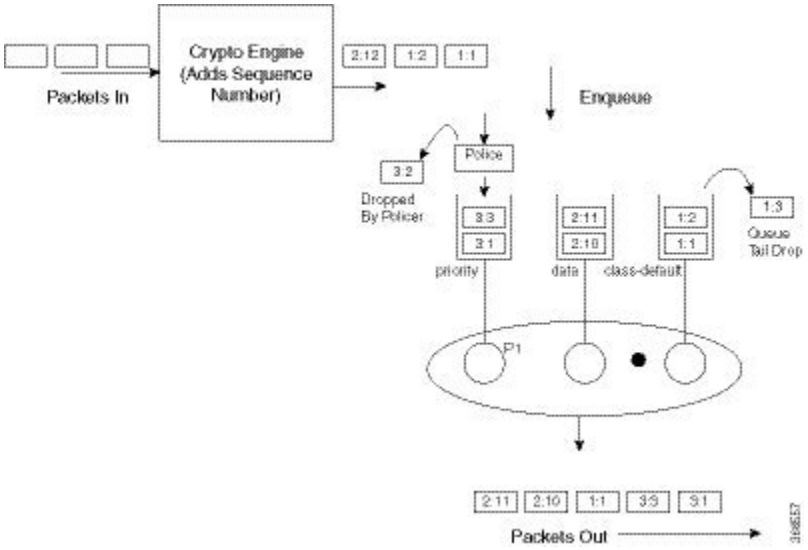


上の図は、QoS がパケットの順序を変更するときに、アンチリプレイ保護システムがどのように問題を引き起こすのかを示しています。暗号化エンジンはシーケンス番号を追加します。これらの番号が追加されると、パケットは、そのパケット内のアプリケーションに応じて出力キューに入れられます。図の例では、シーケンス番号 101 および 102 のパケットがプライオリティキューに入れられるときに、パケットがすでに帯域幅キュー（data および class-default）に

存在しています。プライオリティパケットが最初にスケジュールされます。復号デバイスがシーケンス番号 101 のパケットを受信すると、スライディングウィンドウの履歴は 101 に移動します。これは、スライディングウィンドウがシーケンス番号 30 ～ 101 の履歴を作成することを意味します。シーケンス番号 102 を持つ次のパケットが受信されると、スライディングウィンドウの履歴が 39 ～ 102 に変更されます。この時点で、プライオリティキューにパケットがないため、他のキューのいずれかからパケット（たとえば、シーケンス番号 1 のパケット）が取得されます。復号デバイスがシーケンス番号 1 のパケットを受信するのはこれが初めてですが、スライディングウィンドウで履歴が維持されているため、パケットはドロップされます。

暗号化の前に QoS スケジューリングを移動すると、アンチリプレイの問題が解決される可能性がありますが、QoS 機能が役に立たなくなります。さらに、スケジューリングは、出力インターフェイス（またはそのインターフェイスのシェイパー）の輻輳によって駆動される必要があります。アンチリプレイウィンドウのサイズを大きくすると、この機能を処理するデバイスのメモリに大きな負荷がかかります。

そのため、セキュリティアソシエーションごとに複数のシーケンス番号スペースを維持するソリューションが導入されました。特定のキュー内のすべてのパケットが同じシーケンス番号スペースからシーケンス番号を受け取るように、番号スペースが出力キューイングスキームに合わせて調整されます。シーケンス番号スペース内のすべてのパケットが同じキューを通過するため、出力 QoS によってそれらのパケットの順序が変更される可能性がなくなります。番号スペース内の順序変更がネットワークの他の場所で発生する可能性は依然としてあります（ただし、可能性は低い）。パケットがシーケンス番号どおりにキューに入れられずにテールドロップされた（順不同で入れられたのではない）場合でも、シーケンス番号は受信側で受信されます。そのため、シーケンス番号スペースごとの履歴ウィンドウは維持されますが、その履歴はかなり短くなります。



この図は、シーケンス番号がセレクタとシーケンス番号の 2 つの部分で設定されていることを示しています。受信側は、セレクタを使用して、使用する正しい履歴を選択し、シーケンス番号は通常どおりに動作します。

（注） 複数のシーケンス番号スペース（マルチ SNS）が有効になっている場合、IPsec アンチリプレイ機能は Group Encrypted Transport VPN（GETVPN）をサポートしません。

IPsec アンチリプレイパケット損失の回避

IPsec アンチリプレイパケット損失の回避の機能により、QoS が IPsec で設定されている場合に、不要な IPsec アンチリプレイパケットのドロップが回避されます。ただし、IPSec アンチリプレイが有効な状態で QoS が使用されている場合、特定の状況下で一部のパケットのドロップが発生する可能性があります。暗号インターフェイスがピアルータに接続されているときにクラスマップが追加または削除されると、マルチ SNS が有効になっている場合、1 ～ 2 秒間、アンチリプレイドロップが発生します。トラフィックは数秒後に回復し、その後はドロップが見られません。

アンチリプレイドロップは、次の状況で発生する可能性があります。

- パケットの転送中に、クラスが QoS ポリシーマップから削除されます。このクラスに属するパケットが使い果たされ、着信パケットが、class-default キューに入っているすべてのパケットの後にキューイングされます。これにより、シーケンス番号スペースが壊れ、アンチリプレイドロップが発生する可能性があります。キューが空になり、システムはすぐに回復して通常の動作を再開します。
- ESP ベースのハイアベイラビリティが設定され、オーバーサブスクライブされたトラフィックがすべてのシーケンス番号スペースを介して送信されるときに、アンチリプレイドロップが発生します。送信側でオーバーサブスクライブされたトラフィックがある場合、トラフィックは QoS ポリシーに基づいてシェーピングされます。その結果、受信側ルータが、シーケンス番号の順序が正しくないパケットを受信します。これらのドロップは一時的であり、すぐに回復します。
- セキュリティ アソシエーション（SA）のキー再生成中に、ルータが、新旧両方のインバウンド セキュリティ パラメータ インデックス（SPI）を短期間保持します。古い SA は短期間で削除されます。古い SA が削除された後、ルータが古い SPI を持つパケットを受信すると（QoS ポリシーが存在する場合に発生する可能性があります）、無効 SPI エラーによりパケットがドロップされます。

QoS のための IPsec アンチリプレイの設定

次に、IPsec SA ごとに複数のシーケンス番号スペースを有効にするコマンドを示します。

```
Device(config)#crypto ipsec security-association multi-sn
```

注意 この機能を設定する前に、既存のすべてのセッションをクリアする必要があります。そうしないと、既存のセッションからのトラフィックがドロップされます。

注意 この機能は、IPsec 接続の両方のトンネルルータで設定する必要があります。この機能が一方のルータでしか有効になっていない場合、もう一方のルータはパケットをドロップします。

コマンドの表示

show platform hardware qfp active feature ipsec datapath crypto-sa

このコマンドにより、QFP の IPsec SA におけるシーケンス番号スペースとシーケンス番号の間のマッピングが表示されます。

```
Device# show platform hardware qfp active feature ipsec datapath crypto-sa 4
Crypto Context Handle: e8b06b60
peer sa handle: 0
anti-replay enabled
esn disabled
Outbound SA
Total SNS: 16
Space                current seq number
----------------------------------------
   0                                   0
   1                                   0
   2                                   0
   3                                   0
   4                                   0
   5                                   0
   6                                   0
   7                                   0
   8                                   0
   9                                   0
  10                                   0
  11                                 100
  12                                   0
  13                                   0
  14                                   0
  15                                   0
```

show platform hardware qfp active feature ipsec sa

このコマンドは、Cisco QuantumFlow Processor（Cisco QFP）の IPsec SA を表示します。

```
Device# show platform hardware qfp active feature ipsec sa 6
QFP ipsec sa Information

         QFP sa  id: 6
          pal sa id: 170
         QFP spd id: 1
          QFP sp id: 2
            QFP spi: 0xa4a5244(172642884)
        crypto ctx: 0x00000000e8b14a20
              flags: 0x4640068 (Details below)
                   : src:IKE  valid:Yes  soft-life-expired:No  hard-life-expired:No
                   : replay-check:No  proto:ESP  mode:Receive-only  direction:Egress
                  : qos_preclassify:No  qos_group:No
                   : frag_type:AFTER_ENCRYPT  df_bit_type:COPY
                   : sar_enable:No  getvpn_mode:SNDRCV_SA
```

```
                    : doing_translation:No  assigned_outside_rport:No
                    : inline_tagging_enabled:No
          qos_group: 0x0
                mtu: 0x59e=1438
            mtu_adj: 0x588=1416
          sar_delta: 0
         sar_window: 0x0
         sibling_sa: 0x0
             sp_ptr: 0xe8abc000
            sbs_ptr: 0xe8a73878
     local endpoint: 33.0.0.3
    remote endpoint: 33.0.0.4
   cgid.cid.fid.rid: 1.1.1.11141121
              ivrf: 0
              fvrf: 0
    trans udp sport: 0
    trans udp dport: 0
    first intf name: Tunnel0
nat fixup src port: 0
    nat fixup  ip: 0.0.0.0
```

show platform software ipsec fp active flow

このコマンドは、指定されたフロー ID の fman-fp プロセスの IPsec SA を表示します。

```
Device# show platform software ipsec fp active flow identifier 169
Flow id: 169
                mode: tunnel
           direction: inbound
            protocol: esp
                 SPI: 0xbcd8840
      local IP addr: 33.0.0.3
     remote IP addr: 33.0.0.4
   crypto device id: 0
      crypto map id: 1
              SPD id: 1
          QFP SPD id: 1
    ACE line number: 1
      QFP SA handle: 5
IOS XE interface id: 11
     interface name: Tunnel0
   Crypto SA ctx id: 0x00000000e8b148c0
             cipher: AES-128
               auth: SHA256
initial seq.number: 0
       timeout, mins: 0
              flags: exp time;exp traffic;
Time limits

    soft limit(sec): 3401
    hard limit(sec): 3568
Traffic limits

     soft limit(kb): 3962880
     hard limit(kb): 4608000
     inline_tagging: DISABLED
anti-replay window: 64
SPI Selector:

   remote addr low: 0.0.0.0
  remote addr high: 0.0.0.0
    local addr low: 33.0.0.3
   local addr high: 33.0.0.3
```

```
Classifier: range

   src IP addr low: 33.0.0.3
  src IP addr high: 33.0.0.3
   dst IP addr low: 33.0.0.4
  dst IP addr high: 33.0.0.4
      src port low: 0
     src port high: 65535
      dst port low: 0
     dst port high: 65535
      protocol low: 47
     protocol high: 47
------------- Statistics

            octets(delta): 0
      total octets(delta): 4718576880
           packets(delta): 0
   dropped packets(delta): 0
      replay drops(delta): 0
      auth packets(delta): 0
        auth fails(delta): 0
encrypted packets(delta): 0
     encrypt fails(delta): 0
---------- End statistics

       object state: active
--------------- AOM

         cpp aom id: 894
         cgm aom id: 0
          n2 aom id: 891
          if aom id: 0
```

show crypto ipsec sa <ip> peer

このコマンドは、指定されたピアの IPsec SA ID を取得し、IOS レイヤから QFP レイヤまでのすべてのレイヤの SA を表示します。

```
Device# polaris-csr#show crypto ipsec sa peer 33.0.0.4 platform

interface: Tunnel0
    Crypto map tag: Tunnel0-head-0, local addr 33.0.0.3

   protected vrf: (none)
   local  ident (addr/mask/prot/port): (33.0.0.3/255.255.255.255/47/0)
   remote ident (addr/mask/prot/port): (33.0.0.4/255.255.255.255/47/0)
   current_peer 33.0.0.4 port 500
     PERMIT, flags={origin_is_acl,}
    #pkts encaps: 190, #pkts encrypt: 190, #pkts digest: 190
    #pkts decaps: 190, #pkts decrypt: 190, #pkts verify: 190
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0
    #pkts not decompressed: 0, #pkts decompress failed: 0
    #send errors 0, #recv errors 0

     local crypto endpt.: 33.0.0.3, remote crypto endpt.: 33.0.0.4
     plaintext mtu 1438, path mtu 1500, ip mtu 1500, ip mtu idb GigabitEthernet2
     current outbound spi: 0xA4A5244(172642884)
     PFS (Y/N): N, DH group: none

     inbound esp sas:
      spi: 0xBCD8840(198019136)
        transform: esp-aes esp-sha256-hmac ,
```

```
        in use settings ={Tunnel, }
        conn id: 2169, flow_id: CSR:169, sibling_flags FFFFFFFF80004048, crypto map:
Tunnel0-head-0
        sa timing: remaining key lifetime (k/sec): (4607985/3255)
        IV size: 16 bytes
        replay detection support: Y
        Status: ACTIVE(ACTIVE)

     inbound ah sas:

     inbound pcp sas:

     outbound esp sas:
      spi: 0xA4A5244(172642884)
        transform: esp-aes esp-sha256-hmac ,
        in use settings ={Tunnel, }
        conn id: 2170, flow_id: CSR:170, sibling_flags FFFFFFFF80004048, crypto map:
Tunnel0-head-0
        sa timing: remaining key lifetime (k/sec): (4607989/3255)
        IV size: 16 bytes
        replay detection support: Y
        Status: ACTIVE(ACTIVE)

     outbound ah sas:

     outbound pcp sas:
```

その他の参考資料

次の項では、IPsec アンチ リプレイ ウィンドウの拡張無効化の関連資料を示します。

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『Cisco IOS Security Command Reference』
IP セキュリティおよび暗号化	IPsec を使用した VPN のセキュリティの設定

標準

標準	タイトル
この機能でサポートされる新規の標準または変更された標準はありません。また、既存の標準のサポートは変更されていません。	--

MIB

MIB	MIB のリンク
この機能によってサポートされる新しい MIB または変更された MIB はありません。またこの機能による既存MIBのサポートに変更はありません。	選択したプラットフォーム、Cisco IOS XE リリース、およびフィーチャ セットの MIB を検索してダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

RFC

RFC	タイトル
この機能によりサポートされた新規 RFC または改訂 RFC はありません。またこの機能による既存 RFC のサポートに変更はありません。	--

シスコのテクニカル サポート

説明	リンク
シスコのサポート Web サイトでは、シスコの製品やテクノロジーに関するトラブルシューティングにお役立ていただけるように、マニュアルやツールをはじめとする豊富なオンライン リソースを提供しています。 お使いの製品のセキュリティ情報や技術情報を入手するために、Cisco Notification Service（Field Notice からアクセス）、Cisco Technical Services Newsletter、Really Simple Syndication（RSS）フィードなどの各種サービスに加入できます。 シスコのサポート Web サイトのツールにアクセスする際は、Cisco.com のユーザ ID およびパスワードが必要です。	http://www.cisco.com/en/US/support/index.html

IPsec アンチ リプレイ ウィンドウの拡張と無効化の機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *240 : IPsec* アンチ リプレイ ウィンドウの機能情報：拡張と無効化

機能名	リリース	機能情報
IPsec アンチ リプレイ ウィンドウの拡張と無効化	Cisco IOS XE Release 2.1 IPsec アンチリプレイウィンドウの拡張と無効化（2615ページ）	次のコマンドが導入または変更されました。**crypto ipsec security-association replay disable**、**ipsec security-association replay window-size**、**security-association replay disable**、**security-association replay window-size**
IPsec アンチリプレイは、CSR プラットフォームで QoS が有効になっている場合に機能します。	Cisco IOS XE リリース 16.6.1	この機能により、Cisco Cloud Services Router 1000V シリーズで QoS が有効になっている場合、IPSec アンチリプレイメカニズムのサポートが有効になります。 次のコマンドが導入または変更されました。**show platform hardware qfp active feature ipsec**、**show platform software ipsec fp active flow**、**show crypto ipsec sa**。
IPsec アンチリプレイは、ISR 4300/4200 プラットフォームで QoS が有効になっている場合に機能します。	Cisco IOS XE リリース 16.7.1	この機能により、ISR 44xx を除く ISR プラットフォームで QoS が有効になっている場合、IPsec アンチリプレイメカニズムが確実に機能します。
アンチリプレイ QoS/IPsec パケット損失の回避	Cisco IOS XE リリース 16.8.1	この機能により、IPSec アンチリプレイが有効な状態で QoS が使用されている場合に、IPsec アンチリプレイパケットのドロップが回避されます。 このサポートは、Octeon ベースの ASR プラットフォームにのみ追加されます。

第 178 章

IPsec VPN の Pre-fragmentation

IPsec VPN の Pre-fragmentation 機能で、最大伝送ユニット（MTU）サイズに近いパケットに対し、暗号化スループットが暗号化ハードウェア アクセラレータの速度で提供されることにより、Cisco IOS XE ルータと VPN クライアントとの間のパフォーマンスが向上します。同じサイズの単位にパケットが分割され、以降の処理ではフラグメンテーションが不要になります。

IPsec VPN の Pre-fragmentation の制約事項

この機能の設定前に次の情報を考慮してください。

- IPsec VPN の Pre-fragmentation は IPsec トンネル モードおよび GRE を使用する IPsec トンネル モードで動作し、IPsec トランスポート モードでは動作しません。
- トラフィックが単一方向のネットワーク上で復号ルータに IPsec VPN の Pre-fragmentation を設定しても、パフォーマンスは向上せず、それぞれのピアの動作は変わりません。
- 発信パケットの圧縮がオンになっている場合は、IPsec VPN の Pre-fragmentation は変換前に実行されます。
- IPsec VPN の Pre-fragmentation は、出力インターフェイス **crypto ipsec df-bit** の設定と着信パケットの「do not fragment」（DF）ビットの状態によって機能が異なります。次の表を参照してください。

表 *241 : IPsec VPN* の *Pre-fragmentation* の依存関係

IPsec VPN の Pre-fragmentation 機能の状態（イネーブル/ディセーブル）	出力インターフェイス「crypto ipsec df-bit」の設定	着信パケット DF ビットの状態	結果
イネーブル	crypto ipsec df-bit クリア	0	暗号化前にフラグメンテーションが実行されます。
イネーブル	crypto ipsec df-bit クリア	1	暗号化前にフラグメンテーションが実行されます。
ディセーブル	crypto ipsec df-bit クリア	0	暗号化後にフラグメンテーションが実行され、復号前にパケットが再編成されます。
ディセーブル	crypto ipsec df-bit クリア	1	暗号化後にフラグメンテーションが実行され、復号前にパケットが再編成されます。
イネーブル	crypto ipsec df-bit セット	0	暗号化前にフラグメンテーションが実行されます。
イネーブル	crypto ipsec df-bit セット	1	パケットがドロップされます。
ディセーブル	crypto ipsec df-bit セット	0	暗号化後にフラグメンテーションが実行され、復号前にパケットが再編成されます。
ディセーブル	crypto ipsec df-bit セット	1	パケットがドロップされます。
イネーブル	crypto ipsec df-bit コピー	0	暗号化前にフラグメンテーションが実行されます。
イネーブル	crypto ipsec df-bit コピー	1	パケットがドロップされます。
ディセーブル	crypto ipsec df-bit コピー	0	暗号化の後にフラグメンテーションが発生し、復号化の前にパケットがリアセンブルされます。
ディセーブル	crypto ipsec df-bit コピー	1	パケットがドロップされます。

IPsec VPN の Pre-fragmentation に関する情報

IPsec VPN の Pre-fragmentation

パケットのサイズが暗号化ルータのアウトバウンドリンクのMTUのサイズに近く、IPsecヘッダー付きでカプセル化されている場合は、アウトバウンドリンクのMTUを超えることがあります。これにより、暗号化後にパケット フラグメンテーションが発生します。よって復号化ルータでは、その復号化ルータのパフォーマンスを低下させているプロセスパスの当該パケットがリアセンブルされる必要があります。

IPsec VPN の Pre-fragmentation 機能により、プロセス パスではなく高パフォーマンスの CEF パスで復号化ルータが動作可能になるため、その復号化ルータのパフォーマンスが向上します。復号化ルータでは、トランスフォームセット（IPsecセキュリティアソシエーション（SA）の一部として設定）の利用可能な情報を基に、カプセル化されているパケットのサイズを事前に確認できます。パケットのサイズが出力インターフェイスの MTU を超えることが前もって確認されると、パケットは暗号化前にフラグメント化（分割）されます。この機能を使用すると、復号化前にプロセス レベルでパケットをリアセンブルすることがなくなるため、復号化のパフォーマンスと IPsec トラフィックの全体的なスループットが向上します。

（注） トンネル インターフェイスの Pre-fragmentation 機能はデフォルトでオフになっています。Pre-fragmentation によってパフォーマンスを向上させるには、トンネル インターフェイスの両端に同じ MTU があるようにしてから、Pre-fragmentation をオンにします。

暗号マップは、暗号化の前後に発生するフラグメンテーションの動作を定義するためには使用されなくなっています。現在、IPsec 仮想トンネル インターフェイス（仮想テンプレート インターフェイスともいう）（VTI）のフラグメンテーションの動作は、VTI で設定されている IP MTU の設定によって決定されます。

VTI の詳細については、IPsec 仮想トンネル インターフェイス機能のドキュメントを参照してください。

（注） フラグメンテーションを暗号化後に動作させる場合、VTI の IP MTU は、出力ルータ インターフェイスの IP MTU よりも大きい値に設定します。IP MTU の値を表示するには、**show ip interface tunnel** コマンドを使用します。

IPsec VPN の Pre-fragmentation の設定方法

IPsec VPN の Pre-fragmentation の設定

このタスクを実行して、IPsec VPN の Pre-Fragmentation を設定します。

手順の概要

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **ip mtu** *bytes*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface** *type number* 例： `Router(config-if)# interface tunnel0`	VTI が設定されるインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	**ip mtu** *bytes* 例： `Router(config-if)# ip mtu 1500` 例：	IPsec VPN の出力インターフェイスにおける IP パケットの VTI MTU サイズをバイト単位で設定します。 （注） フラグメンテーションを暗号化後に動作させる場合、VTI の IP MTU は、出力ルータ インターフェイスの IP MTU よりも大きい値に設定します。IP MTU の値を表示するには、**show ip interface tunnel** コマンドを使用します。

その他の参考資料

関連資料

関連項目	マニュアル タイトル
セキュリティ コマンド	『Cisco IOS Security Command Reference』
IPSec	IPsec 仮想トンネル インターフェイス機能のドキュメント

MIB

MIB	MIB のリンク
なし	選択したプラットフォーム、Cisco ソフトウェア リリース、およびフィーチャ セットの MIB を検索してダウンロードする場合は、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

シスコのテクニカル サポート

説明	リンク
右の URL にアクセスして、シスコのテクニカル サポートを最大限に活用してください。これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

IPsec VPN の Pre-fragmentation の機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *242 : IPsec VPN* の *Pre-fragmentation* の機能情報

機能名	リリース	機能情報
IPsec VPN の Pre-fragmentation	Cisco IOS XE 2.1	この機能で、最大伝送ユニット（MTU）サイズに近いパケットに対し、暗号化スループットが暗号化ハードウェア アクセラレータの速度で提供されることにより、Cisco IOS XE ルータと VPN クライアントとの間のパフォーマンスが向上します。同じサイズの単位にパケットが分割され、以降の処理ではフラグメンテーションが不要になります。 次のコマンドが導入または変更されました。**ip mtu (interface configuration) .**

第 179 章

Invalid Security Parameter Index Recovery

IP セキュリティ（IPsec）パケットの処理中に無効なセキュリティ パラメータ インデックス エラー（「Invalid SPI」として表示されます）が発生した場合、Invalid Security Parameter Index Recovery 機能によって、インターネット キー エクスチェンジ（IKE）セキュリティ アソシエーション（SA）を確立できます。「IKE」モジュールによって「Invalid SPI」エラーの通知が、発信側の IPsec ピアに対して送信され、セキュリティ アソシエーション データベース（SADB）の再同期化と、成功したパケット処理の再開が可能になります。

Invalid Security Parameter Index Recovery の前提条件

Invalid Security Parameter Index Recovery 機能を設定する前に、ルータ上で IKE および IPsec を有効化しておく必要があります。

Invalid Security Parameter Index Recovery の制約事項

IPsec ピアに対して「Invalid SPI」エラーを通知するために IKE SA を開始する場合、サービス妨害（DoS）攻撃が発生するリスクがあります。Invalid Security Parameter Index Recovery 機能には、そのようなリスクを最小化するためのメカニズムが内蔵されていますが、リスクが存在するため、Invalid Security Parameter Index Recovery 機能は、デフォルトでは有効化されていません。コマンドライン インターフェイス（CLI）を使用してコマンドをイネーブルにする必要があります。

Invalid Security Parameter Index Recovery に関する情報

機能の動作

あるIPsecピアが「死ぬ」（たとえば、リブートが発生したり、IPsecピアが何らかの理由によりリセットされたりした場合にピアが「死ぬ」可能性があります）と、IPsecの「ブラックホール化」が発生します。ピアの1つ（受信側のピア）は完全にリセットされるため、そのピアでは他のピアとのIKE SAが失われます。一般に、IPsecピアによって、SAを検出できないパケットが受信されると、そのピアによって、そのデータの発信者に対するIKE「INVALID SPI NOTIFY」メッセージの送信が試行されます。この通知はIKE SAを使用して送信されます。IKE SAが使用できない場合、受信側のピアによってパケットが廃棄されます。

（注） 1つのSAにつきピアは2つだけです。しかし、SADBは複数のSAを持てます。これにより、各SAは異なるピアとのアソシエーションを持ちます。

無効なセキュリティパラメータインデックス（SPI）が発生した場合、Invalid Security Parameter Index機能によって、データの発信者にIKE SAが設定され、IKE「INVALID SPI NOTIFY」メッセージが送信されます。データを発信したピアによって「INVALID SPI NOTIFY」メッセージが「参照」され、無効なSPIを持つIPsec SAが削除されます。発信側のピアからトラフィックがさらにある場合、IPsec SAは存在せず、新しいSAが設定されます。トラフィックが再び流れます。デフォルトの動作（つまり、Invalid Security Parameter Index機能が設定されていない状態）では、無効なSPIエラーの原因となったデータパケットは廃棄されます。発信側のピアによって、無効なSPIを持つIPsec SAを使用したデータの送信が続けられ、受信側のピアによってトラフィックが廃棄され続けます（その結果、「ブラックホール」が作成されます）。

IPsecモジュールではIKEモジュールが使用され、他のピアにIKE「INVALID SPI NOTIFY」メッセージが送信されます。無効なSPIリカバリが行われると、IPsec SAの設定自体によっていくつかのパケットが廃棄されますが、意味のあるパケット廃棄は一切行われません。

Invalid Security Parameter Index Recovery機能用にルータを設定するには、**crypto isakmp invalid-spi-recovery**コマンドを使用します。IKE SAは、このコマンドを設定しない限り開始されません。

Invalid Security Parameter Index Recovery の設定方法

Invalid Security Parameter Index Recovery の設定

Invalid Security Parameter Index Recovery機能を設定するには、次の手順を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **crypto isakmp invalid-spi-recovery**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**crypto isakmp invalid-spi-recovery** 例： `Router (config)# crypto isakmp invalid-spi-recovery`	IKE モジュール プロセスを開始します。それにより、IKE モジュールによって、受信側ピアに対して「Invalid SPI」エラーが発生したことが通知されます。

事前共有設定の確認

2 つのピア間におけるトラフィックに関する IPsec SA のステータスを確認するには、**show crypto ipsec sa** コマンドを使用します。IPsec SA が、あるピアでは使用可能で、他のピアでは使用不可の場合、「ブラック ホール化」の状況が発生します。この場合、無効な SPI エラーが受信側のピアのログに記録されます。コンソール ロギングをオンにするか、シスログ サーバを確認すると、これらのエラーもログに記録されていることがわかります。

次の図に、一般的な事前共有設定のトポロジを示します。ホスト 1 が発信側のピア（発信側）、ホスト 2 が受信側のピア（応答側）です。

図 *89 :* 事前共有設定トポロジ

手順の概要

1. ホスト 1 とホスト 2 の間における IKE および IPsec SA を開始します。
2. ルータ B 上の IKE および IPsec SA をクリアします。
3. ホスト 1 からのトラフィックをホスト 2 に送信し、新しい IKE および IPsec SA が正しく確立されているかどうかを確認します。
4. ルータ B に無効な SPI メッセージがないか確認します。

手順の詳細

ステップ 1 ホスト 1 とホスト 2 の間における IKE および IPsec SA を開始します。

Router A

例：

```
Router# show crypto isakmp sa
  f_vrf/i_vrf   dst            src             state       conn-id slot
       / 10.2.2.2              10.1.1.1        QM_IDLE               1       0
```

ルータ B

例：

```
Router# show crypto isakmp sa
  f_vrf/i_vrf   dst            src             state       conn-id slot
       /        10.1.1.1       10.2.2.2        QM_IDLE               1       0
```

ルータ A

例：

```
Router# show crypto ipsec sa interface fastethernet0/0
interface: FastEthernet0/0
    Crypto map tag: testtag1, local addr. 10.1.1.1
   protected vrf:
   local  ident (addr/mask/prot/port): (10.0.0.1/255.255.255.255/0/0)
   remote ident (addr/mask/prot/port): (10.0.2.2/255.255.255.255/0/0)
   current_peer: 10.2.2.2:500
     PERMIT, flags={origin_is_acl,}
    #pkts encaps: 10, #pkts encrypt: 10, #pkts digest: 10
    #pkts decaps: 10, #pkts decrypt: 10, #pkts verify: 10
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0
    #pkts not decompressed: 0, #pkts decompress failed: 0
    #send errors 0, #recv errors 0
     local crypto endpt.: 10.1.1.1, remote crypto endpt.: 10.2.2.2
     path mtu 1500, media mtu 1500
     current outbound spi: 7AA69CB7
     inbound esp sas:
      spi: 0x249C5062(614223970)
        transform: esp-des esp-sha-hmac ,
        in use settings ={Tunnel, }
        slot: 0, conn id: 5123, flow_id: 1, crypto map: testtag1
        crypto engine type: Hardware
        sa timing: remaining key lifetime (k/sec): (4537831/3595)
        IV size: 8 bytes
        replay detection support: Y
     inbound ah sas:
      spi: 0xB16D1587(2976716167)
        transform: ah-sha-hmac ,
        in use settings ={Tunnel, }
        slot: 0, conn id: 5121, flow_id: 1, crypto map: testtag1
        crypto engine type: Hardware
        sa timing: remaining key lifetime (k/sec): (4537831/3595)
        replay detection support: Y
     inbound pcp sas:
     outbound esp sas:
      spi: 0x7AA69CB7(2057739447)
```

```
        transform: esp-des esp-sha-hmac ,
        in use settings ={Tunnel, }
        slot: 0, conn id: 5124, flow_id: 2, crypto map: testtag1
        crypto engine type: Hardware
        sa timing: remaining key lifetime (k/sec): (4537835/3595)
        IV size: 8 bytes
        replay detection support: Y
      outbound ah sas:
       spi: 0x1214F0D(18960141)
        transform: ah-sha-hmac ,
        in use settings ={Tunnel, }
        slot: 0, conn id: 5122, flow_id: 2, crypto map: testtag1
        crypto engine type: Hardware
        sa timing: remaining key lifetime (k/sec): (4537835/3594)
        replay detection support: Y
      outbound pcp sas:
```

ルータ B

例：

```
Router# show crypto ipsec sa interface Fastethernet1/0
interface: FastEthernet1/0
    Crypto map tag: testtag1, local addr. 10.2.2.2
   protected vrf:
   local  ident (addr/mask/prot/port): (10.0.2.2/255.255.255.255/0/0)
   remote ident (addr/mask/prot/port): (10.0.0.1/255.255.255.255/0/0)
   current_peer: 10.1.1.1:500
     PERMIT, flags={origin_is_acl,}
    #pkts encaps: 10, #pkts encrypt: 10, #pkts digest: 10
    #pkts decaps: 10, #pkts decrypt: 10, #pkts verify: 10
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0
    #pkts not decompressed: 0, #pkts decompress failed: 0
    #send errors 0, #recv errors 0
     local crypto endpt.: 10.2.2.2, remote crypto endpt.: 10.1.1.1
     path mtu 1500, media mtu 1500
     current outbound spi: 249C5062
     inbound esp sas:
      spi: 0x7AA69CB7(2057739447)
        transform: esp-des esp-sha-hmac ,
        in use settings ={Tunnel, }
        slot: 0, conn id: 5123, flow_id: 1, crypto map: testtag1
        crypto engine type: Hardware
        sa timing: remaining key lifetime (k/sec): (4421281/3593)
        IV size: 8 bytes
        replay detection support: Y
     inbound ah sas:
      spi: 0x1214F0D(18960141)
        transform: ah-sha-hmac ,
        in use settings ={Tunnel, }
        slot: 0, conn id: 5121, flow_id: 1, crypto map: testtag1
        crypto engine type: Hardware
        sa timing: remaining key lifetime (k/sec): (4421281/3593)
        replay detection support: Y
     inbound pcp sas:
     outbound esp sas:
      spi: 0x249C5062(614223970)
        transform: esp-des esp-sha-hmac ,
        in use settings ={Tunnel, }
        slot: 0, conn id: 5124, flow_id: 2, crypto map: testtag1
        crypto engine type: Hardware
        sa timing: remaining key lifetime (k/sec): (4421285/3593)
        IV size: 8 bytes
```

```
        replay detection support: Y
      outbound ah sas:
       spi: 0xB16D1587(2976716167)
        transform: ah-sha-hmac ,
        in use settings ={Tunnel, }
        slot: 0, conn id: 5122, flow_id: 2, crypto map: testtag1
        crypto engine type: Hardware
        sa timing: remaining key lifetime (k/sec): (4421285/3592)
        replay detection support: Y
      outbound pcp sas:
```

ステップ 2 ルータ B 上の IKE および IPsec SA をクリアします。

例：

```
Router# clear crypto isakmp
Router# clear crypto sa
Router# show crypto isakmp sa
  f_vrf/i_vrf   dst            src             state       conn-id slot
       /        10.2.2.2.       10.1.1.1      MM_NO_STATE           1       0 (deleted)
Router# show crypto ipsec sa
interface: FastEthernet1/0
    Crypto map tag: testtag1, local addr. 10.2.2.2
   protected vrf:
   local  ident (addr/mask/prot/port): (10.0.2.2/255.255.255.255/0/0)
   remote ident (addr/mask/prot/port): (10.0.0.1/255.255.255.255/0/0)
   current_peer: 10.1.1.1:500
     PERMIT, flags={origin_is_acl,}
    #pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
    #pkts decaps: 0, #pkts decrypt: 0, #pkts verify: 0
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0
    #pkts not decompressed: 0, #pkts decompress failed: 0
    #send errors 0, #recv errors 0
     local crypto endpt.: 10.2.2.2, remote crypto endpt.: 10.1.1.1
     path mtu 1500, media mtu 1500
     current outbound spi: 0
     inbound esp sas:
     inbound ah sas:
     inbound pcp sas:
     outbound esp sas:
     outbound ah sas:
     outbound pcp sas:
```

ステップ 3 ホスト 1 からのトラフィックをホスト 2 に送信し、新しい IKE および IPsec SA が正しく確立されているかどうかを確認します。

例：

```
ping
Protocol [ip]: ip
Target IP address: 10.0.2.2
Repeat count [5]: 30
Datagram size [100]: 100
Timeout in seconds [2]:
Extended commands [n]: no
Sweep range of sizes [n]: n
Type escape sequence to abort.
Sending 30, 100-byte ICMP Echos to 10.0.2.2, timeout is 2 seconds:
..!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Success rate is 93 percent (28/30), round-trip min/avg/max = 1/3/8 ms
RouterB# show crypto isakmp sa
```

```
  f_vrf/i_vrf   dst            src             state       conn-id slot
       /        10.1.1.1       10.2.2.2     QM_IDLE              3       0
       /        10.1.1.1       10.2.2.2      MM_NO_STATE          1       0 (deleted)
RouterB# show crypto ipsec sa
interface: FastEthernet1/0
    Crypto map tag: testtag1, local addr. 10.2.2.2
   protected vrf:
   local  ident (addr/mask/prot/port): (10.0.2.2/255.255.255.255/0/0)
   remote ident (addr/mask/prot/port): (10.0.0.1/255.255.255.255/0/0)
   current_peer: 10.1.1.1:500
     PERMIT, flags={origin_is_acl,}
    #pkts encaps: 28, #pkts encrypt: 28, #pkts digest: 28
    #pkts decaps: 28, #pkts decrypt: 28, #pkts verify: 28
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0
    #pkts not decompressed: 0, #pkts decompress failed: 0
    #send errors 0, #recv errors 0
     local crypto endpt.: 10.2.2.2, remote crypto endpt.: 10.1.1.1
     path mtu 1500, media mtu 1500
     current outbound spi: D763771F
     inbound esp sas:
      spi: 0xE7AB4256(3886760534)
        transform: esp-des esp-sha-hmac ,
        in use settings ={Tunnel, }
        slot: 0, conn id: 5127, flow_id: 3, crypto map: testtag1
        crypto engine type: Hardware
        sa timing: remaining key lifetime (k/sec): (4502463/3596)
        IV size: 8 bytes
        replay detection support: Y
     inbound ah sas:
      spi: 0xF9205CED(4179647725)
        transform: ah-sha-hmac ,
        in use settings ={Tunnel, }
        slot: 0, conn id: 5125, flow_id: 3, crypto map: testtag1
        crypto engine type: Hardware
        sa timing: remaining key lifetime (k/sec): (4502463/3596)
        replay detection support: Y
     inbound pcp sas:
     outbound esp sas:
      spi: 0xD763771F(3613619999)
        transform: esp-des esp-sha-hmac ,
        in use settings ={Tunnel, }
        slot: 0, conn id: 5128, flow_id: 4, crypto map: testtag1
        crypto engine type: Hardware
        sa timing: remaining key lifetime (k/sec): (4502468/3596)
        IV size: 8 bytes
        replay detection support: Y
     outbound ah sas:
      spi: 0xEB95406F(3952427119)
        transform: ah-sha-hmac ,
        in use settings ={Tunnel, }
        slot: 0, conn id: 5126, flow_id: 4, crypto map: testtag1
        crypto engine type: Hardware
        sa timing: remaining key lifetime (k/sec): (4502468/3595)
        replay detection support: Y
     outbound pcp sas:
RouterA# show crypto isakmp sa
  f_vrf/i_vrf   dst            src             state       conn-id slot
       /        10.2.2.2       10.1.1.1      MM_NO_STATE          1       0 (deleted)
       /        10.2.2.2       10.1.1.1      QM_IDLE              2       0
```

ステップ 4 ルータ B に無効な SPI メッセージがないか確認します。

例：

```
Router# show logging
Syslog logging: enabled (10 messages dropped, 13 messages rate-limited, 0 flushes, 0 overruns, xml
 disabled)
    Console logging: disabled
    Monitor logging: level debugging, 0 messages logged, xml disabled
    Buffer logging: level debugging, 43 messages logged, xml disabled
    Logging Exception size (8192 bytes)
    Count and timestamp logging messages: disabled
    Trap logging: level informational, 72 message lines logged
Log Buffer (8000 bytes):
*Mar 24 20:55:45.739: %CRYPTO-4-RECVD_PKT_INV_SPI: decaps: rec'd IPSEC packet has invalid spi for
        destaddr=10.2.2.2, prot=51, spi=0x1214F0D(18960141), srcaddr=10.1.1.1
*Mar 24 20:55:47.743: IPSEC(validate_proposal_request): proposal part #1,
  (key eng. msg.) INBOUND local= 10.2.2.2, remote= 10.1.1.1,
    local_proxy= 10.0.2.2/255.255.255.255/0/0 (type=1),
    remote_proxy= 10.0.0.1/255.255.255.255/0/0 (type=1),
    protocol= AH, transform= ah-sha-hmac ,
    lifedur= 0s and 0kb,
    spi= 0x0(0), conn_id= 0, keysize= 0, flags= 0x2
*Mar 24 20:55:47.743: IPSEC(validate_proposal_request): proposal part #2,
  (key eng. msg.) INBOUND local= 10.2.2.2, remote= 10.1.1.1,
    local_proxy= 10.0.2.2/255.255.255.255/0/0 (type=1),
    remote_proxy= 10.0.0.1/255.255.255.255/0/0 (type=1),
    protocol= ESP, transform= esp-des esp-sha-hmac ,
    lifedur= 0s and 0kb,
    spi= 0x0(0), conn_id= 0, keysize= 0, flags= 0x2
*Mar 24 20:55:47.743: IPSEC(kei_proxy): head = testtag1, map->ivrf = , kei->ivrf =
*Mar 24 20:55:47.743: IPSEC(key_engine): got a queue event with 2 kei messages
*Mar 24 20:55:47.743: IPSEC(spi_response): getting spi 4179647725 for SA
        from 10.2.2.2        to 10.1.1.1     for prot 2
*Mar 24 20:55:47.747: IPSEC(spi_response): getting spi 3886760534 for SA
        from 10.2.2.2     to 10.1.1.1        for prot 3
*Mar 24 20:55:48.071: IPSec: Flow_switching Allocated flow for flow_id 939524099
*Mar 24 20:55:48.071: IPSec: Flow_switching Allocated flow for flow_id 939524100
*Mar 24 20:55:48.135: IPSEC(key_engine): got a queue event with 4 kei messages
*Mar 24 20:55:48.135: IPSEC(initialize_sas): ,
  (key eng. msg.) INBOUND local= 10.2.2.2, remote= 10.1.1.1,
    local_proxy= 10.0.2.2/0.0.0.0/0/0 (type=1),
    remote_proxy= 10.0.0.1/0.0.0.0/0/0 (type=1),
    protocol= AH, transform= ah-sha-hmac ,
    lifedur= 3600s and 4608000kb,
    spi= 0xF9205CED(4179647725), conn_id= 939529221, keysize= 0, flags= 0x2
*Mar 24 20:55:48.135: IPSEC(initialize_sas): ,
  (key eng. msg.) OUTBOUND local= 10.2.2.2, remote= 10.1.1.1,
    local_proxy= 10.0.2.2/0.0.0.0/0/0 (type=1),
    remote_proxy= 10.0.0.1/0.0.0.0/0/0 (type=1),
    protocol= AH, transform= ah-sha-hmac ,
    lifedur= 3600s and 4608000kb,
    spi= 0xEB95406F(3952427119), conn_id= 939529222, keysize= 0, flags= 0xA
*Mar 24 20:55:48.135: IPSEC(initialize_sas): ,
  (key eng. msg.) INBOUND local= 10.2.2.2, remote= 10.1.1.1,
    local_proxy= 10.0.2.2/0.0.0.0/0/0 (type=1),
    remote_proxy= 10.0.0.1/0.0.0.0/0/0 (type=1),
    protocol= ESP, transform= esp-des esp-sha-hmac ,
    lifedur= 3600s and 4608000kb,
    spi= 0xE7AB4256(3886760534), conn_id= 939529223, keysize= 0, flags= 0x2
*Mar 24 20:55:48.135: IPSEC(initialize_sas): ,
  (key eng. msg.) OUTBOUND local= 10.2.2.2, remote= 10.1.1.1,
    local_proxy= 10.0.2.2/0.0.0.0/0/0 (type=1),
    remote_proxy= 10.0.0.1/0.0.0.0/0/0 (type=1),
    protocol= ESP, transform= esp-des esp-sha-hmac ,
    lifedur= 3600s and 4608000kb,
    spi= 0xD763771F(3613619999), conn_id= 939529224, keysize= 0, flags= 0xA
```

```
*Mar 24 20:55:48.139: IPSEC(kei_proxy): head = testtag1, map->ivrf = , kei->ivrf =
*Mar 24 20:55:48.139: IPSEC(mtree_add_ident): src 10.2.2.2, dest 10.1.1.1, dest_port 0
*Mar 24 20:55:48.139: IPSEC(create_sa): sa created,
  (sa) sa_dest= 10.1.1.1, sa_prot= 51,
    sa_spi= 0xF9205CED(4179647725),
    sa_trans= ah-sha-hmac , sa_conn_id= 939529221
*Mar 24 20:55:48.139: IPSEC(create_sa): sa created,
  (sa) sa_dest= 10.2.2.2, sa_prot= 51,
    sa_spi= 0xEB95406F(3952427119),
    sa_trans= ah-sha-hmac , sa_conn_id= 939529222
*Mar 24 20:55:48.139: IPSEC(create_sa): sa created,
  (sa) sa_dest= 10.1.1.1, sa_prot= 50,
    sa_spi= 0xE7AB4256(3886760534),
    sa_trans= esp-des esp-sha-hmac , sa_conn_id= 939529223
*Mar 24 20:55:48.139: IPSEC(create_sa): sa created,
  (sa) sa_dest= 10.2.2.2, sa_prot= 50,
    sa_spi= 0xD763771F(3613619999),
    sa_trans= esp-des esp-sha-hmac , sa_conn_id= 939529224
ipseca-72a#
```

Invalid Security Parameter Index Recovery の設定例

Invalid Security Parameter Index Recovery：例

次に、Invalid Security Parameter Index Recovery がルータ A とルータ B に設定されている例を示します。次の例には、この例で使用されるトポロジが示されています。

ルータ A

```
Router# show running-config
Building configuration...
Current configuration : 2048 bytes
!
version 2.1
no service pad
service timestamps debug datetime msec localtime
service timestamps log datetime msec localtime
no service password-encryption
service tcp-small-servers
!
hostname ipseca-71a
!
logging queue-limit 100
no logging console
enable secret 5 $1$4GZB$L2YOmnenOCNAu0jgFxebT/
enable password lab
!
clock timezone PST -8
clock summer-time PDT recurring
ip subnet-zero
!
!
no ip domain lookup
!
```

```
ip cef
ip audit notify log
ip audit po max-events 100
mpls ldp logging neighbor-changes
no ftp-server write-enable
!
!
no voice hpi capture buffer
no voice hpi capture destination
!
!
crypto isakmp policy 1
 authentication pre-share
 lifetime 180
crypto isakmp key 0 1234 address 10.2.2.2
crypto isakmp invalid-spi-recovery
!
!
crypto ipsec transform-set auth2 ah-sha-hmac esp-des esp-sha-hmac
!
crypto map testtag1 10 ipsec-isakmp
 set peer 10.2.2.2
 set transform-set auth2
 match address 150
!
!
controller ISA 5/1
!
!
interface FastEthernet0/0
 ip address 10.1.1.1 255.0.0.0
 no ip route-cache cef
 duplex full
 speed 100
 crypto map testtag1
!
interface FastEthernet0/1
 ip address 10.0.0.1 255.0.0.0
 no ip route-cache cef
 duplex auto
 speed auto
!
interface Serial1/0
 no ip address
 no ip route-cache
 no ip mroute-cache
 shutdown
 serial restart_delay 0
 clockrate 128000
!
interface Serial1/1
 no ip address
 no ip route-cache
 no ip mroute-cache
 shutdown
 serial restart_delay 0
 clockrate 128000
!
interface Serial1/2
 no ip address
 no ip route-cache
 no ip mroute-cache
 shutdown
 serial restart_delay 0
```

```
!
interface Serial1/3
 no ip address
 no ip route-cache
 no ip mroute-cache
 shutdown
 no keepalive
 serial restart_delay 0
 clockrate 128000
!
ip classless
ip route 10.3.3.3 255.0.0.0 10.2.0.1
no ip http server
no ip http secure-server
!
!
access-list 150 permit ip host 10.0.0.1 host 10.0.2.2
dialer-list 1 protocol ip permit
dialer-list 1 protocol ipx permit
!
!
call rsvp-sync
!
!
mgcp profile default
!
!
line con 0
 exec-timeout 0 0
line aux 0
line vty 0 4
 password lab
 login
!
!
end
ipseca-71a#
```

ルータ B

```
Router# show running-config
Building configuration...
Current configuration : 2849 bytes
!
version 2.1
no service pad
service timestamps debug datetime msec localtime
service timestamps log datetime msec localtime
no service password-encryption
service udp-small-servers
service tcp-small-servers
!
hostname ipseca-72a
!
logging queue-limit 100
no logging console
enable secret 5 $1$kKqL$5Th5Qhw1ubDkkK90KWFxi1
enable password lab
!
clock timezone PST -8
clock summer-time PDT recurring
ip subnet-zero
!
```

```
!
no ip domain lookup
!
ip cef
ip audit notify log
ip audit po max-events 100
mpls ldp logging neighbor-changes
no ftp-server write-enable
!
!
no voice hpi capture buffer
no voice hpi capture destination
!
!
mta receive maximum-recipients 0
!
!
crypto isakmp policy 1
 authentication pre-share
 lifetime 180
crypto isakmp key 0 1234 address 10.1.1.1
crypto isakmp invalid-spi-recovery
!
!
crypto ipsec transform-set auth2 ah-sha-hmac esp-des esp-sha-hmac
!
crypto map testtag1 10 ipsec-isakmp
 set peer 10.1.1.1
 set transform-set auth2
 match address 150
!
!
controller ISA 5/1
!
!
interface FastEthernet0/0
 no ip address
 no ip route-cache
 no ip mroute-cache
 shutdown
 duplex half
!
interface FastEthernet1/0
 ip address 10.2.2.2 255.0.0.0
 no ip route-cache cef
 duplex half
 crypto map testtag1
!
interface FastEthernet1/1
 ip address 10.0.2.2 255.0.0.0
 no ip route-cache cef
 duplex half
!
interface FastEthernet1/2
 no ip address
 no ip route-cache
 no ip mroute-cache
 shutdown
 duplex half
!
interface FastEthernet1/3
 no ip address
 no ip route-cache
 no ip mroute-cache
```

```
 shutdown
 duplex half
!
interface FastEthernet1/4
 no ip address
 no ip route-cache
 no ip mroute-cache
 shutdown
 duplex half
!
interface FastEthernet1/5
 no ip address
 no ip route-cache
 no ip mroute-cache
 shutdown
 duplex half
!
interface FastEthernet1/6
 no ip address
 no ip route-cache
 no ip mroute-cache
 shutdown
 duplex half
!
interface FastEthernet1/7
 no ip address
 no ip route-cache
 no ip mroute-cache
 shutdown
 duplex half
!
interface Serial3/0
 no ip address
 no ip route-cache
 no ip mroute-cache
 shutdown
 serial restart_delay 0
!
interface Serial3/1
 no ip address
 no ip route-cache
 no ip mroute-cache
 shutdown
 serial restart_delay 0
 clockrate 128000
!
interface Serial3/2
 no ip address
 no ip route-cache
 no ip mroute-cache
 shutdown
 serial restart_delay 0
!
interface Serial3/3
 no ip address
 no ip route-cache
 no ip mroute-cache
 shutdown
 no keepalive
 serial restart_delay 0
 clockrate 128000
!
ip classless
ip route 10.0.0.0 255.0.0.0 10.2.0.1
```

```
no ip http server
no ip http secure-server
!
!
access-list 150 permit ip host 10.0.2.2 host 10.0.0.1
dialer-list 1 protocol ip permit
dialer-list 1 protocol ipx permit
!
!
call rsvp-sync
!
!
mgcp profile default
!
dial-peer cor custom
!
!
gatekeeper
 shutdown
!
!
line con 0
 exec-timeout 0 0
 stopbits 1
line aux 0
 stopbits 1
line vty 0 4
 password lab
 login
!
!
end
```

その他の参考資料

次の項では、Invalid Security Parameter Index Recovery に関連した参考資料を示します。

関連資料

関連項目	マニュアル タイトル
IKE の設定	「Configuring Internet Key Exchange for IPsec VPNs」

標準

標準	タイトル
この機能でサポートされる新規の標準または変更された標準はありません。また、既存の標準のサポートは変更されていません。	--

MIB

MIB	MIB のリンク
この機能によってサポートされる新しい MIB または変更された MIB はありません。またこの機能による既存 MIB のサポートに変更はありません。	選択したプラットフォーム、Cisco IOS XE ソフトウェア リリース、およびフィーチャ セットの MIB の場所を検索しダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

RFC

RFC	タイトル
この機能によりサポートされた新規 RFC または改訂 RFC はありません。またこの機能による既存 RFC のサポートに変更はありません。	--

シスコのテクニカル サポート

説明	リンク
シスコのサポート Web サイトでは、シスコの製品やテクノロジーに関するトラブルシューティングにお役立ていただけるように、マニュアルやツールをはじめとする豊富なオンライン リソースを提供しています。 お使いの製品のセキュリティ情報や技術情報を入手するために、Cisco Notification Service（Field Notice からアクセス）、Cisco Technical Services Newsletter、Really Simple Syndication（RSS）フィードなどの各種サービスに加入できます。 シスコのサポート Web サイトのツールにアクセスする際は、Cisco.com のユーザ ID およびパスワードが必要です。	http://www.cisco.com/en/US/support/index.html

Invalid Security Parameter Index Recovery の機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだ

けを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *243 : Invalid Security Parameter Index Recovery* の機能情報

機能名	リリース	機能情報
Invalid Special Parameter Index（SPI）Recovery	Cisco IOS XE Release 2.1	IPsec パケット処理で、無効な SPI が検出された場合は、Invalid Security Parameter Index Recovery 機能によって、IKE SA が確立されます。「IKE」モジュールによって「Invalid SPI」エラーの通知が、発信側の IPsec ピアに対して送信され、セキュリティ アソシエーション データベース（SADB）の再同期化と、成功したパケット処理の再開が可能になります。 次のコマンドが導入または変更されました。**crypto isakmp invalid-spi-recovery.**

第 180 章

「IPsec Dead Peer Detection Periodic Message Option」

IPSecデッドピア検出定期メッセージオプション機能を使用すれば、ルータに対し、そのインターネットキーエクスチェンジ（IKE）ピアの活性を定期的に照会するよう設定できます。このオプションを使用すると、デフォルトのオンデマンドデッドピア検出機能を使用した場合に比べ、停止しているピアをより早期に検出できます。

IPSec デッド ピア検出定期メッセージ オプションの前提条件

IPSecデッドピア検出定期メッセージオプション機能を設定するには、次のことが必要です。

- IP セキュリティ（IPsec）の設定についての知識。
- DPD（Dead Peer Detection）がサポートされている IKE ピア。DPD をサポートしているのは、Cisco VPN 3000 コンセントレータ、Cisco PIX ファイアウォール、Cisco VPN Client、およびすべての動作モードの Cisco IOS XE ソフトウェア（サイト間および Easy VPN サーバー）などです。

IPSec デッド ピア検出定期メッセージ オプションの制約事項

定期的な DPD を使用すると、ルータによって、オンデマンドの DPD と比較してより速い応答時間で無応答の IKE ピアを検知できる可能性があります。ただし、定期的な DPD では、余分なオーバーヘッドが発生します。大量の IKE ピアと通信する場合は、オンデマンドの DPD の方を検討してください。

IPSec デッド ピア検出定期メッセージ オプションに関する情報

DPD および Cisco IOS XE キープアライブ機能の動作

DPD および Cisco IOS XE キープアライブは、タイマーに基づいて機能します。タイマーが 10 秒に設定されている場合、ルータは10秒毎に「hello」メッセージが送信されます（もちろん、ルータによってピアからの「hello」メッセージが受信された場合は除きます）。IOS キープアライブおよび定期的な DPD の利点は、デッド ピアの検知が早くなることです。しかし、IOS キープアライブおよび定期的な DPD では、かなりの頻度でメッセージを定期的に送信する必要があります。頻繁にメッセージを送信する結果、通信を行うピアによって暗号化および復号化しなければならないパケット数が増加します。

DPDにはオンデマンド方式もあります。対称的なこのオンデマンド方式がデフォルトです。オンデマンド DPD では、トラフィック パターンに基づいてメッセージが送信されます。たとえば、ルータによって発信トラフィックが送信される必要があり、ピアの活性に疑問がある場合、ルータによって DPD メッセージが送信され、ピアのステータスが照会されます。ルータに送信するトラフィックがない場合、DPD メッセージは送信されません。ピアが停止しており、ピアに送信するトラフィックがルータにない場合、IKE または IPsec セキュリティ アソシエーション（SA）のキー再生成が必要でないかぎり、ルータによる検知は行われません（ルータによるピアとの通信が行われない場合、ピアの活性は重要ではありません）。一方、ピアに送信するトラフィックがルータにあり、ピアの応答がない場合は、ピアのステートを判断するために、ルータによって DPD メッセージが開始されます。

IPSec デッド ピア検出定期メッセージ オプションの使用

IPSec デッド ピア検出（DPD）定期メッセージ オプション機能では、DPD メッセージが定期的に「強制される」ようルータを設定できます。この強制方式の結果、デッドピアが早期に検知されます。たとえば、送信するトラフィックがルータにない場合でも、DPDメッセージが定期的に送信され、ピアが停止していた場合、IKE SAによる検知がタイムアウトになるまでルータが待機する必要はありません。

DPD 定期メッセージオプションを設定する場合、**crypto isakmp keepalive** コマンドは **periodic** キーワードを指定して使用する必要があります。**periodic** キーワードを指定しない場合、ルータはデフォルトのオンデマンド方式になります。

（注） **crypto isakmp keepalive** コマンドを設定すると、Cisco IOS ソフトウェアは、ピアがサポートしているプロトコルに応じて、Cisco IOS キープアライブまたは DPD の使用についてネゴシエーションを行います。

暗号マップ内の複数のピアとの DPD および Cisco IOS XE キープアライブ機能の使用

暗号マップ内で DPD および Cisco IOS XE キープアライブ機能を複数のピアと組み合わせることにより、ステートレス フェールオーバーを実現できます。DPD により、ルータによる停止 IKE ピアの検知が可能となり、ルータによって停止状態が検知されると、ルータによってピアに対する IPsec と IKE SA が削除されます。複数のピアを設定している場合、ルータによって、次にリストされているピアへの切り替えが行われ、ステートレス フェールオーバーが実現します。

IPSec デッド ピア検出定期メッセージ オプションの設定方法

定期的な DPD メッセージの設定

定期的な DPD メッセージを設定するには、次の手順を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **crypto isakmp keepalive** *seconds* [*retries*] [**periodic** | **on-demand**]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。

	コマンドまたはアクション	目的
ステップ 2	**configure terminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**crypto isakmp keepalive** *seconds* [*retries*] [**periodic** | **on-demand**] 例： `Router (config)# crypto isakmp keepalive 10 periodic`	ゲートウェイによるピアへの DPD メッセージの送信を許可します。 • *seconds*：**periodic** キーワードを使用する場合、この引数には DPD メッセージの間隔を秒数で指定します。範囲は 10 ～ 3600 秒です。 **on-demand** キーワードを使用する場合、この引数には、送信するデータ（IPSec）トラフィックがあるときに、DPD リトライメッセージを送信するまでピアからトラフィックを受信しない間に待機する秒数を指定します。範囲は 10 ～ 3600 秒です。 （注） 間隔を指定しない場合、エラーメッセージが表示されます。 • *retry-seconds*：（任意）ピアによって DPD リトライメッセージが失われた場合の DPD リトライメッセージの送信間隔を秒数で指定します。範囲は 2 ～ 60 秒です。 1 つの DPD メッセージがピアで失われると、ルータはよりアグレッシブな状態に移行し、より短いリトライ間隔で DPD リトライ メッセージを送信します。ピアによって DPD リトライ メッセージが失われた場合のこの間隔は、DPD リトライ間の秒数です。デフォルトで、DPD リトライ メッセージは 2 秒ごとに送信されます。アグレッシブな 5 回の DPD リトライ メッセージが失われると、トンネルがダウンした状態としてマークされます。 （注） IPsec ハイ アベイラビリティ（HA）を使用して DPD を設定するには、デフォルト（2 秒）以外の値を使用することを推奨します。HA には、キープアライブ時間を 10 秒、試行を 5 回に設定するのが適しています。その時間が、ルータがアクティブ モードになるためにかかる時間であるからです。

	コマンドまたはアクション	目的
		• **periodic**：（任意）DPD メッセージが定期的に送信されます。 • **on-demand**：（任意）デフォルトの動作です。DPD リトライがオンデマンドで送信されます。 （注） このオプションはデフォルトであるため、**on-demand** キーワードは設定の出力に表示されません。

暗号マップ内の複数のピアとの DPD および Cisco IOS XE キープアライブの設定

DPD および IOS キープアライブを、クリプト マップと組み合わせて使用するように設定し、ステートレス フェールオーバーを実現するには、次の手順を実行します。この設定により、最初のピアが停止していることが検知されると、ルータによってピア リストが循環されます。

手順の概要

1. **enable**
2. **configure terminal**
3. **crypto map** *map-name seq-num* **ipsec-isakmp**
4. **set peer** {*host-name* [**dynamic**] | *ip-address*}
5. **set transform-set** *transform-set-name*
6. **match address** [*access-list-id* | *name*]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**crypto map** *map-name seq-num* **ipsec-isakmp** 例： `Router (config)# crypto map green 1 ipsec-isakmp`	クリプト マップ コンフィギュレーション モードを開始して、クリプト マップ エントリを作成または変更します。

	コマンドまたはアクション	目的
		• **ipsec-isakmp** キーワードは、このクリプトマップエントリによって指定されたトラフィックを保護するための IPsec SA を確立するために、IKE が使用されることを示します。
ステップ 4	**set peer** {*host-name* [**dynamic**] | *ip-address*} 例： `Router (config-crypto-map)# set peer 10.12.12.12`	クリプト マップ内の IPsec ピアを指定します。 • このコマンドを繰り返すことによって、複数のピアを指定できます。
ステップ 5	**set transform-set** *transform-set-name* 例： `Router (config-crypto-map)# set transform-set txfm`	クリプト マップ エントリで使用可能なトランスフォーム セットを指定します。 • このコマンドを繰り返すことによって、複数のトランスフォーム セットを指定できます。
ステップ 6	**match address** [*access-list-id* | *name*] 例： `Router (config-crypto-map)# match address 101`	クリプト マップ エントリの拡張アクセス リストを指定します。

DPD が有効化されていることの確認

DPD を使用すれば、ピアが到達不能になった時に、ルータによる IKE ステートのクリアが可能になります。DPD が有効化されており、ピアがしばらくの間到達不能になった場合、**clear crypto session** コマンドを使用して、手動で IKE と IPsec SA をクリアできます。

debug crypto isakmp コマンドを使用すると、DPD が有効化されていることを確認できます。

手順の概要

1. **enable**
2. **clear crypto session** [**local** *ip-address* [**port** *local-port*]] [**remote** *ip-address* [**port** *remote-port*]] | [**fvrf** *vrf-name*] [**ivrf** *vrf-name*]
3. **debug crypto isakmp**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。

	コマンドまたはアクション	目的
ステップ 2	**clear crypto session** [**local** *ip-address* [**port** *local-port*]] [**remote** *ip-address* [**port** *remote-port*]] | [**fvrf** *vrf-name*] [**ivrf** *vrf-name*] 例： `Router# clear crypto session`	暗号セッション（IPsec および IKE SA）を削除します。
ステップ 3	**debug crypto isakmp** 例： `Router# debug crypto isakmp`	IKE イベントに関するメッセージを表示します。

IPSec デッド ピア検出定期メッセージ オプションの設定例

定期的な DPD を有効化したサイト間設定の例

次の設定は、定期的な DPD が有効になっているサイト間設定用です。設定は、IKE フェーズ 1 ポリシー用と IKE 事前共有キー用です。

IKE フェーズ 1 ポリシー

```
crypto isakmp policy 1
  encryption aes
  authentication pre-share
  group 14
!
```

IKE 事前共有キー

```
crypto isakmp key kd94j1ksldz address 10.2.80.209 255.255.255.0
crypto isakmp keepalive 10 periodic
crypto ipsec transform-set Trans1 esp-aes esp-sha-hmac

!
!
interface
  ip address 10.1.32.14 255.255.255.0
  speed auto

!
```

debug crypto isakmp コマンドを使用した DPD 設定の確認の例

次の **debug crypto isakmp** コマンドの出力例では、IKE DPD が有効化されていることを確認しています。

```
*Mar 25 15:17:14.131: ISAKMP:(0:1:HW:2):IKE_DPD is enabled, initializing timers
```

IKE DPD がイネーブルになっていること（および、ピアによって DPD がサポートされていること）を確認するには、定期的な DPD をイネーブルにする時に、コマンドによって指定された間隔で次のデバッグ メッセージが出力されることを確認する必要があります。

```
*Mar 25 15:18:52.107: ISAKMP:(0:1:HW:2): sending packet to 10.2.80.209 my_port
500 peer_port 500 (I) QM_IDLE
*Mar 25 15:18:52.107: ISAKMP:(0:1:HW:2):purging node 899852982 *Mar 25 15:18:52.111:
ISAKMP:(0:1:HW:2):Input = IKE_MESG_FROM_TIMER,
IKE_TIMER_IM_ALIVE
*Mar 25 15:18:52.111: ISAKMP:(0:1:HW:2):Old State = IKE_P1_COMPLETE  New State =
IKE_P1_COMPLETE
```

上記のメッセージは、DPD R_U_THERE メッセージの送信に対応しています。

```
*Mar 25 15:18:52.123: ISAKMP (0:268435457): received packet from 10.2.80.209
dport 500 sport 500 Global (I) QM_IDLE
*Mar 25 15:18:52.123: ISAKMP: set new node -443923643 to QM_IDLE *Mar 25 15:18:52.131:
ISAKMP:(0:1:HW:2): processing HASH payload. message ID =
-443923643
*Mar 25 15:18:52.131: ISAKMP:(0:1:HW:2): processing NOTIFY R_U_THERE_ACK protocol 1
 spi 0, message ID = -443923643, sa = 81BA4DD4
*Mar 25 15:18:52.135: ISAKMP:(0:1:HW:2): DPD/R_U_THERE_ACK received from peer
10.2.80.209, sequence 0x9
*Mar 25 15:18:52.135: ISAKMP:(0:1:HW:2):deleting node -443923643 error FALSE
reason "informational (in) state 1"
*Mar 25 15:18:52.135: ISAKMP:(0:1:HW:2):Input = IKE_MESG_FROM_PEER, IKE_INFO_NOTIFY *Mar
 25 15:18:52.135: ISAKMP:(0:1:HW:2):Old State = IKE_P1_COMPLETE  New State =
IKE_P1_COMPLETE
```

上記のメッセージは、ピアからの確認応答（ACK）メッセージに対応しています。

```
Router#
*Mar 25 15:47:35.335: ISAKMP: set new node -90798077 to QM_IDLE *Mar 25 15:47:35.343:
ISAKMP:(0:1:HW:2): sending packet to 10.2.80.209 my_port
500 peer_port 500 (I) QM_IDLE
*Mar 25 15:47:35.343: ISAKMP:(0:1:HW:2):purging node -90798077 *Mar 25 15:47:35.347:
ISAKMP:(0:1:HW:2):Input = IKE_MESG_FROM_TIMER,
IKE_TIMER_IM_ALIVE
*Mar 25 15:47:35.347: ISAKMP:(0:1:HW:2):Old State = IKE_P1_COMPLETE  New State =
IKE_P1_COMPLETE
*Mar 25 15:47:36.611: ISAKMP:(0:1:HW:2):purging node 1515050537 *Mar 25 15:47:37.343:
ISAKMP:(0:1:HW:2):incrementing error counter on sa:
PEERS_ALIVE_TIMER
*Mar 25 15:47:37.343: ISAKMP: set new node -1592471565 to QM_IDLE *Mar 25 15:47:37.351:
 ISAKMP:(0:1:HW:2): sending packet to 10.2.80.209 my_port
500 peer_port 500 (I) QM_IDLE
*Mar 25 15:47:37.351: ISAKMP:(0:1:HW:2):purging node -1592471565 *Mar 25 15:47:37.355:
ISAKMP:(0:1:HW:2):Input = IKE_MESG_FROM_TIMER,
IKE_TIMER_PEERS_ALIVE
*Mar 25 15:47:37.355: ISAKMP:(0:1:HW:2):Old State = IKE_P1_COMPLETE  New State =
IKE_P1_COMPLETE
*Mar 25 15:47:39.355: ISAKMP:(0:1:HW:2):incrementing error counter on sa:
```

```
PEERS_ALIVE_TIMER
*Mar 25 15:47:39.355: ISAKMP: set new node 1758739401 to QM_IDLE *Mar 25 15:47:39.363:
ISAKMP:(0:1:HW:2): sending packet to 10.2.80.209 my_port
500 peer_port 500 (I) QM_IDLE
*Mar 25 15:47:39.363: ISAKMP:(0:1:HW:2):purging node 1758739401 *Mar 25 15:47:39.367:
ISAKMP:(0:1:HW:2):Input = IKE_MESG_FROM_TIMER,
IKE_TIMER_PEERS_ALIVE
*Mar 25 15:47:39.367: ISAKMP:(0:1:HW:2):Old State = IKE_P1_COMPLETE  New State =
IKE_P1_COMPLETE
*Mar 25 15:47:41.367: ISAKMP:(0:1:HW:2):incrementing error counter on sa:
PEERS_ALIVE_TIMER
*Mar 25 15:47:41.367: ISAKMP: set new node 320258858 to QM_IDLE *Mar 25 15:47:41.375:
ISAKMP:(0:1:HW:2): sending packet to 10.2.80.209 my_port
500 peer_port 500 (I) QM_IDLE
*Mar 25 15:47:41.379: ISAKMP:(0:1:HW:2):purging node 320258858 *Mar 25 15:47:41.379:
ISAKMP:(0:1:HW:2):Input = IKE_MESG_FROM_TIMER,
IKE_TIMER_PEERS_ALIVE
*Mar 25 15:47:41.379: ISAKMP:(0:1:HW:2):Old State = IKE_P1_COMPLETE  New State =
IKE_P1_COMPLETE
*Mar 25 15:47:43.379: ISAKMP:(0:1:HW:2):incrementing error counter on sa:
PEERS_ALIVE_TIMER
*Mar 25 15:47:43.379: ISAKMP: set new node -744493014 to QM_IDLE *Mar 25 15:47:43.387:
ISAKMP:(0:1:HW:2): sending packet to 10.2.80.209 my_port
500 peer_port 500 (I) QM_IDLE
*Mar 25 15:47:43.387: ISAKMP:(0:1:HW:2):purging node -744493014 *Mar 25 15:47:43.391:
ISAKMP:(0:1:HW:2):Input = IKE_MESG_FROM_TIMER,
IKE_TIMER_PEERS_ALIVE
*Mar 25 15:47:43.391: ISAKMP:(0:1:HW:2):Old State = IKE_P1_COMPLETE  New State =
IKE_P1_COMPLETE
*Mar 25 15:47:45.391: ISAKMP:(0:1:HW:2):incrementing error counter on sa:
PEERS_ALIVE_TIMER
*Mar 25 15:47:45.391: ISAKMP:(0:1:HW:2):peer 10.2.80.209 not responding! *Mar 25
15:47:45.391: ISAKMP:(0:1:HW:2):peer does not do paranoid keepalives.
*Mar 25 15:47:45.391: ISAKMP:(0:1:HW:2):deleting SA reason "peers alive" state
(I) QM_IDLE       (peer 10.2.80.209) input queue 0
*Mar 25 15:47:45.395: ISAKMP: Unlocking IPSEC struct 0x81E5C4E8 from
delete_siblings, count 0
*Mar 25 15:47:45.395: %CRYPTO-5-SESSION_STATUS: Crypto tunnel is DOWN.  Peer
10.2.80.209:500       Id: 10.2.80.209
*Mar 25 15:47:45.399: ISAKMP: set new node -2061951065 to QM_IDLE *Mar 25 15:47:45.411:
 ISAKMP:(0:1:HW:2): sending packet to 10.2.80.209 my_port
500 peer_port 500 (I) QM_IDLE
*Mar 25 15:47:45.411: ISAKMP:(0:1:HW:2):purging node -2061951065 *Mar 25 15:47:45.411:
ISAKMP:(0:1:HW:2):Input = IKE_MESG_FROM_TIMER,
IKE_TIMER_PEERS_ALIVE
*Mar 25 15:47:45.411: ISAKMP:(0:1:HW:2):Old State = IKE_P1_COMPLETE  New State =
IKE_DEST_SA
*Mar 25 15:47:45.415: ISAKMP:(0:1:HW:2):deleting SA reason "peers alive" state
(I) QM_IDLE       (peer 10.2.80.209) input queue 0
*Mar 25 15:47:45.415: ISAKMP: Unlocking IKE struct 0x81E5C4E8 for
isadb_mark_sa_deleted(), count 0
*Mar 25 15:47:45.415: ISAKMP: Deleting peer node by peer_reap for 10.2.80.209:
81E5C4E8
*Mar 25 15:47:45.415: ISAKMP:(0:1:HW:2):deleting node -1067612752 error TRUE
reason "peers alive"
*Mar 25 15:47:45.415: ISAKMP:(0:1:HW:2):deleting node -114443536 error TRUE
reason "peers alive"
*Mar 25 15:47:45.419: ISAKMP:(0:1:HW:2):deleting node 2116015069 error TRUE
reason "peers alive"
*Mar 25 15:47:45.419: ISAKMP:(0:1:HW:2):deleting node -1981865558 error TRUE
reason "peers alive"
*Mar 25 15:47:45.419: ISAKMP:(0:1:HW:2):Input = IKE_MESG_INTERNAL, IKE_PHASE1_DEL *Mar
25 15:47:45.419: ISAKMP:(0:1:HW:2):Old State = IKE_DEST_SA  New State =
IKE_DEST_SA
```

```
*Mar 25 15:47:45.419: ISAKMP: received ke message (4/1)
*Mar 25 15:47:45.419: ISAKMP: received ke message (3/1)
*Mar 25 15:47:45.423: ISAKMP: ignoring request to send delete notify (no ISAKMP
sa) src 10.1.32.14 dst 10.2.80.209 for SPI 0x3A7B69BF
*Mar 25 15:47:45.423: ISAKMP:(0:1:HW:2):deleting SA reason "" state (I)
MM_NO_STATE (peer 10.2.80.209) input queue 0
*Mar 25 15:47:45.423: ISAKMP:(0:1:HW:2):deleting node -1067612752 error FALSE
reason ""
*Mar 25 15:47:45.423: ISAKMP:(0:1:HW:2):deleting node -114443536 error FALSE
reason ""
*Mar 25 15:47:45.423: ISAKMP:(0:1:HW:2):deleting node 2116015069 error FALSE
reason ""
*Mar 25 15:47:45.427: ISAKMP:(0:1:HW:2):deleting node -1981865558 error FALSE
reason ""
*Mar 25 15:47:45.427: ISAKMP:(0:1:HW:2):Input = IKE_MESG_FROM_PEER, IKE_MM_EXCH *Mar 25
 15:47:45.427: ISAKMP:(0:1:HW:2):Old State = IKE_DEST_SA  New State =
IKE_DEST_SA
```

上記のメッセージは、リモート ピアが到達不能なっている時に何が発生しているのかを示しています。ルータによって、最終的にIPsecおよびSAが削除される前に、1つのDPD R_U_THEREメッセージおよび4つの転送が送信されます。

暗号マップ内の複数のピアとの組み合わせで使用される DPD および Cisco IOS XE キープアライブ：例

次に、セキュリティアソシエーション（SA）を確立するためにIKEが使用される場合に、DPDおよびCisco IOS XEキープアライブが暗号マップ設定内の複数のピアとの組み合わせで使用される例を示します。この例では、SA が、10.0.0.1、10.0.0.2、または 10.0.0.3 の IPsec ピアに設定される可能性があります。

```
crypto isakmp keepalive 10 periodic
crypto map green 1 ipsec-isakmp
  set peer 10.0.0.1
  set peer 10.0.0.2
  set peer 10.0.0.3
  set transform-set txfm
  match address 101
```

その他の参考資料

次の項では、IPSec デッド ピア検出定期メッセージ オプションの関連資料を示します。

関連資料

関連項目	マニュアル タイトル
IPsec の設定	IPsec を使用した VPN のセキュリティの設定
IPsec コマンド	『Cisco IOS Security Command Reference』

標準

標準	タイトル
この機能でサポートされる新規の標準または変更された標準はありません。また、既存の標準のサポートは変更されていません。	--

MIB

MIB	MIB のリンク
この機能によってサポートされる新しい MIB または変更された MIB はありません。またこの機能による既存MIBのサポートに変更はありません。	選択したプラットフォーム、Cisco IOS リリース、およびフィーチャ セットに関する MIB を探してダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

RFC

RFC	タイトル
DPD は、インターネット ドラフト「draft-ietf-ipsec-dpd-04.txt」に準拠しています。このドラフトは、Informational RFC（番号はまだ割り当てられていません）として公表の検討中です。	--

シスコのテクニカル サポート

説明	リンク
シスコのサポート Web サイトでは、シスコの製品やテクノロジーに関するトラブルシューティングにお役立ていただけるように、マニュアルやツールをはじめとする豊富なオンライン リソースを提供しています。 お使いの製品のセキュリティ情報や技術情報を入手するために、Cisco Notification Service（Field Notice からアクセス）、Cisco Technical Services Newsletter、Really Simple Syndication（RSS）フィードなどの各種サービスに加入できます。 シスコのサポート Web サイトのツールにアクセスする際は、Cisco.com のユーザ ID およびパスワードが必要です。	http://www.cisco.com/en/US/support/index.html

デッドピア検出定期メッセージオプションの機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *244 :* デッド ピア検出の機能情報

機能名	リリース	機能情報
デッドピア検出定期メッセージオプション	Cisco IOS XE Release 2.1	この機能により、ルータに対し、そのIKEピアの有効性について定期的に照会が行われるよう設定できます。このオプションを使用すると、デフォルトのオンデマンドデッドピア検出機能を使用した場合に比べ、停止しているピアをより早期に検出できます。 次のコマンドが導入または変更されました。**crypto isakmp keepalive**。

第 181 章

IPsec NAT 透過性

IPsec NAT透過性機能では、ネットワーク アドレス変換（NAT）とポートアドレス変換（PAT）の間における多くの既知の非互換性に対処することによって、ネットワーク内の NAT ポイントまたは PAT ポイントを経由して送信される IP セキュリティ（IPsec）のサポートが導入されています。

IPsec NAT 透過性の制約事項

この機能では、NAT および IPsec 間における多くの非互換性に対して対処が行われていますが、次の問題が依然として残されています。

インターネット キー交換（IKE）IP アドレスと NAT

この非互換性が問題になるのは、IPアドレスを、事前共有キーを検索するための検索キーとして使用する場合だけです。NAT またはリバース NAT によって IP 発信元アドレスまたは宛先アドレスが変更されると、IP アドレスと事前共有キーの間でミスマッチが生じます。

組み込み IP アドレスと NAT

ペイロードの完全性は保護されているので、NAT によって IPsec パケット内の IP アドレスを変換することが不可能です。組み込みIPアドレスを使用するプロトコルには、FTP、インターネット リレー チャット（IRC）、簡易ネットワーク管理プロトコル（SNMP）、Lightweight Directory Access Protocol（LDAP）、H.323、および Session Initiation Protocol（SIP）などがあります。

IPsec NAT 透過性に関する情報

IPsec NAT 透過性の利点

IPsec パケットの配信パス内に 1 つ以上の NAT または PAT ポイントがない場合、この機能を導入しなければ、標準の IPsec バーチャル プライベート ネットワーク（VPN）トンネルは動作しません。この機能によって NAT が IPsec 認識となり、その結果、リモート アクセス ユーザは、ホーム ゲートウェイへの IPsec トンネルを構築できます。

IPsec NAT Traversal の機能設計

IPsec NAT 透過性機能では、ユーザ データグラム プロトコル（UDP）ラッパ内に IPsec パケットをカプセル化することによって、NAT または PAT ポイントを通過する IPsec トラフィックのサポートが導入されており、その結果、パケットによる各 NAT デバイス間の通過が可能となっています。次の項では、NAT トラバーサルの詳細を定義します。

IKE フェーズ 1 ネゴシエーション：NAT 検出

インターネット キー エクスチェンジ（IKE）のフェーズ 1 ネゴシエーション中、IKE Quick Mode が開始される前に、NAT サポート、およびネットワーク パス上の NAT イグジスタンスという、2 つのタイプの NAT 検出が実行されます。

NAT サポートを検出するには、リモート ピアとベンダー ID ストリングを交換する必要があります。IKE フェーズ 1 のメイン モード（MM）1 および MM 2 の間、リモート ピアによって、ベンダー ID ストリング ペイロードが、そのピアに送信され、このバージョンでは NAT トラバーサルがサポートされていることが示されます。その後、ネットワーク パス上の NAT イグジスタンスを検出できます。

ネットワーク パス上に NAT が存在しているかどうかを検出すると、2 つのピア間のすべての NAT と、NAT の正確な位置がわかります。NAT デバイスによって、プライベート IP アドレスおよびポートがパブリック値に（またはパブリックからプライベートに）変換されます。パケットがデバイスを通過すると、この変換によって IP アドレスとポートが変更されます。ネットワーク パス上に NAT デバイスが存在しているかどうかを検出するには、ピアによって、各終端からの送信元アドレスと宛先アドレスの両方の IP アドレスおよびポートのハッシュを持つペイロードが送信される必要があります。両端でハッシュが計算され、ハッシュが一致した場合、各ピアによって、両ピア間におけるネットワーク パス上に NAT デバイスが存在しないことが認識されます。ハッシュが一致しない（つまり、誰かがアドレスまたはポートを変換した）場合、各終端では、NAT トラバーサルを実行し、ネットワークを介して IPsec パケットを取得する必要があります。

ハッシュは一連の NAT Discovery（NAT-D）ペイロードとして送信されます。各ペイロードには 1 つのハッシュが格納されます。複数のハッシュが存在する場合、複数の NAT-D が送信されます。ほとんどの環境では、NAT-D ペイロードは 2 つだけです。1 つは送信元 アドレスおよびポート用、もう 1 つは宛先アドレスおよびポート用です。最初に宛先 NA-D ペイロードが

送信され、次に送信元 NAT-D ペイロードが送信されます。これは、受信側では、最初にローカル NAT-D ペイロードを処理し、次にリモート NAT-D ペイロードを処理することを予期する必要があることを意味します。メイン モードでは、NAT-D ペイロードは 3 番目および 4 番目のメッセージに格納され、アグレッシブ モード（AM）では、2 番目および 3 番目のメッセージ内に格納されます。

IKE フェーズ 2 ネゴシエーション：NAT トラバーサル決定

IKE フェーズ 1 による NAT サポート、およびネットワーク パス上の NAT イグジスタンスの検出中に、IKE フェーズ 2 によって両端の各ピアによって NAT トラバーサルが使用されるかどうかが決定されます。QM1 および QM2 におけるクイック モード（QM）セキュリティ アソシエーション（SA）ペイロードは、NAT トラバーサル ネゴシエーション用に使用されます。

NAT デバイスによって IP アドレスおよびポート番号が変更されるので、NAT と IPsec との間に非互換性が発生する可能性があります。そのため、元の送信元アドレスを交換することで、いかなる非互換性も回避できます。

NAT Traversal 用 IPsec パケットの UDP カプセル化

UDP カプセル化によって、IPsec パケットが NAT デバイスを経由できるようにするだけでなく、IPsec、NAT、および PAT 間における多くの非互換性問題に対処できます。解決できる問題は以下のとおりです。

IPsec ESP と PAT との間における非互換性：解決

PAT によって立法 IP アドレスおよびポートが検出されると、その PAT によって Encapsulating Security Payload（ESP）パケットが廃棄されます。このようなシナリオを防ぐために、UDP カプセル化が使用され、UDP ヘッダーの背後に ESP パケットが隠蔽されます。その結果、PAT によって ESP パケットが UDP パケットとして扱われ、ESP パケットが通常の UDP パケットとして処理されます。

チェックサムと NAT との間における非互換性：解決

新しい UDP ヘッダー内では、チェックサムの値は必ずゼロに割り当てられます。この値によって、中間デバイスによるパケットのチェックサムを参照したチェックサムの確認が防止され、それにより、NAT によって IP 送信元アドレスおよび宛先アドレスが変更されるので、TCP UDP チェックサム問題が解決されます。

固定 IKE 宛先ポートおよび PAT 間における非互換性：解決

PAT によって、新しい変換用 UDP ヘッダー内のポート アドレスが変更され、元のペイロードは変更されないままとなります。

UDP カプセル化によってどのように IPSec パケットの送信が可能になるのかを確認するには、次の図を参照してください。

図 *90 : NAT/PAT* ポイントを介した標準的な *IPsec* トンネル（*UDP* カプセル化なし）

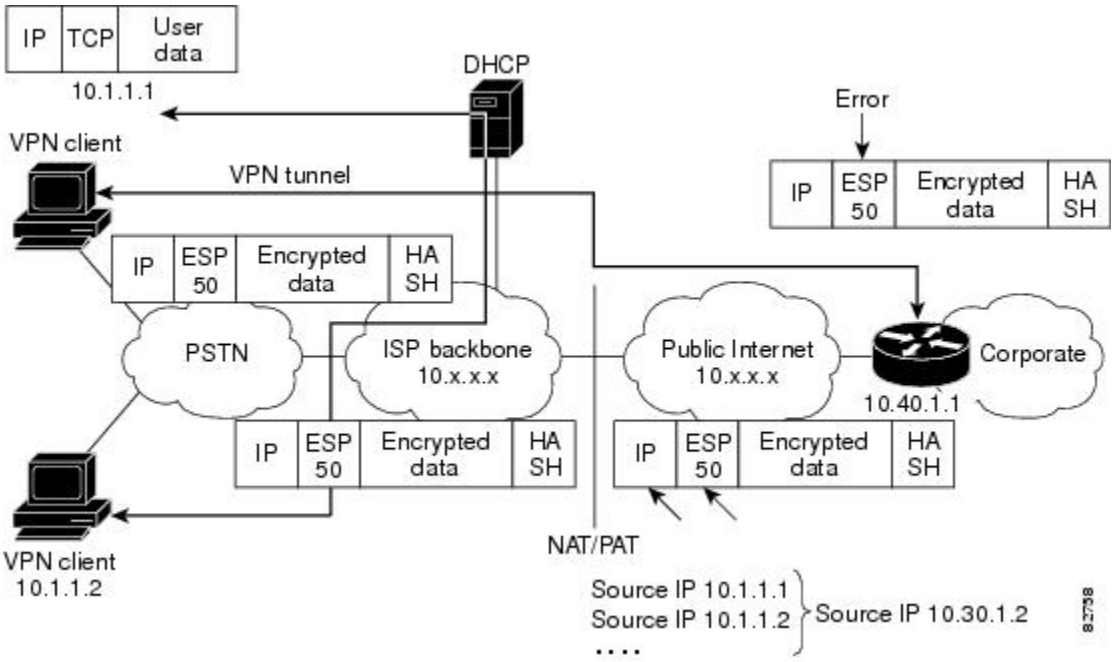
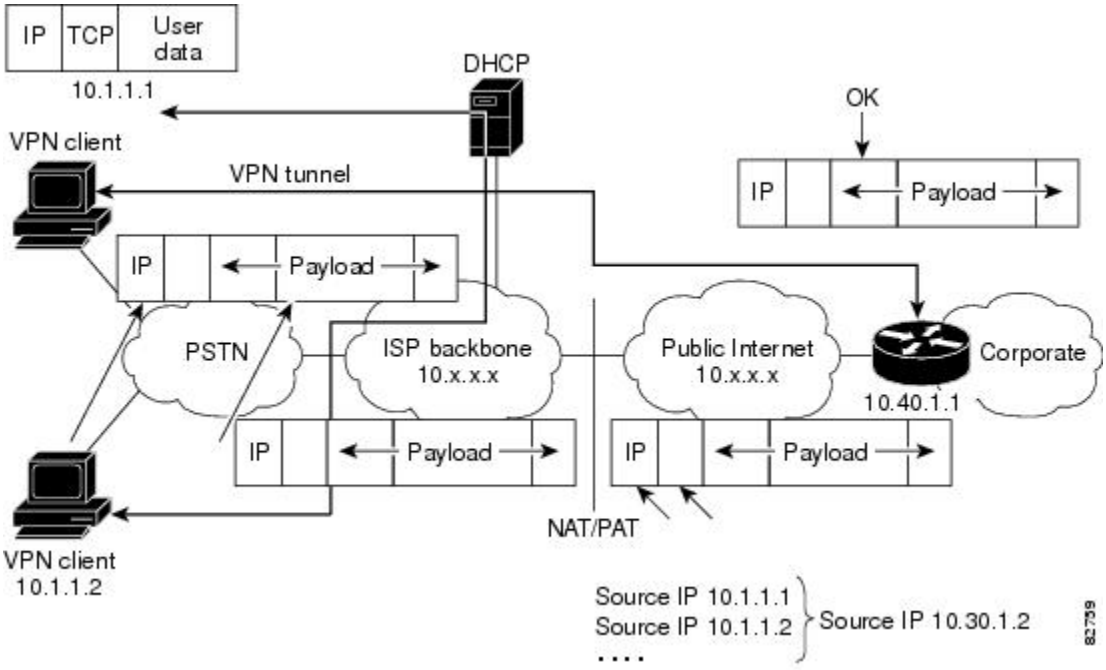


図 *91 : UDP* カプセル化を使用した *IPsec* パケット



ソフトウェア エンジン用 UDP カプセル化処理：トランスポート モードおよびトンネル モード EDP カプセル化

IPsec パケットがハードウェア アクセラレータまたはソフトウェア暗号化エンジンによって暗号化されると、UDP ヘッダーおよび非 IKE マーカ（長さは 8 バイト）が、元の IP ヘッダーと ESP ヘッダーの間に挿入されます。合計長フィールド、プロトコルフィールド、およびチェックサム フィールドはこの変更に合せて変更されます。次の 1 番目の図に、トランスポート モードが適用される前後の IPsec パケットを示します。2 番目の図には、トンネル モードが適用される前後の IPsec パケットを示します。

図 *92*：トランスポート モード：*ESP* カプセル化前後の *IPsec* パケット

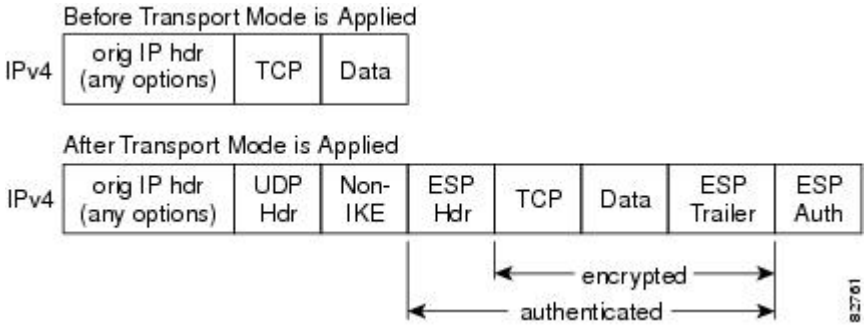
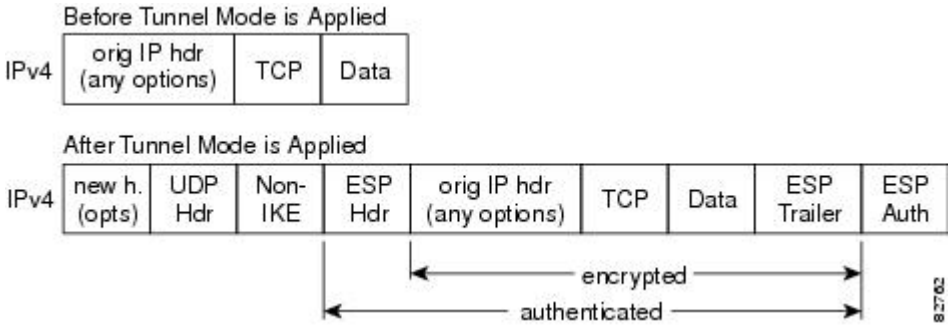


図 *93*：トンネル モード：*ESP* カプセル化前後の *IPsec* パケット



NAT キープアライブ

NAT キープアライブは、2 つのピア間の接続中におけるダイナミック NAT マッピングをアライブに保つためにイネーブルにされます。NAT キープアライブは、1 バイトの非暗号化ペイロードを持つ UDP パケットです。現在の Dead Peer Detection（DPD）実装は NAT キープアライブとほぼ同じですが、若干の違いがあります。DPD は、ピアのステータスを検出するために使用されます。一方、NAT キープアライブは、指定された期間（有効範囲は 5 ～ 3600 秒）にパケットが IPsec エンティティによって送信も受信されなかった場合に送信されます。

NAT キープアライブを（**crypto isakmp nat keepalive** コマンドを使用して）有効化する場合、アイドル値は NAT マッピングの有効期間（20 秒）より小さくなるようにする必要があります。

NAT および IPsec の設定方法

NAT Traversal の設定

NAT Traversal は、VPN デバイスによって自動検出される機能です。Cisco IOS XE Release 2.1 を実行するルータに設定するものはありません。両端の VPN デバイスが NAT-T 対応の場合、NAT Traversal が自動検出され、自動ネゴシエーションが行われます。

NAT Traversal の無効化

ご使用のネットワークですでに IPsec 認識 NAT が使用されている（spi マッチング スキーム）ことがわかっている場合、NAT トラバーサルをディセーブルにする必要が生じることがあります。NAT トラバーサルをディセーブルにするには、次のコマンドを使用します。

手順の概要

1. **enable**
2. **configure terminal**
3. **no crypto ipsec nat-transparency udp-encapsulation**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードなど、高位の権限レベルを有効にします。 パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。

ステップ 3	**no crypto ipsec nat-transparency udp-encapsulation**
	例：
	`Router(config)#`
	`no crypto ipsec nat-transparency udp-encapsulation`
		NAT トラバーサルをディセーブルにします。

NAT キープアライブの設定

ルータを、NAT キープアライブを送信するように設定するには、次のコマンドを使用します。

手順の概要

1. **enable**
2. **configure terminal**
3. **crypto isakmp nat keepalive** *seconds*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードなど、高位の権限レベルを有効にします。 パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。

ステップ 3	**crypto isakmp nat keepalive** *seconds*
	例：
	`Router(config)#`
	`crypto isakmp nat keepalive 20`
		IPsec ノードによる NAT キープアライブ パケットの送信を可能にします。
		• *seconds*：キープアライブパケット間の秒数。範囲は 5 ～ 3,600 秒。
		（注） タイマーが変更されると、インターネット セキュリティ アソシエーションおよびキー管理プロトコル（ISAKMP）SA のキープアライブが既存のタイマーに基づく場合、この秒数は SA ごとに変更されます。
		（注） セキュリティ アソシエーションでキーの再生成の衝突が発生するのを防止するため、5% のジッタ メカニズム値がタイマーに適用されます。ピア ルータが多数あるときに、タイマーが低く設定されすぎている場合、ルータの CPU 使用率が高くなることがあります。

IPsec 設定の確認

設定を確認するには、次の任意の手順を実行します。

手順の概要

1. **enable**
2. **show crypto ipsec sa** [**map** *map-name* | **address** | **identity**] [**detail**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードなど、高位の権限レベルを有効にします。 パスワードを入力します（要求された場合）。
ステップ 2	**show crypto ipsec sa** [**map** *map-name*	**address**	**identity**] [**detail** 例： `Router# show crypto ipsec sa`	現在の SA によって使用されている設定を表示します。

IPsec および NAT の設定例

NAT キープアライブの設定例

次に、NAT キープアライブを、20 秒毎に送信されるようにイネーブルにする方法の例を示します。

```
crypto isakmp policy 1
 authentication pre-share
crypto isakmp key 1234 address 10.0.0.1
crypto isakmp nat keepalive 20
!
!
crypto ipsec transform-set t2 esp-des esp-sha-hmac
!
crypto map test2 10 ipsec-isakmp
 set peer 10.0.0.1
 set transform-set t2
 match address 101
```

その他の参考資料

次の項では、IPsec NAT 透過性機能に関連した関連資料を示します。

関連資料

関連項目	マニュアル タイトル
その他の NAT 設定タスク	• 『*Cisco IOS XE IP Addressing Services Configuration Guide*』の「Configuring NAT for IP Address Conservation」モジュール • 『*Cisco IOS XE IP Addressing Services Configuration Guide*』の「Using Application Level Gateways with NAT」モジュール • 『*Cisco IOS XE IP Addressing Services Configuration Guide*』の「Configuring NAT for High Availability」モジュール • 『*Cisco IOS XE IP Addressing Services Configuration Guide*』の「Integrating NAT with MPLS VPNs」モジュール
その他の NAT コマンド	『Cisco IOS IP Addressing Services Command Reference』
その他の IPsec 設定タスク	『*Cisco IOS XE Security Configuration Guide: Secure Connectivity*』の「Configuring Security for VPNs with IPsec」モジュール
その他の IPsec コマンド	『Cisco IOS Security Command Reference』
IKE に関する情報	『*Cisco IOS XE Security Configuration Guide: Secure Connectivity*』の「Configuring Internet Key Exchange for IPsec VPNs」モジュール
IKE デッド ピア検出の追加情報	『*Cisco IOS XE Security Configuration Guide: Secure Connectivity*』の「Easy VPN Server」モジュール

標準

標準	タイトル
この機能によってサポートされる新しい MIB または変更された MIB はありません。またこの機能による既存 MIB のサポートに変更はありません。	--

MIB

MIB	MIB のリンク
この機能によってサポートされる新しい MIB または変更された MIB はありません。またこの機能による既存 MIB のサポートに変更はありません。	選択したプラットフォーム、Cisco IOS XE ソフトウェア リリース、およびフィーチャ セットの MIB の場所を検索しダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://tools.cisco.com/ITDIT/MIBS/servlet/index

RFC

RFC[22]	Title
RFC 2402	『IP Authentication Header』
RFC 2406	『IP Encapsulating Security Payload (ESP)』

[22] サポートされている RFC がすべて記載されているわけではありません。

シスコのテクニカル サポート

説明	リンク
シスコのサポート Web サイトでは、シスコの製品やテクノロジーに関するトラブルシューティングにお役立ていただけるように、マニュアルやツールをはじめとする豊富なオンライン リソースを提供しています。 お使いの製品のセキュリティ情報や技術情報を入手するために、Cisco Notification Service（Field Notice からアクセス）、Cisco Technical Services Newsletter、Really Simple Syndication（RSS）フィードなどの各種サービスに加入できます。 シスコのサポート Web サイトのツールにアクセスする際は、Cisco.com のユーザ ID およびパスワードが必要です。	http://www.cisco.com/techsupport

IPsec NAT 透過性の機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *245 : IPsec NAT* 透過性の機能情報

機能名	リリース	機能情報
IPsec NAT 透過性	Cisco IOS XE Release 2.1	IPsec NAT 透過性機能では、ネットワーク アドレス変換（NAT）とポート アドレス変換（PAT）の間における多くの既知の非互換性に対処することによって、ネットワーク内の NAT ポイントまたは PAT ポイントを経由して送信される IP セキュリティ（IPsec）のサポートが導入されています。 次のコマンドが導入または変更されました。**crypto isamkp nat keepalive**、 **access-list (IP extended)**、 **show crypto ipsec sa**

用語集

IKE：Internet Key Exchange（インターネット キー エクスチェンジ）。Oakley キー交換や Skeme キー交換をインターネット セキュリティ アソシエーションおよびキー管理プロトコル（ISAKMP）フレームワーク内部に実装したハイブリッド プロトコルです。IKE は、他のプロトコルでも使用できますが、初期実装されるのは IPsec です。IKE は、IPsec ピアを認証し、IPsec キーをネゴシエーションし、IPsec セキュリティ アソシエーション（SA）を実行します。

IPsec：IP Security（IP セキュリティ）。インターネット技術特別調査委員会（IETF）によって開発されたオープン規格のフレームワークです。IPSec は、インターネットなどの保護されていないネットワークを使用して機密情報を送信する場合に、セキュリティを提供します。IPsec はネットワーク層で機能し、Cisco ルータなどの参加している IPsec 装置（ピア）間の IP パケットを保護および認証します。

NAT：Network Address Translation（ネットワークアドレス変換）。企業内で使用されているプライベート IP アドレスを、インターネットなど企業外で使用される、ルーティング可能なパブリック アドレスに変換します。NAT は、アドレスのプライベートからパブリックへの 1 対 1 のマッピングと見なされます。

PAT：Port Address Translation（ポートアドレス変換）。NAT と同様、PAT でもプライベート IP アドレスからルーティング可能なパブリック アドレスへの変換が行われます。NAT とは異なり、PAT では、プライベート アドレスのパブリック アドレスへの多対 1 のマッピングが提供されます。パブリック アドレスの各インスタンスは、一意性を確保するために特定のポート番号と関連付けられます。PAT は、一連のパブリック アドレスを取得するコストが組織にとって高すぎるような環境で使用可能です。

第 182 章

IPsec 拡張シーケンス番号

拡張シーケンス番号（ESN）は、IPsec 標準シーケンス番号に追加され、高速 IPsec 実装を支援するために使用されます。IPsec パケットには 32 ビットのシーケンス番号があり、IKE キー付き IPsec セキュリティ アソシエーション（SA）では、シーケンス番号のロールオーバー後のキー再生成が必須です。ESN は、シーケンス番号を 64 ビットに拡張することにより、この高い IPsec SA キー再生成レートの低下を試みます。これにより、必須のキー再生成までの時間が長くなります。

IPsec 拡張シーケンス番号の前提条件

- ESN は、セキュアな接続の確立に関与する両方の IPsec ピアでサポートされている必要があります。いずれかのピアが ESN をサポートしていない場合、この機能は機能しません。
- ESN を使用する場合は、アンチリプレイ設定が必要です。詳細については、「IPsec アンチリプレイ ウィンドウの拡張と無効化」を参照してください。

IPsec 拡張シーケンス番号に関する制約事項

- ESN は、Cisco Catalyst 8500 シリーズ エッジ プラットフォームと Cisco ASR 1000 シリーズ ESP 100-X および ESP 200-X でのみサポートされています。
- ESN 機能は、DES または 3DES アルゴリズムではサポートされません。

IPsec 拡張シーケンス番号に関する情報

IPsec 拡張シーケンス番号

拡張シーケンス番号（ESN）は、IPsec 標準シーケンス番号に追加され、高速 IPsec 実装を支援するために使用されます。ESN は、標準のシーケンス番号よりも大きなシーケンス番号スペースを使用します。これにより、顧客は、キーを再生成せずに大量のデータを高速で送信できます。

IPsec パケットには 32 ビットのシーケンス番号があり、IKE キー付き IPsec セキュリティ アソシエーション（SA）では、シーケンス番号のロールオーバー後のキー再生成が必須です。ESN は、シーケンス番号を 64 ビットに拡張することにより、この高い IPsec SA キー再生成レートの低下を試みます。これにより、必須のキー再生成までの時間が長くなり、シーケンス番号のロールオーバーが防止されます。その結果、システムリソースの使用率が低下し、高速 IPsec 接続や、長い IPsec SA ライフタイムを必要とする IPsec 実装での、頻繁なキー再生成が防止されます。

IPsec 拡張シーケンス番号の設定方法

IPsec 拡張シーケンス番号の設定

IPsec 拡張シーケンス番号のサポートを設定するには、次の手順を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **crypto ipsec transform-set** *transform-set-name transform1* [*transform2*]
4. **esn**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 3	**crypto ipsec transform-set** *transform-set-name transform1* [*transform2*] 例： `Router (config)# crypto ipsec transform-set foo esp-aes esp-sha-hmac`	IPsec 用のトランスフォームセットを設定します。 • transform 引数に使用できるエントリを定義する複合ルールがあります。これらルールについては、**crypto ipsec transform-set** コマンドのコマンド解説で説明します。また、「トランスフォームセットの概要」の表に、許可されるトランスフォームの組み合わせのリストを示します。
ステップ 4	**esn** 例： `Router(cfg-crypto-trans)#[no] esn [optional]`	（オプション）IPsec ESN を有効にします。

その他の参考資料

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『Cisco IOS セキュリティ コマンド リファレンス』

IPsec ESN サポートに関する機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *246 : IPsec* 拡張シーケンス番号に関する機能情報

機能名	リリース	機能情報
IPsec 拡張シーケンス番号（ESN）	Cisco IOS XE Gibraltar 16.11.1 リリース	この機能は、次のプラットフォームに導入されました。 • Cisco Catalyst 8500 シリーズ エッジプラットフォーム • Cisco ASR 1000 シリーズ ESP 100-X および ESP 200-X

第 183 章

IPsec トンネルを使用する DF ビット オーバーライド機能

IPsec トンネル機能による DF ビット オーバライド機能では、トンネル モード IPsec トラフィックを、グローバル レベルまたは各インターフェイス レベルでカプセル化する際に、DF ビットを設定できます。したがって、ルータが DF ビットを消去するように設定されている場合、ルータは、元の DF のパケット設定に関係なく、パケットを断片化できます。

IPsec トンネルを使用する DF ビット オーバーライド機能の前提条件

ルータで IPsec がイネーブルに設定されている必要があります。

IPsec トンネルを使用する DF ビット オーバーライド機能の制約事項

パフォーマンス上の影響

各パケットがプロセス レベルで再アセンブルされるため、高いデータ レートでパフォーマンスに大きな影響が生じます。主な警告事項には、次の 2 つがあります。

- 再アセンブル キューが満杯になると、フラグメントが強制的に廃棄されることがあります。
- プロセス スイッチングにより、トラフィックの速度は低下します。

DF ビットの設定要件

複数のインターフェイスがローカル アドレス機能を使用して同じクリプト マップを共有する場合、これらのインターフェイスは同じ DF ビット設定を共有する必要があります。

機能のアベイラビリティ

この機能は IPsec トンネル モードだけで使用できます（IPsec トランスポート モードは、カプセル化 IP ヘッダーを提供しないので、影響を受けません）。

IPsec トンネルを使用する DF ビット オーバーライド機能に関する情報

機能の概要

IPsec トンネル機能による DF ビット オーバライド機能により、ルータがカプセル化ヘッダーの Don't Fragment（DF）ビットをクリア、設定、またはコピーするかどうかを指定できます。DF ビットは IP ヘッダー内のビットで、このビットは、ルータがパケットを断片化することを許可されているかどうか判別します。

一部のユーザ設定のホストでは、次の機能を実行します。

- 送信されたパケットに DF ビットを設定する。
- ファイアウォールを使用して、ファイアウォールの外部からくるインターネット制御メッセージ プロトコル（ICMP）エラーをブロックし、ホストがファイアウォールの外部から最大伝送単位（MTU）サイズを認識できないようにする。
- IP セキュリティ（IPsec）を使用してパケットをカプセル化し、MTU サイズを縮小する。

使用可能な MTU サイズを認識できないようにホストが設定されている場合、DF ビットをクリアし、パケットを断片化するよう、ルータを設定できます。

（注） この機能は、RFC 2401 に準拠して、グローバルに、またはインターフェイスごとに設定できます。両方のレベルを設定すると、インターフェイス コンフィギュレーションにより、グローバル コンフィギュレーションが上書きされます。

IPsec トンネルを使用する DF ビット オーバーライド機能の設定方法

トンネル モードでのカプセル化ヘッダーへの DF ビットの設定

トンネル モードで DF ビットをカプセル化ヘッダーに設定するには、次の手順を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **crypto ipsec df-bit** [**clear** | **set** | **copy**]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**crypto ipsec df-bit** [**clear**	**set**	**copy**] 例： `Router (config)# crypto ipsec df-bit set`	すべてのインターフェイスのトンネル モードで DF ビットをカプセル化ヘッダーに設定します。 指定されたインターフェイスに DF ビットを設定するには、インターフェイス コンフィギュレーション モードで **crypto ipsec df-bit** コマンドを使用します。 （注） DF ビット インターフェイス コンフィギュレーション設定によって、すべての DF ビット グローバル コンフィギュレーション設定が上書きされます。

DF ビット設定の確認

ルータ上の現在の DF ビット設定を確認するには、 **show running-config** コマンドを EXEC モードで使用します。

IPsec トンネルを使用する DF ビット オーバーライド機能の設定例

DF ビットの設定例

次の例では、DF ビットの設定をグローバルに消去し、DF ビットを FastEthernet というインターフェイスにコピーするようにルータが設定されています。したがって、FastEthernet 以外のすべてのインターフェイスでは、ルータは使用可能な MTU サイズより大きいパケットを送信でき、FastEthernet では、ルータはパケットをフラグメント化できます。

```
crypto isakmp policy 1
   hash md5
   authentication pre-share
crypto isakmp key Delaware address 192.168.10.66
crypto isakmp key Key-What-Key address 192.168.11.19
!
!
crypto ipsec transform-set exampleset ah-md5-hmac esp-des
crypto ipsec df-bit clear
!
!
crypto map armadillo 1 ipsec-isakmp
set peer 192.168.10.66
set transform-set exampleset
match address 101
!
crypto map basilisk 1 ipsec-isakmp
set peer 192.168.11.19
set transform-set exampleset
match address 102
!
!
interface FastEthernet
   ip address 192.168.10.38 255.255.255.0
   ip broadcast-address 0.0.0.0
   media-type 10BaseT
   crypto map armadillo
   crypto ipsec df-bit copy
!
interface FastEthernet1
   ip address 192.168.11.75 255.255.255.0
   ip broadcast-address 0.0.0.0
   media-type 10BaseT
   crypto map basilisk
!
interface Serial0
   no ip address
   ip broadcast-address 0.0.0.0
   no ip route-cache
   no ip mroute-cache
```

その他の参考資料

次のセクションには、IPsec トンネル機能による DF ビット オーバライド機能の関連資料が記載されています。

関連資料

関連項目	マニュアル タイトル
インターネット キー エクスチェンジ ネットワークと IPsec ネットワーク	「Configuring Internet Key Exchange for IPsec VPNs」
IPSec ネットワークのコマンド	『Cisco IOS Security Command Reference』

標準

標準	タイトル
この機能でサポートされる新規の標準または変更された標準はありません。また、既存の標準のサポートは変更されていません。	--

MIB

MIB	MIB のリンク
この機能がサポートする新しい MIB または変更された MIB はありません。また、この機能で変更された既存規格のサポートはありません。	選択したプラットフォーム、Cisco IOS XE リリース、およびフィーチャ セットの MIB を検索してダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

RFC

RFC	タイトル
この機能がサポートする新しい RFC または変更された RFC はありません。また、この機能は既存の規格に対するサポートに影響を及ぼしません。	--

シスコのテクニカル サポート

説明	リンク
シスコのサポート Web サイトでは、シスコの製品やテクノロジーに関するトラブルシューティングにお役立ていただけるように、マニュアルやツールをはじめとする豊富なオンライン リソースを提供しています。 お使いの製品のセキュリティ情報や技術情報を入手するために、Cisco Notification Service（Field Notice からアクセス）、Cisco Technical Services Newsletter、Really Simple Syndication（RSS）フィードなどの各種サービスに加入できます。 シスコのサポート Web サイトのツールにアクセスする際は、Cisco.com のユーザ ID およびパスワードが必要です。	http://www.cisco.com/en/US/support/index.html

IPsec トンネルを使用する DF ビット オーバーライド機能の機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *247 : IPsec* トンネルを使用する *DF* ビット オーバーライド機能の機能情報

機能名	リリース	機能情報
IPsec トンネルを使用する DF ビット オーバーライド機能	Cisco IOS XE Release 2.1	この機能により、ルータがカプセル化ヘッダーから Don't Fragment（DF）ビットを消去、設定、またはコピーするかどうかを指定できます。DF ビットは IP ヘッダー内のビットで、このビットは、ルータがパケットを断片化することを許可されているかどうか判別します。 次のコマンドが導入または変更されました。**crypto ipsec df-bit**。

第 184 章

IPsec SA アイドル タイマー

Cisco IOS XE ソフトウェアを実行しているルータによってピアの IPsec セキュリティ アソシエーション（SA）が作成される場合、そのSAを維持するためにリソースを割り当てる必要があります。SA には、メモリと、複数の管理されたタイマーが必要です。ピアがアイドル状態だと、それらのリソースが無駄になってしまいます。あまりに多くのリソースがアイドル状態のピアによって浪費されてしまうと、ルータによる他のピアとの新しい SA の作成ができなくなる可能性があります。IPsec SA アイドル タイマー機能では、SA のアクティビティをモニタリングするための、設定可能なアイドルタイマーが導入されており、これにより、アイドル状態のピアの SA を削除できます。この機能には、次のような利点があります。

- 向上したリソースの可用性
- Cisco IOS XE IPSec 配置のスケーラビリティの向上この機能によって、アイドル状態のピアによるリソースの浪費を防止できるので、より多くのリソースを、必要に応じた新しい SA の作成に使用できます。

IPsec セキュリティ アソシエーション アイドル タイマーの前提条件

インターネット キー エクスチェンジ（IKE）は、『*Cisco IOS XE Security Configuration Guide*』の「Configuring Internet Key Exchange Security Protocol」の章に従って設定する必要があります。

IPsec セキュリティ アソシエーション アイドル タイマーに関する情報

IPsec セキュリティ アソシエーションのライフタイム

現在、Cisco IOS ソフトウェアでは、IPsec SA のライフタイムの設定が可能です。ライフタイムは、グローバルに、またはクリプトマップごとに設定できます。ライフタイムには、「指定時刻」ライフタイムと「トラフィック量」ライフタイムの2つがあります。これらのライフタイムに到達すると、セキュリティ アソシエーションが期限切れになります。

IPsec SA アイドル タイマー

IPsec SA アイドル タイマーは、IPsec SA のグローバル ライフタイムとは異なります。グローバルライフタイムの有効期間は、ピアのアクティビティとは独立しています。IPsec SA アイドル タイマーを使用すれば、非アクティブなピアに関連付けられた SA を、グローバル ライフタイムが期限切れになる前に削除できます。

IPsec SA アイドル タイマーが設定されていない場合、IPsec SA のグローバル ライフタイムだけが適用されます。SA は、ピアのアクティビティと関わりなく、グローバル タイマーが有効期限切れになるまで維持されます。

（注） アイドル タイマーの期限切れのために、特定のピアに対する最新の IPsec SA が削除された場合、そのピアに対する IKE も削除されます。

IPsec セキュリティ アソシエーション アイドル タイマーの設定方法

IPSec SA アイドル タイマーのグローバルな設定

このタスクでは、IPsec SA アイドル タイマーをグローバルに設定します。このアイドル タイマーの設定は、すべての SA に適用されます。

手順の概要

1. **enable**
2. **configure terminal**
3. **crypto ipsec security-association idle-time** *seconds*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**crypto ipsec security-association idle-time** *seconds* 例： `Router(config)# crypto ipsec security-association idle-time 600`	IPsec SA アイドル タイマーを設定します。 • *seconds* 引数では、アイドル タイマーが非アクティブ ピアによる SA の維持を許可する時間を秒単位で指定します。*seconds* 引数の有効な値の範囲は 60 ～ 86400 です。

IPSec SA アイドル タイマーのクリプト マップ単位での設定

このタスクでは、指定されたクリプト マップの IPsec SA アイドル タイマーを設定します。アイドル タイマーの設定は、指定されたクリプト マップ下のすべての SA に適用されます。

手順の概要

1. **enable**
2. **configure terminal**
3. **crypto map** *map-name seq-number* **ipsec-isakmp**
4. **set security-association idle-time** *seconds*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 3	**crypto map** *map-name seq-number* **ipsec-isakmp** 例： `Router(config)# crypto map test 1 ipsec-isakmp`	クリプト マップ エントリを作成または変更し、クリプト マップ コンフィギュレーション モードを開始します。
ステップ 4	**set security-association idle-time** *seconds* 例： `Router(config-crypto-map)# set security-association idle-time 600`	デフォルト ピアが使用される前に、現在のピアをアイドル状態にしておける最大期間を指定します。 • *seconds* 引数は、デフォルト ピアが使用される前に現在のピアをアイドル状態にできる秒数です。有効値は 60 ～ 86400 です。

IPsec セキュリティ アソシエーション アイドル タイマーの設定例

IPsec SA アイドル タイマー のグローバル設定例

次に、IPsec SA アイドル タイマー をグローバルに設定して、600 秒後に非アクティブなピアの SA を廃棄している例を示します。

```
crypto ipsec security-association idle-time 600
```

暗号マップごとの IPsec SA アイドル タイマーの設定例

次に、test という名前のクリプト マップの IPsec SA アイドル タイマーを設定して、600 秒後に非アクティブなピアの SA を廃棄している例を示します。

```
crypto map test 1 ipsec-isakmp
 set security-association idle-time 600
```

その他の参考資料

ここでは、IPsec セキュリティ アソシエーション アイドル タイマー機能の関連資料について説明します。

関連資料

関連項目	マニュアル タイトル
IKE の設定に関する追加情報	「Internet Key Exchange for IPsec VPNs」

関連項目	マニュアル タイトル
IPsec SA のグローバル ライフタイムの設定に関する追加情報	• IPsec を使用した VPN のセキュリティの設定 • IPSEC 優先ピア
追加セキュリティ コマンド	『Cisco IOS Security Command Reference』

標準

標準	タイトル
この機能でサポートされる新規の標準または変更された標準はありません。また、既存の標準のサポートは変更されていません。	--

MIB

MIB	MIB のリンク
この機能によってサポートされる新しい MIB または変更された MIB はありません。またこの機能による既存 MIB のサポートに変更はありません。	選択したプラットフォーム、Cisco IOS XE ソフトウェア リリース、およびフィーチャ セットの MIB の場所を検索しダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

RFC

RFC	タイトル
この機能によりサポートされた新規 RFC または改訂 RFC はありません。またこの機能による既存 RFC のサポートに変更はありません。	---

シスコのテクニカル サポート

説明	リンク
シスコのサポート Web サイトでは、シスコの製品やテクノロジーに関するトラブルシューティングにお役立ていただけるように、マニュアルやツールをはじめとする豊富なオンライン リソースを提供しています。 お使いの製品のセキュリティ情報や技術情報を入手するために、Cisco Notification Service（Field Notice からアクセス）、Cisco Technical Services Newsletter、Really Simple Syndication（RSS）フィードなどの各種サービスに加入できます。 シスコのサポート Web サイトのツールにアクセスする際は、Cisco.com のユーザ ID およびパスワードが必要です。	http://www.cisco.com/en/US/support/index.html

IPsec セキュリティ アソシエーション アイドル タイマーの機能仕様

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *248 : IPsec* セキュリティ アソシエーション アイドル タイマーの機能仕様

機能名	リリース	機能情報
IPsec SA アイドル タイマー	Cisco IOS XE Release 2.1	Cisco IOS XE ソフトウェアを実行しているルータによってピアの IPsec セキュリティ アソシエーション（SA）が作成される場合、その SA を維持するためにリソースを割り当てる必要があります。SA には、メモリと、複数の管理されたタイマーが必要です。ピアがアイドル状態だと、それらのリソースが無駄になってしまいます。あまりに多くのリソースがアイドル状態のピアによって浪費されてしまうと、ルータによる他のピアとの新しい SA の作成ができなくなる可能性があります。IPsec SA アイドル タイマー機能では、SA のアクティビティをモニタリングするための、設定可能なアイドル タイマーが導入されており、これにより、アイドル状態のピアの SA を削除できます。 次のコマンドが導入または変更されました。**crypto ipsec security-association idle-time**
	Cisco IOS XE Release 2.1	**set security-association idle-time** コマンドが追加され、指定された暗号マップに対する IPsec アイドル タイマーの設定が可能になりました。 次のコマンドが導入または変更されました。**set security-association idle-time**。

第 185 章

IPv6 IPsec の QoS

IPv6 IPsec QoS 機能は、Quality of Service（QoS）ポリシーを IPv6 IPsec に適用できるようにします。

IPv6 IPsec QoS に関する情報

IPv6 IPsec QoS の概要

IPv6 IPsec QoS 機能は、IPv6 IPsec に Quality of Service（QoS）ポリシーを適用します。この機能は、次の機能をサポートしています。

- Crypto LLQ QoS：従来の Cisco モジュラ QoS CLI（MQC）の QoS 設定（PAK_PRIORITY など）により QoS に分類されて優先度レベル 1 または 2 にマークされたトラフィックがエンキューされ、暗号プロセッサの前にプライオリティ キューに入れられます。IPsec 暗号化エンジンの低遅延キューイング（LLQ）により、プライオリティ トラフィックのパケット遅延を軽減できます。
- IPsec QoS Pre-Classify：QoS Pre-Classify が暗号マップの下で設定されることで、暗号化の前に IPSec で元のレイヤ 3 およびレイヤ 4 ヘッダーを保存できるようにします。これにより QoS では、保存されたヘッダーを使用した分類ができます。
- QoS group-based LLQ：QoS group-based LLQ 機能により、IPsec で LLQ QoS グループの設定を確認することで、パケットが低遅延キューイング（LLQ）にエンキューされる前に高プライオリティ パケットであるかどうかを判断できます。

IPv6 IPsec QoS の設定方法

Crypto LLQ QoS の設定

IPsec と QoS が物理インターフェイスに設定され、QoS ポリシーにプライオリティ クラスがある場合、IPSecはインターフェイスにアタッチしたポリシーに基づいてパケットを分類します。プライオリティ クラスに一致するパケットを低遅延キューにエンキューします。優先順位の高いパケットは低遅延キューイング（LLQ）にエンキューされます。

このタスクを実行して、サービス ポリシーを出力インターフェイスにアタッチし、IPsec 暗号化エンジンの LLQ を有効化します。

手順の概要

1. **enable**
2. **configure terminal**
3. **interface** *physical-interface-name*
4. **ipv6 address** *{ipv6-address /prefix-length | prefix-name sub-bits/prefix-length}*
5. **service-policy output** *policy-map*
6. **ipv6 crypto map** *map-name*
7. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface** *physical-interface-name* 例： `Device(config)# interface GigabitEthernet0/0/1`	IPsec 暗号化エンジンの LLQ を使ってインターフェイスを指定します。
ステップ 4	**ipv6 address** *{ipv6-address /prefix-length | prefix-name sub-bits/prefix-length}* 例：	インターフェイスで IPv6 アドレスを設定します。

	コマンドまたはアクション	目的
	`Device(config-if)# ipv6 address 2001:DB8:FFFF::2/64`	
ステップ 5	**service-policy output** *policy-map* 例： `Device(config-if)# service-policy output p1`	指定したサービス ポリシー マップを出力インターフェイスにアタッチし、IPsec暗号化エンジンのLLQをイネーブルにします。
ステップ 6	**ipv6 crypto map** *map-name* 例： `Device(config-if)# ipv6 crypto map CMAP_1`	インターフェイスで IPv6 暗号マップを有効化します。
ステップ 7	**end** 例： `Device(config-if)# end`	インターフェイス コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

QoS Pre-classify の設定

暗号マップ上での Pre-classify の設定

qos pre-classify コマンドは暗号マップに適用され、トンネル単位の設定が可能です。QoS ポリシーは、暗号化の前に、L3 および L4 ヘッダーに基づいて、パケットに適用されます。

このタスクを実行して、QoS Pre-classify を暗号マップに適用します。

手順の概要

1. **enable**
2. **configure terminal**
3. **ipv6 crypto map** *map-name*
4. **qos pre-classify**
5. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。

	コマンドまたはアクション	目的
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ipv6 crypto map** *map-name* 例： `Device(config-if)# ipv6 crypto map CM_V6`	暗号マップ コンフィギュレーション モードを開始し、設定する暗号マップを指定します。
ステップ 4	**qos pre-classify** 例： `Device(config-if)# qos pre-classify`	QoS Pre-classify を暗号マップで有効化します。
ステップ 5	**end** 例： `Device(config-if)# end`	インターフェイス コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

トンネル インターフェイス上での Pre-classify の設定

qos pre-classify コマンドは、IPv6 IPsec トンネル インターフェイスに適用され、QoS で設定オプションをトンネル単位にします。

このタスクを実行して、QoS Pre-classify をトンネル インターフェイスに適用します。

手順の概要

1. **enable**
2. **configure terminal**
3. **interface** *tunnel-interface-name*
4. **ipv6 address** *{ipv6-address /prefix-length | prefix-name sub-bits/prefix-length}*
5. **qos pre-classify**
6. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。

	コマンドまたはアクション	目的
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface** *tunnel-interface-name* 例： `Device(config)# interface Tunnel1`	インターフェイス コンフィギュレーション モードを開始して、設定するトンネルまたは仮想インターフェイスを指定します。
ステップ 4	**ipv6 address** *{ipv6-address /prefix-length | prefix-name sub-bits/prefix-length}* 例： `Device(config-if)# ipv6 address 2001:DB8:FFFF::2/64`	インターフェイスで IPv6 アドレスを設定します。
ステップ 5	**qos pre-classify** 例： `Device(config-if)# qos pre-classify`	QoS Pre-classify をトンネル インターフェイスで有効化します。
ステップ 6	**end** 例： `Device(config-if)# end`	インターフェイス コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

LLQ QoS グループの設定

platform ipsec llq qos-group コマンドは、このコマンドで設定される QoS グループに一致するトラフィックの低遅延キューイングを有効化します。

このタスクを実行して、QoS グループの LLQ を有効化します。

手順の概要

1. **enable**
2. **configure terminal**
3. **platform ipsec llq qos-group** *group-number*
4. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**platform ipsec llq qos-group** *group-number* 例： `Device(config)# platform ipsec llq qos-group 1`	LLQ を有効化する QoS グループを指定します。有効値は 1 ～ 99 です。
ステップ 4	**end** 例： `Device(config-if)# end`	インターフェイス コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

QoS の設定例

例：Crypto LLQ QoS の設定

次の例では、出力インターフェイスに対してサービス ポリシーマップを指定し、インターフェイスで IPv6 暗号マップを有効にする方法を示します。

```
!
class-map match-all c2
  match precedence 5  6  7
class-map match-all c1
  match precedence 0  1  2  3

policy-map p1
  class c1
    priority percent 10
  class c2
    bandwidth remaining percent 3

crypto map ipv6 CMAP_1 1 ipsec-isakmp
  set peer address 2001:DB8:FFFF::1
  set transform-set ESP-3DES-SHA
  match address 102

interface GigabitEthernet0/0/1
```

```
  ipv6 address 2001:DB8:FFFF::2/64
  ipv6 crypto map CMAP_1
  service-policy output p1
```

例：暗号マップ上での Pre-classify の設定

次の例では、暗号マップ CM_V6 で **qos pre-classify** コマンドを使用して QoS 事前分類を有効化する方法を示します。

```
!
crypto map ipv6 CM_V6 10 ipsec-isakmp
  match address ACL_IPV6_1
  set transform-set set1
  set peer 2001:DB8:FFFF::1
  qos pre-classify
!
interface GigabitEthernet0/0/1
  ipv6 address 2001:DB8:FFFF::2/64
  service-policy output policy1
  ipv6 crypto map CM_V6
```

例：トンネル インターフェイス上での Pre-classify の設定

次の例では、トンネル インターフェイス tunnel1 で **qos pre-classify** コマンドを使用して QoS 事前分類を有効化する方法を示します。

```
interface GigabitEthernet1/1/2
  ipv6 address 2001:DB8:1::F/64
  service-policy output policy1
!
interface Tunnel1
  ipv6 address 2001:DB8:2::F/64
  qos pre-classify
  ipv6 mtu 1400
  tunnel protection ipsec profile greprof
```

例：LLQ QoS グループの設定

次の例では、QoS グループで低遅延キューイングを設定する方法を示します。

```
!
platform ipsec llq qos-group 1
platform ipsec llq qos-group 49
!
!
crypto map ipv6 cmap 1 ipsec-isakmp
  set peer 2001:DB8:FFFF:1::E/64
  set security-association lifetime seconds 600
  set transform-set aes-192
  match address 102
!
```

```
!
class-map match-all c1
  match precedence 5
class-map match-all c2
  match precedence 2
class-map match-all c3
  match precedence 4
class-map match-all c4
  match precedence 3
!
policy-map p1
  class c3
    set qos-group 20
  class c1
    set qos-group 49
  class c4
    set qos-group 77
!
policy-map p2
  class class-default
    set qos-group 1
!
interface GigabitEthernet0/2/0
  ipv6 address
  negotiation auto
  cdp enable
  ipv6 crypto map cmap
  service-policy input p2
!
!
interface GigabitEthernet0/2/7
  ipv6 address 2001:DB8:FFFF:1::F/64
  negotiation auto
  cdp enable
  service-policy input p1
!
```

IPv6 IPsec QoS の追加情報

関連資料

関連項目	マニュアル タイトル
セキュリティ コマンド	• 『*Cisco IOS Security Command Reference: Commands A to C*』 • 『*Cisco IOS Security Command Reference: Commands D to L*』 • 『*Cisco IOS Security Command Reference: Commands M to R*』 • 『*Cisco IOS Security Command Reference: Commands S to Z*』
IPv6 コマンド	『*IPv6 Command Reference*』
QoS コマンド	『*Cisco IOS Quality of Service Solutions Command Reference*』

関連項目	マニュアル タイトル
IPv6 アドレッシングと接続	『*IPv6 Configuration Guide*』

シスコのテクニカル サポート

説明	リンク
右の URL にアクセスして、シスコのテクニカル サポートを最大限に活用してください。これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

IPv6 IPsec QoS の機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *249 : IPv6 IPsec QoS* の機能情報

機能名	リリース	機能情報
IPv6 IPsec QoS	15.4(1)S	IPv6 IPsec QoS 機能は、QoS ポリシーを IPv6 IPsec に適用できるようにします。この機能は、次の機能をサポートしています。 • Crypto LLQ QoS • IPsec QoS Pre-Classify • QoS group-based LLQ 次のコマンドが変更されました。**ipv6 crypto map**

第 186 章

IPv6 仮想トンネル インターフェイス

シスコのネットワーク デバイス用の Cisco IOS IPv6 セキュリティ機能を利用すると、ネットワークをパフォーマンスの劣化や障害から保護するだけでなく、故意に行われる攻撃や、善意のネットワーク ユーザの意図しない危険な間違いにより生ずるデータの紛失または毀損に対しても保護できます。

Cisco IOS IPsec 機能では、IP パケット レベルのネットワーク データ暗号化を利用して、標準規格に準拠した堅牢なセキュリティが提供されています。また、IPsec では、データ機密保持サービスだけでなく、データ認証およびリプレイ攻撃防止サービスも提供されています。

IPsec は、IPv6 仕様の必須コンポーネントです。IPv6 ユニキャストおよびマルチキャスト トラフィックを保護するために、IPv6 IPsec トンネル モードおよびカプセル化が使用されます。このマニュアルでは IPv6 セキュリティへの IPsec の実装について説明します。

IPv6 仮想トンネル インターフェイスに関する情報

IPsec for IPv6

IP セキュリティ（IPsec）は Internet Engineering Task Force (IETF)によって開発されたオープン規格のフレームワークであり、インターネットなどの保護されていないネットワークを介して機密情報を送信する際のセキュリティを確保します。IPsec はネットワーク層で機能し、Cisco ルータなどの参加している IPsec 装置（ピア）間の IP パケットを保護および認証します。IPsec は、次のオプションのネットワーク セキュリティ サービスを提供します一般に、ローカル セキュリティ ポリシーにより、これらのサービスを 1 つ以上使用するよう指示されます。

- データ機密性：IPsec 送信者はネットワークを通じてパケットを送信する前に、パケットを暗号化できます。

- データ整合性：IPSec受信者は、IPSec送信者から送信されたパケットを認証し、伝送中にデータが変更されていないようにします。
- データ送信元認証：IPSec受信者は、送信されたIPSecパケットの送信元を認証できます。このサービスはデータ整合性サービスに依存します。
- アンチ リプレイ：IPsec 受信者はリプレイされたパケットを検出し、拒否できます。

IPsecを使用すれば、データを、観測、変更、またはスプーフィングされることなく、パブリック ネットワークを介して送信できます。IPsec 機能は IPv6 と IPv4 の両方で似ていますが、サイト間トンネル モードは IPv6 だけでサポートされています。

IPv6 では、IPsec は AH 認証ヘッダーと ESP 拡張ヘッダーを使用して実装されます。認証ヘッダーは、送信元の整合性と認証を提供します。再送されたパケットに対するオプションの保護も提供します。認証ヘッダーによって、ほとんどの IP ヘッダー フィールドの整合性が保護され、シグニチャベースのアルゴリズムに従って送信元が認証されます。ESPヘッダーは、機密性、送信元の認証、内部パケットのコネクションレス型整合性、アンチリプレイ、および制限されたトラフィック フローの機密性を提供します。

インターネット キー交換（IKE）プロトコルとは、IPsec とともに使用されるキー管理プロトコル標準です。IPsec の設定には必ずしも IKE は必要ありませんが、IKE では、IPsec 標準に対する新機能が追加されているほか、設定をより柔軟かつ容易に行えるよう、IPsec のサポートが強化されています。

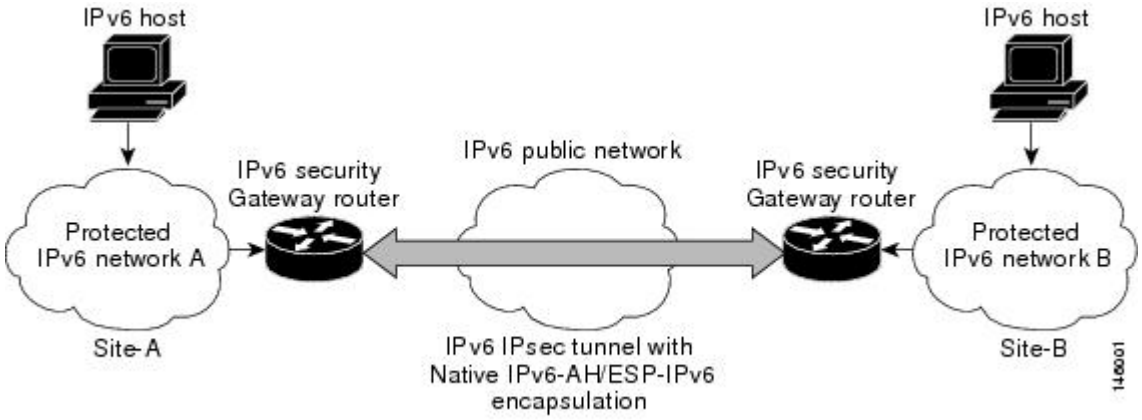
IKE は、Oakley キー交換や Skeme キー交換を Internet Security Association Key Management Protocol（ISAKMP）フレームワークの内部に実装したハイブリッドプロトコルです（ISAKMP、Oakley、および Skeme は IKE によって実装されるセキュリティ プロトコルです）。次の図を参照してください。この機能は、IPv4 IPsec 保護を使用したセキュリティ ゲートウェイ モデルと似ています。

仮想トンネル インターフェイスを使用する IPv6 IPsec サイト間保護

IPsec 仮想トンネル インターフェイス（VTI）は、IPv6 トラフィックのサイト間 IPv6 暗号保護を提供します。IPv6 ユニキャストと IPv6 マルチキャストのあらゆるタイプのトラフィックを保護するために、ネイティブ IPv6 IPsec カプセル化が使用されます。

IPsec VTI では、IPv6 ルータがセキュリティ ゲートウェイとして機能し、他のセキュリティ ゲートウェイ ルータ間に IPsec トンネルを確立したり、トラフィックが内部ネットワークからパブリック IPv6 インターネットを介して送信された場合に暗号 IPsec 保護を提供したりできます（次の図を参照）。この機能は、IPv4 IPsec 保護を使用したセキュリティ ゲートウェイ モデルと似ています。

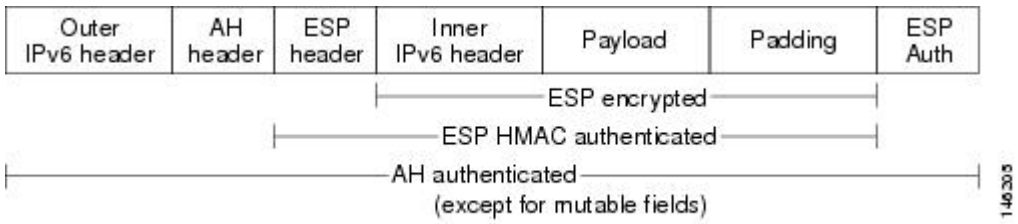
図 *94 : IPv6* の *IPsec* トンネル インターフェイス



IPsec トンネルを設定すると、トンネル インターフェイスの回線プロトコルがアップ状態に変わる前に、IKE および IPsec セキュリティ アソシエーション（SA）がネゴシエーションされ、設定されます。リモート IKE ピアは、トンネルの宛先アドレスと同じです。ローカル IKE ピアは、トンネルの宛先アドレスと同じ IPv6 アドレス スコープを持つトンネルの送信元インターフェイスから選択されたアドレスです。

次の図に、IPsec パケット形式を示します。

図 *95 : IPv6 IPsec* パケット形式



IPv6 仮想トンネル インターフェイスの設定方法

サイト間 IPv6 IPsec 保護用の VTI の設定

IPv6 での IKE ポリシーおよび事前共有キーの定義

IKE ネゴシエーションは保護する必要があるため、各 IKE ネゴシエーションは、共有（共通）の IKE ポリシーについて両ピアが同意することで開始されます。このポリシーには、次の IKE ネゴシエーションを保護するために使用するセキュリティ パラメータとピアの認証方法を記述します。

両ピアがポリシーに同意すると、各ピアに確立されている SA によってポリシーのセキュリティ パラメータが識別され、ネゴシエーションにおける以降すべての IKE トラフィックに適用されます。

パラメータ値の組み合わせをそれぞれ変えることにより各ピアにプライオリティをつけたポリシーを複数設定できます。ただし、そのうちの少なくとも 1 つのポリシーには、リモート ピアのポリシーのいずれかとまったく同じ暗号化、ハッシュ、認証、Diffie-Hellman パラメータの各値が設定されている必要があります。作成する各ポリシーに対して、一意のプライオリティを割り当てます（1 ～ 10,000 で指定し、1 が最大のプライオリティ）。

（注） サポートされているパラメータの値が 1 つしかないデバイスを使用する場合は、もう一方のデバイスでサポートされている値を設定する必要があります。この制限を別にすれば、セキュリティとパフォーマンスには通常トレードオフの関係があり、パラメータ値の多くにはこのトレードオフがあります。ネットワークのセキュリティ リスクのレベルと、そのリスクに対する許容度を評価する必要があります。

IKE ネゴシエーションが開始されると、IKE は、両方のピアにある同じ IKE ポリシーを検索します。ネゴシエーションを開始したピアがすべてのポリシーをリモート ピアに送信し、リモート ピアの方では一致するポリシーを探そうとします。リモート ピアは、自分のプライオリティ 1 位のポリシーと、相手のピアから受け取ったポリシーを比較し、一致するポリシーを探します。一致するポリシーが見つかるまで、リモート ピアは優先順位が高い順に各ポリシーをチェックします。

2 つのピアのポリシーが一致するのは、両方のピアが同じ暗号化、ハッシュ、認証、Diffie-Hellman パラメータの各値を持ち、リモート ピアのポリシーに指定されているライフタイムが、比較対象のポリシーのライフタイム以下の場合です（ライフタイムが同一でない場合は、リモート ピアのポリシーでの、より短いライフタイムが使用されます）。

一致した場合は、IKE がネゴシエーションを完了し、IPsec セキュリティ アソシエーションが作成されます。一致するポリシーが見つからなかった場合は、IKEはネゴシエーションを拒否し、IPsec は確立されません。

（注） ポリシーに指定する認証方式によっては、追加の設定が必要な場合があります。ピアのポリシーに必要な関連設定がされていないと、一致するポリシーをリモート ピアで検索するときに、ピアはポリシーを送信しません。

IKE ポリシーで事前共有キーを使用するピアそれぞれについて ISAKMP ID を設定する必要があります。

2 つのピアが IKE を使って IPsec SA を確立する場合、各ピアが自分の ID をもう一方のピア（リモート ピア）に送信します。各ピアは、ルータの ISAKMP ID の設定に従い、ホスト名または IPv6 アドレスを送信します。

デフォルトでは、ピアの ISAKMP ID はピアの IPv6 アドレスになっています。必要に応じて ID をピアのホスト名に変更します。一般的に、すべてのピアの ID は同じ設定（すべてのピアで

IPv6アドレスを設定するか、すべてのピアでホスト名を設定）にします。お互いの識別にホスト名を使うピアとIPv6アドレスを使うピアが混在していると、リモート ピアのIDが識別されない場合にDNS lookupでIDを解決できなくなり、IKEネゴシエーションが失敗することがあります。

このタスクを実行して、IPv6 での IKE ポリシーおよび事前共有キーを作成します。

手順の概要

1. **enable**
2. **configure terminal**
3. **crypto isakmp policy** *priority*
4. **authentication** {**rsa-sig** | **rsa-encr** | **pre-share**}
5. **hash** {**sha** | **md5**}
6. **group** {**1** | **2** | **5**}
7. **encryption** {**des** | **3des** | **aes** | **aes 192** | **aes 256**}
8. **lifetime** *seconds*
9. **exit**
10. **crypto isakmp key** password-type keystring *keystring* { **address** *peer-address*| **ipv6** {*ipv6-address* / *ipv6-prefix*} | **hostname** *hostname*} [**no-xauth**]
11. **crypto keyring** *keyring-name* [**vrf** *fvrf-name*]
12. **pre-shared-key** {**address** *address* [*mask*] | **hostname** *hostname* | **ipv6** {*ipv6-address* | *ipv6-prefix*}} **key** *key*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**crypto isakmp policy** *priority* 例： `Router(config)# crypto isakmp policy 15`	IKEポリシーを定義し、ISAKMPポリシー コンフィギュレーション モードを開始します。 • ポリシー番号1は、最もプライオリティが高いポリシーを示します。*priority* 引数の値が小さいほど、プライオリティは高くなります。
ステップ 4	**authentication** {**rsa-sig**	**rsa-encr**	**pre-share**} 例：	IKE ポリシー内の認証方式を指定します。 • **rsa-sig** キーワードと **rsa-encr** キーワードはIPv6でサポートされません。

	コマンドまたはアクション	目的
	`Router(config-isakmp-policy)# authentication pre-share`	
ステップ 5	**hash** {**sha** | **md5**} 例： `Router(config-isakmp-policy)# hash md5`	IKE ポリシー内のハッシュ アルゴリズムを指定します。
ステップ 6	**group** {**1** | **2** | **5**} 例： `Router(config-isakmp-policy)# group 2`	IKE ポリシー内部での D-H グループの識別番号を指定します。
ステップ 7	**encryption** {**des** | **3des** | **aes** | **aes 192** | **aes 256**} 例： `Router(config-isakmp-policy)# encryption 3des`	IKE ポリシー内の暗号化アルゴリズムを指定します。
ステップ 8	**lifetime** *seconds* 例： `Router(config-isakmp-policy)# lifetime 43200`	IKE SA のライフタイムを指定します。 • IKE ライフタイム値の設定は任意です。
ステップ 9	**exit** 例： `Router(config-isakmp-policy)# exit`	ISAKMP ポリシー コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードを開始します。
ステップ 10	**crypto isakmp key** password-type keystring *keystring* { **address** *peer-address*| **ipv6** {*ipv6-address* / *ipv6-prefix*} | **hostname** *hostname} [* **no-xauth** *]* 例： `Router(config)# crypto isakmp key 0 my-preshare-key-0 address ipv6 3ffe:1001::2/128`	事前共有認証キーを設定します。
ステップ 11	**crypto keyring** *keyring-name* [**vrf** *fvrf-name*] 例： `Router(config)# crypto keyring keyring1`	IKE 認証で使用される暗号キーリングを定義し、config-keyring モードを開始します。
ステップ 12	**pre-shared-key** {**address** *address* [*mask*] | **hostname** *hostname* | **ipv6** {*ipv6-address* | *ipv6-prefix*}} **key** *key* 例： `Router (config-keyring)# pre-shared-key ipv6 3FFE:2002::A8BB:CCFF:FE01:2C02/128`	IKE 認証に使用する事前共有キーを定義します。

ISAKMP アグレッシブ モードの設定

一般的には、サイト間シナリオではアグレッシブ モードを設定する必要はありません。通常、デフォルト モードが使用されます。

手順の概要

1. **enable**
2. **configure terminal**
3. **crypto isakmp peer** {**address** {*ipv4-address* | **ipv6** *ipv6-address ipv6-prefix-length*} | **hostname** *fqdn-hostname*}
4. **set aggressive-mode client-endpoint** {*client-endpoint* | **ipv6** *ipv6-address*}
5. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**crypto isakmp peer** {**address** {*ipv4-address* | **ipv6** *ipv6-address ipv6-prefix-length*} | **hostname** *fqdn-hostname*} 例： `Router(config)# crypto isakmp peer address ipv6 3FFE:2002::A8BB:CCFF:FE01:2C02/128`	IPsec ピアによるトンネル属性の IKE クエリーをイネーブルにします。
ステップ 4	**set aggressive-mode client-endpoint** {*client-endpoint* | **ipv6** *ipv6-address*} 例： `Router(config-isakmp-peer)# set aggressive mode client-endpoint ipv6 3FFE:2002::A8BB:CCFF:FE01:2C02/128`	リモート ピアの IPv6 アドレスを定義します。このアドレスは、アグレッシブ モードのネゴシエーションで使用されます。通常、リモート ピアのアドレスはクライアント側のエンドポイント アドレスです。
ステップ 5	**end** 例： `Router(config-isakmp-peer)# end`	crypto ISAKMP ピア コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

IPsec トランスフォーム セットおよび IPsec プロファイルの定義

このタスクを実行して、IPsec トランスフォーム セットを定義します。トランスフォーム セットは、IPsec ルータに受け入れられるセキュリティ プロトコルとアルゴリズムの組み合わせです。

手順の概要

1. **enable**
2. **configure terminal**
3. **crypto ipsec transform-set** *transform-set-name transform1* [*transform2*] [*transform3*] [*transform4*]
4. **crypto ipsec profile** *name*
5. **set transform-set** *transform-set-name* [*transform-set-name2...transform-set-name6*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**crypto ipsec transform-set** *transform-set-name transform1* [*transform2*] [*transform3*] [*transform4*] 例： `Router(config)# crypto ipsec transform-set myset0 ah-sha-hmac esp-3des`	トランスフォームセットを定義し、ルータを暗号化トランスフォーム コンフィギュレーション モードにします。
ステップ 4	**crypto ipsec profile** *name* 例： `Router(config)# crypto ipsec profile profile0`	2 つの IPsec ルータ間における IPsec 暗号化のために使用される IPsec パラメータを定義します。
ステップ 5	**set transform-set** *transform-set-name* [*transform-set-name2...transform-set-name6* 例： `Router (config-crypto-transform)# set-transform-set myset0`	クリプト マップ エントリで使用可能なトランスフォーム セットを指定します。

IPv6 での ISAKMP プロファイルの定義

手順の概要

1. **enable**
2. **configure terminal**
3. **crypto isakmp profile** *profile-name* [**accounting** *aaalist*
4. **self-identity** {**address** | **address ipv6**] | **fqdn** | **user-fqdn** *user-fqdn*}
5. **match identity** {**group** *group-name* | **address** {*address* [*mask*] [*fvrf*] | **ipv6** *ipv6-address*} | **host** *host-name* | **host domain** *domain-name* | **user** *user-fqdn* | **user domain** *domain-name*}
6. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**crypto isakmp profile** *profile-name* [**accounting** *aaalist* 例： `Router(config)# crypto isakmp profile profile1`	ISAKMP プロファイルを定義し、IPsec ユーザ セッションを監査します。
ステップ 4	**self-identity** {**address**	**address ipv6**]	**fqdn**	**user-fqdn** *user-fqdn*} 例： `Router(config-isakmp-profile)# self-identity address ipv6`	ローカル IKE がリモート ピアに対して IKE 自身を識別させるために使用する ID を定義します。
ステップ 5	**match identity** {**group** *group-name*	**address** {*address* [*mask*] [*fvrf*]	**ipv6** *ipv6-address*}	**host** *host-name*	**host domain** *domain-name*	**user** *user-fqdn*	**user domain** *domain-name*} 例： `Router(config-isakmp-profile)# match identity address ipv6 3FFE:2002::A8BB:CCFF:FE01:2C02/128`	ISAKMP プロファイルでリモート ピアの ID を照合します。

	コマンドまたはアクション	目的
ステップ 6	**end** 例： `Router(config-isakmp-profile)# end`	ISAKMP プロファイル コンフィギュレーション モードを終了し、特権 sEXEC モードに戻ります。

IPv6 IPsec VTI の設定

始める前に

ipv6 unicast-routing コマンドを使用して、IPv6 ユニキャストルーティングを有効化します。

手順の概要

1. **enable**
2. **configure terminal**
3. **ipv6 unicast-routing**
4. **interface tunnel** *tunnel-number*
5. **ipv6 address** *ipv6-address/prefix*
6. **ipv6 enable**
7. **tunnel source** {*ip-address* | *ipv6-address* | *interface-type interface-number*}
8. **tunnel destination** {*host-name* | *ip-address* | *ipv6-address*}
9. **tunnel mode** {**aurp** | **cayman** | **dvmrp** | **eon** | **gre** | **gre multipoint** | **gre ipv6** | **ipip** [**decapsulate-any**] | **ipsec ipv4** | **iptalk** | **ipv6** | **ipsec ipv6** | **mpls** | **nos** | **rbscp**}
10. **tunnel protection ipsec profile** *name* [**shared**]
11. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ipv6 unicast-routing** 例： `Router(config)# ipv6 unicast-routing`	IPv6 ユニキャスト ルーティングをイネーブルにします。設定するインターフェイス トンネルの数に関係なく、IPv6 ユニキャスト ルーティングを有効化する必要があるのは 1 回だけです。

	コマンドまたはアクション	目的
ステップ 4	**interface tunnel** *tunnel-number* 例： `Router(config)# interface tunnel 0`	トンネル インターフェイスおよび番号を指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 5	**ipv6 address** *ipv6-address/prefix* 例： `Router(config-if)# ipv6 address 3FFE:C000:0:7::/64 eui-64`	IPv6 トラフィックをこのトンネルにルーティングできるように、このトンネル インターフェイスに対する IPv6 アドレスを指定します。
ステップ 6	**ipv6 enable** 例： `Router(config-if)# ipv6 enable`	このトンネル インターフェイスに対して IPv6 をイネーブルにします。
ステップ 7	**tunnel source** {*ip-address* | *ipv6-address* | *interface-type interface-number*} 例： `Router(config-if)# tunnel source ethernet0`	トンネル インターフェイスの送信元アドレスを設定します。
ステップ 8	**tunnel destination** {*host-name* | *ip-address* | *ipv6-address*} 例： `Router(config-if)# tunnel destination 2001:DB8:1111:2222::1`	トンネル インターフェイスの宛先を指定します。
ステップ 9	**tunnel mode** {**aurp** | **cayman** | **dvmrp** | **eon** | **gre** | **gre multipoint** | **gre ipv6** | **ipip** [**decapsulate-any**] | **ipsec ipv4** | **iptalk** | **ipv6** | **ipsec ipv6** | **mpls** | **nos** | **rbscp**} 例： `Router(config-if)# tunnel mode ipsec ipv6`	トンネル インターフェイスのカプセル化モードを設定します。IPsec では、**ipsec ipv6** キーワードだけがサポートされています。
ステップ 10	**tunnel protection ipsec profile** *name* [**shared**] 例： `Router(config-if)# tunnel protection ipsec profile profile1`	トンネル インターフェイスを IPsec プロファイルに関連付けます。IPv6 では、**shared** キーワードはサポートされていません。
ステップ 11	**end** 例： `Router(config-if)# end`	インターフェイス コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

IPsec トンネル モード設定の確認

手順の概要

1. **show adjacency** [**summary** [*interface-type interface-number*]] | [**prefix**] [**interface** *interface-number*] [**connectionid** *id*] [**link** {**ipv4**| **ipv6** | **mpls**}] [**detail**]
2. **show crypto engine** {**accelerator** | **brief** | **configuration** | **connections** [**active** | **dh** | **dropped-packet** | **show**] | **qos**}
3. **show crypto ipsec sa** [**ipv6**] [*interface-type interface-number*] [**detailed**]
4. **show crypto isakmp peer** [**config** | **detail**]
5. **show crypto isakmp policy**
6. **show crypto isakmp profile** [**tag** *profilename* | **vrf** *vrfname*]
7. **show crypto map** [**interface** *interface* | **tag** *map-name*]
8. **show crypto session** [**detail**] | [**local** *ip-address* [**port** *local-port*] | [**remote** *ip-address* [**port** *remote-port*]] | **detail**] | **fvfr** *vrf-name* | **ivrf** *vrf-name*]
9. **show crypto socket**
10. **show ipv6 access-list** [*access-list-name*]
11. **show ipv6 cef** [*ipv6-prefix / prefix-length*] | [*interface-type interface-number*] [**longer-prefixes** | **similar-prefixes** | **detail** | **internal** | **platform** | **epoch** | **source**]]
12. **show interface** *type number* **stats**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**show adjacency** [**summary** [*interface-type interface-number*]]	[**prefix**] [**interface** *interface-number*] [**connectionid** *id*] [**link** {**ipv4**	**ipv6**	**mpls**}] [**detail**] 例： `Router# show adjacency detail`	シスコ エクスプレス フォワーディングの隣接関係テーブルまたはハードウェア レイヤ 3 スイッチングの隣接関係テーブルに関する情報を表示します。
ステップ 2	**show crypto engine** {**accelerator**	**brief**	**configuration**	**connections** [**active**	**dh**	**dropped-packet**	**show**]	**qos**} 例： `Router# show crypto engine connection active`	暗号化エンジンの設定情報の要約を表示します。
ステップ 3	**show crypto ipsec sa** [**ipv6**] [*interface-type interface-number*] [**detailed**] 例： `Router# show crypto ipsec sa ipv6`	IPv6 で現在の SA によって使用されている設定を表示します。
ステップ 4	**show crypto isakmp peer** [**config**	**detail**] 例：	ピアの説明を表示します。

	コマンドまたはアクション	目的
	`Router# show crypto isakmp peer detail`	
ステップ 5	**show crypto isakmp policy** 例： `Router# show crypto isakmp policy`	各 IKE ポリシーのパラメータを表示します。
ステップ 6	**show crypto isakmp profile** [**tag** *profilename* | **vrf** *vrfname*] 例： `Router# show crypto isakmp profile`	ルータに定義されている ISAKMP プロファイルをすべてリストします。
ステップ 7	**show crypto map** [**interface** *interface* | **tag** *map-name*] 例： `Router# show crypto map`	クリプト マップの設定内容を表示します。 このコマンド出力で表示されるクリプトマップは、ダイナミックに生成されます。ユーザはクリプトマップを設定する必要はありません。
ステップ 8	**show crypto session** [**detail**] | [**local** *ip-address* [**port** *local-port*] | [**remote** *ip-address* [**port** *remote-port*]] | **detail**] | **fvfr** *vrf-name* | **ivrf** *vrf-name*] 例： `Router# show crypto session`	アクティブな暗号セッションのステータス情報を表示します。 IPv6 では、**fvfr** キーワード、**ivrf** キーワード、または *vrf-name* 引数はサポートされていません。
ステップ 9	**show crypto socket** 例： `Router# show crypto socket`	暗号ソケットのリストを表示します。
ステップ 10	**show ipv6 access-list** [*access-list-name*] 例： `Router# show ipv6 access-list`	現在のすべての IPv6 アクセスリストの内容を表示します。
ステップ 11	**show ipv6 cef** [*ipv6-prefix* / *prefix-length*] | [*interface-type interface-number*] [**longer-prefixes** | **similar-prefixes** | **detail** | **internal** | **platform** | **epoch** | **source**]] 例： `Router# show ipv6 cef`	IPv6 転送情報ベース（FIB）のエントリを表示します。

	コマンドまたはアクション	目的
ステップ 12	**show interface** *type number* **stats** 例： `Router# show interface fddi 3/0/0 stats`	プロセススイッチング、ファーストスイッチング、および分散スイッチングされたパケットの数を表示します。

IPsec for IPv6 の設定と動作のトラブルシューティング

手順の概要

1. **enable**
2. **debug crypto ipsec**
3. **debug crypto engine packet** [**detail**]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router# enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**debug crypto ipsec** 例： `Router# debug crypto ipsec`	IPsec ネットワーク イベントを表示します。
ステップ 3	**debug crypto engine packet** [**detail**] 例： `Router# debug crypto engine packet`	IPv6 パケットの内容を表示します。 **注意** 複数のパケットが暗号化される場合、このコマンドを使用すると、システムのフラッディングが発生し、CPU 使用率が高くなる可能性があります。

IPv6 仮想トンネル インターフェイスの設定例

例：サイト間 IPv6 IPsec 保護用の VTI の設定

```
crypto isakmp policy 1
  encryption aes
  authentication pre-share
  group 14
```

```
!
crypto isakmp key myPreshareKey0 address ipv6 3FFE:2002::A8BB:CCFF:FE01:2C02/128
crypto isakmp keepalive 30 30
!
crypto ipsec transform-set Trans1 ah-sha-hmac esp-aes
!
crypto ipsec profile profile0
  set transform-set Trans1
!
ipv6 cef
!
interface Tunnel0
  ipv6 address 3FFE:1001::/64 eui-64
  ipv6 enable
  ipv6 cef
  tunnel source Ethernet2/0
  tunnel destination 3FFE:2002::A8BB:CCFF:FE01:2C02
  tunnel mode ipsec ipv6
  tunnel protection ipsec profile profile0
```

その他の参考資料

関連資料

関連項目	マニュアル タイトル
セキュリティ コマンド	『Cisco IOS Security Command Reference』
QoS コマンド	『Cisco IOS Quality of Service Solutions Command Reference』
重み付け均等化キューイング	「Configuring Weighted Fair Queueing」機能モジュール

MIB

MIB	MIB のリンク
なし	選択したプラットフォーム、Cisco ソフトウェア リリース、およびフィーチャ セットの MIB を検索してダウンロードする場合は、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

シスコのテクニカル サポート

説明	リンク
右の URL にアクセスして、シスコのテクニカル サポートを最大限に活用してください。これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

IPv6 仮想トンネル インターフェイスの機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *250 : IPv6* 仮想トンネル インターフェイスの機能情報

機能名	リリース	機能情報
IPv6 仮想トンネル インターフェイス	Cisco IOS XE Release 2.4	IPsecは、インターネットなどの保護されていないネットワーク上の機密情報の送信にセキュリティを提供します。IPsec はネットワーク層で機能し、Cisco ルータなどの参加している IPsec 装置（ピア）間の IP パケットを保護および認証します。 次のコマンドが導入または変更されました。**authentication (IKE policy)**、**crypto ipsec profile**、**crypto isakmp key**、**crypto isakmp peer**、**crypto isakmp policy**、**crypto isakmp profile**、**crypto keyring**、**debug crypto ipv6 ipsec**、**encryption (IKE policy)**、**group (IKE policy)**、**hash (IKE policy)**、**lifetime (IKE policy)**、**match identity**、**pre-shared-key**、**self-identity**、**set aggressive-mode client-endpoint**、**set transform-set**、**show adjacency**、**show crypto engine**、**show crypto ipsec sa**、**show crypto isakmp peers**、**show crypto isakmp policy**、**show crypto isakmp profile**、**show crypto map**、**show crypto session**、**show crypto socket**、**show ipv6 access-list**、**show ipv6 cef**、**tunnel destination**、**tunnel mode**、**tunnel source**。

第 XVIII 部

IPsec 管理プレーン

第 187 章

IPsec VPN モニタリング

IP Security VPN モニタリング機能では、VPN セッション モニタリング拡張機能によって、バーチャル プライベート ネットワーク（VPN）のトラブルシューティングを行い、エンドユーザ インターフェイスをモニタリングできます。セッション モニタリング拡張には、次のものが含まれます。

- コンフィギュレーション ファイル内のインターネット キー交換（IKE）ピアの説明を指定する機能
- 暗号セッション ステータスの一覧
- 暗号セッションのアップまたはダウン ステータスの Syslog 通知
- 1 つのコマンドライン インターフェイス（CLI）を使用して、IKE と IP Security（IPsec）の両方のセキュリティ アソシエーション（SA）をクリアする機能。

IP Security VPN モニタリングの前提条件

- IPSec と暗号化についての知識が必要です。
- ご使用のルータで IPSec がサポートされている必要があります。また IPsec VPN モニタリング機能を使用する前に、ルータ上で IPSec を設定しておく必要があります。

IP Security VPN モニタリングの制限事項

- ルータ上で Cisco IOS XE k8 または k9 暗号イメージを実行する必要があります。

IPsec VPN モニタリングに関する情報

暗号セッションの背景知識

暗号化セッションは、2 つの暗号エンドポイント間における一連の IPSec 接続（フロー）です。2 つの暗号エンドポイントで、IKE をキーイング プロトコルとして使用している場合、それらの暗号エンドポイントは互いに対して IKE ピアになります。一般に、暗号化セッションは、1 つの IKE セキュリティ アソシエーション（制御トラフィック用）と、少なくとも 2 つの IPSec セキュリティ アソシエーション（データ トラフィック用、各方向に 1 つ）で構成されています。キー再生成中、または両サイドから同時に設定要求が行われたことにより、同じセッションの IKE SA と IPSec SA が重複したり、IKE SA または IPSec SA が重複したりする可能性があります。

Per-IKE ピアの説明

Per-IKE Peer Description 機能を使用すれば、IKE ピアの選択に関する説明を入力できます。一意なピアの説明（最大 80 文字）は、特定の IKE ピアを参照する場合に使用することができます。ピアの説明を追加するには、**description** コマンドを使用します。

（注） ネットワーク アドレス変換（NAT）デバイスの背後に「配置」された IKE ピアは一意に識別することができないため、同じピアの説明を共有する必要があります。

この説明フィールドの主要な利用目的はモニタリングです（たとえば、**show** コマンドを使用するときや、ロギング（Syslog メッセージ）などのためです）。説明フィールドは純粋に記述用です（たとえば、クリプト マップを定義する際のピア アドレスや FQDN の置換としては使用できません）。

暗号化セッション ステータスのサマリー リスト

すべてのアクティブな VPN セッションの一覧を表示するには、**show crypto session** コマンドを入力します。一覧には次の項目が含まれます。

- インターフェイス
- IKE ピアの説明（存在している場合）

- IPSec SA を作成したピアに関連付けられた IKE SA
- セッションのフローにサービスを提供する IPSec SA

同じピア（同じセッション）に対して複数の IKE または IPSec SA が確立される場合があります。その場合、IKE ピアの説明は、ピアに関連付けられている各 IKE SA に対して、また、セッションのフローにサービスを提供する各 IPSec SA に対して、異なる値で繰り返されます。

このコマンドの **show crypto session detail** バリアントを使用して、セッションに関してより詳しい情報を取得することもできます。

暗号化セッションのアップまたはダウンステータスに関するSyslog通知

暗号セッションのアップまたはダウン ステータスのSyslog通知を実行する機能では、暗号セッションがアップおよびダウンする度に Syslog 通知を行います。

次に、暗号セッションがアップしたことを示す Syslog 通知の例を示します。

```
%CRYPTO-5-SESSION_STATUS: Crypto session is UP. Peer 10.6.6.1:500 fvrf=name10 ivrf=name20
  Description: SJC24-2-VPN-Gateway Id: 10.5.5.2
```

次に、暗号セッションがダウンしたことを示す Syslog 通知の例を示します。

```
%CRYPTO-5-SESSION_STATUS: Crypto session is DOWN. Peer 10.6.6.1:500 fvrf=name10 ivrf=name20
 Description: SJC24-2-VPN-Gateway Id: 10.5.5.2
```

IKE および IPsec セキュリティ交換のクリア コマンド

clear crypto session コマンドを使用すると、1 つのコマンドで IKE と IPSec の両方をクリアできます。特定の暗号化セッションや、すべてのセッションのサブセット（たとえば、あるリモート サイトへの単一のトンネル）をクリアするには、ローカルまたはリモート IP アドレス、ローカルまたはリモート ポート、フロント ドア VPN ルーティングおよび転送（FVRF）名、内部 VRF（IVRF）名といった、セッション固有のパラメータを指定する必要があります。削除する単一のトンネルを指定する場合、リモート IP アドレスを使用するのが一般的です。

clear crypto session コマンドを入力するとき、パラメータとしてローカル IP アドレスを指定すると、その IP アドレスをローカルの暗号化エンドポイント（IKE ローカルアドレス）として共有するすべてのセッション（および各セッションの IKE SA と IPsec SA）がクリアされます。**clear crypto session** コマンドを使用する際に、パラメータを指定しなかった場合、ルータ内のすべての IPsec SA および IKE SA が削除されます。

IP Security VPN モニタリングの設定方法

IKE ピアの説明の追加

IKE ピアの説明を IPsec VPN セッションに追加するには、次の手順を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **crypto isakmp peer** {**ip-address** *ip-address*}
4. **description**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**crypto isakmp peer** {**ip-address** *ip-address*} 例： `Router (config)# crypto isakmp peer address 10.2.2.9`	IPSec ピアによるアグレッシブ モードのトンネル属性に関する認証、許可、アカウンティング（AAA）のIKEクエリーをイネーブルにし、ISAKMP ピア コンフィギュレーション モードを開始します。
ステップ 4	**description** 例： `Router (config-isakmp-peer)# description connection from site A`	IKE ピアの説明を追加します。

ピアの記述の確認

ピアの説明を確認するには、**show crypto isakmp peer** コマンドを使用します。

手順の概要

1. **enable**
2. **show crypto isakmp peer**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**show crypto isakmp peer** 例： `Router# show crypto isakmp peer`	ピアの説明を表示します。

例

次に、説明の例を示します。IKE ピア 10.2.2.9 の説明として「connection from site A」が追加されていることが確認できます。

```
Router# show crypto isakmp peer
Peer: 10.2.2.9 Port: 500
 Description: connection from site A
  flags: PEER_POLICY
```

アドレス 10.2.2.9 のピアが接続され、セッションがアップになると、Syslog のステータスが次のように表示されます。

```
%CRYPTO-5-SESSION_STATUS: Crypto tunnel is UP. Peer 10.2.2.9:500 Description: connection
 from site A Id: ezvpn
```

次に、説明の例を示します。IKE ピア 10.2.2.9 の説明として「connection from site A」が追加されていることが確認できます。

```
Router# show crypto isakmp peer
Peer: 10.2.2.9 Port: 500
 Description: connection from site A
  flags: PEER_POLICY
```

アドレス 10.2.2.9 のピアが接続され、セッションがアップになると、Syslog のステータスが次のように表示されます。

```
%CRYPTO-5-SESSION_STATUS: Crypto tunnel is UP. Peer 10.2.2.9:500 Description: connection
 from site A Id: ezvpn
```

暗号化セッションのクリア

暗号セッションをクリアするには、ルータのコマンドラインから **clear crypto session** コマンドを使用します。このコマンドを使用するうえで、コンフィギュレーション ファイル内のコンフィギュレーション文は不要です。

手順の概要

1. **enable**
2. **clear crypto session**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**clear crypto session** 例： `Router# clear crypto session`	暗号セッション（IPSec および IKE SA）を削除します。

IP Security VPN モニタリングの設定例

show crypto session コマンドの出力例

次に、 **detail** キーボードを使用しない場合の **show crypto session** の出力例を示します。

```
Router# show crypto session
Crypto session current status
Interface: FastEthernet0/1
Session status: UP-ACTIVE
Peer: 172.0.0.2/500
   IKE SA: local 172.0.0.1/500 remote 172.0.0.2/500 Active
   IPSEC FLOW: permit ip 10.10.10.0/255.255.255.0 10.30.30.0/255.255.255.0
         Active SAs: 2, origin: crypto map
```

次に、**show crypto session command and the detail** キーワードを使用する場合の出力例を示します。

```
Router# show crypto session detail
Interface: Tunnel0
Session status: UP-ACTIVE
Peer: 10.1.1.3 port 500 fvrf: (none) ivrf: (none)
      Desc: this is my peer at 10.1.1.3:500 Green
```

```
    Phase1_id: 10.1.1.3
IKE SA: local 10.1.1.4/500 remote 10.1.1.3/500 Active
        Capabilities:(none) connid:3 lifetime:22:03:24
IPSEC FLOW: permit 47 host 10.1.1.4 host 10.1.1.3
      Active SAs: 0, origin: crypto map
      Inbound:  #pkts dec'ed 0 drop 0 life (KB/Sec) 0/0
      Outbound: #pkts enc'ed 0 drop 0 life (KB/Sec) 0/0
IPSEC FLOW: permit ip host 10.1.1.4 host 10.1.1.3
      Active SAs: 4, origin: crypto map
      Inbound:  #pkts dec'ed 4 drop 0 life (KB/Sec) 4605665/2949
      Outbound: #pkts enc'ed 4 drop 1 life (KB/Sec) 4605665/2949
```

その他の参考資料

ここでは、IPsec VPN モニタリングの関連資料について説明します。

関連資料

関連項目	マニュアル タイトル
IP セキュリティ、暗号化、および IKE	• 「Configuring Internet Key Exchange for IPsec VPNs」 • IPsec を使用した VPN のセキュリティの設定
セキュリティ コマンド	『*Cisco IOS Security Command Reference*』

標準

標準	タイトル
この機能でサポートされる新規または改訂された標準規格はありません。また、この機能による既存の標準規格サポートの変更はありません。	--

MIB

MIB	MIB のリンク
この機能によってサポートされる新しい MIB または変更された MIB はありません。またこの機能による既存 MIB のサポートに変更はありません。	選択したプラットフォーム、Cisco IOS XE ソフトウェア リリース、およびフィーチャ セットの MIB の場所を検索しダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

RFC

RFC	タイトル
この機能によりサポートされた新規 RFC または改訂 RFC はありません。またこの機能による既存 RFC のサポートに変更はありません。	--

シスコのテクニカル サポート

説明	リンク
シスコのサポート Web サイトでは、シスコの製品やテクノロジーに関するトラブルシューティングにお役立ていただけるように、マニュアルやツールをはじめとする豊富なオンライン リソースを提供しています。 お使いの製品のセキュリティ情報や技術情報を入手するために、Cisco Notification Service（Field Notice からアクセス）、Cisco Technical Services Newsletter、Really Simple Syndication（RSS）フィードなどの各種サービスに加入できます。 シスコのサポート Web サイトのツールにアクセスする際は、Cisco.com のユーザ ID およびパスワードが必要です。	http://www.cisco.com/techsupport

IP Security VPN モニタリングの機能履歴

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *251 : IP Security VPN* モニタリングの機能履歴

機能名	リリース	機能情報
IPsec VPN モニタリング	Cisco IOS XE Release 2.1	IP Security VPN モニタリング機能では、VPN セッション モニタリング拡張機能によって、VPNのトラブルシューティングを行い、エンドユーザ インターフェイスをモニタリングできます。セッション モニタリング拡張には、次のものが含まれます。 • コンフィギュレーション ファイル内の IKE ピアの説明を指定する機能。 • 暗号セッション ステータスの一覧 • 暗号セッションのアップまたはダウン ステータスの Syslog 通知 CLI を使用して IKE と IPsec SA の両方を削除する機能 • 次のコマンドが導入または変更されました。**clear crypto session**、 **description (isakmp peer)**、 **show crypto isakmp peer**、 **show crypto session**。

第 188 章

Cisco VRF-Aware IPsec の IPsec および IKE MIB サポート

バーチャルプライベートネットワークのルーティングと転送（VRF）対応 IP security（IPsec）機能を使用すると、MIB で VRF 対応 IPsec を管理できます。これにより、VRF ごとに IPsec 統計情報とパフォーマンス メトリックの詳細が表示されます。

Cisco VRF-Aware IPsec の IPsec および IKE MIB サポートに関する前提条件

- 簡易ネットワーク管理プロトコル（SNMP）の知識が必要です。

Cisco VRF-Aware IPsec の IPsec および IKE MIB サポートに関する情報

Cisco VRF 対応 IPsec の IPsec および IKE MIB サポート機能でサポートされる MIB

- CISCO-IPSEC-FLOW-MONITOR-MIB は、トンネル履歴と障害情報ごとに IKE および IPSEC をサポートします。この履歴と障害情報の長さは設定することができ、VRF ごとに維持す

る必要があります。テーブルサイズは、グローバル コンフィギュレーション モードで **crypto mib ipsec flowmib history tunnel size number** コマンドおよび **crypto mib ipsec flowmib history failure size** コマンドを使用することによって制御されます。

- CISCO-IPSEC-MIB
- CISCO-IPSEC-POLICY-MAP-MIB はサポートされています。しかし、この MIB は、特定の VPN VRF インスタンスに対してではなくルータ全体に適用されるので、VRF 対応ではありません。そのため、この MIB に所属するオブジェクト ID（OID）は、グローバル VRF コンテキストに関連して実行されます。

Cisco VRF-Aware IPSec の IPSec および IKE MIB サポート機能によってサポートされる SNMP トラップ

次の IKE および IPsec トンネルの開始と終了トラップは、対応する VRF と一致する必要があります。

- IPSEC_TUNNEL_STOP
- IKE_TUNNEL_STOP
- IPSEC_TUNNEL_START
- IKE_TUNNEL_START

次のトラップは、Cisco VRF-Aware IPsec 機能に合わせて変更されたグローバル トラップです。

- TOO_MANY_SAS_CREATED
- CRYPTOMAP_ADDED
- CRYPTOMAPSET_ATTACHED
- CRYPTOMAP_DELETED
- CRYPTOMAPSET_DELETED
- ISAKMP_POLICY_ADDED
- ISAKMP_POLICY_DELETED

Cisco VRF-Aware IPSec の IPSec および IKE MIB サポートの設定方法

この機能を使用するに当たって、特別な設定は必要ありません。SNMP フレームワークを使用して、MIB を使用した VRF 対応 IPsec を管理できます。詳細については、「Cisco VRF-Aware IPSec の IPSec および IKE MIB サポートの設定例」の項を参照してください。

この機能のトラブルシューティングに関する情報は、次の項に記載されています。

Cisco VRF-Aware IPSec の IPSec および IKE MIB サポート機能のトラブルシューティング方法

次の **debug crypto mib** コマンドおよびキーワードを使用して、Cisco VRF-aware IPsec に関連している IPsec およびインターネットキー交換（IKE）MIB に関する情報を表示できます。

手順の概要

1. **enable**
2. **debug crypto mib detail**
3. **debug crypto mib error**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**debug crypto mib detail** 例： `Router# debug crypto mib detail`	IPsec MIB サブシステムで発生する各種イベントを表示します。 • **detail** キーワードの出力は非常に長くなる可能性があるので、**debug crypto mib detail** をイネーブルにすることは慎重に検討する必要があります。
ステップ 3	**debug crypto mib error** 例： `Router# debug crypto mib error`	MIB エージェント内のエラー イベントを表示します。

Cisco VRF-Aware IPSec の IPSec および IKE MIB サポートの設定例

2 つの VRF を持つ設定の例

次に、2 つの VRF を持つハブ設定の典型的な出力例を示します。この出力は、IPsec セキュリティ アソシエーション（SA）に対してポーリングを実行する場合の出力です。ルータ 3745b は VRF 対応ルータです。

2 つの VRF を設定

次の出力は、2 つの VRF（vrf1 および vrf2）が設定されていることを示しています。

```
Router3745b# show running-config
Building configuration...
Current configuration : 6567 bytes
!
version 12.4
service timestamps debug datetime msec localtime
service timestamps log uptime
no service password-encryption
!
hostname ipsecf-3745b
!
boot-start-marker
boot-end-marker
!
no logging console
enable password lab
!
no aaa new-model
!
resource policy
!
memory-size iomem 5
clock timezone PST -8
clock summer-time PDT recurring
ip subnet-zero
ip cef
!
!
ip vrf vrf1
 rd 1:101
 context vrf-vrf1-context
 route-target export 1:101
 route-target import 1:101
!
ip vrf vrf2
 rd 2:101
 context vrf-vrf2-context
 route-target export 2:101
 route-target import 2:101
!
no ip domain lookup
!
!
crypto keyring vrf1-1 vrf vrf1
  pre-shared-key address 10.1.1.1 255.255.255.0 key vrf1-1
crypto keyring vrf2-1 vrf vrf2
  pre-shared-key address 10.1.2.1 255.255.255.0 key vrf2-1
!
!
crypto isakmp policy 1
 authentication pre-share
!
crypto isakmp policy 50
 authentication pre-share
crypto isakmp key global1-1 address 10.1.151.1
crypto isakmp key global2-1 address 10.1.152.1
crypto isakmp profile vrf1-1
   keyring vrf1-1
   match identity address 10.1.1.1 255.255.255.255 vrf1
```

```
crypto isakmp profile vrf2-1
   keyring vrf2-1
   match identity address 10.1.2.1 255.255.255.255 vrf2
!
crypto ipsec security-association lifetime kilobytes 99000
crypto ipsec security-association lifetime seconds 5000
!
crypto ipsec transform-set tset ah-sha-hmac esp-des esp-sha-hmac
!
crypto map global1-1 10 ipsec-isakmp
 set peer 10.1.151.1
 set transform-set tset
 match address 151
!
crypto map global2-1 10 ipsec-isakmp
 set peer 10.1.152.1
 set transform-set tset
 match address 152
!
crypto map vrf1-1 10 ipsec-isakmp
 set peer 10.1.1.1
 set transform-set tset
 set isakmp-profile vrf1-1
 match address 101
!
crypto map vrf2-1 10 ipsec-isakmp
 set peer 10.1.2.1
 set transform-set tset
 set isakmp-profile vrf2-1
 match address 102
!
!
interface FastEthernet0/0
 ip address 10.1.38.25 255.255.255.0
 no ip mroute-cache
 duplex auto
 speed auto
!
interface Serial0/0
 no ip address
 shutdown
 clock rate 2000000
!
interface FastEthernet0/1
 no ip address
 no ip mroute-cache
 shutdown
 duplex auto
 speed auto
!
interface Serial0/1
 no ip address
 shutdown
 clock rate 2000000
!
interface Serial1/0
 no ip address
 encapsulation frame-relay
 no ip route-cache cef
 no ip route-cache
 no ip mroute-cache
 no keepalive
 serial restart-delay 0
 clock rate 128000
```

```
 no frame-relay inverse-arp
!
interface Serial1/0.1 point-to-point
 ip vrf forwarding vrf1
 ip address 10.3.1.1 255.255.255.0
 no ip route-cache
 frame-relay interface-dlci 21
!
interface Serial1/0.2 point-to-point
 ip vrf forwarding vrf2
 ip address 10.3.2.1 255.255.255.0
 no ip route-cache
 frame-relay interface-dlci 22
!
interface Serial1/0.151 point-to-point
 ip address 10.7.151.1 255.255.255.0
 no ip route-cache
 frame-relay interface-dlci 151
!
interface Serial1/0.152 point-to-point
 ip address 10.7.152.1 255.255.255.0
 no ip route-cache
 frame-relay interface-dlci 152
!
interface Serial1/1
 no ip address
 no ip mroute-cache
 shutdown
 serial restart-delay 0
!
interface Serial1/2
 no ip address
 encapsulation frame-relay
 no ip route-cache cef
 no ip route-cache
 no ip mroute-cache
 no keepalive
 serial restart-delay 0
 no frame-relay inverse-arp
!
interface Serial1/2.1 point-to-point
 ip vrf forwarding vrf1
 ip address 10.1.1.2 255.255.255.0
 no ip route-cache
 frame-relay interface-dlci 21
 crypto map vrf1-1
!
interface Serial1/2.2 point-to-point
 ip vrf forwarding vrf2
 ip address 10.1.2.2 255.255.255.0
 no ip route-cache
 frame-relay interface-dlci 22
 crypto map vrf2-1
!
interface Serial1/2.151 point-to-point
 ip address 10.5.151.2 255.255.255.0
 no ip route-cache
 frame-relay interface-dlci 151
 crypto map global1-1
!
interface Serial1/2.152 point-to-point
 ip address 10.5.152.2 255.255.255.0
 no ip route-cache
 frame-relay interface-dlci 152
```

```
 crypto map global2-1
!
interface Serial1/3
 no ip address
 no ip mroute-cache
 shutdown
 serial restart-delay 0
!
ip default-gateway 10.1.38.1
ip classless
ip route 10.1.1.6 255.255.255.255 10.1.151.1
ip route 10.2.1.6 255.255.255.255 10.1.152.1
ip route 10.6.2.1 255.255.255.255 10.7.151.2
ip route 10.6.2.2 255.255.255.255 10.7.152.2
ip route 172.19.216.110 255.255.255.255 FastEthernet0/0
ip route vrf vrf1 10.20.1.1 255.255.255.255 10.1.1.1
ip route vrf vrf1 10.22.1.1 255.255.255.255 10.30.1.1
ip route vrf vrf2 10.20.2.1 255.255.255.255 10.1.2.1
ip route vrf vrf2 10.22.2.1 255.255.255.255 10.30.1.2
!
!
ip http server
no ip http secure-server
!
ip access-list standard vrf-vrf1-context
ip access-list standard vrf-vrf2-context
!
access-list 101 permit ip host 10.22.1.1 host 10.20.1.1
access-list 102 permit ip host 10.22.2.1 host 10.20.2.1
access-list 151 permit ip host 10.6.2.1 host 10.1.1.6
access-list 152 permit ip host 10.6.2.2 host 10.2.1.6
snmp-server group abc1 v2c context vrf-vrf1-context read view_vrf1 notify
*tv.FFFFFFFF.FFFFFFFF.FFFFFFFF.F access vrf-vrf1-context
snmp-server group abc2 v2c context vrf-vrf2-context read view_vrf2 notify
*tv.FFFFFFFF.FFFFFFFF.FFFFFFFF.F access vrf-vrf2-context
snmp-server view view_vrf1 iso included
snmp-server view view_vrf2 iso included
snmp-server community abc1 RW
snmp-server community global1 RW
snmp-server community abc2 RW
snmp-server community global2 RW
snmp-server enable traps tty
snmp-server enable traps config
snmp-server host 172.19.216.110 version 2c abc1
snmp-server host 172.19.216.110 vrf vrf1 version 2c abc1 udp-port 2001  ipsec isakmp
snmp-server host 172.19.216.110 version 2c abc2
snmp-server host 172.19.216.110 vrf vrf2 version 2c abc2 udp-port 2002  ipsec isakmp
snmp-server context vrf-vrf1-context
snmp-server context vrf-vrf2-context
!
!
snmp mib community-map  abc1 context vrf-vrf1-context
snmp mib community-map  abc2 context vrf-vrf2-context
!
!
control-plane
!
!
line con 0
 exec-timeout 0 0
line aux 0
line vty 0 4
 login
!
```

```
!
webvpn context Default_context
 ssl authenticate verify all
 !
 no inservice
!
!
end
```

両方の VRF をクリア

次の出力（abc1 および abc2 の出力）は、両方の VRF が、すべてのカウンタが必ず既知の値に初期化されるように「クリア」されていることを示しています。

次の出力は、VRF abc1 がクリアされていることを示しています。

```
orcas:2> setenv SR_MGR_CONF /users/green1
orcas:3> setenv SR_UTIL_SNMP_VERSION v2c
orcas:5> setenv SR_UTIL_COMMUNITY abc1
orcas:6> setenv SR_MGR_CONF_DIR /users/green1
orcas:7> /auto/sw/packages/snmpr/10.14.2.0/solaris2bin/getmany -v2c 10.1.38.25
cipSecMIBObjects
cipSecMibLevel.0 = 1
cikeGlobalActiveTunnels.0 = 0
cikeGlobalPreviousTunnels.0 = 0
cikeGlobalInOctets.0 = 0
cikeGlobalInPkts.0 = 0
cikeGlobalInDropPkts.0 = 0
cikeGlobalInNotifys.0 = 0
cikeGlobalInP2Exchgs.0 = 0
cikeGlobalInP2ExchgInvalids.0 = 0
cikeGlobalInP2ExchgRejects.0 = 0
cikeGlobalInP2SaDelRequests.0 = 0
cikeGlobalOutOctets.0 = 0
cikeGlobalOutPkts.0 = 0
cikeGlobalOutDropPkts.0 = 0
cikeGlobalOutNotifys.0 = 0
cikeGlobalOutP2Exchgs.0 = 0
cikeGlobalOutP2ExchgInvalids.0 = 0
cikeGlobalOutP2ExchgRejects.0 = 0
cikeGlobalOutP2SaDelRequests.0 = 0
cikeGlobalInitTunnels.0 = 0
cikeGlobalInitTunnelFails.0 = 0
cikeGlobalRespTunnelFails.0 = 0
cikeGlobalSysCapFails.0 = 0
cikeGlobalAuthFails.0 = 0
cikeGlobalDecryptFails.0 = 0
cikeGlobalHashValidFails.0 = 0
cikeGlobalNoSaFails.0 = 0
cipSecGlobalActiveTunnels.0 = 0
cipSecGlobalPreviousTunnels.0 = 0
cipSecGlobalInOctets.0 = 0
cipSecGlobalHcInOctets.0 = 0x00
cipSecGlobalInOctWraps.0 = 0
cipSecGlobalInDecompOctets.0 = 0
cipSecGlobalHcInDecompOctets.0 = 0x00
cipSecGlobalInDecompOctWraps.0 = 0
cipSecGlobalInPkts.0 = 0
cipSecGlobalInDrops.0 = 0
cipSecGlobalInReplayDrops.0 = 0
cipSecGlobalInAuths.0 = 0
cipSecGlobalInAuthFails.0 = 0
```

```
cipSecGlobalInDecrypts.0 = 0
cipSecGlobalInDecryptFails.0 = 0
cipSecGlobalOutOctets.0 = 0
cipSecGlobalHcOutOctets.0 = 0x00
cipSecGlobalOutOctWraps.0 = 0
cipSecGlobalOutUncompOctets.0 = 0
cipSecGlobalHcOutUncompOctets.0 = 0x00
cipSecGlobalOutUncompOctWraps.0 = 0
cipSecGlobalOutPkts.0 = 0
cipSecGlobalOutDrops.0 = 0
cipSecGlobalOutAuths.0 = 0
cipSecGlobalOutAuthFails.0 = 0
cipSecGlobalOutEncrypts.0 = 0
cipSecGlobalOutEncryptFails.0 = 0
cipSecGlobalProtocolUseFails.0 = 0
cipSecGlobalNoSaFails.0 = 0
cipSecGlobalSysCapFails.0 = 0
cipSecHistTableSize.0 = 200
cipSecHistCheckPoint.0 = ready(1)
cipSecFailTableSize.0 = 200
cipSecTrapCntlIkeTunnelStart.0 = enabled(1)
cipSecTrapCntlIkeTunnelStop.0 = enabled(1)
cipSecTrapCntlIkeSysFailure.0 = disabled(2)
cipSecTrapCntlIkeCertCrlFailure.0 = disabled(2)
cipSecTrapCntlIkeProtocolFail.0 = disabled(2)
cipSecTrapCntlIkeNoSa.0 = disabled(2)
cipSecTrapCntlIpSecTunnelStart.0 = enabled(1)
cipSecTrapCntlIpSecTunnelStop.0 = enabled(1)
cipSecTrapCntlIpSecSysFailure.0 = disabled(2)
cipSecTrapCntlIpSecSetUpFailure.0 = disabled(2)
cipSecTrapCntlIpSecEarlyTunTerm.0 = disabled(2)
cipSecTrapCntlIpSecProtocolFail.0 = disabled(2)
cipSecTrapCntlIpSecNoSa.0 = disabled(2)
```

次の出力は、VRF abc2 がクリアされていることを示しています。

```
orcas:8> setenv SR_UTIL_COMMUNITY abc2
orcas:9> /auto/sw/packages/snmpr/14.2.0.0/solaris2bin/getmany -v2c 10.1.38.25
cipSecMIBObjects
cipSecMibLevel.0 = 1
cikeGlobalActiveTunnels.0 = 0
cikeGlobalPreviousTunnels.0 = 0
cikeGlobalInOctets.0 = 0
cikeGlobalInPkts.0 = 0
cikeGlobalInDropPkts.0 = 0
cikeGlobalInNotifys.0 = 0
cikeGlobalInP2Exchgs.0 = 0
cikeGlobalInP2ExchgInvalids.0 = 0
cikeGlobalInP2ExchgRejects.0 = 0
cikeGlobalInP2SaDelRequests.0 = 0
cikeGlobalOutOctets.0 = 0
cikeGlobalOutPkts.0 = 0
cikeGlobalOutDropPkts.0 = 0
cikeGlobalOutNotifys.0 = 0
cikeGlobalOutP2Exchgs.0 = 0
cikeGlobalOutP2ExchgInvalids.0 = 0
cikeGlobalOutP2ExchgRejects.0 = 0
cikeGlobalOutP2SaDelRequests.0 = 0
cikeGlobalInitTunnels.0 = 0
cikeGlobalInitTunnelFails.0 = 0
cikeGlobalRespTunnelFails.0 = 0
cikeGlobalSysCapFails.0 = 0
cikeGlobalAuthFails.0 = 0
cikeGlobalDecryptFails.0 = 0
```

```
cikeGlobalHashValidFails.0 = 0
cikeGlobalNoSaFails.0 = 0
cipSecGlobalActiveTunnels.0 = 0
cipSecGlobalPreviousTunnels.0 = 0
cipSecGlobalInOctets.0 = 0
cipSecGlobalHcInOctets.0 = 0x00
cipSecGlobalInOctWraps.0 = 0
cipSecGlobalInDecompOctets.0 = 0
cipSecGlobalHcInDecompOctets.0 = 0x00
cipSecGlobalInDecompOctWraps.0 = 0
cipSecGlobalInPkts.0 = 0
cipSecGlobalInDrops.0 = 0
cipSecGlobalInReplayDrops.0 = 0
cipSecGlobalInAuths.0 = 0
cipSecGlobalInAuthFails.0 = 0
cipSecGlobalInDecrypts.0 = 0
cipSecGlobalInDecryptFails.0 = 0
cipSecGlobalOutOctets.0 = 0
cipSecGlobalHcOutOctets.0 = 0x00
cipSecGlobalOutOctWraps.0 = 0
cipSecGlobalOutUncompOctets.0 = 0
cipSecGlobalHcOutUncompOctets.0 = 0x00
cipSecGlobalOutUncompOctWraps.0 = 0
cipSecGlobalOutPkts.0 = 0
cipSecGlobalOutDrops.0 = 0
cipSecGlobalOutAuths.0 = 0
cipSecGlobalOutAuthFails.0 = 0
cipSecGlobalOutEncrypts.0 = 0
cipSecGlobalOutEncryptFails.0 = 0
cipSecGlobalProtocolUseFails.0 = 0
cipSecGlobalNoSaFails.0 = 0
cipSecGlobalSysCapFails.0 = 0
cipSecHistTableSize.0 = 200
cipSecHistCheckPoint.0 = ready(1)
cipSecFailTableSize.0 = 200
cipSecTrapCntlIkeTunnelStart.0 = enabled(1)
cipSecTrapCntlIkeTunnelStop.0 = enabled(1)
cipSecTrapCntlIkeSysFailure.0 = disabled(2)
cipSecTrapCntlIkeCertCrlFailure.0 = disabled(2)
cipSecTrapCntlIkeProtocolFail.0 = disabled(2)
cipSecTrapCntlIkeNoSa.0 = disabled(2)
cipSecTrapCntlIpSecTunnelStart.0 = enabled(1)
cipSecTrapCntlIpSecTunnelStop.0 = enabled(1)
cipSecTrapCntlIpSecSysFailure.0 = disabled(2)
cipSecTrapCntlIpSecSetUpFailure.0 = disabled(2)
cipSecTrapCntlIpSecEarlyTunTerm.0 = disabled(2)
cipSecTrapCntlIpSecProtocolFail.0 = disabled(2)
cipSecTrapCntlIpSecNoSa.0 = disabled(2)
orcas:10>
orcas:10>
orcas:10>
```

VRF abc1 に対する ping の実行

次の出力は、VRF abc1 に対して ping が実行されていることを示しています。

```
Router3745a# ping
Protocol [ip]:
Target IP address: 10.22.1.1
Repeat count [5]:
Datagram size [100]:
Timeout in seconds [2]:
Extended commands [n]: y
```

```
Source address or interface: 10.20.1.1
Type of service [0]:
Set DF bit in IP header? [no]:
Validate reply data? [no]:
Data pattern [0xABCD]:
Loose, Strict, Record, Timestamp, Verbose[none]:
Sweep range of sizes [n]:
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.22.1.1, timeout is 2 seconds:
Packet sent with a source address of 10.20.1.1
```

VRF abc1 に対するポーリングの実行

VRF abc1 に対してポーリングを実行すると次の出力が行われます。

（注） ping 実行後、カウンタにはゼロ以外の何らかの値が表示されます。

```
orcas:10>
orcas:12> setenv SR_UTIL_COMMUNITY abc1
orcas:13> /auto/sw/packages/snmpr/10.14.2.0/solaris2bin/getmany -v2c 10.1.38.25
cipSecMIBObjects
cipSecMibLevel.0 = 1
cikeGlobalActiveTunnels.0 = 1
cikeGlobalPreviousTunnels.0 = 0
cikeGlobalInOctets.0 = 336
cikeGlobalInPkts.0 = 2
cikeGlobalInDropPkts.0 = 0
cikeGlobalInNotifys.0 = 1
cikeGlobalInP2Exchgs.0 = 2
cikeGlobalInP2ExchgInvalids.0 = 0
cikeGlobalInP2ExchgRejects.0 = 0
cikeGlobalInP2SaDelRequests.0 = 0
cikeGlobalOutOctets.0 = 344
cikeGlobalOutPkts.0 = 2
cikeGlobalOutDropPkts.0 = 0
cikeGlobalOutNotifys.0 = 0
cikeGlobalOutP2Exchgs.0 = 1
cikeGlobalOutP2ExchgInvalids.0 = 0
cikeGlobalOutP2ExchgRejects.0 = 0
cikeGlobalOutP2SaDelRequests.0 = 0
cikeGlobalInitTunnels.0 = 0
cikeGlobalInitTunnelFails.0 = 0
cikeGlobalRespTunnelFails.0 = 0
cikeGlobalSysCapFails.0 = 0
cikeGlobalAuthFails.0 = 0
cikeGlobalDecryptFails.0 = 0
cikeGlobalHashValidFails.0 = 0
cikeGlobalNoSaFails.0 = 0
cikePeerLocalAddr.1.15.48.49.48.46.48.48.49.46.48.48.49.46.48.48.50.1.15.48.49.48.46.48.48.49.46.48.48.49.46.48.48.49.1
 = 0a 01  01 02
cikePeerRemoteAddr.1.15.48.49.48.46.48.48.49.46.48.48.49.46.48.48.50.1.15.48.49.48.46.48.48.49.46.48.48.49.46.48.48.49.1
 = 0a 01  01 01
cikePeerActiveTime.1.15.48.49.48.46.48.48.49.46.48.48.49.46.48.48.50.1.15.48.49.48.46.48.48.49.46.48.48.49.46.48.48.49.1
 = 13743
cikePeerActiveTunnelIndex.1.15.48.49.48.46.48.48.49.46.48.48.49.46.48.48.50.1.15.48.49.48.46.48.48.49.46.48.48.49.46.48.48.49.1
 = 1
cikeTunLocalType.1 = ipAddrPeer(1)
cikeTunLocalValue.1 = 010.001.001.002
cikeTunLocalAddr.1 = 0a 01  01 02
```

```
cikeTunLocalName.1 = ipsecf-3745b
cikeTunRemoteType.1 = ipAddrPeer(1)
cikeTunRemoteValue.1 = 010.001.001.001
cikeTunRemoteAddr.1 = 0a 01  01 01
cikeTunRemoteName.1 =
cikeTunNegoMode.1 = main(1)
cikeTunDiffHellmanGrp.1 = dhGroup1(2)
cikeTunEncryptAlgo.1 = des(2)
cikeTunHashAlgo.1 = sha(3)
cikeTunAuthMethod.1 = preSharedKey(2)
cikeTunLifeTime.1 = 86400
cikeTunActiveTime.1 = 13752
cikeTunSaRefreshThreshold.1 = 0
cikeTunTotalRefreshes.1 = 0
cikeTunInOctets.1 = 336
cikeTunInPkts.1 = 2
cikeTunInDropPkts.1 = 0
cikeTunInNotifys.1 = 1
cikeTunInP2Exchgs.1 = 2
cikeTunInP2ExchgInvalids.1 = 0
cikeTunInP2ExchgRejects.1 = 0
cikeTunInP2SaDelRequests.1 = 0
cikeTunOutOctets.1 = 344
cikeTunOutPkts.1 = 2
cikeTunOutDropPkts.1 = 0
cikeTunOutNotifys.1 = 0
cikeTunOutP2Exchgs.1 = 1
cikeTunOutP2ExchgInvalids.1 = 0
cikeTunOutP2ExchgRejects.1 = 0
cikeTunOutP2SaDelRequests.1 = 0
cikeTunStatus.1 = active(1)
cikePeerCorrIpSecTunIndex.1.15.48.49.48.46.48.48.49.46.48.48.49.46.48.48.50.1.15.48.49.48.46.48.48.49.46.48.48.49.46.48.48.49.1.1
 = 1
cipSecGlobalActiveTunnels.0 = 1
cipSecGlobalPreviousTunnels.0 = 0
cipSecGlobalInOctets.0 = 400
cipSecGlobalHcInOctets.0 = 0x0190
cipSecGlobalInOctWraps.0 = 0
cipSecGlobalInDecompOctets.0 = 400
cipSecGlobalHcInDecompOctets.0 = 0x0190
cipSecGlobalInDecompOctWraps.0 = 0
cipSecGlobalInPkts.0 = 4
cipSecGlobalInDrops.0 = 0
cipSecGlobalInReplayDrops.0 = 0
cipSecGlobalInAuths.0 = 4
cipSecGlobalInAuthFails.0 = 0
cipSecGlobalInDecrypts.0 = 4
cipSecGlobalInDecryptFails.0 = 0
cipSecGlobalOutOctets.0 = 704
cipSecGlobalHcOutOctets.0 = 0x02c0
cipSecGlobalOutOctWraps.0 = 0
cipSecGlobalOutUncompOctets.0 = 704
cipSecGlobalHcOutUncompOctets.0 = 0x02c0
cipSecGlobalOutUncompOctWraps.0 = 0
cipSecGlobalOutPkts.0 = 4
cipSecGlobalOutDrops.0 = 0
cipSecGlobalOutAuths.0 = 4
cipSecGlobalOutAuthFails.0 = 0
cipSecGlobalOutEncrypts.0 = 4
cipSecGlobalOutEncryptFails.0 = 0
cipSecGlobalProtocolUseFails.0 = 0
cipSecGlobalNoSaFails.0 = 0
cipSecGlobalSysCapFails.0 = 0
cipSecTunIkeTunnelIndex.1 = 1
```

```
cipSecTunIkeTunnelAlive.1 = true(1)
cipSecTunLocalAddr.1 = 0a 01  01 02
cipSecTunRemoteAddr.1 = 0a 01  01 01
cipSecTunKeyType.1 = ike(1)
cipSecTunEncapMode.1 = tunnel(1)
cipSecTunLifeSize.1 = 99000
cipSecTunLifeTime.1 = 5000
cipSecTunActiveTime.1 = 13749
cipSecTunSaLifeSizeThreshold.1 = 64
cipSecTunSaLifeTimeThreshold.1 = 10
cipSecTunTotalRefreshes.1 = 0
cipSecTunExpiredSaInstances.1 = 0
cipSecTunCurrentSaInstances.1 = 4
cipSecTunInSaDiffHellmanGrp.1 = dhGroup1(2)
cipSecTunInSaEncryptAlgo.1 = des(2)
cipSecTunInSaAhAuthAlgo.1 = hmacSha(3)
cipSecTunInSaEspAuthAlgo.1 = hmacSha(3)
cipSecTunInSaDecompAlgo.1 = none(1)
cipSecTunOutSaDiffHellmanGrp.1 = dhGroup1(2)
cipSecTunOutSaEncryptAlgo.1 = des(2)
cipSecTunOutSaAhAuthAlgo.1 = hmacSha(3)
cipSecTunOutSaEspAuthAlgo.1 = hmacSha(3)
cipSecTunOutSaCompAlgo.1 = none(1)
cipSecTunInOctets.1 = 400
cipSecTunHcInOctets.1 = 0x0190
cipSecTunInOctWraps.1 = 0
cipSecTunInDecompOctets.1 = 400
cipSecTunHcInDecompOctets.1 = 0x0190
cipSecTunInDecompOctWraps.1 = 0
cipSecTunInPkts.1 = 4
cipSecTunInDropPkts.1 = 0
cipSecTunInReplayDropPkts.1 = 0
cipSecTunInAuths.1 = 4
cipSecTunInAuthFails.1 = 0
cipSecTunInDecrypts.1 = 4
cipSecTunInDecryptFails.1 = 0
cipSecTunOutOctets.1 = 704
cipSecTunHcOutOctets.1 = 0x02c0
cipSecTunOutOctWraps.1 = 0
cipSecTunOutUncompOctets.1 = 704
cipSecTunHcOutUncompOctets.1 = 0x02c0
cipSecTunOutUncompOctWraps.1 = 0
cipSecTunOutPkts.1 = 4
cipSecTunOutDropPkts.1 = 0
cipSecTunOutAuths.1 = 4
cipSecTunOutAuthFails.1 = 0
cipSecTunOutEncrypts.1 = 4
cipSecTunOutEncryptFails.1 = 0
cipSecTunStatus.1 = active(1)
cipSecEndPtLocalName.1.1 =
cipSecEndPtLocalType.1.1 = singleIpAddr(1)
cipSecEndPtLocalAddr1.1.1 = 16 01  01 01
cipSecEndPtLocalAddr2.1.1 = 16 01  01 01
cipSecEndPtLocalProtocol.1.1 = 0
cipSecEndPtLocalPort.1.1 = 0
cipSecEndPtRemoteName.1.1 =
cipSecEndPtRemoteType.1.1 = singleIpAddr(1)
cipSecEndPtRemoteAddr1.1.1 = 14 01  01 01
cipSecEndPtRemoteAddr2.1.1 = 14 01  01 01
cipSecEndPtRemoteProtocol.1.1 = 0
cipSecEndPtRemotePort.1.1 = 0
cipSecSpiDirection.1.1 = in(1)
cipSecSpiDirection.1.2 = out(2)
cipSecSpiDirection.1.3 = in(1)
```

```
cipSecSpiDirection.1.4 = out(2)
cipSecSpiValue.1.1 = 3891970674
cipSecSpiValue.1.2 = 1963217493
cipSecSpiValue.1.3 = 3691920464
cipSecSpiValue.1.4 = 3458912974
cipSecSpiProtocol.1.1 = ah(1)
cipSecSpiProtocol.1.2 = ah(1)
cipSecSpiProtocol.1.3 = esp(2)
cipSecSpiProtocol.1.4 = esp(2)
cipSecSpiStatus.1.1 = active(1)
cipSecSpiStatus.1.2 = active(1)
cipSecSpiStatus.1.3 = active(1)
cipSecSpiStatus.1.4 = active(1)
cipSecHistTableSize.0 = 200
cipSecHistCheckPoint.0 = ready(1)
cipSecFailTableSize.0 = 200
cipSecTrapCntlIkeTunnelStart.0 = enabled(1)
cipSecTrapCntlIkeTunnelStop.0 = enabled(1)
cipSecTrapCntlIkeSysFailure.0 = disabled(2)
cipSecTrapCntlIkeCertCrlFailure.0 = disabled(2)
cipSecTrapCntlIkeProtocolFail.0 = disabled(2)
cipSecTrapCntlIkeNoSa.0 = disabled(2)
cipSecTrapCntlIpSecTunnelStart.0 = enabled(1)
cipSecTrapCntlIpSecTunnelStop.0 = enabled(1)
cipSecTrapCntlIpSecSysFailure.0 = disabled(2)
cipSecTrapCntlIpSecSetUpFailure.0 = disabled(2)
cipSecTrapCntlIpSecEarlyTunTerm.0 = disabled(2)
cipSecTrapCntlIpSecProtocolFail.0 = disabled(2)
cipSecTrapCntlIpSecNoSa.0 = disabled(2)
orcas:14>
orcas:14>
orcas:14>
```

VRF abc2 に対するポーリングの実行

VRF abc2 に対してポーリングを実行すると次の出力が行われます。

（注） ping は VRF abc1 に関してだけ完了しています。そのため、VRF abc2 のカウンタは初期化されたステートのままです。

```
setenv SR_UTIL_COMMUNITY abc2
orcas:15>
orcas:15> /auto/sw/packages/snmpr/10.14.2.0/solaris2bin/getmany -v2c 10.1.38.25
cipSecMIBObjects
cipSecMibLevel.0 = 1
cikeGlobalActiveTunnels.0 = 0
cikeGlobalPreviousTunnels.0 = 0
cikeGlobalInOctets.0 = 0
cikeGlobalInPkts.0 = 0
cikeGlobalInDropPkts.0 = 0
cikeGlobalInNotifys.0 = 0
cikeGlobalInP2Exchgs.0 = 0
cikeGlobalInP2ExchgInvalids.0 = 0
cikeGlobalInP2ExchgRejects.0 = 0
cikeGlobalInP2SaDelRequests.0 = 0
cikeGlobalOutOctets.0 = 0
cikeGlobalOutPkts.0 = 0
cikeGlobalOutDropPkts.0 = 0
cikeGlobalOutNotifys.0 = 0
```

```
cikeGlobalOutP2Exchgs.0 = 0
cikeGlobalOutP2ExchgInvalids.0 = 0
cikeGlobalOutP2ExchgRejects.0 = 0
cikeGlobalOutP2SaDelRequests.0 = 0
cikeGlobalInitTunnels.0 = 0
cikeGlobalInitTunnelFails.0 = 0
cikeGlobalRespTunnelFails.0 = 0
cikeGlobalSysCapFails.0 = 0
cikeGlobalAuthFails.0 = 0
cikeGlobalDecryptFails.0 = 0
cikeGlobalHashValidFails.0 = 0
cikeGlobalNoSaFails.0 = 0
cipSecGlobalActiveTunnels.0 = 0
cipSecGlobalPreviousTunnels.0 = 0
cipSecGlobalInOctets.0 = 0
cipSecGlobalHcInOctets.0 = 0x00
cipSecGlobalInOctWraps.0 = 0
cipSecGlobalInDecompOctets.0 = 0
cipSecGlobalHcInDecompOctets.0 = 0x00
cipSecGlobalInDecompOctWraps.0 = 0
cipSecGlobalInPkts.0 = 0
cipSecGlobalInDrops.0 = 0
cipSecGlobalInReplayDrops.0 = 0
cipSecGlobalInAuths.0 = 0
cipSecGlobalInAuthFails.0 = 0
cipSecGlobalInDecrypts.0 = 0
cipSecGlobalInDecryptFails.0 = 0
cipSecGlobalOutOctets.0 = 0
cipSecGlobalHcOutOctets.0 = 0x00
cipSecGlobalOutOctWraps.0 = 0
cipSecGlobalOutUncompOctets.0 = 0
cipSecGlobalHcOutUncompOctets.0 = 0x00
cipSecGlobalOutUncompOctWraps.0 = 0
cipSecGlobalOutPkts.0 = 0
cipSecGlobalOutDrops.0 = 0
cipSecGlobalOutAuths.0 = 0
cipSecGlobalOutAuthFails.0 = 0
cipSecGlobalOutEncrypts.0 = 0
cipSecGlobalOutEncryptFails.0 = 0
cipSecGlobalProtocolUseFails.0 = 0
cipSecGlobalNoSaFails.0 = 0
cipSecGlobalSysCapFails.0 = 0
cipSecHistTableSize.0 = 200
cipSecHistCheckPoint.0 = ready(1)
cipSecFailTableSize.0 = 200
cipSecTrapCntlIkeTunnelStart.0 = enabled(1)
cipSecTrapCntlIkeTunnelStop.0 = enabled(1)
cipSecTrapCntlIkeSysFailure.0 = disabled(2)
cipSecTrapCntlIkeCertCrlFailure.0 = disabled(2)
cipSecTrapCntlIkeProtocolFail.0 = disabled(2)
cipSecTrapCntlIkeNoSa.0 = disabled(2)
cipSecTrapCntlIpSecTunnelStart.0 = enabled(1)
cipSecTrapCntlIpSecTunnelStop.0 = enabled(1)
cipSecTrapCntlIpSecSysFailure.0 = disabled(2)
cipSecTrapCntlIpSecSetUpFailure.0 = disabled(2)
cipSecTrapCntlIpSecEarlyTunTerm.0 = disabled(2)
cipSecTrapCntlIpSecProtocolFail.0 = disabled(2)
cipSecTrapCntlIpSecNoSa.0 = disabled(2)
orcas:16>
```

その他の参考資料

関連資料

関連項目	マニュアル タイトル
テクノロジーごとの Cisco IOS コマンド	『Cisco IOS Release Command References』
Cisco IOS マスター コマンド リスト	『Master Command List』
SNMP の設定	『*Cisco IOS Network Management Configuration Guide*』の「Configuring SNMP Support」の章
VRF-Aware IPsec の設定	「VRF-Aware IPSec」

標準

標準	タイトル
なし。	--

MIB

MIB	MIB のリンク
• CISCO-IPSEC-FLOW-MONITOR-MIB • CISCO-IPSEC-MIB • CISCO-IPSEC-POLICY-MAP-MIB	選択したプラットフォーム、Cisco IOS ソフトウェア リリース、およびフィーチャセットの MIB を検索してダウンロードする場合は、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

RFC

RFC	タイトル
なし。	--

シスコのテクニカル サポート

説明	リンク
シスコのサポート Web サイトでは、シスコの製品やテクノロジーに関するトラブルシューティングにお役立ていただけるように、マニュアルやツールをはじめとする豊富なオンライン リソースを提供しています。 お使いの製品のセキュリティ情報や技術情報を入手するために、Cisco Notification Service（Field Notice からアクセス）、Cisco Technical Services Newsletter、Really Simple Syndication（RSS）フィードなどの各種サービスに加入できます。 シスコのサポート Web サイトのツールにアクセスする際は、Cisco.com のユーザ ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

Cisco VRF-Aware IPSec の IPsec および IKE MIB サポートに関する機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *252 : Cisco VRF-Aware IPSec* の *IPsec* および *IKE MIB* サポートに関する機能情報

機能名	リリース	機能情報
Cisco VRF-Aware IPSec の IPSec および IKE MIB サポート	IOS XE 3.1S	バーチャル プライベート ネットワークのルーティングと転送（VRF）対応 IP security（IPsec）機能を使用すると、MIB で VRF 対応 IPsec を管理できます。これにより、VRF ごとに IPsec 統計情報とパフォーマンス メトリックの詳細が表示されます。 この機能は、Cisco IOS Release 12.4(4)T で導入されました。 この機能は、Cisco IOS Release XE 3.1S に統合されました。 次のコマンドが導入または変更されました。**debug crypto mib**。

第 189 章

IPsec SNMP サポート

IP セキュリティ（IPsec）SNMP サポート機能には、業界標準の IPsec MIB および Cisco IOS XE ソフトウェア固有の IPsec MIB が導入されています。

この機能のコマンドを使用すれば、IPsec MIB 機能のバージョンを確認したり、SNMP トラップをディセーブルにしたり、この機能によって使用されるバッファのサイズをモニタリングおよび制御したりできます。

（注） このマニュアルでは、Cisco IPsec MIB の Cisco IOS XE CLI サポートを中心に説明します。また、このマニュアルでは現在サポートされている MIB の要素も示します。このマニュアルでは、Cisco IPsec MIB の（ネットワーク管理ステーションからの）SNMP 設定については説明しません。

IPsec SNMP サポートの制限事項

- IPsec--SNMP サポート機能でサポートされるトンネル設定エラー ログは次のものだけです。
  - NOTIFY_MIB_IPSEC_PROPOSAL_INVALID
  - 「A tunnel could not be established because the peer did not supply an acceptable proposal.」
  - NOTIFY_MIB_IPSEC_ENCRYPT_FAILURE
  - 「A tunnel could not be established because it failed to encrypt a packet to be sent to a peer.」
  - NOTIFY_MIB_IPSEC_SYSCAP_FAILURE
  - 「A tunnel could not be established because the system ran out of resources.」

- NOTIFY_MIB_IPSEC_LOCAL_FAILURE
- 「A tunnel could not be established because of an internal error.」

これらのエラー通知はエラーテーブルに記録されますが、SNMP 通知（トラップ）としては使用できないことに注意してください。

- 次の機能は、IPsec MIB 機能ではサポートされていません。
  - チェックポインティング
  - CISCO-IPSEC-MIB の Dynamic Cryptomap テーブル
- CISCO-IPSEC-POLICY-MAP-MIB（ciscoIpSecPolMap）で定義されている通知はありません（「IPSec Policy Map Notifications Group」は空です）。

IPsec SNMP サポートの情報

IP セキュリティ（IPsec）SNMP サポート機能には、業界標準の IPsec MIB および Cisco IOS XE ソフトウェア固有の IPsec MIB が導入されています。

IPsec MIB を使用すれば、SNMP を使用した IPsec 設定のモニタリングおよび IPsec ステータスのモニタリングが可能です。また、IPsec MIB を各種バーチャル プライベート ネットワーク（VPN）ソリューションに統合できます。

たとえば、この機能を使用すれば、Cisco IOS XE CLI を使用して、トンネル履歴テーブルやトンネル エラー テーブルのサイズを細かく指定できます。履歴テーブルには、トンネルに関する属性および統計情報がアーカイブされます。エラーテーブルには、トンネルのエラーの原因とエラーが発生した時刻がアーカイブされます。エラー履歴テーブルは、トンネルの終了が通常のものか異常なものかを区別するための簡単な手段として使用できます。つまり、トンネル履歴テーブル内のトンネル エントリに関連するエラー レコードがない場合、トンネルは正常に終了したことになります。ただし、すべてのエラーがトンネルのものとは限らないので、トンネル履歴テーブルがすべてのエラーテーブルを伴うわけではありません。そのため、サポート対象の設定エラーはエラーテーブルに記録されますが、関連する履歴テーブルは、トンネルが設定されていないので、記録されません。

この機能では、ネットワーク管理システムで使用される IPsec 簡易ネットワーク管理プロトコル（SNMP）通知も提供されます。

関連機能およびテクノロジー

IPsec--SNMP サポート機能は、VPN Device Manager（VDM）をサポートするように設計されました。VDM によって、ネットワーク管理者は、Web ブラウザから単一デバイス上のサイト間 VPN を管理および設定でき、また、リアルタイムで変更の効果を確認できます。VDM では、IPsec プロトコルを使用したサイト間 VPN の設定プロセスを簡単にするために、ウィザードベースのグラフィカル ユーザ インターフェイス（GUI）が実装されます。VDM ソフトウェアは Cisco VPN ルータに直接インストールされます。また、VDM ソフトウェアは、次世代の Device Manager 製品で使用でき、互換性を保つように設計されています。

IPsec SNMP サポートの設定方法

IPsec SNMP 通知のイネーブル化

IPsec SNMP 通知をイネーブルにするには、次の手順を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **snmp-server enable traps ipsec cryptomap** [**add** | **delete** | **attach** | **detach**]
4. **snmp-server enable traps isakmp** [**policy** {**add** | **delete**} | **tunnel** {**start** | **stop**}]
5. **snmp-server host** *host-address* **traps** *community-string* **ipsec**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**snmp-server enable traps ipsec cryptomap** [**add**	**delete**	**attach**	**detach**] 例： `Router (config)# snmp-server enable traps ipsec cryptomap add`	ルータを、IPsec SNMP 通知を送信するようにルータをイネーブルにします。
ステップ 4	**snmp-server enable traps isakmp** [**policy** {**add**	**delete**}	**tunnel** {**start**	**stop**}] 例： `Router (config)# snmp-server enable traps isakmp policy add`	ルータを、IPsec ISAKMP SNMP 通知を送信するようにルータをイネーブルにします。
ステップ 5	**snmp-server host** *host-address* **traps** *community-string* **ipsec** 例：	IPsec SNMP 通知動作の受信者を指定します。

	コマンドまたはアクション	目的
	`Router (config)# snmp-server host my.example.com traps version2c`	

次のタスク

SNMP の設定の詳細については、『*Cisco IOS XE Configuration Fundamentals Configuration Guide*』の「Configuring SNMP Support」章を参照してください。

IPsec エラー履歴テーブルのサイズの設定

デフォルトのエラー履歴テーブルのサイズは200です。エラー履歴テーブルのサイズを変更するには、次の手順を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **crypto mib ipsec flowmib history failure size** *number*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**crypto mib ipsec flowmib history failure size** *number* 例： `Router (config)# crypto mib ipsec flowmib history failure size 220`	IPsec エラー履歴テーブルのサイズを変更します。

IPsec トンネル履歴テーブルのサイズの設定

デフォルトのトンネル履歴テーブルのサイズは200です。トンネル履歴テーブルのサイズを変更するには、次の手順を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **crypto mib ipsec flowmib history tunnel size** *number*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**crypto mib ipsec flowmib history tunnel size** *number* 例： `Router (config)# crypto mib ipsec flowmib history tunnel size`	IPsec トンネル履歴テーブルのサイズを変更します。

IPsec MIB 設定の確認

IPsec MIB 機能が正しく設定されているかどうかを確認するには、次のタスクを実行します。

- **show crypto mib ipsec flowmib history failure size** 特権 EXEC コマンドを入力して、エラー履歴テーブルのサイズを表示します。

```
Router# show crypto mib ipsec flowmib history failure size
IPSec Failure Window Size: 140
```

- **show crypto mib ipsec flowmib history tunnel size** 特権 EXEC コマンドを入力して、トンネル履歴テーブルのサイズを表示します**:**

```
Router# show crypto mib ipsec flowmib history tunnel size
IPSec History Window Size: 130
```

- **show crypto mib ipsec flowmib version** 特権 EXEC コマンドを入力して、管理アプリケーションによって使用される MIB バージョンを表示して、フィーチャセットを識別します。

```
Router# show crypto mib ipsec flowmib version
IPSec Flow MIB version: 1
```

- **debug crypto mib** コマンドを入力して、IPsec MIB デバッグメッセージ通知を表示します。

```
Router# debug crypto mib
Crypto IPSec Mgmt Entity debugging is on
```

IPsec MIB のモニタおよびメンテナンス

IPsec MIB 情報のステータスをモニタリングするには、次のコマンドのいずれかを使用します。

手順の概要

1. **enable**
2. **show crypto mib ipsec flowmib history failure size**
3. **show crypto mib ipsec flowmib history tunnel size**
4. **show crypto mib ipsec flowmib version**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**show crypto mib ipsec flowmib history failure size** 例： `Router# show crypto mib ipsec flowmib history failure size`	IPsec エラー履歴テーブルのサイズを表示します。
ステップ 3	**show crypto mib ipsec flowmib history tunnel size** 例： `Router# show crypto mib ipsec flowmib history tunnel size`	IPsec トンネル履歴テーブルのサイズを表示します。
ステップ 4	**show crypto mib ipsec flowmib version** 例： `Router# show crypto mib ipsec flowmib version`	ルータによって使用される IPsec Flow MIB のバージョンを表示します。

IPsec SNMP サポートの設定例

IPsec 通知のイネーブル化の例

次に、IPsec 通知がイネーブルにされている例を示します。

```
snmp-server enable traps ipsec isakmp
```

次に、ルータが、ホスト nms1.example.com に IPsec 通知を送信するように設定されている例を示します。

```
snmp-server host nms1.example.com public ipsec isakmp
Translating "nms1.example.com"...domain server (172.00.0.01) [OK]
```

履歴テーブルのサイズの指定例

次に、指定したエラー履歴テーブルのサイズが 140 になっている例を示します。

```
crypto mib ipsec flowmib history failure size 140
```

次に、指定したトンネル履歴テーブルのサイズが 130 になっている例を示します。

```
crypto mib ipsec flowmib history tunnel size 130
```

その他の参考資料

関連資料

関連項目	マニュアル タイトル
AAA アカウンティングの設定	• 「Configuring Accounting」
IPsec VPN アカウンティングの設定	• 「Configuring Security for VPNs with IPsec」
基本 AAA RADIUS の設定	• Cisco.com にある『*Cisco IOS Security Configuration Guide: User Services*』の「Configuring RADIUS」の章
ISAKMP プロファイルの設定	「VRF Aware IPsec」
TACACS+ および RADIUS での権限レベル	• 「Configuring TACACS+」 • Cisco.com にある『*Cisco IOS Security Configuration Guide: User Services*』の「Configuring RADIUS」の章
IP セキュリティ、RADIUS、および AAA コマンド	『*Cisco IOS Security Command Reference*』
推奨される暗号化アルゴリズム	『Next Generation Encryption』

MIB

MIB	MIB のリンク
なし	選択したプラットフォーム、Cisco IOS リリース、およびフィーチャ セットに関する MIB を探してダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

シスコのテクニカル サポート

説明	リンク
右の URL にアクセスして、シスコのテクニカル サポートを最大限に活用してください。これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

IPsec SNMP サポートの機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *253 : IPsec SNMP* サポートの機能情報

機能名	リリース	機能情報
IPsec SNMP サポート	Cisco IOS XE Release 2.1	IP セキュリティ（IPsec）SNMP サポート機能には、業界標準の IPsec MIB および Cisco IOS XE ソフトウェア固有の IPsec MIB が導入されています。 次のコマンドが導入または変更されました。**crypto mib ipsec flowmib history failure size, crypto mib ipsec flowmib history tunnel size, debug crypto mib, show crypto mib ipsec flowmib history failure size, show crypto mib ipsec flowmib history tunnel size, show crypto mib ipsec flowmib version, snmp-server enable traps ipsec, snmp-server enable traps isakmp, snmp-server host**。

用語集

CA ：認証局。認証局（CA）は、メッセージ暗号化用のセキュリティ証明書および公開キー（X509v3 証明書の形式）を発行および管理する、ネットワーク内のエンティティです。CA は、公開キー インフラストラクチャ（PKI）の一部として、デジタル証明書の要求側が提供した情報を確認するために登録局（RA）に問い合わせます。RA によって要求側の情報が確認されると、CA は証明書を発行できます。一般に、証明書には、オーナーの公開キー、証明書の失効日、およびそ公開キーのオーナーに関するその他の情報が含まれています。

IP Security ：「IPsec」を参照してください。

IPsec ：インターネット プロトコル セキュリティ。参加ピア間でのデータの機密性、整合性、および認証を提供するオープン スタンダードの枠組みです。IPsec では、これらのセキュリティ サービスが IP レイヤで実現されます。IPsec では、インターネット キー交換（IKE）によって、ローカル ポリシーに基づいたプロトコルおよびアルゴリズムのネゴシエーションが処理され、IPsec によって使用される暗号キーおよび認証キーが生成されます。IPsec は、1 組のホスト間、1 組のセキュリティ ゲートウェイ間、またはセキュリティ ゲートウェイとホスト間で 1 つ以上のデータ フローを保護するために使用できます。

Management Information Base ：「MIB」を参照してください。

MIB ：管理情報ベース。ネットワーク管理情報のデータベースです。これらの情報は、簡易ネットワーク管理プロトコル（SNMP）や共通管理情報プロトコル（CMIP）などのネットワーク管理プロトコルにより使用および保持されます。MIB オブジェクトの値は、SNMP コマンドまたは CMIP コマンドを使用して変更および取得できます。これらのコマンドは通常、グラフィカル ユーザ インターフェイス（GUI）のネットワーク管理システム（NMS）から実行します。MIB オブジェクトはツリー構造であり、ツリーにはパブリック（標準）ブランチとプライベート（独自）ブランチを含みます。

Simple Network Management Protocol ：「SNMP」を参照してください。

SNMP ：簡易ネットワーク管理プロトコル。アプリケーション層プロトコルであり、SNMP マネージャと SNMP エージェントとの通信に使用されるメッセージ形式を規定します。

trap ：重要なイベントを知らせるためのメッセージです。指定された重大な状況が発生したり、しきい値を超過した場合、SNMP エージェントから、ネットワーク管理システム、コンソール、または端末へ送信されます。

第 190 章

IPsec VPN アカウンティング

IPsec VPN アカウンティング機能を使用すれば、セッションが開始される時と終了する時を指示することによって、セッションをアカウンティングできます。

VPNセッションとは、インターネットキー交換（IKE）セキュリティアソシエーション（SA）および、IKE SAによって作成される1つ以上のSAペアとして定義されます。セッションは、最初のIPセキュリティ（IPsec）ペアが作成されると開始し、すべてのIPsec SAが削除されると停止します。

セッション識別情報およびセッション使用状況情報は、標準RADIUS属性とベンダー固有属性を介して、Remote Authentication Dial-In User Service（RADIUS）サーバに渡されます。

IPsec VPN アカウンティングの前提条件

- RADIUSと認証、許可、アカウンティング（AAA）アカウンティングの設定方法を理解します。
- IPsecアカウンティングの設定方法を理解します。

IPsec VPN アカウンティングに関する情報

RADIUS アカウンティング

多くの大規模ネットワークでは、監査のために、ユーザアクティビティを記録する必要があります。多く使用される方式は、RADIUS アカウンティングです。

RADIUSアカウンティングを使用すれば、セッションが開始される時と終了する時を指示することによって、セッションをアカウンティングできます。また、セッション識別情報およびセッション使用状況情報が、RADIUS属性およびVSAを介してRADIUSサーバに渡されます。

RADIUS 開始アカウンティング

RADIUS 開始パケットには、一般的には、サービスを要求する者、およびサービスのプロパティの構成を特定する多くの属性が格納されています。次の表に、開始に必要な属性を示します。

表 *254 : RADIUS* アカウンティング開始パケット属性

RADIUS 属性値	属性	説明
1	user-name	拡張認証（XAUTH）で使用されるユーザ名。XAUTH が使用されない場合、ユーザ名が NULL になる場合があります。
4	nas-ip-address	ユーザにサービスを提供するネットワーク アクセス サーバ（NAS）の IP アドレスの識別。RADIUS サーバのスコープ内の NAS に対して一意である必要があります。
5	nas-port	ユーザにサービスを提供する NAS の物理ポート番号。
8	framed-ip-address	IPsecセッション用に割り当てられたプライベートアドレス。
40	acct-status-type	ステータス タイプ。この属性では、このアカウンティング要求がマーキングするのが、セッションの開始（start）、終了（stop）、または更新のいずれかなのかを示します。
41	acct-delay-time	クライアントが特定のレコードの送信を試行した秒数。
44	acct-session-id	ログ ファイル内の開始レコードと終了レコードのマッチングを容易にする一意のアカウンティング ID。
26	vrf-id	Virtual Route Forwarder（VRF）の名前を表す文字列。
26	isakmp-initiator-ip	リモートIKEの発信側（V4）のエンドポイントIPアドレス。

RADIUS 属性値	属性	説明
26	isakmp-group-id	アカウンティングに使用される VPN グループ プロファイルの名前。
26	isakmp-phase1-id	セッションの発信側の識別を可能にする、IKE によって使用されるフェーズ 1 識別情報（ID）（たとえば、ドメイン名（DN）、完全修飾ドメイン名（FQDN）、IPアドレスなど）。

RADIUS 終了アカウンティング

RADIUS 終了パケットには、セッションの使用状況を識別する多くの属性が格納されています。表 2 に、RADIUS 終了パケットに必要な追加属性を示します。開始パケットなしで終了パケットだけを送信することは、そのように設定すれば可能です。終了パケットだけを送信すれば、これにより、AAA サーバに送信されるレコードの数を簡単に減らせます。

表 *255 : RADIUS* アカウンティング終了パケット属性

RADIUS 属性値	属性	説明
42	acct-input-octets	サービスが提供されている間に Unity クライアントから受信されたオクテット数。
43	acct-output-octets	このサービスの配信中に Unity クライアントに送信されたオクテット数。
46	acct-session-time	Unity クライアントがサービスを受信した時間の長さ（秒単位）。
47	acct-input-packets	このサービスの配信中に Unity クライアントから受信したパケット量。
48	acct-output-packets	このサービスの配信中に Unity クライアントに送信したパケット量。
49	acct-terminate-cause	未使用。
52	acct-input-gigawords	このサービスの間に Acct-Input-Octets カウンタの値が 232（2 の 32 乗）を超えた回数。
52	acct-output-gigawords	このサービスの間に Acct-Input-Octets カウンタの値が 232（2 の 32 乗）を超えた回数。

RADIUS 更新アカウンティング

RADIUS 更新アカウンティングがサポートされています。パケットおよびオクテットカウントが更新内に表示されます。

IKE および IPsec サブシステムの相互作用

Accounting Start

IPsec アカウンティングが設定されている場合、IKE フェーズが終了すると、アカウンティング開始レコードがセッション用に生成されます。キー再生成中は、新しいアカウンティングレコードは生成されません。

次に、ルータ上で生成されており、定義されている AAA サーバに送信されるアカウント開始レコードを示します。

```
*Aug 23 04:06:20.131: RADIUS(00000002): sending
*Aug 23 04:06:20.131: RADIUS(00000002): Send Accounting-Request to 10.1.1.4:1646 id 4,
len 220
*Aug 23 04:06:20.131: RADIUS:  authenticator 38 F5 EB 46 4D BE 4A 6F - 45 EB EF 7D B7
19 FB 3F
*Aug 23 04:06:20.135: RADIUS:  Acct-Session-Id     [44]  10  "00000001"
*Aug 23 04:06:20.135: RADIUS:  Vendor, Cisco       [26]  31
*Aug 23 04:06:20.135: RADIUS:   Cisco AVpair       [1]   25  "isakmp-group-id=cclient"
*Aug 23 04:06:20.135: RADIUS:  Framed-IP-Address   [8]   6   10.13.13.1
*Aug 23 04:06:20.135: RADIUS:  Vendor, Cisco       [26]  20
*Aug 23 04:06:20.135: RADIUS:   Cisco AVpair       [1]   14  "vrf-id=cisco"
*Aug 23 04:06:20.135: RADIUS:  Vendor, Cisco       [26]  35
*Aug 23 04:06:20.135: RADIUS:   Cisco AVpair      [1]   29  "isakmp-initator-ip=10.1.2.2"
*Aug 23 04:06:20.135: RADIUS:  Vendor, Cisco       [26]  36
*Aug 23 04:06:20.135: RADIUS:   Cisco AVpair      [1]   30  "connect-progress=No Progress"
*Aug 23 04:06:20.135: RADIUS:  User-Name           [1]   13  "username1"
*Aug 23 04:06:20.135: RADIUS:  Acct-Status-Type    [40]  6   Start
[1]
*Aug 23 04:06:20.135: RADIUS:  Vendor, Cisco       [26]  25
*Aug 23 04:06:20.135: RADIUS:   cisco-nas-port     [2]   19  "FastEthernet0/0.1"
*Aug 23 04:06:20.135: RADIUS:  NAS-Port            [5]   6   0
*Aug 23 04:06:20.135: RADIUS:  NAS-IP-Address      [4]   6   10.1.1.147
*Aug 23 04:06:20.135: RADIUS:  Acct-Delay-Time     [41]  6   0
*Aug 23 04:06:20.139: RADIUS: Received from id 21645/4 10.1.1.4:1646, Accounting-response,
 len 20
*Aug 23 04:06:20.139: RADIUS:  authenticator B7 E3 D0 F5 61 9A 89 D8 - 99 A6 8A 8A 98
79 9D 5D
```

アカウンティング終了

リモートピアでのフロー（IPsec SA ペア）がなくなると、アカウンティング終了パケットが生成されます。

アカウンティング終了レコードには次の情報が格納されます。

- パケット出力
- パケット入力
- オクテット出力

- ギガワード入力
- ギガワード出力

次に、ルータ上で生成されたアカウント開始レコードを示します。アカウント開始レコードは、定義されている AAA サーバに送信されます。

```
*Aug 23 04:20:16.519: RADIUS(00000003): Using existing nas_port 0
*Aug 23 04:20:16.519: RADIUS(00000003): Config NAS IP: 100.1.1.147
*Aug 23 04:20:16.519: RADIUS(00000003): sending
*Aug 23 04:20:16.519: RADIUS(00000003): Send Accounting-Request to 100.1.1.4:1646 id 19,
 len 238
*Aug 23 04:20:16.519: RADIUS:  authenticator 82 65 5B 42 F0 3F 17 C3 - 23 F3 4C 35 A2
8A 3E E6
*Aug 23 04:20:16.519: RADIUS:  Acct-Session-Id     [44]  10  "00000002"
*Aug 23 04:20:16.519: RADIUS:  Vendor, Cisco       [26]  20
*Aug 23 04:20:16.519: RADIUS:   Cisco AVpair       [1]   14  "vrf-id=cisco"
*Aug 23 04:20:16.519: RADIUS:  Vendor, Cisco       [26]  35
*Aug 23 04:20:16.519: RADIUS:   Cisco AVpair      [1]   29  "isakmp-initator-ip=10.1.1.2"
*Aug 23 04:20:16.519: RADIUS:  Vendor, Cisco       [26]  36
*Aug 23 04:20:16.519: RADIUS:   Cisco AVpair      [1]   30  "connect-progress=No Progress"
*Aug 23 04:20:16.519: RADIUS:  Acct-Session-Time   [46]  6   709
*Aug 23 04:20:16.519: RADIUS:  Acct-Input-Octets   [42]  6   152608
*Aug 23 04:20:16.519: RADIUS:  Acct-Output-Octets  [43]  6   152608
*Aug 23 04:20:16.519: RADIUS:  Acct-Input-Packets  [47]  6   1004
*Aug 23 04:20:16.519: RADIUS:  Acct-Output-Packets [48]  6   1004
*Apr 23 04:20:16.519: RADIUS:  Acct-Input-Giga-Word[52]  6   0
*Apr 23 04:20:16.519: RADIUS:  Acct-Output-Giga-Wor[53]  6   0

*Aug 23 04:20:16.519: RADIUS:  Acct-Terminate-Cause[49]  6   none
[0]
*Aug 23 04:20:16.519: RADIUS:  Vendor, Cisco       [26]  32
*Aug 23 04:20:16.519: RADIUS:   Cisco AVpair       [1]   26  "disc-cause-ext=No Reason"
*Aug 23 04:20:16.519: RADIUS:  Acct-Status-Type    [40]  6   Stop
[2]
*Aug 23 04:20:16.519: RADIUS:  Vendor, Cisco       [26]  25
*Aug 23 04:20:16.519: RADIUS:   cisco-nas-port     [2]   19  "FastEthernet0/0.1"
*Aug 23 04:20:16.519: RADIUS:  NAS-Port            [5]   6   0
*Aug 23 04:20:16.519: RADIUS:  NAS-IP-Address      [4]   6   100.1.1.147
*Aug 23 04:20:16.519: RADIUS:  Acct-Delay-Time     [41]  6   0
*Aug 23 04:20:16.523: RADIUS: Received from id 21645/19 100.1.1.4:1646,
Accounting-response, len 20
*Aug 23 04:20:16.523: RADIUS:  authenticator F1 CA C1 28 CE A0 26 C9 - 3E 22 C9 DA EA
B8 22 A0
```

アカウンティング更新

アカウンティング更新がイネーブルな場合、セッションが「アップ」であればアカウンティング更新が送信されます。更新間隔は設定可能です。アカウンティング更新をイネーブルにするには、**aaa accounting update** コマンドを使用します。

次に、ルータから送信されるアカウンティング更新を示します。

```
Router#
*Aug 23 21:46:05.263: RADIUS(00000004): Using existing nas_port 0
*Aug 23 21:46:05.263: RADIUS(00000004): Config NAS IP: 100.1.1.147
*Aug 23 21:46:05.263: RADIUS(00000004): sending
*Aug 23 21:46:05.263: RADIUS(00000004): Send Accounting-Request to 100.1.1.4:1646 id 22,
 len 200
```

```
*Aug 23 21:46:05.263: RADIUS:  authenticator 30 FA 48 86 8E 43 8E 4B - F9 09 71 04 4A
F1 52 25
*Aug 23 21:46:05.263: RADIUS:  Acct-Session-Id     [44]  10  "00000003"
*Aug 23 21:46:05.263: RADIUS:  Vendor, Cisco       [26]  20
*Aug 23 21:46:05.263: RADIUS:   Cisco AVpair       [1]   14  "vrf-id=cisco"
*Aug 23 21:46:05.263: RADIUS:  Vendor, Cisco       [26]  35
*Aug 23 21:46:05.263: RADIUS:   Cisco AVpair      [1]   29  "isakmp-initator-ip=10.1.1.2"
*Aug 23 21:46:05.263: RADIUS:  Vendor, Cisco       [26]  36
*Aug 23 21:46:05.263: RADIUS:   Cisco AVpair      [1]   30  "connect-progress=No Progress"
*Aug 23 21:46:05.263: RADIUS:  Acct-Session-Time   [46]  6   109
*Aug 23 21:46:05.263: RADIUS:  Acct-Input-Octets   [42]  6   608
*Aug 23 21:46:05.263: RADIUS:  Acct-Output-Octets  [43]  6   608
*Aug 23 21:46:05.263: RADIUS:  Acct-Input-Packets  [47]  6   4
*Aug 23 21:46:05.263: RADIUS:  Acct-Output-Packets [48]  6   4
*Aug 23 21:46:05.263: RADIUS:  Acct-Status-Type    [40]  6   Watchdog
[3]
*Aug 23 21:46:05.263: RADIUS:  Vendor, Cisco       [26]  25
*Aug 23 21:46:05.263: RADIUS:   cisco-nas-port     [2]   19  "FastEthernet0/0.1"
*Aug 23 21:46:05.263: RADIUS:  NAS-Port            [5]   6   0
*Aug 23 21:46:05.263: RADIUS:  NAS-IP-Address      [4]   6   100.1.1.147
*Aug 23 21:46:05.263: RADIUS:  Acct-Delay-Time     [41]  6   0
*Aug 23 21:46:05.267: RADIUS: Received from id 21645/22 100.1.1.4:1646,
Accounting-response, len 20
*Aug 23 21:46:05.267: RADIUS:  authenticator 51 6B BB 27 A4 F5 D7 61 - A7 03 73 D3 0A
AC 1C
```

IPsec VPN アカウンティングの設定方法

IPsec VPN アカウンティングの設定

始める前に

IPsec は、IPsec VPN アカウンティングを設定するより先に設定する必要があります。

手順の概要

1. **enable**
2. **configure terminal**
3. **aaa new-model**
4. **aaa authentication login** *list-name method*
5. **aaa authorization network** *list-name method*
6. **aaa accounting network list-name start-stop** [**broadcast**] **group** *group-name*
7. **aaa session-id common**
8. **crypto isakmp profile** *profile-name*
9. **vrf** *ivrf*
10. **match identity group** *group-name*
11. **client authentication list** *list-name*
12. **isakmp authorization list** *list-name*
13. **client configuration address** [**initiate** | **respond**]
14. **accounting** *list-name*
15. **exit**

16. **crypto dynamic-map** *dynamic-map-name dynamic-seq-num*
17. **set transform-set** *transform-set-name*
18. **set isakmp-profile** *profile-name*
19. **reverse-route** [**remote-peer**]
20. **exit**
21. **crypto map** *map-name* **ipsec-isakmp dynamic** *dynamic-template-name*
22. **radius-server host** *ip-address* [**auth-port** *port-number]* [**acct-port** *port-number*]
23. **radius-server key** *string*
24. **radius-server vsa send accounting**
25. **interface** *type slot / port*
26. **crypto map** *map-name*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**aaa new-model** 例： `Router (config)# aaa new-model`	アカウンティング サーバに送信される定期的中間アカウンティング レコードをイネーブルにします。
ステップ 4	**aaa authentication login** *list-name method* 例： `Router (config)# aaa authentication login cisco-client group radius`	RADIUS またはローカル経由で、認証、許可、および拡張認可（XAUTH）のアカウンティング（AAA）認証を実行します。
ステップ 5	**aaa authorization network** *list-name method* 例： `Router (config)# aaa authorization network cisco-client group radius`	RADIUS またはローカルから、リモート クライアント上の AAA 認証パラメータを設定します。
ステップ 6	**aaa accounting network list-name start-stop** [**broadcast**] **group** *group-name* 例：	RADIUS または TACACS+ を使用する場合の課金またはセキュリティのために、要求されたサービスの AAA アカウンティングをイネーブルにします。

	コマンドまたはアクション	目的
	`Router (config)# aaa accounting network acc start-stop broadcast group radius`	
ステップ 7	**aaa session-id common** 例： `Router (config)# aaa session-id common`	コール内の各 AAA アカウンティング サービス タイプに、同じセッション ID を使用するかどうか、または、各アカウンティング サービス タイプに対して異なるセッション ID を割り当てるかどうかを指定します。
ステップ 8	**crypto isakmp profile** *profile-name* 例： `Route (config)# crypto isakmp profile cisco`	IPsec ユーザ セッションを監査し、isakmp-profile サブモードを開始します。
ステップ 9	**vrf** *ivrf* 例： `Router (conf-isa-prof)# vrf cisco`	オンデマンド アドレス プールを、バーチャル プライベート ネットワーク（VPN）Routing and Forwarding（VRF）インスタンス名に関連付けます。
ステップ 10	**match identity group** *group-name* 例： `Router(conf-isa-prof)# match identity group cisco`	ISAKMP プロファイルのピアの ID を一致させます。
ステップ 11	**client authentication list** *list-name* 例： `Router(conf-isa-prof)# client authentication list cisco`	Internet Security Association and Key Management Protocol（ISAKMP）プロファイル内の IKE 拡張認証（XAUTH）を設定します。
ステップ 12	**isakmp authorization list** *list-name* 例： `Router(conf-isa-prof)# isakmp authorization list cisco-client`	ISAKMP プロファイル内の AAA サーバを使用して、IKE 共有秘密およびその他のパラメータを設定します。一般に、共有秘密およびその他のパラメータは、モード設定（MODECFG）を介して、リモート ピアへプッシュされます。
ステップ 13	**client configuration address** [**initiate** | **respond**] 例： `Router(conf-isa-prof)# client configuration address respond`	ISAKMP プロファイル内で IKE モード設定（MODECFG）を設定します。
ステップ 14	**accounting** *list-name* 例： `Router(conf-isa-prof)# accounting acc`	この ISAKMP プロファイルを介して接続しているすべてのピアの AAA アカウンティング サービスをイネーブルにします。

	コマンドまたはアクション	目的
ステップ 15	**exit** 例： `Router(conf-isa-prof)# exit`	isakmp-profile サブモードを終了します。
ステップ 16	**crypto dynamic-map** *dynamic-map-name dynamic-seq-num* 例： `Router(config)# crypto dynamic-map mymap 10 ipsec-isakmp`	ダイナミック クリプト マップ テンプレートを作成し、クリプト マップ コンフィギュレーション コマンド モードを開始します。
ステップ 17	**set transform-set** *transform-set-name* 例： `Router(config-crypto-map)# set transform-set aswan`	クリプト マップ テンプレートで使用可能なトランスフォーム セットを指定します。
ステップ 18	**set isakmp-profile** *profile-name* 例： `Router(config-crypto-map)# set isakmp-profile cisco`	ISAKMP プロファイル名を設定します。
ステップ 19	**reverse-route** [**remote-peer**] 例： `Router(config-crypto-map)# reverse-route`	ルート（IP アドレス）を、VPN リモート トンネル エンドポイントの背後の宛先に対して注入できるようにします。また、トンネルエンドポイント自体に対するルートを設定することも可能です（クリプト マップの **remote-peer** キーワードを使用します）。
ステップ 20	**exit** 例： `Router(config-crypto-map)# exit`	ダイナミック クリプト マップ コンフィギュレーション モードを終了します。
ステップ 21	**crypto map** *map-name* **ipsec-isakmp dynamic** *dynamic-template-name* 例： `Router(config)# crypto map mymap ipsec-isakmp dynamic dmap`	クリプト マップ コンフィギュレーション モードを開始します。
ステップ 22	**radius-server host** *ip-address* [**auth-port** *port-number]* [**acct-port** *port-number*] 例： `Router(config)# radius-server host 172.16.1.4`	RADIUS サーバ ホストを指定します。

	コマンドまたはアクション	目的
ステップ 23	**radius-server key** *string* 例： `Router(config)# radius-server key nsite`	ルータおよび RADIUS デーモン間のすべての RADIUS コミュニケーションの認証キーおよび暗号キーを指定します。
ステップ 24	**radius-server vsa send accounting** 例： `Router(config)# radius-server vsa send accounting`	ベンダー固有属性を認識し使用するために、ネットワーク アクセス サーバーを設定します。
ステップ 25	**interface** *type slot / port* 例： `Router(config)# interface FastEthernet 1/0`	インターフェイス タイプを設定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 26	**crypto map** *map-name* 例： `Router(config-if)# crypto map mymap`	インターフェイスに対して以前に定義されたクリプト マップ セットを適用します。

アカウンティング更新の設定

セッションが「up」中にアカウンティング更新を送信するには、次の任意の作業を実行します。

始める前に

IPSec VPN アカウンティングは、アカウンティング更新の設定前に設定する必要があります。詳細については、「IPsec VPN アカウンティングの設定 （2768 ページ）」を参照してください。

手順の概要

1. **enable**
2. **configure terminal**
3. **aaa accounting update periodic** *number*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。

	コマンドまたはアクション	目的
ステップ 2	**configure terminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**aaa accounting update periodic** *number* 例： `Router (config)# aaa accounting update periodic 1-2147483647`	（任意）アカウンティング サーバに送信される定期的中間アカウンティング レコードをイネーブルにします。

IPsec VPN アカウンティングのトラブルシューティング

IPsec アカウンティング イベントに関するメッセージを表示するには、次の任意の作業を実行します。

手順の概要

1. **enable**
2. **debug crypto isakmp aaa**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**debug crypto isakmp aaa** 例： `Router# debug crypto isakmp aaa`	IKE に関するメッセージを表示します。 • **aaa** キーワードによって、アカウンティングイベントが指定されます。

IPsec VPN アカウンティングの設定例

アカウンティングおよび ISAKMP プロファイル例

次に、アカウンティングおよび ISAKMP プロファイルを持つリモート アクセス クライアントをサポートするための設定する例を示します。

```
version 2.1
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname sheep
!
aaa new-model
!
!
aaa accounting network ipsecaaa start-stop group radius
aaa accounting update periodic 1
aaa session-id common
ip subnet-zero
ip cef
!
!
no ip domain lookup
ip domain name cisco.com
ip name-server 172.29.2.133
ip name-server 172.29.11.48
!
!
crypto isakmp policy 1
authentication pre-share
group 2
!
crypto isakmp policy 10
hash md5
authentication pre-share
lifetime 200
crypto isakmp key cisco address 172.31.100.2
crypto iakmp client configuration group cclient
 key jegjegjhrg
 pool addressA

crypto-isakmp profile groupA
 vrf cisco
 match identity group cclient
 client authentication list cisco-client
 isakmp authorization list cisco-client
 client configuration address respond
 accounting acc
!
!
crypto ipsec transform-set esp-des-md5 esp-des esp-md5-hmac
!
crypto dynamic-map remotes 1
set peer 172.31.100.2
set security-association lifetime seconds 120
set transform-set esp-des-md5
reverse-route
!
crypto map test 10 ipsec-isakmp dynamic remotes
!
voice call carrier capacity active
!
interface Loopback0
ip address 10.20.20.20 255.255.255.0
no ip route-cache
no ip mroute-cache
!
interface FastEthernet0/0
```

```
ip address 10.2.80.203 255.255.255.0
no ip mroute-cache
load-interval 30
duplex full
!
interface FastEthernet1/0
ip address 192.168.219.2 255.255.255.0
no ip mroute-cache
duplex auto
speed auto
!
interface FastEthernet1/1
ip address 172.28.100.1 255.255.255.0
no ip mroute-cache
duplex auto
speed auto
crypto map test
!
no fair-queue
ip default-gateway 10.2.80.1
ip classless
ip route 10.0.0.0 0.0.0.0 10.2.80.1
ip route 10.20.0.0 255.0.0.0 10.2.80.56
ip route 10.10.10.0 255.255.255.0 172.31.100.2
ip route 10.0.0.2 255.255.255.255 10.2.80.73
ip local pool addressA 192.168.1.1 192.168.1.253
no ip http server
ip pim bidir-enable
!
!
ip access-list extended encrypt
permit ip host 10.0.0.1 host 10.5.0.1
!
access-list 101 permit ip host 10.20.20.20 host 10.10.10.10
!
!
radius-server host 172.27.162.206 auth-port 1645 acct-port 1646 key cisco123
radius-server retransmit 3
radius-server authorization permit missing Service-Type
radius-server vsa send accounting
call rsvp-sync
!
!
mgcp profile default
!
dial-peer cor custom
!
!
gatekeeper
shutdown
!
!
line con 0
exec-timeout 0 0
exec prompt timestamp
line aux 0
line vty 5 15
 ntp server 172.31.150.52
end
```

ISAKMP プロファイルなしのアカウンティング例

次に、ISAKMP プロファイルが使用されていない時にアカウンティング リモート アクセス ピアをサポートする Cisco IOS XE 設定全体の例を示します。

```
version 2.1
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname sheep
!
aaa new-model
!
!
aaa accounting network ipsecaaa start-stop group radius
aaa accounting update periodic 1
aaa session-id common
ip subnet-zero
ip cef
!
!
no ip domain lookup
ip domain name cisco.com
ip name-server 172.29.2.133
ip name-server 172.29.11.48
!
!
crypto isakmp policy 1
 authentication pre-share
 group 2
!
crypto isakmp policy 10
 hash md5
 authentication pre-share
 lifetime 200
crypto isakmp key cisco address 172.31.100.2
!
!
crypto ipsec transform-set esp-des-md5 esp-des esp-md5-hmac
!
crypto map test client accounting list ipsecaaa
crypto map test 10 ipsec-isakmp
 set peer 172.31.100.2
 set security-association lifetime seconds 120
 set transform-set esp-des-md5
 match address 101
!
voice call carrier capacity active
!
interface Loopback0
 ip address 10.20.20.20 255.255.255.0
 no ip route-cache
 no ip mroute-cache
!
interface FastEthernet0/0
 ip address 10.2.80.203 255.255.255.0
 no ip mroute-cache
 load-interval 30
 duplex full
!
interface FastEthernet1/0
```

```
 ip address 192.168.219.2 255.255.255.0
 no ip mroute-cache
 duplex auto
 speed auto
!
interface FastEthernet1/1
 ip address 172.28.100.1 255.255.255.0
 no ip mroute-cache
 duplex auto
 speed auto
 crypto map test
!
no fair-queue
ip default-gateway 10.2.80.1
ip classless
ip route 10.0.0.0 0.0.0.0 10.2.80.1
ip route 10.30.0.0 255.0.0.0 10.2.80.56
ip route 10.10.10.0 255.255.255.0 172.31.100.2
ip route 10.0.0.2 255.255.255.255 10.2.80.73
no ip http server
ip pim bidir-enable
!
!
ip access-list extended encrypt
 permit ip host 10.0.0.1 host 10.5.0.1
!
access-list 101 permit ip host 10.20.20.20 host 10.10.10.10
!
!
radius-server host 172.27.162.206 auth-port 1645 acct-port 1646 key cisco123
radius-server retransmit 3
radius-server authorization permit missing Service-Type
radius-server vsa send accounting
call rsvp-sync
!
!
mgcp profile default
!
dial-peer cor custom
!
!
gatekeeper
 shutdown
!
!
line con 0
 exec-timeout 0 0
 exec prompt timestamp
line aux 0
line vty 5 15
!
exception core-file ioscrypto/core/sheep-core
exception dump 172.25.1.129
ntp clock-period 17208229
ntp server 172.71.150.52
!
end
```

その他の参考資料

関連資料

関連項目	マニュアル タイトル
AAA アカウンティングの設定	『*Cisco IOS XE Security Configuration Guide: Securing User Services*』の「Configuring Accounting」モジュール
IPsec VPN アカウンティングの設定	『*Cisco IOS XE Security Configuration Guide: Secure Connectivity*』の「Configuring Security for VPNs with IPsec」モジュール
基本 AAA RADIUS の設定	『*Cisco IOS XE Security Configuration Guide: Securing User Services*』の「Configuring RADIUS」モジュール
ISAKMP プロファイルの設定	『*Cisco IOS XE Security Configuration Guide: Secure Connectivity*』の「VRF-Aware IPsec」モジュール
TACACS+ および RADIUS での権限レベル	• 『*Cisco IOS XE Security Configuration Guide: Securing User Services*』の「Configuring TACACS+」モジュール • 『*Cisco IOS XE Security Configuration Guide: Securing User Services*』の「Configuring RADIUS」モジュール
IP セキュリティ、RADIUS、および AAA コマンド	『*Cisco IOS Security Command Reference*』

標準

標準	タイトル
なし。	--

MIB

MIB	MIB のリンク
なし。	選択したプラットフォーム、Cisco ソフトウェア リリース、およびフィーチャ セットの MIB を検索してダウンロードする場合は、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

RFC

RFC	タイトル
なし。	

シスコのテクニカル サポート

説明	リンク
シスコのサポート Web サイトでは、シスコの製品やテクノロジーに関するトラブルシューティングにお役立ていただけるように、マニュアルやツールをはじめとする豊富なオンライン リソースを提供しています。 お使いの製品のセキュリティ情報や技術情報を入手するために、Cisco Notification Service（Field Notice からアクセス）、Cisco Technical Services Newsletter、Really Simple Syndication（RSS）フィードなどの各種サービスに加入できます。 シスコのサポート Web サイトのツールにアクセスする際は、Cisco.com のユーザ ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

IPsec VPN アカウンティングの機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだ

けを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *256 : IPsec VPN* アカウンティングの機能情報

機能名	リリース	機能情報
IPsec VPN アカウンティング	Cisco IOS XE Release 2.1	IPsec VPN アカウンティング機能を使用すれば、セッションが開始される時と終了する時を指示することによって、セッションをアカウンティングできます。 VPN セッションとは、IKE SA および、IKE SA によって作成される 1 つ以上の SA ペアとして定義されます。セッションは、最初の IPsec ペアが作成されると開始し、すべての IPsec SA が削除されると停止します。 セッション識別情報およびセッション使用状況情報が、標準的な RADIUS 属性および VSA を介して、RADIUS サーバに渡されます。 次のコマンドが導入または変更されました。**client authentication list, client configuration address, crypto isakmp profile, crypto map (global IPsec), debug crypto isakmp, isakmp authorization list, match identity, set isakmp-profile, vrf**。

用語集

IKE：Internet Key Exchange（インターネット キー エクスチェンジ）。IKE によって、キーが必要なサービス（IP セキュリティ（IPsec）など）のための共有セキュリティ ポリシーおよび認証キーが確立されます。IPsec トラフィックを通過させる前に、ルータ、ファイアウォール、ホストそれぞれでピアの ID を検証する必要があります。それには、事前共有キーを両ホストに手動で入力するか、認証局（CA）サービスを使用します。

IPsec：IP security（IP セキュリティ）。IPsec はオープン規格のフレームワークであり、これにより、参加ピア間でデータ機密性、データ整合性、およびデータ認証が提供されます。IPsec では、これらのセキュリティ サービスが IP レイヤで実現されます。IPsec では、ローカル ポリシーに基づいたプロトコルやアルゴリズムのネゴシエーションの処理や、IPsec に使用される暗号キーや認証キーの生成が、IKE を通じて行われます。IPsec は、1 組のホスト間、1 組のセキュリティ ゲートウェイ間、またはセキュリティ ゲートウェイとホスト間で 1 つ以上のデータ フローを保護するために使用できます。

ISAKMP：Internet Security Association and Key Management Protocol。ISAKMP は、セキュリティ アソシエーションのネゴシエーション、確立、変更、および削除を行うインターネット IPsec プロトコル（RFC 2408）です。また、キー生成および認証データ（特定のキー生成メカニズム

とは独立しています）、キー確立プロトコル、暗号化アルゴリズム、または認証メカニズムも交換されます。

L2TP session：Layer 2 Transport Protocol（レイヤ 2 転送プロトコル）。L2TP は、単一の PPP 接続のトンネリングがサポートされた、L2TP アクセス コンセントレータ（LAC）と L2TP ネットワーク サーバ（LNS）の間における通信トランザクションです。PPP 接続、L2TP セッション、および L2TP コールの間に 1 対 1 の関係があります。

NAS ：ネットワーク アクセス サーバー。NAS は、パケットの世界（インターネットなど）と回線の世界（公衆電話交換網（PSTN））との間のインターフェイスとなるシスコのプラットフォーム（または複数のプラットフォームの集まり。AccessPath システムなど）です。

PFS：Perfect Forward Secrecy。PFS は、導き出される共有秘密値に関連する暗号特性です。PFS を使用すると、1 つのキーが損なわれても、これ以降のキーは前のキーの取得元から取得されないため、前および以降のキーには影響しません。

QM：Queue Manager（キューマネージャ）。Cisco IP Queue Manager（IP QM）は、インテリジェントで、IP ベースの、コール処理およびルーティング ソリューションであり、Cisco IP Contact Center（PCC）ソリューションの一部として、強力なコール処理オプションが提供されます。

RADIUS ：リモート認証ダイヤルイン ユーザー サービス。RADIUS は、モデムおよび ISDN 接続の認証、および接続のトラッキングのためのデータベースです。

RSA：Rivest, Shamir, and Adelman（Rivest、Shamir、および Adelman）。Rivest、Shamir、および Adelman は、暗号化および認証に使用可能な公開キー暗号化システムの発明者たちです。

SA：Security Association（セキュリティ アソシエーション）。SA は、データ フローに適用されるセキュリティ ポリシーおよびキー関連情報のインスタンスです。

TACACS+：Terminal Access Controller Access Control System Plus（TACAS+）。TACACS+ は、ユーザーによるルータまたはネットワーク アクセス サーバーへのアクセス試行の集中的な確認を可能にするセキュリティアプリケーションです。

VPN：Virtual Private Network（仮想プライベートネットワーク）。VPN を使用すると、ネットワーク間のトラフィックをすべて暗号化することにより、パブリック TCP/IP ネットワーク経由でも IP トラフィックをセキュアに転送できます。VPN は「トンネリング」を使用して、IP レベルですべての情報を暗号化します。

VRF：VPN Routing/Forwarding instance（VPN ルーティング/転送インスタンス）。VRF は、IP ルーティング テーブル、取得されたルーティング テーブル、そのルーティング テーブルを使用する一連のインターフェイス、ルーティング テーブルに登録されるものを決定する一連のルールおよびルーティング プロトコルで構成されています。一般に、VRF には、PE ルータに付加されるカスタマー VPN サイトが定義されたルーティング情報が格納されています。

VSA：Vendor-Specific Attribute（ベンダー固有属性）。VSA は、特定のベンダーによって実装された属性です。Vendor-Specific 属性が使用された結果、AV ペアがカプセル化されます。基本的には、Vendor-Specific = プロトコル:Attribute = 値となります。

XAUTH：Extended Authentication（拡張認証）。XAUTH は、IKE フェーズ 1 と IKE フェーズ 2 の間における任意の交換です。XAUTH では、ルータが、（ピアの認証ではなく）実際のユーザの認証試行において、追加の認証情報を要求します。

第 191 章

IPsec Usability Enhancements

IPsec Usability Enhancements 機能では、IPsec バーチャル プライベート ネットワーク（VPN）の設定およびモニタリングを簡単にする機能が導入されています。この機能の利点としては、IPsec およびインターネット キー交換（IKE）のインテリジェントなデフォルト、および IPsec VPN を簡単に確認およびトラブルシューティングできる機能などがあります。

IPsec Usability Enhancements の前提条件

- IPsec、IKE、および暗号化の知識が必要です。
- IPsec を設定し、ルータ上の IKE をイネーブルにしておく必要があります。
- ルータ上で Cisco IOS XE k9 暗号イメージを実行する必要があります。

IPsec Usability Enhancements に関する情報

IPsec の概要

IPsec は、インターネット技術特別調査委員会（IETF）によって開発されたオープン規格のフレームワークであり、パブリック ネットワークを介して機密性の高い情報を送信する際にセキュリティを確保します。IPsec はネットワーク層で機能し、Cisco ルータなどの参加している IPsec 装置（ピア）間の IP パケットを保護および認証します。

IPsecでは、2つのピア間におけるセキュアなトンネルが提供されます。機密性の高いパケットを定義し、そのパケットをこれらのセキュアなトンネルを介して送信されるように定義できます。また、トンネルの特性を指定することによって、このように機密性の高いパケットを保護するために使用されるパラメータを定義できます。IPsec ピアによってこのように機密性の高いパケットが検出されたら、そのピアによって、適切かつセキュアなトンネルが設定され、そのパケットがトンネルからリモート ピアに送信されます。

IPsec の動作

IPsecの動作は5つの基本的な手順で構成されています。対象となるトラフィックの識別、IKEフェーズ1、IKEフェーズ2、トンネルまたはIPsecセッションの確立、そして最後にトンネルの切断です。

ステップ1：対象となるトラフィックの識別

VPNデバイスによって、検出対象のトラフィック、つまり機密性の高いパケットが認識されます。IPsec が機密性の高いパケットに適用されるか、パケットがバイパスされるか、または、パケットが廃棄されます。トラフィックのタイプに基づき、IPsecが適用されると、IKEフェーズ 1 が開始されます。

ステップ2：IKE フェーズ1

IKE セキュリティ ポリシーのネゴシエーションを行い、セキュアなチャネルを確立するために、VPN デバイス間で 3 回の交換が実行されます。

最初の交換の間、VPN デバイスによって、IKE 交換を保護するための IKE トランスフォーム セットのマッチングのネゴシエーションが行われ、その結果、使用する Internet Security Association and Key Management Protocol（ISAKMP）ポリシーが確立されます。ISAKMP ポリシーは、暗号化アルゴリズム、ハッシュ アルゴリズム、認証アルゴリズム、デフィーヘルマン（DH）グループ、およびライフタイム パラメータで構成されています。

8種類のデフォルトISAKMPポリシーがサポートされています。デフォルトISAKMPポリシーの詳細については、IKE フェーズ1 ISAKMP デフォルト ポリシーの確認（2785ページ）を参照してください。

2 番目の交換は Diffie-Hellman 交換です。共有秘密が確立されます。

3番目の交換では、ピアのアイデンティティが認証されます。ピアが認証されると、IKEフェーズ 2 が開始されます。

ステップ3：IKE フェーズ2

VPN デバイスによって、IPsec データの保護に使用される IPsec セキュリティ ポリシーのネゴシエーションが行われます。IPsec トランスフォーム セットがネゴシエートされます。

トランスフォーム セットは、ネットワーク トラフィックのセキュリティ ポリシーを制定するアルゴリズムおよびプロトコルの組み合わせです。デフォルト トランスフォーム セットの詳細については、デフォルトIPsecトランスフォームセットの確認（2789ページ）を参照してください。VPN トンネル確立の準備ができました。

ステップ 4：**Tunnel--IPsec の確立**

VPNデバイスによって、セキュリティ サービスがIPsecトラフィックに適用され、次に、IPsecデータが送信されます。セキュリティアソシエーション（SA）がピア間で交換されます。IPsecセッションがアクティブの間、ネゴシエートされたセキュリティ サービスがトンネル トラフィックに適用されます。

ステップ 5：**トンネルの終了**

IPsecSAライフタイムのタイムアウトが発生するか、パケットカウンタが超過すると、トンネルが切断されます。IPsec SA が削除されます。

IPsec Usability Enhancements の活用方法

IKE フェーズ 1 ISAKMP デフォルト ポリシーの確認

IKEネゴシエーションが開始されると、ピアによって共通ポリシーの検出が試行され、検出はリモートピア上で指定された最も高いプライオリティを持つポリシーから開始されます。一致が存在するまで、ピアによって、ポリシーセットのネゴシエーションが行われます。各ピアに共通のポリシーセットが複数存在する場合、最も低いプライオリティを持つ番号が使用されます。

IKE フェーズ 1、ISAKMP、ポリシーのプライオリティの範囲および動作によって定義された各種ポリシーの 3 つのグループがあります。

- デフォルト ISAKMP ポリシー。自動的にイネーブルにされます。
- ユーザーISAKMP設定ポリシー。**crypto isakmp policy** コマンドを使用して設定できます。
- Easy VPN ISAKMP ポリシー。Easy VPN 設定中に使用可能にされます。

このセクションでは、ISAKMP ポリシーの 3 つのグループに関して、互いの関係の中での動作、使用中のポリシーを適切な **show** コマンドを使用して特定する方法、および、デフォルト ISAKMP ポリシーをディセーブルにする方法について説明します。

デフォルト IKE フェーズ 1 ポリシー

8 種類のデフォルト IKE フェーズ 1、ISAKMP、各種ポリシーがサポートされています（下表を参照）。自動的にイネーブルにされます。**crypto isakmp policy** コマンドを使用して IKE ポリシーを手動で設定していない場合、または **no crypto isakmp default policy** コマンドを使用してデフォルト IKE ポリシーを無効にしていない場合、ピア IKE ネゴシエーション中はデフォルトの IKE ポリシーが使用されます。**show crypto isakmp policy** コマンドまたは **show crypto isakmp default policy** コマンドのいずれかを発行して、デフォルトの IKE ポリシーが使用されていることを確認できます。

（注） セキュリティに対する脅威は、脅威からの保護に役立つ暗号化技術と同様に絶え間なく変化しています。最新のシスコの暗号化に関する推奨事項については、『Next Generation Encryption（NGE）ホワイト ペーパー』を参照してください。

デフォルト IKE ポリシーによって、次のポリシー セット パラメータが定義されます。

- プライオリティ、65507 ～ 65514。65507 が最も高いプライオリティで、65514 が最も低いプライオリティ。
- 認証方式、Rivest、Shamir、および Adelman（RSA）または事前共有キー（PSK）。
- 暗号方式、Advanced Encryption Standard（AES）または Triple Data Encryption Standard（3DES）。
- ハッシュ関数、Secure Hash Algorithm（SHA-1）または Message-Digest algorithm 5（MD5）。
- DH グループ仕様 DH2 または DH5。
  - DH2 では、768 ビット DH グループが指定されます。
  - DH5 では、1536 ビット DH グループが指定されます。

（注） 3DES、MD5、および DH グループ 1、2、5 の使用は推奨しません。シスコの最新の暗号化に関する推奨事項については、『Next Generation Encryption（NGE）』ホワイト ペーパーを参照してください。IKE 設定の詳細については、『*Internet Key Exchange for IPsec VPNs Configuration Guide*』の「Configuring Internet Key Exchange for IPsec VPNs」の章を参照してください。

表 *257*：デフォルト *IKE* フェーズ *1*、*ISAKMP*、ポリシー

プライオリティ	認証	暗号化	ハッシュ	Diffie-Hellman
65507	RSA	AES	SHA	DH5
65508	PSK	AES	SHA	DH5
65509	RSA	AES	MD5	DH5
65510	PSK	AES	MD5	DH5
65511	RSA	3DES	SHA	DH2
65512	PSK	3DES	SHA	DH2
65513	RSA	3DES	MD5	DH2
65514	PSK	3DES	MD5	DH2

ユーザ設定 IKE ポリシー

crypto isakmp policy コマンドを使用して、IKE ポリシーを設定できます。ユーザ設定 IKE ポリシーは一意に識別され、1 ～ 10000 の範囲のプライオリティ番号が使用されて設定されます。1 が最も高いプライオリティで、10000 は最も低いプライオリティです。

1 ～ 10000 のプライオリティを持つ 1 つ以上の IKE ポリシーを設定した結果は次のとおりです。

- ピア IKE ネゴシエーション中にユーザ設定ポリシーが使用されます。
- ピア IKE ネゴシエーション中にデフォルト IKE ポリシーが使用されます。
- **show crypto isakmp policy** コマンドを発行することによって、ユーザー設定ポリシーを表示できます。

Easy VPN ISAKMP ポリシー

Easy VPN を設定した場合、使用中のデフォルト Easy VPN ISAKMP ポリシーは、65515 ～ 65535 の範囲のプライオリティ番号で一意に識別されます。65515 が最も高いプライオリティで、65535 は最も低いプライオリティです。

ユーザが Easy VPN を設定した結果は次のとおりです。

- ピア Easy VPN ISAKMP ネゴシエーション中に、デフォルト EzVPN ISAKMP ポリシーおよびデフォルト IKE ポリシーが使用されます。
- **show crypto isakmp policy** コマンドを発行することによって、Easy VPN ISAKMP ポリシーおよびデフォルト IKE ポリシーを表示できます。
- デフォルト ISAKMP ポリシーは、**no crypto isakmp default policy** コマンドを発行して無効にしない限り、**show crypto isakmp default policy** コマンドを発行すると表示されます。

手順の概要

1. **enable**
2. **show crypto isakmp default policy**
3. **configure terminal**
4. **no crypto isakmp default policy**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。

	コマンドまたはアクション	目的
ステップ 2	**show crypto isakmp default policy** 例： `Router# show crypto isakmp default policy`	（任意）1 ～ 10000 のプライオリティを持つポリシーが設定されていない場合、デフォルト ISAKMP ポリシーを表示します。
ステップ 3	**configure terminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 4	**no crypto isakmp default policy** 例： `Router(config)# no crypto isakmp default policy`	（任意）65507 ～ 65514 のプライオリティを持つデフォルト ISAKMP ポリシーをオフにします。

例

次に、**show crypto isakmp default policy** コマンドの出力例を示します。デフォルト ポリシーがディセーブルにされていないので、デフォルト ポリシーが表示されています。

```
Router# show crypto isakmp default policy

Default IKE policy
Default protection suite of priority 65507
        encryption algorithm:   AES - Advanced Encryption Standard (128 bit key.
        hash algorithm:         Secure Hash Standard
        authentication method:  Rivest-Shamir-Adleman Signature
        Diffie-Hellman group:   #5 (1536 bit)
        lifetime:               86400 seconds, no volume limit
Default protection suite of priority 65508
        encryption algorithm:   AES - Advanced Encryption Standard (128 bit key.
        hash algorithm:         Secure Hash Standard
        authentication method:  Pre-Shared Key
        Diffie-Hellman group:   #5 (1536 bit)
        lifetime:               86400 seconds, no volume limit
Default protection suite of priority 65509
        encryption algorithm:   AES - Advanced Encryption Standard (128 bit key.
        hash algorithm:         Message Digest 5
        authentication method:  Rivest-Shamir-Adleman Signature
        Diffie-Hellman group:   #5 (1536 bit)
        lifetime:               86400 seconds, no volume limit
Default protection suite of priority 65510
        encryption algorithm:   AES - Advanced Encryption Standard (128 bit key.
        hash algorithm:         Message Digest 5
        authentication method:  Pre-Shared Key
        Diffie-Hellman group:   #5 (1536 bit)
        lifetime:               86400 seconds, no volume limit
Default protection suite of priority 65511
        encryption algorithm:   Three key triple DES
        hash algorithm:         Secure Hash Standard
        authentication method:  Rivest-Shamir-Adleman Signature
```

```
        Diffie-Hellman group:   #2 (1024 bit)
        lifetime:               86400 seconds, no volume limit
Default protection suite of priority 65512
        encryption algorithm:   Three key triple DES
        hash algorithm:         Secure Hash Standard
        authentication method:  Pre-Shared Key
        Diffie-Hellman group:   #2 (1024 bit)
        lifetime:               86400 seconds, no volume limit
Default protection suite of priority 65513
        encryption algorithm:   Three key triple DES
        hash algorithm:         Message Digest 5
        authentication method:  Rivest-Shamir-Adleman Signature
        Diffie-Hellman group:   #2 (1024 bit)
        lifetime:               86400 seconds, no volume limit
Default protection suite of priority 65514
        encryption algorithm:   Three key triple DES
        hash algorithm:         Message Digest 5
        authentication method:  Pre-Shared Key
        Diffie-Hellman group:   #2 (1024 bit)
        lifetime:               86400 seconds, no volume limit
```

次に、デフォルト IKE ポリシーがディセーブルにされてからの、**show crypto isakmp default policy** コマンドの出力結果の例を示します。ここでは、結果は空白になっています。

```
Router# configure terminal
Router(config)# no crypto isakmp default policy
Router(config)# exit
Router# show crypto isakmp default policy
Router#
!There is no output since the default IKE policies have been disabled.
```

次に、デフォルトISAKMPポリシーが使用中の時はいつでも生成されるシステム ログ メッセージの例を示します。

```
%CRYPTO-6-IKMP_POLICY_DEFAULT: Using ISAKMP Default policies
```

デフォルト IPsec トランスフォーム セットの確認

トランスフォーム セットは、特定のセキュリティ プロトコルとアルゴリズムを組み合わせたものです。IPsecSAのネゴシエーション中に、ピアは、特定のトランスフォームセットを使用して特定のデータ フローを保護することに合意します。

IKEとのIPsecSAのネゴシエーション中に、ピアは両方のピア上で同じトランスフォームセットを検索します。同一のトランスフォーム セットが検出された場合、そのトランスフォームセットが選択され、両方のピアのIPsecSAの一部として、保護するトラフィックに適用されます。

デフォルト トランスフォーム セット

他のトランスフォームセットが設定されておらず、次の条件が満たされている場合、1つのデフォルトトランスフォームセットがすべてのクリプトマップまたはIPsecプロファイルによって使用されます。

- デフォルト トランスフォーム セットが **no crypto ipsec default transform-set** コマンドによって無効にされていない。
- 使用中の暗号化エンジンで、暗号化アルゴリズムがサポートされている。

下図に示すとおり、2 つのデフォルト トランスフォーム セットのそれぞれによって、Encapsulation Security Protocol（ESP）暗号化トランスフォーム タイプおよび ESP 認証トランスフォーム タイプが定義されます。

表 *258 :* デフォルト トランスフォーム セットおよびパラメータ

デフォルト トランスフォーム名	ESP 暗号化トランスフォームおよび説明	ESP 認証トランスフォームおよび説明
#$!default_transform_set_0	esp-3des （168 ビット 3DES またはトリプル DES 暗号化アルゴリズムを持つ EDP）	esp-sha-hmac
#$!default_transform_set_1	esp-aes （128 ビット AES 暗号化アルゴリズムを持つ ESP）	esp-sha-hmac （SHA-1、ハッシュ メッセージ認証コード [HMAC] バリアント認証アルゴリズムを持つ ESP）

手順の概要

1. **enable**
2. **show crypto ipsec default transform-set**
3. **configure terminal**
4. **no crypto ipsec default transform-set**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**show crypto ipsec default transform-set** 例： `Router# show crypto ipsec default transform-set`	（任意）IKE によって現在使用中のデフォルト IPsec トランスフォーム セットを表示します。
ステップ 3	**configure terminal** 例：	グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
	`Router# configure terminal`	
ステップ 4	**no crypto ipsec default transform-set** 例： `Router(config)# no crypto ipsec default transform-set`	（任意）デフォルト IPsec トランスフォーム セットを表示します。

例

```
The following example displays output from the show crypto ipsec default transform-set
 command when the default transform sets are enabled, the default setting:
Router# show crypto ipsec default transform-set
Transform set #$!default_transform_set_1: { esp-aes esp-sha-hmac  }
   will negotiate = { Transport,  },

Transform set #$!default_transform_set_0: { esp-3des esp-sha-hmac  }
   will negotiate = { Transport,  },
```

次に、**no crypto ipsec default transform-set** コマンドを使用してデフォルト トランスフォーム セットを無効にした場合の、**show crypto ipsec default transform-set** コマンドの出力例を示します。

```
Router(config)# no crypto ipsec default transform-set
Router(config)# exit
Router#
Router# show crypto ipsec default transform-set
! There is no output.
Router#
```

次に、IPsec SA がデフォルト トランスフォーム セットでネゴシエーションを行った時はいつでも生成されるシステム ログ メッセージ例を示します。

```
%CRYPTO-5-IPSEC_DEFAULT_TRANSFORM: Using Default IPsec transform-set
```

IPsec VPN 確認および IPsec VPN のトラブルシューティング

IKE フェーズ 1 または IKE フェーズ 2 を確認したいのか、または IPsec VPN のトラブルシューティングを行いたいのかによって、この項における次の任意の作業のいずれかを実行します。

IKE フェーズ 1 ISAKMP の確認

ISAKMP トンネルの統計情報を表示するには、次のオプション コマンドを使用します。

手順の概要

1. **show crypto mib isakmp flowmib failure [vrf** *vrf-name* **]**
2. **show crypto mib isakmp flowmib global [vrf** *vrf-name* **]**

3. **show crypto mib isakmp flowmib history [vrf** *vrf-name* **]**
4. **show crypto mib isakmp flowmib peer [index** *peer-mib-index* **] [vrf** *vrf-name* **]**
5. **show crypto mib isakmp flowmib tunnel [index** *tunnel-mib-index* **] [vrf** *vrf-name* **]**

手順の詳細

ステップ 1 show crypto mib isakmp flowmib failure [vrf *vrf-name*]

ISAKMP トンネルにエラーが発生した場合、このコマンドでイベント情報を表示できます。次に、このコマンドのサンプル出力を示します。

例：

```
Router# show crypto mib isakmp flowmib failure
 vrf Global
  Index:                       1
  Reason:                      peer lost
  Failure time since reset:    00:07:27
  Local type:                  ID_IPV4_ADDR
  Local value:                192.0.2.1
  Remote type:                 ID_IPV4_ADDR
  Remote Value:                192.0.2.2
  Local Address:               192.0.2.1
  Remote Address:              192.0.2.2
  Index:                       2
  Reason:                      peer lost
  Failure time since reset:    00:07:27
  Local type:                  ID_IPV4_ADDR
  Local value:                192.0.3.1
  Remote type:                 ID_IPV4_ADDR
  Remote Value:                192.0.3.2
  Local Address:               192.0.3.1
  Remote Address:              192.0.3.2
  Index:                       3
  Reason:                      peer lost
  Failure time since reset:    00:07:32
  Local type:                  ID_IPV4_ADDR
  Remote type:                 ID_IPV4_ADDR
  Remote Value:                192.0.2.2
  Local Address:               192.0.2.1
  Remote Address:              192.0.2.2
```

ステップ 2 show crypto mib isakmp flowmib global [vrf *vrf-name*]

このコマンドを発行することによって、グローバル ISAKMP トンネル統計情報が表示されます。次に、このコマンドのサンプル出力を示します。

例：

```
Router# show crypto mib isakmp flowmib global
vrf Global
  Active Tunnels:                          3
  Previous Tunnels:                        0
  In octets:                               2856
  Out octets:                              3396
  In packets:                              16
  Out packets:                             19
  In packets drop:                         0
```

```
  Out packets drop:                       0
  In notifys:                             4
  Out notifys:                            7
  In P2 exchg:                            3
  Out P2 exchg:                           6
  In P2 exchg invalids:                   0
  Out P2 exchg invalids:                  0
  In P2 exchg rejects:                    0
  Out P2 exchg rejects:                   0
  In IPSEC delete:                        0
  Out IPSEC delete:                       0
  SAs locally initiated:                  3
  SAs locally initiated failed:           0
  SAs remotely initiated failed:          0
  System capacity failures:               0
  Authentication failures:                0
  Decrypt failures:                       0
  Hash failures:                          0
  Invalid SPI:                            0
```

ステップ 3 **show crypto mib isakmp flowmib history [vrf** *vrf-name* **]**

アクティブにならない ISAKMP トンネルの情報については、このコマンドによって、トンネルが終了した原因を含むイベント情報を表示できます。次に、このコマンドのサンプル出力を示します。

例：

```
Router# show crypto mib isakmp flowmib history
vrf Global
  Reason:                             peer lost
  Index:                              2
  Local type:                         ID_IPV4_ADDR
  Local address:                      192.0.2.1
  Remote type:                        ID_IPV4_ADDR
  Remote address:                     192.0.2.2
  Negotiation mode:                   Main Mode
  Diffie Hellman Grp:                 2
  Encryption algo:                    des
  Hash algo:                          sha
  Auth method:                        psk
  Lifetime:                           86400
  Active time:                        00:06:30
  Policy priority:                    1
  Keepalive enabled:                  Yes
  In octets:                          3024
  In packets:                         22
  In drops:                           0
  In notifys:                         18
  In P2 exchanges:                    1
  In P2 exchg invalids:               0
  In P2 exchg rejected:                 0
  In P2 SA delete reqs:                 0
  Out octets:                           4188
  Out packets:                          33
  Out drops:                            0
  Out notifys:                          28
  Out P2 exchgs:                        2
  Out P2 exchg invalids:                0
  Out P2 exchg rejects:                 0
  Out P2 Sa delete requests:            0
  Reason:                               peer lost
  Index:                                3
  Local type:                           ID_IPV4_ADDR
```

```
  Local address:                        192.0.3.1
  Remote type:                          ID_IPV4_ADDR
  Remote address:                       192.0.3.2
  Negotiation mode:                     Main Mode
  Diffie Hellman Grp:                   2
  Encryption algo:                      des
  Hash algo:                            sha
  Auth method:                          psk
  Lifetime:                             86400
  Active time:                          00:06:25
  Policy priority:                      1
  Keepalive enabled:                    Yes
  In octets:                            3140
  In packets:                           23
  In drops:                             0
  In notifys:                           19
  In P2 exchanges:                      1
  In P2 exchg invalids:                 0
  In P2 exchg rejected:                 0
  In P2 SA delete reqs:                 0
  Out octets:                           4304
  Out packets:                          34
  Out drops:                            0
  Out notifys:                          29
  Out P2 exchgs:                        2
  Out P2 exchg invalids:                0
  Out P2 exchg rejects:                 0
  Out P2 Sa delete requests:            0
```

ステップ 4 **show crypto mib isakmp flowmib peer [index** *peer-mib-index* **] [vrf** *vrf-name* **]**

アクティブな ISAKMP ピアアソシエーションについては、このコマンドによって、インデックス、接続タイプ、および IP アドレスを含む情報を表示できます。次に、このコマンドのサンプル出力を示します。

例：

```
Router# show crypto mib isakmp flowmib peer
vrf Global
  Index:              1
  Local type:         ID_IPV4_ADDR
  Local address:      192.0.2.1
  Remote type:        ID_IPV4_ADDR
  Remote address:     192.0.2.2
  Index:              2
  Local type:         ID_IPV4_ADDR
  Local address:      192.0.3.1
  Remote type:        ID_IPV4_ADDR
  Remote address:     192.0.3.1
  Index:              3
  Local type:         ID_IPV4_ADDR
  Local address:      192.0.4.1
  Remote type:        ID_IPV4_ADDR
  Remote address:     192.0.4.1
```

ステップ 5 **show crypto mib isakmp flowmib tunnel [index** *tunnel-mib-index* **] [vrf** *vrf-name* **]**

アクティブな ISAKMP トンネルについては、このコマンドによって、トンネルの統計情報を表示できます。次に、このコマンドのサンプル出力を示します。

例：

```
Router# show crypto mib isakmp flowmib tunnel
```

```
vrf Global
  Index:                        1
  Local type:                   ID_IPV4_ADDR
  Local address:                192.0.2.1
  Remote type:                  ID_IPV4_ADDR
  Remote address:               192.0.2.2
  Negotiation mode:             Main Mode
  Diffie Hellman Grp:           2
  Encryption algo:              des
  Hash algo:                    sha
  Auth method:                  psk
  Lifetime:                     86400
  Active time:                  00:03:08
  Policy priority:              1
  Keepalive enabled:            Yes
  In octets:                    2148
  In packets:                   15
  In drops:                     0
  In notifys:                   11
  In P2 exchanges:              1
  In P2 exchg invalids:         0
  In P2 exchg rejected:         0
  In P2 SA delete reqs:         0
  Out octets:                   2328
  Out packets:                  16
  Out drops:                    0
  Out notifys:                  12
  Out P2 exchgs:                2
  Out P2 exchg invalids:        0
  Out P2 exchg rejects:         0
  Out P2 Sa delete requests:    0
```

IKE フェーズ 2 の確認

IPsec フェーズ2 トンネルの統計情報を表示するには、次のオプション コマンドを使用します。

手順の概要

1. **show crypto mib ipsec flowmib endpoint [vrf** *vrf-name* **]**
2. **show crypto mib ipsec flowmib failure [vrf** *vrf-name* **]**
3. **show crypto mib ipsec flowmib global [vrf** *vrf-name* **]**
4. **show crypto mib ipsec flowmib history [vrf** *vrf-name* **]**
5. **show crypto mib ipsec flowmib spi [vrf** *vrf-name* **]**
6. **show crypto mib ipsec flowmib tunnel** [**index** *tunnel-mib-index*] **[vrf** *vrf-name* **]**

手順の詳細

ステップ 1 **show crypto mib ipsec flowmib endpoint [vrf** *vrf-name* **]**

このコマンドを発行することによって、IPsec フェーズ 2 トンネルに関連付けられた、各アクティブ エンドポイント、ローカルまたはリモート デバイスの情報が表示されます。次に、このコマンドのサンプル出力を示します。

例：

```
Router#  show crypto mib ipsec flowmib endpoint
vrf Global
  Index:               1
  Local type:          Single IP address
  Local address:       192.1.2.1
  Protocol:            0
  Local port:          0
  Remote type:         Single IP address
  Remote address:      192.1.2.2
  Remote port:         0
  Index:               2
  Local type:          Subnet
  Local address:       192.1.3.0 255.255.255.0
  Protocol:            0
  Local port:          0
  Remote type:         Subnet
  Remote address:      192.1.3.0 255.255.255.0
  Remote port:         0
```

ステップ 2 **show crypto mib ipsec flowmib failure [vrf** *vrf-name* **]**

ISAKMP トンネルにエラーが発生した場合、このコマンドでイベント情報を表示できます。次に、このコマンドのサンプル出力を示します。

例：

```
Router# show crypto mib ipsec flowmib failure
vrf Global
  Index:                       1
  Reason:                      Operation request
  Failure time since reset:    00:25:18
  Src address:                 192.1.2.1
  Destination address:         192.1.2.2
  SPI:                         0
```

ステップ 3 **show crypto mib ipsec flowmib global [vrf** *vrf-name* **]**

このコマンドを発行することによって、グローバル IKE フェーズ 2 トンネルの統計情報が表示されます。次に、このコマンドのサンプル出力を示します。

例：

```
Router# show crypto mib ipsec flowmib global
 vrf Global
  Active Tunnels:                   2
  Previous Tunnels:                 0
  In octets:                        800
  Out octets:                       1408
  In packets:                       8
  Out packets:                      8
  Uncompressed encrypted bytes:    1408
  In packets drops:                 0
  Out packets drops:                2
  In replay drops:                  0
  In authentications:               8
  Out authentications:              8
  In decrypts:                      8
  Out encrypts:                     8
  Compressed bytes:                 0
  Uncompressed bytes:               0
  In uncompressed bytes:            0
```

```
  Out uncompressed bytes:             0
  In decrypt failures:                0
  Out encrypt failures:               0
  No SA failures:                     0
! Number of SA Failures.
  Protocol use failures:              0
  System capacity failures:           0
  In authentication failures:         0
  Out authentication failures:        0
```

ステップ 4 **show crypto mib ipsec flowmib history [vrf** *vrf-name* **]**

アクティブにならない IKE フェーズ 2 トンネルの情報については、このコマンドによって、トンネルが終了した原因を含むイベント情報を表示できます。次に、このコマンドのサンプル出力を示します。

例：

```
Router# show crypto mib ipsec flowmib history
vrf Global
  Reason:                       Operation request
  Index:                        1
  Local address:                192.1.2.1
  Remote address:               192.1.2.2
  IPSEC keying:                 IKE
  Encapsulation mode:           1
  Lifetime (KB):                4608000
  Lifetime (Sec):               3600
  Active time:                  00:24:32
  Lifetime threshold (KB):      423559168
  Lifetime threshold (Sec):     3590000
  Total number of refreshes:    0
  Expired SA instances:         4
  Current SA instances:         4
  In SA DH group:               14
  In sa encrypt algorithm       aes
  In SA auth algorithm:         rsig
  In SA ESP auth algo:          ESP_HMAC_SHA
  In SA uncompress algorithm:   None
  Out SA DH group:              14
  Out SA encryption algorithm:  aes
  Out SA auth algorithm:        ESP_HMAC_SHA
  Out SA ESP auth algorithm:    ESP_HMAC_SHA
  Out SA uncompress algorithm:  None
  In octets:                    400
  Decompressed octets:          400
  In packets:                   4
  In drops:                         0
  In replay drops:                  0
  In authentications:               4
  In authentication failures:       0
  In decrypts:                      4
  In decrypt failures:              0
  Out octets:                       704
  Out uncompressed octets:          704
  Out packets:                      4
  Out drops:                        1
  Out authentications:              4
  Out authentication failures:      0
  Out encryptions:                  4
  Out encryption failures:          0
  Compressed octets:                0
  Decompressed octets:              0
  Out uncompressed octets:          704
```

ステップ 5 **show crypto mib ipsec flowmib spi [vrf** *vrf-name* **]**

security protection index（SPI）テーブルには、アクティブおよび期限切れの各セキュリティ IKE フェーズ 2 アソシエーションのエントリが格納されます。次に、このコマンドのサンプル出力を示します。SPI テーブルが表示されています。

例：

```
Router# show crypto mib ipsec flowmib spi
vrf Global
  Tunnel Index:          1
  SPI Index:            1
  SPI Value:            0xCC57D053
  SPI Direction:        In
  SPI Protocol:         AH
  SPI Status:           Active
  SPI Index:            2
  SPI Value:            0x68612DF
  SPI Direction:        Out
  SPI Protocol:         AH
  SPI Status:           Active
  SPI Index:            3
  SPI Value:            0x56947526
  SPI Direction:        In
  SPI Protocol:         ESP
  SPI Status:           Active
  SPI Index:            4
  SPI Value:            0x8D7C2204
  SPI Direction:        Out
  SPI Protocol:         ESP
  SPI Status:           Active
```

ステップ 6 **show crypto mib ipsec flowmib tunnel** [**index** *tunnel-mib-index*] **[vrf** *vrf-name* **]**

アクティブな IKE フェーズ 2 トンネルについては、このコマンドによって、トンネルの統計情報を表示できます。次に、このコマンドのサンプル出力を示します。

例：

```
Router# show crypto mib ipsec flowmib tunnel
vrf Global
  Index:                            1
  Local address:                    192.0.2.1
  Remote address:                   192.0.2.2
  IPSEC keying:                     IKE
  Encapsulation mode:               1
  Lifetime (KB):                    4608000
  Lifetime (Sec):                   3600
  Active time:                      00:05:46
  Lifetime threshold (KB):          64
  Lifetime threshold (Sec):         10
  Total number of refreshes:        0
  Expired SA instances:             0
  Current SA instances:             4
  In SA DH group:                   14
  In sa encrypt algorithm:          aes
  In SA auth algorithm:             rsig
  In SA ESP auth algo:              ESP_HMAC_SHA
  In SA uncompress algorithm:       None
  Out SA DH group:                  14
  Out SA encryption algorithm:      aes
```

```
Out SA auth algorithm:              ESP_HMAC_SHA
Out SA ESP auth algorithm:          ESP_HMAC_SHA
Out SA uncompress algorithm:        None
In octets:                             400
Decompressed octets:                   400
In packets:                            4
In drops:                              0
In replay drops:                       0
In authentications:                    4
In authentication failures:            0
In decrypts:                           4
In decrypt failures:                   0
Out octets:                            704
Out uncompressed octets:               704
Out packets:                           4
Out drops:                             1
Out authentications:                   4
Out authentication failures:           0
Out encryptions:                       4
Out encryption failures:               0
Compressed octets:                     0
Decompressed octets:                   0
Out uncompressed octets:               704
```

IPsec VPN のトラブルシューティング

問題のトラブルシューティングを行う場合、**show tech-support ipsec** コマンドを使用すれば、IPsec 関連情報の収集が簡単にできます。

手順の概要

1. **show tech-support ipsec**

手順の詳細

show tech-support ipsec

show tech-support ipsec コマンドには、次の 3 つのバリエーションがあります。

- **show tech-support ipsec**
- **show tech-support ipsec peer** *ipv4address*
- **show tech-support ipsec vrf** *vrf-name*

各バリエーションについて次に示す個々の **show** コマンドに関する **show tech-support ipsec** コマンドからの出力のサンプル表示については、以下のセクションを参照してください。

show tech-support ipsec コマンドの出力

キーワードを何も指定しないで **show tech-support ipsec** コマンドを入力すると、コマンドの出力には、次の **show** コマンドが出力順に表示されます。

- **show version**

- **show running-config**
- **show crypto isakmp sa count**
- **show crypto ipsec sa count**
- **show crypto session summary**
- **show crypto session detail**
- **show crypto isakmp sa detail**
- **show crypto ipsec sa detail**
- **show crypto isakmp peers**
- **show crypto ruleset detail**
- **show processes memory | include Crypto IKMP**
- **show processes cpu | include Crypto IKMP**
- **show crypto eli**
- **show crypto engine accelerator statistic**

show tech-support ipsec peer コマンドの出力

peer キーワードと *ipv4address* 引数を指定して **show tech-support ipsec** コマンドを入力すると、出力に次の **show** コマンドが、指定したピアの出力順に表示されます。

- **show version**
- **show running-config**
- **show crypto session remote** *ipv4address* **detail**
- **show crypto isakmp sa peer** *ipv4address* **detail**
- **show crypto ipsec sa peer** *ipv4address* **detail**
- **show crypto isakmp peers** *ipv4address*
- **show crypto ruleset detail**
- **show processes memory | include Crypto IKMP**
- **show processes cpu | include Crypto IKMP**
- **show crypto eli**
- **show crypto engine accelerator statistic**

show tech-support ipsec vrf コマンドの出力

vrf キーワードと *vrf-name* 引数を指定して **show tech-support ipsec** コマンドを入力すると、出力に次の **show** コマンドが、指定した Virtual Routing and Forwarding（VRF）の出力順に表示されます。

- **show version**
- **show running-config**

- **show crypto isakmp sa count vrf** *vrf-name*
- **show crypto ipsec sa count vrf** *vrf-name*
- **show crypto session ivrf** *ivrf-name* **detail**
- **show crypto session fvrf** *fvrf-name* **detail**
- **show crypto isakmp sa vrf** *vrf-name* **detail**
- **show crypto ipsec sa vrf** *vrf-name* **detail**
- **show crypto ruleset detail**
- **show processes memory | include Crypto IKMP**
- **show processes cpu | include Crypto IKMP**
- **show crypto eli**
- **show crypto engine accelerator statistic**

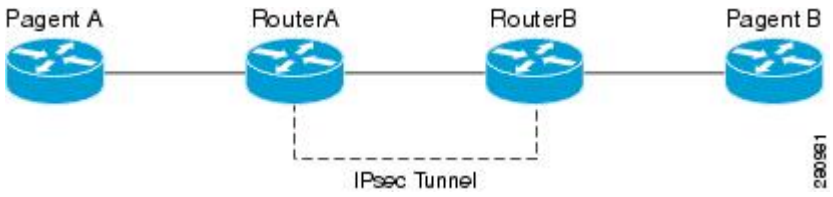
例：

IPsec Usability Enhancements の設定例

IKE デフォルト ポリシーの例

次に、クリプト マップが RouterA および RouterB 上で設定されており、デフォルト IKE ポリシーが使用中になっている例を示します。トラフィックは Pagent A から Pagent B にルーティングされます。Peer A および Peer B のシステム ログをチェックすると、デフォルトの IKE ポリシーが両方のピアで使用中であることを確認できます（下図を参照）。

図 *96*：サイトツーサイト トポロジーの例




```
! Configuring RouterA.
RouterA(config)# crypto isakmp key identity address 209.165.200.226
RouterA(config)# crypto map testmap 10 ipsec-isakmp
% NOTE: This new crypto map will remain disabled until a peer
 and a valid access list have been configured.
RouterA(config-crypto-map)# set peer 209.165.200.226
RouterA(config-crypto-map)# match address 101
RouterA(config-crypto-map)# exit
```

```
RouterA(config)# ip route 209.165.200.225 255.255.255.224 209.165.200.226
RouterA(config)# access-list 101 permit ip host 209.165.200.227 host 209.165.200.225
RouterA(config)# end
RouterA(config)# interface FastEthernet1/2
RouterA(config-if)# crypto map testmap
RouterA(config-if)# end
RouterA(config)# crypto ipsec transform test_transf esp-aes esp-sha-hmac
RouterA(cfg-crypto-trans)# mode tunnel
RouterA(cfg-crypto-trans)# end
RouterA(config)# crypto map testmap 10
RouterA(config-crypto-map)# set transform-set test_transf
RouterA(config-crypto-map)# end
! Configuring RouterB.
RouterB(config)# crypto isakmp key identity address 209.165.200.228
RouterB(config)# crypto dynamic-map dyn_testmap 10
RouterB(config-crypto-map)# crypto map testmap 10 ipsec-isakmp dynamic dyn_testmap
RouterB(config)# ip route 209.165.200.227 255.255.255.224 209.165.200.228
RouterB(config)# end
RouterB(config)# interface GigabitEthernet0/1
RouterB(config-if)# crypto map testmap
RouterB(config-if)# end
RouterB(config)# crypto ipsec transform test_transf esp-aes esp-sha-hmac
RouterB(cfg-crypto-trans)# mode tunnel
RouterB(cfg-crypto-trans)# end
RouterB(config)# crypto dynamic-map dyn_testmap 10
RouterB(config-crypto-map)# set transform-set test_transf
RouterB(config-crypto-map)# end
! Routing traffic from PagentA to PagentB.
PagentA(config)# ip route 209.165.200.225 255.255.255.224 209.165.200.229
PagentA(config)# end
! Routing traffic from PagentB to PagentA.
PagentB(config)# ip route 209.165.200.227 255.255.255.224 209.165.200.230
PagentB(config)# end
! Checking the system log on RouterA confirms that the default IKE policies are in use.
RouterA# show log | include %CRYPTO-6-IKMP_POLICY_DEFAULT*
Jun  5 09:17:59.251 PDT: %CRYPTO-6-IKMP_POLICY_DEFAULT: Using ISAKMP Default policies
! Checking the system log on RouterB confirms that the default IKE policies are in use.
RouterB# show log | include %CRYPTO-6-IKMP_POLICY_DEFAULT*
Jun  5 09:17:59.979 PDT: %CRYPTO-6-IKMP_POLICY_DEFAULT: Using ISAKMP Default policies
```

デフォルト トランスフォーム セットの例

次に、スタティック クリプト マップが RouterA 上で設定され、ダイナミック クリプト マップが RouterB 上で設定されている例を示します。トラフィックは Pagent A から Pagent B にルーティングされます。IPsec SA はデフォルト トランスフォーム セットとネゴシエーションを行い、トラフィックは暗号化されます。両方のピアで **show crypto map** コマンドを実行すると、デフォルト トランスフォーム セットが使用中であることを確認できます。

```
! Configuring RouterA.
RouterA(config)# crypto isakmp key identify address 209.165.200.225
RouterA(config)# crypto map testmap 10 ipsec-isakmp
% NOTE: This new crypto map will remain disabled until a peer
 and a valid access list have been configured.
RouterA(config-crypto-map)# set peer 209.165.200.225
RouterA(config-crypto-map)# match address 101
RouterA(config-crypto-map)# exit
RouterA(config)# ip route 209.165.200.226 255.255.255.255 209.165.200.225
RouterA(config)# access-list 101 permit ip host 209.165.200.227 host 209.165.200.226
```

```
RouterA(config)# end
RouterA(config)# interface FastEthernet1/2
RouterA(config-if)# crypto map testmap
RouterA(config-if)# end
RouterA(config)# crypto isakmp policy 10
RouterA(config-isakmp)# encryption aes
RouterA(config-isakmp)# authentication pre-share
RouterA(config-isakmp)# hash sha
RouterA(config-isakmp)# group 5
RouterA(config-isakmp)# end
! Configuring RouterB.
RouterB(config)# crypto isakmp key identity address 209.165.200.229
RouterB(config)# crypto dynamic-map dyn_testmap 10
RouterB(config-crypto-map)# crypto map testmap 10 ipsec-isakmp dynamic dyn_testmap
RouterB(config)# ip route 209.165.200.227 255.255.255.255 209.165.200.229
RouterB(config)# end
RouterB(config)# interface GigabitEthernet0/1
RouterB(config-if)# crypto map testmap
RouterB(config-if)# end
RouterB(config)# crypto isakmp policy 10
RouterB(config-isakmp)# encryption aes
RouterB(config-isakmp)# authentication pre-share
RouterB(config-isakmp)# hash sha
RouterB(config-isakmp)# group 5
RouterB(config-isakmp)# end
! The SA is using the default transform set and traffic is encrypted on RouterA.
RouterA# show crypto isakmp sa detail | include 209.165.200.229.*209.165.200.225.*ACTIVE
13007  209.165.200.229     209.165.200.225     ACTIVE aes  sha  psk  5  23:59:56
13006  209.165.200.229     209.165.200.225     ACTIVE aes  sha  psk  5  0
13005  209.165.200.229     209.165.200.225     ACTIVE aes  sha  psk  5  0
! The SA is using the default transform set and traffic is encrypted on RouterB.
RouterB# show crypto isakmp sa detail | include 209.165.200.225.*209.165.200.229.*ACTIVE
7007  209.165.200.225      209.165.200.229      ACTIVE aes  sha  psk  5  23:59:55
7006  209.165.200.225      209.165.200.229      ACTIVE aes  sha  psk  5  0
7005  209.165.200.225      209.165.200.229      ACTIVE aes  sha  psk  5  0
! Verifying that the default transform sets are in use on RouterA.
RouterA# show crypto map
Crypto Map "testmap" 10 ipsec-isakmp
 Peer = 209.165.200.225
 Extended IP access list 101
     access-list 101 permit ip host 209.165.200.227 host 209.165.200.226
 Current peer: 209.165.200.225
 Security association lifetime: 4608000 kilobytes/3600 seconds
 PFS (Y/N): N
 Transform sets={
  #$!default_transform_set_1:  { esp-aes esp-sha-hmac  } ,
  #$!default_transform_set_0:  { esp-3des esp-sha-hmac  } ,
 }
 Interfaces using crypto map testmap:
  FastEthernet1/2
! Verifying that the default transform sets are in use on RouterB.
RouterB# show crypto map
Crypto Map "testmap" 10 ipsec-isakmp
 Dynamic map template tag: dyn_testmap
Crypto Map "testmap" 65536 ipsec-isakmp
 Peer = 209.165.200.229
 Extended IP access list
     access-list permit ip host 209.165.200.226 host 209.165.200.227
     dynamic (created from dynamic map dyn_testmap/10)
 Current peer: 209.165.200.229
 Security association lifetime: 4608000 kilobytes/3600 seconds
 PFS (Y/N): N
 Transform sets={
```

```
 #$!default_transform_set_1:  { esp-aes esp-sha-hmac  } ,
}
Interfaces using crypto map testmap:
 GigabitEthernet0/1
```

その他の参考資料

次の項では、IPsec Usability Enhancement 機能の関連資料を示します。

関連資料

関連項目	マニュアル タイトル
IKE 設定	『*Cisco IOS XE Security Configuration Guide: Secure Connectivity*』の「Configuring Internet Key Exchange for IPsec VPNs」モジュール
IPsec の設定	『*Cisco IOS XE Security Configuration Guide: Secure Connectivity*』の「Configuring Security for VPNs with IPsec」モジュール
Easy VPN サーバ	『*Cisco IOS XE Security Configuration Guide: Secure Connectivity*』の「Easy VPN Server」モジュール
Cisco IOS XE セキュリティ コマンド	『*Cisco IOS Security Command Reference*』

標準

標準	タイトル
この機能でサポートされる新規の標準または変更された標準はありません。また、既存の標準のサポートは変更されていません。	--

MIB

MIB	MIB のリンク
この機能によってサポートされる新しい MIB または変更された MIB はありません。またこの機能による既存MIBのサポートに変更はありません。	選択したプラットフォーム、Cisco IOS XE リリース、およびフィーチャ セットの MIB を検索してダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

RFC

RFC	タイトル
この機能によりサポートされた新規 RFC または改訂 RFC はありません。またこの機能による既存 RFC のサポートに変更はありません。	--

シスコのテクニカル サポート

説明	リンク
シスコのサポート Web サイトでは、シスコの製品やテクノロジーに関するトラブルシューティングにお役立ていただけるように、マニュアルやツールをはじめとする豊富なオンライン リソースを提供しています。 お使いの製品のセキュリティ情報や技術情報を入手するために、Cisco Notification Service（Field Notice からアクセス）、Cisco Technical Services Newsletter、Really Simple Syndication（RSS）フィードなどの各種サービスに加入できます。 シスコのサポート Web サイトのツールにアクセスする際は、Cisco.com のユーザ ID およびパスワードが必要です。	http://www.cisco.com/en/US/support/index.html

IPsec Usability Enhancements の機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *259 : IPsec Usability Enhancements* の機能情報

機能名	リリース	機能情報
IPsec Usability Enhancements	Cisco IOS XE Release 2.4	この機能では、IKE および IPsec のインテリジェントなデフォルト、および、MIB 統計情報にアクセスするためおよびトラブルシューティングを支援するための各種**show**コマンドが導入されています。 次のコマンドが導入または変更されました。**crypto ipsec default transform-set**、**crypto isakmp default policy**、**crypto isakmp policy**、**show crypto ipsec default transform-set**、**show crypto ipsec transform-set**、**show crypto isakmp default policy**、**show crypto isakmp policy**、**show crypto map (IPsec)**、**show crypto mib ipsec flowmib endpoint**、**show crypto mib ipsec flowmib failure**、**show crypto mib ipsec flowmib global**、**show crypto mib ipsec flowmib history**、**show crypto mib ipsec flowmib spi**、**show crypto mib ipsec flowmib tunnel**、**show crypto mib isakmp flowmib failure**、**show crypto mib isakmp flowmib global**、**show crypto mib isakmp flowmib history**、**show crypto mib isakmp flowmib peer**、**show crypto mib isakmp flowmib tunnel**、**show tech-support ipsec**。

用語集

ピア：ここでのピアとは、IPsec に参加するルータまたはその他の装置です。

SA：セキュリティ アソシエーション。2 つ以上のエンティティが、特定のデータ フローにおいて安全に通信するために、特定のセキュリティ プロトコル（AH または ESP）と関連してセキュリティ サービスを使用する方法を記述します。トラフィックを保護するために、トランスフォームと共有秘密キーが使用されます。

トランスフォーム：データ認証、データ機密性、およびデータ圧縮を実現するためにデータ フローで実行される処理のリスト。たとえば、トランスフォームには、HMAC MD5 認証アルゴリズムを使用する ESP プロトコル、56 ビット DES 暗号規格アルゴリズムを使用する AH プロトコルおよび HMAC-SHA 認証アルゴリズムを使用する ESP プロトコルなどがあります。

トンネル：ここで使用するトンネルとは、2 つのピア間（2 台のルータなど）の安全な通信パスです。トンネル モードで IPsec を使用することではありません。

第 XIX 部

VPN のアベイラビリティ

第 192 章

逆ルート注入

逆ルート注入（RRI）とは、リモート トンネル エンドポイントによって保護されているネットワークおよびホストのルーティング プロセスに、スタティック ルートを自動的に組み込む機能です。保護されているこれらのホストおよびネットワークは、リモート プロキシ アイデンティティと呼ばれます。

各ルートは、リモート プロキシ ネットワークとマスクを基にして作成され、リモート トンネル エンドポイントがこのネットワークへのネクスト ホップとなります。ネクスト ホップとしてバーチャル プライベート ネットワーク（VPN）のリモート ルータを使い、暗号化プロセスによってトラフィックを強制的に暗号化します。

逆ルート注入の前提条件

- RRI で生成されたスタティック ルートの伝播にダイナミック ルーティング プロトコルを使用する場合は、IP ルーティングをイネーブルにし、スタティック ルートを再配布する必要があります。

逆ルート注入の制約事項

- スタティック クリプト マップでは、適用済みのクリプト マップに RRI が設定されている場合、必ずルートが存在します。スタティックマップに常に表示されるルートのデフォルト動作は、**static** キーワードが **reverse-route** コマンドに追加されない限り適用されません。

- RIB のプレフィックスに、手動で設定されたタグ付きのスタティックルートと、RRI を介して挿入されたタグのないルートがあるとします。このようなシナリオでは、ルート選択に一貫性がなくなり、手動設定ルートまたはRRIルートのいずれかが選択される可能性があります。

  そのような一貫性のなさを回避するには、次の作業のいずれかを行う必要があります。

  - ルータのすべてのピア VPN ネットワークへのスタティックルートを手動で設定する場合は、暗号マップからリバースルート設定を削除することでRRIを無効にします。
  - RRI を介して挿入されたルートの暗号マップに同一のタグを設定します。

逆ルート注入に関する情報

逆ルート注入

RRI とは、リモート トンネル エンドポイントによって保護されているネットワークとホストのルーティング プロセスに、スタティック ルートを自動的に組み込む機能です。保護されているこれらのホストおよびネットワークは、リモート プロキシ アイデンティティと呼ばれます。

各ルートは、リモート プロキシ ネットワークとマスクを基にして作成され、リモート トンネル エンドポイントがこのネットワークへのネクスト ホップとなります。リモート VPN ルータをネクストホップとして使用することによって、トラフィックは強制的に暗号プロセスを通して暗号化されます。

VPN ルータでスタティック ルートが作成されたあと、この情報がアップストリーム デバイスに伝播されます。これにより、アップストリーム デバイスでは、IPsec 状態フローを維持するためのリターン トラフィックの送信先として適切なVPNルータを特定できるようになります。適切な VPN ルータを判定することができれば、サイトで複数の VPN ルータを使用してロードバランシングやフェールオーバーを実行する場合や、デフォルト ルートでリモート VPN デバイスにアクセスできない場合に特に役立ちます。ルートは、グローバル ルーティング テーブルまたは適切な Virtual Routing and Forwarding（VRF）テーブルに作成されます。

スタティック クリプト マップ テンプレートであってもダイナミック クリプト マップ テンプレートであっても、RRI はクリプトマップごとに適用されます。この2つのタイプのマップのデフォルト動作は次のとおりです。

- ダイナミック クリプト マップでは、ルートは、リモート プロキシの IPsec セキュリティ アソシエーション（SA）が正常に確立されるとすぐに作成されます。リモート プロキシへのネクスト ホップは、リモートVPNルータ経由となります。リモートVPNルータのアドレスは、ダイナミック クリプト マップ テンプレートの作成中に学習および適用されます。ルートは、SA が削除されたあとに削除されます。スタティック クリプト マップの IPsec 送信元プロキシで作成されたルートは、スタティック マップのデフォルト動作であり、クリプト ACL（次の項目を参照）に基づいたルートの作成よりも優先されます。

- スタティック クリプト マップでは、クリプト アクセス リストに定義されている宛先情報を基にルートが作成されます。ネクスト ホップは、クリプト マップにアタッチされている最初の set peer 文から取得します。RRI、ピア、またはアクセス リストがクリプト マップから削除されると、必ずルートも削除されます。この動作は、以降の項で説明するように、RRI の拡張機能を追加することで変わります。

RRI の設定方法

スタティック クリプト マップを使用した RRI の設定

手順の概要

1. **enable**
2. **configure terminal**
3. **crypto map {** *map-name* **} {** *seq-name***} ipsec-isakmp**
4. **reverse-route** [**static** | **tag** *tag-id* [**static**] | **remote-peer**[**static**] | **remote-peer** *ip-address* [**static**]]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**crypto map {** *map-name* **} {** *seq-name***} ipsec-isakmp** 例： `Router (config)# crypto map mymap 1 ipsec-isakmp`	クリプト マップ エントリを作成または変更し、クリプト マップ コンフィギュレーション モードを開始します。
ステップ 4	**reverse-route** [**static** | **tag** *tag-id* [**static**] | **remote-peer**[**static**] | **remote-peer** *ip-address* [**static**]] 例： `Router (config-crypto-map)# reverse-route remote peer 10.1.1.1`	クリプト マップ エントリのソース プロキシ情報を作成します。

ダイナミック マップ テンプレートでの RRI の設定

手順の概要

1. **enable**
2. **configure terminal**
3. **crypto dynamic-map** *dynamic-map-name dynamic-seq-name*
4. **reverse-route** [**static** | **tag** *tag-id* [**static**] | **remote-peer**[**static**] | **remote-peer** *ip-address* [**static**]]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**crypto dynamic-map** *dynamic-map-name dynamic-seq-name* 例： `Router (config)# crypto dynamic-map mymap 1`	ダイナミック クリプト マップ エントリを作成し、クリプト マップ コンフィギュレーション コマンド モードを開始します。
ステップ 4	**reverse-route** [**static** | **tag** *tag-id* [**static**] | **remote-peer**[**static**] | **remote-peer** *ip-address* [**static**]] 例： `Router (config-crypto-map)# reverse-route remote peer 10.1.1.1`	クリプト マップ エントリのソース プロキシ情報を作成します。

RRI の設定例

Crypto ACL が存在する場合の RRI の設定例

次に、すべてのリモート VPN ゲートウェイを 192.168.0.3 でルータに接続している例を示します。RRI がスタティック クリプト マップに追加され、crypto アクセス コントロール リスト（ACL）で定義されている発信元ネットワークおよび発信元ネットマスクを基にルートを作成します。

```
crypto map mymap 1 ipsec-isakmp
 set peer 10.1.1.1
 reverse-route
 set transform-set esp-3des-sha
 match address 102
Interface FastEthernet 0/0/1
 ip address 192.168.0.2 255.255.255.0
 standby name group1
 standby ip 192.168.0.3
 crypto map mymap redundancy group1
access-list 102 permit ip 192.168.1.0 0.0.0.255 10.0.0.0 0.0.255.255
```

2 つのルート（リモート エンドポイント用とルート再帰用）を作成する場合の RRI の設定例

次に、クリプト マップが設定されているインターフェイスを介して、リモート エンドポイント用とリモート エンドポイントへのルート再帰用の 2 つのルートを作成する場合の例を示します。

```
reverse-route remote-peer
```

その他の参考資料

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『*Cisco IOS Master Commands List, All Releases*』
セキュリティ コマンド	• 『*Cisco IOS Security Command Reference Commands A to C*』 • 『*Cisco IOS Security Command Reference Commands D to L*』 • 『*Cisco IOS Security Command Reference Commands M to R*』 • 『*Cisco IOS Security Command Reference Commands S to Z*』
推奨される暗号化アルゴリズム	『Next Generation Encryption』

シスコのテクニカル サポート

説明	リンク
右の URL にアクセスして、シスコのテクニカル サポートを最大限に活用してください。これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

RRI の機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *260 : RRI* の機能情報

機能名	リリース	機能情報
逆ルート注入	Cisco IOS XE Release 2.1	逆ルート注入（RRI）とは、リモート トンネル エンドポイントによって保護されているネットワークおよびホストのルーティング プロセスに、スタティック ルートを自動的に組み込む機能です。保護されているこれらのホストおよびネットワークは、リモート プロキシ アイデンティティと呼ばれます。 各ルートは、リモート プロキシ ネットワークとマスクを基にして作成され、リモート トンネル エンドポイントがこのネットワークへのネクスト ホップとなります。ネクスト ホップとしてバーチャル プライベート ネットワーク（VPN）のリモート ルータを使い、暗号化プロセスによってトラフィックを強制的に暗号化します。 この機能に関する詳細については、次の各項を参照してください。 この機能により、次のコマンドが導入または変更されました。**reverse-route**。

第 193 章

IPsec VPN ハイアベイラビリティ拡張機能

IPsec VPN ハイ アベイラビリティ拡張機能：逆ルート注入（RRI）およびホットスタンバイ ルータ プロトコル（HSRP）と IPsec。これらの 2 つの機能を一緒に使用すると、VPN におけるネットワーク設計を簡素化できるほか、ゲートウェイ リストを定義する場合にリモート ピアの設定の複雑さを低減することができます。

（注） セキュリティに対する脅威は、脅威からの保護に役立つ暗号化技術と同様に絶え間なく変化しています。シスコの暗号化に関する最新の推奨事項の詳細は、『Next Generation Encryption』（NGE）ホワイトペーパーを参照してください。

IPsec VPN ハイ アベイラビリティ拡張機能に関する情報

逆ルート注入

逆ルート注入（RRI）は、冗長性やロードバランシングが求められるバーチャルプライベート ネットワーク（VPN）のネットワーク設計を簡素化します。RRI は、ダイナミック クリプト マップとスタティック クリプト マップのどちらを使用する場合でも適用できます。

RRI には次の利点があります。

- 複数の（冗長な）VPN ヘッドエンド デバイスがある環境で、IPsec トラフィックを特定の VPN ヘッドエンド デバイスにルーティングできます。
- 特に、リモート デバイスのルート フラッピングが多く発生する環境で IKE キープアライブを使用するとき、ヘッドエンド デバイス間のリモート セッションの予測可能なフェー

ルオーバー時間を保証します（ルート収束の効果は考慮されません。これは、使用されるルーティング プロトコルとネットワークの規模によって異なるためです）。

- ルートが動的にアップストリーム デバイスで学習されるので、アップストリーム デバイス上でスタティック ルートを管理する必要はありません。

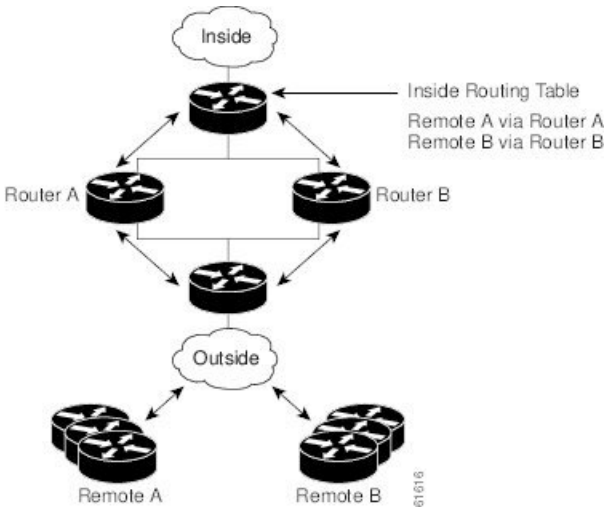
ダイナミック クリプト マップと連動する場合、リモート ピアが RRI 対応のルータとの IPsec セキュリティ アソシエーション（SA）を確立すると、スタティック ルートが、そのリモート ピアによって保護されたサブネットまたはホストごとに作成されます。スタティック クリプト マップの場合、スタティック ルートが拡張アクセス リスト ルールの各宛先に対して作成されます。アクセス コントロール リスト（ACL）を持つスタティック クリプト マップで RRI を使用すると、IPsec SA のネゴシエーションがなくても、ルートは常に存在します。

（注） RRI を使用する ACL では、any キーワードを使用できません。

作成されたルートは任意のダイナミック ルーティング プロトコルに注入され、周囲のデバイスに配布されます。このトラフィック フローでは、IPsec を正しい SA 全体に転送するために適切な RRI ルータに誘導し、IPsec ポリシーの不一致およびパケット喪失を回避する必要があります。

次の図は、RRI設定機能のトポロジを示します。リモートAにルータAがサービスを提供し、リモートBはルータBに接続します。このようにして、セントラル サイトにある VPN ゲートウェイ全体にロードバランシングを提供します。セントラルサイトのデバイスのRRIにより、ネットワーク内部の他のルータは、正しい転送判断を自動的に実行できるようになります。また、RRI により、内部ルータのスタティック ルートを管理する必要がなくなります。

図 *97* : 逆ルート注入設定機能を示すトポロジ



ホットスタンバイ ルータ プロトコルおよび IPsec

ホットスタンバイ ルータ プロトコル（HSRP）は、1 つのルータのアベイラビリティに頼らなくても、イーサネットネットワークのホストから IP トラフィックをルーティングすることで、ネットワークのハイ アベイラビリティを実現します。HSRP は、ICMP Router Discovery Protocol（IRDP）などのルータ ディスカバリ プロトコルをサポートしないホスト、および選択したルータがリロードしたときまたはオフになったときに新しいルータに切り替える機能を備えていないホストには特に便利です。この機能がないと、ルータ障害が原因でデフォルト ゲートウェイを失うルータはネットワークと通信できません。

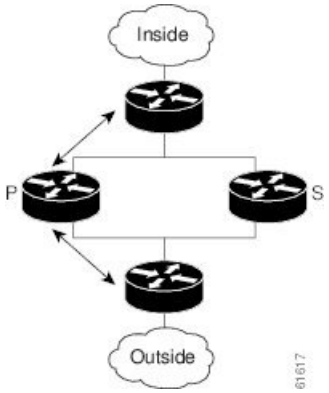
HSRP は、スタンバイ コマンドライン インターフェイス（CLI）コマンドを使用して LAN インターフェイス上に設定できます。インターフェイスから、ローカル IPsec ID またはローカル トンネル エンドポイントとしてスタンバイ IP アドレスを使用できます。

スタンバイ IP アドレスをトンネル エンドポイントとして使用すると、HSRP を使用してフェールオーバーを VPN ルータに適用できます。リモート VPN ゲートウェイは、HSRP グループ内のアクティブ デバイスに所属するスタンバイ アドレスを使用してローカル VPN ルータに接続します。フェールオーバーの際、スタンバイ デバイスはスタンバイ IP アドレスの所有権を引き継いで、リモート VPN ゲートウェイへのサービスを開始します。

フェールオーバーは、HSRP を使用して VPN ルータに適用できます。リモート VPN ゲートウェイは、HSRP グループ内のアクティブ デバイスに所属するスタンバイ アドレスを使用してローカル VPN ルータに接続します。この機能では、定義の必要があるのは HSRP スタンバイ アドレスだけなので、ゲートウェイ リストの定義に関してリモート ピア上での設定の複雑さが軽減されます。

次の図は、拡張 HSRP 機能のトポロジを示します。トラフィックは、スタンバイ グループのアクティブ装置である、アクティブ ルータ P でサービスが提供されています。フェールオーバーが発生した場合、トラフィックは、元のスタンバイ装置であるルータ S に迂回されます。ルータ S は新しいアクティブ ルータの役割を想定し、スタンバイ IP アドレスの所有権を引き継ぎます。

図 *98 :* ホットスタンバイ ルータ プロトコル機能を示すトポロジ



（注） フェールオーバーの場合、HSRP は、VPN ルータ間の IPsec 状態情報の転送を促進しません。つまり、この状態の転送が行われない場合、リモートに対する SA が削除され、インターネット キー交換（IKE）および IPsec SA を再確立する必要があります。IPsec フェールオーバーをさらに効率的に行うために、IKE キープアライブをすべてのルータ上でイネーブルにすることを推奨します。

IPsec VPN ハイ アベイラビリティ拡張機能の設定方法

ダイナミック クリプト マップでの逆ルート注入の設定

標準スタティック クリプト マップ エントリのようなダイナミック クリプト マップ エントリは各セットにグループ化されます。セットは、すべて同じダイナミック マップ名を持つダイナミック クリプト マップ エントリのグループですが、ダイナミック シーケンス番号はそれぞれ異なります。セットの各メンバーは、RRI に設定できます。

ダイナミック クリプト マップ エントリを作成し、RRI をイネーブルにするには、この項の手順を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **crypto dynamic-map** *map-name seq-num*
4. **set transform-set**
5. **reverse-route**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 3	**crypto dynamic-map** *map-name seq-num* 例： `Router(config)# crypto dynamic-map mymap`	ダイナミック クリプト マップ エントリを作成し、クリプト マップ コンフィギュレーション モードを開始します。
ステップ 4	**set transform-set** 例： `Router(config-crypto-m)#set transform-set`	このクリプト マップ エントリで許可するトランスフォーム セットを指定します。複数のトランスフォームセットをプライオリティの順に表示します（最もプライオリティの高いものを先頭に表示）。 このエントリは、ダイナミック クリプト マップ エントリで必要とされる唯一の設定文です。
ステップ 5	**reverse-route** 例： `Router(config-crypto-m)#reverse-route`	送信元プロキシの情報を作成します。

スタティック クリプト マップでの逆ルート注入の設定

スタティック クリプト マップに RRI を設定する前に、次の内容に注意してください。

- 逆ルートが mymap 2 でイネーブルになっていない場合、ルートはアクセス リスト 102 に基づいて作成されません。RRIは、デフォルトでイネーブルになっておらず、ルータ設定に表示されません。
- アップストリーム デバイスに VPN ルートを配布するには、ルーティング プロトコルをイネーブルにしてください。
- RRI 用に設定された VPN ルータ上でシスコ エクスプレス フォワーディング（CEF）が実行されている場合は、ネクスト ホップ デバイスを使用して、RRI 注入されたネットワークごとに隣接を設定する必要があります。これらのルートに対してネクストホップがルーティング テーブルで明示的に定義されていないので、プロキシ ARP をネクスト ホップ ルータ上でイネーブルにする必要があります（このルータによりそのデバイスのレイヤ 2 アドレスを使用して CEF 隣接関係を設定できます）。RRI 注入ルートが多い場合、RRI ルートが表す各サブネットからエントリがデバイスごとに作成されるので、隣接関係テーブルが非常に大きくなることがあります。

スタティック クリプト マップ セットに RRI を追加するには、この項の手順を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **crypto map** *map-name seq-num* **ipsec-isakmp**
4. **set peer** *ip-address*

5. **reverse-route**
6. **match address**
7. **set transform-set** *transform-set-name*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**crypto map** *map-name seq-num* **ipsec-isakmp** 例： `Router(config)#crypto map mymap 3 ipsec-isakmp`	ダイナミック クリプト マップ セットをスタティック クリプト マップ セットに追加し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	**set peer** *ip-address* 例： `Router(config-if)#set peer 209.165.200.248`	クリプト マップ エントリに対して IPsec ピアの IP アドレスを指定します。
ステップ 5	**reverse-route** 例： `Router (config-if)#reverse-route`	スタティック ルートをクリプト アクセス コントロール リスト（ACL）に基づいて動的に作成します。
ステップ 6	**match address** 例： `Router(config-if)# match address`	クリプト マップ エントリの拡張アクセス リストを指定します。
ステップ 7	**set transform-set** *transform-set-name* 例： `Router (config-if)# set transform-set my_t_set1`	このクリプト マップ エントリで許可するトランスフォーム セットを指定します。複数のトランスフォームセットをプライオリティ順（最高のプライオリティのものが最初）に列挙します。

IPsec を使用した HSRP の設定

IPsec を使用して HSRP を設定する場合、次の条件を満たさなければならないことがあります。

- スタンバイ IP アドレスまたはスタンバイ名をインターフェイス上で変更した場合、HSRP をインターフェイス上のクリプト マップに適用するときに、クリプト マップを再度適用する必要があります。
- HSRP がインターフェイス上のクリプトマップに適用され、そのインターフェイスからスタンバイ IP アドレスまたはスタンバイ名を削除した場合、暗号トンネル エンドポイントは、そのインターフェイスの実際の IP アドレスに再初期化されます。
- IPsec フェールオーバーの要件があるインターフェイスにスタンバイ IP アドレスおよびスタンバイ名を追加する場合、適切な冗長情報を使用してクリプトマップを再度適用する必要があります。
- スタンバイ プライオリティは、アクティブ ルータとスタンバイ ルータ上で等しくなる必要があります。等しくない場合、プライオリティが高いルータがアクティブ ルータを引き継ぎます。以前アクティブだったルータが再度アップ状態になり、ただちにアクティブ ロールを引き継いたためスタンバイの報告がされず同期化しない場合、接続は廃棄されます。
- HSRP 追跡されるインターフェイスの、スタンバイ ルータおよびアクティブ ルータ上の IP アドレスは、他方のルータより低く、あるいは高くする必要があります。プライオリティが等しい（HA 要件）場合、HSRP はアクティブ状態に基づいた IP アドレスを割り当てます。ルータ A のパブリック IP アドレスはルータ B のパブリック IP アドレスよりも低いが、プライベートインターフェイスに関してはその逆になるようなアドレッシング方式が存在する場合、アクティブ/スタンバイとスタンバイ/アクティブのように分裂した状況が発生し、接続が切断される可能性があります。

（注） IPsec を使用せずに HSRP を設定するには、『*IP Application Services Configuration Guide*』の「Configuring IP Services」モジュールを参照してください。

インターフェイスにクリプト マップ セットを適用するには、この項の手順を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **interface** *type slot / port*
4. **standby name** *group-name*
5. **standby ip** *ip-address*
6. **crypto map** *map-name* **redundancy** [*standby-name*]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例：	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。

	コマンドまたはアクション	目的
	`Router>enable`	
ステップ 2	**configure terminal** 例： `Router#configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface** *type slot / port* 例： `Router(config)#interface GigabitEthernet 0/0`	インターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	**standby name** *group-name* 例： `Router(config-if)#standby name mygroup`	スタンバイのグループ名を指定します。
ステップ 5	**standby ip** *ip-address* 例： `Router(config-if)#standby ip 209.165.200.249`	スタンバイ グループの IP アドレスを指定します。 • グループ内のデバイスごとにこのコマンドが必要です。
ステップ 6	**crypto map** *map-name* **redundancy** [*standby-name*] 例： `Router (config-if)#crypto map mymap redundancy`	IPsec のトンネル エンドポイントとして IP 冗長アドレスを指定します。

VPN IPsec 暗号設定の確認

手順の概要

1. **enable**
2. **show crypto ipsec transform-set**
3. **show crypto map** [**interface** *interface* | **tag** *map-name*]
4. **show crypto ipsec sa** [**map** *map-name* | **address** | **identity**] [**detail**]
5. **show crypto dynamic-map** [**tag** *map-name*]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例：	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。

	コマンドまたはアクション	目的
	`Router> enable`	
ステップ 2	**show crypto ipsec transform-set** 例： `Router#show crypto ipsec transform-set`	トランスフォーム セットの設定を表示します。
ステップ 3	**show crypto map** [**interface** *interface* | **tag** *map-name*] 例： `Router#show crypto map tag mycryptomap`	クリプト マップ コンフィギュレーションを表示します。
ステップ 4	**show crypto ipsec sa** [**map** *map-name* | **address** | **identity**] [**detail**] 例： `Router#show crypto ipsec sa address detail`	IPsec SA に関する情報を表示します。
ステップ 5	**show crypto dynamic-map** [**tag** *map-name*] 例： `Router#show crypto dynamic-map tag mymap`	ダイナミック クリプト マップに関する情報を表示します。

IPsec VPN ハイ アベイラビリティ拡張機能の設定例

例：ダイナミック クリプト マップでの逆ルート注入の設定

次の例では、ダイナミック クリプト マップ テンプレートの定義で **reverse-route** コマンドを使用することにより、接続しているリモート IPsec ピアによって保護されている、すべてのリモートプロキシ（サブネットまたはホスト）に対してルートが確実に作成されるようにします。

```
crypto dynamic mydynmap 1
 set transform-set my-transform-set
 reverse-route
```

このテンプレートは、「親」クリプトマップ文に関連付けられてから、インターフェイスに適用されます。

```
crypto map mymap 3 ipsec-isakmp dynamic mydynmap
 interface FastEthernet 0/0
 crypto map mymap
```

例：スタティック クリプト マップでの逆ルート注入の設定

RRI は、暗号化されたトラフィックを VPN ルータに転送し、他のトラフィックをすべて別のルータに転送する必要があるトポロジに適したソリューションです。このようなシナリオでは、RRI により、デバイスにスタティック ルートを手動で定義する必要はなくなります。

単一の VPN ルータが使用され、すべてのトラフィックがそのルータのネットワークのパスに出入りするときに VPN ルータを通過する場合、RRI は不要です。

リモート プロキシの VPN ルータに手動でスタティック ルートを定義し、これらのルートを永続的にルーティング テーブルにインストールする場合には、同じリモート プロキシをカバーするクリプト マップ インスタンスで RRI をイネーブルにしないでください。この場合、ユーザ定義のスタティック ルートが RRI によって削除されません。

ルーティング コンバージェンスの影響で、ルートのアドバタイズ（リンク状態と定期的な更新）に使用される、ルーティング プロトコルに基づくフェールオーバーの成否が左右されることがあります。ルーティング ステートの変更が検出された直後に、ルーティング アップデートが確実に送信されるようにして、コンバージェンス時間を短縮するには、OSPF などのリンク ステート ルーティング プロトコルを使用することを推奨します。

次の例では、RRI が mymap 2 に対してではなく、mymap 1 に対してイネーブルにされています。インターフェイスにクリプト マップが適用されると、ルートが次のようなアクセス リスト 101 に基づいて作成されます。

```
IP route 172.17.11.0 255.255.255.0 FastEthernet 0/0
crypto map mymap 1 ipsec-isakmp
 set peer 172.17.11.1
 reverse-route
 set transform-set my-transform-set
 match address 101
crypto map mymap 2 ipsec-isakmp
 set peer 10.1.1.1
 set transform-set my-transform-set
 match address 102
access-list 101 permit ip 192.168.1.0 0.0.0.255 172.17.11.0 0.0.0.255
access-list 102 permit ip 192.168.1.0 0.0.0.255 10.0.0.0 0.0.255.255
interface FastEthernet 0/0
 crypto map mymap
```

例：IPsec を使用した HSRP の設定

次の例では、すべてのリモート VPN ゲートウェイを、192.168.0.3 を介してルータに接続する方法を示します。インターフェイス上のクリプトマップは、このスタンバイ アドレスを *mymap* のすべてのインスタンスのローカル トンネル エンドポイントとしてバインドすると同時に、group1 と呼ばれる同じスタンバイ グループに属しているアクティブ デバイスとスタンバイ デバイスの間で HSRP フェールオーバーが確実に行われるようにします。

RRI により、HSRP グループ内のアクティブ デバイスだけが、リモート プロキシへのネクストホップ VPN ゲートウェイとして、内部のデバイスにアドバタイズできることにも注意してください。フェールオーバーが発生すると、ルートは、以前アクティブだったデバイス上から削除され、新たにアクティブになったデバイス上に作成されます。

```
crypto map mymap 1 ipsec-isakmp
 set peer 10.1.1.1
 reverse-route
 set transform-set esp-aes-sha
 match address 102
Interface FastEthernet 0/0
 ip address 192.168.0.2 255.255.255.0
 standby name group1
 standby ip 192.168.0.3
 crypto map mymap redundancy group1
access-list 102 permit ip 192.168.1.0 0.0.0.255 10.0.0.0 0.0.255.255
```

スタンバイ名はスタンバイ グループ内のすべてのデバイスに設定する必要があり、スタンバイ アドレスはグループの少なくとも 1 つのメンバーに設定する必要があります。スタンバイ名がルータから削除されると、IPsec SA は削除されます。スタンバイ名が再度追加された場合、使用される名前が同じかどうかにかかわらず、（冗長オプションを使用して）クリプトマップをインターフェイスに再度適用する必要があります。

その他の参考資料

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『Cisco IOS Master Command List, All Releases』
IPsec を使用しない HSRP の設定	『*IP Application Services Configuration Guide*』の「Configuring IP Services」モジュール
IP security（IPsec）用のステートフル フェールオーバーの設定	『*Security Configuration Guide: Secure Connectivity*』の「Stateful Failover for IPsec」モジュール
推奨される暗号化アルゴリズム	『Next Generation Encryption』

MIB

MIB	MIB のリンク
なし	選択したプラットフォーム、Cisco ソフトウェア リリース、およびフィーチャ セットの MIB を検索してダウンロードする場合は、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

シスコのテクニカル サポート

説明	リンク
右の URL にアクセスして、シスコのテクニカル サポートを最大限に活用してください。これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

IPsec VPN ハイ アベイラビリティ拡張機能の機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *261 : IPsec VPN* ハイ アベイラビリティ拡張機能の機能情報

機能名	リリース	機能情報
IPsec VPN ハイ アベイラビリティ拡張機能	Cisco IOS XE 3.1.0S	IPsec VPN ハイ アベイラビリティ拡張機能は次の 2 つの機能から構成されます。逆ルート注入（RRI）およびホット スタンバイ ルータ プロトコル（HSRP）と IPsec。これらの 2 つの機能を一緒に使用すると、VPN におけるネットワーク設計を簡素化できるほか、ゲートウェイ リストを定義する場合にリモート ピアの設定の複雑さを低減することができます。 次のコマンドが導入または変更されました。**crypto map**（インターフェイス IPsec）、**reverse-route**。

第 194 章

IPSEC 優先ピア

IP セキュリティ（IPsec）優先ピア機能を使用すれば、フェールオーバー シナリオでクリプト マップ上の複数のピアが試行される環境を制御できます。

この機能には、次の機能が含まれます。

- デフォルト ピア設定
- デフォルト ピアでの IPsec アイドル タイマーの使用

IPsec 優先ピアの前提条件

- クリプト マップを正しく定義し、完成させておく必要があります。

IPsec 優先ピアの制約事項

デフォルト ピア

- この機能はデッド ピア検出（DPD）と組み合わせて使用する必要があります。定期モードで DPD が実行されている、リモート サイト上で使用するのが最も有効です。DPD によって、デバイスの障害が素早く検出され、デフォルト ピアが次に試行される接続用に試行されるようにピア リストがリセットされます。

- クリプト マップ内のデフォルト ピアとして指定できるピアは 1 つだけです。
- デフォルト ピアはピア リスト内の最初のピアである必要があります。

デフォルト ピアでの IPsec アイドル タイマーの使用

- この機能は、それが設定されているクリプトマップ上でだけ動作します。すべてのクリプト マップ用に機能をグローバルに設定はできません。
- グローバル アイドル タイマーが存在する場合、クリプトマップ アイドル タイマー値とグローバル値は異なっている必要があります。同じである場合、アイドルタイマーがクリプト マップに追加されません。

IPsec フェールオーバー

Cisco ASR 1000 シリーズ ルータの IPSec は、ステートレス フェールオーバーのみをサポートします。IPsec フェールオーバーは、IPsec ネットワークの合計稼働時間（または可用性）を増やす機能です。従来、これは元の（アクティブな）ルータに加えて冗長（スタンバイ）ルータを使用することで実現されています。アクティブ ルータが何らかの理由で使用できなくなると、スタンバイ ルータは、IKE および IPsec の処理を引き継ぎます。

IPsec フェールオーバーは、ステートスレス フェールオーバーおよびステートフル フェールオーバーの 2 種類に分類されます。ステートレス フェールオーバーは、ホット スタンバイ ルータ プロトコル（HSRP）のようなプロトコルを使用して、プライマリからセカンダリへのカットオーバーを行い、さらにアクティブおよびスタンバイの VPN ゲートウェイを許可して、共通の仮想 IP アドレスを共有することができます。

IPsec 優先ピアに関する情報

IPsec

IPsec は、インターネット技術特別調査委員会（IETF）によって開発されたオープン規格のフレームワークです。IPSec は、インターネットなどの保護されていないネットワークを使用して機密情報を送信する場合に、セキュリティを提供します。IPsecはネットワーク層で機能し、Cisco ルータなどの参加している IPsec 装置（ピア）間のインターネット プロトコル（IP）パケットを保護および認証します。

IPSec は、次のネットワーク セキュリティ サービスを提供します。これらのサービスはオプションです。一般に、ローカル セキュリティ ポリシーにより、これらのサービスを 1 つ以上使用するよう指示されます。

- データ機密性：ネットワークにパケットを伝送する前に IPSec 送信側がパケットを暗号化できます。
- データ整合性：IPSec受信者は、IPSec送信者から送信されたパケットを認証し、伝送中にデータが変更されていないかを確認できます。

- データ送信元認証：IPSec受信者は、送信されたIPSecパケットの送信元を認証できます。
- アンチ リプレイ：IPsec 受信者は再送されたパケットを検出し、拒否できます。

IPSec を使用すれば、データを、観察、変更、またはスプーフィングされることを心配することなく、パブリック ネットワークを介して転送できます。これにより、インターネット、エクストラネット、およびリモート ユーザー アクセスを含む、バーチャル プライベート ネットワーク（VPN）などのアプリケーションが可能となります。

IPsec は、2 つのピア（2 台のルータなど）間にセキュア トンネルを確立します。機密性が高く、セキュア トンネルを介して送信する必要があるパケットを定義し、セキュア トンネルの特性を指定することによって、機密性の高いパケットを保護するパラメータを定義します。IPsec ピアによってこのように機密性の高いパケットが検出されたら、そのピアによって、適切な、セキュアなトンネルが設定され、そのパケットがトンネルからリモート ピアに送信されます。

Dead Peer Detection

VPN クライアントでは、DPD と呼ばれるキープアライブ メカニズムが使用され、IPsec トンネルの反対側の VPN デバイスが利用できるかどうかがチェックされます。ネットワークが極端にビジーだったり、信頼性が低下していたりした場合、ピアがこれからアクティブになることがないかどうか判断するまで VPN クライアントが待機する時間の秒数を増加できます。

トラフィックが受信されると、キープアライブ パケットは送信されません。これにより、DPD に関連したオーバーヘッドが低下します。高い負荷がかかっているネットワーク上では、トラフィックがトンネル上で受信されるために、送信されるキープアライブ パケットがきわめて少なくなるからです。さらに、DPD によってキープアライブ パケットが送信されるのは、送信されるユーザ トラフィックがある（そして受信されるユーザ トラフィックがない）場合だけです。

インターネット キー交換（IKE）を、発信ユーザ データが存在しているかどうかにかかわらず DPD によってキープアライブ パケットが送信されるように設定できます。つまり、受信ユーザ データがないかぎり、キープアライブパケットは設定されたキープアライブ インターバルで送信されます。

デフォルト ピア設定

接続タイムアウトが発生した場合、現在のピアへの接続は終了します。**set peer** コマンドを使用すれば、最初のピアをデフォルトピアとして設定できます。デフォルトピアが存在している状態で次回の接続が開始された場合、その接続は、ピア リスト内の次のピアではなく、デフォルト ピアに直接接続されます。デフォルト ピアの応答がない場合、ピア リスト内の次のピアが現在のピアとなり、クリプトマップを介した次からの接続では、そのピアが試行されます。

この機能は、物理リンク上のトラフィックがリモートピアの障害により停止した場合に便利です。DPD によって、リモート ピアが使用できないことが示されますが、そのピアは現在のピアのままです。

デフォルト ピアによって、過去に使用不可になったがサービスに復帰した優先ピアへのフェールオーバーが容易になります。ユーザは、特定のピアに対してフェールオーバーのイベントにおけるプリファレンスを与えることが可能です。これは、元の障害の原因がリモート ピアの障害ではなく、ネットワーク接続の問題であった場合に便利です。

アイドル タイマー

ルータでピアの IPSec セキュリティ アソシエーション（SA）を作成する場合、SA を維持するためのリソースを割り当てる必要があります。SA には、メモリと、複数の管理されたタイマーが必要です。ピアがアイドル状態だと、それらのリソースが無駄になってしまいます。あまりに多くのリソースがアイドル状態のピアによって浪費されてしまうと、ルータによる他のピアとの新しい SA の作成ができなくなる可能性があります。

IPsec SA アイドル タイマーを使用すると、アイドル状態のピアに関連した SA を削除することによってリソースの可用性を高めることが可能です。IPsec SA アイドル タイマーによってアイドル状態のピアによるリソースの浪費が防止されるので、必要に応じて新しい SA を作成するためにより多くのリソースを利用できるようになります。

IPsec SA アイドル タイマーが設定されていない場合、IPsec SA のグローバル ライフタイムだけが適用されます。SA は、ピアのアクティビティと関わりなく、グローバル タイマーが有効期限切れになるまで維持されます。

デフォルト ピアでの IPsec アイドル タイマーの使用

現在のピアへのすべての接続がタイムアウトした場合、次に接続が開始された時には、**set peer** コマンドで設定されたデフォルトピアに直接接続されます。デフォルト ピアが設定されていない状態で接続タイムアウトが発生した場合、現在のピアはタイムアウトしたピアのままになります。

この機能拡張により、過去に使用不可になったが現在では稼働中の優先ピアに対するフェールオーバーが容易になります。

クリプト マップ上のピア

クリプト マップ セットには複数のエントリを含めることができ、それぞれが異なるアクセスリストに対応します。ルータでは、クリプト マップ エントリが順番に検索され、そのエントリ内で指定されたアクセス リストとパケットの照合が試行されます。

パケットが特定のアクセスリスト内の **permit** エントリと一致し、対応するクリプトマップエントリが Cisco としてタグが付けられていた場合、クリプトマップ内のピア設定ステートメントで指定されたリモートピアとの接続が確立されます。

IPsec 優先ピアの設定方法

デフォルト ピアの設定

デフォルト ピアを設定するには、次の手順を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **crypto map** *map-name seq-num* [**ipsec-isakmp**] [**dynamic** *dynamic-map-name*] [**discover**] [**profile** *profile-name*]
4. **set peer** {*host-name* [**dynamic**] [**default**] | *ip-address* [**default**] }
5. **exit**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**crypto map** *map-name seq-num* [**ipsec-isakmp**] [**dynamic** *dynamic-map-name*] [**discover**] [**profile** *profile-name*] 例： `Router(config)# crypto map mymap 10 ipsec-isakmp`	クリプト マップ コンフィギュレーション モードを開始します。クリプト マップ エントリを作成または変更するか、動的に作成されるクリプトマップ設定のテンプレートを提供する暗号プロファイルを作成するか、またはクライアント アカウンティング リストを設定します。
ステップ 4	**set peer** {*host-name* [**dynamic**] [**default**]	*ip-address* [**default**] } 例： `Router(config-crypto-map)# set peer 10.0.0.2 default`	クリプト マップ内の IPsec ピアを指定します。指定した最初のピアがデフォルト ピアとして定義されていることを確認します。

	コマンドまたはアクション	目的
ステップ 5	**exit** 例： `Router(config-crypto-map)# exit`	クリプト マップ コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードに戻ります。

アイドル タイマーの設定

アイドル タイマーを設定するには、次の手順を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **crypto map** *map-name seq-num* [**ipsec-isakmp**] [**dynamic** *dynamic-map-name*] [**discover**] [**profile** *profile-name*]
4. **set security-association idletime** *seconds* [**default**]
5. **exit**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**crypto map** *map-name seq-num* [**ipsec-isakmp**] [**dynamic** *dynamic-map-name*] [**discover**] [**profile** *profile-name*] 例： `Router(config)# crypto map mymap 10 ipsec-isakmp`	クリプト マップ コンフィギュレーション モードを開始します。クリプト マップ エントリを作成または変更するか、動的に作成されるクリプトマップ設定のテンプレートを提供する暗号プロファイルを作成するか、またはクライアント アカウンティング リストを設定します。
ステップ 4	**set security-association idletime** *seconds* [**default**] 例： `Router(config-crypto-map)# set security-association idletime 120 default`	デフォルト ピアが使用される前に、現在のピアをアイドル状態にしておける最大期間を指定します。

	コマンドまたはアクション	目的
ステップ 5	**exit** 例： `Router(config-crypto-map)# exit`	クリプト マップ コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードに戻ります。

IPsec 優先ピアの設定例

デフォルト ピアの設定例

次に、IP アドレスが 10.1.1.1 である最初のピアがデフォルト ピアである例を示します。

```
crypto map tohub 1 ipsec-isakmp
 set peer 10.1.1.1 default
 set peer 10.2.2.2
```

IPsec アイドル タイマーの設定例

次の例では、現在のピアが 120 秒間アイドルであった場合、次の接続試行ではデフォルトピア 10.1.1.1（**set peer** コマンドで指定）が使用されます。

```
crypto map tohub 1 ipsec-isakmp
 set peer 10.1.1.1 default
 set peer 10.2.2.2
 set security-association idletime 120 default
```

その他の参考資料

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『Cisco IOS Master Commands List, All Releases』
IPSec	『*Security for VPNs with IPsec*』
クリプト マップ	• 『*Security for VPNs with IPsec*』 • 「*Configuring Internet Key Exchange for IPsec VPNs*」
DPD	『*IPsec Dead Peer Detection Periodic Message Option*』

関連項目	マニュアル タイトル
セキュリティ コマンド	『*Cisco IOS Security Command Reference*』

MIB

MIB	MIB のリンク
なし。	選択したプラットフォーム、Cisco IOS ソフトウェア リリース、およびフィーチャ セットの MIB を検索してダウンロードする場合は、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

シスコのテクニカル サポート

説明	リンク
右の URL にアクセスして、シスコのテクニカル サポートを最大限に活用してください。これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

IPsec 優先ピアの機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *262 : IPsec* 優先ピアの機能情報

機能名	リリース	機能情報
IPSEC 優先ピア	Cisco IOS XE Release 2.1	IPsec 優先ピア機能を使用すれば、フェールオーバー シナリオでクリプト マップ上の複数のピアが試行される環境を制御できます。 次のコマンドが導入または変更されました。**set peer** (IPsec) および **set security-association idle-time**。

用語集

crypto access list：暗号によって保護する IP トラフィック、および暗号によって保護しないトラフィックが定義されたリスト。

crypto map：IPsec によって保護する必要があるトラフィック、送信する必要がある IPsec 保護対象トラフィック、およびこのトラフィックに適用する必要がある IPsec トランスフォームセットが指定されたマップ。

dead peer detection：応答しないピアを検出することをルータに可能にさせる機能。

keepalive message：1 つのネットワークデバイスからもう 1 つのネットワークデバイスに対して、2 つのネットワークデバイス間の仮想回線がまだアクティブであることを通知するために送信されるメッセージ。

peer：IPsec および IKE に参加するルータまたはその他のデバイス。IPsec においては、ピアは、キーの交換またはデジタル証明書の交換のどちらかを通じてセキュアに通信するデバイスまたはエンティティです。

SA：Security Association（セキュリティ アソシエーション）。データ フローに適用されるセキュリティ ポリシーとキー関連情報のインスタンスです。SA は、IKE と IPsec の双方で使用されますが、各 SA は互いに独立しています。IPsec SA は単方向通信であり、セキュリティ プロトコルごとに一意です。IKE SA は、IPsec SA とは異なって双方向通信であり、使用されるのは IKE に限られます。SA のネゴシエーションおよび確立は、IPsec ではなく IKE によって行われます。また、IPsec SA はユーザが手動で確立できます。保護されたデータ パイプでは 1 組の SA が必要であり、プロトコルごとに 1 方向あたり 1 つずつ必要です。たとえば、ピア間でカプセル化セキュリティ ペイロード（ESP）をサポートするパイプに対しては、それぞれの通信方向ごとに 1 つの ESP SA が必要です。SA は、宛先（IPsec エンドポイント）のアドレス、セキュリティ プロトコル（AH または ESP）、およびセキュリティ パラメータ インデックス（SPI）によって一意に識別されます。

transform set：IPsec 保護されたトラフィックに適用されるセキュリティプロトコル、アルゴリズムおよびその他の設定の適切な組み合わせです。IPsec SA のネゴシエーション中に、ピアは、特定のトランスフォーム セットを使用して特定のデータ フローを保護することに合意します。

第 195 章

IPsec トンネル ピアの Real-Time Resolution

リモート IP セキュリティ（IPsec）ピアにホスト名（IP アドレスではない）を指定した後、IPsec トンネル ピアの Real-Time Resolution 機能を使用すると、ルータが IPsec トンネルを確立する前にドメイン ネーム サーバ（DNS）でホスト名を名前解決できます。これにより、ピアの IP アドレスが変更されたかどうかをルータが直ちに検出できます。

IPsec トンネル ピアの Real-Time Resolution の制約事項

セキュア DNS の要件

この機能はセキュア DNS とだけ使用し、さらに、DNS の応答を認証できる場合に使用することを推奨します。それ以外の場合に使用すると、攻撃者が DNS の応答を偽装または強制し、証明書などのインターネット キー交換（IKE）認証データへのアクセス権を取得するおそれがあります。攻撃者は、発信側のホストによって信頼されている証明書を取得すると、フェーズ 1 の IKE セキュリティ アソシエーション（SA）を確立したり、発信側と実際の応答側で共有されている事前共有キーを推測しようとしたりします。

DNS 発信側

DNS によるリモート IPsec ピアの名前解決が機能するのは、ピアを発信側として使用する場合だけです。暗号化される最初のパケットが DNS ルックアップを開始します。DNS ルックアップが完了すると、これに続くパケットによって IKE が開始されます。

IPsec トンネル ピアの Real-Time Resolution に関する情報

セキュア DNS による Real-Time Resolution

リモート IPsec ピアのホスト名を **set peer** コマンドで指定する際、キーワード **dynamic** も発行できますが、このキーワードを使用すると IPsec トンネルが確立される直前まで、DNS によるホスト名の解決が遅れます。解決が遅れることで、ソフトウェアはリモート IPsec ピアの IP アドレスが変更されたかどうかを検出できます。こうしてこのソフトウェアは、新しい IP アドレスでこのピアと通信できるようになります。

キーワード **dynamic** を発行しない場合は、ホスト名は指定後すぐに解決されます。このため、ソフトウェアは IP アドレスの変更を検知できず、以前に解決した IP アドレスに対して接続を試みます。

DNS 解決によって、確立した IPsec トンネルがセキュアで、認証済みであることが保証されます。

Real-Time Resolution の設定方法

IPsec ピアの Real-Time Resolution の設定

この作業で、DNS によるリモート IPsec ピアのリアルタイム DNS 決を実行するようにルータを設定します。これにより、DNS ルックアップによるピアのホスト名の解決は、ルータがピアと接続（IPsec トンネル）を確立する直前になります。

始める前に

クリプト マップを作成する前に、次の作業を実行してください。

- Internet Security Association Key Management Protocol（ISAKMP）ポリシーの定義。
- IPsec トランスフォーム セットの定義。

手順の概要

1. **enable**
2. **configure terminal**
3. **crypto map** *map-name seq-num* **ipsec-isakmp**
4. **match address** *access-list-id*
5. **set peer** {*host-name* [**dynamic**] | *ip-address*
6. **set transform-set** *transform-set-name1* [*transform-set-name2 ... transform-set-name6*]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**crypto map** *map-name seq-num* **ipsec-isakmp** 例： `Router(config)# crypto map secure_b 10 ipsec-isakmp`	作成または変更するクリプト マップ エントリを指定して、クリプト マップ コンフィギュレーション モードを開始します。
ステップ 4	**match address** *access-list-id* 例： `Router(config-crypto-m)# match address 140`	拡張アクセス リストに名前を付けます。 このアクセス リストは、このクリプト マップ エントリに照らして、IPsec で保護する必要があるトラフィックと、IPsec で保護しないトラフィックを決定します。
ステップ 5	**set peer** {*host-name* [**dynamic**] | *ip-address* 例： `Router(config-crypto-m)# set peer b.cisco.com dynamic`	リモート IPsec ピアを指定します。 このピアは、IPsec で保護されたトラフィックの転送先となるピアです。 • **dynamic**：ルータがリモートピアとの間で IPsec トンネルを確立する直前に DNS ルックアップでホスト名を解決するようにします。このキーワードを指定しない場合、ホスト名は指定後すぐに解決されます。 複数のリモート ピアに対して、同じ作業を繰り返します。
ステップ 6	**set transform-set** *transform-set-name1* [*transform-set-name2 ... transform-set-name6*] 例： `Router(config-crypto-m)# set transform-set myset`	このクリプト マップ エントリで許可するトランスフォーム セットを指定します。複数のトランスフォームセットをプライオリティ順（最高のプライオリティのものが最初）に列挙します。

トラブルシューティングのヒント

暗号マップの設定情報を表示するには、**show crypto map** コマンドを使用します。

次の作業

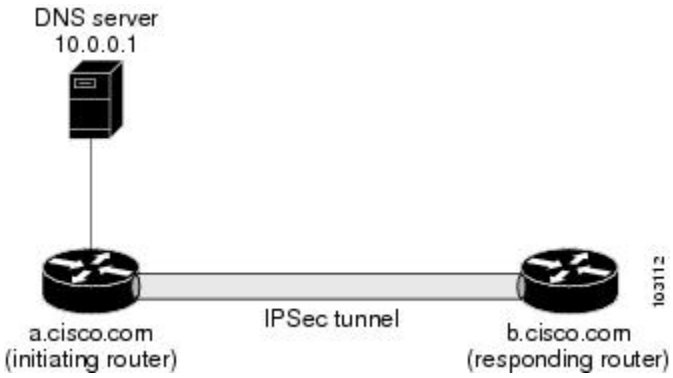
IPSec トラフィック フローが通過する各インターフェイスにクリプト マップ セットを適用する必要があります。インターフェイスにクリプト マップ セットを適用すると、ルータには、接続中にクリプトマップセットに対してすべてのインターフェイスのトラフィックを評価し、暗号で保護するトラフィックのために、指定されたポリシーまたは SA のネゴシエーションを使用するように指示されます。

Real-Time Resolution の設定例

IPsec ピアの Real-Time Resolution の設定例

次の図および例を使って、ソフトウェアがリモート IPsec ピアとの間で接続を確立しようとする直前に、そのピアのホスト名を DNS ルックアップで DNS 解決するように設定する暗号マップの作成方法を説明します。

図 *99 : Real-Time Resolution* のサンプル トポロジ




```
! Configure the initiating router.
hostname a.cisco.com
ip domain name cisco.com
ip name server 10.0.0.1
!
crypto map secure_b 10 ipsec-isakmp
  match address 140
  set peer b.cisco.com dynamic
  set transform-set xset
interface serial1
  ip address 10.10.0.1
  crypto map secure_b
access-list 140 permit ...
!
! Configure the responding router (the remote IPSec peer).
hostname b.cisco.com
!
crypto map secure_a 10 ipsec-isakmp
  match address 150
  set peer 10.10.0.1
  set transform-set
```

```
interface serial0/1
  ip address 10.0.0.1
  crypto map secure_a
access-list 150 ...
! DNS server configuration
b.cisco.com 10.0.0.1       # the address of serial0/1 of b.cisco.com
```

その他の参考資料

関連資料

関連項目	マニュアル タイトル
クリプト マップ	『*Security for VPNs with IPsec Configuration Guide*』の「Configuring Security for VPNs with IPsec」モジュール
ISAKMP ポリシー	『*Internet Key Exchange for IPsec VPNs Configuration Guide*』の「Configuring Internet Key Exchange for IPsec VPNs」モジュール
IPsec および IKE のコンフィギュレーション コマンド	『*Cisco IOS Security Command Reference*』

標準

標準	タイトル
この機能によってサポートされる新しい規格または変更された規格はありません。またこの機能による既存規格のサポートに変更はありません。	--

MIB

MIB	MIB のリンク
この機能によってサポートされる新しい MIB または変更された MIB はありません。またこの機能による既存 MIB のサポートに変更はありません。	選択したプラットフォーム、Cisco IOS XE ソフトウェア リリース、およびフィーチャ セットの MIB の場所を検索しダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

RFC

RFC	タイトル
この機能によりサポートされた新規 RFC または改訂 RFC はありません。またこの機能による既存 RFC のサポートに変更はありません。	--

シスコのテクニカル サポート

説明	リンク
シスコのサポート Web サイトでは、シスコの製品やテクノロジーに関するトラブルシューティングにお役立ていただけるように、マニュアルやツールをはじめとする豊富なオンライン リソースを提供しています。 お使いの製品のセキュリティ情報や技術情報を入手するために、Cisco Notification Service（Field Notice からアクセス）、Cisco Technical Services Newsletter、Really Simple Syndication（RSS）フィードなどの各種サービスに加入できます。 シスコのサポート Web サイトのツールにアクセスする際は、Cisco.com のユーザ ID およびパスワードが必要です。	http://www.cisco.com/techsupport

IPsec トンネル ピアの Real-Time Resolution の機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *263 : IPsec* トンネル ピアの *Real-Time Resolution* の機能情報

機能名	リリース	機能情報
IPsec トンネル ピアの Real-Time Resolution	Cisco IOS XE Release 2.1	リモート IP セキュリティ（IPsec）ピアにホスト名（IP アドレスではない）を指定した後、この機能を使用すると、ルータが IPsec トンネルを確立する前にドメイン ネーム サーバ（DNS）でホスト名を名前解決できます。これにより、ピアの IP アドレスが変更されたかどうかをルータが直ちに検出できます。 次のコマンドが導入または変更されました。**set peer (IPsec)**。

第 XX 部

Internet Key Exchange

第 196 章

「Configuring Internet Key Exchange for IPsec VPNs」

この章では、基本的な IP Security（IPsec）バーチャル プライベート ネットワーク（VPN）用のインターネット キー エクスチェンジ（IKE）プロトコルの設定方法について説明します。IKE とは、IPsec 標準とともに使用されるキー管理プロトコル標準です。IPsec は、IP パケットに対して強力な認証や暗号化を実現する IP セキュリティ機能です。

IPsec の設定には必ずしも IKE は必要ありませんが、IKE では、IPsec 標準に対する新機能が追加されているほか、設定をより柔軟かつ容易に行えるよう、IPsec のサポートが強化されています。

IKE は、Oakley キー交換や Skeme キー交換をインターネット セキュリティ アソシエーションおよびキー管理プロトコル（ISAKMP）フレームワーク内部に実装したハイブリッドプロトコルです（ISAKMP、Oakley、および Skeme は、IKE により実装されるセキュリティ プロトコルです）。

（注） セキュリティに対する脅威は、脅威からの保護に役立つ暗号化技術と同様に絶え間なく変化しています。シスコの暗号化に関する最新の推奨事項の詳細は、『Next Generation Encryption』（NGE）ホワイトペーパーを参照してください。

IKE 設定の前提条件

- 「Configuring Security for VPNs with IPsec」モジュールで説明している概念およびタスクを理解している必要があります。
- ご使用のアクセス コントロール リスト（ACL）が IKE と互換性があることを確認してください。IKE ネゴシエーションではポート 500 でUser Datagram Protocol（UDP）を使用するため、IKE および IPsec が使用するインターフェイスで UDP ポート 500 のトラフィックがブロックされないように ACL を設定しておく必要があります。場合によっては、UDP ポート 500 のトラフィックを明示的に許可するために、ACL にステートメントを追加する必要があります。

IKE 設定の制約事項

- プロファイルがロックされたり、DMI 劣化状態が発生したりしないようにするには、**config-replace** コマンドを使用して設定を置き換える前に、必ず、トンネルインターフェイスをシャットダウンして、すべての暗号セッションとトンネル設定を停止させてください。
- 開始ルータでは、リモートピアに関連付けられた証明書が必要ありません。
- 事前共有キーは、両方のピアで完全修飾ドメイン名（FQDN）を使用する必要があります（事前共有キーを設定するには、**crypto isakmp key** コマンドを入力します）。
- 各通信ルータは、互いの FQDN ホスト エントリを設定に保持している必要があります。
- 通信ルータはホスト名で認証するように設定する必要があります（IP アドレスでは必要ありません）。このため、**crypto isakmp identity hostname** コマンドを使用する必要があります。
- **show crypto eli** コマンドを使用して、デバイスのソフトウェア暗号化制限事項を決定します。ハードウェア モジュールがない場合の制限事項は次のとおりです。
  - IPSec セキュリティ アソシエーション（SA）数：1000
  - IKE SA 数：100
  - Diffie-Hellman（DH）セッション キー数：50
- サイト間 VPN での TCP フローのパフォーマンスを向上させるには、**no crypto batch allowed** コマンドを使用して暗号バッチ機能を無効にします。ただし、暗号バッチ機能を無効にすると、CPU 使用率が影響を受ける可能性があります。
- Cisco IOS リリース 15.0(1)SY 以降では、Cisco Catalyst 6500 シリーズ スイッチで **crypto ipsec** コマンドを使用して IPsec ネットワークセキュリティ機能を設定できません。これらのスイッチで IPsec をサポートするには、ハードウェア暗号化エンジンを使用する必要があります。

IPsec VPN の IKE 設定に関する情報

IKE での使用でサポート対象となる標準

シスコでは次の標準を採用しています。

- IPsec：IP セキュリティ プロトコル。IPsec はオープン規格のフレームワークであり、これにより、参加ピア間でデータ機密性、データ整合性、およびデータ認証が提供されます。IPsec は、これらのセキュリティ サービスを IP レイヤで提供します。IPsec は、IKE を使用して、ローカル ポリシーに基づいてプロトコルのネゴシエーションおよびアルゴリズムを処理し、IPsec で使用される暗号キーと認証キーを生成します。IPsec は、1 組のホスト間、1 組のセキュリティ ゲートウェイ間、またはセキュリティ ゲートウェイとホスト間で 1 つ以上のデータ フローを保護するために使用できます。
- ISAKMP：インターネット セキュリティ アソシエーションおよびキー管理プロトコル。ペイロード形式、キー交換プロトコル実装の方法、およびセキュリティ アソシエーションのネゴシエーションを定義するプロトコル フレームワークです。
- Oakley：キー交換プロトコルの 1 つで、認証済みのキー関連情報を取得する方法を定義します。
- Skeme：キー交換プロトコルの 1 つで、キーをすばやく更新しながら認証済みのキー関連情報を取得する方法を定義します。

（注） シスコは現在、DES、3DES、MD5（HMAC バリアント含む）、および Diffie-Hellman（DH）グループ 1、2、および 5 の使用は推奨していません。代わりに、AES、SHA-256、および DH グループ 14 以降を使用する必要があります。Cisco の暗号化に関する最新の推奨事項の詳細については、『Next Generation Encryption（NGE）』ホワイト ペーパーを参照してください。

IKE での使用に備えて実装されているコンポーネント テクノロジーには次のものがあります。

- AES：Advanced Encryption Standard（AES）。暗号アルゴリズムの 1 つで、重要ではあるが機密扱いではない情報を保護します。AES は、IPsec および IKE 用のプライバシー変換であり、データ暗号規格（DES）に代わる規格として開発されました。AES は DES よりセキュリティを向上させるために設計されています。具体的には、AES は、キーのサイズが従来より大きく、侵入者が既知の方式でメッセージを解読するには、キーを総当たりで試すしかありません。AES のキーは可変長であり、アルゴリズムは 128 ビット キー（デフォルト）、192 ビット キー、または 256 ビット キーを指定できます。
- DES：データ暗号規格（DES）。パケット データの暗号化に使用されるアルゴリズムです。IKE は Explicit IV 標準の 56 ビット DES-CBC を実装しています。Cipher Block Chaining（CBC）では、暗号化の開始に初期ベクター（IV）が必要です。IV は IPSec パケットに明示的に指定されます。

また Cisco IOS ソフトウェアは、特定のプラットフォームで使用可能なソフトウェア バージョンに応じて、Triple DES（168 ビット）暗号化も実装します。トリプル DES（3DES）は強力な暗号化方式であり、これにより、機密性の高い情報を非信頼ネットワーク上で送信できます。この暗号化方式を使用することで、（特に金融業界の）お客様はネットワーク層での暗号化を実現できます。

（注） 強力な暗号化を使用する Cisco IOS イメージ（56 ビット データ暗号化フィーチャ セットを含むがこれに限定されない）は、米国輸出規制の対象となり、配布が制限されます。米国以外の国でインストールされるイメージには、輸出許可が必要です。米国政府の規制により、お客様の注文が拒否されたり、納入が遅れたりすることがあります。詳細については、営業担当者または販売業者、あるいは export@cisco.com までお問い合わせください。

- SEAL：ソフトウェア暗号化アルゴリズム（SEAL）。ソフトウェアベースの DES、3DES、および AES に代わるアルゴリズムです。SEAL 暗号化では、160 ビットの暗号キーが使用され、他のソフトウェアベースのアルゴリズムに比べて、CPU に与える影響は小さくなります。

- SHA-2 および SHA-1 ファミリ（HMAC バリアント）：セキュア ハッシュ アルゴリズム（SHA）の 1 および 2。SHA-1 および SHA-2 は、パケット データの認証および IKE プロトコルの整合性確認メカニズムの検証に使用されるハッシュ アルゴリズムです。HMAC は、追加レベルのハッシュを提供するバリアントです。SHA-2 ファミリには、SHA-256 ビットのハッシュ アルゴリズムと SHA-384 ビットのハッシュ アルゴリズムが加わっています。この機能は Suite-B の要件に含まれています。Suite-B は、IKE および IPSec で使用するための暗号化アルゴリズムの 4 つのユーザ インターフェイス スイートで構成され、RFC 4869 に記述されています。各スイートは、暗号化アルゴリズム、デジタル署名アルゴリズム、キー合意アルゴリズム、ハッシュまたはメッセージ ダイジェスト アルゴリズムで構成されています。Cisco IOS での Suite-B サポートについての詳細は、「Configuring Security for VPNs with IPsec」機能モジュールを参照してください。

- RSA シグニチャおよび RSA 暗号化ナンス：RSA は、ロナルド・リベスト、アディ・シャミア、レオナルド・エーデルマンの 3 人によって開発された公開キー暗号化システムです。RSA シグニチャは否認防止を実行し、RSA 暗号化ナンスは否認を実行します（否認および否認防止は追跡可能性と関係があります）。

- Diffie-Hellman：公開キー暗号法プロトコルの 1 つで、2 者間に、安全でない通信チャネルでの共有秘密を確立できます。Diffie-Hellman は、IKE 内でセッション キーを確立するために使用されます。これは、768 ビット（デフォルト）、1024 ビット、1536 ビット、2048 ビット、3072 ビット、および 4096 ビット DH グループをサポートします。また、256 ビット サブグループを含む 2048 ビット DH グループと、256 ビットと 384 ビットの Elliptic Curve DH（ECDH）もサポートします。Cisco では、2048 ビット以上の DH キー交換または ECDH キー交換を使用することを推奨します。

- MD5：Message Digest 5（ハッシュ ベースのメッセージ認証コード（HMAC））バリアント）。パケット データの認証に使用するハッシュ アルゴリズム。HMAC は、追加レベルのハッシュを提供するバリアントです。

IKE は、X.509v3 証明書と相互運用されます。X.509v3 は、認証に公開キーが必要な場合に、IKEプロトコルに沿って使用されます。この証明書サポートを使用すると、各デバイスに同等のデジタル ID カードを付与することで、保護されたネットワークを拡張できます。2 つの装置が通信する際、デジタル証明書を交換することで ID を証明します（これにより、各ピアで公開キーを手動で交換したり、各ピアで共有キーを手動で指定したりする必要がなくなります）。

IKE の利点

IKE は自動で IPsec セキュリティ アソシエーション（SA）をネゴシエーションするため、手間のかかる手動の事前設定をすることなしに IPsec によるセキュアな通信を実現できます。特に、IKE には次のような利点があります。

- IPsec SA のライフタイムが指定可能。
- IPsec セッション中に暗号キーの変更が可能。
- IPsec でアンチ リプレイ サービスが使用可能。
- 認証局（CA）のサポートにより、管理可能でスケーラブルな IPsec を実現可能。
- ピアのダイナミック認証が可能です。

IKE のメイン モードとアグレッシブ モード

IKE では、キーのネゴシエーションにフェーズ 1 とフェーズ 2 の 2 つのフェーズがあります。フェーズ 1 では、2 つの IKE ピア間でセキュリティ アソシエーション（キー）のネゴシエーションをします。フェーズ 1 でキーのネゴシエーションをすることで、フェーズ 2 で IKE ピアが安全に通信できるようになります。フェーズ 2 のネゴシエーションでは、IKE が IPsec など他の適用でのキー（セキュリティ アソシエーション）を設定します。

フェーズ 1 のネゴシエーションは、メイン モードまたはアグレッシブ モードを使用して実行されます。メインモードでは、ネゴシエーション中にすべての情報が保護されるため、攻撃者が情報にアクセスできなくなります。メイン モードを使用すると、2 つの IKE ピアの ID が非表示になります。このモードでの運用は非常にセキュアですが、ネゴシエーションの実行に比較的時間がかかります。アグレッシブ モードでは、メインモードよりも少ない時間でピア間のキーのネゴシエーションを実行します。ただし、メインモードでのネゴシエーションでは可能なセキュリティが一部失われます。たとえば、セキュリティアソシエーションを確立しようとしている 2 つの装置の ID が傍受者に見えてしまいます。

この 2 つのモードは異なった目的で使用し、それぞれ別の強みがあります。メインモードは、アグレッシブ モードに比べると低速ですが、アグレッシブ モードよりも IKE ピアのセキュリティが高いため、セキュアで柔軟性があります。アグレッシブ モードは柔軟性とセキュリティの点で劣りますが、より高速です。

Cisco IOS ソフトウェアでは、この 2 つのモードの設定はできません。IKE 認証（rsa-sig、rsa-encr、または事前共有）ではデフォルトでメイン モードを起動しますが、認証の起動に対応する情報がなく、ピアのホスト名に関連づけられている事前共有キーがある場合、Cisco IOS

ソフトウェアはアグレッシブ モードを起動できます。Cisco IOS ソフトウェアでは、アグレッシブ モードを開始した IKE ピアには、アグレッシブ モードで応答します。

IKE ネゴシエーション用 IKE ポリシー セキュリティ パラメータ

IKEポリシーを使い、IKEネゴシエーション中に使用するセキュリティ パラメータの組み合わせを定義します。IKEエクスチェンジに参加する各ピアでIKEポリシーを作成する必要があります。

IKE ポリシーを 1 つも設定しない場合、ルータはデフォルトのポリシーを使用します。デフォルトのポリシーは、常にプライオリティが最低に設定されており、各パラメータはデフォルト値に設定されています。

IKE ポリシーについて

IKEネゴシエーションは保護する必要があるため、各IKEネゴシエーションは、共有（共通）のIKEポリシーについて両ピアが同意することで開始されます。このポリシーには、次のIKEネゴシエーションを保護するために使用するセキュリティ パラメータとピアの認証方法を記述します。

両ピアがポリシーに同意すると、各ピアに確立されている SA によってポリシーのセキュリティ パラメータが識別され、ネゴシエーションにおける以降すべての IKE トラフィックに適用されます。

各ピアには、パラメータ値の組み合わせをそれぞれ変えることでプライオリティをつけたポリシーを複数設定できます。ただし、そのうちの少なくとも1つのポリシーには、リモート ピアのポリシーのいずれかとまったく同じ暗号化、ハッシュ、認証、Diffie-Hellman パラメータの各値が設定されている必要があります。作成する各ポリシーに対して、一意のプライオリティを割り当てます（1 ～ 10,000 で指定し、1 が最大のプライオリティ）。

ヒント　サポートされているパラメータの値が1つしかないデバイスを使用する場合は、もう一方のデバイスでサポートされている値を設定する必要があります。この制限を別にすれば、セキュリティとパフォーマンスには通常トレードオフの関係があり、パラメータ値の多くにはこのトレードオフがあります。ネットワークのセキュリティ リスクのレベルと、そのリスクに対する許容度を評価する必要があります。

一致する IKE ポリシーでの IKE ピアの合意

IKE ネゴシエーションが開始されると、IKE は、両方のピアにある同じ IKE ポリシーを検索します。ネゴシエーションを開始したピアがすべてのポリシーをリモート ピアに送信し、リモート ピアの方では一致するポリシーを探そうとします。リモート ピアは、自分のプライオリティ 1 位のポリシーと、相手のピアから受け取ったポリシーを比較し、一致するポリシーを探します。一致するポリシーが見つかるまで、リモート ピアは優先順位が高い順に各ポリシーをチェックします。

一致が成立するのは、2 つのピアからの両方のポリシーに、同じ暗号化、ハッシュ、認証、Diffie-Hellman パラメータ値が含まれているときです。

一致した場合は、IKE がネゴシエーションを完了し、IPsec セキュリティ アソシエーションが作成されます。一致するポリシーが見つからなかった場合は、IKEはネゴシエーションを拒否し、IPsec は確立されません。

（注） このパラメータ値は、IKE SA の確立後 IKE ネゴシエーションに適用されます。ポリシーに指定する認証方式によっては、追加の設定が必要な場合があります。詳細については、IKE認証の設定 （2855 ページ）を参照してください。

ピアのポリシーに必要な関連設定がされていないと、一致するポリシーをリモート ピアで検索するときに、ピアはポリシーを送信しません。

IKE 認証

IKE 認証は次のオプションで構成され、各認証方式には追加の設定が必要です。

RSA シグニチャ

RSA シグニチャでは、CA から証明書を取得するようにピアを設定できます（証明書を発行するよう、CA が正しく設定されている必要があります）。CA を使用すると、IPSec ネットワークの管理性と拡張性が大幅に改善されます。また、RSA シグニチャ ベースの認証で使用できる公開キー操作は 2 つだけです。これに対し、RSA 暗号化では 4 つの公開キー操作を使用しますが、その分だけ全体のパフォーマンスが下がります。CA サポートを正しく設定するには、モジュール「PKI 内での RSA キーの展開」を参照してください。

証明書は公開キーを安全に交換するために各ピアで使用されますRSA シグネチャでは、各ピアに、リモートピアの公開シグネチャキーが必要です。双方のピアに有効な証明書がある場合、RSA シグニチャを使用する IKE ネゴシエーションの一環として、ピア間で公開キーが自動的に交換されます。

公開キーは手動で交換することもできます。これについては、RSA 暗号化ナンスの RSA キーの手動設定 （2855 ページ） を参照してください。

RSA シグニチャにより、IKE ネゴシエーションで否認防止が可能になりますさらに、リモートピアとの IKE ネゴシエーションを実際に実行することで、第三者に対する証明が可能になります。

RSA 暗号化ナンス

RSA暗号化ナンスを使用するには、各ピアが他のピアの公開キーを持つようにする必要があります。

RSA シグニチャとは異なり、RSA 暗号化ナンス方式では、証明書を使って公開キーを交換できません。その代わりに、各ピアが他のピアの公開キーを持つようにする必要があります。それには次の方法のいずれかを実行します。

- RSA キーを手動で設定する（「RSA 暗号化ナンスの RSA キーの手動設定（2855 ページ）」を参照）。
- 証明書を使用する RSA シグニチャを使って IKE 交換がピア間で実行されていることを確認する（証明書を使用すると、RSA シグニチャ ベースの IKE ネゴシエーション中にピアの公開キーが交換されます）。IKE 交換が実行されるようにするには、RSA 暗号化ナンスによる高プライオリティのポリシーと、RSA シグニチャによる低プライオリティのポリシーの 2 つのポリシーを指定します。RSA シグニチャは IKE ネゴシエーションが実行されるときに初めて使用されます。これは、各ピアに他のピアの公開キーがまだないためです。公開キーが交換されることで、以後の IKE ネゴシエーションで RSA 暗号化ナンスを使用できるようになります。この方法では、CA サポートをあらかじめ設定しておく必要があります。

RSA 暗号化ナンスでは IKE ネゴシエーションを否認できます。ただし、RSA シグニチャとは異なり、リモート ピアと IKE ネゴシエーションを実行したことを第三者に対して証明はできません。

事前共有キー

事前共有キーの概要

事前共有キーは、大規模なセキュア ネットワークでは、成長するネットワークにうまく対応できないため、適していません。ただし、RSA シグニチャのように CA を使用する必要がないため、10 ノード未満の規模の小さいネットワークではセットアップが簡単です。また、事前共有キーによる認証に比べ、RSA シグニチャによる認証の方が安全です。

（注） RSA 暗号化を設定し、シグニチャ モードがネゴシエーションされ、シグニチャ モードに証明書が使用されると、ピアはシグニチャと暗号キーを要求します。基本的にルータは、コンフィギュレーションでサポートされているできる限り多くのキーを要求します。RSA 暗号化が設定されていない場合は、ルータはシグニチャ キーだけを要求します。

事前共有キーの ISAKMP ID の設定

IKE ポリシーで事前共有キーを使用するピアそれぞれについて ISAKMP ID を設定する必要があります。

2 つのピアが IKE を使って IPsec SA を確立する場合、各ピアが自分の ID をもう一方のピア（リモート ピア）に送信します。各ピアは、ルータの ISAKMP ID の設定に従い、ホスト名または IP アドレスを送信します。

デフォルトでは、ピアの ISAKMP ID はピアの IP アドレスになっています。必要に応じて ID をピアのホスト名に変更します。一般的に、すべてのピアの ID は同じ設定（すべてのピアで IP アドレスを設定するか、すべてのピアでホスト名を設定）にします。お互いの識別にホスト名を使うピアと IP アドレスを使うピアが混在していると、リモート ピアの ID が識別されない場合にドメイン ネーム システム（DNS）lookup で ID を解決できなくなり、IKE ネゴシエーションが失敗することがあります。

マスク事前共有キー

マスク事前共有キーを使用すると、認証レベルが同じリモートユーザのグループで、IKE事前共有キーを共有できます。IKE認証を実行するには、リモートピアの事前共有キーと、ローカル ピアの事前共有キーが一致している必要があります。

マスク事前共有キーは通常、アウトオブバンドの安全なチャネル経由で配信されます。リモート ピアとローカル ピアが通信する場合、IKE 事前共有キーが設定されているリモート ピアとローカル ピアとの間で、IKE SA を確立できます。

mask キーワードの指定を **crypto isakmp key** コマンドで行う場合、サブネットアドレスを使用するかどうかはユーザーが決定します。使用すると、より多くのピアとの間で同じキーを共有できます。つまり、事前共有キーが 2 人のユーザ間の使用に制限されないということです。

（注） サブネット アドレスとして 0.0.0.0 の使用は推奨しません。この設定ではグループで事前共有キーを保持できるため（すべてのピアが同じグループ キーを持つことが可能）、ユーザ認証のセキュリティが低下するからです。

特定の IPsec ピアの Xauth の無効化

静的 IPsec ピアの拡張認証（Xauth）を無効にすると、ルータで Xauth 情報（ユーザ名とパスワード）が表示されなくなります。

IKE モード設定

Internet Engineering Task Force（IETF）によって定義されているように、IKE モード コンフィギュレーションでは、ゲートウェイにより、IP アドレス（およびその他のネットワーク レベルの設定）を、IKEネゴシエーションの一環で、クライアントにダウンロードできます。このエクスチェンジを使用することで、IP アドレスはゲートウェイによって IKE クライアントに渡され、IPsec でカプセル化された「内部」IP アドレスとして使用されます。この方式では、IPsec ポリシーと一致する可能性のある、クライアントの既知の IP アドレスが渡されます。

ダイナミック IP アドレスと会社のゲートウェイが設定されたリモート アクセス クライアント間に IPsec VPN を実装するには、各クライアントが認証された後、拡張可能な IPsec ポリシーをゲートウェイでダイナミックに管理する必要があります。IKEモードコンフィギュレーションにより、各クライアントの IP アドレスに関係なく、非常に規模の大きいクライアント群に対して拡張可能なポリシーをゲートウェイでセットアップできます。

IKE モード コンフィギュレーションには次の 2 つのタイプがあります。

- ゲートウェイ始動：ゲートウェイがクライアントでコンフィギュレーション モードを開始する。クライアントが応答すると、IKEが送信者のIDを変更し、メッセージが処理され、クライアントが応答を受信します。
- クライアント始動：クライアントがゲートウェイでコンフィギュレーション モードを開始する。クライアントに割り当てた IP アドレスでゲートウェイが応答します。

IPsec VPN 用 IKE の設定方法

IPsec 実装で IKE を使用しない場合は、**no crypto isakmp** コマンドを使ってすべての IPsec ピアの IKE を無効にし、この章の残りは実行せずに、IPsec VPN を開始します。

IKE はデフォルトでイネーブルになっています。各インターフェイスについて IKE を個別にイネーブルにする必要はなく、ルータのすべてのインターフェイスについてグローバルにイネーブルになっています。

（注） セキュリティに対する脅威は、脅威からの保護に役立つ暗号化技術と同様に絶え間なく変化しています。最新のシスコの暗号化に関する推奨事項については、『Next Generation Encryption』（NGE）ホワイト ペーパーを参照してください。

IPsec ピアの認証、IPsec SA のネゴシエーション、IPsec キーの確立を実行するには、次の作業を実行します。

トラブルシューティングのヒント

- **clear crypto sa** EXEC コマンドを使用して、IPsec SA を消去（および再初期化）します。

パラメータを指定せずに **clear crypto sa** コマンドを使用すると、SA データベースの内容が完全に消去されるので、アクティブなセキュリティセッションが消去されます。SA データベースのサブセットだけを消去するには、**peer**、**map**、または **entry** キーワードも指定します。詳細については、『Cisco IOS Security Command Reference』の **clear crypto sa** コマンドを参照してください。

- デフォルトポリシーおよび設定されているポリシーのデフォルト値は、**show running-config** コマンドの発行時には設定に表示されません。デフォルトポリシーおよび設定されているポリシーのデフォルト値を確認するには、**show crypto isakmp policy** コマンドを使用してください。
- 使用しているハードウェアがサポートしていない IPsec トランスフォームまたは IKE 暗号化方式はすべて無効にしてください。無効にしておくと、ピアとのネゴシエーションのときに常に無視されます。

ハードウェアがサポートしていない IPsec トランスフォームまたは IKE 暗号化方式を入力すると、警告メッセージが表示されます。この警告メッセージはブート時にも表示されます。暗号化カードを挿入すると、現在の設定がスキャンされます。ハードウェアがサポートしていない IPsec トランスフォームまたは IKE 暗号化方式が検出されると、警告メッセージが表示されます。

次の作業

IKE ポリシーで指定した認証方式（RSA シグニチャ、RSA 暗号化ナンス、事前共有キー）によっては、IKE および IPsec が IKE ポリシーを正常に使用できるように、特定の設定作業を追加で実行する必要があります。これらの追加作業の完了に関する詳細については、IKE 認証の設定 （2855 ページ） を参照してください。

AES ベースのトランスフォーム セットを設定する方法については、モジュール「Configuring Security for VPNs with IPsec」を参照してください。

IKE 認証の設定

認証方式を指定（またはデフォルト方式を設定）した IKE ポリシーを少なくとも 1 つ作成したら、認証方式を設定する必要があります。認証方式を正常に設定しなければ、IPsec が IKE ポリシーを使用できません。

（注） IKE 認証を設定する前に、認証方式を指定した（またはデフォルトの RSA シグニチャにした）IKE ポリシーを最低 1 つは設定しておく必要があります。

IKE 認証を設定するには、状況に応じて次の作業のいずれかを実行する必要があります。

前提条件

認証方式を指定した（またはデフォルトの RSA シグニチャを設定した）IKE ポリシーを最低 1 つは設定しておく必要があります。

RSA 暗号化ナンスの RSA キーの手動設定

（注） この作業を実行するのは、CA を使用していない場合だけです。

RSA キーを手動で設定するには、IKE ポリシーで RSA 暗号化ナンスを使用する IPsec ピアそれぞれについて、この作業を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **crypto key generate rsa**{**general-keys**} | **usage-keys**} [**label** *key-label*] [**exportable**] [**modulus** *modulus-size*]
4. **crypto key generate ec keysize** [**256** | **384**] [**label** *label-string*]
5. **exit**
6. **show crypto key mypubkey rsa**
7. **configure terminal**

8. **crypto key pubkey-chain rsa**
9. 次のいずれかを実行します。
   - **named-key** *key-name* [**encryption** | **signature**]
   - **addressed-key** *key-address* [**encryption** | **signature**]
10. **address** *ip-address*
11. **key-string** key-string
12. **quit**
13. IKE ポリシーで RSA 暗号化ナンスを使用するピアそれぞれについて上記の手順を繰り返します。
14. **exit**
15. **exit**
16. **show crypto key pubkey-chain rsa** [**name** *key-name* | **address** *key-address*]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードを有効にします。プロンプトが表示されたらパスワードを入力します。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**crypto key generate rsa**{**general-keys**} | **usage-keys**} [**label** *key-label*] [**exportable**] [**modulus** *modulus-size*] 例： `Router(config)# crypto key generate rsa general-keys modulus 360`	RSA キーを生成します。 • *key-label* 引数を指定していない場合、ルータの完全修飾ドメイン名（FQDN）であるデフォルト値が使用されます。
ステップ 4	**crypto key generate ec keysize** [**256** | **384**] [**label** *label-string*] 例： `Router(config)# crypto key generate ec keysize 256 label Router_1_Key`	EC キーを生成します。 • 256 キーワードは、キーのサイズを 256 ビットに指定します。 • 384 キーワードは、キーのサイズを 384 ビットに指定します。 • **label** キーワードと *label-string* 引数を使用して、EC キーにラベルを指定できます。 （注） ラベルを指定しない場合は、FQDN の値が使用されます。

	コマンドまたはアクション	目的
ステップ 5	**exit** 例： `Router(config)# exit`	（任意）グローバル コンフィギュレーション モードを終了します。
ステップ 6	**show crypto key mypubkey rsa** 例： `Router# show crypto key mypubkey rsa`	（任意）生成された RSA 公開キーを表示します。
ステップ 7	**configure terminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードに戻ります。
ステップ 8	**crypto key pubkey-chain rsa** 例： `Router(config)# crypto key pubkey-chain rsa`	公開キー コンフィギュレーション モード（他のデバイスの RSA 公開キーの手動設定が可能）にします。

ステップ 9	次のいずれかを実行します。
	• **named-key** *key-name* [**encryption** | **signature**]
	• **addressed-key** *key-address* [**encryption** | **signature**]
	例：
	`Router(config-pubkey-chain)# named-key otherpeer.example.com`
	例：
	`Router(config-pubkey-chain)# addressed-key 10.1.1.2 encryption`
		どのリモート ピアの RSA 公開キーを指定するのかを示し、公開キー コンフィギュレーション モードを開始します。
		• リモートピアが ISAKMP ID にホスト名を使用している場合は、**named-key** コマンドを使用し、リモートピアの FQDN（somerouter.example.com など）を *key-name* に指定します。
		• リモートピアが ISAKMP ID に IP アドレスを使用している場合は、**addressed-key** コマンドを使用し、リモートピアの IP アドレスを *key-address* に指定します。

ステップ 10	**address** *ip-address* 例： `Router(config-pubkey-key)# address 10.5.5.1`	リモート ピアの IP アドレスを指定します。 • **named-key** コマンドを使用するのは、このコマンドを使用してピアの IP アドレスを指定する必要がある場合です。

ステップ 11	**key-string** key-string
	例：
	`Router(config-pubkey-key)# key-string`
	例：
	`Router(config-pubkey)# 00302017 4A7D385B 1234EF29 335FC973`
	例：
		リモート ピアの RSA 公開キーを指定します。
		• （このキーは、リモート ルータの RSA キーが生成されたときに、リモート ピアの管理者が確認したキーです）

	コマンドまたはアクション	目的

	`Router(config-pubkey)# 2DD50A37 C4F4B0FD 9DADE748 429618D5`
	例：
	`Router(config-pubkey)# 18242BA3 2EDFBDD3 4296142A DDF7D3D8`
	例：
	`Router(config-pubkey)# 08407685 2F2190A0 0B43F1BD 9A8A26DB`
	例：
	`Router(config-pubkey)# 07953829 791FCDE9 A98420F0 6A82045B`
	例：
	`Router(config-pubkey)# 90288A26 DBC64468 7789F76E EE21`	

ステップ 12	**quit** **例：** `Router(config-pubkey-key)# quit`	公開キー チェーン コンフィギュレーション モードに戻ります。
ステップ 13	IKE ポリシーで RSA 暗号化ナンスを使用するピアそれぞれについて上記の手順を繰り返します。	—
ステップ 14	**exit** **例：** `Router(config-pubkey-key)# exit`	グローバル コンフィギュレーション モードに戻ります。
ステップ 15	**exit** **例：** `Router(config)# exit`	特権 EXEC モードに戻ります。
ステップ 16	**show crypto key pubkey-chain rsa** [**name** *key-name* | **address** *key-address*] **例：** `Router# show crypto key pubkey-chain rsa`	（任意）ルータに保存されているすべての RSA 公開キーのリスト、またはルータに保存されている特定の RSA キーの詳細を表示します。

事前共有キーの設定

事前共有キーを設定するには、IKEポリシーで事前共有キーを使用するピアそれぞれについて以下の手順を実行します。

（注） 事前共有は、規模が拡大しているネットワークではうまく拡張できない。マスク事前共有キーには次の制約事項があります。

- 同じ事前共有キーのすべての IPsec ピアを設定するまで、IPsec ピア間に SA を確立できない。
- マスク事前共有キーは、さまざまなレベルの認可を要求しているリモートユーザごとに、明確に異なっている必要がある。認証のレベルごとに新しい事前共有キーを設定し、適切なキーを適切なユーザに割り当てる必要があります。正しく設定しないと、認証を受けていない人物が、保護されているデータに対するアクセス権を取得する場合があります。

手順の概要

1. **enable**
2. **configure terminal**
3. **crypto isakmp identity** {**address** | **dn** | **hostname**}
4. **ip host** *hostname address1* [*address2...address8*]
5. 次のいずれかを実行します。
   - **crypto isakmp key** *keystring* **address** *peer-address* [**mask**] [**no-xauth**]
   - **crypto isakmp key** *keystring* **hostname** *hostname* [**no-xauth**]
6. 次のいずれかを実行します。
   - **crypto isakmp key** *keystring* **address** *peer-address* [**mask**] [**no-xauth**]
   - **crypto isakmp key** *keystring* **hostname** *hostname* [**no-xauth**]
7. IKEポリシーで事前共有キーを使用するピアそれぞれについて以上の手順を繰り返します。

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**crypto isakmp identity** {**address**	**dn**	**hostname**} 例： `Router(config)# crypto isakmp identity address`	ローカル ピアの IP アドレスまたは認定者名（DN）ホスト名を使ってピアの ISAKMP ID を指定します。 • **address**：通常は、ピアが IKE ネゴシエーションに使用するインターフェイスが 1 つだけ（したがって IP アドレスが 1 つだけ）で、IP アドレスがわかっている場合に使用します。

	コマンドまたはアクション	目的
		• **dn**：通常は、IKE 処理中、ISAKMP ID としてルータ証明書の DN が指定および選択される場合に使用します。dn キーワードは、証明書ベースの認証にだけ使用します。 • **hostname**：IKE ネゴシエーションに使用するインターフェイスがピアに複数ある場合か、（IP アドレスのダイナミック割り当てなどで）インターフェイスの IP アドレスが不明の場合に使用する必要があります。
ステップ 4	**ip host** *hostname address1* [*address2...address8*] 例： `Router(config)# ip host RemoteRouter.example.com 192.168.0.1`	ホスト名を使ってローカル ピアの ISAKMP ID を指定した場合、すべてのリモート ピアについて、ピアのホスト名を IP アドレスにマップします （ホスト名または IP アドレスが DNS サーバでマップ済みの場合はこの手順は不要）。

ステップ 5	次のいずれかを実行します。
	• **crypto isakmp key** *keystring* **address** *peer-address* [**mask**] [**no-xauth**]
	• **crypto isakmp key** *keystring* **hostname** *hostname* [**no-xauth**]
	例：
	`Router(config)# crypto isakmp key sharedkeystring address 192.168.1.33 no-xauth`
	例：
	`Router(config) crypto isakmp key sharedkeystring hostname RemoteRouter.example.com`
		特定のリモート ピアで使用する共有キーをローカル ピアで指定します。
		• リモートピアで ISAKMP ID を IP アドレスで指定した場合は、この手順で **address** キーワードを使用し、それ以外の場合は、この手順で **hostname** キーワードを使用します。
		• **no-xauth--**：ルータがピアに Xauth 情報のプロンプトを出力しないようにします。
		（注） 事前共有キーは、IKE メイン モードでの事前共有キー認証の設計に従い、ピアの IP アドレスを基にしている必要があります。事前共有キー認証の ID としてホスト名を送信できますが、キーはピアの IP アドレスを基に検索されます。（IP アドレスに基づいて）キーが検索されなかった場合、ネゴシエーションが失敗します。

ステップ 6	次のいずれかを実行します。 • **crypto isakmp key** *keystring* **address** *peer-address* [**mask**] [**no-xauth**] • **crypto isakmp key** *keystring* **hostname** *hostname* [**no-xauth**] 例：	ローカル ピアで使用する共有キーをリモート ピアで指定します。 • これは、ローカル ピアで指定したキーと同じキーです。 • ローカルピアで ISAKMP ID を IP アドレスで指定した場合は、この手順で **address** キーワード

	コマンドまたはアクション	目的

	`Router(config) crypto isakmp key sharedkeystring address 10.0.0.1`
	例：
	`Router(config) crypto isakmp key sharedkeystring hostname LocalRouter.example.com`
		を使用し、それ以外の場合は、この手順で **hostname** キーワードを使用します。

ステップ 7	IKE ポリシーで事前共有キーを使用するピアそれぞれについて以上の手順を繰り返します。	--

IKE モード コンフィギュレーションの設定

（注） IKE モード コンフィギュレーションには次の制約事項があります。

手順の概要

1. **enable**
2. **configure terminal**
3. **ip local pool** *pool-name start-addr end-addr*
4. **crypto isakmp client configuration address-pool local** *pool-name*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ip local pool** *pool-name start-addr end-addr* 例： `Router(config)# ip local pool pool1 172.16.23.0 172.16.23.255`	アドレス一式が定義されている既存のローカル アドレス プールを定義します。
ステップ 4	**crypto isakmp client configuration address-pool local** *pool-name* 例： `Router(config)# crypto isakmp client configuration address-pool local pool1`	IKE コンフィギュレーションのローカル アドレス プールを参照します。

IPsec SA ネゴシエーションのための IKE 暗号マップの設定

（注） セキュリティに対する脅威は、脅威からの保護に役立つ暗号化技術と同様に絶え間なく変化しています。最新のシスコの暗号化に関する推奨事項については、『Next Generation Encryption』（NGE）ホワイト ペーパーを参照してください。

手順の概要

1. **enable**
2. **configure terminal**
3. **crypto map** *tag sequence* **ipsec-isakmp**
4. **set pfs** {**group1** | **group2** | **group5** | **group14** | **group15** | **group16**}

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**crypto map** *tag sequence* **ipsec-isakmp** 例： `Router(config)# crypto map example 1 ipsec-ipsec-isakmp`	クリプトマップを指定し、クリプトマップ コンフィギュレーション モードを開始します。 • *tag* 引数には、暗号マップを指定します。 • *sequence* 引数には、暗号マップ エントリに挿入するシーケンスを指定します。 • **ipsec-isakmp** キーワードには、IKEv1 を使用する IPsec（ISAKMP）を指定します。
ステップ 4	**set pfs** {**group1**	**group2**	**group5**	**group14**	**group15**	**group16**} 例： `Router(config-isakmp)# set pfs 14`	IPSec SA ネゴシエーションの DH グループ ID を指定します。 • デフォルトではDHグループ1が使用されます。 • **group1**：768 ビット DH（非推奨） • **group2**：1024 ビット DH（非推奨） • **group5**：1536 ビット DH（非推奨）

	コマンドまたはアクション	目的
		• **group14**：2048 ビット DH グループを指定します。 • **group15**：3072 ビット DH グループを指定します。 • **group16**：4096 ビット DH グループを指定します。 選択するグループは、ネゴシエーション中の IPsec キーを保護するため、十分強力（十分なビット数がある）である必要があります。一般に受け入れられているガイドラインでは、2013 年以降（2030 年まで）は 2048 ビット グループの使用が推奨されています。このガイドラインを満たすには、いずれかの group14 を選択してください。より長期にわたるセキュリティ方式が必要であっても、楕円曲線暗号の使用が推奨されますが、group15 と group16 も検討できます。

IKE コンフィギュレーションの設定例

例：IKE ポリシーの作成

このセクションには、AES IKE ポリシーおよび 3DES IKE ポリシーの設定方法を示す次の例が含まれています。

（注） シスコでは、3DES の使用は推奨していません。代わりに、AES を使用してください。シスコの暗号化に関する最新の推奨事項の詳細は、『Next Generation Encryption』（NGE）ホワイトペーパーを参照してください。

例：3DES IKE ポリシーの作成

この例では、2 つの IKE ポリシー（最大のプライオリティとして policy 15、次のプライオリティとして policy 20）を作成し、最小のプライオリティとして既存のデフォルト プライオリティを使用します。また、IP アドレスが 192.168.224.33 のリモート ピアに、policy 20 で使用する事前共有キーも作成します。

```
crypto isakmp policy 15
 encryption 3des
 hash md5
 authentication rsa-sig
 group 2
```

```
 lifetime 5000
!
crypto isakmp policy 20
 authentication pre-share
 lifetime 10000
!
crypto isakmp key 1234567890 address 192.168.224.33
```

この例では、暗号化 DES のポリシーのデフォルト値は、暗号化アルゴリズム パラメータのデフォルト値のため、記述した設定には表示されません。

この設定で **show crypto isakmp policy** コマンドを発行すると、出力は次のようになります。

```
Protection suite priority 15
encryption algorithm:3DES - Triple Data Encryption Standard (168 bit keys)
hash algorithm:Message Digest 5
authentication method:Rivest-Shamir-Adleman Signature
Diffie-Hellman group:#2 (1024 bit)
lifetime:5000 seconds, no volume limit
Protection suite priority 20
encryption algorithm:DES - Data Encryption Standard (56 bit keys)
hash algorithm:Secure Hash Standard
authentication method:preshared Key
Diffie-Hellman group:#1 (768 bit)
lifetime:10000 seconds, no volume limit
Default protection suite
encryption algorithm:DES - Data Encryption Standard (56 bit keys)
hash algorithm:Secure Hash Standard
authentication method:Rivest-Shamir-Adleman Signature
Diffie-Hellman group:#1 (768 bit)
lifetime:86400 seconds, no volume limit
```

ライフタイムに「no volume limit」と出力されていますが、time ライフタイム（86,400 秒など）だけは設定できます。volume limit ライフタイムは設定できません。

例：AES IKE ポリシーの作成

次に、**show running-config** コマンドの出力例を示します。この例では、AES 256 ビット キーが有効になっています。

```
Current configuration : 1665 bytes
!
version 12.2
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname "Router1"
!
!
ip subnet-zero
!
!
no ip domain lookup
!
ip audit notify log
ip audit po max-events 100
!
crypto isakmp policy 10
 encryption aes 256
```

```
 authentication pre-share
 lifetime 180
crypto isakmp key cisco123 address 10.0.110.1
!
!
crypto ipsec transform-set aesset esp-aes 256 esp-sha-hmac
 mode transport

.
.
.
```

例：IKE 認証の設定

次の例は、2 つの IPsec ピアの RSA 公開キーを手動で指定する方法を示しています。10.5.5.1 のピアは汎用キーを使用し、もう一方のピアは特殊な用途のキーを使用しています。

```
crypto key pubkey-chain rsa
 named-key otherpeer.example.com
 address 10.5.5.1
 key-string
 005C300D 06092A86 4886F70D 01010105
 00034B00 30480241 00C5E23B 55D6AB22
 04AEF1BA A54028A6 9ACC01C5 129D99E4
 64CAB820 847EDAD9 DF0B4E4C 73A05DD2
 BD62A8A9 FA603DD2 E2A8A6F8 98F76E28
 D58AD221 B583D7A4 71020301 0001
 quit
 exit
 addressed-key 10.1.1.2 encryption
 key-string
 00302017 4A7D385B 1234EF29 335FC973
 2DD50A37 C4F4B0FD 9DADE748 429618D5
 18242BA3 2EDFBDD3 4296142A DDF7D3D8
 08407685 2F2190A0 0B43F1BD 9A8A26DB
 07953829 791FCDE9 A98420F0 6A82045B
 90288A26 DBC64468 7789F76E EE21
 quit
 exit
 addressed-key 10.1.1.2 signature
 key-string
 0738BC7A 2BC3E9F0 679B00FE 53987BCC
 01030201 42DD06AF E228D24C 458AD228
 58BB5DDD F4836401 2A2D7163 219F882E
 64CE69D4 B583748A 241BED0F 6E7F2F16
 0DE0986E DF02031F 4B0B0912 F68200C4
 C625C389 0BFF3321 A2598935 C1B1
 quit
 exit
 exit
```

次の作業

IKE ネゴシエーションを正常に設定したら、IPsec の設定を開始します。このタスクの実行についての詳細は、モジュール「Configuring Security for VPNs with IPsec」を参照してください。

その他の参考資料

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『Cisco IOS Master Commands List, All Releases』
セキュリティ コマンド：コマンド構文の詳細、コマンド モード、コマンド履歴、デフォルト設定、使用上の注意事項、および例	• 『Cisco IOS Security Command Reference Commands A to C』 • 『Cisco IOS Security Command Reference: Commands D to L』 • 『Cisco IOS Security Command Reference: Commands M to R』 • 『Cisco IOS Security Command Reference Commands S to Z』
IPsec の設定	『Configuring Security for VPNs with IPsec』
IKE バージョン 2	「Configuring Internet Key Exchange Version 2 and FlexVPN」
CA から証明書を取得するように RSA キーを設定	PKI 内での RSA キーの展開
Suite-B の ESP トランスフォーム	『Configuring Security for VPNs with IPsec』
Suite-B 整合性アルゴリズム タイプのトランスフォームの設定	「Configuring Internet Key Exchange Version 2 and FlexVPN」
IPsec SA ネゴシエーションでの Suite-B の Elliptic Curve Diffie-Hellman（ECDH）のサポート	「Configuring Internet Key Exchange Version 2 and FlexVPN」
PKI の証明書登録のための Suite-B サポート	「Configuring Certificate Enrollment for a PKI」
推奨される暗号化アルゴリズム	『Next Generation Encryption』

標準

標準	タイトル
なし	--

MIB

MIB	MIB のリンク
なし	選択したプラットフォーム、Cisco IOS ソフトウェア リリース、およびフィーチャセットの MIB を検索してダウンロードする場合は、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

RFC

RFC	タイトル
RFC 2408	『Internet Security Association and Key Management Protocol (ISAKMP)』
RFC 2409	『The Internet Key Exchange (IKE)』
RFC 2412	『The OAKLEY Key Determination Protocol』

シスコのテクニカル サポート

説明	リンク
右の URL にアクセスして、シスコのテクニカル サポートを最大限に活用してください。これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

IPsec VPN の IKE 設定の機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだ

けを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *264 : IPsec VPN の IKE* 設定の機能情報

機能名	リリース	機能情報
スタティック IPsec ピアの拡張認証を無効にする機能	12.2(4)T	この機能により、ルータ間 IPsec の事前共有キー設定中に Xauth を無効にできます。したがって、ルータによりピアのユーザ名およびパスワードは要求されません。これらは、VPN クライアント対 Cisco IOS IPsec の Xauth が発生するときに転送されます。 この機能により、次のコマンドが変更されました。**crypto isakmp key.**
Advanced Encryption Standard（AES）	12.2(8)T	この機能により、新しい暗号化規格 AES に対するサポートが追加されます。AES は、DES の後継として開発された IPsec および IKE のプライバシー トランスフォームです。 この機能により、次のコマンドが変更されました。**crypto ipsec transform-set, encryption (IKE policy), show crypto ipsec transform-set, crypto ipsec transform-set, show crypto isakmp policy.**
SEAL 暗号化	12.3(7)T	この機能により、IPsec での SEAL 暗号化に対するサポートが追加されました。 この機能により、次のコマンドが変更されました。**crypto ipsec transform-set.**
IOS SW の暗号化での Suite-B のサポート	15.1(2)T	Cisco IOS で、パケット データの認証および IKE プロトコルの整合性確認メカニズムの検証に使用される SHA-2 ファミリ（HMAC バリアント）のハッシュ アルゴリズムに、Suite-B のサポートが追加されました。HMAC は、追加レベルのハッシュを提供するバリアントです。この機能により、IPsec SA ネゴシエーションに Elliptic Curve Diffie-Hellman（ECDH）のサポートも追加されました。 Cisco IOS での Suite-B サポートについての詳細は、「Configuring Security for VPNs with IPsec」機能モジュールを参照してください。 この機能により、次のコマンドが変更されました。**authentication, crypto key generate ec keysize, crypto map, group, hash, set pfs.**

第 197 章

「Call Admission Control for IKE」

IKE 用コール アドミッション制御機能は、Cisco IOS ソフトウェアでのインターネット キー エクスチェンジ（IKE）プロトコルに対し、コールアドミッション制御（CAC）を適用したものです。CAC は、IKE と IPsec セキュリティ アソシエーション（SA）（つまり CAC へのコール）をルータが同時に確立できる数を制限します。

IKE 用コール アドミッション制御に関する前提条件

- このデバイスで IKE を設定します。

IKE 用コール アドミッション制御に関する情報

IKE セッション

デバイスが別のデバイスとの間で確立できるインターネット キー エクスチェンジ（IKE）セキュリティ アソシエーション（SA）の数を制限する方法には、次の 2 つがあります。

- **crypto call admission limit** コマンドを入力して、IKE SA の絶対制限値を設定します。設定された制限値に達すると、デバイスは新しい IKE SA 要求をドロップします。
- **call admission limit** コマンドを入力して、システムリソース制限値を設定します。チャージ単位で設定されたレベルのシステム リソースが使用されている場合、デバイスは新しい IKE SA 要求をドロップします。

コール アドミッション制御（CAC）は新しい SA のみ（つまり、ピア間に SA がまだ存在しないとき）に適用されます。既存の SA を保存するためにあらゆる処置が行われます。新しい SA 要求が拒否されるのは、システム リソースが不足しているか、あるいは設定された IKE SA 制限値に達したことが原因です。

セキュリティ アソシエーション制限

SA（セキュリティ アソシエーション）は、2 つ以上のエンティティがセキュリティ サービスを使用して特定のデータ フローのために安全に通信する方法を記述したものです。IKE は接続のパラメータを識別するために、必ず SA を使用します。IKE では、独自に SA をネゴシエーションして確立できます。IKE SA は、IKE だけで使用され、双方向です。IKE SA は、IPsec を制限できません。

IKE は、ユーザが設定した SA 制限値に基づいて SA 要求をドロップします。IKE SA 制限値を設定するには、**crypto call admission limit** コマンドを入力します。ピア ルータから新しい SA 要求があると、IKE はアクティブな IKE SA の数とネゴシエーション中の SA の数が、設定された SA 制限値を満たしているか、超えているかを判別します。この数が制限値より大きい、または等しい場合、新しい SA 要求は拒否され、syslog が生成されます。このログには、SA 要求の送信元および宛先 IP アドレスが含まれます。

crypto call admission limit コマンドの **ipsec sa** *number* および **ike sa** *number* キーワードと引数のペアには、確立された IPsec SA と IKE SA の数の制限値を設定します。

ネゴシエーション時の IKE 接続数の制限

Cisco リリースに基づいて、デバイスで設定できる内部 IKE ネゴシエーション接続の数を制限できます。このタイプの IKE 接続は、認証および実際の確立前のアグレッシブ モード IKE SA またはメイン モード IKE SA を表します。IKEv2 の最大内部ネゴシエーション CAC のデフォルト値は 40 です。

crypto call admission limit ike in-negotiation-sa *number* コマンドを使用すると、IKE が新しい SA 要求の拒否を開始する前にデバイスが確立できるインターネット キー エクスチェンジ（IKE）と IPsec セキュリティ アソシエーション（SA）の最大数を指定できます。

crypto call admission limit コマンドの **all in-negotiation-sa** *number* と **ike in-negotiation-sa** *number* のキーワードと引数のペアは、ネゴシエーション時のすべての SA とネゴシエーション時の IKE SA を制限します。

システム リソースの使用状況

ルータの CPU サイクルまたはメモリ バッファが不足した場合に、IKE がそのことを認識できるように、CAC はグローバル情報リソース モニタをポーリングします。システム リソースの使用量レベルを表す制限値を 1 ～ 100000 までの範囲で設定できます。設定レベルのリソースが使用されると、IKE は SA 要求を廃棄します（新たに受け入れません）。システムリソース使用量の制限を設定するには、**call admission limit** コマンドを入力します。

新しい着信 SA 要求ごとに、ルータにかかる現在の負荷が数値に変換され、システムリソースの使用量レベルが表示されます。また、この数値と、**call admission limit** コマンドによって設定されたリソース制限値が比較されます。現在の負荷が、設定されたリソース制限値を超えると、IKE は新しい SA 要求を廃棄します。ルータの負荷には、アクティブな SA、CPU の使用量、および考慮される SA 要求が含まれます。

call admission load コマンドを実行すると、現在のシステムリソース使用量の倍率を表す 0 ～ 1000 の乗数値と 1 ～ 32 秒の負荷メトリックのポーリングレートが設定されます。システム リソースの使用量レベルの数値は、（倍率 * 現在のシステム リソースの使用量）/ 100 という式で計算されます。Cisco Technical Assistance Center（TAC）技術者からの指示がないかぎり、**call admission load** コマンドを使用することは推奨しません。

IKE 用コール アドミッション制御の設定方法

IKE セキュリティ アソシエーション制限の設定

IKE SA の絶対制限値を設定するには、次の作業を実行します。制限値に達すると、ルータは新しい IKE SA 要求を廃棄します。

手順の概要

1. **enable**
2. **configure terminal**
3. **crypto call admission limit** {**all in-negotiation-sa** *number* | **ipsec sa** *number* | **ike** {**in-negotiation-sa** *number* | **sa** *number*}}
4. **exit**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**crypto call admission limit** {**all in-negotiation-sa** *number*	**ipsec sa** *number*	**ike** {**in-negotiation-sa** *number*	**sa** *number*}} 例：	ネゴシエーション時の IKE SA の最大数、合計 SA 数、または IKE が新しい SA 要求を拒否し始める前に確立できる IKE SA またはIPsec SA の最大数を指定します。IKEv1 の推奨 CAC 値は 40 です。

	コマンドまたはアクション	目的
	`Router(config)# crypto call admission limit ike sa 25`	
ステップ 4	**exit** 例： `Router(config)# exit`	グローバル コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

IKEv2 セキュリティ アソシエーション制限の設定

IKEv2 SA の絶対制限値を設定するには、次の作業を実行します。制限値に達すると、ルータは新しい IKE SA 要求を廃棄します。

手順の概要

1. **enable**
2. **configure terminal**
3. **crypto ikev2 limit** {**max-in-negotiation-sa limit** *number* | **max-sa limit** *number*}
4. **exit**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**crypto ikev2 limit** {**max-in-negotiation-sa limit** *number*	**max-sa limit** *number*} 例： `Router(config)# crypto ikev2 limit max-in-negotation-sa 5000`	コールアドミッション制御を次のようにイネーブルにします。 • max-in-negotation-sa limit：ノード上での IKEv2 SA のネゴシエーションの受け入れの合計数を制限します。 • max-sa limit：ノード上での IKEv2 SA の合計数を制限します。
ステップ 4	**exit** 例：	グローバル コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

	コマンドまたはアクション	目的
	`Router(config)# exit`	

システム リソース制限の設定

システム リソースの制限値を設定するには、次の作業を実行します。負荷単位で設定されたレベルのシステム リソースが使用されている場合、ルータは新しい IKE SA 要求を廃棄します。

手順の概要

1. **enable**
2. **configure terminal**
3. **call admission limit** *charge*
4. **exit**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**call admission limit** *charge* 例： `Router(config)# call admission limit 1000`	システム リソースを使用する場合、システム リソースのレベルを設定して、IKE による新しい SA 要求の受け入れを停止します。 • *charge*：有効な値は 1 ～ 100000 です。
ステップ 4	**exit** 例： `Router(config)# exit`	グローバル コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

IKE の CAC の設定確認

IKE 設定の CAC を確認するには、次の手順を実行します。

手順の概要

1. **show call admission statistics**
2. **show crypto call admission statistics**

手順の詳細

ステップ 1 **show call admission statistics**

このコマンドを使用して、グローバル CAC コンフィギュレーション パラメータおよび CAC の動作をモニタします。

例：

```
Router# show call admission statistics
Total Call admission charges: 82, limit 1000
Total calls rejected 1430, accepted 0
Load metric: charge 82, unscaled 82%
```

ステップ 2 **show crypto call admission statistics**

このコマンドを使用して、暗号 CAC 統計情報をモニタします。

例：

```
Router# show crypto call admission statistics
----------------------------------------------------------------------
               Crypto Call Admission Control Statistics
----------------------------------------------------------------------
System Resource Limit:      111 Max IKE SAs:     0 Max in nego:  1000
Total IKE SA Count:           0 active:          0 negotiating:     0
Incoming IKE Requests:        0 accepted:        0 rejected:        0
Outgoing IKE Requests:        0 accepted:        0 rejected:        0
Rejected IKE Requests:        0 rsrc low:        0 Active SA limit: 0
                                                   In-neg SA limit: 0
IKE packets dropped at dispatch:        0
Max IPSEC SAs:   111
Total IPSEC SA Count:           0 active:          0 negotiating:     0
Incoming IPSEC Requests:        0 accepted:        0 rejected:        0
Outgoing IPSEC Requests:        0 accepted:        0 rejected:        0
Phase1.5 SAs under negotiation:         0
```

IKE 用コール アドミッション制御の設定例

IKE セキュリティ アソシエーション制限値の設定例

次の例では、IKE が新しい SA 要求を拒否し始めるまでの SA の最大値を 25 に指定する方法を示します。

```
Router(config)# crypto call admission limit ike sa 25
```

システム リソース制限値の設定例

次の例では、負荷単位で設定されたシステム リソースのレベルが 9000 に達したときに、IKE が SA 要求を廃棄するように指定する方法を示します。

```
Router(config)# call admission limit 9000
```

その他の参考資料

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『Cisco IOS Master Commands List, All Releases』
IKE の設定	「Configuring Internet Key Exchange for IPsec VPNs」
IKE コマンド	『*Cisco IOS Security Command Reference*』

標準

標準	タイトル
なし	--

MIB

MIB	MIB のリンク
なし	選択したプラットフォーム、Cisco ソフトウェア リリース、およびフィーチャ セットの MIB を検索してダウンロードする場合は、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

RFC

RFC	タイトル
RFC 2409	『*The Internet Key Exchange*』

シスコのテクニカル サポート

説明	リンク
右の URL にアクセスして、シスコのテクニカル サポートを最大限に活用してください。これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

IKE 用コール アドミッション制御の機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *265 : IKE* 用コール アドミッション制御の機能情報

機能名	リリース	機能情報
「Call Admission Control for IKE」	12.3(8)T 12.2(18)SXD1 12.4(6)T 12.2(33)SRA 12.2(33)SXH	IKE 用コール アドミッション制御機能は、Cisco IOS ソフトウェアでのインターネット キー エクスチェンジ（IKE）プロトコルに対し、コール アドミッション制御（CAC）を適用したものです。 この機能は、Cisco IOS Release 12.3(8)T で導入されました。 この機能は Cisco IOS Release 12.2(18)SXD1 に統合され、Cisco 6500 および Cisco 7600 ルータに実装されました。 Cisco IOS Release 12.4(6)T では、ネゴシエーション時の IKE 接続数の制限を設定する機能が追加されました。 この機能に関する詳細については、次の各項を参照してください。 次のコマンドが導入または変更されました。**call admission limit**、 **clear crypto call admission statistics**、 **crypto call admission limit**、 **show call admission statistics**、 **show crypto call admission statistics**。

機能名	リリース	機能情報
IKEv1 の強化	15.1(3)T	IKEv1 の強化機能とは、IKE 機能のコール アドミッション制御（CAC）に対して行われた拡張機能を表します。 この機能は、Cisco IOS Release 15.1(3)T で導入されました。 この機能に関する詳細については、次の各項を参照してください。 次のコマンドが導入または変更されました。**crypto call admission limit**、 **show crypto call admission statistics**。

第 198 章

証明書/ISAKMP プロファイルマッピング

証明書/ISAKMP プロファイルマッピング機能を使用すると、証明書内の任意のフィールドの内容に基づいて、ピアに Internet Security Association and Key Management Protocol（ISAKMP）プロファイルを割り当てることができます。また、この機能では、ISAKMP プロファイルに割り当てられたピアにグループ名を割り当てることもできます。

証明書/ISAKMP プロファイルマッピングの前提条件

- 証明書マップの設定を理解している必要があります。
- ISAKMP プロファイルの設定を理解している必要があります。

証明書/ISAKMP プロファイルマッピングの制約事項

証明書を交換しないで、Rivest、Shamir、Adelman（RSA）シグニチャまたは RSA 暗号化認証を使用する場合は、この機能を適用できません。ISAKMP ピアは、証明書を使用して RSA シグニチャまたは RSA 暗号化認証を実行するように設定する必要があります。

同じ認証局（CA）サーバに登録された 2 つのトラストポイントを使用する IPsec はサポートされません。2 つ以上の ISAKMP プロファイルがあり、各プロファイルが、同じ CA サーバに登録されているが異なるトラストポイントを持っている場合、応答側は最後のグローバル トラストポイントを選択します（トラストポイントは、グローバルに定義された順序と逆の順序で選択されます）。ピアが IPsec トンネルの確立を成功させるには、発信側が選択したトラストポ

イントは、応答側が選択したトラストポイントと一致する必要があります。トラストポイントが一致しない場合、他のすべての IPsec トンネルは、接続の確立に失敗します。

証明書/ISAKMP プロファイルマッピングに関する情報

証明書/ISAKMP プロファイルマッピングの概要

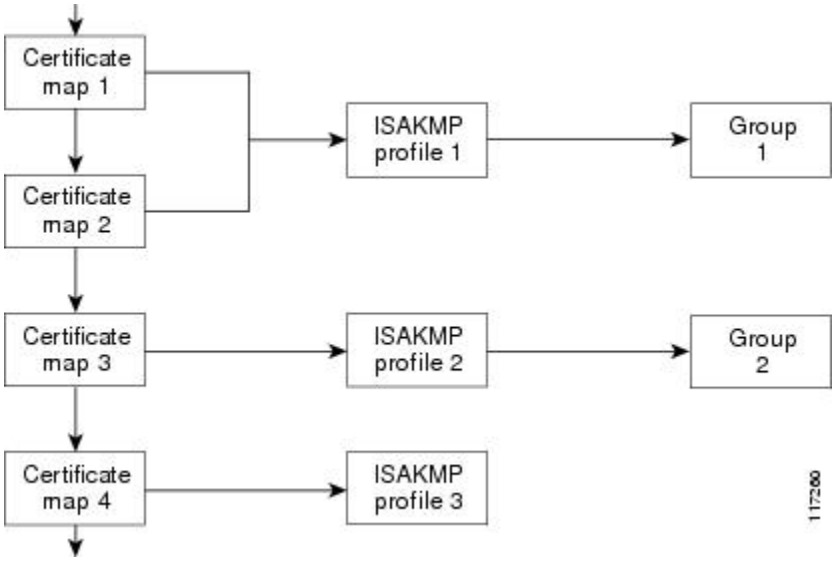
Cisco IOS Release12.3(8)T 以前では、ピアを ISAKMP プロファイルにマッピングする方法は、次の方法だけでした。ISAKMP 交換の ISAKMP ID フィールドは、ピアを ISAKMP プロファイルにマッピングするために使用されていました。証明書が認証に使用されるとき、ISAKMP ID ペイロードに証明書からの所有者名が含まれていました。CA が、要求されたグループ値を証明書の最初の組織ユニット（OU）フィールドに表示しなかった場合、ISAKMP プロファイルをピアに割り当てることはできませんでした。

Cisco IOS Release 12.3(8)T でも、上記のように、ピアをマッピングできます。証明書/ISAKMP プロファイルマッピング機能を使用すると、証明書内の任意のフィールドの内容に基づいて、ピアに ISAKMP プロファイルを割り当てることができます。以前は、証明書の所有者名に基づいて ISAKMP プロファイルを割り当てるという方法しかありませんでした。また、この機能により、ISAKMP プロファイルが割り当てられたピアにグループを割り当てることができます。

証明書/ISAKMP プロファイルマッピングのしくみ

次の図に、証明書マップを ISAKMP プロファイルに接続し、証明書マップにグループ名を割り当てる方法を示します。

図 *100* : プロファイル グループ割り当てにマッピングされる証明書マップ



ISAKMP プロファイルには複数の証明書マップを接続できますが、証明書マップは 1 つの ISAKMP プロファイルにしか接続できません。

証明書マップにより、証明書を指定の一連の基準と照合できるようになります。ISAKMP プロファイルは、自身を証明書マップにバインドできます。また、提示された証明書が ISAKMP プロファイル内に存在する証明書マップと一致した場合、ピアに ISAKMP プロファイルが割り当てられます。ISAKMP プロファイルにクライアント設定グループ名が含まれている場合、同じグループ名がピアに割り当てられます。この ISAKMP プロファイル情報により、ID_KEY_ID アイデンティティまたは証明書の最初の OU フィールドの情報が上書きされます。

ピアへの ISAKMP プロファイルおよびグループ名の割り当て

証明書内の任意のフィールドに基づいて、ピアに ISAKMP プロファイルを割り当てるには、ISAKMP プロファイルを定義してから、**match certificate** コマンドを使用します。

ピアに割り当てられる ISAKMP プロファイルにグループ名を関連付けるのは、同様に ISAKMP プロファイルを定義してから、**client configuration group** コマンドを使用します。

証明書/ISAKMP プロファイルマッピングの設定方法

証明書/ISAKMP プロファイル マッピング

ISAKMP プロファイルに証明書をマッピングするには、次の手順を実行します。この設定により、証明書内の任意のフィールドの内容に基づいて、ピアに ISAKMP プロファイルを割り当てることができます。

手順の概要

1. **enable**
2. **configure terminal**
3. **crypto isakmp profile** *profile-name*
4. **match certificate** *certificate-map*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router# enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例：	グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
	`Router# configure terminal`	
ステップ 3	**crypto isakmp profile** *profile-name* 例： `Router (config)# crypto isakmp profile vpnprofile`	ISAKMP プロファイルを定義し、暗号 ISAKMP プロファイル コンフィギュレーション モードを開始します。
ステップ 4	**match certificate** *certificate-map* 例： `Router (conf-isa-prof)# match certificate map1`	証明書マップの名前を受け入れます。

証明書がマッピングされたことの確認

次の **show** コマンドを使って、証明書マップの所有者名が正しく設定されているか確認できます。

手順の概要

1. **enable**
2. **show crypto ca certificates**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router# enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**show crypto ca certificates** 例： `Router# show crypto ca certificates`	証明書に関する情報を表示します。

ピアへのグループ名の割り当て

ピアを ISAKMP プロファイルにマッピングするときにグループ名をピアに関連付けるには、次の手順を実行します。

手順の概要

1. **enable**

2. **configure terminal**
3. **crypto isakmp profile** *profile-name*
4. **client configuration group** *group-name*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router# enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**crypto isakmp profile** *profile-name* 例： `Router (config)# crypto isakmp profile vpnprofile`	ISAKMP プロファイルを定義し、ISAKMP プロファイル コンフィギュレーション モードを開始します。
ステップ 4	**client configuration group** *group-name* 例： `Router (conf-isa-prof)# client configuration group group1`	この暗号 ISAKMP プロファイルにピアを割り当てるときに、そのピアに割り当てられるグループ名を受け入れます。

証明書/ISAKMP プロファイルマッピングのモニタおよびメンテナンス

ISAKMP プロファイルマッピングに対応する証明書をモニターしメンテナンスするには、次の **debug** コマンドを使用します。

手順の概要

1. **enable**
2. **debug crypto isakmp**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router# enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。

	コマンドまたはアクション	目的
ステップ 2	**debug crypto isakmp** 例： `Router# debug crypto isakmp`	証明書が、証明書マップの照合を経て、ISAKMP プロファイルと一致することを示す出力を表示します。 このコマンドは、ピアにグループが割り当てられたことを確認する場合にも使用できます。

証明書/ISAKMP プロファイルマッピングの設定例

任意のフィールドに基づいた ISAKMP プロファイルへの証明書のマッピング：例

次の設定例では、証明書に「ou = green」が含まれているときは必ず、ISAKMP プロファイル「cert_pro」がピアに割り当てられる、ということを示します。

```
crypto pki certificate map cert_map 10
 subject-name co ou = green
!
!
crypto isakmp identity dn
crypto isakmp profile cert_pro
   ca trust-point 2315
   ca trust-point LaBcA
   initiate mode aggressive
   match certificate cert_map
```

ISAKMP プロファイルに関連付けられたピアに割り当てられるグループ名の例

次の例は、グループ「some_group」が、ISAKMP プロファイルが割り当てられたピアに関連付けられていることを示しています。

```
crypto isakmp profile id_profile
   ca trust-point 2315
   match identity host domain cisco.com
   client configuration group some_group
```

ISAKMP プロファイルへの証明書のマッピング検証例

次の例は、ISAKMP プロファイルに証明書がマッピングされたことを示します。この例には、応答側および発信側の設定、証明書マップの所有者名が設定されたことを確認する **show command** 出力、および証明書が証明書マップの照合を経て ISAKMP プロファイルに一致したことを示す **debug** コマンド出力が含まれています。

応答側の設定

```
crypto pki certificate map cert_map 10
! The above line is the certificate map definition.
 subject-name co ou = green
! The above line shows that the subject name must have “ou = green.”
!
crypto isakmp profile certpro
! The above line shows that this is the ISAKMP profile that will match if the certificate
 of the peer matches cert_map (shown on third line below).
   ca trust-point 2315
   ca trust-point LaBcA
   match certificate cert_map
   initiate mode aggressive
```

発信側の設定

```
crypto ca trustpoint LaBcA
 enrollment url http://10.76.82.20:80/cgi-bin/openscep
 subject-name ou=green,c=IN
! The above line ensures that the subject name “ou = green” is set.
 revocation-check none
```

発信側の **show crypto ca certificates** コマンド出力

```
Router# show crypto ca certificates
Certificate
  Status: Available
  Certificate Serial Number: 21
  Certificate Usage: General Purpose
  Issuer:
    cn=blue-lab CA
    o=CISCO
    c=IN
  Subject:
    Name: Router1.cisco.com
    c=IN
    ou=green
! The above line is a double check that “ou = green” has been set as the subject name.
    hostname=Router1.cisco.com
  Validity Date:
    start date: 14:34:30 UTC Mar 31 2004
    end   date: 14:34:30 UTC Apr 1 2009
    renew date: 00:00:00 UTC Jan 1 1970
  Associated Trustpoints: LaBcA
```

応答側の **debug crypto isakmp** コマンド出力

```
Router# debug crypto isakmp
6d23h: ISAKMP (0:268435460): received packet from 192.0.0.2 dport 500 sport 500 Global
(R) MM_KEY_EXCH
6d23h: ISAKMP: Main Mode packet contents (flags 1, len 892):
6d23h:           ID payload
6d23h:             FQDN <Router1.cisco.com> port 500 protocol 17
6d23h:           CERT payload
6d23h:           SIG payload
6d23h:           KEEPALIVE payload
6d23h:           NOTIFY payload
```

```
6d23h: ISAKMP:(0:4:HW:2):Input = IKE_MESG_FROM_PEER, IKE_MM_EXCH
6d23h: ISAKMP:(0:4:HW:2):Old State = IKE_R_MM4  New State = IKE_R_MM5
6d23h: ISAKMP:(0:4:HW:2): processing ID payload. message ID = 0
6d23h: ISAKMP (0:268435460): ID payload
        next-payload : 6
        type         : 2
        FQDN name    : Router1.cisco.com
        protocol     : 17
        port         : 500
        length       : 28
6d23h: ISAKMP:(0:4:HW:2):: peer matches *none* of the profiles
6d23h: ISAKMP:(0:4:HW:2): processing CERT payload. message ID = 0
6d23h: ISAKMP:(0:4:HW:2): processing a CT_X509_SIGNATURE cert
6d23h: ISAKMP:(0:4:HW:2): peer's pubkey isn't cached
6d23h: ISAKMP:(0:4:HW:2): OU = green
6d23h: ISAKMP:(0:4:HW:2): certificate map matches certpro profile
! The above line shows that the certificate has gone through certificate map matching
and that it matches the “certpro” profile.
6d23h: ISAKMP:(0:4:HW:2): Trying to re-validate CERT using new profile
6d23h: ISAKMP:(0:4:HW:2): Creating CERT validation list: 2315, LaBcA,
6d23h: ISAKMP:(0:4:HW:2): CERT validity confirmed.
```

ピアに割り当てられたグループ名の検証例

次の設定およびデバッグ出力は、グループがピアに割り当てられたことを示します。

発信側の設定

```
crypto isakmp profile certpro
   ca trust-point 2315
   ca trust-point LaBcA
   match certificate cert_map
   client configuration group new_group
! The statement on the above line will assign the group “new_group” to any peer that
matches the ISAKMP profile “certpro.”
   initiate mode aggressive
!
```

応答側の **debug crypto isakmp** プロファイル コマンド出力

次のデバッグ出力例は、ピアが「certpro」という ISAKMP プロファイルと照合され、「new_group」というグループが割り当てられたことを示します。

```
Router# debug crypto isakmp profile
6d23h: ISAKMP (0:268435461): received packet from 192.0.0.2 dport 500 sport 500 Global
(R) MM_KEY_EXCH
6d23h: ISAKMP: Main Mode packet contents (flags 1, len 892):
6d23h:           ID payload
6d23h:             FQDN <Router1.cisco.com> port 500 protocol 17
6d23h:           CERT payload
6d23h:           SIG payload
6d23h:           KEEPALIVE payload
6d23h:           NOTIFY payload
6d23h: ISAKMP:(0:5:HW:2):Input = IKE_MESG_FROM_PEER, IKE_MM_EXCH
6d23h: ISAKMP:(0:5:HW:2):Old State = IKE_R_MM4  New State = IKE_R_MM5
6d23h: ISAKMP:(0:5:HW:2): processing ID payload. message ID = 0
6d23h: ISAKMP (0:268435461): ID payload
        next-payload : 6
```

```
        type          : 2
        FQDN name     : Router1.cisco.com
        protocol      : 17
        port          : 500
        length        : 28
6d23h: ISAKMP:(0:5:HW:2):: peer matches *none* of the profiles
6d23h: ISAKMP:(0:5:HW:2): processing CERT payload. message ID = 0
6d23h: ISAKMP:(0:5:HW:2): processing a CT_X509_SIGNATURE cert
6d23h: ISAKMP:(0:5:HW:2): peer's pubkey isn't cached
6d23h: ISAKMP:(0:5:HW:2): OU = green
6d23h: ISAKMP:(0:5:HW:2): certificate map matches certpro profile
6d23h: ISAKMP:(0:5:HW:2): Trying to re-validate CERT using new profile
6d23h: ISAKMP:(0:5:HW:2): Creating CERT validation list: 2315, LaBcA,
6d23h: ISAKMP:(0:5:HW:2): CERT validity confirmed.
6d23h: ISAKMP:(0:5:HW:2):Profile has no keyring, aborting key search
6d23h: ISAKMP:(0:5:HW:2): Profile certpro assigned peer the group named new_group
```

その他の参考資料

関連資料

関連項目	マニュアル タイトル
ISAKMP プロファイルの設定	VRF 認識 IPSec
セキュリティ コマンド	『*Cisco IOS Security Command Reference*』

標準

標準	タイトル
なし	--

MIB

MIB	MIB のリンク
なし	選択したプラットフォーム、Cisco IOS ソフトウェア リリース、およびフィーチャセットの MIB を検索してダウンロードする場合は、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

RFC

RFC	タイトル
なし	--

シスコのテクニカル サポート

説明	リンク
シスコのサポート Web サイトでは、シスコの製品やテクノロジーに関するトラブルシューティングにお役立ていただけるように、マニュアルやツールをはじめとする豊富なオンライン リソースを提供しています。 お使いの製品のセキュリティ情報や技術情報を入手するために、Cisco Notification Service（Field Notice からアクセス）、Cisco Technical Services Newsletter、Really Simple Syndication（RSS）フィードなどの各種サービスに加入できます。 シスコのサポート Web サイトのツールにアクセスする際は、Cisco.com のユーザ ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

証明書/ISAKMP プロファイルマッピングの機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *266 :* 証明書*/ISAKMP* プロファイルマッピングの機能情報

機能名	リリース	機能情報
証明書/ISAKMP プロファイルマッピング	12.3(8)T 12.2(33)SRA 12.2(33)SXH	証明書/ISAKMPプロファイルマッピング機能を使用すると、証明書内の任意のフィールドの内容に基づいて、ピアにInternet Security Association and Key Management Protocol（ISAKMP）プロファイルを割り当てることができます。また、この機能では、ISAKMPプロファイルに割り当てられたピアにグループ名を割り当てることもできます。 この機能は、Cisco IOS Release12.3(8)T で導入されました。 この機能は、Cisco IOS Release 12.2(33)SRA に統合されました。 この機能は、Cisco IOS Release 12.2(33)SXH に統合されました。

第 199 章

「Encrypted Preshared Key」

暗号化事前共有キー機能を使用すると、プレーンテキストのパスワードをタイプ 6（暗号化）形式で NVRAM に安全に保管できます。

暗号化事前共有キーの制約事項

- 古い ROM モニタ（ROMMON）およびブート イメージでは、新しいタイプ 6 パスワードが認識されません。そのため、旧来の ROMMON から起動すると、エラーが発生します。
- Cisco 836 ルータでは、Advanced Encryption Standard（AES）を使用できるのは IP Plus イメージ上に限ります。

暗号化事前共有キーに関する情報

暗号化事前共有キーの使用によるパスワードのセキュアな保存

暗号化事前共有キー機能を使用すると、コマンドライン インターフェイス（CLI）から、プレーンテキストのパスワードをタイプ 6 形式で NVRAM へセキュアに保存できます。タイプ 6 のパスワードは暗号化されています。暗号化されたパスワード自体を、確認したり取得したりすることは可能ですが、それを復号化して実際のパスワードを特定することは困難です。**key config-key** コマンドを **password encryption aes** コマンドとともに使用すると、パスワードを設定してイネーブルにできます（キーの暗号化には対称キー暗号である AES が使用されます）。**config-key password-encryption** コマンドを使用して設定されたパスワード（キー）は、ルータ内のその他すべてのキーを暗号化するマスター暗号キーとして使用されます。

password encryption aes コマンドを設定する際、同時に **key config-key** コマンドを設定しないと、**show running-config** コマンドや **copy running-config startup-config** コマンドなどが設定されている起動時や不揮発性生成（NVGEN）プロセス中に次のようなメッセージが出力されます。

```
"Can not encrypt password. Please configure a configuration-key with 'key config-key'"
```

パスワードの変更

key config-key password-encryption コマンドを使用してパスワード（マスターキー）が変更された場合、または再暗号化された場合には、リストレジストリから、タイプ6暗号が使用されているアプリケーションモジュールへ、変更前のキーと変更後のキーが渡されます。

パスワードの削除

key config-key password-encryption コマンドを使用して設定されたマスターキーがシステムから削除されると、タイプ6のパスワードすべてが使用不可になるという内容の警告が出力されます（同時に、確認用のプロンプトも表示されます）。セキュリティ対策として、暗号化されたパスワードは、ソフトウェアによって復号されることはなくなります。ただし、すでに説明したように、パスワードを再暗号化することはできます。

⚠

注意 **key config-key password-encryption** コマンドを使用して設定されたパスワードは、一度失われると回復できません。パスワードは、安全な場所に保存することを推奨します。

パスワード暗号化の設定解除

no password encryption aes コマンドを使用してパスワード暗号化の設定を解除しても、既存のタイプ 6 パスワードはすべて変更されずに残されます。**key config-key password-encryption** コマンドを使用して設定したパスワード（マスターキー）があれば、アプリケーションで必要に応じてタイプ 6 パスワードを復号できます。

パスワードの保存

（**key config-key password-encryption** コマンドを使用して設定された）パスワードは誰にも「判読」できないため、ルータからパスワードを取得する方法はありません。既存の管理ステーションでは、その内部にキーが格納されるよう強化されることで初めて、パスワードの内容を「知る」ことができます。その場合、パスワードは管理ステーション内部に安全に保存する必要があります。TFTP を使用して保存された設定は、スタンドアロンではないため、ルータにはロードできません。設定をルータにロードする前後には、（**key config-key password-encryption** コマンドを使用して）パスワードを手動で追加する必要があります。このパスワードは、保存された設定に手動で追加できますが、それによって設定内のすべてのパスワードを誰もが復号化できるようになるため、手動によるパスワードの追加は行わないことを推奨します。

新規パスワードまたは不明パスワードの設定

入力またはカット アンド ペーストした暗号文は、それがマスター キーに適合しない場合やマスター キーが存在しない場合でも、受理または保存されます。ただしこの場合にはアラート メッセージが出力されます。アラート メッセージの内容は次のとおりです。

```
"ciphertext>[for username bar>] is incompatible with the configured master key."
```

マスターキーを新規に設定すると、プレーンテキストのキーはすべて暗号化され、タイプ 6 のキーになります。すでにタイプ 6 であるキーは暗号化されず、現在の状態が維持されます。

既存のマスターキーが失われた場合、またはその内容が不明の場合は、**no key config-key password-encryption** コマンドを使用してそのマスターキーを削除できます。**no key config-key password-encryption** コマンドを使用してマスターキーを削除しても、既存の暗号化パスワードは、暗号化された状態のままルータ設定内に保持されます。これらのパスワードは復号化されません。

暗号化事前共有キーのイネーブル化

password encryption aes コマンドを使用すると、暗号化されたパスワードを有効化できます。

暗号化事前共有キーの設定方法

暗号化事前共有キーの設定

暗号化事前共有キーを設定するには、次の手順を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **key config-key password-encryption** [*text*]
4. **password encryption aes**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例：	グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
	`Router# configure terminal`	
ステップ 3	**key config-key password-encryption** [*text*] 例： `Router (config)# key config-key password-encryption`	タイプ 6 の暗号キーをプライベート NVRAM に保存します。 • （Enter キーを使用して）インタラクティブにキーボード操作を行う場合、暗号キーがすでに存在すれば、Old key、New key、Confirm key という 3 つのプロンプトが表示されます。 • インタラクティブにキーボード操作を行う場合、暗号キーが存在しなければ、New key、Confirm key という 2 つのプロンプトが表示されます。 • すでに暗号化されているパスワードを削除する場合は、次のプロンプトが表示されます。「WARNING: All type 6 encrypted keys will become unusable. Continue with master key deletion? [yes/no]:」
ステップ 4	**password encryption aes** 例： `Router (config)# password-encryption aes`	暗号化事前共有キーのイネーブル化

トラブルシューティングのヒント

「ciphertext >[for username bar>] is incompatible with the configured master key」という警告メッセージが表示された場合は、入力またはカット アンド ペーストした暗号文がマスター キーに適合しないか、またはマスター キーが存在しないと判断できます（暗号文は受理または保存されます）。この警告メッセージを手掛かりにすれば、設定の不具合箇所を特定できます。

暗号化事前共有キーのモニタリング

暗号化事前共有キーに関するロギングを出力するには、次の手順を実行します。

1. **enable**
2. **password logging**

手順の概要

1. **enable**
2. **password logging**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**password logging** 例： `Router# password logging`	タイプ 6 パスワードの処理に関するデバッグ出力のログを表示します。

例

次に示すのは、**password logging** によるデバッグ出力の表示例です。ここでは、マスターキーが新規に設定された場合と、その新しいマスターキーを使用してそのキーが暗号化された場合が表示されています。

```
Router (config)# key config-key password-encrypt
New key:
Confirm key:
Router (config)#
01:40:57: TYPE6_PASS: New Master key configured, encrypting the keys with
the new master keypas
Router (config)# key config-key password-encrypt
Old key:
New key:
Confirm key:
Router (config)#
01:42:11: TYPE6_PASS: Master key change heralded, re-encrypting the keys
with the new master key
01:42:11: TYPE6_PASS: Mac verification successful
01:42:11: TYPE6_PASS: Mac verification successful
01:42:11: TYPE6_PASS: Mac verification successful
```

次の作業

次に示す作業を実行できます。これらの各作業は、互いに独立したものです。

ISAKMP 事前共有キーの設定

ISAKMP 事前共有キーを設定するには、次の手順を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **crypto isakmp key** *keystring* **address** *peer-address*

4. **crypto isakmp key** *keystring* **hostname** *hostname*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router# enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**crypto isakmp key** *keystring* **address** *peer-address* 例： `Router (config)# crypto isakmp key cisco address 10.2.3.4`	事前共有認証キーを設定します。 • *peer-address* 引数には、リモート ピアの IP アドレスを指定します。
ステップ 4	**crypto isakmp key** *keystring* **hostname** *hostname* 例： `Router (config)# crypto isakmp key mykey hostname mydomain.com`	事前共有認証キーを設定します。 • *hostname* 引数には、ピアの完全修飾ドメイン名（FQDN）を指定します。

例

次に示すのは、暗号化事前共有キーが設定された場合の出力例です。

```
crypto isakmp key 6 _Hg[^^ECgLGGPF^RXTQfDDWQ][YAAB address 10.2.3.4
crypto isakmp key 6 `eR\eTRaKCUZPYYQfDgXRWi_AAB hostname mydomain.com
```

ISAKMP キーリングの ISAKMP 事前共有キーの設定

IPSec 仮想経路フォワーディング（VRF）で使用される ISAKMP リングの ISAKMP 事前共有キーを設定するには、次の手順を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **crypto keyring** *keyring-name*
4. **pre-shared-key address** *address* **key** *key*
5. **pre-shared-key hostname** *hostname* **key** *key*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router# enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**crypto keyring** *keyring-name* 例： `Router (config)# crypto keyring mykeyring`	インターネット キー交換（IKE）認証で使用する暗号キーリングを定義し、キーリング コンフィギュレーション モードを開始します。
ステップ 4	**pre-shared-key address** *address* **key** *key* 例： `Router (config-keyring)# pre-shared-key address 10.2.3.5 key cisco`	IKE 認証に使用する事前共有キーを定義します。 • *address* 引数には、リモート ピアの IP アドレスを指定します。
ステップ 5	**pre-shared-key hostname** *hostname* **key** *key* 例： `Router (config-keyring)# pre-shared-key hostname mydomain.com key cisco`	IKE 認証に使用する事前共有キーを定義します。 • *hostname* 引数には、ピアの FQDN を指定します。

例

次に示すのは、ISAKMP キーリングの暗号化された事前共有キーが設定された場合の **how-running-config** による出力例です。

```
crypto keyring mykeyring
  pre-shared-key address 10.2.3.5 key 6 `WHCJYR_Z]GRPF^RXTQfDcfZ]GPAAB
  pre-shared-key hostname mydomain.com key 6 aE_REHDcOfYCPF^RXTQfDJYVVNSAAB
```

ISAKMP アグレッシブ モードの設定

ISAKMP アグレッシブ モードを設定するには、次の手順を実行します。

手順の概要

1. **enable**

2. **configure terminal**
3. **crypto isakmp peer ip-address** *ip-address*
4. **set aggressive-mode client-endpoint** *client-endpoint*
5. **set aggressive-mode password** *password*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router# enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**crypto isakmp peer ip-address** *ip-address* 例： `Router (config)# crypto isakmp peer ip-address 10.2.3.4`	アグレッシブ モードのトンネル属性に関し、IP セキュリティ（IPSec）ピアによる認証、許可、アカウンティング（AAA）の IKE クエリーをイネーブルにし、ISAKMP ピア コンフィギュレーション モードを開始します。
ステップ 4	**set aggressive-mode client-endpoint** *client-endpoint* 例： `Router (config-isakmp-peer)# set aggressive-mode client-endpoint fqdn cisco.com`	ISAKMP ピア設定内で、Tunnel-Client-Endpoint 属性を指定します。
ステップ 5	**set aggressive-mode password** *password* 例： `Router (config-isakmp-peer)# set aggressive-mode password cisco`	ISAKMP ピア設定内で、Tunnel-Password 属性を指定します。

例

次に示すのは、ISAKMP アグレッシブモードで、暗号化された事前共有キーが設定された場合の **how-running-config** による出力例です。

```
crypto isakmp peer address 10.2.3.4
 set aggressive-mode password 6 ^aKPIQ_KJE_PPF^RXTQfDTIaLNeAAB
 set aggressive-mode client-endpoint fqdn cisco.com
```

Unity サーバ グループ ポリシーの設定

Unity サーバ グループ ポリシーを設定するには、次の手順を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **crypto isakmp client configuration group** *group-name*
4. **pool** *name*
5. **domain name**
6. **key** *name*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router# enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**crypto isakmp client configuration group** *group-name* 例： `Router (config)# crypto isakmp client configuration group mygroup`	定義するグループのポリシー プロファイルを指定し、ISAKMP グループ コンフィギュレーション モードを開始します。
ステップ 4	**pool** *name* 例： `Router (config-isakmp-group)# pool mypool`	ローカル プール アドレスを定義します。
ステップ 5	**domain name** 例： `Router (config-isakmp-group)# domain cisco.com`	グループが属するドメイン ネーム サービス（DNS）ドメインを指定します。
ステップ 6	**key** *name* 例： `Router (config-isakmp-group)# key cisco`	グループ ポリシー属性の定義に使用する IKE 事前共有キーを指定します。

例

次に示すのは、暗号化されたキーが Unity サーバーグループポリシーに対して設定された場合の **show-running-config** による出力例です。

```
crypto isakmp client configuration group mygroup
 key 6 cZZgDZPOE\dDPF^RXTQfDTIaLNeAAB
 domain cisco.com
 pool mypool
```

Easy VPN クライアントの設定

Easy VPN クライアントを設定するには、次の手順を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **crypto ipsec client ezvpn** *name*
4. **peer** *ipaddress*
5. **mode client**
6. **group** *group-name* **key** *group-key*
7. **connect manual**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router# enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**crypto ipsec client ezvpn** *name* 例： `Router (config)# crypto ipsec client ezvpn myclient`	Cisco Easy VPN Remote コンフィギュレーションを作成し、Cisco Easy VPN Remote コンフィギュレーション モードを開始します。
ステップ 4	**peer** *ipaddress* 例：	VPN 接続に対して、ピアの IP アドレスを設定します。

	コマンドまたはアクション	目的
	`Router (config-isakmp-peer)# peer 10.2.3.4`	
ステップ 5	**mode client** 例： `Router (config-isakmp-ezpvy)# mode client`	ネットワーク アドレス変換（NAT）またはピア アドレス変換（PAT）を使用する Cisco Easy VPN クライアント モードでの動作用にルータを自動設定します。
ステップ 6	**group** *group-name* **key** *group-key* 例： `Router (config-isakmp-ezvpn)# group mygroup key cisco`	VPN 接続に使用するグループ名およびキー値を指定します。
ステップ 7	**connect manual** 例： `Router (config-isakmp-ezvpn)# connect manual`	手動設定を指定して、Cisco Easy VPN Remote クライアントに対し、コマンドまたはアプリケーション プログラミング インターフェイス（API）のコールを待機してから、Cisco Easy VPN リモート接続の確立を試行するよう指示します。

例

次に、Easy VPN クライアントが設定されていることを示す **show-running-config** の出力例を示します。このキーは暗号化されています。

```
crypto ipsec client ezvpn myclient
 connect manual
 group mygroup key 6 gdMI`S^^[GIcPF^RXTQfDFKEO\RAAB
 mode client
 peer 10.2.3.4
```

暗号化事前共有キーの設定例

暗号化事前共有キー：例

次に示すのは、タイプ 6 の事前共有キーが暗号化された場合の設定例です。この中には、ユーザに対して表示されるプロンプトやメッセージも含まれています。

```
Router (config)# crypto isakmp key cisco address 10.0.0.2
Router (config)# exit
Router# show running-config | include crypto isakmp key
 crypto isakmp key cisco address 10.0.0.2
Router#
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
```

```
Router (config)# password encryption aes

Router (config)# key config-key password-encrypt

New key:
Confirm key:
Router (config)#
01:46:40: TYPE6_PASS: New Master key configured, encrypting the keys with
the new master key
Router (config)# exit
Router # show running-config | include crypto isakmp key
crypto isakmp key 6 CXWdhVTZYB_Vcd^`cIHDOahiFTa address 10.0.0.2
```

キーが存在しない場合の例

次の設定例には、以前のキーがありません。

```
Router (config)#
```

キーが存在する場合の例

次の設定例には、キーがすでに存在しています。

```
Router (config)#
Old key:
Router (config)#
```

キーが存在する状況でユーザがインタラクティブにキーを入力する場合の例

次の設定例では、ユーザは対話形式の入力を求めていますが、キーはすでに存在しています。**key config-key** コマンドを入力し、Enter キーを押して対話モードを開始すると、画面には Old key、New key、Confirm key という 3 つのプロンプトが表示されます。

```
Router (config)#
Old key:
New key:
Confirm key:
```

キーが存在しない状況でユーザがインタラクティブにキーを入力する場合の例

次に示すのは、キーが存在しない状況でユーザがインタラクティブにキーボード操作を行う場合の設定例です。対話モードを開始すると、画面には New key および Confirm key という 2 つのプロンプトが表示されます。

```
Router (config)#
```

```
New key:
Confirm key:
```

パスワード暗号化の設定解除の例

次に示すのは、ユーザがパスワード暗号化の設定を解除する場合の設定例です。「WARNING: All type 6 encrypted keys will become unusable. Continue with master key deletion? [yes/no]:」というプロンプトが画面に表示されます（インタラクティブ モードの場合）。

```
Router (config)#
WARNING: All type 6 encrypted keys will become unusable. Continue with master key deletion
 ? [yes/no]: y
```

次の作業

その他の事前共有キーを設定します。

その他の参考資料

関連資料

関連項目	マニュアル タイトル
パスワードの設定	『*Cisco IOS Security Command Reference*』

標準

標準	タイトル
なし	--

MIB

MIB	MIB のリンク
なし	選択したプラットフォーム、Cisco IOS ソフトウェア リリース、およびフィーチャセットの MIB を検索してダウンロードする場合は、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

RFC

RFC	タイトル
なし	--

シスコのテクニカル サポート

説明	リンク
右の URL にアクセスして、シスコのテクニカル サポートを最大限に活用してください。これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

第 200 章

識別名ベースのクリプト マップ

機能の履歴

リリース	変更内容
12.2(4)T	この機能が導入されました。

（注） セキュリティに対する脅威は、脅威からの保護に役立つ暗号化技術と同様に絶え間なく変化しています。シスコの暗号化に関する最新の推奨事項の詳細は、『Next Generation Encryption』（NGE）ホワイトペーパーを参照してください。

この章では、Cisco IOS Release 12.2(4)T の識別名ベースの暗号マップ機能について説明します。次のセクションで構成されています。

機能の概要

識別名ベースのクリプト マップ機能により、証明書（特に特定の識別名（DN）持つ特定の証明書）を持つピアの選択された暗号化インターフェイスだけに、アクセスを制限するようにルータを設定できます。

以前まで、暗号化ピアからルータが証明書または共有秘密を受け入れる場合、Cisco IOS では暗号化ピアの IP アドレスによって制限する以外、暗号化されたインターフェイスとピアが通信するのを防ぐ方法がありませんでした。この機能により、ピアが自身の認証に使用した DN に基づいて、ピアが使用できるクリプトマップを設定し、特定の DN を持つピアがアクセスできる暗号化インターフェイスを制御できます。

利点

識別名ベースの暗号マップ機能では、暗号化インターフェイスを選択し、特定の証明書（なかでも特別な DN を持つ証明書）を持つピアがそのインターフェイスにアクセスしないよう、ルータに制限を設定できます。

機能制限

システム要件

この機能を設定するには、ルータが IP セキュリティをサポートする必要があります。

パフォーマンス上の影響

アクセスを制限するDNが多い場合、少数のアイデンティティセクションを参照する多数のクリプト マップを指定するよりも、多数のアイデンティティ セクションを参照する少数のクリプト マップを指定することを推奨します。

関連資料

次のマニュアルには、識別名ベースのクリプト マップ機能の関連情報が記載されています。

- 『Cisco IOS Security Command Reference』
- 『Cisco IOS Security Configuration Guide: Secure Connectivity, Release 12.4T』
- Next Generation Encryption （NGE）ホワイトペーパー。

サポートされるプラットフォーム

この機能は、次のプラットフォームでサポートされます。

- Cisco 1700 シリーズ
- Cisco 2600 シリーズ
- Cisco 3620
- Cisco 3640
- Cisco 3660
- Cisco 7100 シリーズ
- Cisco 7200 シリーズ
- Cisco uBR905 ケーブル アクセス ルータ
- Cisco uBR925 ケーブル アクセス ルータ

Feature Navigator を使用したプラットフォーム サポートの判別

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

サポートされている規格 MIB および RFC

標準

なし

MIB

なし

選択したプラットフォーム、Cisco IOS リリース、およびフィーチャ セットに関する MIB を探してダウンロードするには、次の URL にある Cisco MIB Locator を使用します。

http://www.cisco.com/go/mibs

RFC

なし

前提条件

DN ベースのクリプト マップを設定する前に、次の作業を実行する必要があります。

- ピアごとに IKE ポリシーを作成します。

IKE ポリシーの作成についての詳細は、『*Cisco IOS Security Configuration Guide: Secure Connectivity*』の「Configuring Internet Key Exchange for IPsec VPNs」の章を参照してください。

- IPSec のクリプト マップ エントリを作成します。

暗号マップエントリの作成についての詳細は、『*Cisco IOS Security Configuration Guide: Secure Connectivity*』の「Configuring Security for VPNs with IPsec」の章を参照してください。

設定作業

クリプト マップ エントリの作成に関する詳細については、「IPsec VPN のセキュリティの設定」を参照してください。一覧内の各作業は、必須と任意に分けています。

- （DN によって認証された）DN ベースの暗号マップの設定 （2908 ページ） （必須）
- （ホスト名によって認証された）DN ベースの暗号マップの設定 （2908 ページ） （必須）

- DN ベースの暗号マップへの ID の適用 （2909 ページ） （必須）
- DN ベースの暗号マップの確認 （2909 ページ） （任意）

（DN によって認証された）DN ベースの暗号マップの設定

DN によって認証されたピアだけが使用できる DN ベースのクリプト マップを設定するには、グローバル コンフィギュレーション モードの開始時に次のコマンドを使用します。

手順の概要

1. Router(config)# **crypto identity** *name*
2. Router(crypto-identity)# **dn** *name=string* [,*name=string*]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	Router(config)# **crypto identity** *name*	ルータの証明書内にある指定 DN リストを使用してルータのアイデンティティを設定し、暗号アイデンティティ コンフィギュレーション モードを開始します。
ステップ 2	Router(crypto-identity)# **dn** *name=string* [,*name=string*]	ルータの証明書内にある DN に、ルータのアイデンティティを関連付けます。 （注） ピアのアイデンティティは、交換された証明書のアイデンティティと一致する必要があります。

（ホスト名によって認証された）DN ベースの暗号マップの設定

ホスト名によって認証されたピアだけが使用できるDNベースのクリプトマップを設定するには、グローバル コンフィギュレーション モードの開始時に次のコマンドを使用します。

手順の概要

1. Router(config)# **crypto identity** *name*
2. Router(crypto-identity)# **fqdn** *name*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	Router(config)# **crypto identity** *name*	ルータの証明書内にある指定 DN リストを使用してルータのアイデンティティを設定し、暗号アイデン

	コマンドまたはアクション	目的
		ティティ コンフィギュレーション モードを開始します。
ステップ 2	Router(crypto-identity)# **fqdn** *name*	ピアの認証に使用したホスト名にルータのアイデンティティを関連付けます。 （注） ピアのアイデンティティは、交換された証明書のアイデンティティと一致する必要があります。

DN ベースの暗号マップへの ID の適用

（クリプト マップのコンテキスト内で）アイデンティティを適用するには、グローバル コンフィギュレーション モードの開始時に次のコマンドを使用します。

手順の概要

1. Router(config)# **crypto map** *map-name seq-num* **ipsec-isakmp**
2. Router(config-crypto-map)# **identity** *name*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	Router(config)# **crypto map** *map-name seq-num* **ipsec-isakmp**	クリプト マップ エントリを作成または変更し、クリプト マップ コンフィギュレーション モードを開始します。
ステップ 2	Router(config-crypto-map)# **identity** *name*	クリプト マップに対して ID を適用します。 このコマンドを適用した場合、**identity** *name* でリストされているコンフィギュレーションと一致するホストだけが、指定した暗号マップを使用できます。 （注） 暗号マップ内に **identity** コマンドが表示されない場合は、暗号化ピアの IP アドレスを除き、暗号化接続に制約はありません。

DN ベースの暗号マップの確認

この機能が適切に設定されているかを確認するには、EXEC モードで次のコマンドを使用します。

コマンド	目的
Router# **show crypto identity**	設定したアイデンティティを表示します。

トラブルシューティングのヒント

暗号化ピアが接続を確立しようと試み、それが DN ベースのクリプト マップ設定によってブロックされた場合、次のエラー メッセージが記録されます。

```
<time>: %CRYPTO-4-IKE_QUICKMODE_BAD_CERT: encrypted connection attempted with a peer
without the configured certificate attributes.
```

設定例

DN ベースの暗号マップの設定例

次の例では、DN およびホスト名によって認証された DN ベースのクリプト マップを設定する方法を示します。間にコマンドを説明するためのコメントが含まれています。

```
! DN based crypto maps require you to configure an IKE policy at each peer.
crypto isakmp policy 15
 encryption aes
 hash sha
 authentication rsa-sig
 group 14
 lifetime 5000
crypto isakmp policy 20
 encryption aes
 hash sha
 authentication pre-share
 group 14
 lifetime 10000
crypto isakmp key 1234567890 address 171.69.224.33
!
! The following is an IPSec crypto map (part of IPSec configuration). It can be used
only
! by peers that have been authenticated by DN and if the certificate belongs to BigBiz.
crypto map map-to-bigbiz 10 ipsec-isakmp
 set peer 172.21.114.196
 set transform-set my-transformset
 match address 124
 identity to-bigbiz
!
crypto identity to-bigbiz
 dn ou=BigBiz
!
!
! This crypto map can be used only by peers that have been authenticated by hostname
! and if the certificate belongs to little.com.
crypto map map-to-little-com 10 ipsec-isakmp
 set peer 172.21.115.119
 set transform-set my-transformset
```

```
 match address 125
 identity to-little-com
!
crypto identity to-little-com
 fqdn little.com
!
```

第 201 章

IPsec と Quality of Service

IPsec と Quality of Service 機能を使用すれば、Cisco IOS Quality of Service（QoS）ポリシーを、QoS グループに基づいて、IP Security（IPsec）パケット フローに適用できます。QoS グループは、現在の Internet Security Association and Key Management Protocol（ISAKMP）プロファイルに適用できます。

（注） セキュリティに対する脅威は、脅威からの保護に役立つ暗号化技術と同様に絶え間なく変化しています。最新のシスコの暗号化に関する推奨事項については、『Next Generation Encryption』（NGE）ホワイト ペーパーを参照してください。

プラットフォームおよび Cisco IOS ソフトウェア イメージのサポート情報の検索

Cisco Feature Navigator を使用すると、プラットフォーム、および Cisco IOS ソフトウェア イメージの各サポート情報を検索できます。Cisco Feature Navigator には、http://tools.cisco.com/ITDIT/CFN/jsp/index.jsp からアクセスできます。アクセスするには、Cisco.com のアカウントが必要です。アカウントをお持ちでない場合や、ユーザー名やパスワードを忘れた場合は、ログインダイアログボックスで **[Cancel]** をクリックし、表示される説明に従ってください。

IPsec と Quality of Service の前提条件

- IPsec、および ISAKMP プロファイルの概念についての知識が必要です。
- Cisco IOS QoS の知識が必要です。

IPsec と Quality of Service の制約事項

- この機能を適用できるのはISAKMPプロファイルを介してだけです。QoSアプリケーションに対して使用できる QoS グループは 128 個までという制限はこの機能にも当てはまります。
- IPsec QoS グループを適用できるのは、発信サービス ポリシーに対してだけです。
- QoS は、ソフトウェア暗号化に関してはサポートされません。

IPsec と Quality of Service に関する情報

IPsec と Quality of Service の概要

IPsec と Quality of Service 機能を使用すれば、QoS グループを ISAKMP プロファイルに追加することによって、トラフィック ポリシングおよびシェーピングなどの QoS ポリシーを QoS ポリシーに適用できます。QoSグループが追加されると、このグループの値が、QoSクラスマップ内で定義されたものと同じ QoS グループにマッピングされます。この QoS グループ タグを利用している現在の QoS 方式はすべて、IPsec パケット フローに適用できます。パケット フローの共通グルーピングには、IPsec QoS グループを QoS メカニズムにとって使用可能にすることによって、特定のポリシー クラスを適用できます。IPsecフローをマーキングすれば、QoS メカニズムを、特定のグループが使用可能な帯域幅の制限や特定のフロー上のタイプオブサービス（ToS）ビットのマーキングなどをサポート可能なトラフィックのクラスに適用できます。

ISAKMPプロファイルは、アイデンティティ照合基準方式によってデバイスを一意に識別できるプロファイルなので、QoS グループのアプリケーションは、ISAKMP プロファイル レベルで適用されます。これらの基準は、インターネットキー交換（IKE）IDに基づいています。この ID は、受信 IKE 接続によって提供され、IP アドレス、完全修飾ドメイン名（FQDN）、およびグループ（つまり、バーチャル プライベート ネットワーク [VPN] リモート クライアント グルーピング）などが格納されます。アイデンティティ照合基準の粒度によって、指定された QoS ポリシーの粒度に制約が課せられます。たとえば、「Engineering」という名前の VPN クライアント グループに所属するすべてのトラフィックを、「TOS 5」としてマーキングします。指定した QoS ポリシーの粒度に制約を課すその他の例としては、発信 WAN リンクの 30 パーセントをリモート VPN デバイスの特定のグループへ割り当てるなどがあります。

IPsec と Quality of Service の設定方法

IPsec と Quality of Service の設定

QoS ポリシーを ISAKMP プロファイルに適用するには、次の手順を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **crypto isakmp-profile** *profile-number*
4. **qos-group** *group-number*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**crypto isakmp-profile** *profile-number* 例： `Router (config)# crypto isakmp-profile vpnprofile`	ISAKMP プロファイルを定義し、IPsec ユーザ セッションを監査し、ISAKMP プロファイル コンフィギュレーション モードを開始します。
ステップ 4	**qos-group** *group-number* 例： `Router(config-isa-prof)# qos-group 1`	QoS グループ値を ISAKMP プロファイルに適用します。

IPsec と Quality of Service セッションの確認

IPsec and QoS セッションを確認するには、次の手順を実行します。**show** コマンドは、任意の順序か互いに独立させて使用できます。

手順の概要

1. **enable**
2. **show crypto isakmp profile**
3. **show crypto ipsec sa**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例：	特権 EXEC モードを有効にします。

	コマンドまたはアクション	目的
	`Router> enable`	• パスワードを入力します（要求された場合）。
ステップ 2	**show crypto isakmp profile** 例： `Router# show crypto isakmp profile`	QoS グループがプロファイルに適用されていることを表示します。
ステップ 3	**show crypto ipsec sa** 例： `Router# show crypto ipsec sa`	QoS グループが、IPsec セキュリティ アソシエーション（SA）の特定のペアに適用されていることを表示します。

トラブルシューティングのヒント

IPsec セッションおよび QoS セッションに問題が発生した場合、次が実行されているかどうかを確認します。

- 『*Cisco IOS Quality of Service Solutions Command Reference*』に記載されている QoS 専用コマンドを使用して、QoS の適用を QoS サービスごとに確認している。
- クラス マップ一致基準に指定されたものと同じ QoS グループと一致しているルータ上の QoS ポリシーを設定している。
- クリプト マップが適用されるものと同じインターフェイスにサービス ポリシーを適用している。

IPsec と Quality of Service の設定例

リモート ユーザの 2 つのグループに適用された QoS ポリシーの例

次に、特定の QoS ポリシーがリモート ユーザの 2 つのグループに適用されている例を示します。2 つのプロファイルが、IKE を介した最初の接続上でリモート ユーザが特定のプロファイルにマッピングされるように設定されています。そのプロファイルから、そのリモートに対して作成されたすべての IPsec SA が特定の QoS グループでマーキングされます。トラフィックが発信インターフェイスを出ると、QoS サービスによって、その発信インターフェイス上で適用されているサービス ポリシーを構成するクラス マップ内で指定された QoS グループで IPsec 設定 QoS グループがマッピングされます。

```
version 12.3
!
aaa authentication login group group radius
aaa authorization network autho local
aaa accounting update periodic 1
```

```
aaa session-id common
ip subnet-zero
!
!
ip cef
no ip domain lookup
!
class-map match-all yellow
 match qos-group 3
class-map match-all blue
match qos-group 2
!
!
policy-map clients
 class blue
  set precedence 5
 class yellow
  set precedence 7
!
!
crypto isakmp policy 1
 encr aes
 hash sha
 authentication pre-share
 group 14
 lifetime 300
!
crypto isakmp keepalive 10 periodic
crypto isakmp xauth timeout 20
!
crypto isakmp client configuration group blue
 key cisco
 dns 10.2.2.2 10.2.2.3
 wins 10.6.6.6
 pool blue
 save-password
 include-local-lan
 backup-gateway corky1.cisco.com
!
crypto isakmp client configuration group yellow
 dns 10.2.2.2 10.2.2.3
 wins 10.6.6.5
 pool yellow
!
crypto isakmp profile blue
   match identity group cisco
   client authentication list autho
   isakmp authorization list autho
   client configuration address respond
   qos-group 2
crypto isakmp profile yellow
   match identity group yellow
   match identity address 10.0.0.11 255.255.255.255
   client authentication list autho
   isakmp authorization list autho
   client configuration address respond
   qos-group 3
!
!
crypto ipsec transform-set combo ah-sha-hmac esp-aes esp-sha-hmac
crypto ipsec transform-set client esp-aes esp-sha-hmac comp-lzs
!
crypto dynamic-map mode 1
 set security-association lifetime seconds 180
```

```
 set transform-set client
 set isakmp-profile blue
 reverse-route
crypto dynamic-map mode 2
 set transform-set combo
 set isakmp-profile yellow
 reverse-route
!
crypto map mode 1 ipsec-isakmp dynamic mode
!
interface FastEthernet0/0
 ip address 10.0.0.110 255.255.255.0
 no ip redirects
 no ip proxy-arp
 no ip mroute-cache
 duplex half
 no cdp enable
 crypto map mode
 service-policy out clients
!
ip local pool yellow 192.168.2.1 192.168.2.10
ip local pool blue 192.168.6.1 192.168.6.6
no ip classless
!
radius-server host 10.0.0.13 auth-port 1645 acct-port 1646
radius-server key XXXXXX
radius-server vsa send accounting
radius-server vsa send authentication
```

show crypto isakmp profile コマンドの例

次の出力では、QoS グループ「2」が ISAKMP プロファイル「blue」に適用され、QoS グループ「3」が ISAKMP プロファイル「yellow」に適用されていることを示しています。

```
Router# show crypto isakmp profile
ISAKMP PROFILE blue
   Identities matched are:
    group blue
   QoS Group 2 is applied
ISAKMP PROFILE yellow
   Identities matched are:
    ip-address 10.0.0.13 255.255.255.255
    group yellow
   QoS Group 3 is applied
```

show crypto ipsec sa コマンドの例

次の出力では、QoS グループが IPsec SA の特定のペアに適用されていることを示しています。

```
Router# show crypto ipsec sa
interface: FastEthernet0/0
    Crypto map tag: mode, local addr. 10.0.0.110
   protected vrf:
   local  ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
   remote ident (addr/mask/prot/port): (10.12.12.0/255.255.255.0/0/0)
   current_peer: 10.0.0.11:500
     PERMIT, flags={}
    #pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
```

```
#pkts decaps: 0, #pkts decrypt: 0, #pkts verify: 0
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 0, #pkts compr. failed: 0
#pkts not decompressed: 0, #pkts decompress failed: 0
#send errors 0, #recv errors 0
 qos group is set to 2
```

その他の参考資料

ここでは、IPsec と Quality of Service 機能の関連資料について説明します。

関連資料

関連項目	マニュアル タイトル
IPSec	IPsec を使用した VPN のセキュリティの設定
QoS オプション	『*Cisco IOS Quality of Service Solutions Configuration Guide*』（Cisco.com）
QoS コマンド	『*Cisco IOS Quality of Service Solutions Command Reference*』
セキュリティ コマンド	『*Cisco IOS Security Command Reference*』
推奨される暗号化アルゴリズム	『Next Generation Encryption』

標準

標準	タイトル
この機能がサポートする新しい規格または変更された規格はありません。	--

MIB

MIB	MIB のリンク
この機能によってサポートされる新しい MIB または変更された MIB はありません。	選択したプラットフォーム、Cisco IOS リリース、およびフィーチャ セットに関する MIB を探してダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

RFC

RFC	タイトル
この機能でサポートが追加または変更されたRFCはありません。	--

シスコのテクニカル サポート

説明	リンク
シスコのサポートWebサイトでは、シスコの製品やテクノロジーに関するトラブルシューティングにお役立ていただけるように、マニュアルやツールをはじめとする豊富なオンライン リソースを提供しています。 お使いの製品のセキュリティ情報や技術情報を入手するために、Cisco Notification Service（Field Noticeからアクセス）、Cisco Technical Services Newsletter、Really Simple Syndication（RSS）フィードなどの各種サービスに加入できます。 シスコのサポートWebサイトのツールにアクセスする際は、Cisco.comのユーザID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

IPsec と Quality of Service の機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *267 : IPsec* と *Quality of Service* の機能情報

機能名	リリース	機能情報
IPsec と Quality of Service	Cisco IOS XE Release 3.9S	IPsec と Quality of Service 機能を使用すれば、Cisco IOS Quality of Service（QoS）ポリシーを、QoS グループに基づいて、IP Security（IPsec）パケット フローに適用できます。QoS グループは、現在の Internet Security Association and Key Management Protocol（ISAKMP）プロファイルに適用できます。 次のコマンドが導入または変更されました。 **qos-group.**

第 202 章

VRF 認識 IPSec

VRF-Aware IPsec 機能には、マルチプロトコル ラベル スイッチング（MPLS）バーチャル プライベート ネットワーク（VPN）に対する IP Security（IPsec）トンネル マッピングが導入されています。

（注） セキュリティに対する脅威は、脅威からの保護に役立つ暗号化技術と同様に絶え間なく変化しています。シスコの暗号化に関する最新の推奨事項の詳細は、『Next Generation Encryption』（NGE）ホワイトペーパーを参照してください。

VRF-Aware IPsec に関する制約事項

- クリプト マップ設定を使用して VRF-Aware IPsec 機能を設定し、Inside VRF（IVRF）が Front Door VRF（FVRF）とは異なる場合、ユニキャスト RPF（uRPF）がクリプト マップ インターフェイス上でイネーブルになっていると、この機能と uRPFの相互運用はできなくなります。ネットワークに URPF が必要な場合、クリプト マップではなく、IPsec の Virtual Tunnel Interface（VTI）を使用することを推奨します。
- VRF-Aware IPsec 機能では、VRF 間における IPsec トンネル マッピングはできません。たとえば、VRF vpn1 から VRF vpn2 への IPsec トンネル マッピングはできません。
- VRF-Aware IPsec 機能をクリプト マップと使用した場合、このクリプト マップではグローバル VRF を IVRF として使用し、非グローバル VRF を FVRF として使用することはできません。しかし、仮想トンネルインターフェイスに基づく設定にその制限はありません。

VTI またはダイナミック VTI（DVTI）を使用した場合、グローバル VRF を IVRF と使用すると同時に、非グローバル VRF を FVRF として使用できます。

- ISAKMP プロファイルとキーリング内で VRF と一緒にローカルアドレスを使用している場合は、**local-address** コマンドに VRF を含める必要があります。

VRF-Aware IPsec に関する情報

VRF インスタンス

VRF は、VPN ごとのルーティング情報リポジトリであり、プロバイダー エッジ（PE）ルータに接続されたカスタマー サイトの VPN メンバーシップが定義されています。VRF は、IP ルーティング テーブル、派生シスコ エクスプレス フォワーディング（CEF）テーブル、転送テーブルを使用するインターフェイスのセット、ルーティング テーブルに含まれる情報を制御するルールおよびルーティング プロトコル パラメータのセットで構成されています。各 VPN カスタマーに対して、別個の一連のルーティング テーブルおよび Cisco Express Forwarding（CEF）テーブルが維持されます。

MPLS 配信プロトコル

MPLS配信プロトコルは、高性能のパケット転送テクノロジーであり、データ リンク層スイッチングのパフォーマンスおよびトラフィック管理機能と、ネットワーク層ルーティングのスケーラビリティ、柔軟性、およびパフォーマンスが統合されています。

VRF-Aware IPsec 機能の概要

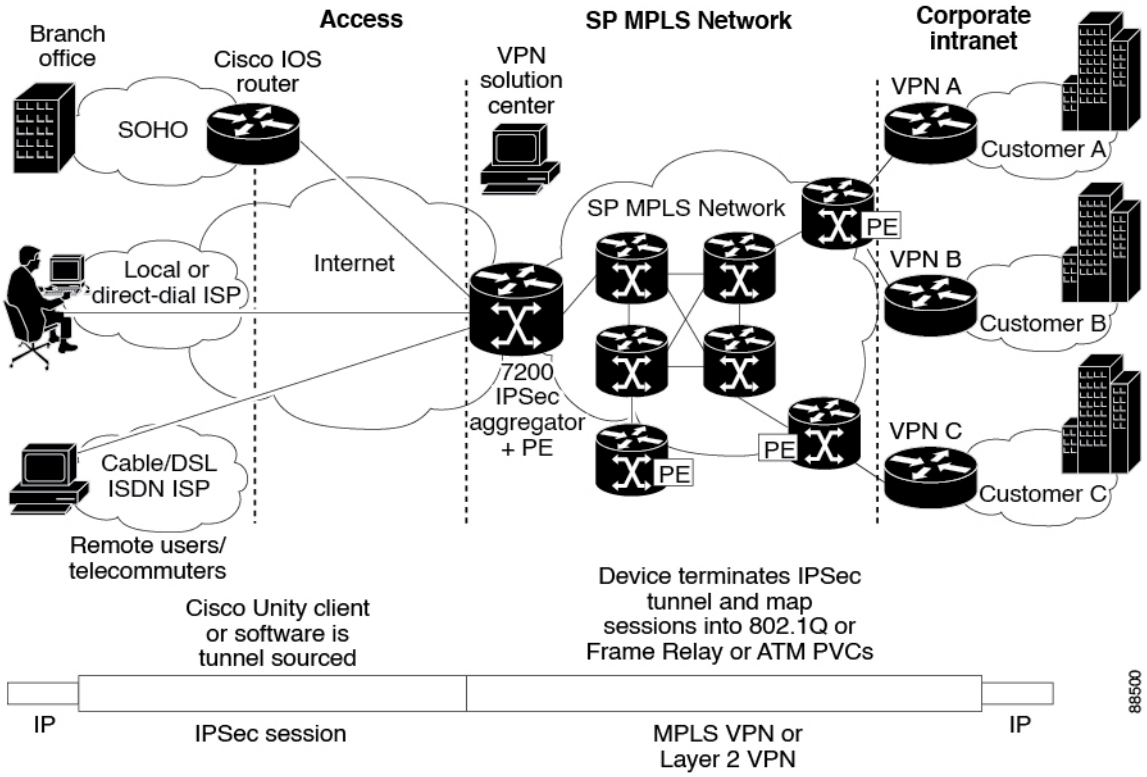
Front Door VRF（FVRF）と Inside VRF（IVRF）が、この機能を理解するうえで重要な概念となります。

各 IPsec トンネルは、2 つの VRF ドメインに関連付けられます。外部のカプセル化されたパケットは 1 つの VRF ドメイン（本マニュアルでは FVRF と呼びます）に所属し、内部の保護された IP パケットは IVRF と呼ばれる別のドメインに所属します。言い換えると、IPsec トンネルのローカルエンドポイントはFVRFに所属し、内部パケットの発信元および宛先アドレスは IVRF に所属します。

1 つ以上の IPsec トンネルを、単一のインターフェイス上で終了できます。これらのトンネルのすべての FVRF は同じものであり、そのインターフェイス上で設定されている VRF に設定されます。これらのトンネルの IVRF は異なる可能性があり、クリプト マップ エントリに付加された Security Association and Key Management Protocol（ISAKMP）プロファイル内で定義されている VRF に依存します。

次の図は、MPLS およびレイヤ 2 VPN に対する IPsec のシナリオを示しています。

図 *101 : MPLS* およびレイヤ *2 VPN* に対する *IPsec*



IPsec トンネルへのパケット フロー

- VPN パケットが、サービス プロバイダー MPLS のバックボーン ネットワークから PE へ到着し、インターネット方向のインターフェイスを介してルーティングされます。
- パケットが Security Policy Database（SPD）と照合され、IPsec カプセル化されます。SPD には、IVRF とアクセス コントロール リスト（ACL）が格納されています。
- 次に、IPsec カプセル化パケットが、FVRF ルーティング テーブルによって転送されます。

IPsec トンネルからのパケット フロー

- IPsec カプセル化パケットが、リモート IPsec エンドポイントから PE ルータに到着します。
- IPsec によって、セキュリティ パラメータ インデックス（SPI）、宛先、およびプロトコルのセキュリティ アソシエーション（SA）検索が実行されます。
- パケットが、SA によってカプセル開放され、IVRF に関連付けられます。
- パケットが、IVRF ルーティング テーブルによって、さらに転送されます。

VRF-Aware IPsec の設定方法

暗号化キーリングの設定

暗号化キーリングは、事前共有キーおよびRivest, Shamir, and Adelman（RSA）公開キーのリポジトリです。Cisco IOS ルータ上には、0 以上のキーリングを設定できます。

手順の概要

1. **enable**
2. **configure terminal**
3. **crypto keyring** *keyring-name* [**vrf** *fvrf-name*]
4. **description** *string*
5. **pre-shared-key** {**address** *address* [*mask*] | **hostname** *hostname*} **key** *key*
6. **rsa-pubkey** {**address** *address* | **name** *fqdn*} [**encryption** | **signature**]
7. **address** *ip-address*
8. **serial-number** *serial-number*
9. **key-string**
10. **text**
11. **quit**
12. **exit**
13. **exit**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**crypto keyring** *keyring-name* [**vrf** *fvrf-name*] 例： `Router (config)# crypto keyring VPN1`	キーリングの名前として *keyring-name* を指定してキーリングを定義し、キーリング コンフィギュレーション モードを開始します。 • （任意）**vrf** キーワードおよび *fvrf-name* 引数は、キーリングがFront Door Virtual Routing and Forwarding（FVRF）にバインドされることを意味します。ローカルエンドポイントがFVRF

	コマンドまたはアクション	目的
		内にある場合、キーリング内のキーが検索されます。**vrf** を指定しない場合、キーリングはグローバルにバインドされます。
ステップ 4	**description** *string* 例： 例： `Router (config-keyring)# description The keys for VPN1`	（任意）キーリングに関する 1 行の説明です。
ステップ 5	**pre-shared-key** {**address** *address* [*mask*] | **hostname** *hostname*} **key** *key* 例： `Router (config-keyring)# pre-shared-key address 10.72.23.11 key VPN1`	（任意）アドレスまたはホスト名によって、事前共有キーを定義します。
ステップ 6	**rsa-pubkey** {**address** *address* | **name** *fqdn*} [**encryption** | **signature**] 例： `Router(config-keyring)# rsa-pubkey name host.vpn.com`	（任意）アドレスまたはホスト名によって RSA 公開キーを定義し、rsa-pubkey コンフィギュレーション モードを開始します。 • オプションの **encryption** キーワードでは、キーが暗号化のために使用されることが指定されます。 • オプションの **signature** キーワードでは、キーがシグニチャ用に使用されることが指定されます。デフォルトでは、キーはシグニチャ用に使用されます。
ステップ 7	**address** *ip-address* 例： `Router(config-pubkey-key)# address 10.5.5.1`	（任意）RSA 公開キーの IP アドレスを定義します。
ステップ 8	**serial-number** *serial-number* 例： `Router(config-pubkey-key)# serial-number 1000000`	（任意）公開キーのシリアル番号を指定します。値は 0 から始まり、無制限です。
ステップ 9	**key-string** 例： `Router (config-pubkey-key)# key-string`	公開キーを定義するためのテキスト モードを開始します。

	コマンドまたはアクション	目的
ステップ 10	**text** 例： `Router (config-pubkey)# 00302017 4A7D385B 1234EF29 335FC973`	公開キーを指定します。 （注） この手順で追加できる公開キーは 1 つだけです。
ステップ 11	**quit** 例： `Router (config-pubkey)# quit`	公開キー コンフィギュレーション モードを終了します。
ステップ 12	**exit** 例： `Router (config-pubkey)# exit`	キーリング コンフィギュレーション モードに戻ります。
ステップ 13	**exit** 例： `Router(config-keyring)# exit#`	グローバル コンフィギュレーション モードに戻ります。

ISAKMP プロファイルの設定

ISAKMP プロファイルは、一連のピアのインターネット キー交換（IKE）フェーズ 1 および IKE フェーズ 1.5 設定のリポジトリです。ISAKMP プロファイルでは、IKE フェーズ 1 およびフェーズ 1.5 交換中に、キープアライブ、トラストポイント、ピアの ID、および XAUTH AAA リストなどのアイテムが定義されます。Cisco IOS ルータ上には、0 以上の ISAKMP プロファイルを設定できます。

（注） ルータから認証局（CA）へのトラフィック（認証および登録用、または、証明書失効リスト（CRL）取得用）、または Lightweight Directory Access Protocol（LDAP）サーバーへのトラフィック（CRL 取得用）を VRF を介してルーティングする必要がある場合、トラストポイントに **vrf** コマンドを追加する必要があります。追加しない場合、トラフィックはデフォルトのルーティング テーブルを使用します。

- プロファイルに 1 つ以上のトラストポイントが指定されていない場合、ルータ内のすべてのトラストポイントが使用されて、ピアの証明書の確認が試行されます（IKE メイン モードまたはシグニチャ認証）。1 つ以上のトラストポイントが指定されている場合、それらのトラストポイントだけが使用されます。

（注） IKE を開始するルータと IKE 要求に応答するルータのトラストポイント設定は互いに対称的である必要があります。たとえば、RSA シグニチャ暗号化および認証を実行中の応答ルータ（IKE メイン モード）では、CERT-REQ ペイロードの送信時に、グローバル コンフィギュレーション内で定義されたトラストポイントが使用されている場合があります。しかし、そのルータでは、証明書の確認のために ISAKMP プロファイル内で定義されたトラストポイントの制限リストが使用されている場合があります。ピア（IKE の発信側）が、トラストポイントが応答ルータのグローバル リスト内に存在するが、応答ルータの ISAKMP プロファイル内には存在しない証明書を使用するように設定されている場合、その証明書は拒否されます（ただし、開始ルータによって、応答ルータのグローバルコンフィギュレーション内のトラストポイントが認識されていない場合は、その証明書は認証されます）。

>

手順の概要

1. **enable**
2. **configure terminal**
3. **crypto isakmp profile** *profile-name*
4. **description** *string*
5. **vrf** *ivrf-name*
6. **keepalive** *seconds* **retry** *retry-seconds*
7. **self-identity** {**address** | **fqdn**| **user-fqdn** *user-fqdn*}
8. **keyring** *keyring-name*
9. **ca trust-point** {*trustpoint-name*}
10. **match identity** {**group** *group-name* | **address** *address* [*mask*] [*fvrf*] | **host** *host-name* | **host domain** *domain-name* | **user** *user-fqdn* | **user domain** *domain-name*}
11. **client configuration address** {**initiate** | **respond**}
12. **client authentication list** *list-name*
13. **isakmp authorization list** *list-name*
14. **initiate mode aggressive**
15. **exit**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 3	**crypto isakmp profile** *profile-name* 例： `Router (config)# crypto isakmp profile vpnprofile`	Internet Security Association and Key Management Protocol（ISAKMP）プロファイルを定義し、isakmp プロファイル コンフィギュレーション モードを開始します。
ステップ 4	**description** *string* 例： `Router (conf-isa-prof)# description configuration for VPN profile`	（任意）ISAKMP プロファイルの 1 行の説明を指定します。
ステップ 5	**vrf** *ivrf-name* 例： `Router (conf-isa-prof)# vrf VPN1`	（任意）IPsec トンネルを Virtual Routing and Forwarding（VRF）インスタンスにマッピングします。 （注） VRF は、Security Policy Database（SPD）の照合のためのマッチングのためのセレクタにもなります。VRF が ISAKMP プロファイル内で指定されていない場合、IPsec トンネルの IVRF は、その FVRF と同じになります。
ステップ 6	**keepalive** *seconds* **retry** *retry-seconds* 例： `Router (conf-isa-prof)# keepalive 60 retry 5`	（任意）ゲートウェイに対して、Dead Peer Detection（DPD）メッセージのピアへの送信を許可します。 • 定義しない場合、ゲートウェイではグローバル コンフィギュレーション値が使用されます。 • *seconds*：DPD メッセージ間の秒数。指定できる範囲は 10 ～ 3600 秒です。 • **retry** *retry-seconds*：DPD メッセージがエラーになった場合の、リトライ間の秒数指定できる範囲は 2 ～ 60 秒です。
ステップ 7	**self-identity** {**address** | **fqdn**| **user-fqdn** *user-fqdn*} 例： `Router (conf-isa-prof)# self-identity address`	（任意）ローカル IKE によって、リモート ピアに対して IKE 自身を識別させるために使用される、ID を指定します。 • 定義しない場合、IKE ではグローバル コンフィギュレーション値が使用されます。 • **address**：出力インターフェイスの IP アドレスを使用します。 • **fqdn--**：ルータの完全修飾ドメイン名（FQDN）を使用します。

	コマンドまたはアクション	目的
		• **user-fqdn**：指定された値を使用します。
ステップ 8	**keyring** *keyring-name* 例： `Router (conf-isa-prof)# keyring VPN1`	（任意）フェーズ1認証用に使用するキーリングを指定します。 • キーリングを指定しない場合、グローバルキー定義が使用されます。
ステップ 9	**ca trust-point** {*trustpoint-name*} 例： `Router (conf-isa-prof)# ca trustpoint VPN1-trustpoint`	（任意）Rivest、Shamir、Adelman（RSA）証明書を確認するためのトラストポイントを指定します。 • ISAKMP プロファイル内でトラストポイントが指定されていない場合、Cisco IOS ルータ上で設定されているすべてのトラストポイントが証明書の確認に使用されます。
ステップ 10	**match identity** {**group** *group-name* | **address** *address* [*mask*] [*fvrf*] | **host** *host-name* | **host domain** *domain-name* | **user** *user-fqdn* | **user domain** *domain-name*} 例： `Router (conf-isa-prof)# match identity address 10.1.1.1`	照合されるクライアント IKE の ID を指定します。 • **group** *group-name*：*group-name* と ID タイプ ID_KEY_ID を照合します。また、*group-name* と認定者名（DN）の組織ユニット（OU）フィールドも照合します。 • **address** *address* [*mask*] *fvrf*：*address* と ID タイプ ID_IPV4_ADDR を照合します。*Mask* 引数を使用して、アドレスの範囲を指定できます。*fvrf* 引数では、アドレスが Front Door Virtual Routing and Forwarding（FVRF）にあることを指定します。 • **host** *hostname*：*hostname* と ID タイプ ID_FQDN を照合します。 • **host domain** *domain-name*：*domain-name* を、ドメイン名が *domain-name* と同じ IP タイプ ID_FQDN と照合します。このコマンドを使用して、ドメイン内のすべてのホストを照合します。 • **user** *username*：*username* と ID タイプ ID_USER_FQDN を照合します。 • **user domain** *domainname*：ドメイン名が *domainname* と一致する ID タイプ ID_USER_FQDN を照合します。

	コマンドまたはアクション	目的
ステップ 11	**client configuration address** {**initiate** | **respond**} 例： `Router (conf-isa-prof)# client configuration address initiate`	（任意）モード設定交換を開始するか、モード設定要求に応答するかを指定します。
ステップ 12	**client authentication list** *list-name* 例： `Router (conf-isa-prof)# client authentication list xauthlist`	（任意）Extended Authentication（XAUTH）交換中にリモート クライアントを認証するために使用する AAA（認証、許可、アカウンティング）。
ステップ 13	**isakmp authorization list** *list-name* 例： `Router (conf-isa-prof)# isakmp authorization list ikessaaalist`	（任意）フェーズ 1 キーおよびその他の AV のペアを受信するためのネットワーク認証サーバ。
ステップ 14	**initiate mode aggressive** 例： `Router (conf-isa-prof)# initiate mode aggressive`	（任意）アグレッシブ モード交換を開始します。 • 指定しない場合、IKE によって、メイン モード交換が常に開始されます。
ステップ 15	**exit** 例： `Router (conf-isa-prof)# exit`	グローバル コンフィギュレーション モードに戻ります。

次の作業

暗号マップ上における ISAKMP プロファイルの設定 （2932 ページ） に進みます。

暗号マップ上における ISAKMP プロファイルの設定

ISAKMP プロファイルを、クリプト マップに適用する必要があります。ISAKMP プロファイル上の IVRF は、VPN トラフィックの照合時にセレクタとして使用されます。ISAKMP プロファイル上に IVRF が存在しない場合、IVRF は FVRF と同じになります。クリプト マップ上の ISAKMP プロファイルを設定するには、次の作業を実行します。

始める前に

クリプト マップ上で ISAKMP プロファイルを設定する前に、ルータに対して基本 IPsec の設定を行っておく必要があります。

手順の概要

1. **enable**
2. **configure terminal**
3. **crypto map** *map-name* **isakmp-profile** *isakmp-profile-name*
4. **set isakmp-profile** *profile-name*
5. **exit**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**crypto map** *map-name* **isakmp-profile** *isakmp-profile-name* 例： `Router (config)# crypto map vpnmap isakmp-profile vpnprofile`	（任意）クリプト マップ セット用に Internet Key Exchange and Key Management Protocol（ISAKMP）プロファイルを指定し、クリプトマップ コンフィギュレーション モードを開始します。 • ISAKMP プロファイルは、IKE 交換中に使用されます。
ステップ 4	**set isakmp-profile** *profile-name* 例： `Router (config-crypto-map)# set isakmp-profile vpnprofile`	（任意）トラフィックがクリプト マップ エントリと一致した際に使用する ISAKMP プロファイルを指定します。
ステップ 5	**exit** 例： `Router (config-crypto-map)# exit`	グローバル コンフィギュレーション モードに戻ります。

IKE フェーズ 1 ネゴシエーション中に拡張認証を無視する設定

IKE フェーズ 1 ネゴシエーション中に XAUTH を無視するには、**no crypto xauth** コマンドを使用します。Unity クライアントの拡張認証が不要な場合、 **no crypto xauth** コマンドを使用します。

手順の概要

1. **enable**
2. **configure terminal**
3. **no crypto xauth** *interface*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**no crypto xauth** *interface* 例： `Router(config)# no crypto xauth ethernet0`	インターフェイスの IP アドレスを宛先とする要求の XAUTH 提案を無視します。デフォルトでは、IKE によって、XAUTH 提案が処理されます。

VRF-Aware IPsec の確認

VRF-Aware IPsec の設定を確認するには、次の **show** コマンドを使用します。これらの **show** コマンドによって、設定情報およびセキュリティ アソシエーション（SA）を表示できます。

手順の概要

1. **enable**
2. **show crypto ipsec sa** [**map** *map-name*| **address** | **identity** | **interface** *interface* | **peer** [**vrf** *fvrf-name*] **address** | **vrf** *ivrf-name*] [**detail**]
3. **show crypto isakmp key**
4. **show crypto isakmp profile**
5. **show crypto key pubkey-chain rsa**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。

	コマンドまたはアクション	目的
ステップ 2	**show crypto ipsec sa** [**map** *map-name*| **address** | **identity** | **interface** *interface* | **peer** [**vrf** *fvrf-name*] **address** | **vrf** *ivrf-name*] [**detail**] 例： `Router# show crypto ipsec sa vrf vpn1`	現在の SA によって使用される設定の表示を許可します。
ステップ 3	**show crypto isakmp key** 例： `Router# show crypto isakmp key`	すべてのキーリングおよびその事前共有キーを一覧表示します。 • このコマンドを使用して、クリプトキーリング設定を確認します。
ステップ 4	**show crypto isakmp profile** 例： `Router# show crypto isakmp profile`	すべての ISAKMP プロファイルおよびその設定を一覧表示します。
ステップ 5	**show crypto key pubkey-chain rsa** 例： `Router# show crypto key pubkey-chain rsa`	ルータに保存されている、ピアの RSA 公開キーを表示します。 • 出力が、公開キーが所属するキーリングを表示するように拡張されます。

セキュリティ アソシエーションのクリア

次の **clear** コマンドによって、SA をクリアできます。

手順の概要

1. **enable**
2. **clear crypto sa** [**counters** | **map** *map-name* | **peer**[**vrf** *fvrf-name*] *address* | **spi** *address* {**ah** | **esp**} *spi* | **vrf** *ivrf-name*]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**clear crypto sa** [**counters** | **map** *map-name* | **peer**[**vrf** *fvrf-name*] *address* | **spi** *address* {**ah** | **esp**} *spi* | **vrf** *ivrf-name*]	IPsec SA をクリアします。

	コマンドまたはアクション	目的
	例： `Router# clear crypto sa vrf VPN1`	

VRF-Aware IPsec のトラブルシューティング

VRF-Aware IPsec のトラブルシューティングを行うには、次の **debug** コマンドを使用します。

手順の概要

1. **enable**
2. **debug crypto ipsec**
3. **debug crypto isakmp**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**debug crypto ipsec** 例： `Router# debug crypto ipsec`	IP セキュリティ（IPsec）イベントを表示します。
ステップ 3	**debug crypto isakmp** 例： `Router(config)# debug crypto isakmp`	IKE に関するメッセージを表示します。

VRF-Aware IPsec のデバッグ例

次に、VRF-aware IPsec 設定のサンプル デバッグ出力を示します。

IPsec PE

```
Router# debug crypto ipsec
Crypto IPSEC debugging is on
IPSEC-PE#debug crypto isakmp
Crypto ISAKMP debugging is on
IPSEC-PE#debug crypto isakmp d
04:31:28: ISAKMP (0:12): purging SA., sa=6482B354, delme=6482B354
04:31:28: ISAKMP: Unlocking IKE struct 0x63C142F8 for declare_sa_dead(), count 0
IPSEC-PE#debug crypto isakmp detail
```

```
Crypto ISAKMP internals debugging is on
IPSEC-PE#
IPSEC-PE#
IPSEC-PE#
04:32:07: ISAKMP: Deleting peer node by peer_reap for 10.1.1.1: 63C142F8
04:32:55: ISAKMP cookie gen for src 172.16.1.1 dst 10.1.1.1
04:32:55: ISAKMP cookie 3123100B DC887D4E
04:32:55: ISAKMP cookie gen for src 10.1.1.1 dst 172.68.1.1
04:32:55: ISAKMP cookie AA8F7B41 49A60E88
04:32:55: ISAKMP cookie gen for src 172.16.1.1 dst 10.1.1.1
04:32:55: ISAKMP cookie 3123100B DBC8E125
04:32:55: ISAKMP cookie gen for src 10.1.1.1 dst 172.16.1.1
04:32:55: ISAKMP cookie AA8F7B41 B4BDB5B7
04:32:55: ISAKMP (0:0): received packet from 10.1.1.1 dport 500 sport 500 Global (N) NEW
 SA
04:32:55: ISAKMP: local port 500, remote port 500
04:32:55: ISAKMP: hash from 729FA94 for 619 bytes
04:32:55: ISAKMP: Packet hash:
64218CC0:                   B91E2C70 095A1346          9.,p.Z.F
64218CD0: 0EDB4CA6 8A46784F B314FD3B 00        .[L&.FxO.};.
04:32:55: ISAKMP cookie gen for src 10.1.1.1 dst 172.18.1.1
04:32:55: ISAKMP cookie AA8F7B41 F7ACF384
04:32:55: ISAKMP cookie gen for src 10.1.1.1 dst 172.18.1.1
04:32:55: ISAKMP cookie AA8F7B41 0C07C670
04:32:55: ISAKMP: insert sa successfully sa = 6482B354
04:32:55: ISAKMP (0:13): processing SA payload. message ID = 0
04:32:55: ISAKMP (0:13): processing ID payload. message ID = 0
04:32:55: ISAKMP (0:13): peer matches vpn2-ra profile
04:32:55: ISAKMP: Looking for a matching key for 10.1.1.1 in default
04:32:55: ISAKMP: Created a peer struct for 10.1.1.1, peer port 500
04:32:55: ISAKMP: Locking peer struct 0x640BBB18, IKE refcount 1 for
crypto_ikmp_config_initialize_sa
04:32:55: ISAKMP (0:13): Setting client config settings 648252B0
04:32:55: ISAKMP (0:13): (Re)Setting client xauth list and state
04:32:55: ISAKMP (0:13): processing vendor id payload
04:32:55: ISAKMP (0:13): vendor ID seems Unity/DPD but major 157 mismatch
04:32:55: ISAKMP (0:13): vendor ID is NAT-T v3
04:32:55: ISAKMP (0:13): processing vendor id payload
04:32:55: ISAKMP (0:13): vendor ID seems Unity/DPD but major 123 mismatch
04:32:55: ISAKMP (0:13): vendor ID is NAT-T v2
04:32:55: ISAKMP (0:13) Authentication by xauth preshared
04:32:55: ISAKMP (0:13): Checking ISAKMP transform 1 against priority 1 policy
04:32:55: ISAKMP:      encryption AES-CBC
04:32:55: ISAKMP:      hash SHA
04:32:55: ISAKMP:      default group 14
04:32:55: ISAKMP:      auth XAUTHInitPreShared
04:32:55: ISAKMP:      life type in seconds
04:32:55: ISAKMP:      life duration (VPI) of 0x0 0x20 0xC4 0x9B
04:32:55: ISAKMP (0:13): atts are acceptable. Next payload is 3
04:32:55: ISAKMP (0:13): processing vendor id payload
04:32:55: ISAKMP (0:13): vendor ID seems Unity/DPD but major 157 mismatch
04:32:55: ISAKMP (0:13): vendor ID is NAT-T v3
04:32:55: ISAKMP (0:13): processing vendor id payload
04:32:55: ISAKMP (0:13): vendor ID seems Unity/DPD but major 123 mismatch
04:32:55: ISAKMP (0:13): vendor ID is NAT-T v2
04:32:55: ISAKMP (0:13): processing KE payload. message ID = 0
04:32:55: ISAKMP (0:13): processing NONCE payload. message ID = 0
04:32:55: ISAKMP (0:13): processing vendor id payload
04:32:55: ISAKMP (0:13): vendor ID is DPD
04:32:55: ISAKMP (0:13): processing vendor id payload
04:32:55: ISAKMP (0:13): vendor ID seems Unity/DPD but major 175 mismatch
04:32:55: ISAKMP (0:13): vendor ID is XAUTH
04:32:55: ISAKMP (0:13): processing vendor id payload
04:32:55: ISAKMP (0:13): claimed IOS but failed authentication
```

```
04:32:55: ISAKMP (0:13): processing vendor id payload
04:32:55: ISAKMP (0:13): vendor ID is Unity
04:32:55: ISAKMP (0:13): Input = IKE_MESG_FROM_PEER, IKE_AM_EXCH
04:32:55: ISAKMP (0:13): Old State = IKE_READY  New State = IKE_R_AM_AAA_AWAIT
04:32:55: ISAKMP cookie gen for src 11.1.1.1 dst 172.16.1.1
04:32:55: ISAKMP cookie AA8F7B41 7AE6E1DF
04:32:55: ISAKMP:        isadb_post_process_list: crawler: 4 AA 31 (6482B354)
04:32:55:       crawler my_cookie AA8F7B41 F7ACF384
04:32:55:        crawler his_cookie E46E088D F227FE4D
04:32:55: ISAKMP: got callback 1
04:32:55: ISAKMP (0:13): SKEYID state generated
04:32:55: ISAKMP: Unity/DPD ID: vendor_id_payload:
        next: 0xD, reserved: 0x0, len 0x14
04:32:55: ISAKMP: Unity/DPD ID payload dump:
63E66D70:                            0D000014              ....
63E66D80: 12F5F28C 457168A9 702D9FE2 74CC0100  .ur.Eqh)p-.btL..
63E66D90: 00                                   .
04:32:55: ISAKMP: Unity/DPD ID: vendor_id_payload:
        next: 0xD, reserved: 0x0, len 0x14
04:32:55: ISAKMP: Unity/DPD ID payload dump:
63E66D90: 0D000014 AFCAD713 68A1F1C9 6B8696FC  ..../JW.h!qIk..|
63E66DA0: 77570100 00                          wW...
04:32:55: ISAKMP (0:13): constructed NAT-T vendor-03 ID
04:32:55: ISAKMP (0:13): SA is doing pre-shared key authentication plus XAUTH using id
type ID_IPV4_ADDR
04:32:55: ISAKMP (13): ID payload
        next-payload : 10
        type         : 1
        addr         : 172.16.1.1
        protocol     : 17
        port         : 0
        length       : 8
04:32:55: ISAKMP (13): Total payload length: 12
04:32:55: ISAKMP (0:13): constructed HIS NAT-D
04:32:55: ISAKMP (0:13): constructed MINE NAT-D
04:32:55: ISAKMP (0:13): sending packet to 10.1.1.1 my_port 500 peer_port 500 (R)
AG_INIT_EXCH
04:32:55: ISAKMP (0:13): Input = IKE_MESG_FROM_AAA, PRESHARED_KEY_REPLY
04:32:55: ISAKMP (0:13): Old State = IKE_R_AM_AAA_AWAIT  New State = IKE_R_AM2
04:32:55: ISAKMP cookie gen for src 172.16.1.1 dst 10.1.1.1
04:32:55: ISAKMP cookie 3123100B D99DA70D
04:32:55: ISAKMP cookie gen for src 10.1.1.1 dst 172.16.1.1
04:32:55: ISAKMP cookie AA8F7B41 9C69F917
04:32:55: ISAKMP:        isadb_post_process_list: crawler: 5 21FF 1 (6482B354)
04:32:55:       crawler my_cookie AA8F7B41 F7ACF384
04:32:55:        crawler his_cookie E46E088D F227FE4D
04:32:55: ISAKMP cookie gen for src 172.16.1.1 dst 10.1.1.1
04:32:55: ISAKMP cookie 3123100B 00583224
04:32:55: ISAKMP cookie gen for src 10.1.1.1 dst 172.16.1.1
04:32:55: ISAKMP cookie AA8F7B41 C1B006EE
04:32:55: ISAKMP:        isadb_post_process_list: crawler: 5 21FF 1 (6482B354)
04:32:55:       crawler my_cookie AA8F7B41 F7ACF384
04:32:55:        crawler his_cookie E46E088D F227FE4D
04:32:55: ISAKMP (0:13): received packet from 10.1.1.1 dport 500 sport 500 Global (R)
AG_INIT_EXCH
04:32:55: ISAKMP: hash from 7003A34 for 132 bytes
04:32:55: ISAKMP: Packet hash:
64218CC0:                   D1202D99 2BB49D38          Q -.+4.8
64218CD0: B8FBB1BE 7CDC67D7 4E26126C 63        8{1>|\gWN&.lc
04:32:55: ISAKMP (0:13): processing HASH payload. message ID = 0
04:32:55: ISAKMP:received payload type 17
04:32:55: ISAKMP (0:13): Detected NAT-D payload
04:32:55: ISAKMP (0:13): recalc my hash for NAT-D
04:32:55: ISAKMP (0:13): NAT match MINE hash
```

```
04:32:55: ISAKMP:received payload type 17
04:32:55: ISAKMP (0:13): Detected NAT-D payload
04:32:55: ISAKMP (0:13): recalc his hash for NAT-D
04:32:55: ISAKMP (0:13): NAT match HIS hash
04:32:55: ISAKMP (0:13): processing NOTIFY INITIAL_CONTACT protocol 1
        spi 0, message ID = 0, sa = 6482B354
04:32:55: ISAKMP (0:13): Process initial contact,
bring down existing phase 1 and 2 SA's with local 172.16.1.1 remote 10.1.1.1 remote port
 500
04:32:55: ISAKMP (0:13): returning IP addr to the address pool
04:32:55: ISAKMP cookie gen for src 10.1.1.1 dst 172.16.1.1
04:32:55: ISAKMP cookie AA8F7B41 05D315C5
04:32:55: ISAKMP cookie gen for src 172.16.1.1 dst 10.1.1.1
04:32:55: ISAKMP cookie 3123100B 041A85A6
04:32:55: ISAKMP (0:13): SA has been authenticated with 10.1.1.1
04:32:55: ISAKMP: Trying to insert a peer 172.16.1.1/10.1.1.1/500/,  and inserted
successfully.
04:32:55: ISAKMP: set new node -803402627 to CONF_XAUTH
04:32:55: IPSEC(key_engine): got a queue event...
04:32:55: ISAKMP (0:13): sending packet to 10.1.1.1 my_port 500 peer_port 500 (R) QM_IDLE

04:32:55: ISAKMP (0:13): purging node -803402627
04:32:55: ISAKMP: Sending phase 1 responder lifetime 86400
04:32:55: ISAKMP (0:13): Input = IKE_MESG_FROM_PEER, IKE_AM_EXCH
04:32:55: ISAKMP (0:13): Old State = IKE_R_AM2  New State = IKE_P1_COMPLETE
04:32:55: ISAKMP cookie gen for src 10.1.1.1 dst 172.168.1.1
04:32:55: ISAKMP cookie AA8F7B41 25EEF256
04:32:55: ISAKMP:        isadb_post_process_list: crawler: 9 27FF 2 (6482B354)
04:32:55:       crawler my_cookie AA8F7B41 F7ACF384
04:32:55:        crawler his_cookie E46E088D F227FE4D
04:32:55: ISAKMP (0:13): Need XAUTH
04:32:55: ISAKMP (0:13): Input = IKE_MESG_INTERNAL, IKE_PHASE1_COMPLETE
04:32:55: ISAKMP (0:13): Old State = IKE_P1_COMPLETE  New State =
IKE_XAUTH_AAA_START_LOGIN_AWAIT
04:32:55: ISAKMP cookie gen for src 10.1.1.1 dst 172.16.1.1
04:32:55: ISAKMP cookie AA8F7B41 2CCFA491
04:32:55: ISAKMP:        isadb_post_process_list: crawler: B 27FF 12 (6482B354)
04:32:55:       crawler my_cookie AA8F7B41 F7ACF384
04:32:55:        crawler his_cookie E46E088D F227FE4D
04:32:55: ISAKMP: got callback 1
04:32:55: ISAKMP: set new node -1447732198 to CONF_XAUTH
04:32:55: ISAKMP/xauth: request attribute XAUTH_USER_NAME_V2
04:32:55: ISAKMP/xauth: request attribute XAUTH_USER_PASSWORD_V2
04:32:55: ISAKMP (0:13): initiating peer config to 10.1.1.1. ID = -1447732198
04:32:55: ISAKMP (0:13): sending packet to 10.1.1.1 my_port 500 peer_port 500 (R)
CONF_XAUTH
04:32:55: ISAKMP (0:13): Input = IKE_MESG_FROM_AAA, IKE_AAA_START_LOGIN
04:32:55: ISAKMP (0:13): Old State = IKE_XAUTH_AAA_START_LOGIN_AWAIT  New State =
IKE_XAUTH_REQ_SENT
04:33:00: ISAKMP (0:13): retransmitting phase 2 CONF_XAUTH    -1447732198 ...
04:33:00: ISAKMP (0:13): incrementing error counter on sa: retransmit phase 2
04:33:00: ISAKMP (0:13): incrementing error counter on sa: retransmit phase 2
04:33:00: ISAKMP (0:13): retransmitting phase 2 -1447732198 CONF_XAUTH
04:33:00: ISAKMP (0:13): sending packet to 10.1.1.1 my_port 500 peer_port 500 (R)
CONF_XAUTH
04:33:03: ISAKMP cookie gen for src 172.18.1.1 dst 10.1.1.1
04:33:03: ISAKMP cookie 3123100B 124D4618
04:33:03: ISAKMP cookie gen for src 10.1.1.1 dst 172.18.1.1
04:33:03: ISAKMP cookie AA8F7B41 B0C91917
04:33:03: ISAKMP:        isadb_post_process_list: crawler: B 27FF 2 (6482B354)
04:33:03:       crawler my_cookie AA8F7B41 F7ACF384
04:33:03:        crawler his_cookie E46E088D F227FE4D
04:33:03: ISAKMP cookie gen for src 172.18.1.1 dst 10.1.1.1
04:33:03: ISAKMP cookie 3123100B 0E294692
```

```
04:33:03: ISAKMP cookie gen for src 10.1.1.1 dst 172.18.1.1
04:33:03: ISAKMP cookie AA8F7B41 091A7695
04:33:03: ISAKMP:        isadb_post_process_list: crawler: B 27FF 2 (6482B354)
04:33:03:       crawler my_cookie AA8F7B41 F7ACF384
04:33:03:        crawler his_cookie E46E088D F227FE4D
04:33:03: ISAKMP (0:13): received packet from 10.1.1.1 dport 500 sport 500 Global (R)
CONF_XAUTH
04:33:03: ISAKMP: hash from 7292D74 for 92 bytes
04:33:03: ISAKMP: Packet hash:
64218CC0:                   84A1AF24 5D92B116          .!/$].1.
64218CD0: FC2C6252 A472C5F8 152AC860 63        |,bR$rEx.*H`c
04:33:03: ISAKMP (0:13): processing transaction payload from 11.1.1.1. message ID =
-1447732198
04:33:03: ISAKMP: Config payload REPLY
04:33:03: ISAKMP/xauth: reply attribute XAUTH_USER_NAME_V2
04:33:03: ISAKMP/xauth: reply attribute XAUTH_USER_PASSWORD_V2
04:33:03: ISAKMP (0:13): deleting node -1447732198 error FALSE reason "done with xauth
request/reply exchange"
04:33:03: ISAKMP (0:13): Input = IKE_MESG_FROM_PEER, IKE_CFG_REPLY
04:33:03: ISAKMP (0:13): Old State = IKE_XAUTH_REQ_SENT  New State =
IKE_XAUTH_AAA_CONT_LOGIN_AWAIT
04:33:03: ISAKMP cookie gen for src 10.1.1.1 dst 172.18.1.1
04:33:03: ISAKMP cookie AA8F7B41 A1B3E684
04:33:03: ISAKMP:        isadb_post_process_list: crawler: B 27FF 12 (6482B354)
04:33:03:       crawler my_cookie AA8F7B41 F7ACF384
04:33:03:        crawler his_cookie E46E088D F227FE4D
04:33:03: ISAKMP: got callback 1
04:33:03: ISAKMP: set new node 524716665 to CONF_XAUTH
04:33:03: ISAKMP (0:13): initiating peer config to 10.1.1.1. ID = 524716665
04:33:03: ISAKMP (0:13): sending packet to 10.1.1.1 my_port 500 peer_port 500 (R)
CONF_XAUTH
04:33:03: ISAKMP (0:13): Input = IKE_MESG_FROM_AAA, IKE_AAA_CONT_LOGIN
04:33:03: ISAKMP (0:13): Old State = IKE_XAUTH_AAA_CONT_LOGIN_AWAIT  New State =
IKE_XAUTH_SET_SENT
004:33:03: ISAKMP cookie gen for src 172.18.1.1 dst 10.1.1.1
04:33:03: ISAKMP cookie 3123100B 5C83A09D
04:33:03: ISAKMP cookie gen for src 10.1.1.1 dst 172.18.1.1
04:33:03: ISAKMP cookie AA8F7B41 2BEBEFD4
04:33:03: ISAKMP:        isadb_post_process_list: crawler: B 27FF 2 (6482B354)
04:33:03:       crawler my_cookie AA8F7B41 F7ACF384
04:33:03:        crawler his_cookie E46E088D F227FE4D
04:33:03: ISAKMP cookie gen for src 172.18.1.1 dst 10.1.1.1
04:33:03: ISAKMP cookie 3123100B DA00A46B
04:33:03: ISAKMP cookie gen for src 10.1.1.1 dst 172.18.1.1
04:33:03: ISAKMP cookie AA8F7B41 FDD27773
04:33:03: ISAKMP:        isadb_post_process_list: crawler: B 27FF 2 (6482B354)
04:33:03:       crawler my_cookie AA8F7B41 F7ACF384
04:33:03:        crawler his_cookie E46E088D F227FE4D
04:33:03: ISAKMP (0:13): received packet from 10.1.1.1 dport 500 sport 500 Global (R)
CONF_XAUTH
04:33:03: ISAKMP: hash from 7292A34 for 68 bytes
04:33:03: ISAKMP: Packet hash:
64218CC0:                   5034B99E B8BA531F          P49.8:S.
64218CD0: 6267B8BD F3006989 DC118796 63        bg8=s.i.\...c
04:33:03: ISAKMP (0:13): processing transaction payload from 11.1.1.1. message ID =
524716665
04:33:03: ISAKMP: Config payload ACK
04:33:03: ISAKMP (0:13):        XAUTH ACK Processed
04:33:03: ISAKMP (0:13): deleting node 524716665 error FALSE reason "done with transaction"
04:33:03: ISAKMP (0:13): Input = IKE_MESG_FROM_PEER, IKE_CFG_ACK
04:33:03: ISAKMP (0:13): Old State = IKE_XAUTH_SET_SENT  New State = IKE_P1_COMPLETE
04:33:03: ISAKMP cookie gen for src 10.1.1.1 dst 172.18.1.1
04:33:03: ISAKMP cookie AA8F7B41 E0BB50E9
04:33:03: ISAKMP:        isadb_post_process_list: crawler: 9 27FF 2 (6482B354)
```

```
04:33:03:       crawler my_cookie AA8F7B41 F7ACF384
04:33:03:        crawler his_cookie E46E088D F227FE4D
04:33:03: ISAKMP (0:13): Input = IKE_MESG_INTERNAL, IKE_PHASE1_COMPLETE
04:33:03: ISAKMP (0:13): Old State = IKE_P1_COMPLETE  New State = IKE_P1_COMPLETE
04:33:03: ISAKMP cookie gen for src 172.18.1.1 dst 10.1.1.1
04:33:03: ISAKMP cookie 3123100B 7794EF6E
04:33:03: ISAKMP cookie gen for src 10.1.1.1 dst 172.18.1.1
04:33:03: ISAKMP cookie AA8F7B41 C035AAE5
04:33:03: ISAKMP:        isadb_post_process_list: crawler: 9 27FF 2 (6482B354)
04:33:03:       crawler my_cookie AA8F7B41 F7ACF384
04:33:03:        crawler his_cookie E46E088D F227FE4D
04:33:03: ISAKMP cookie gen for src 172.18.1.1 dst 10.1.1.1
04:33:03: ISAKMP cookie 3123100B F1FCC25A
04:33:03: ISAKMP cookie gen for src 10.1.1.1 dst 172.18.1.1
04:33:03: ISAKMP cookie AA8F7B41 31744F44
04:33:03: ISAKMP:        isadb_post_process_list: crawler: 9 27FF 2 (6482B354)
04:33:03:       crawler my_cookie AA8F7B41 F7ACF384
04:33:03:        crawler his_cookie E46E088D F207FE4D
04:33:03: ISAKMP (0:13): received packet from 10.1.1.1 dport 500 sport 500 Global (R)
QM_IDLE
04:33:03: ISAKMP: set new node -1639992295 to QM_IDLE
04:33:03: ISAKMP: hash from 7293A74 for 100 bytes
04:33:03: ISAKMP: Packet hash:
64218CC0:                   9D7DF4DF FE3A6403          .}t_~:d.
64218CD0: 3F1D1C59 C5D138CE 50289B79 07        ?..YEQ8NP(.y.
04:33:03: ISAKMP (0:13): processing transaction payload from 10.1.1.1. message ID =
-1639992295
04:33:03: ISAKMP: Config payload REQUEST
04:33:03: ISAKMP (0:13): checking request:
04:33:03: ISAKMP:    IP4_ADDRESS
04:33:03: ISAKMP:    IP4_NETMASK
04:33:03: ISAKMP:    IP4_DNS
04:33:03: ISAKMP:    IP4_DNS
04:33:03: ISAKMP:    IP4_NBNS
04:33:03: ISAKMP:    IP4_NBNS
04:33:03: ISAKMP:    SPLIT_INCLUDE
04:33:03: ISAKMP:    DEFAULT_DOMAIN
04:33:03: ISAKMP (0:13): Input = IKE_MESG_FROM_PEER, IKE_CFG_REQUEST
04:33:03: ISAKMP (0:13): Old State = IKE_P1_COMPLETE  New State =
IKE_CONFIG_AUTHOR_AAA_AWAIT
04:33:03: ISAKMP cookie gen for src 10.1.1.1 dst 172.18.1.1
04:33:03: ISAKMP cookie AA8F7B41 B02E0D67
04:33:03: ISAKMP:        isadb_post_process_list: crawler: C 27FF 12 (6482B354)
04:33:03:       crawler my_cookie AA8F7B41 F7ACF384
04:33:03:        crawler his_cookie E46E088D F227FE4D
04:33:03: ISAKMP: got callback 1
04:33:03: ISAKMP (0:13): attributes sent in message:
04:33:03:         Address: 10.2.0.0
04:33:03: ISAKMP (0:13): allocating address 10.4.1.4
04:33:03: ISAKMP: Sending private address: 10.4.1.4
04:33:03: ISAKMP: Sending DEFAULT_DOMAIN default domain name: vpn2.com
04:33:03: ISAKMP (0:13): responding to peer config from 10.1.1.1. ID = -1639992295
04:33:03: ISAKMP (0:13): sending packet to 10.1.1.1 my_port 500 peer_port 500 (R) CONF_ADDR

04:33:03: ISAKMP (0:13): deleting node -1639992295 error FALSE reason ""
04:33:03: ISAKMP (0:13): Input = IKE_MESG_FROM_AAA, IKE_AAA_GROUP_ATTR
04:33:03: ISAKMP (0:13): Old State = IKE_CONFIG_AUTHOR_AAA_AWAIT  New State =
IKE_P1_COMPLETE
04:33:03: ISAKMP cookie gen for src 172.18.1.1 dst 10.1.1.1
04:33:03: ISAKMP cookie 3123100B 881D5411
04:33:03: ISAKMP cookie gen for src 11.1.1.1 dst 172.18.1.1
04:33:03: ISAKMP cookie AA8F7B41 6FD82541
04:33:03: ISAKMP:        isadb_post_process_list: crawler: 9 27FF 2 (6482B354)
04:33:03:       crawler my_cookie AA8F7B41 F7ACF384
```

```
04:33:03:        crawler his_cookie E46E088D F227FE4D
04:33:03: ISAKMP cookie gen for src 172.18.1.1 dst 10.1.1.1
04:33:03: ISAKMP cookie 3123100B 8A94C1BE
04:33:03: ISAKMP cookie gen for src 10.1.1.1 dst 172.18.1.1
04:33:03: ISAKMP cookie AA8F7B41 F3BA766D
04:33:03: ISAKMP:        isadb_post_process_list: crawler: 9 27FF 2 (6482B354)
04:33:03:       crawler my_cookie AA8F7B41 F7ACF384
04:33:03:        crawler his_cookie E46E088D F207FE4D
04:33:03: ISAKMP (0:13): received packet from 10.1.1.1 dport 500 sport 500 Global (R)
QM_IDLE
04:33:03: ISAKMP: set new node 17011691 to QM_IDLE
04:33:03: ISAKMP: hash from 70029F4 for 540 bytes
04:33:03: ISAKMP: Packet hash:
64218CC0:                   AFBA30B2 55F5BC2D          /:02Uu<-
64218CD0: 3A86B1C9 00D2F5BA 77BF5589 07        :.1I.Ru:w?U..
04:33:03: ISAKMP (0:13): processing HASH payload. message ID = 17011691
04:33:03: ISAKMP (0:13): processing SA payload. message ID = 17011691
04:33:03: ISAKMP (0:13): Checking IPSec proposal 1
04:33:03: ISAKMP: transform 1, ESP_AES
04:33:03: ISAKMP:   attributes in transform:
04:33:03: ISAKMP:      encaps is 1
04:33:03: ISAKMP:      SA life type in seconds
04:33:03: ISAKMP:      SA life duration (VPI) of  0x0 0x20 0xC4 0x9B
04:33:03: ISAKMP:      SA life type in kilobytes
04:33:03: ISAKMP:      SA life duration (VPI) of  0x0 0x46 0x50 0x0
04:33:03: ISAKMP:      authenticator is HMAC-SHA
04:33:03: ISAKMP (0:13): atts are acceptable.
04:33:03: IPSEC(validate_proposal_request): proposal part #1,
  (key eng. msg.) INBOUND local= 172.18.1.1, remote= 10.1.1.1,
    local_proxy= 0.0.0.0/0.0.0.0/0/0 (type=4),
    remote_proxy= 10.4.1.4/255.255.255.255/0/0 (type=1),
    protocol= ESP, transform= esp-aes esp-sha-hmac,
    lifedur= 0s and 0kb,
    spi= 0x0(0), conn_id= 0, keysize= 0, flags= 0x2
04:33:03: IPSEC(kei_proxy): head = ra, map->ivrf = vpn1, kei->ivrf = vpn2
04:33:03: IPSEC(kei_proxy): head = ra, map->ivrf = vpn2, kei->ivrf = vpn2
04:33:03: IPSEC(validate_transform_proposal): transform proposal not supported for
identity:
    {esp-aes esp-sha-hmac}
04:33:03: ISAKMP (0:13): IPSec policy invalidated proposal
04:33:03: ISAKMP (0:13): Checking IPSec proposal 2
04:33:03: ISAKMP: transform 1, ESP_AES
04:33:03: ISAKMP:   attributes in transform:
04:33:03: ISAKMP:      encaps is 1
04:33:03: ISAKMP:      SA life type in seconds
04:33:03: ISAKMP:      SA life duration (VPI) of  0x0 0x20 0xC4 0x9B
04:33:03: ISAKMP:      SA life type in kilobytes
04:33:03: ISAKMP:      SA life duration (VPI) of  0x0 0x46 0x50 0x0
04:33:03: ISAKMP:      authenticator is HMAC-SHA
04:33:03: ISAKMP (0:13): atts are acceptable.
04:33:03: IPSEC(validate_proposal_request): proposal part #1,
  (key eng. msg.) INBOUND local= 172.18.1.1, remote= 10.1.1.1,
    local_proxy= 0.0.0.0/0.0.0.0/0/0 (type=4),
    remote_proxy= 10.4.1.4/255.255.255.255/0/0 (type=1),
    protocol= ESP, transform= esp-aes esp-sha-hmac,
    lifedur= 0s and 0kb,
    spi= 0x0(0), conn_id= 0, keysize= 0, flags= 0x2
04:33:03: IPSEC(kei_proxy): head = ra, map->ivrf = vpn1, kei->ivrf = vpn2
04:33:03: IPSEC(kei_proxy): head = ra, map->ivrf = vpn2, kei->ivrf = vpn2
04:33:03: ISAKMP (0:13): processing NONCE payload. message ID = 17011691
04:33:03: ISAKMP (0:13): processing ID payload. message ID = 17011691
04:33:03: ISAKMP (0:13): processing ID payload. message ID = 17011691
04:33:03: ISAKMP (0:13): asking for 1 spis from ipsec
04:33:03: ISAKMP (0:13): Node 17011691, Input = IKE_MESG_FROM_PEER, IKE_QM_EXCH
```

```
04:33:03: ISAKMP (0:13): Old State = IKE_QM_READY  New State = IKE_QM_SPI_STARVE
04:33:03: IPSEC(key_engine): got a queue event...
04:33:03: IPSEC(spi_response): getting spi 2749516541 for SA
        from 172.18.1.1     to 10.1.1.1        for prot 3
04:33:03: ISAKMP: received ke message (2/1)
04:33:04: ISAKMP (13): ID payload
        next-payload : 5
        type         : 1
        addr         : 10.4.1.4
        protocol     : 0
        port         : 0
04:33:04: ISAKMP (13): ID payload
        next-payload : 11
        type         : 4
        addr         : 0.0.0.0
        protocol     : 0
        port         : 0
04:33:04: ISAKMP (0:13): sending packet to 10.1.1.1 my_port 500 peer_port 500 (R) QM_IDLE

04:33:04: ISAKMP (0:13): Node 17011691, Input = IKE_MESG_FROM_IPSEC, IKE_SPI_REPLY
04:33:04: ISAKMP (0:13): Old State = IKE_QM_SPI_STARVE  New State = IKE_QM_R_QM2
04:33:04: ISAKMP cookie gen for src 172.18.1.1 dst 10.1.1.1
04:33:04: ISAKMP cookie 3123100B 93DE46D2
04:33:04: ISAKMP cookie gen for src 10.1.1.1 dst 172.18.1.1
04:33:04: ISAKMP cookie AA8F7B41 088A0A16
04:33:04: ISAKMP:        isadb_post_process_list: crawler: 9 27FF 2 (6482B354)
04:33:04:       crawler my_cookie AA8F7B41 F7ACF384
04:33:04:        crawler his_cookie E46E088D F227FE4D
04:33:04: ISAKMP cookie gen for src 172.18.1.1 dst 10.1.1.1
04:33:04: ISAKMP cookie 3123100B A8F23F73
04:33:04: ISAKMP cookie gen for src 10.1.1.1 dst 172.18.1.1
04:33:04: ISAKMP cookie AA8F7B41 93D8D879
04:33:04: ISAKMP:        isadb_post_process_list: crawler: 9 27FF 2 (6482B354)
04:33:04:       crawler my_cookie AA8F7B41 F7ACF384
04:33:04:        crawler his_cookie E46E088D F227FE4D
04:33:04: ISAKMP (0:13): received packet from 10.1.1.1 dport 500 sport 500 Global (R)
QM_IDLE
04:33:04: ISAKMP: hash from 7290DB4 for 60 bytes
04:33:04: ISAKMP: Packet hash:
64218CC0:                   4BB45A92 7181A2F8          K4Z.q."x
64218CD0: 73CC12F8 091875C0 054F77CD 63        sL.x..u@.OwMc
04:33:04: ISAKMP: Locking peer struct 0x640BBB18, IPSEC refcount 1 for stuff_ke
04:33:04: ISAKMP (0:13): Creating IPSec SAs
04:33:04:         inbound SA from 10.1.1.1 to 172.18.1.1 (f/i)  0/ 2
        (proxy 10.4.1.4 to 0.0.0.0)
04:33:04:         has spi 0xA3E24AFD and conn_id 5127 and flags 2
04:33:04:         lifetime of 2147483 seconds
04:33:04:         lifetime of 4608000 kilobytes
04:33:04:         has client flags 0x0
04:33:04:         outbound SA from 172.18.1.1     to 10.1.1.1        (f/i)  0/ 2 (proxy
 0.0.0.0         to 10.4.1.4       )
04:33:04:         has spi 1343294712 and conn_id 5128 and flags A
04:33:04:         lifetime of 2147483 seconds
04:33:04:         lifetime of 4608000 kilobytes
04:33:04:         has client flags 0x0
04:33:04: ISAKMP (0:13): deleting node 17011691 error FALSE reason "quick mode done
(await)"
04:33:04: ISAKMP (0:13): Node 17011691, Input = IKE_MESG_FROM_PEER, IKE_QM_EXCH
04:33:04: ISAKMP (0:13): Old State = IKE_QM_R_QM2  New State = IKE_QM_PHASE2_COMPLETE
04:33:04: IPSEC(key_engine): got a queue event...
04:33:04: IPSEC(initialize_sas): ,
  (key eng. msg.) INBOUND local= 172.18.1.1, remote= 10.1.1.1,
    local_proxy= 0.0.0.0/0.0.0.0/0/0 (type=4),
    remote_proxy= 10.4.1.4/0.0.0.0/0/0 (type=1),
```

```
    protocol= ESP, transform= esp-aes esp-sha-hmac ,
    lifedur= 2147483s and 4608000kb,
    spi= 0xA3E24AFD(2749516541), conn_id= 5127, keysize= 0, flags= 0x2
04:33:04: IPSEC(initialize_sas): ,
  (key eng. msg.) OUTBOUND local= 172.18.1.1, remote= 10.1.1.1,
    local_proxy= 0.0.0.0/0.0.0.0/0/0 (type=4),
    remote_proxy= 10.4.1.4/0.0.0.0/0/0 (type=1),
    protocol= ESP, transform= esp-aes esp-sha-hmac,
    lifedur= 2147483s and 4608000kb,
    spi= 0x50110CF8(1343294712), conn_id= 5128, keysize= 0, flags= 0xA
04:33:04: IPSEC(kei_proxy): head = ra, map->ivrf = vpn1, kei->ivrf = vpn2
04:33:04: IPSEC(kei_proxy): head = ra, map->ivrf = vpn2, kei->ivrf = vpn2
04:33:04: IPSEC(rte_mgr): VPN Route Added 10.4.1.4 255.255.255.255 via 10.1.1.1 in vpn2
04:33:04: IPSEC(add mtree): src 0.0.0.0, dest 10.4.1.4, dest_port 0
04:33:04: IPSEC(create_sa): sa created,
  (sa) sa_dest= 172.18.1.1, sa_prot= 50,
    sa_spi= 0xA3E24AFD(2749516541),
    sa_trans= esp-aes esp-sha-hmac, sa_conn_id= 5127
04:33:04: IPSEC(create_sa): sa created,
  (sa) sa_dest= 10.1.1.1, sa_prot= 50,
    sa_spi= 0x50110CF8(1343294712),
    sa_trans= esp-aes esp-sha-hmac, sa_conn_id= 5128
04:33:53: ISAKMP (0:13): purging node -1639992295
04:33:54: ISAKMP (0:13): purging node 17011691
```

VRF-Aware IPsec の設定例

例：静的 IPsec-to-MPLS VPN

次のサンプルでは、IPsec トンネルを MPLS VPN にマッピングするスタティック設定を示しています。この設定により、IPsec トンネルが MPLS VPN、「VPN1」および「VPN2」にマッピングされます。IPsec トンネルは両方とも、シングル パブリック方向インターフェイス上で終了します。

IPsec PE の設定

```
ip vrf vpn1
 rd 100:1
 route-target export 100:1
 route-target import 100:1
!
ip vrf vpn2
 rd 101:1
 route-target export 101:1
 route-target import 101:1
!
crypto keyring vpn1
  pre-shared-key address 172.16.1.1 key vpn1
crypto keyring vpn2
  pre-shared-key address 10.1.1.1 key vpn2
!
crypto isakmp policy 1
 encr aes
 authentication pre-share
 group 14
!
```

```
crypto isakmp profile vpn1
 vrf vpn1
 keyring vpn1
 match identity address 172.16.1.1 255.255.255.255
!
crypto isakmp profile vpn2
 vrf vpn2
 keyring vpn2
 match identity address 10.1.1.1 255.255.255.255
!
crypto ipsec transform-set vpn1 esp-aes esp-sha-hmac
crypto ipsec transform-set vpn2 esp-aes esp-sha-hmac
!
crypto map crypmap 1 ipsec-isakmp
 set peer 172.16.1.1
 set transform-set vpn1
 set isakmp-profile vpn1
 match address 101
crypto map crypmap 3 ipsec-isakmp
 set peer 10.1.1.1
 set transform-set vpn2
 set isakmp-profile vpn2
 match address 102
!
interface Ethernet1/1
 ip address 172.17.1.1 255.255.0.0
 tag-switching ip
!
interface Ethernet1/2
 ip address 172.18.1.1 255.255.255.0
 crypto map crypmap
!
ip route 172.16.1.1 255.255.255.255 172.18.1.2
ip route 10.1.1.1 255.255.255.255 172.18.1.2
ip route vrf vpn1 10.2.0.0 255.255.0.0 172.18.1.2 global
ip route vrf vpn2 10.2.0.0 255.255.0.0 172.18.1.2 global
!
access-list 101 permit ip 10.1.0.0 0.0.255.255 10.2.0.0 0.0.255.255
access-list 102 permit ip 10.1.0.0 0.0.255.255 10.2.0.0 0.0.255.255
```

VPN1 用 IPsec Customer Provided Edge（CPE）設定

```
crypto isakmp policy 1
 encr aes
 authentication pre-share
 group 14
crypto isakmp key vpn1 address 172.18.1.1
!
!
crypto ipsec transform-set vpn1 esp-aes esp-sha-hmac
!
crypto map vpn1 1 ipsec-isakmp
 set peer 172.18.1.1
 set transform-set vpn1
 match address 101
!
interface FastEthernet1/0
 ip address 172.16.1.1 255.255.255.0
 crypto map vpn1
!
interface FastEthernet1/1
 ip address 10.2.1.1 255.255.0.0
!
```

```
access-list 101 permit ip 10.2.0.0 0.0.255.255 10.1.0.0 0.0.255.255
!
```

VPN2 用 IPsec CPE 設定

```
crypto isakmp policy 1
 encr aes
 authentication pre-share
 group 14
!
crypto isakmp key vpn2 address 172.18.1.1
!
!
crypto ipsec transform-set vpn2 esp-aes esp-sha-hmac
!
crypto map vpn2 1 ipsec-isakmp
 set peer 172.18.1.1
 set transform-set vpn2
 match address 101
!
interface FastEthernet0
 ip address 10.1.1.1 255.255.255.0
 crypto map vpn2
!
interface FastEthernet1
 ip address 10.2.1.1 255.255.0.0
!
access-list 101 permit ip 10.2.0.0 0.0.255.255 10.1.0.0 0.0.255.255
```

例：RSA 暗号化を使用した IPsec-to-MPLS VPN

次の例では、RSA 暗号化を使用した IPsec-to-MPLS VPN 設定を示します。

PE ルータ設定

```
ip vrf vpn1
 rd 100:1
 route-target export 100:1
 route-target import 100:1
!
crypto isakmp policy 10
 authentication rsa-encr
!
crypto keyring vpn1
 rsa-pubkey address 172.16.1.1 encryption
  key-string
   305C300D 06092A86 4886F70D 01010105 00034B00 30480241 00DBF381 00DDECC8
   DC4AA490 40320C52 9912D876 EB36717C 63DCA95C 7E5EC02A 84F276CE 292B42D7
   D664F324 3726F4E0 39D33093 ECB81B95 482511A5 F064C4B3 D5020301 0001
   quit
!
crypto isakmp profile vpn1
 vrf vpn1
 keyring vpn1
 match identity address 172.16.1.1 255.255.255.255
!
crypto ipsec transform-set vpn1 esp-aes esp-sha-hmac
!
crypto map crypmap 1 ipsec-isakmp
```

```
 set peer 172.16.1.1
 set transform-set vpn1
 set isakmp-profile vpn1
 match address 101
!
interface Ethernet1/1
 ip address 172.17.1.1 255.255.0.0
 tag-switching ip
!
interface Ethernet1/2
 ip address 172.18.1.1 255.255.255.0
 crypto map crypmap
!
ip route 172.16.1.1 255.255.255.255 172.18.1.2
ip route vrf vpn1 10.2.0.0 255.255.0.0 172.18.1.2 global
!
access-list 101 permit ip 10.1.0.0 0.0.255.255 10.2.0.0 0.0.255.255
```

VPN1 用 IPsec CPE 設定

```
crypto isakmp policy 10
 authentication rsa-encr
!
crypto key pubkey-chain rsa
 addressed-key 172.18.1.1 encryption
 key-string
  3082011B 300D0609 2A864886 F70D0101 01050003 82010800 30820103 0281FB00
  C90CC78A 6002BDBA 24683396 B7D7877C 16D08C47 E00C3C10 63CF13BC 4E09EA23
  92EB8A48 4113F5A4 8796C8BE AD7E2DC1 3B0742B6 7118CE7C 1B0E21D1 AA9724A4
  4D74FCEA 562FF225 A2B11F18 E53C4415 61C3B741 3A06E75D B4F9102D 6163EE40
  16C68FD7 6532F660 97B59118 9C8DE3E5 4E2F2925 BBB87FCB 95223D4E A5E362DB
  215CB35C 260080805 17BBE1EF C3050E13 031F3D5B 5C22D16C FC8B1EC5 074F07A5
  D050EC80 7890D9C5 EC20D6F0 173FE2BA 89F5B5F9 2EADC9A6 D461921E 3D5B60016
  ABB8B6B9 E2124A21 93F0E4AE B487461B E7F1F1C4 032A0B0E 80DC3E15 CB268EC9
  5D76B9BD 3C78CB75 CE9F68C6 484D6573 CBC3EB59 4B5F3999 8F9D0203 010001
  quit
!
crypto ipsec transform-set vpn1 esp-aes esp-sha-hmac
!
crypto map vpn1 1 ipsec-isakmp
 set peer 172.18.1.1
 set transform-set vpn1
 match address 101
!
interface FastEthernet1/0
 ip address 172.16.1.1 255.255.255.0
 crypto map vpn1
!
interface FastEthernet1/1
 ip address 10.2.1.1 255.255.0.0
!
access-list 101 permit ip 10.2.0.0 0.0.255.255 10.1.0.0 0.0.255.255
!
```

例：RSA シグニチャを使用した IPsec-to-MPLS VPN

次のに、RSA シグニチャを使用した IPsec-to-MPLS VPN 設定を示します。

PE ルータ設定

```
ip vrf vpn1
 rd 100:1
 route-target export 100:1
 route-target import 100:1
!
crypto ca trustpoint bombo
 enrollment url http://172.31.68.59:80
 crl optional
!
crypto ca certificate chain bombo
 certificate 03C0
 308203BF 308202A7 A0030201 02020203 C0300D06 092A8648 86F70D01 01050500
 . . .
 quit
 certificate ca 01
 30820379 30820261 A0030201 02020101 300D0609 2A864886 F70D0101 05050030
 . . .
 quit
!
crypto isakmp profile vpn1
 vrf vpn1
 ca trust-point bombo
 match identity address 172.16.1.1 255.255.255.255
!
crypto ipsec transform-set vpn1 esp-aes esp-sha-hmac
!
crypto map crypmap 1 ipsec-isakmp
 set peer 172.16.1.1
 set transform-set vpn1
 set isakmp-profile vpn1
 match address 101
!
interface Ethernet1/1
 ip address 172.31.1.1 255.255.0.0
 tag-switching ip
!
interface Ethernet1/2
 ip address 172.18.1.1 255.255.255.0
 crypto map crypmap
!
ip route 172.16.1.1 255.255.255.255 172.18.1.2
ip route vrf vpn1 10.2.0.0 255.255.0.0 172.18.1.2 global
!
access-list 101 permit ip 10.1.0.0 0.0.255.255 10.2.0.0 0.0.255.255
!
```

VPN1 用 IPsec CPE 設定

```
crypto ca trustpoint bombo
 enrollment url http://172.31.68.59:80
 crl optional
 !
crypto ca certificate chain bombo
 certificate 03BF
  308203BD 308202A5 A0030201 02020203 BF300D06 092A8648 86F70D01 01050500
  . . .
  quit
 certificate ca 01
  30820379 30820261 A0030201 02020101 300D0609 2A864886 F70D0101 05050030
  . . .
```

```
  quit
!
crypto ipsec transform-set vpn1 esp-aes esp-sha-hmac
!
crypto map vpn1 1 ipsec-isakmp
 set peer 172.18.1.1
 set transform-set vpn1
 match address 101
!
interface FastEthernet1/0
 ip address 172.16.1.1 255.255.255.0
 crypto map vpn1
!
interface FastEthernet1/1
 ip address 10.2.1.1 255.255.0.0
!
access-list 101 permit ip 10.2.0.0 0.0.255.255 10.1.0.0 0.0.255.255
!
```

例：IPsec Remote Access-to-MPLS VPN

次に、IPsec Remote Access-to-MPLS VPN 設定を示します。この設定により、IPsec トンネルが MPLS VPN にマッピングされます。IPsec トンネルが、シングル パブリック方向インターフェイス上で終了します。

PE ルータ設定

```
aaa new-model
!
aaa group server radius vpn1
 server-private 10.1.1.1 auth-port 1645 acct-port 1646 timeout 5 retransmit 3 key vpn1
!
aaa group server radius vpn2
 server-private 10.1.1.1 auth-port 1645 acct-port 1646 timeout 5 retransmit 3 key vpn2
!
aaa authorization network aaa-list group radius
!
ip vrf vpn1
 rd 100:1
 route-target export 100:1
 route-target import 100:1
!
ip vrf vpn2
 rd 101:1
 route-target export 101:1
 route-target import 101:1
!
crypto isakmp profile vpn1-ra
   vrf vpn1
   match identity group vpn1-ra
   client authentication list vpn1
   isakmp authorization list aaa-list
   client configuration address initiate
   client configuration address respond
crypto isakmp profile vpn2-ra
   vrf vpn2
   match identity group vpn2-ra
   client authentication list vpn2
   isakmp authorization list aaa-list
   client configuration address initiate
```

```
   client configuration address respond
!
!
crypto ipsec transform-set vpn1 esp-aes esp-sha-hmac
crypto ipsec transform-set vpn2 esp-aes esp-sha-hmac
!
crypto dynamic-map vpn1 1
 set transform-set vpn1
 set isakmp-profile vpn1-ra
 reverse-route
!
crypto dynamic-map vpn2 1
 set transform-set vpn2
 set isakmp-profile vpn2-ra
 reverse-route
!
!
crypto map ra 1 ipsec-isakmp dynamic vpn1
crypto map ra 2 ipsec-isakmp dynamic vpn2
!
interface Ethernet1/1
 ip address 172.17.1.1 255.255.0.0
 tag-switching ip
!
interface Ethernet1/2
 ip address 172.18.1.1 255.255.255.0
 crypto map ra
!
ip local pool vpn1-ra 10.4.1.1 10.4.1.254 group vpn1-ra
ip local pool vpn2-ra 10.4.1.1 10.4.1.254 group vpn2-ra
!
```

Cisco Network-Based IPsec VPN Solution の旧バージョンからのアップデート

Cisco Network-Based IPsec VPN Solution リリース 1.5 における VRF-Aware IPsec 機能では、既存の設定を変更する必要があります。次のサンプル設定では、既存の設定に対して行う必要がある変更を示します。

Site-to-Site 設定のアップグレード

次の設定では、旧バージョンの Network-Based IPsec VPN Solution から Cisco Network-Based IPsec VPN Solution リリース 1.5 への Site-to-Site 設定のアップグレードに必要な変更を示します。

旧バージョンの Site-to-Site 設定

```
crypto isakmp key VPN1 address 172.21.25.74
 crypto isakmp key VPN2 address 172.21.21.74
!
 crypto ipsec transform-set VPN1 esp-aes esp-sha-hmac
 crypto ipsec transform-set VPN2 esp-aes esp-sha-hmac
!
 crypto map VPN1 10 ipsec-isakmp
 set peer 172.21.25.74
 set transform-set VPN1
 match address 101
!
```

```
 crypto map VPN2 10 ipsec-isakmp
 set peer 172.21.21.74
 set transform-set VPN2
 match address 102
!
 interface FastEthernet0/0.1
 encapsulation dot1Q 1 native
 ip vrf forwarding VPN1
 ip address 172.21.25.73 255.255.255.0
 crypto map VPN1
!
 interface FastEthernet0/0.2
  encapsulation dot1Q 2 native
 ip vrf forwarding VPN2
 ip address 172.21.21.74 255.255.255.0
 crypto map VPN2
```

新バージョンの Site-to-Site 設定

次に、同じ Site-to-Site 設定の、Cisco Network-Based IPsec VPN Solution リリース 1.5 ソリューションへアップグレードされたバージョンを示します。

（注） 2 つのキーリングを変更する必要があります。VRF-Aware Upset 機能では、IKE ローカル エンドポイントが VRF 内に存在している場合、キーを VRF に関連付ける必要があります。

```
crypto keyring VPN1-KEYS vrf VPN1
 pre-shared-key address 172.21.25.74 key VPN1
!
 crypto keyring VPN2-KEYS vrf VPN2
  pre-shared-key address 172.21.21.74 key VPN2
!
 crypto ipsec transform-set VPN1 esp-aes esp-sha-hmac
 crypto ipsec transform-set VPN2 esp-aes esp-sha-hmac
!
 crypto map VPN1 10 ipsec-isakmp
 set peer 172.21.25.74
  set transform-set VPN1
 match address 101
!
 crypto map VPN2 10 ipsec-isakmp
 set peer 172.21.21.74
  set transform-set VPN2
 match address 102
!
 interface FastEthernet0/0.1
 encapsulation dot1Q 1 native
 ip vrf forwarding VPN1
 ip address 172.21.25.73 255.255.255.0
 crypto map VPN1
!
 interface FastEthernet0/0.2
 encapsulation dot1Q 2 native
 ip vrf forwarding VPN2
 ip address 172.21.21.74 255.255.255.0
 crypto map VPN2
```

リモート アクセス設定のアップグレード

次の設定では、旧バージョンの Network-Based IPsec VPN Solution から Cisco Network-Based IPsec VPN Solution リリース 1.5 へのリモート アクセス設定のアップグレードに必要な変更を示します。

旧バージョンのリモート アクセス設定

```
crypto isakmp client configuration group VPN1-RA-GROUP
 key VPN1-RA
 pool VPN1-RA
!
 crypto isakmp client configuration group VPN2-RA-GROUP
 key VPN2-RA
 pool VPN2-RA
!
 crypto ipsec transform-set VPN1-RA esp-aes esp-sha-hmac
 crypto ipsec transform-set VPN2-RA esp-aes esp-sha-hmac
!
 crypto dynamic-map VPN1-RA 1
  set transform-set VPN1-RA
 reverse-route
!
 crypto dynamic-map VPN2-RA 1
 set transform-set VPN2-RA
  reverse-route
!
!
 crypto map VPN1 client authentication list VPN1-RA-LIST
 crypto map VPN1 isakmp authorization list VPN1-RA-LIST
 crypto map VPN1 client configuration address initiate
 crypto map VPN1 client configuration address respond
 crypto map VPN1 10 ipsec-isakmp dynamic VPN1-RA
!
 crypto map VPN2 client authentication list VPN2-RA-LIST
 crypto map VPN2 isakmp authorization list VPN2-RA-LIST
 crypto map VPN2 client configuration address initiate
 crypto map VPN2 client configuration address respond
 crypto map VPN2 10 ipsec-isakmp dynamic VPN2-RA
!
 interface FastEthernet0/0.1
 encapsulation dot1Q 1 native
 ip vrf forwarding VPN1
 ip address 172.21.25.73 255.255.255.0
 crypto map VPN1
!
 interface FastEthernet0/0.2
  encapsulation dot1Q 2 native
 ip vrf forwarding VPN2
 ip address 172.21.21.74 255.255.255.0
 crypto map VPN2
```

新バージョンのリモート アクセス設定

次のインスタンスでは、アップグレードはありません。次の設定を変更することを推奨します。

```
crypto isakmp client configuration group VPN1-RA-GROUP
  key VPN1-RA
  pool VPN1-RA
```

```
!
 crypto isakmp client configuration group VPN2-RA-GROUP
 key VPN2-RA
 pool VPN2-RA
!
 crypto isakmp profile VPN1-RA
 match identity group VPN1-RA-GROUP
  client authentication list VPN1-RA-LIST
 isakmp authorization list VPN1-RA-LIST
 client configuration address initiate
 client configuration address respond
!
 crypto isakmp profile VPN2-RA
 match identity group VPN2-RA-GROUP
 client authentication list VPN2-RA-LIST
 isakmp authorization list VPN2-RA-LIST
 client configuration address initiate
 client configuration address respond
!
 crypto ipsec transform-set VPN1-RA esp-aes esp-sha-hmac
 crypto ipsec transform-set VPN2-RA esp-aes esp-sha-hmac
!
 crypto dynamic-map VPN1-RA 1
 set transform-set VPN1-RA
 set isakmp-profile VPN1-RA
 reverse-route
!
 crypto dynamic-map VPN2-RA 1
 set transform-set VPN2-RA
 set isakmp-profile VPN2-RA
 reverse-route
!
 crypto map VPN1 10 ipsec-isakmp dynamic VPN1-RA
!
 crypto map VPN2 10 ipsec-isakmp dynamic VPN2-RA
!
 interface FastEthernet0/0.1
 encapsulation dot1Q 1 native
 ip vrf forwarding VPN1
 ip address 172.21.25.73 255.255.255.0
 crypto map VPN1
!
 interface FastEthernet0/0.2
 encapsulation dot1Q 2 native
 ip vrf forwarding VPN2
 ip address 172.21.21.74 255.255.255.0
 crypto map VPN2
```

Site-to-Site とリモート アクセスの設定の組み合わせのアップグレード

次の設定では、旧バージョンの Network-Based IPsec VPN Solution から Cisco Network-Based IPsec VPN Solution リリース 1.5 への Site-to-Site およびリモート アクセス設定のアップグレードに必要な変更を示します。

旧バージョンの Site-to-Site およびリモート アクセスの設定

```
crypto isakmp key VPN1 address 172.21.25.74 no-xauth
crypto isakmp key VPN2 address 172.21.21.74 no-xauth
!
 crypto isakmp client configuration group VPN1-RA-GROUP
 key VPN1-RA
```

```
 pool VPN1-RA
!
 crypto isakmp client configuration group VPN2-RA-GROUP
 key VPN2-RA
 pool VPN2-RA
!
 crypto ipsec transform-set VPN1 esp-aes esp-sha-hmac
 crypto ipsec transform-set VPN2 esp-aes esp-sha-hmac
!
 crypto ipsec transform-set VPN1-RA esp-aes esp-sha-hmac
 crypto ipsec transform-set VPN2-RA esp-aes esp-sha-hmac
!
 crypto dynamic-map VPN1-RA 1
 set transform-set VPN1-RA
 reverse-route
!
 crypto dynamic-map VPN2-RA 1
 set transform-set VPN2-RA
 reverse-route
!
 crypto map VPN1 client authentication list VPN1-RA-LIST
 crypto map VPN1 isakmp authorization list VPN1-RA-LIST
 crypto map VPN1 client configuration address initiate
 crypto map VPN1 client configuration address respond
 crypto map VPN1 10 ipsec-isakmp
 set peer 172.21.25.74
 set transform-set VPN1
 match address 101
 crypto map VPN1 20 ipsec-isakmp dynamic VPN1-RA
!
 crypto map VPN2 client authentication list VPN2-RA-LIST
 crypto map VPN2 isakmp authorization list VPN2-RA-LIST
 crypto map VPN2 client configuration address initiate
 crypto map VPN2 client configuration address respond
 crypto map VPN2 10 ipsec-isakmp
 set peer 172.21.21.74
 set transform-set VPN2
 match address 102
 crypto map VPN2 20 ipsec-isakmp dynamic VPN2-RA
!
 interface FastEthernet0/0.1
 encapsulation dot1Q 1 native
 ip vrf forwarding VPN1
 ip address 172.21.25.73 255.255.255.0
 crypto map VPN1
!
 interface FastEthernet0/0.2
 encapsulation dot1Q 2 native
 ip vrf forwarding VPN2
 ip address 172.21.21.74 255.255.255.0
 crypto map VPN2
```

新バージョンの Site-to-Site およびリモート アクセスの設定

この設定をアップグレードする必要があります。

（注） Site-to-Site 設定に XAUTH が不要な場合、XAUTH 設定なしで ISAKMP プロファイルを設定します。リモート アクセス設定に XAUTH が必要な場合、XAUTH ありで ISAKMP プロファイルを設定します。

```
crypto keyring VPN1-KEYS vrf VPN1
 pre-shared-key address 172.21.25.74 key VPN1
!
 crypto keyring VPN2-KEYS vrf VPN2
 pre-shared-key address 172.21.21.74 key VPN2
!
 crypto isakmp client configuration group VPN1-RA-GROUP
 key VPN1-RA
 pool VPN1-RA
!
 crypto isakmp client configuration group VPN2-RA-GROUP
 key VPN2-RA
 pool VPN2-RA
!
 crypto isakmp profile VPN1
 keyring VPN1-KEYS
 match identity address 172.21.25.74 VPN1
!
 crypto isakmp profile VPN2
 keyring VPN2-KEYS
 match identity address 172.21.21.74 VPN2
!
 crypto isakmp profile VPN1-RA
 match identity group VPN1-RA-GROUP
 client authentication list VPN1-RA-LIST
 isakmp authorization list VPN1-RA-LIST
 client configuration address initiate
 client configuration address respond
!
 crypto isakmp profile VPN2-RA
 match identity group VPN2-RA-GROUP
 client authentication list VPN2-RA-LIST
 isakmp authorization list VPN2-RA-LIST
 client configuration address initiate
 client configuration address respond
!
 crypto ipsec transform-set VPN1 esp-aes esp-sha-hmac
 crypto ipsec transform-set VPN2 esp-aes esp-sha-hmac
!
 crypto ipsec transform-set VPN1-RA esp-aes esp-sha-hmac
 crypto ipsec transform-set VPN2-RA esp-aes esp-sha-hmac
!
 crypto dynamic-map VPN1-RA 1
 set transform-set VPN1-RA
 set isakmp-profile VPN1-RA
 reverse-route
!
 crypto dynamic-map VPN2-RA 1
 set transform-set VPN2-RA
 set isakmp-profile VPN2-RA
 reverse-route
!
 crypto map VPN1 10 ipsec-isakmp
 set peer 172.21.25.74
 set transform-set VPN1
 set isakmp-profile VPN1
 match address 101
 crypto map VPN1 20 ipsec-isakmp dynamic VPN1-RA
!
 crypto map VPN2 10 ipsec-isakmp
 set peer 172.21.21.74
 set transform-set VPN2
 set isakmp-profile VPN2
```

```
 match address 102
 crypto map VPN2 20 ipsec-isakmp dynamic VPN2-RA
!
 interface FastEthernet0/0.1
 encapsulation dot1Q 1 native
 ip vrf forwarding VPN1
 ip address 172.21.25.73 255.255.255.0
 crypto map VPN1
!
 interface FastEthernet0/0.2
 encapsulation dot1Q 2 native
 ip vrf forwarding VPN2
 ip address 172.21.21.74 255.255.255.0
 crypto map VPN2
```

その他の参考資料

関連資料

関連項目	マニュアル タイトル
IPsec の設定作業	「Configuring Security for VPNs with IPsec」
IPsec コマンド	『*Cisco IOS Security Command Reference*』
IKE フェーズ 1 とフェーズ 2、アグレッシブ モード、およびメイン モード	「Configuring Internet Key Exchange for IPsec VPNs」
IKE DPD	「Easy VPN Server」
推奨される暗号化アルゴリズム	『Next Generation Encryption』

標準

標準	タイトル
なし	--

MIB

MIB	MIB のリンク
なし	選択したプラットフォーム、Cisco ソフトウェア リリース、およびフィーチャセットの MIB を検索してダウンロードする場合は、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

RFC

RFC	タイトル
なし	--

シスコのテクニカル サポート

説明	リンク
右の URL にアクセスして、シスコのテクニカル サポートを最大限に活用してください。これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

VRF-Aware IPsec の機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *268 : VRF-Aware IPsec* の機能情報

機能名	リリース	機能情報
VRF 認識 IPSec	12.2(15)T	VRF-Aware IPsec 機能には、マルチプロトコル ラベル スイッチング（MPLS）バーチャル プライベート ネットワーク（VPN）に対する IP Security（IPsec）トンネル マッピングが導入されています。VRF-Aware IPsec 機能を使用すれば、シングル パブリック方向アドレスによって、VPN ルーティング/転送（VRF）に対して IPsec トンネルをマッピングできます。 この機能は、Cisco IOS Release 12.2(15)T で導入されました。 この機能に関する詳細については、次の各項を参照してください。 次のコマンドが導入または変更されました。**address, ca trust-point, client authentication list, client configuration address, crypto isakmp profile, crypto keyring, crypto map isakmp-profile**、**initiate-mode, isakmp authorization list, keepalive (isakmp profile), keyring, key-string, match identity, no crypto xauth, pre-shared-key, quit, rsa-pubkey, self-identity, serial-number, set isakmp-profile, show crypto isakmp key, show crypto isakmp profile, vrf, clear crypto sa, crypto isakmp peer, crypto map isakmp-profile, show crypto dynamic-map, show crypto ipsec sa, show crypto isakmp sa, show crypto map (IPsec)**。
	15.1(1)S	この機能は、Cisco IOS Release 15.1(1)S に統合されました。

用語集

CA：Certification Authority（認証局）。CA はデジタル証明書を発行するエンティティ（特に X.509 証明書）で、証明書のデータ項目間のバインディングを保証します。

CLI：Command Line Interface（コマンド ライン インターフェイス）。CLI は、ユーザが、コマンドおよびオプションの引数を入力することによって、オペレーティング システムとやり取りをすることを可能にするインターフェイスです。UNIS オペレーティング システムと DOS では、CLI が使用できます。

client：マルチ プロトコル ラベル スイッチング（MPLS）ネットワーク内の UUT の対応する IPsec IOS ピア。

dead peer：到達できなくなった IKE ピア。

DN：Distinguished Name（識別名）。オープン システム インターコネクション（OSI ディレクトリ（X.500））内のエントリの、グローバルな権威ある名前です。

FQDN：Fully Qualified Domain Name（完全修飾ドメイン名）。FQDN は、単なるホスト名ではなく、システムにおける正式な名前です。たとえば、aldebaran はホスト名で、aldebaran.interop.com は FQDN です。

FR：Frame Relay（フレームリレー）。FR は、接続されたデバイス間におけるハイレベルデータ リンク（HDLC）カプセル化を使用して、複数の仮想回線を処理するための、業界標準の、スイッチデータリンク層プロトコルです。フレーム リレーは、一般的に置き代替可能と考えられているプロトコルである X.25 より効率的です。

FVRF：前面扉 Virtual Routing and Forwarding（VRF）のリポジトリ。FVRF は、暗号化されたパケットをピアにルーティングするために使用される VRF です。

IDB：Interface Descriptor Block（インターフェイス記述子ブロック）。IDB サブブロックは、アプリケーションに対してプライベートとなっているメモリ領域です。この領域には、アプリケーションにとって IDB またはインターフェイスに関連付ける必要があるプライベート情報およびステートが格納されます。アプリケーションによって IDB が使用されてポインタがそのサブブロックに登録されますが、サブブロック自体の内容には登録されません。

IKE：Internet Key Exchange（インターネット キー エクスチェンジ）。IKE によって、キーが必要なサービス（IPsec など）のための共有セキュリティ ポリシーおよび認証キーが確立されます。IPsec トラフィックを通過させる前に、ルータ、ファイアウォール、ホストそれぞれでピアの ID を検証する必要があります。それには、事前共有キーを両ホストに手動で入力するか、CA サービスを使用します。

IKE keepalive：IKE ピアの活性を判断するための双方向メカニズム。

IPsec：IP 用セキュリティプロトコル。

IVRF：Inside Virtual Routing and Forwarding。IVRF は、暗号化されていないテキスト パケットの VRF です。

MPLS：Multiprotocol Label Switching（マルチプロトコル ラベル スイッチング）。MPLS は、ラベルを使用して IP トラフィックを転送するスイッチング方式です。このラベルによって、ネットワーク内のルータおよびスイッチが、事前に確立された IP ルーティング情報に基づくパケットの転送先を指示されます。

RSA：Rivest、Shamir、Adelman は、RSA 技術の発明者です。RSA 技術は、暗号化および認証に使用可能な公開キー暗号化システムです。

SA：Security Association（セキュリティ アソシエーション）。SA は、データ フローに適用されるセキュリティ ポリシーおよびキー関連情報のインスタンスです。

VPN：Virtual Private Network（仮想プライベートネットワーク）。VPN を使用すると、ネットワーク間のトラフィックをすべて暗号化することにより、パブリック TCP/IP ネットワーク経由でも IP トラフィックをセキュアに転送できます。VPN は「トンネリング」を使用して、IP レベルですべての情報を暗号化します。

VRF：Virtual Route Forwarding（仮想ルーティングおよびフォワーディング）。VRF は、VPN ルーティングおよび転送インスタンスです。VRF は、IP ルーティング テーブル、取得されたルーティング テーブル、そのルーティング テーブルを使用する一連のインターフェイス、ルーティング テーブルに登録されるものを決定する一連のルールおよびルーティング プロトコルで構成されています。一般に、VRF には、PE ルータに付加されるカスタマー VPN サイトが定義されたルーティング情報が格納されています。

XAUTH：Extended Authentication（拡張認証）。XAUTH は、IKE フェーズ 1 と IKE フェーズ 2 の間における任意の交換です。XAUTH では、ルータが、（ピアの認証ではなく）実際のユーザの認証試行において、追加の認証情報を要求します。

第 203 章

IKE アグレッシブ モードの開始

IKE アグレッシブ モードの開始機能を使用すれば、IP Security（IPsec）ピアの RADIUS トンネル属性を指定して、トンネル属性とのインターネット キー エクスチェンジ（IKE）アグレッシブ モード ネゴシエーションを開始できます。この機能は、暗号ハブアンドスポーク シナリオでの実装に最適です。これにより、スポークが、AAA サーバ上にトンネル属性として指定され保存されている事前共有キーを使用することによって、ハブとの IKE アグレッシブ モード ネゴシエーションを開始します。このシナリオは、事前共有キーが中央リポジトリ（AAA サーバ）に保管され、複数のハブ ルータと 1 つのアプリケーションによるキーの情報の使用が可能になるので、容易に拡張できます。

（注） セキュリティに対する脅威は、脅威からの保護に役立つ暗号化技術と同様に絶え間なく変化しています。シスコの暗号化に関する最新の推奨事項の詳細は、『Next Generation Encryption』（NGE）ホワイトペーパーを参照してください。

IKE アグレッシブ モードの開始の前提条件

IKE：アグレッシブ モードの開始機能を設定する前に、次の作業を実行する必要があります。

- AAA の設定
- IPsec トランスフォームの設定
- 静的暗号マップの設定
- Internet Security Association and Key Management Protocol（ISAKMP）ポリシーの設定

- ダイナミック暗号マップの設定

IKE アグレッシブ モードの開始の制約事項

TED の制約事項

この機能は、トンネル セットアップを開始するために Tunnel Endpoint Discovery（TED）が使用されているダイナミック クリプト マップで使用するものではありません。TED は、各サイトにピアの事前共有キーを保管するための AAA サーバが必要なフル メッシュ セットアップの設定に便利ですが、この設定をこの機能と共に使用するのは実用的ではありません。

Tunnel-Client-Endpoint ID タイプ

この機能では次の ID タイプだけを使用できます。

- ID_IPV4（IPV4 アドレス）
- ID_FQDN（「foo.cisco.com」などの完全修飾ドメイン名）
- ID_USER_FQDN（E メール アドレス）

IKE アグレッシブ モードの開始に関する情報

概要

IKE：アグレッシブ モードの開始機能を使用すれば、IPSec ピアの RADIUS トンネル属性として IKE 事前共有キーを設定できます。これにより、ハブアンドスポーク トポロジ内で IKE 事前共有キーを拡張できます。

IKE事前共有キーは理解しやすく、簡単に導入できるものですが、ユーザの数が増えると拡張が難しくなり、セキュリティ上の脅威が発生しやすくなります。ハブ ルータに事前共有キーを保管するのではなく、この機能を利用すれば、事前共有キーを、認証、許可、アカウンティング（AAA）サーバに保存し、またそこから取得することによって拡張できます。事前共有キーは、Internet Engineering Task Force（IETF）RADIUS トンネル属性として AAA サーバに保存され、ユーザがハブ ルータに「スピーク」を試行する際に取得されます。ハブ ルータによって AAA サーバから事前共有キーが取得され、スポーク（ユーザ）が、Internet Security Association Key Management Policy（ISAKMP）ピア ポリシー内に RADIUS トンネル属性として指定されている事前共有キーを使用して、ハブに対してアグレッシブ モードを開始します。

RADIUS トンネル属性

IKE アグレッシブ モード ネゴシエーションを開始するには、Tunnel-Client-Endpoint（66）および Tunnel-Password（69）属性を、ISAKMP ピア ポリシー内に設定する必要があります。

Tunnel-Client-Endpoint 属性は、該当する IKE ID ペイロード内で符号化されることによって、サーバに伝達されます。Tunnel-Password 属性は、アグレッシブ モード ネゴシエーション用 IKE 事前共有キーとして使用されます。

IKE アグレッシブ モードの開始の設定方法

RADIUS トンネル属性の設定

ISAKMP ピア設定内の Tunnel-Client-Endpoint および Tunnel-Password 属性を設定するには、次の手順を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **crypto map** *map-name* **isakmp authorization list** *list-name*
4. **crypto isakmp peer** {**ip-address** *ip-address* | **fqdn** *fqdn*}
5. **set aggressive-mode client-endpoint** *client-endpoint*
6. **set aggressive-mode password** *password*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**crypto map** *map-name* **isakmp authorization list** *list-name* 例： `Router (config)# crypto map testmap10 isakmp authorization list list ike`	アグレッシブ モードで、トンネル属性に関する AAA の IKE クエリー生成をイネーブルにします。
ステップ 4	**crypto isakmp peer** {**ip-address** *ip-address* | **fqdn** *fqdn*} 例： `Router (config)# crypto isakmp peer ip address 10.10.10.1`	アグレッシブ モードで、トンネル属性に関する AAA の IKE クエリー生成のための IPsec ピアを有効化して、ISAKMP ポリシー コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 5	**set aggressive-mode client-endpoint** *client-endpoint* 例： `Router (config-isakmp)# set aggressive-mode client-endpoint user-fqdn user@cisco.com`	ISAKMP ピア設定内で、Tunnel-Client-Endpoint 属性を指定します。
ステップ 6	**set aggressive-mode password** *password* 例： `Router (config-isakmp)#set aggressive-mode password cisco123`	ISAKMP ピア設定内で、Tunnel-Password 属性を指定します。

RADIUS トンネル属性設定の確認

Tunnel-Client-Endpoint 属性および Tunnel-Password 属性が ISAKMP ピアポリシー内で設定されていることを確認するには、 **show running-config** グローバル コンフィギュレーション コマンドを使用します。

トラブルシューティングのヒント

IKE：アグレッシブモードの開始機能のトラブルシューティングを行うには、次の手順を実行します。

手順の概要

1. **enable**
2. **debug aaa authorization**
3. **debug crypto isakmp**
4. **debug radius**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**debug aaa authorization** 例： `Router# debug aaa authorization`	AAA 認証の情報を表示します。

	コマンドまたはアクション	目的
ステップ 3	**debug crypto isakmp** 例： `Router# debug crypto isakmp`	IKE イベントに関するメッセージを表示します。
ステップ 4	**debug radius** 例： `Router# debug radius`	RADIUS 関連の情報を表示します。

IKE アグレッシブ モードの開始の設定例

ハブの設定例

次に、アグレッシブ モードがサポートされているハブアンドスポーク トポロジのハブを、RADIUS トンネル属性を使用して設定する方法の例を示します。

```
!The AAA configurations are as follows:
aaa new-model
aaa authorization network ike group radius
aaa authentication login default group radius
!
! The Radius configurations are as follows:
radius-server host 10.1.1.1 auth-port 1645 acct-port 1646
radius-server key rad123
!
! The IKE configurations are as follows:
crypto isakmp policy 1
 authentication pre-share
!
! The IPsec configurations are as follows:
crypto ipsec transform-set trans1 esp-aes esp-sha-hmac
!
crypto dynamic-map Dmap 10
 set transform-set trans1
!
crypto map Testtag isakmp authorization list ike
crypto map Testtag 10 ipsec-isakmp dynamic Dmap
!
interface FastEthernet0
 ip address 10.4.4.1 255.255.255.0
 crypto map Testtag
!
interface FastEthernet1
 ip address 10.2.2.1 255.255.255.0
```

スポークの設定例

次に、アグレッシブ モードがサポートされているハブアンドスポーク トポロジのスポークを、RADIUS トンネル属性を使用して設定する方法の例を示します。

```
!The IKE configurations are as follows:
crypto isakmp policy 1
 authentication pre-share
!
! The IPsec configurations are as follows:
crypto ipsec transform-set trans1 esp-aes esp-sha-hmac
 access-list 101 permit ip 10.3.3.0 0.0.0.255 10.2.2.0 0.0.0.255
!
! Initiate aggressive mode using Radius tunnel attributes
crypto isakmp peer address 10.4.4.1
 set aggressive-mode client-endpoint user-fqdn user@cisco.com
 set aggressive-mode password cisco123
!
crypto map Testtag 10 ipsec-isakmp
 set peer 10.4.4.1
 set transform-set trans1
 match address 101
!
interface FastEthernet0
 ip address 10.5.5.1 255.255.255.0
 crypto map Testtag
!
interface FastEthernet1
 ip address 10.3.3.1 255.255.255.0
```

RADIUS ユーザ プロファイルの例

次に、Tunnel-Client-Endpoint および Tunnel-Password 属性がサポートされている RADIUS サーバ上のユーザ プロファイルの例を示します。

```
user@cisco.com  Password = "cisco", Service-Type = Outbound
    Tunnel-Medium-Type = :1:IP,
    Tunnel-Type = :1:ESP,
    Cisco:Avpair = "ipsec:tunnel-password=cisco123",
    Cisco:Avpair = "ipsec:key-exchange=ike"
```

その他の参考資料

次の項では、IKE アグレッシブ モードの開始機能に関連した関連資料を示します。

関連資料

関連項目	マニュアル タイトル
セキュリティ コマンド	『*Cisco IOS Security Command Reference*』
認証の設定	「Configuring Authentication」

関連項目	マニュアル タイトル
IKE の設定	「Configuring Internet Key Exchange for IPsec VPNs」
推奨される暗号化アルゴリズム	『Next Generation Encryption』

標準

標準	タイトル
この機能でサポートされる新規の標準または変更された標準はありません。また、既存の標準のサポートは変更されていません。	--

MIB

MIB	MIB のリンク
この機能によってサポートされる新しい MIB または変更された MIB はありません。またこの機能による既存 MIB のサポートに変更はありません。	選択したプラットフォーム、Cisco IOS XE ソフトウェア リリース、およびフィーチャ セットの MIB の場所を検索しダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

RFC

RFC	タイトル
• RFC 2409 • RFC 2868	• RFC 2409、『*The Internet Key Exchange*』 • RFC 2868、『*RADIUS Attributes for Tunnel Protocol Support*』

シスコのテクニカル サポート

説明	リンク
シスコのサポート Web サイトでは、シスコの製品やテクノロジーに関するトラブルシューティングにお役立ていただけるように、マニュアルやツールをはじめとする豊富なオンライン リソースを提供しています。 お使いの製品のセキュリティ情報や技術情報を入手するために、Cisco Notification Service（Field Notice からアクセス）、Cisco Technical Services Newsletter、Really Simple Syndication（RSS）フィードなどの各種サービスに加入できます。 シスコのサポート Web サイトのツールにアクセスする際は、Cisco.com のユーザ ID およびパスワードが必要です。	http://www.cisco.com/en/US/support/index.html

IKE アグレッシブ モードの開始の機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *269 : IKE* アグレッシブ モードの開始の機能情報

機能名	リリース	機能情報
IKE：アグレッシブ モードの開始	Cisco IOS XE Release 2.1	IKE アグレッシブ モードの開始機能を使用すれば、IPsec ピアの RADIUS トンネル属性を指定し、トンネル属性での IKE アグレッシブ モード ネゴシエーションを開始できます。 次のコマンドが導入または変更されました。**crypto isakmp peer**、**set aggressive-mode client-endpoint**、**set aggressive-mode password**。

第 XXI 部

FlexVPN およびインターネット キー エクスチェンジ

第 204 章

FlexVPN の概要

RFC 4306 に基づく次世代のキー管理プロトコルであるインターネット キー エクスチェンジ バージョン 2（IKEv2）は、IKE プロトコルの機能拡張です。IKEv2 は、相互認証を実行して SA を確立および管理するために使用します。

FlexVPN は、シスコによる IKEv2 標準の実装であり、サイト間アクセス、リモート アクセス、ハブ アンド スポーク トポロジ、および部分メッシュ（スポーク間ダイレクト）を組み合わせたユニファイド パラダイムと CLI を備えています。FlexVPN は、トンネル インターフェイス パラダイムを広範に使用し、かつ暗号マップを使用してレガシー VPN 実装との互換性を維持するシンプルなモジュラ フレームワークを提供します。

本書の構成は、次のとおりです。

インターネット キー エクスチェンジ バージョン 2（IKEv2）および FlexVPN リモート アクセスの設定

このモジュールでは IKEv2 CLI について説明します。このモジュールは、基本セクションと高度なセクションに分かれています。

基本セクションでは、基本のIKEv2コマンドを紹介し、IKEv2スマートデフォルトとFlexVPNリモート アクセスに必要な必須の IKEv2 コマンドについて説明します。このモジュールは、後続の章を理解するための前提条件です。

高度なセクションでは、グローバル IKEv2 コマンドについて説明します。また、デフォルト IKEv2 コマンドをオーバーライドする方法についても説明します。

FlexVPN サーバーの設定

このモジュールでは、FlexVPNサーバーの機能、FlexVPNサーバーの設定に必要なIKEv2コマンド、リモート アクセス クライアント、およびサポートされる RADIUS 属性について説明します。

FlexVPN クライアントの設定

このモジュールでは、FlexVPN クライアント機能と FlexVPN クライアントに必要な IKEv2 コマンドについて説明します。

IKEv2 ロード バランサの設定

このモジュールでは、IKEv2 ロード バランサ サポート機能と、IKEv2 ロード バランサの設定に必要な IKEv2 コマンドについて説明します。

IKEv2 フラグメンテーションの設定

RFC 機能に準拠した IKE フラグメンテーションでは、IETF の **draft-ietf-ipsecme-ikev2-fragmentation-10** ドキュメントの提案に従って、インターネット キー エクスチェンジ バージョン 2 （IKEv2）パケットのフラグメンテーションを実装しました。

IKEv2 再接続の設定

AnyConnect 機能の AutoReconnect 機能の IOS IKEv2 サポートは、Cisco AnyConnect でユーザーが操作しない、IKEv2 ネゴシエーションの再確立に役立ちます。

IKEv2 パケット オブ ディスコネクトの設定

IKEv2 リモート アクセス認可変更（CoA）のパケット オブ ディスコネクト機能は、シスコがサポートするデバイスのアクティブな暗号 IKEv2 セッションを停止します。

IKEv2 認可変更のサポートの設定

FlexVPN - QoS および ACL 用 IKEv2 CoA 機能は、アクティブな IKEv2 暗号セッションでの RADIUS 認可変更（CoA）をサポートしています。

集約認証の設定

FlexVPN RA - Cisco AnyConnect クライアントのサポートを拡張することで、AnyConnect 機能の集約認証サポートは、集約認証方式を実装します。このクライアントでは、独自の AnyConnect EAP 認証方式を使用し、Cisco AnyConnect クライアントと FlexVPN サーバー間にインターネットを介したセキュア トンネルを確立します。

付録：FlexVPN の RADIUS 属性

このモジュールでは、FlexVPN サーバーでサポートされる RADIUS 属性について説明します。

付録：IKEv2 およびレガシー VPN

このモジュールには、暗号化マップやインターネット キー エクスチェンジ バージョン 2（IKEv2）による DMVPN などのレガシー VPN の設定例が含まれています。

第 205 章

インターネット キー エクスチェンジ バージョン2

このモジュールには、基本および高度なインターネット キー エクスチェンジ バージョン 2（IKEv2）の情報と設定手順が含まれています。このモジュールの IKEv2 のタスクおよび設定例は、次のように分類されます。

- 基本の IKEv2：基本の IKEv2 コマンド、IKEv2 スマート デフォルト、基本の IKEv2 プロファイル、および IKEv2 キー リングに関する情報が示されています。
- 高度な IKEv2：グローバルな IKEv2 コマンドに関する情報と、IKEv2 スマート デフォルトのオーバーライド方法が示されています。

（注） セキュリティに対する脅威は、脅威からの保護に役立つ暗号化技術と同様に絶え間なく変化しています。最新のシスコの暗号化に関する推奨事項については、『Next Generation Encryption』（NGE）ホワイト ペーパーを参照してください。

インターネット キー交換バージョン 2 の設定に関する前提条件

「Configuring Security for VPNs with IPsec」モジュールで説明している概念および作業を理解している必要があります。

インターネット キー エクスチェンジ バージョン 2 の設定に関する制約事項

特定のプラットフォーム上でサポートされないオプションを設定することはできません。たとえば、セキュリティ プロトコルでハードウェア クリプト エンジンの機能が重要である場合、エクスポート可能でないイメージ内で Triple Data Encryption Standard（3DES）または Advanced Encryption Standard（AES）の各タイプの暗号化トランスフォームを指定できず、暗号エンジンでサポートされない暗号化アルゴリズムを指定できません。

インターネット キー エクスチェンジ バージョン 2 に関する情報

IKEv2 のサポート対象規格

シスコでは、インターネット キー エクスチェンジ バージョン 2（IKEv2）で使用するための IP セキュリティ（IPsec）プロトコル規格を実装しています。

（注） DES または MD5（HMAC バリアントを含む）の使用は、現在推奨されていません。代わりに、AES および SHA-256 を使用してください。シスコの暗号化に関する最新の推奨事項の詳細は、『Next Generation Encryption』（NGE）ホワイトペーパーを参照してください。

IKEv2 で実装されるコンポーネント技術は、次のとおりです。

- AES-CBC：高度暗号化規格暗号ブロック連鎖（AES-CBC）。
- SHA（HMAC バリアント）：セキュア ハッシュ アルゴリズム（SHA）。
- Diffie-Hellman：公開キー暗号法プロトコル。
- DES：データ暗号規格（現在は推奨されていません）。

- MD5（HMAC（ハッシュベースのメッセージ認証コード）バリアント）：メッセージ ダイジェスト アルゴリズム 5（現在は推奨されていません）。

サポートされる規格およびコンポーネント技術の詳細については、『*Internet Key Exchange for IPsec VPNs Configuration Guide*』の『Configuring Internet Key Exchange for IPsec VPNs』モジュールにある「Supported Standards for Use with IKE」の項を参照してください。

IKEv2 の利点

デッド ピア検出とネットワーク アドレス変換トラバーサル

インターネット キー エクスチェンジ バージョン 2（IKEv2）にはデッド ピア検出（DPD）とネットワーク アドレス変換トラバーサル（NAT-T）のサポートが組み込まれています。

証明書の URL

証明書はIKEv2パケット内で送信されるのではなくURLとハッシュを通じて参照できるため、フラグメンテーションを回避できます。

DoS 攻撃の復元力

IKEv2は、要求者を確認するまで要求を処理しません。これにより、偽の場所から大量の暗号化（高コスト）処理を実行するようにスプーフィングされる可能性があるIKEv1でのサービス妨害（DoS）の問題にある程度対処しています。

EAP のサポート

IKEv2 では認証に Extensible Authentication Protocol（EAP）を使用できます。

複数の暗号エンジン

ネットワークに IPv4 と IPv6 の両方のトラフィックがあり、複数の暗号エンジンがある場合、次のいずれかの設定オプションを選択します。

- 1 つのエンジンで IPv4 トラフィックを処理し、他方のエンジンで IPv6 トラフィックを処理する。
- 1 つのエンジンで IPv4 と IPv6 の両方のトラフィックを処理する。

信頼性と状態管理（ウィンドウイング）

IKEv2 では、信頼性を提供するためにシーケンス番号と確認が使用され、エラー処理ロジスティックと共有状態管理が要求されます。

インターネット キー エクスチェンジ バージョン 2 CLI の構成

IKEv2 プロポーザル

インターネット キー エクスチェンジ バージョン 2（IKEv2）のプロポーザルは、IKE_SA_INIT 交換の一部としてインターネット キー エクスチェンジ（IKE）セキュリティ アソシエーション（SA）のネゴシエーションで使用されるトランスフォームのコレクションです。ネゴシエーションで使用されるトランスフォームのタイプは、次のとおりです。

- 暗号化アルゴリズム
- 整合性アルゴリズム
- Pseudo-Random Function（PRF）アルゴリズム
- デフィーヘルマン（DH）グループ

デフォルト IKEv2 プロポーザルについては、「IKEv2 スマート デフォルト」の項を参照してください。デフォルト IKEv2 プロポーザルをオーバーライドする方法および新しいプロポーザルを定義する方法については、高度な IKEv2 CLI 構造の設定に関する項を参照してください。

IKEv2 ポリシー

IKEv2 ポリシーには、IKE_SA_INIT 交換での暗号化、整合性、PRF アルゴリズム、および DH グループのネゴシエーションに使用されるプロポーザルが含まれています。これには match 文を含めることができ、ネゴシエーション時にポリシーを選択するための選択基準として使用されます。

デフォルト IKEv2 ポリシーについては、「IKEv2 スマート デフォルト」の項を参照してください。デフォルト IKEv2 ポリシーをオーバーライドする方法および新しいポリシーを定義する方法については、高度な IKEv2 CLI 構造の設定に関する項を参照してください。

IKEv2 プロファイル

IKEv2 プロファイルは、IKE SA のネゴシエーション可能でないパラメータ（ローカル ID またはリモート ID および認証方式）と、そのプロファイルと一致する認証相手が使用できるサービスのリポジトリです。IKEv2 プロファイルは、発信側の暗号マップまたは IPsec プロファイルのいずれかにアタッチされる必要があります。IKEv2 プロファイルは、応答側では必須ではありません。

IKEv2 キー リング

IKEv2 キー リングは対称および非対称の事前共有キーのリポジトリであり、IKEv1 キー リングとは無関係です。IKEv2 キー リングは 1 つの IKEv2 プロファイルと関連付けられるため、その IKEv2 プロファイルに一致する一連のピアをサポートします。IKEv2 キー リングは、関連付けられた IKEv2 プロファイルから VPN ルーティングおよび転送（VRF）コンテキストを取得します。

IKEv2 スマート デフォルト

IKEv2 スマート デフォルト機能は、ほとんどの使用例に対応することで FlexVPN 設定を最小化します。IKEv2 スマートデフォルトは特定の使用例向けにカスタマイズできますが、これはお勧めしません。

デフォルト IKEv2 構造を変更する方法については、高度な IKEv2 CLI 構造の設定に関する項を参照してください。

次のルールが IKEv2 スマート デフォルト機能に適用されます。

1. デフォルト設定は、**default** をキーワードとして指定して引数を指定しない、対応する **show** コマンドで表示されます。たとえば、**show crypto ikev2 proposal default** コマンドではデフォルト IKEv2 プロポーザルが表示され、**show crypto ikev2 proposal** コマンドではユーザー設定されたプロポーザルと共にデフォルト IKEv2 プロポーザルが表示されます。
2. デフォルト設定は、**show running-config all** コマンドで表示されます。**show running-config** コマンドでは表示されません。
3. **show running-config all** コマンドで表示されるデフォルト設定を変更できます。
4. コマンドの **no** 形式（**no crypto ikev2 proposal default** など）を使用して、デフォルト設定を無効にすることができます。無効化されたデフォルト設定はネゴシエーションで使用されませんが、設定は **show running-config** コマンドで表示されます。無効化されたデフォルト設定では、ユーザー変更が失われてシステム設定値が復元されます。
5. デフォルト設定は、コマンドのデフォルト形式（**default crypto ikev2 proposal** など）を使用すると再度有効にすることができ、システム設定値が復元されます。
6. デフォルト トランスフォーム セットのデフォルト モードは、トランスポートです。その他すべてのトランスフォーム セットのデフォルト モードは、トンネルです。

（注） MD5（HMAC バリアントを含む）や Diffie-Hellman（DH）グループ 1、2、および 5 の使用は、現在は推奨されていません。代わりに、SHA-256 および DH グループ 14 以降を使用してください。最新のシスコの暗号化の推奨事項の詳細については、『Next Generation Encryption』（NGE）のホワイト ペーパーを参照してください。

次の表に、IKEv2 スマートデフォルト機能によって有効化されるコマンドをデフォルト値と共に示します。

表 *270 : IKEv2* コマンドのデフォルト

コマンド名	デフォルト値

crypto ikev2 authorization policy	`Device# show crypto ikev2 authorization policy default`
	
	`IKEv2 Authorization policy: default`
	`route set interface`
	`route accept any tag: 1 distance: 2`

コマンド名	デフォルト値
crypto ikev2 proposal	Device# **show crypto ikev2 proposal** IKEv2 proposal: default Encryption: AES-CBC-256 Integrity: SHA512 SHA384 PRF: SHA512 SHA384 DH Group: DH_GROUP_256_ECP/Group 19 DH_GROUP_2048_MODP/Group 14 DH_GROUP_521_ECP/Group 21 DH_GROUP_1536_MODP/Group 5
crypto ikev2 policy	Device# **show crypto ikev2 policy default** IKEv2 policy: default Match fvrf: any Match address local: any Proposal: default

crypto ipsec profile	Device# **show crypto ipsec profile default**
	
	IPSEC profile default
	Security association lifetime: 4608000 kilobytes/3600 seconds
	Responder-Only (Y/N): N
	PFS (Y/N): N
	Transform sets={
	default: { esp-aes esp-sha-hmac },
	}

crypto ipsec transform-set	Device# **show crypto ipsec transform-set default** Transform set default: { esp-aes esp-sha-hmac } will negotiate = { Tunnel, },

（注） デフォルト IPsec プロファイルを使用する前に、**tunnel protection ipsec profile default** コマンドを使用してトンネル インターフェイスで **crypto ipsec profile** コマンドを明示的に指定します。

（注） 他の CLI への明示的なマッピングが必要な「デフォルト」キーワードは、YANG 設定で実行されているデバイスではサポートされていません。

IKEv2 Suite-B サポート

Suite-B は、暗号の近代化プログラムの一環として国家安全保障局によって交付された一連の暗号化アリゴリズムです。インターネット キー エクスチェンジ（IKE）および IPsec の Suite-B は、RFC 4869 で定義されます。Suite-B のコンポーネントは、次のとおりです。

- IKEv2 プロポーザルで設定された Advanced Encryption Standard（AES）の 128 ビット キーおよび 256 ビット キー。データ トラフィックの場合、AES は、IPsec トランスフォーム セットに設定されるガロア カウンタ モード（GCM）で使用する必要があります。
- IKEv2 プロファイルに設定された楕円曲線デジタル署名アルゴリズム（ECDSA）。
- IKEv2 プロポーザルおよび IPsec トランスフォーム セットに設定されたセキュア ハッシュ アルゴリズム 2（SHA-256 および SHA-384）。

Suite-B の要件は、IKE および IPSec で使用するために、暗号化アルゴリズムの 4 つのユーザー インターフェイス スイートで構成されています。各スイートは、暗号化アルゴリズム、デジタル署名アルゴリズム、キー合意アルゴリズム、ハッシュまたはメッセージ ダイジェスト アルゴリズムで構成されています。Cisco での Suite-B サポートに関する詳細については、『Configuring Security for VPNs with IPsec』機能モジュールを参照してください。

AES-GCM のサポート

認証済みの暗号化アルゴリズムは、暗号化と整合性の組み合わさった機能を提供します。このようなアルゴリズムは、連結モード アルゴリズムと呼ばれます。IOS 上における IKEv2 暗号としての AES-GCM サポート機能では、ガロア/カウンタ モードの Advanced Encryption Standard（AES-GCM）を追加することによって、IKEv2 プロトコルの暗号化メッセージに認証済みの暗号化アルゴリズムを使用できます。AES-GCM は、128 ビットおよび 256 ビットのキー サイズ（AES-GCM-128 および AES-GCM-256）をサポートします。

（注） 暗号化アルゴリズムが AES-GCM のみの場合、整合性アルゴリズムをプロポーザルに追加することはできません。

IKEv2 での自動トンネル モードのサポート

複数ベンダー シナリオで VPN ヘッドエンドを設定する場合は、ピアまたはレスポンダの技術的な詳細を認識しておく必要があります。たとえば、一部のデバイスは IPsec トンネルを使用しているが、他のデバイスは Generic Routing Encapsulation（GRE）または IPsec トンネルを使用している場合やトンネルが IPv4 または IPv6 の場合があります。最後のケースでは、インターネット キーエクスチェンジ（IKE）プロファイルと仮想テンプレートを設定する必要があります。

トンネルモード自動選択機能は、設定を容易にし、レスポンダの詳細の入手を支援します。この機能は、IKE プロファイルから仮想アクセス インターフェイスが作成されるとすぐに、トンネリング プロトコル（GRE または IPsec）とトランスポート プロトコル（IPv4 または IPv6）を自動的に仮想テンプレートに適用します。この機能は、Cisco AnyConnect VPN Client や Microsoft Windows7 Client などのマルチベンダー リモート アクセスを集約しているデュアル スタック ハブ上で役に立ちます。

（注） トンネル モード自動選択機能は、レスポンダの設定のみを容易にします。トンネルはイニシエータに対して静的に設定する必要があります。

トンネル モードの自動選択機能は、IKEv2 プロファイル設定で **virtual-template** コマンドに **auto mode** キーワードを使用するとアクティブ化できます。

インターネット キー交換バージョン 2 の設定方法

基本のインターネット キー エクスチェンジ バージョン 2 CLI 構造の設定

暗号化インターフェイスで IKEv2 を有効にするには、インターネット キー エクスチェンジ バージョン 2（IKEv2）プロファイルをそのインターフェイスに適用される暗号マップまたは IPsec プロファイルにアタッチします。IKEv2 応答側では、この手順は任意です。

（注） IKEv1 と IKEv2 の違いは、IKEv1 はデバイス上のすべてのインターフェイスでグローバルに有効になっているため、個々のインターフェイスで IKEv1 を有効にする必要がないことです。

基本の IKEv2 構造を手動で設定するには、次のタスクを実行します。

IKEv2 キーリングの設定

このタスクは、ローカルまたはリモート認証方式が事前共有キーの場合に、IKEv2 キーリングを設定するために実行します。

IKEv2 キーリング キーは、ピア サブブロックを定義するピア コンフィギュレーション サブモードで設定する必要があります。IKEv2 キーリングには、複数のピア サブブロックを含めることができます。1 つのピア サブブロックには、ホスト名、ID、および IP アドレスの任意の組み合わせで識別される 1 つのピアまたはピア グループ用の単一の対称または非対称キー ペアが含まれています。

IKEv2 キーリングは IKEv1 キーリングと無関係です。主な違いは次のとおりです。

- IKEv2 キーリングは、対称事前共有キーと非対称事前共有キーをサポートします。
- IKEv2 キーリングは、Rivest、Shamir、および Adleman（RSA）公開キーをサポートしません。
- IKEv2 キーリングは、IKEv2 プロファイル内で指定され、ルックアップされないため、事前共有キー認証方式をネゴシエートするために MM1 の受信時にキーがルックアップされる IKEv1 とは異なります。IKEv2 では、認証方式がネゴシエートされません。

- IKEv2 キーリングは、設定時に VPN ルーティングおよび転送（VRF）と関連付けられません。IKEv2 キーリングの VRF は、そのキーリングを参照している IKEv2 プロファイルの VRF です。
- 複数のキー リングを指定できる IKEv1 プロファイルとは異なり、IKEv2 プロファイルでは 1 つのキー リングを指定できます。
- 同じキーが別々のプロファイルと一致するピア全体で共有されている場合は、1 つのキーリングを複数の IKEv2 プロファイルで指定できます。
- IKEv2 キーリングは 1 つ以上のピア サブブロックとして構造化されます。

IKEv2 イニシエータでは、ピアのホスト名またはアドレスを使用してその順に IKEv2 キーリング キー ルックアップが実行されます。IKEv2 レスポンダでは、ピアの IKEv2 ID またはアドレスを使用してその順にキー ルックアップが実行されます。

（注） 複数のピアで同じ ID を設定することはできません。

手順の概要

1. **enable**
2. **configure terminal**
3. **crypto ikev2 keyring** *keyring-name*
4. **peer** *name*
5. **description** *line-of-description*
6. **hostname** *name*
7. **address** {*ipv4-address* [*mask*] | *ipv6-address prefix*}
8. **identity** {**address** {*ipv4-address* | *ipv6-address*} | **fqdn domain** *domain-name* | **email domain** *domain-name* | **key-id** *key-id*}
9. **pre-shared-key** {**local** | **remote**} [**0** | **6**] *line* **hex** *hexadecimal-string*
10. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**crypto ikev2 keyring** *keyring-name* 例：	IKEv2 キーリングを定義し、IKEv2 キーリング コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
	`Device(config)# crypto ikev2 keyring kyr1`	
ステップ 4	**peer** *name* 例： `Device(config-ikev2-keyring)# peer peer1`	ピアまたはピア グループを定義し、IKEv2 キーリング コンフィギュレーション モードを開始します。
ステップ 5	**description** *line-of-description* 例： `Device(config-ikev2-keyring-peer)# description this is the first peer`	（任意）ピアまたはピア グループを記述します。
ステップ 6	**hostname** *name* 例： `Device(config-ikev2-keyring-peer)# hostname host1`	ホスト名を使用してピアを指定します。
ステップ 7	**address** {*ipv4-address* [*mask*] | *ipv6-address prefix*} 例： `Device(config-ikev2-keyring-peer)# address 10.0.0.1 255.255.255.0`	ピアの IPv4 アドレス、IPv6 アドレス、または範囲を指定します。 （注） この IP アドレスが IKE エンドポイント アドレスであり、ID アドレスとは別個のものです。

ステップ 8	**identity** {**address** {*ipv4-address* | *ipv6-address*} | **fqdn domain** *domain-name* | **email domain** *domain-name* | **key-id** *key-id*}
	例：
	`Device(config-ikev2-keyring-peer)# identity address 10.0.0.5`
		次の ID を使用して IKEv2 ピアを特定します。
		• 電子メール
		• 完全修飾ドメイン名（FQDN）。
		（注） キーリング設定で、ピアを識別するために FQDN が使用されている場合は、FQDN とともにピアの IP アドレスを使用します。
		`crypto ikev2 keyring key1`
		`peer headend-1`
		`address 1.1.1.1 >>>>>>>>>`
		`identity fqdn NFVIS-headend-1.cisco.com`
		`pre-shared-key Cisco123`
		• IPv4 アドレスまたは IPv6 アドレス
		• キー ID
		（注） ID は IKEv2 レスポンダ上のキー ルックアップにしか使用できません。

ステップ 9	**pre-shared-key** {**local** | **remote**} [**0** | **6**] *line* **hex** *hexadecimal-string* 例：	ピアの事前共有キーを指定します。

	コマンドまたはアクション	目的
	`Device(config-ikev2-keyring-peer)# pre-shared-key local key1`	
ステップ 10	**end** 例： `Device(config-ikev2-keyring-peer)# end`	IKEv2 キーリング ピア コンフィギュレーション モードを終了して、特権EXECモードに戻ります。

次の作業

IKEv2 キー リングの設定後、IKEv2 プロファイルを設定します。詳細については、「IKEv2 プロファイルの設定（基本）」セクションを参照してください。

IKEv2 プロファイルの設定（基本）

このタスクは、IKEv2 プロファイル用の必須コマンドを設定するために実行します。

IKEv2 プロファイルは、IKE セキュリティ アソシエーション（SA）（ローカル ID またはリモート ID と認証方式など）のネゴシエーション不能パラメータと、そのプロファイルと一致する認証されたピアが使用可能なサービスのリポジトリです。IKEv2プロファイルは、設定して、IKEv2 イニシエータ上のクリプト マップと IPSec プロファイルのどちらかに関連付ける必要があります。プロファイルを暗号マップまたは IPsec プロファイルに関連付けるには、**set ikev2-profile** *profile-name* コマンドを使用します。プロファイルの関連付けを解除するには、このコマンドの **no** 形式を使用します。

次のルールが match ステートメントに適用されます。

- IKEv2 プロファイルには、match identity ステートメントまたは match certificate ステートメントを含める必要があります。そうしないと、プロファイルが不完全と見なされ、使用されません。IKEv2 プロファイルには、複数の match identity ステートメントまたは match certificate ステートメントを含めることができます。
- IKEv2 プロファイルには、単一の match Front Door VPN routing and forwarding (FVRF) ステートメントを含める必要があります。
- プロファイルを選択すると、同じタイプの複数の match ステートメントが論理的に OR され、違うタイプの複数の match ステートメントが論理的に AND されます。
- match identity ステートメントと match certificate ステートメントは、同じタイプのステートメントと見なされ、OR されます。
- 重複したプロファイルの設定は、設定ミスと見なされます。複数のプロファイルが一致した場合は、どのプロファイルも選択されません。

IKEv2 プロファイルを表示するには、**show crypto ikev2 profile** *profile-name* コマンドを使用します。

手順の概要

1. **enable**

2. **configure terminal**
3. **crypto ikev2 profile** *profile-name*
4. **description** *line-of-description*
5. **aaa accounting** {**psk** | **cert** | **eap**} *list-name*
6. **authentication** {**local** {**rsa-sig** | **pre-share** [**key** {**0** | **6**} *password*}] | **ecdsa-sig** | **eap** [**gtc** | **md5** | **ms-chapv2**] [**username** *username*] [**password** {**0** | **6**} *password*}]} | **remote** {**eap** [**query-identity** | **timeout** *seconds*] | **rsa-sig** | **pre-share** [**key** {**0** | **6**} *password*}] | **ecdsa-sig**}}
7. **dpd** *interval retry-interval* {**on-demand** | **periodic**}
8. **dynamic**
9. **identity local** {**address** {*ipv4-address* | *ipv6-address*} | **dn** | **email** *email-string* | **fqdn** *fqdn-string* | **key-id** *opaque-string*}
10. **initial-contact force**
11. **ivrf** *name*
12. **keyring** {**local** *keyring-name* | **aaa** *list-name* [**name-mangler** *mangler-name* | **password** *password*] }
13. **lifetime** *seconds*
14. **match** {**address local** {*ipv4-address* | *ipv6-address* | **interface** *name*} | **certificate** *certificate-map* | **fvrf** {*fvrf-name* | **any**} | **identity remote address** {*ipv4-address* [*mask*] | *ipv6-address prefix*} | {**email** [*domain string*] | **fqdn** [*domain string*]} *string* | **key-id** *opaque-string*}
15. **nat keepalive** *seconds*
16. **pki trustpoint** *trustpoint-label* [**sign** | **verify**]
17. **virtual-template** *number* **mode auto**
18. **shutdown**
19. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。プロンプトが表示されたらパスワードを入力します。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**crypto ikev2 profile** *profile-name* 例： `Device(config)# crypto ikev2 profile profile1`	IKEv2プロファイルを定義し、IKEv2プロファイル コンフィギュレーション モードを開始します。
ステップ 4	**description** *line-of-description* 例： `Device(config-ikev2-profile)# description This is an IKEv2 profile`	（任意）プロファイルを記述します。

	コマンドまたはアクション	目的
ステップ 5	**aaa accounting** {**psk** | **cert** | **eap**} *list-name* 例： `Device(config-ikev2-profile)# aaa accounting eap list1`	（任意）IPsec セッションの認証、認可、およびアカウンティング（AAA）アカウンティング方式リストを有効にします。 （注） **psk**、**cert**、または **eap** キーワードが指定されなかった場合は、ピア認証方式に関係なく、AAA アカウンティング方式リストが使用されます。
ステップ 6	**authentication** {**local** {**rsa-sig** | **pre-share** [**key** {**0** | **6**} *password*}] | **ecdsa-sig** | **eap** [**gtc** | **md5** | **ms-chapv2**] [**username** *username*] [**password** {**0** | **6**} *password*}]} | **remote** {**eap** [**query-identity** | **timeout** *seconds*] | **rsa-sig** | **pre-share** [**key** {**0** | **6**} *password*}] | **ecdsa-sig**}} 例： `Device(config-ikev2-profile)# authentication local ecdsa-sig`	ローカルまたはリモートの認証方式を指定します。 • **rsa-sig**：認証方式として RSA-sig を指定します。 • **pre-share**：認証方式として事前共有キーを指定します。 • **ecdsa-sig**：認証方式として ECDSA-sig を指定します。 • **eap**：リモート認証方式として EAP を指定します。 • **query-identity**：ピアに EAP ID を問い合わせます。 • **timeout** *seconds*：最初の IKE_AUTH 応答を返してから次の IKE_AUTH 要求を受け取るまでの期間を秒単位で指定します。 （注） ローカル認証方式は 1 つしか指定できませんが、リモート認証方式は複数指定できます。
ステップ 7	**dpd** *interval retry-interval* {**on-demand** | **periodic**} 例： `Device(config-ikev2-profile)# dpd 30 6 on-demand`	この手順は任意です。（任意）プロファイルと一致したピアの Dead Peer Detection（DPD; デッドピア検出）をグローバルに設定します。デフォルトでは、Dead Peer Detection（DPD; デッドピア検出）は無効化されています。

	コマンドまたはアクション	目的
		（注） この手順の例では、着信 ESP トラフィックがない場合、最初の DPD が 30 秒後に送信されます。6 秒間（指定された再試行間隔）待機した後、DPD 再試行が 6 秒間隔でアグレッシブに 5 回送信されます。そのため、合計 66 秒（30 + 6 + 6 X 5 = 66）が経過すると、DPD によって暗号化セッションが切断されます。
ステップ 8	**dynamic** 例： `Device(config-ikev2-profile)# dynamic`	ダイナミック IKEv2 プロファイルを設定します。このキーワードは、Cisco IOS XE 17.2.1 リリースで導入されました。 （注） 動的プロファイルを設定する場合、コマンドラインインターフェイスを使用して、ローカルまたはリモートの認証とアイデンティティを設定することはできません。
ステップ 9	**identity local** {**address** {*ipv4-address* | *ipv6-address*} | **dn** | **email** *email-string* | **fqdn** *fqdn-string* | **key-id** *opaque-string*} 例： `Device(config-ikev2-profile)# identity local email abc@example.com`	この手順は任意です。（任意）ローカル IKEv2 アイデンティティタイプを指定します。 （注） ローカル認証方式が事前共有キーの場合は、デフォルトのローカル ID が IP アドレスになります。ローカル認証方式が Rivest、Shamir、および Adleman（RSA）署名の場合は、デフォルトのローカル ID が識別名になります。
ステップ 10	**initial-contact force** 例： `Device(config-ikev2-profile)# initial-contact force`	初期連絡先通知が IKE_AUTH 交換で受信されなかった場合に、初期連絡先処理を強制します。
ステップ 11	**ivrf** *name* 例： `Device(config-ikev2-profile)# ivrf vrf1`	この手順は任意です。IKEv2 プロファイルがクリプトマップに適用されている場合に、ユーザー定義の VPN ルーティングおよび転送（VRF）またはグローバル VRF を指定します。 • IKEv2 プロファイルをトンネル保護に使用している場合は、トンネルインターフェイス上で内部 VRF（IVRF）を設定する必要があります。

	コマンドまたはアクション	目的
		（注） IVRF は、クリア テキスト パケット用の VRF を指定します。IVRF のデフォルト値は FVRF です。
ステップ 12	**keyring** {**local** *keyring-name* | **aaa** *list-name* [**name-mangler** *mangler-name* | **password** *password*] } 例： `Device(config-ikev2-profile)# keyring aaa keyring1 name-mangler mangler1`	ローカルまたはリモートの事前共有キー認証方式で使用する必要があるローカルまたはAAAベースのキーリングを指定します。 （注） 1 つのキーリングしか指定することができません。ローカル AAA は AAA ベースの事前共有キーに対してサポートされません。 （注） リリースによっては、**local** キーワードと **name-mangler** *mangler-name* キーワード引数ペアを使用する必要があります。 （注） AAAを使用する場合、Radiusアクセス要求のデフォルト パスワードは「cisco」です。パスワードを変更するには、**keyring** コマンド内で **password** キーワードを使用します。 （注） IKEv2 プロファイルからキーリングを削除するには、**no keyring** {**aaa** | **local** | **ppk**} *keyring-name* コマンドを使用します。
ステップ 13	**lifetime** *seconds* 例： `Device(config-ikev2-profile)# lifetime 1000`	IKEv2 SA のライフタイムを秒単位で指定します。
ステップ 14	**match** {**address local** {*ipv4-address* | *ipv6-address* | **interface** *name*} | **certificate** *certificate-map* | **fvrf** {*fvrf-name* | **any**} | **identity remote address** {*ipv4-address* [*mask*] | *ipv6-address prefix*} | {**email** [*domain string*] | **fqdn** [*domain string*]} *string* | **key-id** *opaque-string*} 例： `Device(config-ikev2-profile)# match address local interface Ethernet 2/0`	match ステートメントを使用して、ピア用の IKEv2 プロファイルを選択します。
ステップ 15	**nat keepalive** *seconds* 例： `Device(config-ikev2-profile)# nat keepalive 500`	（任意）NAT キープアライブを有効にして、その期間を秒単位で指定します。 • デフォルトでは、NATは無効になっています。

	コマンドまたはアクション	目的
ステップ 16	**pki trustpoint** *trustpoint-label* [**sign** | **verify**] 例： `Device(config-ikev2-profile)# pki trustpoint tsp1 sign`	RSA 署名認証方式で使用する Public Key Infrastructure（PKI）トラストポイントを指定します。 （注） **sign** または **verify** キーワードが指定されていない場合、トラストポイントは署名と検証に使用されます。 （注） IKEv1 とは対照的に、証明書ベースの認証を成功させるためにトラストポイントを IKEv2 プロファイル内で設定する必要があります。このコマンドが設定内に存在しない場合は、グローバルに設定されたトラストポイントのフォールバックが存在しません。トラストポイント設定は IKEv2 イニシエータおよびレスポンダに適用されます。
ステップ 17	**virtual-template** *number* **mode auto** 例： `Device(config-ikev2-profile)# virtual-template 1 mode auto`	この手順は任意です。仮想アクセスインターフェイス（VAI）のクローニング用の仮想テンプレートを指定します。 • **mode auto**：トンネルモード自動選択機能を有効にします。 （注） IPsec ダイナミック仮想トンネル インターフェイス（DVTI）では、仮想テンプレートを IKEv2 セッションが開始されない IKEv2 プロファイル内で指定する必要があります。
ステップ 18	**shutdown** 例： `Device(config-ikev2-profile)# shutdown`	（任意）IKEv2 プロファイルをシャット ダウンします。
ステップ 19	**end** 例： `Device(config-ikev2-profile)# end`	IKEv2 プロファイル コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

高度なインターネット キー エクスチェンジ バージョン 2 CLI 構造の設定

この項では、グローバル IKEv2 CLI 構造について説明します。また、IKEv2 のデフォルト CLI 構造をオーバーライドする方法についても説明します。IKEv2 スマートデフォルトは、ほとん

どの使用例をサポートします。そのため、デフォルトで対応されない特定の使用例に必要な場合にのみ、デフォルトをオーバーライドすることをお勧めします。

高度な IKEv2 CLI 構造を設定するには、次のタスクを実行します。

グローバル IKEv2 オプションの設定

この作業は、ピアに依存しないグローバル IKEv2 オプションを設定するために実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **crypto ikev2 certificate-cache** *number-of-certificates*
4. **crypto ikev2 cookie-challenge** *number*
5. **crypto ikev2 diagnose error** *number*
6. **crypto ikev2 dpd** *interval retry-interval* {**on-demand** | **periodic**}
7. **crypto ikev2 http-url cert**
8. **crypto ikev2 limit** { **max-in-negotiation-sa** *limit* | **max-sa** *limit*}
9. **crypto ikev2 nat keepalive** *interval*
10. **crypto ikev2 window** *size*
11. **crypto logging ikev2**
12. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**crypto ikev2 certificate-cache** *number-of-certificates* 例： `Device(config)# crypto ikev2 certificate-cache 750`	HTTP URL から取得した証明書を保存するためのキャッシュ サイズを定義します。
ステップ 4	**crypto ikev2 cookie-challenge** *number* 例： `Device(config)# crypto ikev2 cookie-challenge 450`	ハーフオープン セキュリティ アソシエーション（SA）の数が設定された値を超えた場合にだけ、IKEv2 cookie チャレンジを有効にします。 • Cookie チャレンジは、デフォルトで無効化されています。

	コマンドまたはアクション	目的
ステップ 5	**crypto ikev2 diagnose error** *number* 例： `Device(config)# crypto ikev2 diagnose error 500`	IKEv2 エラーの診断を有効にして終了パス データベースのエントリ数を定義します。 • IKEv2 エラー診断はデフォルトでは無効化されています。
ステップ 6	**crypto ikev2 dpd** *interval retry-interval* {**on-demand** | **periodic**} 例： `Device(config)# crypto ikev2 dpd 30 6 on-demand`	ピアを次のようにライブでチェックできるようにします。 • Dead Peer Detection（DPD：デッドピア検出）はデフォルトでは無効化されています。 （注） この手順の例では、着信 ESP トラフィックがない場合、最初の DPD が 30 秒後に送信されます。6 秒間（指定された再試行間隔）待機した後、DPD 再試行が 6 秒間隔でアグレッシブに 5 回送信されます。そのため、合計 66 秒（30 + 6 + 6 X 5 = 66）が経過すると、DPD によって暗号化セッションが切断されます。
ステップ 7	**crypto ikev2 http-url cert** 例： `Device(config)# crypto ikev2 http-url cert`	HTTP CERT サポートを有効にします。 • HTTP CERT は、デフォルトで無効化されています。
ステップ 8	**crypto ikev2 limit** { **max-in-negotiation-sa** *limit* | **max-sa** *limit*} 例：	コネクション アドミッション制御（CAC）を有効にします。 • コネクション アドミッション制御はデフォルトで有効化されています。
ステップ 9	**crypto ikev2 nat keepalive** *interval* 例： `Device(config)# crypto ikev2 nat keepalive 500`	ネットワーク アドレス変換（NAT）のキープアライブを有効にして、インターネットキーエクスチェンジ（IKE）ピア間に NAT がある場合に、任意のトラフィックが欠けることによる NAT の削除を防ぎます。 • NAT キープアライブはデフォルトで無効化されています。
ステップ 10	**crypto ikev2 window** *size* 例： `Device(config)# crypto ikev2 window 15`	送信時に複数の IKEv2 要求と応答のピアを許可します。 • デフォルトのウィンドウ サイズは 5 です。

	コマンドまたはアクション	目的
ステップ 11	**crypto logging ikev2** 例： `Device(config)# crypto logging ikev2`	IKEv2 Syslog メッセージを有効にします。 • デフォルトでは、IKEv2 syslog メッセージは無効化されています。
ステップ 12	**end** 例： `Device(config)# end`	グローバル コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

IKEv2 フラグメンテーションの設定

このタスクを実行して、大規模な IKEv2 パケットのラグメンテーションを有効にします。

手順の概要

1. **enable**
2. **configure terminal**
3. **crypto ikev2 fragmentation** [**mtu** *mtu-size*]
4. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**crypto ikev2 fragmentation** [**mtu** *mtu-size*] 例： `Device(config)# crypto ikev2 fragmentation mtu 100`	IKEv2 フラグメンテーションを設定します。 • MTU の範囲は 96 ～ 1500 バイトです。デフォルトの MTU サイズは、IPv4 パケットでは 576 バイト、IPv6 パケットでは 1280 バイトです。 （注） MTU のサイズは、IP または UDP でカプセル化された IKEv2 パケットを示します。
ステップ 4	**end** 例： `Device(config)# end`	グローバル コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

IKEv2 プロポーザルの設定

デフォルトの IKEv2 プロポーザルについては、「IKEv2 スマート デフォルト」の項を参照してください。

このタスクは、デフォルト プロポーザルを使用しない場合に、デフォルト IKEv2 プロポーザルをオーバーライドするか、手動でプロポーザルを設定するために実行します。

IKEv2 プロポーザルは、IKE_SA_INIT 交換の一部として IKEv2 SA のネゴシエーションに使用されるトランスフォームのセットです。IKEv2 プロポーザルは、少なくとも 1 つの暗号化アルゴリズム、整合性アルゴリズム、および Diffie-Hellman（DH）グループが設定されている場合にのみ、完全であるとみなされます。プロポーザルが設定されておらず、IKEv2 ポリシーにアタッチされていない場合は、デフォルト IKEv2 ポリシー内のデフォルト プロポーザルがネゴシエーションで使用されます。

（注） セキュリティに対する脅威は、脅威からの保護に役立つ暗号化技術と同様に絶え間なく変化しています。最新のシスコの暗号化に関する推奨事項については、『Next Generation Encryption』（NGE）ホワイト ペーパーを参照してください。

IKEv2 プロポーザルは **crypto isakmp policy** コマンドに似ていますが、IKEv2 プロポーザルには次のような違いがあります。

- IKEv2 プロポーザルを使用すると、各トランスフォーム タイプに対して 1 つ以上のトランスフォームを設定できます。
- IKEv2 プロポーザルには関連付けられた優先順位はありません。

手順の概要

1. **enable**
2. **configure terminal**
3. **crypto ikev2 proposal** *name*
4. **encryption** *encryption-type...*
5. **integrity** *integrity-type...*
6. **group** *group-type...*
7. **prf** *prf-algorithm*
8. **end**
9. **show crypto ikev2 proposal** [*name* | **default**]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。

	コマンドまたはアクション	目的
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**crypto ikev2 proposal** *name* 例： `Device(config)# crypto ikev2 proposal proposal1`	デフォルト IKEv2 プロポーザルをオーバーライドして、IKEv2 プロポーザル名を定義し、IKEv2 プロポーザル コンフィギュレーション モードを開始します。
ステップ 4	**encryption** *encryption-type...* 例： `Device(config-ikev2-proposal)# encryption aes-cbc-128 aes-cbc-192`	1 つまたは複数の暗号化タイプのトランスフォームを指定します。タイプは次のとおりです。 • **3des**（非推奨） • **aes-cbc-128** • **aes-cbc-192** • **aes-cbc-256** • **aes-gcm-128** • **aes-gcm-256**
ステップ 5	**integrity** *integrity-type...* 例： `Device(config-ikev2-proposal)# integrity sha1`	次のように、整合性アルゴリズム タイプの 1 つ以上のトランスフォームを指定します。 • **md5** キーワードは、ハッシュ アルゴリズムとして MD5（HMAC バリアント）を指定します。（非推奨） • **sha1** キーワードは、ハッシュ アルゴリズムとして SHA-1（HMAC バリアント）を指定します。 • **sha256** キーワードは、ハッシュ アルゴリズムとして SHA-2 ファミリ 256 ビット（HMAC バリアント）を指定します。 • **sha384** キーワードは、ハッシュ アルゴリズムとして SHA-2 ファミリ 384 ビット（HMAC バリアント）を指定します。 • **sha512** キーワードは、ハッシュ アルゴリズムとして SHA-2 ファミリ 512 ビット（HMAC バリアント）を指定します。 （注） 暗号化タイプとして Advanced Encryption Standard（AES）in Galois/Counter Mode（AES GCM）を指定した場合は、整合性アルゴリズム タイプを指定できません。

	コマンドまたはアクション	目的
ステップ 6	**group** *group-type...* 例： `Device(config-ikev2-proposal)# group 14`	Diffie-Hellman（DH）グループ ID を指定します。 • デフォルトの DH グループ識別子は、IKEv2 プロポーザル内のグループ 2 および 5 です。 • **1**：768 ビット DH（非推奨）。 • **2**：1024 ビット DH（非推奨）。 • **5**：1536 ビット DH（非推奨）。 • **14**：2048 ビット DH グループを指定します。 • **15**：3072 ビット DH グループを指定します。 • **16**：4096 ビット DH グループを指定します。 • **19**：256 ビット Elliptic Curve DH（ECDH）グループを指定します。 • **20**：384 ビット ECDH グループを指定します。 • **24**：2048 ビット DH グループを指定します。 選択するグループは、ネゴシエーション中の IPsec キーを保護するため、十分強力（十分なビット数がある）である必要があります。一般に受け入れられているガイドラインでは、2013 年以降（2030 年まで）は 2048 ビット グループの使用が推奨されています。このガイドラインを満たすために、グループ 14 とグループ 24 のどちらかを選択できます。より寿命の長いセキュリティ方式が必要な場合でも、楕円曲線暗号の使用をお勧めしますが、グループ 15 とグループ 16 も検討してください。
ステップ 7	**prf** *prf-algorithm* 例： `Device(config-ikev2-proposal)# prf sha256 sha512`	次のように、1 つ以上の擬似ランダム関数（PRF）アルゴリズムを指定します。 • **md5** • **sha1** • **sha256** • **sha384** • **sha512**

	コマンドまたはアクション	目的
		（注） この手順は、暗号化タイプが AES-GCM：**aes-gmc-128** または **aes-gmc-256** の場合に必須です。暗号化アルゴリズムが AES-GCM でない場合は、PRF アルゴリズムが指定された整合性アルゴリズムと同じになります。ただし、必要に応じて、PRF アルゴリズムを指定できます。
ステップ 8	**end** 例： `Device(config-ikev2-proposal)# end`	IKEv2 プロポーザル コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。
ステップ 9	**show crypto ikev2 proposal** [*name* | **default**] 例： `Device# show crypto ikev2 proposal default`	（任意）IKEv2 プロポーザルを表示します。

次の作業

IKEv2 プロポーザルを作成した後、ポリシーと接続して、ネゴシエーションでプロポーザルを選択できるようにします。このタスクの完了について、詳細は「IKEv2 ポリシーの設定」セクションを参照してください。

IKEv2 ポリシーの設定

デフォルトの IKEv2 ポリシーについては、「IKEv2 スマート デフォルト」の項を参照してください。

このタスクは、デフォルト ポリシーを使用しない場合に、デフォルト IKEv2 ポリシーをオーバーライドするか、手動でポリシーを設定するために実行します。

IKEv2 ポリシーには、完全だと考えられる 1 つ以上のプロポーザルを含める必要があり、ネゴシエーション用のポリシーを選択するための選択基準として使用される match ステートメントを含めることができます。初期交換中に、ネゴシエートする SA のローカル アドレス（IPv4 または IPv6）と Front Door VRF（FVRF）がポリシーと照合され、プロポーザルが選択されます。

次のルールが match ステートメントに適用されます。

- match ステートメントを含まない IKEv2 ポリシーは、グローバル FVRF 内のすべてのピアと一致します。
- IKEv2 ポリシーには、match FVRF ステートメントを 1 つしか含めることができません。
- IKEv2 ポリシーには、match address local ステートメントを 1 つ以上含めることができます。
- ポリシーを選択すると、同じタイプの複数の match ステートメントが論理的に OR され、違うタイプの match ステートメントが論理的に AND されます。

- タイプが異なる match ステートメントの優先順位はありません。
- 重複したポリシーの設定は、設定ミスと見なされます。複数のポリシーが一致した場合は、最初のポリシーが選択されます。

手順の概要

1. **enable**
2. **configure terminal**
3. **crypto ikev2 policy** *name*
4. **proposal** *name*
5. **match fvrf** {*fvrf-name* | **any**}
6. **match address local** {*ipv4-address* | *ipv6-address*}
7. **end**
8. **show crypto ikev2 policy** [*policy-name* | **default**]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**crypto ikev2 policy** *name* 例： `Device(config)# crypto ikev2 policy policy1`	デフォルト IKEv2 ポリシーをオーバーライドして、IKEv2 ポリシー名を定義し、IKEv2 ポリシー コンフィギュレーション モードを開始します。
ステップ 4	**proposal** *name* 例： `Device(config-ikev2-policy)# proposal proposal1`	このポリシーで使用する必要があるプロポーザルを指定します。 • プロポーザルは、一覧の順の優先順位になります。 （注） 少なくとも 1 つのプロポーザルを指定する必要があります。各プロポーザルを別々のステートメントに分けた追加のプロポーザルを指定できます。
ステップ 5	**match fvrf** {*fvrf-name*	**any**} 例： `Device(config-ikev2-policy)# match fvrf any`	（任意）ポリシーをユーザーが設定した FVRF または任意の FVRF に基づいて照合します。 • デフォルトはグローバル FVRF です。

	コマンドまたはアクション	目的
		（注） 任意の VRF と一致させるには、**match fvrf any** コマンドを明示的に設定する必要があります。FVRF には、IKEv2 パケットのネゴシエーションを行う VRF を指定します。
ステップ 6	**match address local** {*ipv4-address* | *ipv6-address*} 例： `Device(config-ikev2-policy)# match address local 10.0.0.1`	（任意）ローカル IPv4 または IPv6 アドレスに基づいてポリシーを照合します。 • デフォルトは、設定済みの FVRF 内のすべてのアドレスと一致します。
ステップ 7	**end** 例： `Device(config-ikev2-policy)# end`	IKEv2 ポリシー コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。
ステップ 8	**show crypto ikev2 policy** [*policy-name* | **default**] 例： `Device# show crypto ikev2 policy policy1`	（任意）IKEv2 ポリシーを表示します。

インターネット キー エクスチェンジ バージョン 2 の設定例

基本のインターネット キー エクスチェンジ バージョン 2 CLI 構造の設定例

例：IKEv2 キー リングの設定

例：複数のピア サーバブロックを持つ IKEv2 キー リング

次の例は、複数のピア サブブロックを持つインターネット キー エクスチェンジ バージョン 2（IKEv2）キー リングを設定する方法を示します。

```
crypto ikev2 keyring keyring-1
 peer peer1
  description peer1
  address 209.165.200.225 255.255.255.224
  pre-shared-key key-1
 peer peer2
  description peer2
  hostname peer1.example.com
  pre-shared-key key-2
```

```
 peer peer3
  description peer3
  hostname peer3.example.com
  identity key-id abc
  address 209.165.200.228 255.255.255.224
  pre-shared-key key-3
```

例：IP アドレスに基づく対称型事前共有キーを使用した IKEv2 キー リング

次の例は、IP アドレスに基づく対称型事前共有キーを使用する IKEv2 キー リングの設定方法を示します。次は、発信側のキー リングです。

```
crypto ikev2 keyring keyring-1
 peer peer1
  description peer1
  address 209.165.200.225 255.255.255.224
  pre-shared-key key1
```

次は、応答側のキー リングです。

```
crypto ikev2 keyring keyring-1
 peer peer2
  description peer2
  address 209.165.200.228 255.255.255.224
  pre-shared-key key1
```

例：IP アドレスに基づく非対称型事前共有キーを使用した IKEv2 キー リング

次の例は、IP アドレスに基づく非対称型事前共有キーを使用する IKEv2 キー リングの設定方法を示します。次は、発信側のキー リングです。

```
crypto ikev2 keyring keyring-1
 peer peer1
  description peer1 with asymmetric keys
  address 209.165.200.225 255.255.255.224
  pre-shared-key local key1
  pre-shared-key remote key2
```

次は、応答側のキー リングです。

```
crypto ikev2 keyring keyring-1
 peer peer2
  description peer2 with asymmetric keys
  address 209.165.200.228 255.255.255.224
  pre-shared-key local key2
  pre-shared-key remote key1
```

例：ホスト名に基づく非対称型事前共有キーを使用した IKEv2 キー リング

次の例は、ホスト名に基づく非対称型事前共有キーを使用する IKEv2 キー リングの設定方法を示します。次は、発信側のキー リングです。

```
crypto ikev2 keyring keyring-1
 peer host1
  description host1 in example domain
  hostname host1.example.com
  pre-shared-key local key1
  pre-shared-key remote key2
```

次は、応答側のキー リングです。

```
crypto ikev2 keyring keyring-1
 peer host2
  description host2 in abc domain
  hostname host2.example.com
  pre-shared-key local key2
  pre-shared-key remote key1
```

例：アイデンティティに基づく対称型事前共有キーを使用した IKEv2 キー リング

次の例は、アイデンティティに基づく対称型事前共有キーを使用する IKEv2 キー リングの設定方法を示します。

```
crypto ikev2 keyring keyring-4
 peer abc
  description example domain
  identity fqdn example.com
  pre-shared-key abc-key-1
 peer user1
  description user1 in example domain
  identity email user1@example.com
  pre-shared-key abc-key-2
 peer user1-remote
  description user1 example remote users
  identity key-id example
  pre-shared-key example-key-3
```

例：ワイルドカード キーを使用した IKEv2 キー リング

次の例は、ワイルドカード キーを使用する IKEv2 キー リングの設定方法を示します。

```
crypto ikev2 keyring keyring-1
 peer cisco
  description example domain
  address 0.0.0.0 0.0.0.0
  pre-shared-key example-key
```

例：キー リングの照合

次の例は、キー リングの照合方法を示します。

```
crypto ikev2 keyring keyring-1
 peer cisco
  description example.com
  address 0.0.0.0 0.0.0.0
  pre-shared-key xyz-key
 peer peer1
  description abc.example.com
  address 10.0.0.0 255.255.0.0
  pre-shared-key abc-key
 peer host1
  description host1@abc.example.com
  address 10.0.0.1
  pre-shared-key host1-example-key
```

ここに示す例では、ピア 10.0.0.1 を照合するキーは最初にワイルドカード キー example-key と一致し、次にプレフィックス キー example-key と一致し、最後にホスト キー host1-example-key と一致します。最適な一致である host1-example-key が使用されます。

```
crypto ikev2 keyring keyring-2
 peer host1
 description host1 in abc.example.com sub-domain
 address 10.0.0.1
 pre-shared-key host1-example-key
 peer host2
  description example domain
  address 0.0.0.0 0.0.0.0
  pre-shared-key example-key
```

ここに示す例では、ピア 10.0.0.1 を照合するキーは最初にホスト キー host1-abc-key と一致します。これが固有の一致であることから、これ以上の照合は実行されません。

例：プロファイルの設定

例：リモート ID で照合する IKEv2 プロファイル

次のプロファイルは、完全修飾ドメイン名（FQDN）example.com を使用して自身を特定し、トラストポイントリモートを使用して RSA 署名で認証するピアをサポートします。ローカルノードは、keyring-1 を使用する事前共有キーでノード自体を認証します。

```
crypto ikev2 profile profile2
 match identity remote fqdn example.com
 identity local email router2@example.com
 authentication local pre-share
 authentication remote rsa-sig
 keyring keyring-1
 pki trustpoint trustpoint-remote verify
 lifetime 300
 dpd 10 5 on-demand
 virtual-template 1
```

例：2 つのピアをサポートする IKEv2 プロファイル

次の例は、異なる認証方式を使用する 2 つのピアがサポートする、IKEv2 プロファイルの設定方法を示します。

```
crypto ikev2 profile profile2
 match identity remote email user1@example.com
 match identity remote email user2@example.com
 identity local email router2@cisco.com
 authentication local rsa-sig
 authentication remote pre-share
 authentication remote rsa-sig
 keyring keyring-1
 pki trustpoint trustpoint-local sign
 pki trustpoint trustpoint-remote verify
 lifetime 300
 dpd 10 5 on-demand
 virtual-template 1
```

例：証明書および IKEv2 スマート デフォルトを使用するダイナミック ルーティングによる FlexVPN の設定

次の例に、トンネルを介したダイナミック ルーティングによるブランチデバイス（発信者側、スタティック仮想トンネルインターフェイス（sVTI）を使用）と中央デバイス（応答側、ダイナミック仮想トンネルインターフェイス（dVTI）を使用）との間の接続を示します。この例ではIKEv2 スマートデフォルトを使用し、認証は証明書（RSA 署名）を使用して実行されます。

（注） 推奨される RSA モジュラス サイズは 2048 です。

ピアは IKEv2 ID として FQDN を使用し、応答側の IKEv2 プロファイルは ID FQDN のドメインと一致します。

発信側（ブランチ デバイス）での設定は、次のとおりです。

```
hostname branch
ip domain name cisco.com
!
crypto ikev2 profile branch-to-central
 match identity remote fqdn central.cisco.com
 identity local fqdn branch.cisco.com
 authentication local rsa-sig
 authentication remote rsa-sig
 pki trustpoint CA
!
crypto ipsec profile svti
 set ikev2-profile branch-to-central
!
interface Tunnel0
 ip address 172.16.0.101 255.255.255.0
 tunnel source Ethernet0/0
 tunnel mode ipsec ipv4
 tunnel destination 10.0.0.100
 tunnel protection ipsec profile svti
!
interface Ethernet0/0
 ip address 10.0.0.101 255.255.255.0
!
interface Ethernet1/0
 ip address 192.168.101.1 255.255.255.0
!
router rip
 version 2
 passive-interface Ethernet1/0
 network 172.16.0.0
 network 192.168.101.0
 no auto-summary
```

応答側（中央ルータ）での設定は、次のとおりです。

```
hostname central
ip domain name cisco.com
!
crypto ikev2 profile central-to-branch
 match identity remote fqdn domain cisco.com
 identity local fqdn central.cisco.com
```

```
 authentication local rsa-sig
 authentication remote rsa-sig
 pki trustpoint CA
 virtual-template 1
!
interface Loopback0
 ip address 172.16.0.100 255.255.255.0
!
interface Ethernet0/0
 ip address 10.0.0.100 255.255.255.0
!
interface Ethernet1/0
 ip address 192.168.100.1 255.255.255.0
!
interface Virtual-Template1 type tunnel
 ip unnumbered Loopback0
 tunnel source Ethernet0/0
 tunnel mode ipsec ipv4
 tunnel protection ipsec profile default
!
router rip
 version 2
 passive-interface Ethernet1/0
 network 172.16.0.0
 network 192.168.100.0
 no auto-summary
```

高度なインターネット キー エクスチェンジ バージョン 2 CLI 構造の設定例

例：プロポーザルの設定

例：各トランスフォーム タイプに対して 1 つのトランスフォームがある IKEv2 プロポーザル

次の例は、各トランスフォームタイプに対して1つのトランスフォームがあるIKEv2プロポーザルの設定方法を示します。

```
crypto ikev2 proposal proposal-1
 encryption aes-cbc-128
 integrity sha1
 group 14
```

例：各トランスフォーム タイプに対して複数のトランスフォームがある IKEv2 プロポーザル

次の例は、各トランスフォームタイプに対して複数のトランスフォームがあるIKEv2プロポーザルの設定方法を示します。

```
crypto ikev2 proposal proposal-2
 encryption aes-cbc-128 aes-cbc-192
 integrity sha1
 group 14
```

（注） シスコは現在、3DES、MD5（HMAC バリアント含む）、および Diffie-Hellman（DH）グループ 1、2、および 5 の使用は推奨していません。代わりに、AES、SHA-256、および DH グループ 14 以降を使用する必要があります。シスコの暗号化に関する最新の推奨事項の詳細は、『Next Generation Encryption』（NGE）ホワイト ペーパーを参照してください。

ここに示す IKEv2 プロポーザル proposal-2 では、次の組み合わせのトランスフォームの優先順位リストに変換されます。

- aes-cbc-128, sha1, 14
- aes-cbc-192, sha1, 14

例：発信側と応答側の IKEv2 プロポーザル

次の例は、発信側と応答側の IKEv2 プロポーザルの設定方法を示します。発信側のプロポーザルは次のとおりです。

```
crypto ikev2 proposal proposal-1
 encryption aes-cbc-192 aes-cbc-128
 integrity sha-256 sha1
 group 14 24
```

応答側のプロポーザルは次のとおりです。

```
crypto ikev2 proposal proposal-2
 encryption aes-cbc-128 aes-cbc-192
 peer
 integrity sha1 sha-256
 group 24 14
```

選択したプロポーザルは次のようになります。

```
encryption aes-cbc-128
integrity sha1
group 14
```

発信側と応答側に示されるプロポーザルでは、発信側と応答側では設定が競合します。この場合、発信側が応答側よりも優先されます。

例：ポリシーの設定

例：VRF およびローカル アドレスで照合する IKEv2 ポリシー

次の例は、IKEv2 ポリシーが VRF およびローカル アドレスで照合する方法を示します。

```
crypto ikev2 policy policy2
 match vrf vrf1
 match local address 10.0.0.1
 proposal proposal-1
```

例：グローバル VRF 内のすべてのピアを照合する複数のプロポーザルがある IKEv2 ポリシー

次の例は、複数のプロポーザルがある IKEv2 ポリシーがグローバル VRF 内のピアを照合する方法を示します。

```
crypto ikev2 policy policy2
 proposal proposal-A
 proposal proposal-B
 proposal proposal-B
```

例：任意の VRF 内のすべてのピアを照合する IKEv2 ポリシー

次の例は、任意の VRF 内のピアを照合する IKEv2 ポリシーの方法を示します。

```
crypto ikev2 policy policy2
 match vrf any
 proposal proposal-1
```

例：ポリシーの照合

重複するポリシーは設定しないでください。一致する複数の可能性がポリシーにある場合、次の例に示すように、最適な照合が使用されます。

```
crypto ikev2 policy policy1
 match fvrf fvrf1
crypto ikev2 policy policy2
 match fvrf fvff1
 match local address 10.0.0.1
```

vrf1 という FVRF のプロポーザルと 10.0.0.1 というローカル ピアは policy2 および policy2 と一致しますが、policy1 が最適な一致であるためにこちらが選択されます。

次の作業

IKEv2 の設定後、IPsec VPN の設定に進みます。詳細については、『Configuring Security for VPNs with IPsec』モジュールを参照してください。

インターネット キー エクスチェンジ バージョン 2（IKEv2）のその他の関連資料

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『Cisco IOS Master Command List』、すべてのリリース

関連項目	マニュアル タイトル
セキュリティ コマンド	• 『Cisco IOS Security Command Reference: Commands A to C』 • 『Cisco IOS Security Command Reference: Commands D to L』 • 『Cisco IOS Security Command Reference: Commands M to R』 • 『Cisco IOS Security Command Reference: Commands S to Z』
IPsec の設定	『Configuring Security for VPNs with IPsec』
Suite-B の ESP トランスフォーム	『Configuring Security for VPNs with IPsec』
Suite-B SHA-2 ファミリ（HMAC バリアント）および Elliptic Curve（EC）キー ペアの設定	『Configuring Internet Key Exchange for IPsec VPNs』
IPsec SA ネゴシエーションでの Suite-B の Elliptic Curve Diffie-Hellman（ECDH）のサポート	『Configuring Internet Key Exchange for IPsec VPNs』
PKI の証明書登録のための Suite-B サポート	『Configuring Certificate Enrollment for a PKI』
IKE での使用にサポートされている標準	『Internet Key Exchange for IPsec VPNs Configuration Guide』
推奨される暗号化アルゴリズム	『Next Generation Encryption』

RFC

RFC	タイトル
RFC 4306	*Internet Key Exchange (IKEv2) Protocol*
RFC 4869	*Suite B Cryptographic Suites for IPsec*
RFC 5685	*Redirect Mechanism for the Internet Key Exchange Protocol Version 2 (IKEv2)*

シスコのテクニカル サポート

説明	リンク
右の URL にアクセスして、シスコのテクニカル サポートを最大限に活用してください。これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

インターネット キー エクスチェンジ バージョン 2（IKEv2）の設定に関する機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *271 :* インターネット キー エクスチェンジ バージョン *2*（*IKEv2*）の設定に関する機能情報

機能名	リリース	機能情報
IPsec と IKEv2 に対する IPv6 のサポート		この機能によって、IPv6 アドレスを IPsec および IKEv2 プロトコルに追加できます。 次のコマンドが導入または変更されました。 **address (IKEv2 keyring), identity (IKEv2 keyring), identity local, match (IKEv2 policy), match (IKEv2 profile), show crypto ikev2 session, show crypto ikev2 sa, show crypto ikev2 profile, show crypto ikev2 policy, debug crypto condition, clear crypto ikev2 sa.**

機能名	リリース	機能情報
IOS ソフトウェア暗号での Suite-B のサポート		パケットデータの認証およびIKEv2プロポーザル設定の整合性確認メカニズムの検証に使用される SHA-2 ファミリ（HMAC バリアント）のハッシュアルゴリズムに、Suite-Bのサポートが追加されました。HMACは、追加レベルのハッシュを提供するバリアントです。 Suite-B によって、RFC 4754 で定義されているように楕円曲線デジタル署名アルゴリズム（ECDSA）署名（ECDSA-sig）を IKEv2 の認証方式にすることもできます。 Suite-B の要件は、暗号化アルゴリズムの 4 つのユーザー インターフェイス スイートです。アルゴリズムは、RFC 4869 で説明されている IKE および IPSec で使用します。各スイートは、暗号化アルゴリズム、デジタル署名アルゴリズム、キー合意アルゴリズム、およびハッシュまたはメッセージダイジェストアルゴリズムで構成されています。Cisco IOS 上における Suite-B サポートの詳細については、『Configuring Security for VPNs with IPsec』モジュールを参照してください。 次のコマンドが導入または変更されました。 **authentication, group, identity (IKEv2 profile), integrity, match (IKEv2 profile).**
IOS 上における IKEv2 暗号としての AES-GCM のサポート		IKEv2 機能の AES-GCM サポートでは、Galois/カウンタ モードの Advanced Encryption Standard（AES-GCM）の使用方法を説明します。インターネット キー エクスチェンジ バージョン 2（IKEv2）プロトコルの暗号化ペイロードと共に認証済みの暗号化アルゴリズムを使用することについても説明します。 次のコマンドが導入または変更されました。 **encryption (IKEv2 proposal), prf, show crypto ikev2 proposal.**
トンネルモード自動選択		トンネルモード自動選択機能は、設定を容易にし、レスポンダの詳細の入手を支援します。この機能は、IKE プロファイルから仮想アクセスインターフェイスが作成されるとすぐに、トンネリングプロトコル（GRE または IPsec）とトランスポート プロトコル（IPv4 または IPv6）を自動的に仮想テンプレートに適用します。 次のコマンドが導入または変更されました。 **virtual-template (IKEv2 profile), show crypto ikev2 profile.**

第 206 章

ポスト量子事前共有キーを使用した量子安全暗号化の設定

このモジュールでは、ポスト量子事前共有キー（PPK）を使用した量子安全暗号化について説明します。この機能により、PPK を使用した IKEv2 および IPsec パケットの量子安全暗号化のために、RFC 8784 および Cisco Secure Key Integration Protocol（SKIP）が実装されます。

ポスト量子事前共有キーを使用した量子安全暗号化に関する制約事項

- ポスト量子事前共有キーを使用した量子安全暗号化の機能は、GETVPN を除くすべての IKEv2 および IPsec VPN（FlexVPN（SVTI-DVTI）、DMVPN など）に適用できます。

サポートされるプラットフォーム

ポスト量子事前共有キーを使用した量子安全暗号化の機能は、次のプラットフォームで使用できます。

Cisco IOS XE リリース 17.11 以降	Cisco IOS XE リリース 17.12 以降
Cisco Catalyst 8000V Edge ソフトウェア	Cisco 1000 シリーズ サービス統合型ルータ

Cisco IOS XE リリース 17.11 以降	Cisco IOS XE リリース 17.12 以降
Cisco Catalyst 8300 シリーズ エッジ プラットフォーム	Cisco Catalyst 8500 シリーズ エッジプラットフォーム
Cisco ASR 1000 シリーズ アグリゲーション サービス ルータ	

ポスト量子事前共有キーを使用した量子安全暗号化に関する情報

以下のセクションでは、ポスト量子事前共有キーを使用した量子安全暗号化の機能に関する詳細情報を提供します。

量子コンピュータが暗号に与える影響

量子コンピュータは、現在普及している暗号アルゴリズムおよびプロトコルに深刻な課題をもたらします。量子コンピュータは、Diffie-Hellman（DH）および楕円曲線Diffie-Hellman（ECDH）の問題を多項式時間で解決できるため、既存のIKEv2システムのセキュリティが侵害される可能性があります。今日の VPN 通信を保存している中間者は、後で量子コンピュータが使用可能になると、それらを復号できます。

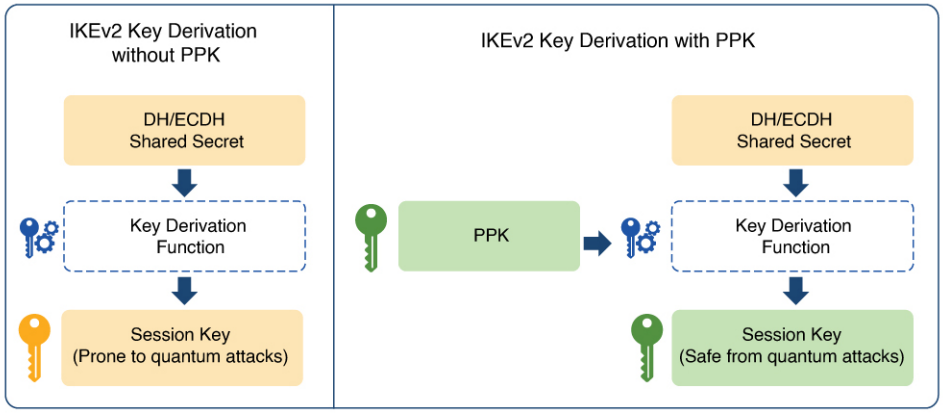
ポスト量子事前共有キー

事前共有キーに十分なエントロピーがあり、疑似乱数関数（PRF）、暗号化、および認証変換が量子セキュアである場合、事前共有キーに基づくセッションキーは、量子攻撃に対して脆弱ではありません。このようにして得られるシステムは、今日の古典的な攻撃者や量子コンピュータを使用する将来の攻撃者に対してセキュアであると考えられます。

RFC 8784（ポスト量子セキュリティのためのIKEv2での事前共有キーの混合）には、「PPK」と呼ばれる事前共有キーを使用して量子コンピュータに対する耐性を実現するIKEv2プロトコルの機能拡張が記述されています。この RFC では、PPK 機能のネゴシエーション、PPK ID の通信、セッションキー導出の追加入力としての PPK の混合、および非 PPK ベースのセッションへのオプションのフォールバックが定義されています。

図 1 に、PPK を使用する場合と使用しない場合の IKEv2 キーの導出を示します。

図 *102 : IKEv2* キーの導出：*PPK* を使用する場合と使用しない場合



DH: Diffie-Hellman
ECDH: Elliptic-curve Diffie-Hellman
PPK: Postquantum Preshared Key

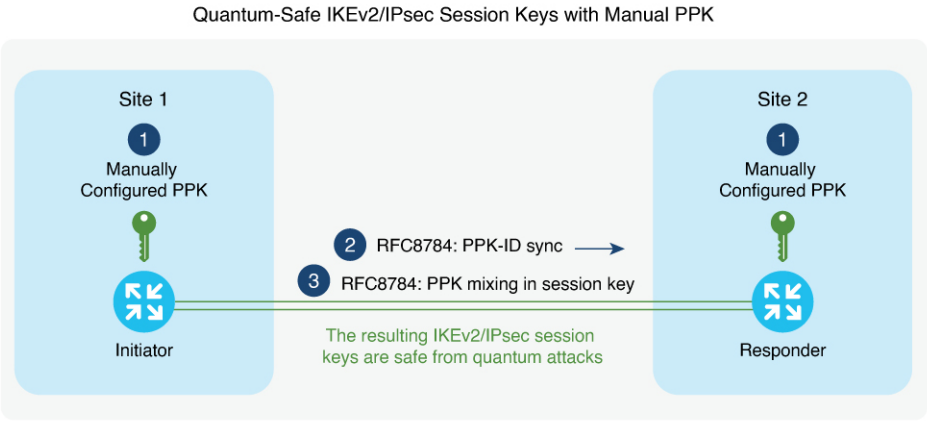
手動ポスト量子事前共有キー

IKEv2 および IPsec の発信側と応答側のペアで同じ PPK を提供する最も簡単なプロビジョニングメカニズムは、両側で PPK を手動で設定することです。手動で設定された PPK は、「手動 PPK」と呼ばれます。

手動 PPK の場合、管理者は、PPK のサイズとエントロピーが十分であり、頻繁にローテーションされることを確認する必要があります。

図 2 は、手動 PPK を使用した量子安全な IKEv2 および IPsec セッションキーを示しています。

図 *103 :* 手動 *PPK* を使用した量子安全な *IKEv2* および *IPsec* セッションキー



Cisco Secure Key Integration Protocol およびダイナミックポスト量子事前共有キー

Cisco SKIP は、ルータなどの暗号化デバイスが外部キーソースから PPK をインポートすることを可能にする HTTPS ベースのプロトコルです。ダイナミック PPK と呼ばれる外部からインポートされた PPK は、自動プロビジョニングおよび更新と、PPK のエントロピーの向上という利点を提供します。

Cisco SKIP は、TLS1.2 と PSK-DHE 暗号スイートを使用して、SKIP プロトコルを量子安全にします。暗号化デバイスは SKIP クライアントを実装する必要があり、外部キーソースは SKIP サーバーを実装する必要があります。

外部キーソースを SKIP 準拠にするには、Cisco SKIP プロトコルを実装し、アウトオブバンド同期メカニズムを使用して、2 つの暗号化デバイス（イニシエータとレスポンダ）に同じ PPK を提供する必要があります。外部キーソースには、量子キー配布（QKD）デバイス、ソフトウェア、もしくはクラウドベースキーソースまたはサービスを使用できます。

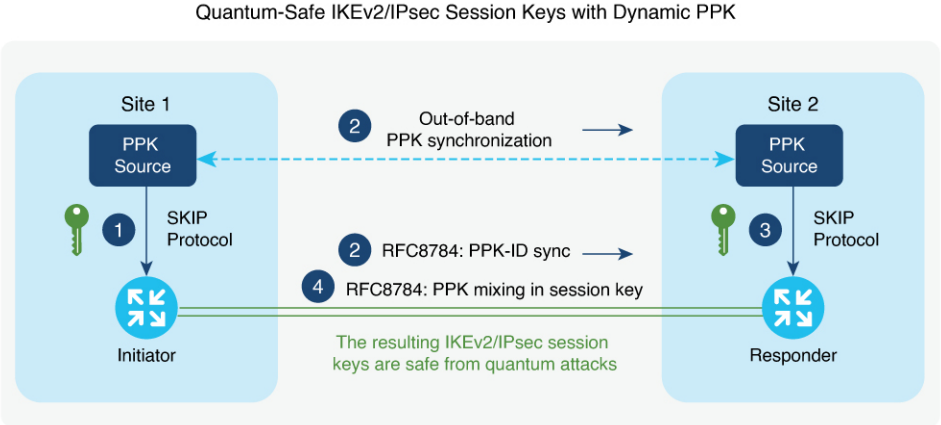
外部キーソースは、SKIP に準拠するために次の要件を満たす必要があります。

- Cisco SKIP 仕様で定義されているように、SKIP プロトコルまたは API を実装する必要があります。
- アウトオブバンド同期メカニズムを使用して、暗号化デバイスのペア（イニシエータとレスポンダ）に同じ PPK を提供する必要があります。

（注） 主要なソースベンダー（QKD ベンダーなど）は、シスコの担当者に連絡して、Cisco SKIP プロトコルを実装する必要があります。

図 3 は、ダイナミック PPK を使用した量子安全な IKEv2 および IPsec セッションキーを示しています。

図 *104* : ダイナミック *PPK* を使用した量子安全な *IKEv2* および *IPsec* セッションキー



IKEv2 イニシエータとレスポンダは、ローカルキーソースに接続され、キーソースの IP アドレスおよびポートと TLS1.2 セッションの事前共有キーを指定する SKIP クライアントで設定されます。PPK ソースは、ローカル キー ソース アイデンティティとピアキーソースのアイデンティティリストを含む SKIP パラメータを使用して設定されます。

次に、Cisco SKIP プロトコルの動作の概要を示します。

1. IKEv2 イニシエータは、そのキーソースに PPK を要求します。キーソースは、PPK と対応する PPK ID で応答します。
2. イニシエータ側のキーソースは、キーソースのタイプに固有のアウトオブバンドメカニズムを使用して、PPK をレスポンダ側のキーソースに同期します。IKEv2 イニシエータは、RFC 8784 の機能拡張を使用して、IKEv2 経由で IKEv2 レスポンダに PPK ID を伝達します。
3. IKEv2 レスポンダは、そのキーソースに、IKEv2 イニシエータから受信した PPK ID に対応する PPK を要求します。キーソースは、PPK ID に対応する PPK で応答します。
4. IKEv2 イニシエータおよびレスポンダは、RFC 8784 で規定されているように、キー導出で PPK を混合します。結果として得られる IKEv2 および IPsec セッションキーは、量子安全です。

ポスト量子事前共有キーを使用した量子安全暗号化の設定方法

以下のセクションでは、ポスト量子事前共有キーを使用した量子安全暗号化の設定に関連するプロセスについて説明します。

手動ポスト量子事前共有キーの設定

手動 PPK を設定するには、次の作業を実行します。

IKEv2 キーリングでの手動ポスト量子事前共有キーの設定

IKEv2 キーリングで 1 つ以上のピアまたはピアグループの手動 PPK を設定するには、次の手順を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **crypto ikev2 keyring** *keyring-name*
4. **peer** *name*
5. 次のコマンドの 1 つを実行します。
   - **address** {*ipv4-address mask* | *ipv6-address prefix*}

- **identity** {**address** {*ipv4-address* | *ipv6-address*} | **fqdn domain** *domain-name* | **email domain** *domain-name* | **key-id** *key-id*}

6. **ppk manual id** *ppk-id* **key** [**0** | **6** | **hex**] *password* [**required**]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 プロンプトが表示されたらパスワードを入力します。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**crypto ikev2 keyring** *keyring-name* 例： `Device(config)# crypto ikev2 keyring keyring1`	IKEv2 キーリングを定義し、IKEv2 キーリング コンフィギュレーション モードを開始します。
ステップ 4	**peer** *name* 例： `Device(config-ikev2-keyring)# peer peer1`	ピアまたはピア グループを定義し、IKEv2 キーリング コンフィギュレーション モードを開始します。

ステップ 5	次のコマンドの 1 つを実行します。
	• **address** {*ipv4-address mask* | *ipv6-address prefix*}
	• **identity** {**address** {*ipv4-address* | *ipv6-address*} | **fqdn domain** *domain-name* | **email domain** *domain-name* | **key-id** *key-id*}
	例：
	`Device(config-ikev2-keyring-peer)# address 10.0.0.1 255.0.0.0`
	例：
	`Device(config-ikev2-keyring-peer)# identity address 10.0.0.1`
		WAN IP アドレスまたは IKEv2 アイデンティティに基づいてリモート IKEv2 ピアを指定します。
		• **address** コマンドは、ピアまたはピアグループの IPv4 または IPv6 アドレスあるいは範囲を指定します。
		（注） この IP アドレスが IKE エンドポイント アドレスであり、ID アドレスとは別個のものです。
		• **identity** コマンドは、次のアイデンティティを使用して IKEv2 ピアを特定します。
		• 電子メール
		• 完全修飾ドメイン名（FQDN）
		• IPv4 アドレスまたは IPv6 アドレス
		• キー ID
		（注） **identity** コマンドは、IKEv2 レスポンダ上のキールックアップにしか使用できません。

	コマンドまたはアクション	目的
ステップ 6	**ppk manual id** *ppk-id* **key** [**0** | **6** | **hex**] *password* [**required**] 例： `Device(config-ikev2-keyring-peer)# ppk manual id ppk_id key cisco123`	特定されたピアの PPK ID および PPK を設定します。 • **ppk manual**：PPK ID と PPK が手動で設定されていることを示します。 • **id** *ppk-id*：PPK ID を指定します。 • **key** *password*：PPK を指定します。 • **required**：PPK を使用した量子安全暗号化が必須であり、通常の IKEv2 または IPsec セッションへのフォールバックが存在してはならないことを示します。 （注） *ppk-id* と PPK は、両方のピアで一致する必要があります。

IKEv2 プロファイルでの IKEv2 キーリングの設定

手順の概要

1. **crypto ikev2 profile** *profile-name*
2. **keyring ppk** *keyring-name*
3. **exit**
4. **exit**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**crypto ikev2 profile** *profile-name* 例： `Device(config-ikev2-keyring-peer)# crypto ikev2 profile profile1`	IKEv2 プロファイルを定義し、IKEv2 プロファイル コンフィギュレーション モードを開始します。
ステップ 2	**keyring ppk** *keyring-name* 例： `Device(config-ikev2-profile)# keyring ppk keyring1`	手動または動的 PPK が設定されているキーリングを指定します。 （注） IKEv2 プロファイルからキーリングを削除するには、**no keyring** {**aaa** | **local** | **ppk**} *keyring-name* コマンドを使用します。
ステップ 3	**exit** 例： `Device(config-ikev2-profile)# exit`	IKEv2 プロファイル コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードに戻ります。

	コマンドまたはアクション	目的
ステップ 4	**exit** 例： `Device(config)# exit`	グローバル コンフィギュレーション モードを終了し、特権 EXEC モードを開始します。

ダイナミックポスト量子事前共有キーの設定

ダイナミック PPK を設定するには、次の作業を実行します。

Secure Key Integration Protocol クライアントの設定

SKIP クライアントの設定では、外部の SKIP 準拠キーソースとセキュアに通信し、そこから PPK を要求するために必要なパラメータを指定します。

手順の概要

1. **enable**
2. **configure terminal**
3. **crypto skip-client** *skip-client-name*
4. **server** {**ipv4** *ipv4-address* | **ipv6** *ipv6-address* | **fqdn** *domain-name*} **port** *port-number*
5. **psk id** *id-name* **key** [**0** | **6** | **hex**] *password*
6. **exit**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 プロンプトが表示されたらパスワードを入力します。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**crypto skip-client** *skip-client-name* 例： `Device(config-crypto-skip-client)# crypto skip-client skip-client-cfg`	SKIP クライアント設定ブロックの名前を指定し、SKIP クライアント コンフィギュレーション モードを開始します。
ステップ 4	**server** {**ipv4** *ipv4-address* | **ipv6** *ipv6-address* | **fqdn** *domain-name*} **port** *port-number* 例： `Device(config-crypto-skip-client)# server ipv4 10.10.0.3 port 9993`	外部キーソースに接続する IP アドレスまたは FQDN とポートを指定します。

	コマンドまたはアクション	目的
ステップ 5	**psk id** *id-name* **key** [**0** | **6** | **hex**] *password* 例： `Device(config-crypto-skip-client)# psk id psk-id key 0 cisco123`	SKIP TLS セッションの事前共有キーアイデンティティと事前共有キーを指定します。
ステップ 6	**exit** 例： `Device(config-crypto-skip-client)# exit`	SKIP クライアント コンフィギュレーション モードを終了して、グローバル コンフィギュレーション モードに戻ります。

IKEv2 キーリングの Secure Key Integration Protocol クライアントの設定

IKEv2 キーリングで 1 つ以上のピアまたはピアグループの手動 PPK を設定するには、次の手順を実行します。

手順の概要

1. **crypto ikev2 keyring** *keyring-name*
2. **peer** *name*
3. 次のいずれかのコマンドを実行します。
   - **address** {*ipv4-address mask* | *ipv6-address prefix*}
   - **identity** {**address** {*ipv4-address* | *ipv6-address*} | **fqdn domain** *domain-name* | **email domain** *domain-name* | **key-id** *key-id*}
4. **ppk dynamic** *skip-client-name* [**required**]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**crypto ikev2 keyring** *keyring-name* 例： `Device(config)# crypto ikev2 keyring keyring1`	IKEv2 キーリングを定義し、IKEv2 キーリング コンフィギュレーション モードを開始します。
ステップ 2	**peer** *name* 例： `Device(config-ikev2-keyring)# peer peer1`	ピアまたはピア グループを定義し、IKEv2 キーリング コンフィギュレーション モードを開始します。
ステップ 3	次のいずれかのコマンドを実行します。 • **address** {*ipv4-address mask* | *ipv6-address prefix*} • **identity** {**address** {*ipv4-address* | *ipv6-address*} | **fqdn domain** *domain-name* | **email domain** *domain-name* | **key-id** *key-id*} 例： `Device(config-ikev2-keyring-peer)# address 10.0.0.1 255.0.0.0`	WAN IP アドレスまたは IKEv2 アイデンティティに基づいてリモート IKEv2 ピアを指定します。 **address** コマンドは、ピアまたはピアグループの IPv4 または IPv6 アドレスあるいは範囲を指定します。 （注） この IP アドレスが IKE エンドポイント アドレスであり、ID アドレスとは別個のものです。

	コマンドまたはアクション	目的
	例： `Device(config-ikev2-keyring-peer)# identity address 10.0.0.1`	**identity** コマンドは、次のアイデンティティを使用して IKEv2 ピアを特定します。 • 電子メール • 完全修飾ドメイン名（FQDN） • IPv4 アドレスまたは IPv6 アドレス • キー ID （注） **identity** コマンドは、IKEv2 レスポンダ上のキールックアップにしか使用できません。
ステップ 4	**ppk dynamic** *skip-client-name* [**required**] 例： `Device(config-ikev2-keyring-peer)# ppk dynamic skip-client1`	ダイナミック PPK に使用する外部キーソースを指定します。 • **ppk dynamic**：PPK が外部キーソースから動的にインポートされることを示します。 • **required**：PPK を使用した量子安全暗号化が必須であり、通常の IKEv2 または IPsec セッションへのフォールバックが存在してはならないことを示します。

IKEv2 プロファイルでの IKEv2 キーリングの設定

手順の概要

1. **crypto ikev2 profile** *profile-name*
2. **keyring ppk** *keyring-name*
3. **exit**
4. **exit**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**crypto ikev2 profile** *profile-name* 例： `Device(config-ikev2-keyring-peer)# crypto ikev2 profile profile1`	IKEv2 プロファイルを定義し、IKEv2 プロファイル コンフィギュレーション モードを開始します。
ステップ 2	**keyring ppk** *keyring-name* 例：	手動または動的 PPK が設定されているキーリングを指定します。

	コマンドまたはアクション	目的
	`Device(config-ikev2-profile)# keyring ppk keyring1`	（注） IKEv2プロファイルからキーリングを削除するには、**no keyring** {**aaa** | **local** | **ppk**} *keyring-name* コマンドを使用します。
ステップ 3	**exit** 例： `Device(config-ikev2-profile)# exit`	IKEv2プロファイル コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードに戻ります。
ステップ 4	**exit** 例： `Device(config)# exit`	グローバル コンフィギュレーション モードを終了し、特権 EXEC モードを開始します。

ポスト量子事前共有キーを使用した量子安全暗号化の設定例

以下のセクションでは、PPK を使用した量子安全暗号化の設定に関連する詳細な設定例を示します。

例：手動ポスト量子事前共有キーの設定

例：イニシエータの設定

次に、イニシエータの PPK を手動で設定する例を示します。

```
conf t
hostname Router1
!
crypto ikev2 keyring ppk-keyring
peer 1
address 10.10.0.1 255.255.255.0
ppk manual id ppk_id key cisco123
!
crypto ikev2 profile prof
match identity remote address 10.10.0.1
authentication local pre-share key cisco
authentication remote pre-share key cisco
keyring ppk ppk-keyring
!
crypto ipsec profile prof
set ikev2-profile prof
!
interface Tunnel0
ip address 10.10.0.1 255.255.255.0
tunnel source GigabitEthernet1
tunnel destination 10.10.10.1
tunnel protection ipsec profile prof
!
```

```
interface GigabitEthernet1
ip address 10.10.10.2 255.255.255.0
no shut
!
```

例：応答側の設定

次に、レスポンダの PPK を手動で設定する例を示します。

```
conf t
hostname Router2
!
crypto ikev2 keyring ppk-keyring
peer 1
address 10.10.0.1 255.255.255.0
ppk manual id ppk_id key cisco
!
crypto ikev2 profile prof
match identity remote address 10.10.0.1
authentication local pre-share key cisco
authentication remote pre-share key cisco
keyring ppk ppk-keyring
!
crypto ipsec profile prof
set ikev2-profile prof
!
interface Tunnel0
ip address 10.10.0.2 255.255.255.0
tunnel source GigabitEthernet1
tunnel destination 10.10.10.2
tunnel protection ipsec profile prof
!
interface GigabitEthernet1
ip address 10.10.0.1 255.255.255.0
no shut
!
```

例：ダイナミックポスト量子事前共有キーの設定

例：イニシエータの設定

次に、イニシエータのダイナミック PPK の設定方法の例を示します。

```
conf t
hostname Router1
!
crypto skip-client skip-client-cfg
server ipv4 10.10.0.4  port 9991
psk id psk-id1 key 0 cisco123
!
crypto ikev2 keyring ppk-keyring
peer 1
address 10.10.0.1 255.255.255.0
ppk dynamic skip-client-cfg
!
crypto ikev2 profile prof
match identity remote address 10.10.0.1
authentication local pre-share key cisco
authentication remote pre-share key cisco
keyring ppk ppk-keyring
```

```
!
crypto ipsec profile prof
set ikev2-profile prof
!
interface Tunnel0
ip address 10.10.0.2 255.255.255.0
tunnel source GigabitEthernet1
tunnel destination 10.10.10.1
tunnel protection ipsec profile prof
!
interface GigabitEthernet1
ip address 10.10.10.2 255.255.255.0
no shut
!
interface GigabitEthernet1
ip address 10.10.10.3 255.255.255.0
no shut
!
```

例：応答側の設定

次に、応答側のダイナミック PPK の設定方法の例を示します。

```
conf t
hostname Router2
!
crypto skip-client skip-client-cfg
server ipv4 10.10.0.4 port 9992
psk id vedge-sim-1 key 0 cisco123
!
crypto ikev2 keyring ppk-keyring
peer 1
address 10.10.0.1 255.255.255.0
ppk dynamic skip-client-cfg
!
crypto ikev2 profile prof
match identity remote address 10.10.0.1
authentication local pre-share key cisco
authentication remote pre-share key cisco
keyring ppk ppk-keyring
!
crypto ipsec profile prof
set ikev2-profile prof
!
interface Tunnel0
ip address 10.10.0.2 255.255.255.0
tunnel source GigabitEthernet1
tunnel destination 10.10.10.2
tunnel protection ipsec profile prof
!
interface GigabitEthernet1
ip address 10.10.10.1 255.255.255.0
no shut
!
interface GigabitEthernet1
ip address 10.10.10.4 255.255.255.0
!
```

ポスト量子事前共有キーの設定の確認

現在の IKEv2 セキュリティ アソシエーションに関する情報を表示するには、**show crypto ikev2 sa detailed** コマンドを使用します。出力に表示される「Quantum Resistance Enabled」メッセージは、PPK ベースの量子安全暗号化が有効になっていることを示します。

次に、**show crypto ikev2 sa detailed** コマンドの出力例を示します。

```
IPv4 Crypto IKEv2  SA
Tunnel-id       Local                Remote                  fvrf/ivrf           Status

   3        <src IP>/SrcPort     <Dst IP>/DstPort              none/none        READY

Encr: AES-CBC, keysize: 256, PRF: SHA512, Hash: SHA512, DH Grp:19,
Auth sign:
.
.
.
Initiator of SA : No
Quantum Resistance Enabled
```

ポスト量子事前共有キーを使用した量子安全暗号化に関する追加情報

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『Cisco IOS Master Command List』、すべてのリリース
セキュリティ コマンド	• 『Cisco IOS Security Command Reference: Commands A to C』 • 『Cisco IOS Security Command Reference: Commands D to L』 • 『Cisco IOS Security Command Reference: Commands M to R』 • 『Cisco IOS Security Command Reference: Commands S to Z』
IPsec の設定	『Configuring Security for VPNs with IPsec』

RFC

RFC	タイトル
RFC 8784	『*Mixing Preshared Keys in the Internet Key Exchange Protocol Version 2 (IKEv2) for Postquantum Security*』

シスコのテクニカル サポート

説明	リンク
右の URL にアクセスして、シスコのテクニカル サポートを最大限に活用してください。これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

ポスト量子事前共有キーを使用した量子安全暗号化に関する機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *272 :* ポスト量子事前共有キーを使用した量子安全暗号化に関する機能情報

機能名	リリース	機能情報
ポスト量子事前共有キーを使用した量子安全暗号化	Cisco IOS XE リリース 17.11.1a	この機能により、ポスト量子事前共有キー（PPK）を使用した IKEv2 および IPsec パケットの量子安全暗号化のために、RFC 8784 および Cisco Secure Key Integration Protocol（SKIP）が実装されます。手動で設定された PPK は「手動 PPK」と呼ばれ、SKIP プロトコルを使用して外部キーソースからインポートされる PPK は「ダイナミック PPK」と呼ばれます。
ポスト量子事前共有キーを使用した量子安全暗号化	Cisco IOS XE リリース 17.12.1a	この機能拡張により、次のプラットフォームに、ポスト量子事前共有キーを使用した量子安全暗号化のサポートが導入されます。 • Cisco 1000 シリーズ サービス統合型ルータ • Cisco Catalyst 8500 シリーズ エッジプラットフォーム

第 207 章

FlexVPN サーバーの設定

このモジュールでは、FlexVPN サーバーの機能、FlexVPN サーバーの設定に必要な IKEv2 コマンド、リモート アクセス クライアント、およびサポートされる RADIUS 属性について説明します。

（注） セキュリティに対する脅威は、そのような脅威からの保護に役立つ暗号化技術と同様に、絶え間なく変化しています。シスコの暗号化に関する最新の推奨事項の詳細は、『Next Generation Encryption』（NGE）ホワイトペーパーを参照してください。

FlexVPN サーバーの制限事項

デュアルスタック トンネル インターフェイスおよび VRF 認識 IPsec

VPN ルーティングおよび転送（VRF）認識 IPsec シナリオでデュアルスタック トンネル インターフェイスを設定する場合、**ip vrf forwarding** コマンドを使用して内部 VPN ルーティングおよび転送（IVRF）インスタンスを設定することはできません。これは有効な設定ではないためです。トンネル インターフェイスの IVRF を定義するには **vrf forwarding** *vrf-name* コマンドを使用します。ここで、*vrf-name* 引数は、定義内に IPv4 および IPv6 アドレス ファミリを指定した **vrf definition** コマンドを使用して定義されます。

SSO の制約事項

- ESP をリロードした場合（スタンバイ ESP なし）、SA シーケンス番号は 0 から再開されます。ピア ルータは、予期されたシーケンス番号を持たないパケットをドロップします。

単一の ESP を使用するシステムで ESP のリロード後にこの問題を回避するには、IPSec セッションを明示的に再確立することが必要になる場合があります。このような場合、リロード中に IPSec セッションでトラフィックの中断が発生することがあります。

FlexVPN サーバーに関する情報

EAP を使用するピア認証

FlexVPN サーバーは、Extensible Authentication Protocol（EAP：拡張可能認証プロトコル）を使用するピア認証をサポートし、クライアントとバックエンド EAP サーバー間で EAP メッセージを中継するパススルー オーセンティケータとして動作します。EAP バックエンド サーバーは、通常、EAP 認証をサポートする RADIUS サーバーです。

（注） FlexVPN クライアントは EAP を使用する FlexVPN クライアントを認証しますが、FlexVPN サーバーは証明書を使用して認証を受ける必要があります。

FlexVPN サーバーは、IKEv2 プロファイル設定モードの **authentication remote eap** コマンドによって、EAP を使用する FlexVPN クライアントを認証するよう設定されています。FlexVPN クライアントは、IKE_AUTH 要求内の AUTH ペイロードをスキップすることで、EAP を使用して認証します。

query-identity キーワードが設定されている場合、FlexVPN サーバーはクライアントからの EAP ID をクエリします。それ以外は、FlexVPN クライアントの IKEv2 ID が EAP ID として使用されます。ただし、**query-identity** キーワードが設定されておらず、FlexVPN クライアントの IKEv2 ID が IPv4 または IPv6 アドレスの場合、IP アドレスを EAP ID として使用できないため、セッションは終了します。

FlexVPN サーバーは、FlexVPN クライアントの EAP ID を EAP サーバーに渡すことで、EAP 認証を開始します。その後、FlexVPN サーバーは、認証が完了するまで、リモート アクセス（RA）クライアントと EAP サーバー間の EAP メッセージを中継します。認証が成功すると、EAP サーバーでは、EAP 成功メッセージ内で認証された EAP の ID が FlexVPN サーバーに返されることが予想されます。

EAP 認証の後、IKEv2 設定に使用された EAP ID は、次の送信元から任意の順で取得されます。

- EAP 成功メッセージで EAP サーバーから提供される EAP ID。
- **query-identity** キーワードの設定時にクライアントからクエリされる EAP ID。
- EAP ID として使用される FlexVPN クライアントの IKEv2 ID。

次の図は、**query-identity** キーワードなしの EAP 認証に対する IKEv2 交換を示します。

図 *105 : query-identity* キーワードなしの *IKEv2* 交換

IKEv2 RA client	IKEv2 RA server	RADIUS-EAP server
HDR, SAi1, KEi, Ni →		
	← HDR, SAr1, KEr, Nr, [CERTREQ]	
HDR, SK {IDi, [CERTREQ,] [IDr,] SAi2, TSi, TSr} →		
	RADIUS Access-Request/ EAP-Message/EAP-Response/(EAP-ID(IKEv2-ID)) →	
		← RADIUS Access-Challenge/EAP-Message/ EAP-Request/(EAP-method)
	← HDR, SK {IDr, [CERT,] AUTH, EAP(EAP-Request(EAP-method))}	
HDR, SK {EAP(EAP-Response(EAP-method)} →		
	RADIUS Access-Request/EAP-Message/EAP-Response/EAP-method) →	
		← RADIUS Access-Accept/EAP-Message/EAP-Success (other attributes))
	← HDR, SK {EAP (success)}	
HDR, SK {AUTH} →		
	← HDR, SK {AUTH, SAr2, TSi, TSr }	

209140

次の図は、**query-identity** キーワードありの EAP 認証に対する IKEv2 交換を示します。

図 *106 : query-identity* キーワードありの *IKEv2* 交換

IKEv2 RA client	IKEv2 RA server	RADIUS-EAP server
HDR, SAi1, KEi, Ni →		
	← HDR, SAr1, KEr, Nr, [CERTREQ]	
HDR, SK {IDi, [CERTREQ,] [IDr,] SAi2, TSi, TSr} →		
	← HDR, SK {IDr, [CERT,] AUTH, EAP (EAP-request (Identity)) }	
HDR, SK {EAP(EAP-Response(Identity)} →		
	RADIUS Access-Request/ EAP-Message/EAP-Response/(EAP-ID) →	
		← RADIUS Access-Challenge/EAP-Message/ EAP-Request/(EAP-method)
	← HDR, SK {IDr, [CERT,] AUTH, EAP(EAP-Request(EAP-method))}	
HDR, SK {EAP(EAP-Response(EAP-method)} →		
	RADIUS Access-Request/EAP-Message/EAP-Response/EAP-method) →	
		← RADIUS Access-Accept/EAP-Message/EAP-Success (EAP-identity) (other attributes))
	← HDR, SK {EAP (success)}	
HDR, SK {AUTH} →		
	← HDR, SK {AUTH, SAr2, TSi, TSr }	

209141

IKEv2 コンフィギュレーション モード

IKEv2 コンフィギュレーション モードで、IKE ピアは IP アドレスやルートなどの設定情報を交換できます。設定情報は、IKEv2 認証から取得されます。プル モデルとプッシュ モデルの両方がサポートされます。プル モデルには、設定要求と応答の交換が含まれます。プッシュ モデルには、設定セットと確認応答の交換が含まれます。

次の表に、発信側と応答側が異なる設定ペイロードタイプを送信するときの状況を示します。

表 *273 :* 設定ペイロード タイプ

設定ペイロード タイプ	送信元...	属性...
CFG_REQUEST	発信側	発信側がFlexVPNクライアントの場合。または、**config-exchange request** コマンドが IKEv2 プロファイルで有効になっている場合。
CFG_REPLY	応答側	応答側が CFG_REQUEST を受信する場合。
CFG_SET	発信側と応答側	発信側：**config-exchange set send** コマンドが IKEv2 プロファイルで有効になっている場合。 応答側：CFG_REQUEST が受信されておらず、設定データを使用可能で、**config-exchange set send** コマンドがIKEv2プロファイルで有効になっている場合。
CFG_ACK	発信側と応答側	発信側：**config-exchange set accept** コマンドがIKEv2プロファイルで有効になっている場合。 応答側：**config-exchange set accept** コマンドがIKEv2プロファイルで有効になっている場合。

（注） 設定要求と設定セットペイロードを送信するためのコマンドは、デフォルトで有効になっています。

ご使用のリリースに応じて、発信側がFlexVPNクライアントの場合にIKEv2発信側がコンフィギュレーション モードをトリガーしたり、IKEv2 プロファイルで **config-mode** コマンドを有効にすることによってIKEv2を発信するスタティック トンネルインターフェイスがコンフィギュレーション モードをトリガーすることができます。

IKEv2 FlexVPN サーバーは、次の標準 IPv4 設定属性をサポートします。

- INTERNAL_IP4_ADDRESS
- INTERNAL_IP4_NETMASK
- INTERNAL_IP4_DNS
- INTERNAL_IP4_NBNS
- INTERNAL_IP4_SUBNET

IKEv2 FlexVPN サーバーは、次の標準 IPv6 設定属性をサポートします。

- INTERNAL_IP6_ADDRESS
- INTERNAL_IP6_DNS
- INTERNAL_IP6_SUBNET

（注） IPv6 設定属性は、Microsoft Windows IKEv2 クライアントによってのみサポートされます。

IKEv2 認証ポリシーで **route set** コマンドと **aaa attribute list** コマンドによって制御されている INTERNAL_IP4_SUBNET および INTERNAL_IP6_SUBNET 設定属性は、SVTI（スタティック仮想トンネルインターフェイス）-to-SVTI トンネルを設定する場合はサポートされません。このような場合、IKEv2 ベースのルート交換の代わりにスタティック ルーティングまたはダイナミック ルーティングを使用する必要があります。

IKEv2 FlexVPN サーバーは、次の標準共通設定属性をサポートします。

- APPLICATION_VERSION

（注） この属性は、Cisco AnyConnect および FlexVPN クライアントにのみ送信されます。

IKEv2 FlexVPN サーバーは、次の Cisco Unity 設定属性をサポートします。

- MODECFG_BANNER
- MODECFG_DEFDOMAIN
- MODECFG_SPLITDNS_NAME
- MODECFG_BACKUPSERVERS
- MODECFG_PFS
- MODECFG_SMARTCARD_REMOVAL_DISCONNECT

（注） Cisco Unity 属性は、Cisco AnyConnect および FlexVPN クライアントにのみ送信されます。

IKEv2 FlexVPN サーバーは、次の Cisco FlexVPN 設定属性をサポートします。

- MODECFG_CONFIG_URL
- MODECFG_CONFIG_VERSION

（注） Cisco FlexVPN 属性は、Cisco FlexVPN クライアントにのみ送信されます。

INTERNAL_IP4_ADDRESS 属性値は、指定された順序で次の送信元から取得されます。

- AAA ユーザー認証で受信した Framed-IP-Address 属性。
- ローカル IP アドレス プール。
- DHCP サーバー。

DHCP サーバー（設定されている場合）は、ローカル IP アドレス プールが設定されていない場合にのみアドレスを割り当てます。ただし、ローカル プールから IP アドレスを割り当てるとエラーが発生する場合、その次のアドレス送信元の DHCP サーバーはアドレスの割り当てに使用されません。

INTERNAL_IP4_NETMASK 属性の値は、次から取得されます。

- IP アドレスが DHCP サーバーから取得される場合、ネットマスクも DHCP サーバーから取得されます。
- IP アドレスが AAA ユーザー認証の Framed-IP-Address 属性またはローカル IP アドレス プールのいずれかから取得される場合、ネットマスクはユーザー認証またはグループ認証で受信した IPv4 ネットマスク属性から取得されます。ネットマスクが使用できない場合、INTERNAL_IP4_NETMASK 属性は設定応答に含まれません。ネットマスクが使用可能な場合、INTERNAL_IP4_ADDRESS 属性が設定応答に含まれるときにのみ、INTERNAL_IP4_NETMASK 属性は含まれます。

IPv4 アドレスは、クライアントがアドレスを要求する場合にのみ割り当てられ、応答に含まれます。クライアントが複数の IPv4 アドレスを要求した場合、応答で送信される IPv4 アドレスは 1 つのみです。可能な場合は、クライアントが要求しなくても残りの属性が応答に含まれます。クライアントが IPv4 アドレスを要求して、FlexVPN サーバーがアドレスを割り当てることができない場合、INTERNAL_ADDRESS_FAILURE メッセージがクライアントに返されます。

ipv6 local pool 設定では常に、プレフィックス長に 128 を使用することをお勧めします。

たとえば、クライアント数が 4 の場合は、プレフィックス長として **ipv6 local pool pool1 afe0::/126 128** を設定する必要があります。クライアント数が 16 の場合は、プレフィックス長として **ipv6 local pool pool1 afe0::/124 128** を設定する必要があります。

IKEv2 認証

IKEv2 認証は、AAA を使用して認証されるセッションに対するポリシーを提供します。このポリシーは、ローカルに定義するか RADIUS サーバーで定義できます。また、このポリシーにはローカルおよび/またはリモート属性が含まれています。認証用のユーザー名は、**name-mangler** キーワードを使用してピア ID から取得するか、コマンドで直接指定することができます。

IKEv2 認証は、ピアがコンフィギュレーション モードを介して IP アドレスを要求する場合にのみ必要です。

IKEv2 認証タイプは、次のとおりです。

- ユーザー認証：ユーザー認証を有効にするには、IKEv2 プロファイルで **aaa authorization user** コマンドを使用します。ユーザー認証は、fqdn-hostname などのピア IKE ID のユーザー固有の部分に基づいています。ユーザー認証の属性は、ユーザー属性と呼ばれます。
- グループ認証：グループ認証を有効にするには、IKEv2 プロファイルで **aaa authorization group** コマンドを使用します。グループ認証は、fqdn-domain などのピア IKE ID の汎用部分に基づいています。グループ認証の属性は、グループ属性と呼ばれます。
- 暗黙的ユーザー認証：暗黙的ユーザー認証を有効にするには、IKEv2 プロファイルで **aaa authorization user cached** コマンドを使用します。暗黙的認証は、EAP 認証の一部として実行されるか、AAA 事前共有キーの取得時に実行されます。暗黙的ユーザー認証の属性は、キャッシュ属性と呼ばれます。

（注） ご使用のリリースに応じて、**aaa authorization user cached** コマンドが使用可能または使用不可能な場合があります。明示的ユーザー認証は、暗黙的ユーザー認証が属性を返さない場合または Framed-IP-Address 属性を持たない場合にのみ実行されます。

属性のマージおよびオーバーライド

異なる送信元からの属性は、使用前にマージされます。マージ属性の優先順位は、次のとおりです。

- 重複する属性をマージする場合、属性の送信元の優先順位が高くなります。
- ユーザー属性およびキャッシュ属性をマージする場合、ユーザー属性の優先順位が高くなります。
- マージ済みのユーザー属性およびグループ属性をマージする場合、デフォルトではマージ済みのユーザー属性の優先順位が高くなります。ただし、この優先順位は **aaa author group override** コマンドを使用して逆にすることができます。

IKEv2 認証ポリシー

IKEv2認証ポリシーでは、ローカル認証ポリシーが定義され、ローカルおよび/またはリモート属性が含まれています。VPN ルーティングおよび転送（VRF）や QOS ポリシーなどのローカル属性は、ローカルに適用されます。ルートなどのリモート属性は、コンフィギュレーションモードでピアにプッシュされます。ローカル ポリシーを定義するには、**crypto ikev2 authorization policy** コマンドを使用します。IKEv2 認証ポリシーは、**aaa authorization** コマンドによって IKEv2 プロファイルから示されます。

IKEv2 名前分割

IKEv2 名前分割は、IKEv2 認証用のユーザー名の取得およびピア IKE ID からの AAA 事前共有キーの取得に使用されます。

IKEv2 マルチ SA

IKEv2 マルチ SA 機能によって、IKEv2 応答側の IKEv2 ダイナミック仮想トンネル インターフェイス（DVTI）セッションは複数の IPsec セキュリティ アソシエーション（SA）をサポートできます。DVTI セッションあたりの IPSec SA の最大数は、AAA 認証から取得されるか IPsec プロファイルで設定されます。AAA からの値が優先されます。IPsec プロファイルでの *max-flow-limit* 引数への変更は現在のセッションには適用されませんが、後続のセッションに適用されます。IKEv2 マルチ SA 機能では、IPsec プロファイルでの IKEv2 プロファイルの設定は任意です。この任意設定によって、同じ仮想テンプレートを使用する IPsec DVTI セッションで異なる IKEv2 プロファイルを使用できるようになり、仮想テンプレート設定の数が削減されます。

（注） IKEv2 マルチ SA 機能では、非 any-any プロキシを持つ複数の IPsec SA が許可されます。ただし、IPSec SA プロキシが any-any の場合は 1 つの IPsec SA が許可されます。

詳細については、『*Security for VPNs with IPsec Configuration Guide*』の『Multi-SA Support for Dynamic Virtual Tunnel Interfaces for IKEv2』モジュールを参照してください。

AnyConnect プロファイルのダウンロード

FlexVPN AnyConnect プロファイルのダウンロード機能を使用すると、Cisco IOS XE ソフトウェアを実行しているデバイスが、Cisco AnyConnect セキュア モビリティ クライアントに IKEv2 プロトコルで接続してプロファイル情報をプッシュできます。

Cisco AnyConnect セキュア モビリティ クライアントには、VPN の設定に使用されるプロファイルが含まれています。このプロファイルは、手動で設定することも、ヘッドエンドからダウンロードすることもできます。ヘッドエンドは、Cisco AnyConnect セキュア モビリティ クライアントのすべてのユーザーにプロファイルをグローバルに展開するように設定できます。

VPN プロファイルを IKEv2 プロファイルと照合するには、**anyconnect profile** コマンドを使用します。

（注） AnyConnect プロファイルのダウンロード機能を設定する際、crypto ssl profile は必須ではありません。

サポートされる RADIUS 属性

次のテーブルに、IKEv2 FlexVPN サーバーがサポートする RADIUS 属性を示します。

- [Scope] フィールドは、属性の方向と、FlexVPN サーバーまたはクライアントでの使用方法を定義します。
  - [Inbound]：FlexVPN サーバーから RADIUS
  - [Outbound]：RADIUS から FlexVPN サーバー
  - [Local]：FlexVPN サーバーによってローカルで使用される
  - [Remote]：FlexVPN サーバーによってクライアントにプッシュされる
- [Local configuration] フィールドは、FlexVPN サーバーでローカルに属性を設定するために使用される、IKEv2 認証ポリシー コマンドを指定します。
- Cisco AV ペアは、vendor-id が 9、vendor-type が 1 の Cisco ベンダー固有属性（VSA）です。VSA は、RADIUS IETF 属性 26 のベンダー固有でカプセル化されます。Cisco AV ペアは、文字列形式「protocol:attribute=value」で指定されます。

例：

```
cisco-avpair = “ipsec:ipv6-addr-pool=v6-pool”
```

次に、標準アクセス リストの Cisco AV ペアの例を示します。

```
cisco-avpair = "ipsec:route-set=access-list 99"
```

表 *274*：着信および双方向の *IETF RADIUS* 属性

属性	スコープ
User-Name	着信と発信（双方向）
User-Password	着信
Calling-Station-Id	着信
Service-Type	着信
EAP-Message	双方向
Message-Authenticator	双方向

表 *275*：発信 *IETF* および *Cisco AV* ペアの *RADIUS* 属性

属性	タイプ	スコープ	ローカル設定
Tunnel-Type	IETF	Local	該当なし
Tunnel-Medium-Type	IETF	Local	該当なし

属性	タイプ	スコープ	ローカル設定
Tunnel-Password	IETF	Local	該当なし
ipsec:ikev2-password-local	Cisco AV ペア	Local	該当なし
ipsec:ikev2-password-remote	Cisco AV ペア	Local	該当なし
ipsec:addr-pool	Cisco AV ペア	Local	pool
ipsec:group-dhcp-server	Cisco AV ペア	Local	dhcp server
ipsec:dhcp-giaddr	Cisco AV ペア	Local	dhcp giaddr
ipsec:dhcp-timeout	Cisco AV ペア	Local	dhcp timeout
ipsec:ipv6-addr-pool	Cisco AV ペア	Local	ipv6 pool
ipsec:route-set=interface	Cisco AV ペア	Local	route set interface
ipsec:route-set=prefix	Cisco AV ペア	Local	該当なし
ipsec:route-accept	Cisco AV ペア	Local	route accept any
ip:interface-config	Cisco AV ペア	Local	aaa attribute list
ipsec:ipsec-flow-limit	Cisco AV ペア	Local	ipsec flow-limit
Framed-IP-Address	IETF	Remote	該当なし
Framed-IP-Netmask	IETF	Remote	netmask
ipsec:dns-servers	Cisco AV ペア	Remote	DNS
ipsec:wins-servers	Cisco AV ペア	Remote	wins
ipsec:route-set=access-list （注 1 を参照）	Cisco AV ペア	Remote	route set access-list （注 1 を参照）
ipsec:addrv6	Cisco AV ペア	Remote	n/a
ipsec:prefix-len	Cisco AV ペア	Remote	n/a
ipsec:ipv6-dns-servers-addr	Cisco AV ペア	Remote	ipv6 dns
ipsec:route-set=access-list ipv6	Cisco AV ペア	Remote	route set access-list ipv6
ipsec:banner	Cisco AV ペア	Remote	banner
ipsec:default-domain	Cisco AV ペア	Remote	def-domain
ipsec:split-dns	Cisco AV ペア	Remote	split-dns

属性	タイプ	スコープ	ローカル設定
ipsec:ipsec-backup-gateway	Cisco AV ペア	Remote	backup-gateway
ipsec:pfs	Cisco AV ペア	Remote	pfs
ipsec:include-local-lan	Cisco AV ペア	Remote	include-local-lan
ipsec:smartcard-removal-disconnect	Cisco AV ペア	Remote	smartcard-removal- disconnect
ipsec:configuration-url	Cisco AV ペア	Remote	configuration url
ipsec:configuration-version	Cisco AV ペア	Remote	configuration version

（注）
- 1. IKEv2 FlexVPN サーバーでアクセス リストを設定するための RADIUS 属性は、標準アクセス リストのみをサポートします。拡張アクセス リストはサポートされていません。

サポートされるリモート アクセス クライアント

FlexVPN サーバーは、Microsoft 7 IKEv2 クライアント、Cisco IKEv2 AnyConnect クライアント、および Cisco FlexVPN クライアントと相互運用されます。

Microsoft Windows 7 IKEv2 クライアント

Microsoft Windows 7 IKEv2 クライアントは、インターネット キー エクスチェンジ（IKE）ID として IP アドレスを送信します。この ID は、Cisco IKEv2 FlexVPN サーバーが IKE ID に基づいてリモート ユーザーを分類するのを防ぎます。Windows 7 IKEv2 クライアントが電子メール アドレス（user@domain）を IKE ID として送信できるようにするには、KB975488（http://support.microsoft.com/kb/975488）に記載されたホットフィックスを Windows 7 に適用し、電子メールアドレスの文字列を、プロンプトが表示された場合は [Username] フィールドまたは証明書の [CommonName] フィールドに、認証方式に応じて指定します。

証明書ベースの認証の場合は、次のように、FlexVPN サーバーと Microsoft Windows 7 クライアントの証明書に拡張キー使用法（EKU）フィールドが含まれている必要があります。

- クライアント証明書では、EKU フィールド = クライアント認証証明書です。
- サーバー証明書では、EKU フィールド = サーバー認証証明書です。
- 証明書は、Microsoft の証明書サーバーまたは IOS CA サーバーから取得できます。

EAP 認証の場合は、Microsoft Windows 7 IKEv2 クライアントが他の EAP 要求の前に EAP ID 要求を待ちます。クライアントに EAP ID 要求を送信するには、IKEv2 FlexVPN サーバー上の IKEv2 プロファイル内で **query-identity** キーワードが設定されていることを確認してください。

Cisco IKEv2 AnyConnect クライアント

証明書ベースの認証では、次のように FlexVPN サーバーと AnyConnect クライアントの証明書に拡張キー使用法（EKU）フィールドが含まれている必要があります。

- クライアント証明書では、EKU フィールド = クライアント認証証明書です。
- サーバー証明書では、EKU フィールド = サーバー認証証明書です。

FlexVPN サーバーが証明書を使用して AnyConnect クライアントを認証する場合、サーバーの IP アドレスまたは完全修飾ドメイン名（FQDN）を含む FlexVPN サーバーの証明書に SubjectAltName の拡張子が必要です。また、**no crypto ikev2 http-url cert** コマンドを使用して、HTTP 認証 URL を FlexVPN サーバーで無効にしておく必要があります。

次の例では、AnyConnect クライアント プロファイルの IKEv2 セッションの EAP-MD5 認証に固有の XML タグを示します。

```
<PrimaryProtocol>IPsec
       <StandardAuthenticationOnly>true
           <AuthMethodDuringIKENegotiation>
               EAP-MD5
           </AuthMethodDuringIKENegotiation>
           <IKEIdentity>DEPT24</IKEIdentity>
       </StandardAuthenticationOnly>
</PrimaryProtocol>
```

（注） 有効になっているすべてのフラップまたは FlexVPN トンネルについて、次のメッセージが表示されます。

```
*Jan 22 22:52:09.833: %SYS-5-CONFIG_P: Configured programmatically by process Crypto INT
 from console as console
*Jan 22 22:52:09.840: %LINEPROTO-5-UPDOWN: Line protocol on Interface Virtual-Access2,
changed state to up
```

詳細については、次のリンクで AnyConnect クライアント 3.0 のドキュメントを参照してください。
http://www.cisco.com/en/US/docs/security/vpn_client/anyconnect/anyconnect30/release/notes/anyconnect30rn.html#wp1268255

FlexVPN サーバーの設定方法

FlexVPN サーバーの IKEv2 プロファイルの設定

このタスクでは、基本的な IKEv2 プロファイル コマンドに加えて、FlexVPN サーバーの設定に必要な IKEv2 プロファイル コマンドについて説明します。基本的な IKEv2 プロファイルの設定方法については、『*Configuring Internet Key Exchange Version 2 (IKEv2)*』機能モジュールの「Configuring IKEv2 Profile (Basic)」タスクを参照してください。

このタスクは、FlexVPN サーバーの IKEv2 プロファイルを設定するために実行します。

ステップ 1 **enable**

例：

特権 EXEC モードを有効にします。

```
Device> enable
```

プロンプトが表示されたらパスワードを入力します。

ステップ 2 **configure terminal**

例：

グローバル コンフィギュレーション モードを開始します。

```
Device# configure terminal
```

ステップ 3 **crypto ikev2 profile** *profile-name*

IKEv2 プロファイル名を定義し、IKEv2 プロファイル コンフィギュレーション モードを開始します。

例：

```
Device(config)# crypto ikev2 profile profile1
```

ステップ 4 **aaa authentication eap** *list-name*

例：

```
Device(config-ikev2-profile)# aaa authentication eap list1
```

（任意）IKEv2 リモートアクセスサーバーの実装中に EAP 認証用の AAA 認証リストを指定します。

- **eap**：外部 EAP サーバーを指定します。
- *list-name*：AAA 認証リスト名。

ステップ 5 **authentication** {**local** {**rsa-sig** | **pre-share** [**key** {**0** | **6**} *password*}] | **ecdsa-sig** | **eap** [**gtc** | **md5** | **ms-chapv2**] [**username** *username*] [**password** {**0** | **6**} *password*}]} | **remote** {**eap** [**query-identity** | **timeout** *seconds*] | **rsa-sig** | **pre-share** [**key** {**0** | **6**} *password*}] | **ecdsa-sig**}}

例：

```
Device(config-ikev2-profile)# authentication local ecdsa-sig
```

ローカルまたはリモートの認証方式を指定します。

- **rsa-sig**：認証方式として RSA-sig を指定します。
- **pre-share**：認証方式として事前共有キーを指定します。
- **ecdsa-sig**：認証方式として ECDSA-sig を指定します。
- **eap**：リモート認証方式として EAP を指定します。
- **query-identity**：ピアに EAP ID を問い合わせます。
- **timeout** *seconds*：最初の IKE_AUTH 応答を返してから次の IKE_AUTH 要求を受け取るまでの期間を秒単位で指定します。

（注）　ローカル認証方式は 1 つしか指定できませんが、リモート認証方式は複数指定できます。

ステップ 6 次のいずれかまたは両方を実行します。

- **aaa authorization user** {**eap** | **psk**} {**cached** | **list** *aaa-listname* [*aaa-username* | **name-mangler** *mangler-name*]}
- **aaa authorization user cert list** *aaa-listname* {*aaa-username* | **name-mangler** *mangler-name*}

例：

```
Device(config-ikev2-profile)# aaa authorization user eap cached
```

例：

```
Device(config-ikev2-profile)# aaa authorization user cert list list1 name-mangler mangler1
```

ユーザー認可用の AAA 方式リストとユーザー名を指定します。

- **user**：ユーザー認可を指定します。
- **cert**：ピアは証明書を使用して認証を受ける必要があることを指定します。
- **eap**：ピアは EAP を使用して認証を受ける必要があることを指定します。
- **psk**：ピアは事前共有キーを使用して認証を受ける必要があることを指定します。
- **cached**：EAP 認証中に受信した属性または AAA 事前共有キーから取得した属性をキャッシュする必要があることを指定します。
- *aaa-listname*：AAA 方式リスト名。
- *aaa-username*：AAA 認可要求で使用する必要があるユーザー名を指定します。
- **name-mangler**：ピア ID から AAA 認可ユーザー名を抽出する name mangler を指定します。
- *mangler-name*：使用する name mangler。

（注）
- **psk** 認証方式と **eap** 認証方式では、*aaa-username* 引数または **name-mangler** キーワードの指定は任意で、指定しなかった場合は、ピア ID がユーザー名として使用されます。
- **psk** 認証方式と **eap** 認証方式では、それぞれ、**cached** キーワードと **list** キーワードを使用して 2 つのユーザー認可用のバリアントを同時に設定できます。
- **cert** 認証ではタイプが識別名（DN）のピア ID を使用できないため、*aaa-username* 引数または **name-mangler** キーワードの指定が必須です。

ステップ 7 次のいずれかまたは両方を実行します。

- **aaa authorization group** [**override**] {**eap** | **psk**} **list** *aaa-listname* [*aaa-username* | **name-mangler** *mangler-name*]
- **aaa authorization group** [**override**] **cert list** *aaa-listname* {*aaa-username* | **name-mangler** *mangler-name*}

例：

```
Device(config-ikev2-profile)# aaa authorization group override psk list list1
```

例：

```
Device(config-ikev2-profile)# aaa authorization group cert list list1 name-mangler mangler1
```

グループ認可用の AAA 方式リストとユーザー名を指定します。

- **group**：グループ認可を指定します。
- **override**：（任意）属性のマージ中はグループ認可からの属性を優先する必要があることを指定します。デフォルトでは、ユーザー属性が優先されます。
- **cert**：ピアは証明書を使用して認証を受ける必要があることを指定します。
- **eap**：ピアは EAP を使用して認証を受ける必要があることを指定します。
- **psk**：ピアは事前共有キーを使用して認証を受ける必要があることを指定します。
- *aaa-listname*：AAA 方式リスト名。
- *aaa-username*：AAA 認可要求で使用する必要があるユーザー名。
- **name-mangler**：ピア ID から AAA 認可ユーザー名を抽出する name mangler を指定します。
- *mangler-name*：使用する name mangler。

（注）
- **psk** 認証方式と **eap** 認証方式では、*aaa-username* 引数または **name-mangler** キーワードの指定は任意で、指定しなかった場合は、ピア ID がユーザー名として使用されます。
- **psk** 認証方式と **eap** 認証方式では、それぞれ、**cached** キーワードと **list** キーワードを使用して 2 つのユーザー認可用のバリアントを同時に設定できます。
- **cert** 認証ではタイプが識別名（DN）のピア ID を使用できないため、*aaa-username* 引数または **name-mangler** キーワードの指定が必須です。

ステップ 8 **config-exchange** {**request** | **set** {**accept** | **send**}}

例：

```
Device(config-ikev2-profile)# config-exchange set accept
```

（任意）設定交換オプションを有効にします。

- **request**：設定交換要求を有効にします。
- **set**：設定交換要求セット オプションを有効にします。
- **accept**：設定交換要求セットを受け入れます。
- **send**：設定交換セットの送信を有効にします。

（注） デフォルトで、request オプションと set オプションが有効になります。

ステップ 9 **end**

例：

```
Device(config-ikev2-profile)# end
```

IKEv2 プロファイル コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

IKEv2 名前分割の設定

このタスクを実行して、IKEv2名前分割を指定します。これを使用して認証要求の名前を生成し、AAA 事前共有キーを取得します。この名前は、リモート IKE ID または EAP ID の異なる形式の指定した部分から派生します。ここで指定した名前分割は、IKEv2プロファイルに結び付けられます。

手順の概要

1. **enable**
2. **configure terminal**
3. **crypto ikev2 name-mangler** *mangler-name*
4. **dn** {**common-name** | **country** | **domain** | **locality** | **organization** | **organization-unit** | **state**}
5. **eap** {**all** | **dn** {**common-name** | **country** | **domain** | **locality** | **organization** | **organization-unit** | **state**} | **prefix** | **suffix** {**delimiter** {**.** | **@** | ****}}}
6. **email** {**all** | **domain** | **username**}
7. **fqdn** {**all** | **domain** | **hostname**}
8. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**crypto ikev2 name-mangler** *mangler-name* 例： `Device(config)# crypto ikev2 name-mangler mangler1`	名前分割を定義し、IKEv2名前分割コンフィギュレーション モードを開始します。
ステップ 4	**dn** {**common-name** | **country** | **domain** | **locality** | **organization** | **organization-unit** | **state**} 例： `Device(config-ikev2-name-mangler)# dn state`	DN （識別名）タイプのリモートIDで、次のフィールドのいずれかから名前が派生します。 • **common-name** • **country** • **domain** • **locality** • **organization** • **organization-unit**

	コマンドまたはアクション	目的
		• **state**
ステップ 5	**eap** {**all** | **dn** {**common-name** | **country** | **domain** | **locality** | **organization** | **organization-unit** | **state**} | **prefix** | **suffix** {**delimiter** {**.** | **@** | \}}} 例： `Device(config-ikev2-name-mangler)# eap prefix delimiter @`	タイプが EAP（Extensible Authentication Protocol）のリモート ID から名前が派生します。 • **all**：EAP ID 全体から名前が派生します。 • **dn**：DN タイプのリモート EAP ID の次のフィールドのいずれかから名前が派生します。 • **common-name** • **country** • **domain** • **locality** • **organization** • **organization-unit** • **state** • **prefix**：EAP ID のプレフィックスから名前が派生します。 • **suffix**：EAP ID のサフィックスから名前が派生します。 • **delimiter** {**.** | **@** | \}：プレフィックスとサフィックスを分割する、EAP ID のデリミタを指定します。
ステップ 6	**email** {**all** | **domain** | **username**} 例： `Device(config-ikev2-name-mangler)# email username`	電子メール タイプのリモート ID から名前が派生します。 • **all**：電子メール タイプのリモート IKE ID 全体から名前が派生します。 • **domain**：リモート IKE ID のドメイン部分から名前が派生します。 • **username**：リモート IKE ID のユーザー名部分から名前が派生します。
ステップ 7	**fqdn** {**all** | **domain** | **hostname**} 例： `Device(config-ikev2-name-mangler)# fqdn domain`	タイプが FQDN（完全修飾ドメイン名）のリモート ID から名前が派生します。 • **all**：FQDN タイプのリモート IKE ID 全体から名前が派生します。 • **domain**：リモート IKE ID のドメイン部分から名前が派生します。

	コマンドまたはアクション	目的
		• **hostname**：リモート IKE ID のホスト名部分から名前が派生します。
ステップ 8	**end** 例： `Device(config-ikev2-name-mangler)# end`	IKEv2 名前分割コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

IKEv2 認証ポリシーの設定

このタスクを実行して、IKEv2 認証ポリシーを設定します。

手順の概要

1. **enable**
2. **configure terminal**
3. **crypto ikev2 authorization policy** *policy-name*
4. **aaa attribute list** *list-name*
5. **backup-gateway** *string*
6. **banner** *banner-text*
7. **configuration url** *url*
8. **configuration version** *version*
9. **def-domain** *domain-name*
10. **dhcp** { **giaddr** *ip-address* | **server** {*ip-address* | *hostname*} | **timeout** *seconds*}
11. [**ipv6**] **dns** *primary-server* [*secondary-server*]
12. **include-local-lan**
13. **ipsec flow-limit** *number*
14. **netmask** *mask*
15. **pfs**
16. [**ipv6**] **pool** *name*
17. **route set** { **interface** *interface* | **access-list** {*access-list-name* | *access-list-number* | **ipv6** *access-list-name*}}
18. **route accept any** [**tag** *value*] [**distance** *value*]
19. **route redistribute** *protocol* [**route-map** *map-name*]
20. **route set remote** { **ipv4** *ip-address mask* | **ipv6** *ip-address*/*mask*}
21. **smartcard-removal-disconnect**
22. **split-dns** *string*
23. **session-lifetime** *seconds*
24. **route set access-list** {*acl-number* | [**ipv6**] *acl-name*}
25. **wins** *primary-server* [*secondary-server*]
26. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**crypto ikev2 authorization policy** *policy-name* 例： `Device(config)# crypto ikev2 authorization policy policy1`	IKEv2 認証ポリシーを指定して、IKEv2 認証ポリシー設定モードを開始します。
ステップ 4	**aaa attribute list** *list-name* 例： `Device(config-ikev2-author-policy)# aaa attribute list list1`	AAA 属性のリストを指定します。 （注） このコマンドで参照されている AAA 属性リストは、グローバル コンフィギュレーション モードで定義する必要があります。
ステップ 5	**backup-gateway** *string* 例： `Device(config-ikev2-author-policy)# backup-gateway gateway1`	最大 10 台のバックアップ サーバー名を指定できます。このパラメータは、非標準 Cisco Unity コンフィギュレーション属性によってクライアントにプッシュされます。このパラメータは、クライアントが使用可能なバックアップ サーバーを指定します。
ステップ 6	**banner** *banner-text* 例： `Device(config-ikev2-author-policy)# banner This is IKEv2`	バナーを指定します。このパラメータは、非標準 Cisco Unity コンフィギュレーション属性によってクライアントに送信されます。
ステップ 7	**configuration url** *url* 例： `Device(config-ikev2-author-policy)# configuration url http://www.cisco.com`	コンフィギュレーション URL を指定します。このパラメータは、非標準 Cisco FlexVPN コンフィギュレーション属性によってクライアントに送信されます。クライアントはこの URL を使用して、コンフィギュレーションをダウンロードできます。
ステップ 8	**configuration version** *version* 例： `Device(config-ikev2-author-policy)# configuration version 2.4`	コンフィギュレーションバージョンを指定します。このパラメータは、非標準 Cisco FlexVPN コンフィギュレーション属性によってクライアントに送信されます。このパラメータは、コンフィギュレーション URL と送信され、クライアントがダウンロードできるバージョンを指定します。

	コマンドまたはアクション	目的
ステップ 9	**def-domain** *domain-name* 例： `Device(config-ikev2-author-policy)# def-domain cisco`	デフォルト ドメインを指定します。このパラメータは、非標準 Cisco Unity コンフィギュレーション属性によってクライアントに送信されます。このパラメータは、クライアントが使用可能なデフォルト ドメインを指定します。
ステップ 10	**dhcp** { **giaddr** *ip-address* | **server** {*ip-address* | *hostname*} | **timeout** *seconds*} 例： `Device(config-ikev2-author-policy)# dhcp giaddr 192.0.2.1`	リモート アクセス クライアントに割り当てられる IP アドレスをリースする DHCP サーバーを指定します。 • **giaddr** *ip-address*：ゲートウェイ IP アドレス（giaddr）を指定します。 • **server** {*ip-address* | *hostname*}：DHCP サーバーの IP アドレスまたはホスト名を指定します。ホスト名は、設定時に解決されます。 • **timeout** *seconds*：DHCP サーバーからの応答待ち時間を秒単位で指定します。 （注） 指定できる DHCP サーバーは 1 つのみです。DHCP サーバーはグローバル ルーティング テーブル経由で到達可能なことが前提であるため、DHCP パケットはグローバル ルーティング テーブルに転送されます。
ステップ 11	[**ipv6**] **dns** *primary-server* [*secondary-server*] 例： `Device(config-ikev2-author-policy)# dns 198.51.100.1 198.51.100.100`	設定応答でクライアントに送信される、プライマリおよびセカンダリ ドメイン名サービス（DNS）サーバーの IP アドレスを指定します。 • **ipv6**：（オプション）DNS サーバーの IPv6 アドレスを指定します。IPv4 アドレスを指定するには、このキーワードなしでコマンドを実行します。 • *primary-server*：プライマリ DNS サーバーの IP アドレス。 • *secondary-server*：（任意）セカンダリ DNS サーバーの IP アドレス。
ステップ 12	**include-local-lan** 例： `Device(config-ikev2-author-policy)# include-local-lan`	ローカル LAN を含めます。このパラメータは、非標準 Cisco Unity コンフィギュレーション属性によってクライアントに送信されます。

	コマンドまたはアクション	目的
ステップ 13	**ipsec flow-limit** *number* 例： `Device(config-ikev2-author-policy)# ipsec flow-limit 12500`	IKEv2 応答側の IKEv2 dVTI セッションが使用できる IPSec SAS の最大数を指定します。範囲は 0 ～ 50000 です。 デフォルトではコマンドは無効であり、dVTI セッションあたりの IPSec フローの数に制限はありません。値 0 では、IPSec SA は許可されません。
ステップ 14	**netmask** *mask* 例： `Device(config-ikev2-author-policy)# netmask 255.255.255.0`	クライアントに IP アドレスを割り当てるサブネットのネットマスクを指定します。 • *mask*：サブネット マスク アドレス。
ステップ 15	**pfs** 例： `Device(config-ikev2-author-policy)# pfs`	パスワード転送セキュリティ（PFS）を有効にします。このパラメータは、非標準 Cisco Unity コンフィギュレーション属性によってクライアントに送信されます。このパラメータは、クライアントで PFS を使用する必要性を指定します。
ステップ 16	[**ipv6**] **pool** *name* 例： `Device(config-ikev2-author-policy)# pool abc`	リモート アクセス クライアントに IP アドレスを割り当てるためのローカル IP アドレス プールを定義します。 • **ipv6**：（オプション）IPv6 アドレス プールを指定します。IPv4 アドレスを指定するには、このキーワードなしでコマンドを実行します。 • *name*：ローカル IP アドレス プールの名前。 （注） **ip local pool** コマンドを使用してすでに定義されているローカル IP アドレス プールを使用する必要があります。
ステップ 17	**route set** { **interface** *interface* | **access-list** {*access-list-name* | *access-list-number* | **ipv6** *access-list-name*}} 例： `Device(config-ikev2-author-policy)# route set interface`	コンフィギュレーションモードでピアに向かうルート設定パラメータを指定し、Border Gateway Protocol（BGP） over VPN などのルーティング プロトコルを実行できます。 • **interface**：ルート インターフェイスを指定します。 • **access-list**：ルート アクセス リストを指定します。 • *access-list-name*：アクセス リストの名前。 • *access-list-number*：標準のアクセス リスト番号。

	コマンドまたはアクション	目的
		• **ipv6**IPv6 アクセス リストを指定します。
ステップ 18	**route accept any** [**tag** *value*] [**distance** *value*] 例： `Device(config-ikev2-author-policy)# route accept any tag 10`	ピアから受信したルートをフィルタリングし、それらのルートをインストールするためにタグとメトリック値を指定します。 • **any**：ピアから受信したすべてのルートを受け入れます。 • **tag** *value*：（オプション）IKEv2 によって追加された静的ルートのタグ ID を指定します。範囲は 1 ～ 497777 です。 • **distance** *value*：（オプション）IKEv2 によって追加された静的ルートの距離を指定します。範囲は 1 ～ 255 です。
ステップ 19	**route redistribute** *protocol* [**route-map** *map-name*] 例： `Device(config-ikev2-author-policy)# route redistribute connected`	ピアから受信したルートをフィルタリングし、それらのルートをインストールするためにタグとメトリック値を指定します。 • *protocol*：ルートの再配布元のプロトコルです。connected または static のいずれかのキーワードを指定できます。 • **route-map** *map-name*：（オプション）ソース ルーティング プロトコルから別のルーティング プロトコルにルートをインポートするためにフィルタ処理する必要があるルートマップ。マップ名を指定しないと、すべてのルートが再配布されます。
ステップ 20	**route set remote** { **ipv4** *ip-address mask* | **ipv6** *ip-address/mask*} 例： `Device(config-ikev2-author-policy)# route set remote ipv6 2001:DB8::1/32`	内部ネットワークの IP アドレスを設定します。
ステップ 21	**smartcard-removal-disconnect** 例： `Device(config-ikev2-author-policy)# smartcard-removal-disconnect`	スマートカードの取り外しと切断を有効にします。このパラメータは、非標準 Cisco Unity コンフィギュレーション属性によってクライアントに送信されます。このパラメータでは、スマート カードが取り外された場合に、クライアントがセッションを停止する必要があることを指定します。

	コマンドまたはアクション	目的
ステップ 22	**split-dns** *string* 例： `Device(config-ikev2-author-policy)# split-dns abc1`	最大 10 台の分割ドメイン名を指定できます。このパラメータは、非標準Cisco Unityコンフィギュレーション属性によってクライアントに送信されます。このパラメータは、クライアントがプライベートネットワークに使用する必要があるドメイン名を指定します。
ステップ 23	**session-lifetime** *seconds* 例： `Device(config-ikev2-author-policy)# session-lifetime 1000`	IKEv2 セッションのライフタイムを指定します。 • **seconds** *seconds*：範囲は 120 ～ 25920000 で、2 分間～ 300 日間に変換されます。
ステップ 24	**route set access-list** {*acl-number* | [**ipv6**] *acl-name*} 例： `Device(config-ikev2-client-config-group)# route set access-list 110`	コンフィギュレーション モードを介してリモートピアにプッシュされるサブネットを指定します。 • *acl-number*：アクセス リスト番号（ACL）。ACL 番号は IPv4 ACL にのみ指定できます。 • **ipv6**：（オプション）IPv6アクセスコントロール リスト（ACL）を指定します。IPv4 属性を指定するには、このキーワードなしでコマンドを実行します。 • *acl-name*：アクセス リスト名。 （注） IPv4 アドレスに標準の、シンプルなアクセス リストのみを指定できます。
ステップ 25	**wins** *primary-server* [*secondary-server*] 例： `Device(config-ikev2-author-policy)# wins 203.0.113.1 203.0.113.115`	設定応答でクライアントに送信される、内部の Windows Internet Naming Service（WINS）サーバーアドレスを指定します。 • *primary-server*：プライマリ WINS サーバーの IP アドレス。 • *secondary-server*：（任意）セカンダリ WINS サーバーの IP アドレス。
ステップ 26	**end** 例： `Device(config-ikev2-author-policy)# end`	IKEv2 認証ポリシー設定モードを終了し、特権 EXEC モードに戻ります。

FlexVPN サーバーの構成例

例：FlexVPN サーバーの設定

例：EAP を使用してピアを認証するための FlexVPN サーバーの設定

この例では、EAPを使用してピアを認証するため、FlexVPNサーバーを設定する方法を示します。

```
aaa new-model
!
aaa group server radius eap-server
 server 192.168.2.1
!
aaa authentication login eap-list group eap-server
!
crypto pki trustpoint trustpoint1
 enrollment url http://192.168.3.1:80
 revocation-check crl
!
crypto ikev2 profile ikev2-profile1
 match identity remote address 0.0.0.0
 authentication local rsa-sig
 authentication remote eap query-identity
 pki trustpoint trustpoint1
 aaa authentication eap eap-list
 virtual-template 1
!
crypto ipsec transform-set transform1 esp-aes esp-sha-hmac
!
crypto ipsec profile ipsec-profile1
 set transform-set trans transform1
 set ikev2-profile ikev2-profile1
!
interface Ethernet0/0
 ip address 192.168.1.1 255.255.255.0
!
interface Virtual-Template1 type tunnel
 ip unnumbered Ethernet0/0
 tunnel mode ipsec ipv4
 tunnel protection ipsec profile ipsec-profile1
!
radius-server host 192.168.2.1 key key1
!
```

例：グループ認証のための FlexVPN サーバーの設定（外部 AAA）

次の例は、グループ認証用に FlexVPN サーバーを設定する方法を示します。認証は RADIUS または TACACS サーバーである外部 AAA を通じて行います。

```
aaa new-model
!
aaa group server radius cisco-acs
 server 192.168.2.2
```

```
!
aaa authorization network group-author-list group cisco-acs
!
crypto pki trustpoint trustpoint1
 enrollment url http://192.168.3.1:80
 revocation-check crl
!
crypto pki certificate map certmap1 1
 subject-name co cisco
!
crypto ikev2 name-mangler group-author-mangler
 dn domain
!
crypto ikev2 profile ikev2-profile1
 match certificate certmap1
 authentication local rsa-sig
 authentication remote rsa-sig
 pki trustpoint trustpoint1
 aaa authorization group cert list group-author-list name-mangler group-author-mangler
 virtual-template 1
!
crypto ipsec transform-set transform1 esp-aes esp-sha-hmac
!
crypto ipsec profile ipsec-profile1
 set transform-set trans transform1
 set ikev2-profile ikev2-profile1
!
interface Ethernet0/0
 ip address 192.168.1.1 255.255.255.0
!
interface Virtual-Template1 type tunnel
 ip unnumbered Ethernet0/0
 tunnel mode ipsec ipv4
 tunnel protection ipsec profile ipsec-profile1
!
radius-server host 192.168.2.2 key key2
!
```

例：グループ認証のための FlexVPN サーバーの設定（ローカル AAA）

次の例は、グループ認証用に FlexVPN サーバーを設定する方法を示します。認証は、IKEv2 認証ポリシーを使用するローカル AAA を通じて行います。認証ポリシーでは、コンフィギュレーション モードでクライアントに送信する、標準の IPv4 および IPv6 属性、Cisco Unity、FlexVPN 属性を指定します。また、認証ポリシーは、ローカル使用に対して、**aaa attribute list** コマンドによってユーザー属性ごとに指定します。

```
aaa new-model
!
aaa authorization network local-group-author-list local
!
!
aaa attribute list attr-list1
 attribute type interface-config "ip mtu 1100"
 attribute type interface-config "tunnel key 10"
!

crypto pki trustpoint trustpoint1
 enrollment url http://192.168.3.1:80
 revocation-check crl
!
crypto pki certificate map certmap1 1
```

```
 subject-name co cisco
!
crypto ikev2 authorization policy author-policy1
 pool pool1
 dhcp server 192.168.4.1
 dhcp timeout 10
 dhcp giaddr 192.168.1.1
 dns 10.1.1.1 10.1.1.2
 route set access-list acl1
 wins 192.168.1.2 192.168.1.3
 netmask 255.0.0.0
 banner ^C flexvpn server ^C
 configuration url http://www.abc.com
 configuration version 10
 def-domain abc.com
 split-dns dns1
 split-dns dns2
 split-dns dns3
 backup-gateway gw1
 backup-gateway gw2
 backup-gateway gw3
 smartcard-removal-disconnect
 include-local-lan
 pfs
 aaa attribute list attr-list1
!
crypto ikev2 profile ikev2-profile1
 match certificate certmap1
 authentication local rsa-sig
 authentication remote rsa-sig
 pki trustpoint trustpoint1
 aaa authorization group cert list local-group-author-list author-policy1
 virtual-template 1
!
crypto ipsec transform-set transform1 esp-aes esp-sha-hmac
!
crypto ipsec profile ipsec-profile1
 set transform-set trans transform1
 set ikev2-profile ikev2-profile1
!
interface Ethernet0/0
 ip address 192.168.1.1 255.255.255.0
!
interface Virtual-Template1 type tunnel
 ip unnumbered Ethernet0/0
 tunnel mode ipsec ipv4
 tunnel protection ipsec profile ipsec-profile1
!
ip local pool pool11 192.168.2.10 192.168.2.100
!
ip access-list extended acl-1
 permit ip 192.168.3.10 192.168.4.100 any
 permit ip 192.168.10.1 192.168.10.100 any
!
```

例：ユーザー認証のための FlexVPN サーバーの設定

次の例は、ユーザー認証用に FlexVPN サーバーを設定する方法を示します。

```
aaa new-model
!
aaa group server radius cisco-acs
```

```
 server 192.168.2.2
!
aaa authorization network user-author-list group cisco-acs
!
crypto pki trustpoint trustpoint1
 enrollment url http:// 192.168.3.1:80
 revocation-check crl
!
crypto pki certificate map certmap1 1
 subject-name co cisco
!
crypto ikev2 name-mangler user-author-mangler
 dn common-name
!
crypto ikev2 profile ikev2-profile1
 match certificate certmap1
 authentication local rsa-sig
 authentication remote rsa-sig
 pki trustpoint trustpoint1
 aaa authorization user cert list user-author-list name-mangler user-author-mangler
 virtual-template 1
!
crypto ipsec transform-set transform1 esp-aes esp-sha-hmac
!
crypto ipsec profile ipsec-profile1
 set transform-set trans transform1
 set ikev2-profile ikev2-profile1
!
interface Ethernet0/0
 ip address 192.168.1.1 255.255.255.0
!
interface Virtual-Template1 type tunnel
 ip unnumbered Ethernet0/0
 tunnel mode ipsec ipv4
 tunnel protection ipsec profile ipsec-profile1
!
radius-server host 192.168.2.2 key key2
!
```

例：IPv6 設定属性による IPv6 セッション用の FlexVPN サーバーの設定

次の例に、IPv6 ダイナミック仮想トンネルインターフェイス（dVTI）セッション用に FlexVPN サーバーを設定する方法を示します。この例では、IKEv2 認証ポリシーを使用するローカル AAA グループ認証を使用します。IPv6 設定属性は、IKEv2 認証ポリシーの下で設定されます。

```
aaa new-model
!
aaa authorization network local-group-author-list local
!
crypto pki trustpoint trustpoint1
 enrollment url http://192.168.3.1:80
 revocation-check crl
!
crypto pki certificate map certmap1 1
 subject-name co cisco
!
crypto ikev2 authorization policy author-policy1
 ipv6 pool v6-pool
 ipv6 dns 2001:DB8:1::11 2001:DB8:1::12
 ipv6 subnet-acl v6-acl
!
crypto ikev2 profile ikev2-profile1
```

```
 match certificate certmap1
 authentication local rsa-sig
 authentication remote rsa-sig
 pki trustpoint trustpoint1
 aaa authorization group cert list local-group-author-list author-policy1
 virtual-template 1
!
crypto ipsec transform-set transform1 esp-aes esp-sha-hmac
!
crypto ipsec profile ipsec-profile1
 set transform-set trans transform1
 set ikev2-profile ikev2-profile1
!
interface Ethernet0/0
 ipv6 address 2001:DB8:1::1/32
!
interface Virtual-Template1 type tunnel
 ipv6 unnumbered Ethernet0/0
 tunnel mode ipsec ipv6
 tunnel protection ipsec profile ipsec-profile1
!
ipv6 local pool v6-pool 2001:DB8:1::10/32 48
!
ipv6 access-list v6-acl
 permit ipv6 host 2001:DB8:1::20 any
 permit ipv6 host 2001:DB8:1::30 any
!
```

例：AnyConnect プロファイルのダウンロードの設定

次の例は、FlexVPN AnyConnectプロファイルのダウンロード機能を設定する方法を示します。

（注） AnyConnect クライアント マシン上のローカル ポリシー ファイルは変更しません。IKEv2 で AnyConnectプロファイルのダウンロード機能を設定すると、必要なXMLプロファイルがクライアント デバイスに自動的にダウンロードされます。

（注） プロファイルダウンロード機能に対して、HTTPS サーバー（ip http secure-server）または SSL ポリシー（crypto ssl policy）のいずれかを無効にする必要があります。これらの機能の両方が同時に有効になっている場合に、デバイスが着信 SSL VPN 接続を受信すると、デバイスがクラッシュする可能性があります。

```
no ip http secure-server
crypto ssl policy ssl-policy
  pki trustpoint CA1 sign
  ip address local 10.0.0.1 port 443
  no shutdown
crypto ssl profile ssl_prof
    match policy ssl-policy
crypto vpn anyconnect profile ANY-PROF bootflash:profile.xml
crypto ikev2 profile ikev2_profile
    anyconnect profile ANY-PROF
```

FlexVPN サーバーの設定に関する追加情報

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『Cisco IOS Master Command List, All Releases』
セキュリティ コマンド	• 『Cisco IOS Security Command Reference Commands A to C』 • 『Cisco IOS Security Command Reference Commands D to L』 • 『Cisco IOS Security Command Reference Commands M to R』 • 『Cisco IOS Security Command Reference Commands S to Z』
Cisco AnyConnect Secure Mobility Client	https://www.cisco.com/c/en/us/support/security/anyconnect-secure-mobility-client/tsd-products-support-series-home.html
IPsec の設定	『*Configuring Security for VPNs with IPsec*』
推奨される暗号化アルゴリズム	『Next Generation Encryption』

シスコのテクニカル サポート

説明	リンク
右の URL にアクセスして、シスコのテクニカル サポートを最大限に活用してください。これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

FlexVPN サーバーの設定の機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだ

けを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *276 : FlexVPN* サーバーの設定の機能情報

機能名	リリース	機能情報
リモート アクセス クライアントの IKEv2 ヘッドエンド サポート	Cisco IOS XE Release 3.5S	この機能は、Anyconnect 3.0、FlexVPN ハードウェア クライアント、および VTI のマルチ SA サポートに対する IKEv2 をサポートします。 次のコマンドが導入または変更されました。 **aaa attribute list, backup-gateway, banner, config-mode set, configuration url, configuration version, def-domain, dhcp, dns, include-local-lan, max flow limit, pfs, pool, route accept, route set interface, smartcard-removal-disconnect, split-dns, subnet-acl.**

第 208 章

FlexVPN クライアントの設定

このモジュールでは、FlexVPN クライアント機能と FlexVPN クライアントの設定に必要なインターネット キー エクスチェンジ バージョン 2（IKEv2）コマンドについて説明します。

（注） セキュリティに対する脅威は、脅威からの保護に役立つ暗号化技術と同様に絶え間なく変化しています。シスコの暗号化に関する最新の推奨事項の詳細は、『Next Generation Encryption』（NGE）ホワイトペーパーを参照してください。

FlexVPN クライアントの制限事項

ローカル認証方式としての EAP

- ローカル認証方式としての Extensible Authentication Protocol（EAP：拡張可能認証プロトコル）は、IKEv2 発信側でのみサポートされます。リモート認証としては、IKEv2 応答側でのみサポートされます。
- EAP がローカル認証方式として指定されている場合、リモート認証方式は証明書ベースである必要があります。
- FlexVPN サーバーで **authentication remote eap query-identity** コマンドが設定されていないと、IP アドレスを EAP 認証方式のユーザー名として使用することはできないため、クライアントはローカル ID として IPv4 アドレスまたは IPv6 アドレスを持つことはできません。

デュアルスタック トンネル インターフェイスおよび VRF 認識 IPsec

VPN ルーティングおよび転送（VRF）認識 IPsec シナリオでデュアルスタック トンネル インターフェイスを設定する場合、**ip vrf forwarding** コマンドを使用して内部 VPN ルーティングおよび転送（IVRF）インスタンスを設定することはできません。これは有効な設定ではないためです。トンネル インターフェイスの IVRF を定義するには **vrf forwarding** *vrf-name* コマンドを使用します。ここで、*vrf-name* 引数は、定義内に IPv4 および IPv6 アドレス ファミリを指定した **vrf definition** コマンドを使用して定義されます。

SSO の制約事項

- ESP をリロードした場合（スタンバイ ESP なし）、SA シーケンス番号は 0 から再開されます。ピアルータは、予期されたシーケンス番号を持たないパケットをドロップします。単一の ESP を使用するシステムで ESP のリロード後にこの問題を回避するには、IPSec セッションを明示的に再確立することが必要になる場合があります。このような場合、リロード中に IPSec セッションでトラフィックの中断が発生することがあります。

FlexVPN クライアントに関する情報

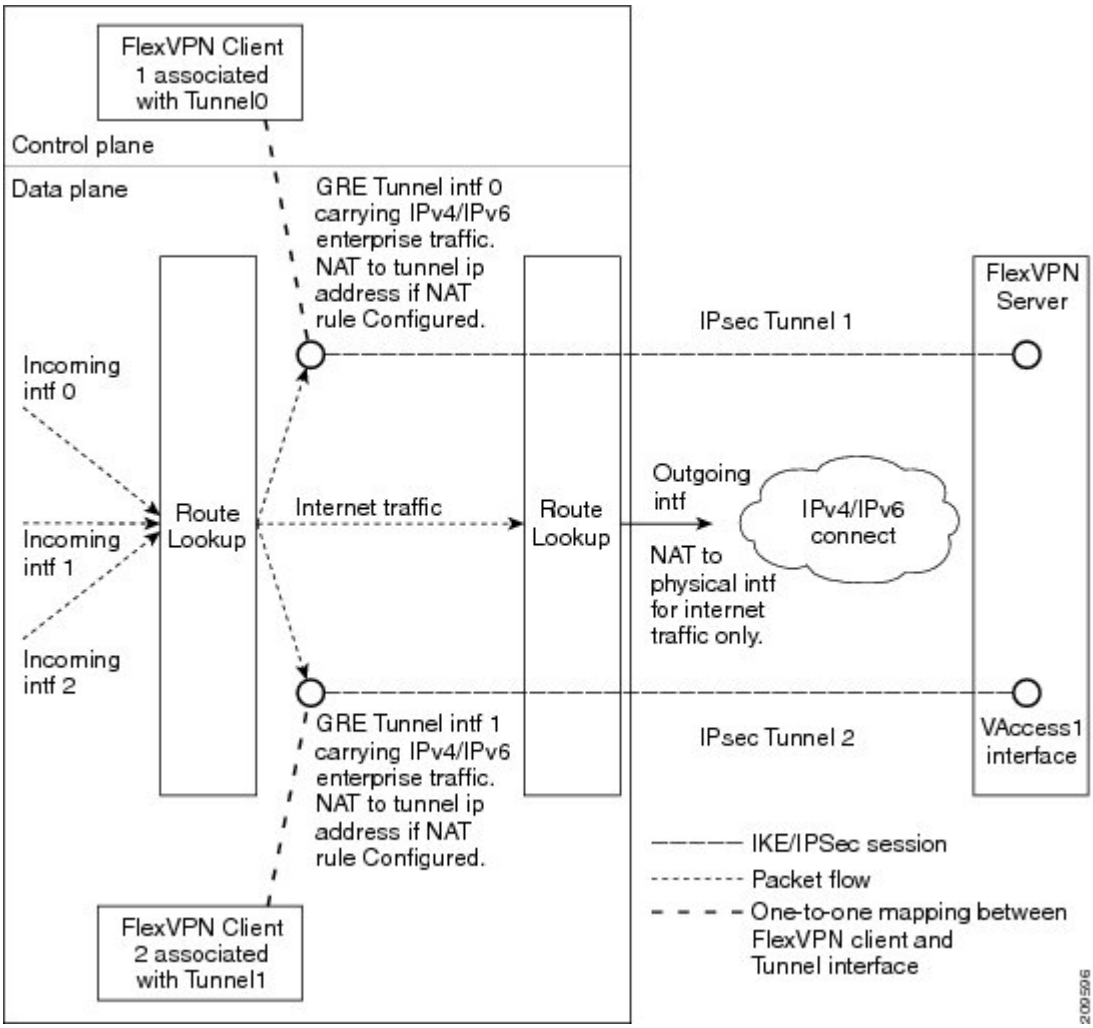
IKEv2 FlexVPN クライアント

IKEv2 FlexVPN クライアント機能は、FlexVPN クライアントと FlexVPN サーバーの間にセキュアな IPsec VPN トンネルを確立します。IKEv2 FlexVPN クライアント機能の利点は、次のとおりです。

- トンネル インフラストラクチャの統合
- IPv4/IPv6 トランスポートを介した IPv4/IPv6 プロキシ サポート
- EasyVPN によってサポートされるいくつかの機能との下位互換性
- ダイナミック ルーティング プロトコルを実行するための柔軟性

各 FlexVPN クライアントは、一意のトンネルインターフェイスに関連付けられます。これは、特定の FlexVPN クライアントによって取得された IPsec セキュリティ アソシエーション（SA）がトンネル インターフェイスにバインドされていることを示します。次の図に、FlexVPN クライアントとトンネル インターフェイスとの間の関連付けを示します。

図 *107 : FlexVPN* クライアントとトンネル インターフェイスの関連付け



動作のシーケンスは、次のとおりです。

- ルーティング：FlexVPN サーバーは、モード設定応答の一部としてネットワーク リストをプッシュします。クライアントは、これらのネットワークにトンネルインターフェイスのルートを追加します。コンフィギュレーションモード設定の一部として、クライアントはネットワークにルートを送信します。サーバーがクライアント側ネットワークにルートを追加できるように、IP アドレスがトンネル インターフェイスに設定されます。
- NAT：ネットワーク アドレス変換（NAT）ルールは、ルート マップを使用して明示的に設定する必要があります。ルールが一致すると、FlexVPN クライアントの背後にあるホストはトンネルの IP アドレスに変換されます。この IP アドレスは、FlexVPN サーバーによるモード設定時にプッシュされる属性の 1 つとして取得できます。
- カプセル化および暗号化：Generic Routing Encapsulation（GRE）および IPSec カプセル化モードがサポートされます。GRE は、IPv4 と IPv6 の両方のトラフィックをサポートします。トンネル インターフェイスに到達するトラフィックは、GRE ヘッダーでカプセル化

され、その後に IPSec 保護が実行されます。その後、暗号化されたトラフィックは発信インターフェイスにルーティングされます。

FlexVPN クライアントによってサポートされる機能について、次の項で説明します。

トンネル有効化

FlexVPN クライアントは、自動的にまたはユーザー操作によって手動で接続できます。FlexVPN 設定が完了すると、FlexVPN クライアントは、自動的にトンネルに接続します。トンネルでタイムアウトまたは障害が発生した場合、トンネルは自動的に再接続し、接続を無制限に再試行します。自動トンネル接続を設定するには、IKEv2 FlexVPN プロファイルで **connect** コマンドに **auto** キーワードを使用します。

手動接続では、FlexVPN クライアントは、接続を確立する前にコマンドを実行するユーザーの操作を待ちます。クライアントがタイムアウトするか、接続に失敗すると、後続の接続ではユーザーの操作が必要になります。手動接続を設定するには、特権 EXEC モードで、**crypto ikev2 client flexvpn connect** コマンドに *flexvpn-name* 引数を使用します。接続を終了するには、**clear crypto ikev2 client flexvpn connect** コマンドに *flexvpn-name* 引数を使用します。

追跡ベースのトンネル有効化

追跡ベースのトンネル有効化機能は、主にバックアップ シナリオで使用されます。FlexVPN クライアントは、オブジェクトの状態変更に関する通知を取得するため、追跡システムに登録されます。この通知はクライアントに、トンネル有効化のための適切なアクションを実行するよう要求します。**connect** コマンドの **track** キーワードによって、クライアントがオブジェクト番号で特定されるオブジェクトの追跡に関心があることを示す、追跡プロセスを通知します。次に、追跡プロセスはクライアントに、オブジェクトの状態がいつ変更されたかを通知します。

connect コマンドの **track** キーワードでトンネル有効化が設定されている場合、オブジェクトが起動すると、オブジェクトがアップ状態にあることを示す通知を受信したクライアントは、接続をトリガーします。**connect** コマンドの **track** キーワードでトンネル有効化が設定されている場合、オブジェクトが停止すると、オブジェクトがダウン状態にあることを示す通知を受信したクライアントは、接続をトリガーします。

バックアップ機能

FlexVPN クライアントは、事前に決定された順序で複数のピアまたはサーバーに接続できます。ピアのリストはゲートウェイ リストまたはバックアップ ゲートウェイ リストと呼ばれ、次のリストを使用して作成されます。

- スタティック バックアップ ゲートウェイ リストまたはスタティック リスト
- ダウンロード バックアップ ゲートウェイ リストまたはダウンロード リスト

スタティック バックアップ ゲートウェイ リストは、シーケンス番号の付いたピアのリストを提供することによって FlexVPN プロファイルで設定されます。ダウンロード バックアップ ゲートウェイ リストは、動的にダウンロードされ、モード設定の応答時に取得されます。ダウンロード リストは、スタティック ゲートウェイ リストを補完してバックアップ ゲートウェイ

リストを作成します。ダウンロードリストは、リストがダウンロードされるピアの後に挿入されます。

ゲートウェイ リストのピアとの既存の接続がダウンすると、クライアントはゲートウェイ リストにある次のピアとの接続を確立しようとします。ダウンロード リストが使用可能でスタティック ピアとの接続に失敗すると、クライアントはダウンロード リストのピアと順番に接続しようとします。クライアントがダウンロードリストのすべてのピアとの接続の確立に失敗すると、クライアントはスタティック リストにある次のピアに接続を試みて、ダウンロードリストは削除されます。

バックアップ ゲートウェイ

バックアップ ゲートウェイ リストにピアを追加するには、**peer** コマンドを使用します。バックアップ ゲートウェイ リストを削除するには、**no peer** コマンドを使用します。

ピアは、優先順に並べられています。シーケンス番号が小さいほど、優先順位が高くなります。

新しいピアとの接続が確立され、そのピアがダウンロードリストに含まれていない場合、ピアはバックアップ ゲートウェイ リストにダウンロード リストを追加し、既存のバックアップ ゲートウェイ リストが新しいリストに置き換えられます。

スタティック ピアを設定して、トラック オブジェクトにアタッチすることができます。ピアのトラック オブジェクトがアップ状態の場合、ピアは「可能なピア」になります。

（注） ダウンロード リストのピアを含め、トラック オブジェクトにアタッチされていないピアは、これらのピアが常にアップ状態であるため「可能なピア」に分類されます。

ピアの選択プロセスは、次のように機能します。接続が確立されると、ゲートウェイ リストが検索され、最初の可能なピアが選択されます。ピアは次のルールに従って選択されます。スタティック ピアは、希望するステータス（アップまたはダウン）のトラック オブジェクトに関連付けることができます。トラック オブジェクトのステータスが設定されたステータスと一致すると、ピアは「可能なピア」と呼ばれます。

（注） ピアがドメイン ネーム サービス（DNS）の名前または完全修飾ドメイン名（FQDN）のいずれかによって識別される場合、名前は動的に解決されます。

ピアの選択プロセスの後に、新しいピアが選択されます。また、既存の条件が満たされない場合は、次のシナリオが発生します。

- アクティブなピアが、活性チェックに応答しなくなります。
- ピア名の DNS 解決が失敗します。
- ピアとの IKE ネゴシエーションが失敗します。
- ピアが「可能なピア」でなくなります（対応するトラック オブジェクトがダウンします）。

（注） 複数の FlexVPN ピアを FlexVPN クライアントで設定したり、プライマリ ピアで IKEv2 SA をクリアすると、そのクリアによってクライアントでの新しいピアの選択がトリガーされます。

プライマリ ピアの再アクティブ化

プライマリ ピアの再アクティブ化機能は、最高優先度のピアが常に接続されるようにします。最高優先度のピアのトラック オブジェクトがオブジェクト ステータスと一致する場合、優先度が低いピアがある既存の接続が切断され、最高優先度のピアへの接続が確立されます。この機能を有効にするには、**peer reactivate** コマンドを使用します。

（注） トラック オブジェクトは、静的に設定されたピアに関連付ける必要があります。

ダイヤル バックアップ（プライマリまたはバックアップ トンネル）

オブジェクトの状態の変化ついて通知を受けるように、FlexVPN クライアントを追跡システムに登録します。クライアントがオブジェクトを追跡したい追跡プロセス（オブジェクト番号で識別）について通知するには、**connect track** コマンドを使用します。追跡プロセスでは、このオブジェクトの状態が変わったときにクライアントに順番に通知されます。追跡しているオブジェクトの状態がアップまたはダウンの場合、この通知によってクライアントは、プライマリまたはバックアップ接続を開始または停止するために対処するよう促されます。

ダイヤル バックアップ機能は、次のように設定できます。

- プライマリおよびバックアップ トンネルの両方が FlexVPN トンネルの場合：
  - アクティブなトンネルは、一度に 1 つのみです。
  - 両方のクライアント プロファイルは **connect track** コマンドを使用して設定され、同じトラック オブジェクトを参照します。
  - オブジェクトがアップしているときにプライマリ トンネルがステータスを追跡する場合、セカンダリ トンネルはオブジェクトがダウンしているときにオブジェクトのステータスを追跡します。
- 1 つのトンネルが FlexVPN トンネルの場合：
  - 残りのトンネルは、セキュアな接続上に存在します。
  - プライマリ接続は FlexVPN ではなく、バックアップ接続が FlexVPN です。
  - クライアント プロファイルは、オブジェクトを指定した **connect track** コマンドを使用して設定され、プライマリ発信インターフェイスを介してプライマリ ピアに到達する能力をトレースします。

バックアップ グループ

バックアップ グループ機能によって、FlexVPN クライアントは、グループに属する FlexVPN クライアントが同じピアとのセッションを確立しているときにピアを省略することができま

す。グループに属している FlexVPN クライアントがピアとの接続を開始すると、FlexVPN クライアントは同じグループ内の別の FlexVPN クライアントが同じピアとのセッションを確立しているかどうかを確認します。接続が存在する場合、FlexVPN クライアントはこのピアを省いて、順番に次のピアを確認します。バックアップ グループを設定するには、*group-number* 引数を指定して **backup group** コマンドを使用します。

デュアル FlexVPN のサポート

デュアル FlexVPN サポート機能によって、同じ内部および外部インターフェイスを共有する 2 つの FlexVPN トンネルを設定することができます。2 つの FlexVPN トンネルは、ルート インジェクションを使用し、対応するトンネルインターフェイスを介して適切なトラフィックを送信します。トンネルがアップしているとき、トンネルはサーバーからネットワーク リストを「学習」します。サーバーがネットワーク リストを転送すると、FlexVPN は特定のルートをそのルーティング テーブル内の宛先ネットワークにインストールし、トンネル インターフェイスからこれらのネットワークにトラフィックを送信します。

（注） トンネル インターフェイスを介してデフォルト ルートと確立できる FlexVPN 接続は、1 つのみです。

スプリット DNS のサポート

スプリット DNS 機能では、FlexVPN クライアントはドメイン ネーム システム（DNS）プロキシとして動作できます。FlexVPN ネゴシエーションの間、DNS リストはモード設定中にダウンロードされます。このリストは、FlexVPN プロファイルと関連付けられた内部インターフェイスで、DNS ビュー リストとして設定されます。ビュー リストは、ドメイン名に基づいて要求と DNS クエリを照合し、一致した要求を DNS サーバーに転送するために使用されます。他の DNS クエリは、デフォルト ビュー（グローバル DNS 設定）を照合するために使用され、ISP DNS に転送されます。

FlexVPN クライアント プロファイル内に 内部インターフェイスについての記載がない場合、DNS ビューはすべてのインターフェイスに適用されますが、設定されたすべてのプロファイルのトンネル インターフェイスとトンネル ソース インターフェイスを除きます。DNS クエリ要求が内部インターフェイスに受信されると、一致する DNS ビューが取得され、要求は DNS IP アドレスに転送されます。

NAT

FlexVPN のネットワーク アドレス変換（NAT）機能では、トラフィックがルーティングされるインターフェイスに基づいて、トラフィックを IP アドレスに変換できます。パケットが、**ip nat inside** コマンドで設定された 1 つのインターフェイスで受信され、**ip nat outside** コマンドで設定された別のインターフェイスに送信される場合、そのパケットは 2 番目のインターフェイスで設定された IP アドレスに変換されます。

サーバーのネットワーク リスト

企業トラフィックのルートは、トンネルインターフェイスを使用して、クライアントによってダイナミックインストールされます。このトラフィックは、発信する物理インターフェイス経由でデフォルトのルートをたどります。企業トラフィックはトンネルIPアドレスに変換され、インターネット トラフィックは外部の発信インターフェイス IP アドレスに変換されます。

サーバーからのデフォルト ルート リスト

デフォルト ルートは、トンネル インターフェイスを介してシーケンス番号がより高いデバイスで設定する必要があります。トンネル インターフェイスは **ip nat outside** コマンドで設定されます。また、トンネルインターフェイスのIPアドレスは、クライアントが送信したIPアドレスによって割り当てられます。内部インターフェイスからの企業トラフィックは、送信アドレスに変換されます。NAT は、ルート マップを使用して NAT ルールを設定することによって実現されます。ルートマップでは、発信インターフェイスに基づいてルールが定義されます。グローバルに設定された NAT ルールは、ルーティングに基づいて適用されます。

トンネル インターフェイスから送信された IPv4 トラフィックは、IPv4 送信アドレスに変換されます。

（注） NAT が不要な場合、トンネル インターフェイスに関連付けられた NAT ルールを設定する必要はありません。

FlexVPN クライアントのネットワーク リストの学習方法

FlexVPNクライアントは、次のいずれかの方法でピアの背後にあるネットワークのリストを学習します。

- モード設定プッシュ：FlexVPN サーバーは、ネットワーク属性のリストをコンフィギュレーション モードのパラメータとしてクライアントに送信します。FlexVPN クライアントは、メトリックが最も高いトンネルインターフェイスを介してこれらのネットワークにルートをインストールします。クライアントは、サーバーが仮想アクセスインターフェイスを介してそれらのルートを追加できるように、モード設定セットまたは確認応答（SET/ACK）の交換でサーバーにそのネットワークを伝達します。
- ルーティング プロトコルの実行：FlexVPN クライアントおよびサーバーはトンネル インターフェイスを介してルーティング プロトコルを実行し、ネットワーク ルートを確立します。これによって、クライアントおよびサーバーは、既存のセッションを切断せずに柔軟にネットワークを追加または削除できます。トンネルアドレスは、ピアとのルートを確立するためにモード設定時に伝達されます。

WINS NBNS およびドメイン名

モード設定中、FlexVPN サーバーはドメイン名、Windows Internet Naming Service（WINS）、またはNetBIOS ネーム サーバー（NBNS）属性をプッシュします。これらの属性は、FlexVPN クライアントで実行されている DHCP サーバーに、動的に更新されます。

イベント トレース

イベント トレース機能は、デバッグのために使用されます。FlexVPN クライアントに通知されたイベントは記録され、その情報はデバッグに使用されます。イベント トレースは、バッファ領域に数バイトのトレース情報を記録する高速メカニズムと、デバッグデータを抽出および復号する表示メカニズムを組み合わせたものです。FlexVPNクライアントは、バッファを保持して、通常の動作時に有効にすることができます。

ローカル認証方式としての Extensible Authentication Protocol

FlexVPN クライアントは、ローカル認証方式として EAP をサポートします。サポートされる EAP 認証方式は、Microsoft Challenge Handshake Authentication Protocol Version 2（MSCHAPv2）、メッセージ ダイジェスト アルゴリズム 5（MD5）、および Generic Token Card（GTC：汎用トークン カード）です。EAP 認証プロセスは、次のとおりです。

- EAP を使用して FlexVPN クライアントを認証するには、IKEv2 プロファイル コンフィギュレーション モードで **authentication local eap** コマンドを使用します。
- FlexVPN クライアントがピアから IKE_AUTH 応答を受信した後、**crypto eap credentials** コマンドを入力します。
- EAP ID 要求を IKE_AUTH 応答で受信した場合、EAP ユーザー名とパスワードを指定する必要があります。
- EAP ID 要求を IKE_AUTH 応答で受信していない場合、ローカル IKEv2 ID をユーザー名として使用するため、パスワードのみを指定します。

（注） ローカル認証方式としての EAP は FlexVPN クライアントと一緒に使用する必要がありますが、IKEv2 発信側では EAP を使用することもできます。EAP サーバーがサポートされていない認証方式を最初に指定すると、FlexVPN EAP 発信側は EAP 否定応答（NAK）パケットで応答し、希望の認証方式として EAP-MSCHAPv2、EAP-MD5、または EAP-GTC を要求します。FlexVPN EAP 応答側で、いずれかの認証方式を選択します。

FlexVPN クライアントの設定方法

IKEv2 VPN クライアント プロファイルの設定

このタスクでは、FlexVPN クライアントの設定に必要な IKEv2 コマンドと基本の IKEv2 コマンドについて説明します。基本の IKEv2 プロファイルの設定については、『*Configuring Internet Key Exchange Version 2 (IKEv2)*』モジュールの「Configuring Basic Internet Key Exchange Version 2 CLI Constructs」タスクを参照してください。

（注） IKEv2プロファイルの認証リストに入力ミスがある場合は、自動的にデフォルトのリストに戻ります。

FlexVPN サーバーの IKEv2 プロファイル設定については、「FlexVPN クライアントの設定方法」の項を参照してください。

トンネル インターフェイスの設定

このタスクを実行して、FlexVPN クライアントが参照するトンネル インターフェイスを設定します。

手順の概要

1. **enable**
2. **configure terminal**
3. **interface tunnel** *number*
4. **ip address** {*ipv4-address* | **negotiated**}
5. **tunnel mode gre ip**
6. **tunnel mode ipsec ipv4**
7. **tunnel source** {*ip-address* | *interface* | **dynamic**}
8. **tunnel destination dynamic**
9. **tunnel protection ipsec-profile** *profile-name*
10. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface tunnel** *number* 例： `Device(config)# interface tunnel 1`	トンネルインターフェイスを作成します。続いて、インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	**ip address** {*ipv4-address*	**negotiated**} 例： `Device(config-if)# ip address negotiated`	（オプション）IPv4 アドレスをトンネル インターフェイスに割り当てます。

	コマンドまたはアクション	目的
ステップ 5	**tunnel mode gre ip** 例： `Device(config-if)# tunnel mode gre ip`	（オプション）トンネル インターフェイスの Generic Route Encapsulation（GRE）モードを有効にします。
ステップ 6	**tunnel mode ipsec ipv4** 例： `Device(config-if)# tunnel mode ipsec ipv4`	（オプション）IPSec カプセル化を有効にします。
ステップ 7	**tunnel source** {*ip-address* | *interface* | **dynamic**} 例： `Device(config-if)# tunnel source 10.0.0.1`	トンネルインターフェイスの送信元を指定します。
ステップ 8	**tunnel destination dynamic** 例： `Device(config-if)# tunnel destination dynamic`	トンネル インターフェイスの宛先を指定します。
ステップ 9	**tunnel protection ipsec-profile** *profile-name* 例： `Device(config-if)# tunnel protection ipsec-profile ipsecprofile1`	トンネルインターフェイスを IPsec プロファイルに関連付けます。
ステップ 10	**end** 例： `Device(config-if)# end`	インターフェイス コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

FlexVPN クライアントの設定

monitor event-trace flexvpn コマンドを使用して、イベント トレースを有効にします。

手順の概要

1. **enable**
2. **configure terminal**
3. **crypto ikev2 client flexvpn** *client-name*
4. **peer** *sequence* {*ipv4-address* | *ipv6-address* | **fqdn** *fqdn-name* [**dynamic** | **ipv6**]} [**track** *track-number* [**up** | **down**]]
5. **connect** {**manual** | **auto** | **track** *track-number* [**up** | **down**]}
6. **client inside** *interface-type interface-number*
7. **client connect tunnel** *interface-number*
8. **source** *sequence-number interface-type interface-number* **track** *track-number*
9. **peer reactivate**
10. **backup group** {*group-number* | **default**}
11. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**crypto ikev2 client flexvpn** *client-name* 例： `Device(config)# crypto ikev2 client flexvpn client1`	IKEv2 FlexVPN クライアント プロファイルを定義し、IKEv2 FlexVPN クライアント プロファイル コンフィギュレーション モードを開始します。
ステップ 4	**peer** *sequence* {*ipv4-address* | *ipv6-address* | **fqdn** *fqdn-name* [**dynamic** | **ipv6**]} [**track** *track-number* [**up** | **down**]] 例： `Device(config-ikev2-flexvpn)# peer 1 10.0.0.1`	IP アドレスまたはホスト名を使用して、静的ピアを定義します。
ステップ 5	**connect** {**manual** | **auto** | **track** *track-number* [**up** | **down**]} 例： `Device(config-ikev2-flexvpn)# connect track 10 up`	FlexVPN トンネルを接続します。 （注） このコマンドに変更を加えると、アクティブなセッションが終了します。
ステップ 6	**client inside** *interface-type interface-number* 例： `Device(config-ikev2-flexvpn)# client inside GigabitEthernet 0/1`	（オプション）内部インターフェイスを指定します。 • FlexVPN クライアント プロファイルには、複数の内部インターフェイスを指定できます。内部インターフェイスは、FlexVPN クライアント プロファイル全体で共有できます。 （注） このコマンドに変更を加えると、アクティブなセッションが終了します。
ステップ 7	**client connect tunnel** *interface-number* 例： `Device(config-ikev2-flexvpn)# client connect tunnel 1`	「トンネル インターフェイスの設定」タスクで作成したトンネル インターフェイスを、FlexVPN クライアントに割り当てます。 • FlexVPN クライアント プロファイルに対して、設定できるトンネル インターフェイスは 1 つのみです。

	コマンドまたはアクション	目的
		（注） このコマンドに変更を加えると、アクティブなセッションが終了します。
ステップ 8	**source** *sequence-number interface-type interface-number* **track** *track-number* 例： `Device(config-ikev2-flexvpn)# source 1 GigabitEthernet 0/1 track 11`	トンネルの送信元アドレスにシーケンス番号を追加します。 • トンネルの送信元アドレスには、トラック オブジェクト番号がアップ状態の最小シーケンス番号があります。 （注） このコマンドに変更を加えると、アクティブなセッションが終了します。
ステップ 9	**peer reactivate** 例： `Device(config-ikev2-flexvpn)# peer reactivate`	プライマリ ピア機能の再アクティベートを有効にします。
ステップ 10	**backup group** {*group-number* | **default**} 例： `Device(config-ikev2-flexvpn)# backup group default`	バックアップ グループにクライアントを割り当てます。 • デフォルトでは、すべてのクライアントがバックアップ グループ 0 に属しています。 （注） このコマンドに変更を加えると、アクティブなセッションが終了します。
ステップ 11	**end** 例： `Device(config-ikev2-flexvpn)# end`	IKEv2 FlexVPN クライアント プロファイル コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

ローカル認証方式としての EAP の設定

このタスクを実行して、FlexVPN クライアントのローカル認証方式として Extensible Authentication Protocol（EAP：拡張可能認証プロトコル）を設定します。

手順の概要

1. **enable**
2. **configure terminal**
3. **crypto ikev2 profile** *profile-name*
4. **authentication local eap**
5. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**crypto ikev2 profile** *profile-name* 例： `Device(config)# crypto ikev2 profile profile1`	IKEv2 プロファイルを定義し、IKEv2 プロファイル コンフィギュレーション モードを開始します。
ステップ 4	**authentication local eap** 例： `Device(config-ikev2-profile)# authentication local eap`	ローカル認証方式として EAP を指定します。 （注） このコマンドは、IKEv2 の発信側でのみサポートされます。
ステップ 5	**end** 例： `Device(config-ikev2-profile)# end`	IKEv2 プロファイル コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

FlexVPN クライアントの構成例

例：IKEv2 FlexVPN クライアント プロファイルの設定

次の例は、IKEv2 FlexVPN クライアント プロファイルを設定する方法を示します。

```
crypto ikev2 client flexvpn flex
  peer 1 10.0.0.1
  connect manual
  client connect Tunnel0
!
crypto ikev2 authorization policy flex
 subnet-acl 199
 route set interface
 route accept any
!
crypto ikev2 keyring key
 peer dvti
  address 0.0.0.0 0.0.0.0
  pre-shared-key cisco
 !
crypto ikev2 profile prof
 match identity remote address 10.0.0.1 255.0.0.0
 authentication local pre-share
```

```
 authentication remote pre-share
 keyring key
 aaa authorization group psk list local-group-author-list flex
 config-mode set
!
crypto ipsec transform-set trans esp-aes
!
crypto ipsec profile ipsecprof
 set transform-set trans
 set pfs group2
 set ikev2-profile prof
!
interface Tunnel0
 ip address negotiated
 tunnel source Ethernet0/0
 tunnel destination dynamic
 tunnel mode ipsec ipv4
 tunnel protection ipsec-profile ipsecprof
!
interface Ethernet0/0
 ip address 172.16.0.1 255.240.0.0
 ip virtual-reassembly in
!
 ip route 0.0.0.0 0.0.0.0 2.2.2.2
access-list 199 permit ip 10.20.20.20 0.0.0.255 any
access-list 199 permit ip 10.30.30.30 0.0.0.255 any
```

例：ローカル認証方式としての EAP の設定

次の例は、EAP をローカル認証方式として設定する方法を示します。

```
crypto ikev2 profile profile1
 authentication remote rsa-sig
 authentication local eap
```

セッションが起動すると、次のように、EAP の認証情報を入力するプロンプトが表示されます。

```
Enter the command "crypto eap credentials profile1"
Device# crypto eap credentials profile1

Enter the Username for profile profile1: cisco
Enter the password for username cisco
```

FlexVPN クライアントの設定に関する追加情報

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『Cisco IOS Master Command List, All Releases』

関連項目	マニュアル タイトル
セキュリティ コマンド	• 『Cisco IOS Security Command Reference Commands A to C』 • 『Cisco IOS Security Command Reference Commands D to L』 • 『Cisco IOS Security Command Reference Commands M to R』 • 『Cisco IOS Security Command Reference Commands S to Z』
IPsec の設定	『*Configuring Security for VPNs with IPsec*』
推奨される暗号化アルゴリズム	『Next Generation Encryption』

シスコのテクニカル サポート

説明	リンク
右の URL にアクセスして、シスコのテクニカル サポートを最大限に活用してください。これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

FlexVPN クライアントの設定の機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *277 : FlexVPN* クライアントの設定の機能情報

機能名	リリース	機能情報
IKEv2 リモートアクセス ハードウェア クライアント		IKEv2 リモートアクセス ハードウェア クライアント機能は、モビリティ、NAT トラバーサル、およびサービス妨害（DoS）攻撃からの復元など、さまざまなソリューションのサポートに必要な、リモートアクセス接続と拡張機能をサポートします。 次のコマンドが導入または変更されました。 **backup group, client connect tunnel, client inside, connect, crypto ikev2 client flexvpn, interface, ip address, peer, peer reactivate, source tunnel destination, tunnel mode, tunnel protection, tunnel source.**
IPsec VPN の IPv6 リモート アクセス		IPsec VPN の IPv6 リモート アクセス機能は、IPv6 サポートと、IKEv2 FlexVPN クライアントのローカル認証方式としての EAP をサポートします。 次のコマンドが変更されました。 **authentication (IKEv2 profile), peer.**

第 209 章

FlexVPN スポークツースポークの設定

最新版発行日：2014 年 3 月 28 日

FlexVPN スポークツースポーク機能によって、FlexVPN クライアントは、仮想トンネル インターフェイス（VTI）、インターネット キー エクスチェンジ バージョン 2（IKEv2）、および Next Hop Resolution Protocol（NHRP）を活用して別の FlexVPN クライアントと直接の暗号トンネルを確立し、スポークツースポーク接続を構築することができます。

FlexVPN スポーク間の前提条件

IKEv2、FlexVPN サーバー、および FlexVPN スポークを設定する必要があります。

FlexVPN スポーク間に関する情報

FlexVPN および NHRP

FlexVPN は、シスコによる IKEv2 標準の実装であり、サイトツーサイト、リモートアクセス、ハブ アンド スポーク トポロジ、および部分メッシュ（スポークツースポーク ダイレクト）を組み合わせたユニファイド パラダイムと CLI を備えています。FlexVPN は、トンネル インターフェイス パラダイムを広範に使用し、かつ暗号マップを使用してレガシー VPN 実装との互換性を維持するシンプルなモジュラ フレームワークを提供します。

FlexVPN サーバーは、FlexVPN のサーバー側機能を提供します。FlexVPN クライアントは、FlexVPN クライアントと別の FlexVPN サーバーの間にセキュアな IPsec VPN トンネルを確立します。

NHRP は、Address Resolution Protocol（ARP）のようなプロトコルで、ノンブロードキャストマルチアクセス（NBMA）ネットワークの問題を軽減します。NHRP を使用すると、NBMA ネットワークに接続されている NHRP は、ネットワークの一部である他のエンティティの NBMA アドレスを動的に学習します。このため、これらのエンティティは、トラフィックに中間ホップを使用せずに直接通信できるようになります。

FlexVPN スポークツースポーク機能は、NHRP と FlexVPN クライアント（スポーク）を統合して、既存の FlexVPN ネットワークにある別のクライアントとの直接の暗号化チャネルを確立します。接続は、仮想トンネル インターフェイス（VTI）、IKEv2、および NHRP を使用して構築されます。ここで、NHRP はネットワーク内の FlexVPN クライアントの解決に使用されます。

FlexVPN では、次のことが推奨されます。

- ルーティング エントリは、スポーク間で交換されません。
- 異なるプロファイルがスポークに使用され、**config-exchange** コマンドはスポーク用に設定されません。

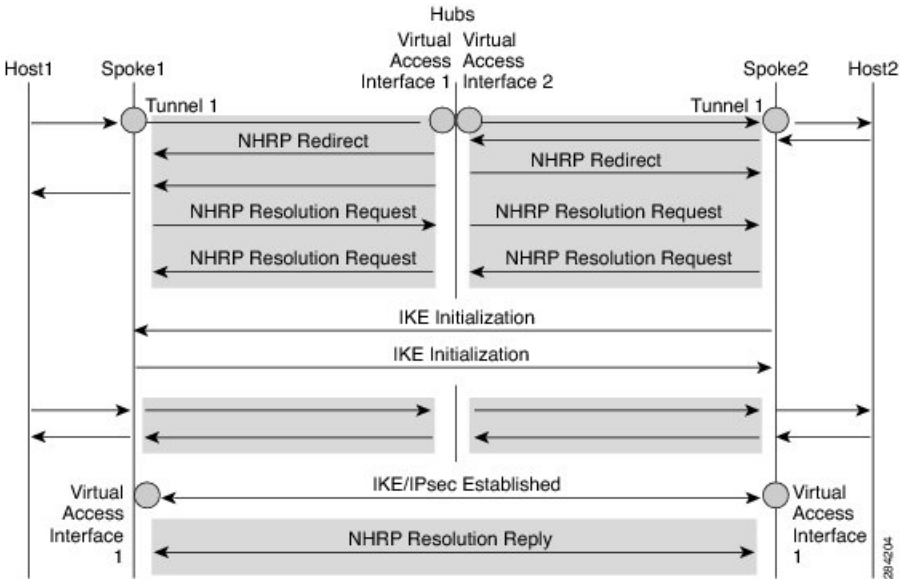
FlexVPN IPv6 ダイレクト スポーク間機能は、FlexVPN スポークに対する IPv6 アドレスの使用をサポートします。IPv6 アドレスのサポートにより、IPv6 over IPv4、IPv4 over IPv6、および IPv6 over IPv6 の転送がサポートされます。

（注） スポーク間 FlexVPN は、ダイナミック AAA 認証をサポートしていません。

NHRP 解決要求と FlexVPN の応答

次の図は、NHRP 解決要求と FlexVPN の応答を示します。

図 *108 : NHRP* 解決要求と応答



双方向のトラフィックにより、同様のイベントが、Spoke1、Spoke2、およびハブの両方向で発生します。明確にするために、Host1 から Host2 へのイベントについて説明します。Spoke1 と Spoke2 の背後にある別のネットワーク N2（192.168.2.0/24）の後に、ネットワーク N1（192.168.1.0/24）があると仮定します。2つのスポーク間のネットワークは、アクセス コントロール リスト（ACL）によって照合されます。これは、両方のスポークの IKEv2 ポリシーに ACL が適用されるためです。

両方のスポークからのプレフィックス情報と共に、ネットワークはIKEv2情報のペイロード交換によってハブに伝達されます。ハブの IKEv2 によるルーティング テーブルへのルート追加が、次のように発生します。

- 192.168.1.0/24：Virtual Access Interface1 から接続される
- 192.168.2.0/24：Virtual Access Interface2 から接続される

このハブは IKEv2 から両方のスポークへ集約ルートをプッシュし、スポークはそれらのルーティング テーブルにこのルートをインストールします。次のようになります。

- 192.168.0.0/16：ネクスト ホップ <ハブのトンネル アドレス> - Interface Tunnel 1

（注） また、ルーティング プロトコルは、ルーティング テーブルにルートを追加できます。

N1 から N2 へトラフィックが移動すると仮定すると、トラフィック フローは次のとおりです。

1. Host1 は、Host2 宛てのトラフィックを送信します。トラフィックは Spoke1 の LAN インターフェイスに到達し、ルートを検索し、集約ルートを見つけて、パケットを Interface Tunnel 1 にルーティングします。
2. トラフィックがハブの Virtual Access Interface1 に到達すると、トラフィックは、Virtual Access Interface2 から直接接続するか、ポイントツーポイントのトンネル インターフェイスを使用する、N2 のルート エントリ用のルート テーブルを検索します。
3. Host1 から Host2 へのトラフィックは、Virtual Access Interface1 と Virtual Access Interface2 を経由してハブを通過します。このハブは、入力インターフェイスおよび出力インターフェイス（Virtual Access Interface1 と Virtual Access Interface2）が同じ NHRP ネットワーク（両方のインターフェイスで設定されたネットワーク D）に属することを判断します。ハブは NHRP リダイレクト メッセージを Virtual Access Interface1 の Spoke1 に送信します。
4. リダイレクトを受信すると、Spoke1 は Host2 への解決要求をポイントツーポイント トンネル インターフェイス（リダイレクトを受信したのと同じインターフェイス）を経由して開始します。解決要求は、ルーティング パス（Spoke1-hub-spoke2）を通過します。解決要求を受信すると、Spoke2 は、それが出力点であり、その解決要求に応答する必要があることを判断します。
5. Spoke2 はトンネル インターフェイスの解決要求を受信し、トンネル インターフェイスから仮想テンプレート番号を取得します。仮想テンプレート番号を使用して、仮想アクセス インターフェイスを作成し、暗号チャネルを開始し、IKEv2 と IPSec のセキュリティ アソシエーション（SA）を確立します。2 つのスポーク間に暗号 SA が確立されると、Spoke2

は Spoke1 に必要な NHRP キャッシュ エントリとそのネットワークを、新しく作成した仮想アクセス インターフェイス以下に設置し、その仮想アクセス インターフェイスを介して解決の応答を送信します。

6. 仮想アクセス インターフェイスから解決要求を受信した後、Spoke1 は Spoke2 に必要なキャッシュ エントリとそのネットワークを設置します。また、Spoke1 は、ハブを示す一時キャッシュ エントリを削除し、Tunnel Interface1 以下のネットワークを解決します。
7. NHRP は、ネクスト ホップ上書き（NHO）または H ルートとしてショートカット ルートを追加します。ショートカット スイッチングの詳細については、「DMVPN ネットワークにおける NHRP のショートカット スイッチング拡張」を参照してください。

FlexVPN スポークツースポークの設定方法

FlexVPN サーバーの仮想トンネル インターフェイスの設定

始める前に

FlexVPN サーバーとクライアントを設定する必要があります。

手順の概要

1. **enable**
2. **configure terminal**
3. **interface virtual-template** *number* **type tunnel**
4. **ip unnumbered loopback** *number*
5. 次のいずれかを実行します。
   - **ip nhrp network-id** *number*
   - **ipv6 nhrp network-id** *number*
6. **ip nhrp redirect** [**timeout** *seconds*]
7. **exit**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 3	**interface virtual-template** *number* **type tunnel** 例： `Device(config)# interface virtual-template 1 type tunnel`	仮想アクセス インターフェイスの作成時にダイナミックに設定および適用される仮想テンプレートインターフェイスを作成します。
ステップ 4	**ip unnumbered loopback** *number* 例： `Device(config-if)# ip unnumbered loopback 0`	既存インターフェイス（通常はループバック インターフェイス）の IP アドレスを仮想トンネル インターフェイスに割り当てます。

ステップ 5	次のいずれかを実行します。
	• **ip nhrp network-id** *number*
	• **ipv6 nhrp network-id** *number*
	例：
	`Device(config-if)# ip nhrp network-id 1`
	例：
	`Device(config-if)# ipv6 nhrp network-id 1`
		インターフェイスで NHRP を有効にします。

ステップ 6	**ip nhrp redirect** [**timeout** *seconds*] 例： `Device(config-if)# ip nhrp redirect`	トラフィックが NHRP ネットワークで転送されている場合、リダイレクト トラフィック通知を有効にします。重複するリダイレクトを送信しないようにするには、**timeout** キーワードと *seconds* 引数を使用して、作成したリダイレクト エントリの有効期限を指定します。
ステップ 7	**exit** 例： `Device(config-if)# exit`	インターフェイス コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードに戻ります。

FlexVPN スポークの NHRP ショートカットの設定

このタスクを実行して、FlexVPN スポークのトンネル インターフェイスで NHRP ショートカットを設定します。

手順の概要

1. **enable**
2. **configure terminal**
3. **interface tunnel** *number*
4. 次のいずれかを実行します。
   - **ip nhrp shortcut** *virtual-template-number*
   - **ipv6 nhrp shortcut** *virtual-template-number*
5. **exit**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface tunnel** *number* 例： `Device(config)# interface tunnel 1`	FlexVPN クライアント インターフェイスを設定し、インターフェイス コンフィギュレーション モードを開始します。

ステップ 4	次のいずれかを実行します。
	• **ip nhrp shortcut** *virtual-template-number*
	• **ipv6 nhrp shortcut** *virtual-template-number*
	例：
	`Device(config-if)# ip nhrp shortcut 1`
	例：
	`Device(config-if)# ipv6 nhrp shortcut 1`
		FlexVPN クライアントのトンネル インターフェイスで NHRP ショートカットを有効にします。これは、スポーク間トンネルの確立に必要です。この設定で指定する仮想テンプレート番号と、「FlexVPN スポークの仮想トンネルインターフェイスの設定（3082 ページ）」タスクで指定する仮想テンプレート番号は同じにする必要があります。

ステップ 5	**exit** 例： `Device(config-if)# exit`	インターフェイス コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードに戻ります。

FlexVPN スポークの仮想トンネル インターフェイスの設定

手順の概要

1. **enable**
2. **configure terminal**
3. **interface virtual-template** *number* **type tunnel**
4. **ip unnumbered tunnel** *number*
5. 次のいずれかを実行します。
   - **ip nhrp network-id** *number*
   - **ipv6 nhrp network-id** *number*
6. 次のいずれかを実行します。
   - **ip nhrp shortcut** *virtual-template-number*
   - **ipv6 nhrp shortcut** *virtual-template-number*

7. **ip nhrp redirect** [**timeout** *seconds*]
8. **exit**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface virtual-template** *number* **type tunnel** 例： `Device(config)# interface virtual-template 1 type tunnel`	仮想アクセス インターフェイスの作成時にダイナミックに設定および適用される仮想テンプレート インターフェイスを作成します。
ステップ 4	**ip unnumbered tunnel** *number* 例： `Device(config-if)# ip unnumbered tunnel 1`	FlexVPN トンネル インターフェイスの IPv4 アドレスを仮想トンネル インターフェイスに割り当てます。

ステップ 5	次のいずれかを実行します。
	• **ip nhrp network-id** *number*
	• **ipv6 nhrp network-id** *number*
	例：
	`Device(config-if)# ip nhrp network-id 1`
	例：
	`Device(config-if)# ipv6 nhrp network-id 1`
		インターフェイスで NHRP を有効にします。

ステップ 6	次のいずれかを実行します。
	• **ip nhrp shortcut** *virtual-template-number*
	• **ipv6 nhrp shortcut** *virtual-template-number*
	例：
	`Device(config-if)# ip nhrp shortcut 1`
	例：
	`Device(config-if)# ipv6 nhrp shortcut 1`
		インターフェイスでNHRP ショートカット スイッチングを有効にします。
		（注） 現在の仮想テンプレート番号を指定する必要があります。仮想テンプレート番号は、FlexVPN クライアント トンネル インターフェイスの設定と同じにする必要があります。

ステップ 7	**ip nhrp redirect** [**timeout** *seconds*] 例： `Device(config-if)# ip nhrp redirect`	仮想トンネルインターフェイスでNHRP のリダイレクトを有効化します。ネットワークがあるスポークから別のスポークに移動する場合は、これが便利です。

	コマンドまたはアクション	目的
		• 重複するリダイレクトを送信しないようにするには、**timeout** キーワードと *seconds* 引数を使用して、作成したリダイレクトエントリの有効期限を指定します。
ステップ 8	**exit** 例： `Device(config-if)# exit`	インターフェイス コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードに戻ります。

FlexVPN スポーク設定の確認

FlexVPN スポークの設定を確認するには、次のコマンドを使用します。

手順の概要

1. **show crypto ikev2 client flexvpn**
2. **show ipv6 route**
3. **show ipv6 nhrp**

手順の詳細

ステップ 1 show crypto ikev2 client flexvpn

例：

```
Device# show crypto ikev2 client flexvpn

  Profile : flexblk
  Current state:ACTIVE
  Peer : 4001::2000:1
  Source : Ethernet0/0
  ivrf : IP DEFAULT
  fvrf : IP DEFAULT
  Backup group: None
  Tunnel interface : Tunnel0
```

FlexVPN サーバーおよびクライアント間の FlexVPN 接続ステータスが表示されます。

ステップ 2 show ipv6 route

例：

```
Device# show ipv6 route

IPv6 Routing Table - default - 15 entries
Codes: C - Connected, L - Local, S - Static, U - Per-user Static route
       B - BGP, HA - Home Agent, MR - Mobile Router, R - RIP
       H - NHRP, I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea
       IS - ISIS summary, D - EIGRP, EX - EIGRP external, NM - NEMO
       ND - ND Default, NDp - ND Prefix, DCE - Destination, NDr - Redirect
       l - LISP
```

```
       O - OSPF Intra, OI - OSPF Inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
       ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
C   3001::/112 [0/0]
     via Tunnel0, directly connected
S   3001::1/128 [2/0], tag 1
     via 3001::1, Virtual-Access1 [Shortcut]
     via Virtual-Access1, directly connected
L   3001::2/128 [0/0]
     via Tunnel0, receive
S   3001::3/128 [2/0], tag 1
     via Tunnel0, directly connected
C   4001::2000:0/112 [0/0]
     via Ethernet0/0, directly connected
L   4001::2000:3/128 [0/0]
     via Ethernet0/0, receive
S   5001::/64 [2/0], tag 1
     via Tunnel0, directly connected
C   5001::2000:0/112 [0/0]
     via Loopback0, directly connected
L   5001::2000:1/128 [0/0]
     via Loopback0, receive
D   5001::3000:0/112 [90/28288000]
     via FE80::A8BB:CCFF:FE01:F400, Tunnel0
D   5001::4000:0/112 [90/28288000]
     via FE80::A8BB:CCFF:FE01:F400, Tunnel0
H   5001::4000:1/128 [250/1]
     via 3001::1, Virtual-Access1
C   5001::5000:0/112 [0/0]
     via Loopback1, directly connected
L   5001::5000:1/128 [0/0]
     via Loopback1, receive
L   FF00::/8 [0/0]
     via Null0, receive
```

IPv6 ルートと Next Hop Resolution Protocol（NHRP）のマッピング情報が表示されます。

ステップ 3 show ipv6 nhrp

例：

```
Device# show ipv6 nhrp

3001::1/128 via 3001::1
   Virtual-Access1 created 00:01:52, expire 01:58:14
   Type: dynamic, Flags: router implicit rib nho
   NBMA address: 172.17.1.9
    (Claimed NBMA address: 172.16.2.1)
5001::4000:1/128 via 3001::1
   Virtual-Access1 created 00:00:56, expire 01:59:03
   Type: dynamic, Flags: router rib
   NBMA address: 172.17.1.9
    (Claimed NBMA address: 172.16.2.1)
5001::5000:1/128 via 3001::2
   Virtual-Access1 created 00:01:52, expire 01:58:14
   Type: dynamic, Flags: router unique local
   NBMA address: 172.17.2.10
```

例：

```
Device# show ipv6 nhrp

3001::1/128 via 3001::1
   Virtual-Access1 created 00:01:52, expire 01:58:14
   Type: dynamic, Flags: router implicit rib nho
```

```
   NBMA address: 4001::2000:2
5001::4000:1/128 via 3001::1
   Virtual-Access1 created 00:00:56, expire 01:59:03
   Type: dynamic, Flags: router rib
   NBMA address: 4001::2000:2
5001::5000:1/128 via 3001::2
   Virtual-Access1 created 00:01:52, expire 01:58:14
   Type: dynamic, Flags: router unique local
   NBMA address: 4001::2000:3
```

NHRP キャッシュ エントリが表示されます。最初の例では、出力に、転送が IPv4（NBMA アドレス）であることが示されます。リモート スポークは、要求された NBMA アドレス フィールドが示すとおり、ネットワーク アドレス変換（NAT）下にあります。このアドレスはリモート スポークの NAT 前アドレスです。また、キャッシュ エントリには、各スポークと関連付けられたフラグが表示され、ルーティング テーブルで各エントリに挿入されたルートの種類が示されます。ネクストホップ上書き（NHO）は、ショートカット ルートを示します。*rib* フラグは、そのキャッシュ エントリに追加された NHRP H ルートを示します。2 番目の例は、転送が IPv6（NBMA アドレス）であることを示します。要求されたアドレスが出力にないため、リモート スポークは NAT 下にはありません。

FlexVPN スポーク設定のトラブルシューティングのヒント

FlexVPN スポーク設定をトラブルシューティングするいくつかのヒントを示します。

1. スポーク間の接続を確認します。
2. クライアント（スポーク）とサーバーの設定を確認します。
3. スポークの背後にあるリモート ホストの到達可能性を確認します。
4. ルートをアドバタイズするために使用される、ルーティング プロトコル設定を確認します。
5. IKEv2 と IPSec が正しく設定されていることを確認します。
6. スポークの NHRP ショートカット設定と、サーバー（ハブ）のリダイレクト設定を確認します。

問題	トラブルシューティングのヒント
スポークからハブへの接続は作成されません。	ハブで作成された仮想アクセス インターフェイスがないことが原因で、接続が作成されない場合があります。 • ハブとスポークの間の接続を確認します。 • **show crypto session** コマンドを使用して、ハブとスポークのセキュリティ アソシエーション（SA）の状態を確認します。 • SA がアクティブ（**show crypto session** コマンドで表示される）の場合、スポークの FlexVPN の状態を、 **show crypto ikev2 client flexvpn** コマンドの出力で確認します。

問題	トラブルシューティングのヒント
スポーク間トンネルは作成されません。	

問題	トラブルシューティングのヒント
	トラフィックは、スポーク間トンネルを開始するため、ハブ経由でスポークからスポークに送られる必要があります。 • ハブの設定で、NHRP リダイレクトが有効かどうかを確認します。 • スポークの設定で、NHRP ショートカットが有効になっているかどうかを確認します。 • **show ip** [**ipv6**] **nhrp traffic** コマンドを使用して、FlexVPN サーバー（ハブ）の設定で、ハブがトラフィック間接参照をスポークに送信するかどうかを確認します。 • **show ip** [**ipv6**] **nhrp traffic** コマンドを使用して、スポークがトラフィックを受信して、解決要求を送信したことを確認します。 • **show ip** [**ipv6**] **nhrp** コマンドを使用して、いずれかのスポークにリモート ホストとスポークの NHRP キャッシュ エントリがあることを確認します。 • **show ip** [**ipv6**] **nhrp traffic** コマンドをリモート スポークで使用して、解決要求を受信したことを確認します。 • **show crypto ikev2 sa** コマンドと **show crypto session** コマンドを使用して、スポークが解決要求を受信し、暗号セッションを開始したことを確認します。 • **show ip** [**ipv6**] **interface brief** コマンドを使用して、仮想アクセス インターフェイスが両方のスポークにあることを確認します。 • **show ip** [**ipv6**] **nhrp traffic** コマンドをスポークで使用して、解決応答が送信され、仮想アクセス インターフェイスのピアによって受信されたことを確認します。 • **show ip** [**ipv6**] **nhrp** コマンドを使用して、リモート ホストのための完全な NHRP キャッシュ エントリがすべてのスポークに存在することを確認します。 • **show ip** [**ipv6**] **route** コマンドを使用して、Hルートやネクストホップ上書き（NHO）ルートがあることを確認します。

FlexVPN スポークツースポークの設定例

例：FlexVPN スポーク間のスタティック ルーティングの設定

次の例では、FlexVPN サーバーおよび FlexVPN クライアントで IKE 伝播されるスタティック ルーティングを使用して、FlexVPN スポーク間を設定する方法を示します。次は、FlexVPN サーバーの設定です。

```
hostname hub
!
crypto ikev2 authorization policy default
 pool flex-pool
 def-domain cisco.com
 route set interface
 route set access-list flex-route
!
crypto ikev2 profile default
 match identity remote fqdn domain cisco.com
 identity local fqdn hub.cisco.com
 authentication local rsa-sig
 authentication remote rsa-sig
 pki trustpoint CA
 aaa authorization group cert list default default
 virtual-template 1
!
crypto ipsec profile default
 set ikev2-profile default
!
interface Loopback0
 ip address 172.16.1.1 255.255.255.255
!
interface Ethernet0/0
 ip address 10.0.0.100 255.255.255.0
!
interface Virtual-Template1 type tunnel
 ip unnumbered Loopback0
 ip nhrp network-id 1
 ip nhrp redirect
 tunnel protection ipsec profile default
!
ip local pool flex-pool 172.16.0.1 172.16.0.254
!
ip access-list standard flex-route
 permit any
```

次は、最初の FlexVPN クライアントの設定です。

```
hostname spoke1
!
crypto ikev2 authorization policy default
 route set interface
 route set access-list flex-route
!
crypto ikev2 profile default
 match identity remote fqdn domain cisco.com
 identity local fqdn spoke1.cisco.com
 authentication local rsa-sig
```

```
 authentication remote rsa-sig
 pki trustpoint CA
 aaa authorization group cert list default default
 virtual-template 1
!
crypto ipsec profile default
 set ikev2-profile default
!
interface Tunnel0
 ip address negotiated
 ip nhrp network-id 1
 ip nhrp shortcut virtual-template 1
 ip nhrp redirect
 tunnel source Ethernet0/0
 tunnel destination 10.0.0.100
 tunnel protection ipsec profile default
!
interface Ethernet0/0
 ip address 10.0.0.110 255.255.255.0
!
interface Ethernet1/0
 ip address 192.168.110.1 255.255.255.0
!
interface Virtual-Template1 type tunnel
 ip unnumbered Tunnel0
 ip nhrp network-id 1
 ip nhrp shortcut virtual-template 1
 ip nhrp redirect
 tunnel protection ipsec profile default
!
ip access-list standard flex-route
 permit 192.168.110.0 0.0.0.255
```

次は、2 番目の FlexVPN クライアントの設定です。

```
hostname spoke2
!
crypto ikev2 authorization policy default
 route set interface
 route set access-list flex-route
!
crypto ikev2 profile default
 match identity remote fqdn domain cisco.com
 identity local fqdn spoke2.cisco.com
 authentication local rsa-sig
 authentication remote rsa-sig
 pki trustpoint CA
 aaa authorization group cert list default default
 virtual-template 1
!
crypto ipsec profile default
 set ikev2-profile default
!
interface Tunnel0
 ip address negotiated
 ip nhrp network-id 1
 ip nhrp shortcut virtual-template 1
 ip nhrp redirect
 tunnel source Ethernet0/0
 tunnel destination 10.0.0.100
 tunnel protection ipsec profile default
!
interface Ethernet0/0
 ip address 10.0.0.120 255.255.255.0
```

```
!
interface Ethernet1/0
 ip address 192.168.120.1 255.255.255.0
!
interface Virtual-Template1 type tunnel
 ip unnumbered Tunnel0
 ip nhrp network-id 1
 ip nhrp shortcut virtual-template 1
 ip nhrp redirect
 tunnel protection ipsec profile default
!
ip access-list standard flex-route
 permit 192.168.120.0 0.0.0.255
```

例：FlexVPN スポーク間の BGP を使用するダイナミック ルーティングの設定

次の例では、FlexVPN サーバーおよび FlexVPN クライアントで BGP を使用する（ダイナミック ネイバー探索により）ダイナミック ルーティングを、FlexVPN スポーク間で設定する方法を示します。次は、FlexVPN サーバーの設定です。

```
hostname hub
!
crypto ikev2 authorization policy default
 pool flex-pool
 def-domain cisco.com
 route set interface
!
crypto ikev2 profile default
 match identity remote fqdn domain cisco.com
 identity local fqdn hub.cisco.com
 authentication local rsa-sig
 authentication remote rsa-sig
 pki trustpoint CA
 aaa authorization group cert list default default
 virtual-template 1
!
crypto ipsec profile default
 set ikev2-profile default
!
interface Loopback0
 ip address 172.16.1.1 255.255.255.255
!
interface Ethernet0/0
 ip address 10.0.0.100 255.255.255.0
!
interface Virtual-Template1 type tunnel
 ip unnumbered Loopback0
 ip nhrp network-id 1
 ip nhrp redirect
 tunnel protection ipsec profile default
!
ip local pool flex-pool 172.16.0.1 172.16.0.254
!
router bgp 65100
 bgp router-id 10.0.0.100
 bgp log-neighbor-changes
 bgp listen range 172.16.0.0/24 peer-group spokes
```

```
 neighbor spokes peer-group
 neighbor spokes remote-as 65100
 neighbor spokes transport connection-mode passive
 neighbor spokes update-source Loopback0
 !
 address-family ipv4
  neighbor spokes activate
  neighbor spokes default-originate
  neighbor spokes prefix-list no-default in
 exit-address-family
!
ip prefix-list no-default seq 5 deny 0.0.0.0/0
ip prefix-list no-default seq 10 permit 0.0.0.0/0 le 32
```

次は、最初の FlexVPN クライアントの設定です。

```
hostname spoke1
!
crypto ikev2 authorization policy default
 route set interface
!
crypto ikev2 profile default
 match identity remote fqdn domain cisco.com
 identity local fqdn spoke1.cisco.com
 authentication local rsa-sig
 authentication remote rsa-sig
 pki trustpoint CA
 aaa authorization group cert list default default
 virtual-template 1
!
crypto ipsec profile default
 set ikev2-profile default
!
interface Tunnel0
 ip address negotiated
 ip nhrp network-id 1
 ip nhrp shortcut virtual-template 1
 ip nhrp redirect
 tunnel source Ethernet0/0
 tunnel destination 10.0.0.100
 tunnel protection ipsec profile default
!
interface Ethernet0/0
 ip address 10.0.0.110 255.255.255.0
!
interface Ethernet1/0
 ip address 192.168.110.1 255.255.255.0
!
interface Virtual-Template1 type tunnel
 ip unnumbered Tunnel0
 ip nhrp network-id 1
 ip nhrp shortcut virtual-template 1
 ip nhrp redirect
 tunnel protection ipsec profile default
!
router bgp 65100
 bgp router-id 10.0.0.110
 bgp log-neighbor-changes
 neighbor hubs peer-group
 neighbor hubs remote-as 65100
 neighbor hubs update-source Tunnel0
 neighbor 172.16.1.1 peer-group hubs
 !
 address-family ipv4
```

```
  network 192.168.110.0
  neighbor 172.16.1.1 activate
 exit-address-family
```

次は、2 番目の FlexVPN クライアントの設定です。

```
hostname spoke2
!
crypto ikev2 authorization policy default
 route set interface
 route set access-list flex-route
!
crypto ikev2 profile default
 match identity remote fqdn domain cisco.com
 identity local fqdn spoke2.cisco.com
 authentication local rsa-sig
 authentication remote rsa-sig
 pki trustpoint CA
 aaa authorization group cert list default default
 virtual-template 1
!
crypto ipsec profile default
 set ikev2-profile default
!
interface Tunnel0
 ip address negotiated
 ip nhrp network-id 1
 ip nhrp shortcut virtual-template 1
 ip nhrp redirect
 tunnel source Ethernet0/0
 tunnel destination 10.0.0.100
 tunnel protection ipsec profile default
!
interface Ethernet0/0
 ip address 10.0.0.120 255.255.255.0
!
interface Ethernet1/0
 ip address 192.168.120.1 255.255.255.0
!
interface Virtual-Template1 type tunnel
 ip unnumbered Tunnel0
 ip nhrp network-id 1
 ip nhrp shortcut virtual-template 1
 ip nhrp redirect
 tunnel protection ipsec profile default
!
router bgp 65100
 bgp router-id 10.0.0.120
 bgp log-neighbor-changes
 neighbor hubs peer-group
 neighbor hubs remote-as 65100
 neighbor hubs update-source Tunnel0
 neighbor 172.16.1.1 peer-group hubs
 !
 address-family ipv4
  network 192.168.120.0
  neighbor 172.16.1.1 activate
 exit-address-family
```

FlexVPN スポーク間の設定に関する追加情報

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『*Cisco IOS Master Command List, All Releases*』
セキュリティ コマンド	• 『*Cisco IOS Security Command Reference Commands A to C*』 • 『*Cisco IOS Security Command Reference Commands D to L*』 • 『*Cisco IOS Security Command Reference Commands M to R*』 • 『*Cisco IOS Security Command Reference Commands S to Z*』
ショートカット スイッチングの強化	『*Shortcut Switching Enhancements for NHRP in DMVPN Networks*』

シスコのテクニカル サポート

説明	リンク
右の URL にアクセスして、シスコのテクニカル サポートを最大限に活用してください。これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

FlexVPN スポーク間の機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *278 : FlexVPN* スポーク間の機能情報

機能名	リリース	機能情報
FlexVPN スポーク間		FlexVPN スポーク間機能では、FlexVPN クライアントは別の FlexVPN クライアントとの直接暗号チャネルを確立できます。この機能はVTI、IKEv2、およびNHRP を利用して、スポーク間接続を構築します。 この機能は、Cisco IOS Release 15.2(2)T で導入されました。 次のコマンドが導入または変更されました。 **ip unnumbered loopback0, tunnel source, tunnel mode gre ip, nhrp network-id, ip nhrp redirect, ip nhrp shortcut.**
FlexVPN IPv6 ダイレクト スポーク間		FlexVPN IPv6 ダイレクト スポーク間機能は、FlexVPN スポークに対する IPv6 アドレスの使用をサポートします。IPv6 アドレスのサポートにより、IPv6 over IPv4、IPv4 over IPv6、および IPv6 over IPv6 の転送がサポートされます。 次のコマンドが導入または変更されました。 **ipv6 nhrp shortcut.**

第 210 章

IKEv2 ロード バランサの設定

IKEv2 ロードバランサ機能は、FlexVPN ゲートウェイのクラスタを有効にするためのサポートを提供し、FlexVPN ゲートウェイ間で受信インターネット キー エクスチェンジ バージョン 2（IKEv2）の接続要求を配信します。この機能は、システムおよび暗号の負荷率に基づいて最も負荷の小さい FlexVPN ゲートウェイに受信 FlexVPN または AnyConnect クライアントの要求をリダイレクトします。

IKEv2 ロード バランサの前提条件

- サーバー側の設定として、Hot Standby Router Protocol（HSRP）および FlexVPN サーバー（IKEv2 プロファイル）が設定されていること。
- クライアント側の設定として、FlexVPN クライアントが設定されていること。

IKEv2 ロード バランサに関する情報

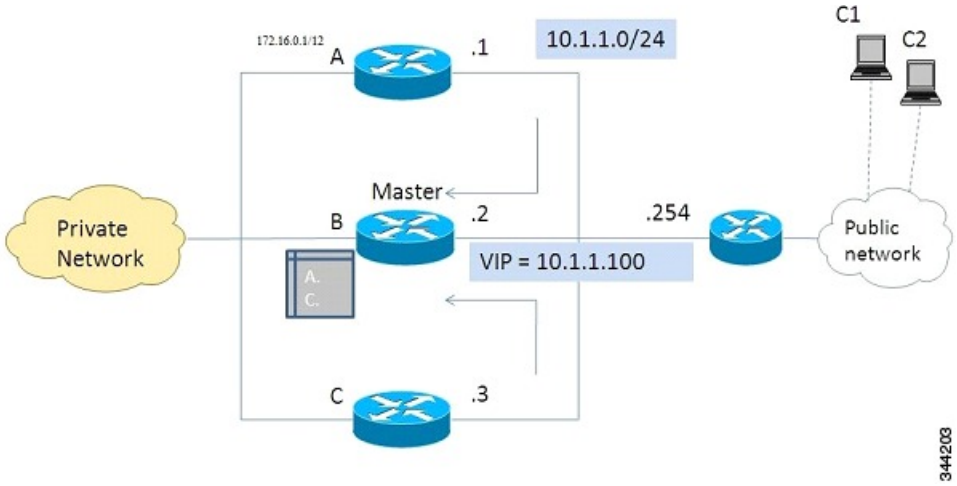
IKEv2 ロード バランサの概要

IKEv2 ロード バランサ サポート機能は、リモート アクセス クライアントからの要求を、Hot Standby Router Protocol（HSRP）グループまたはクラスタ内の最低負荷ゲートウェイ（LLG）にリダイレクトすることで、クラスタロードバランシング（CLB）ソリューションを提供します。HSRP クラスタは、LAN またはエンタープライズ ネットワーク内のゲートウェイまたは FlexVPN サーバーのグループです。CLB ソリューションは、要求の HSRP クラスタ内 LLG へ

のリダイレクトにより、RFC 5685 で定義されたインターネット キー エクスチェンジ バージョン 2（IKEv2）リダイレクト メカニズムと連携します。

次の図は、IKEv2 クラスタのロード バランシング ソリューションの仕組みを示します。

図 *109 : IKEv2* クラスタのロード バランシング ソリューション



1. アクティブ HSRP ゲートウェイは、HSRP グループの「プライマリ」として選択され、グループの仮想 IP アドレス（VIP）の所有権を取得します。プライマリはクラスタ内にゲートウェイのリストを保持して、各ゲートウェイの負荷を追跡し、FlexVPN クライアントの要求を LLG にリダイレクトします。
2. 残りのゲートウェイは「従属」と呼ばれ、負荷の更新をプライマリに定期的に送信します。
3. IKEv2 クライアントが HSRP VIP に接続すると、要求はまずプライマリに到達し、クラスタ内の LLG に順番にリダイレクトされます。

CLB ソリューションのコンポーネントは次のとおりです。

- HSRP
- CLB プライマリ
- CLB 従属
- CLB 通信
- IKEv2 リダイレクト メカニズム

Hot Standby Router Protocol

Hot Standby Router Protocol（HSRP）は、プライマリ HSRP またはアクティブルータ（AR）を選択するために使用されます。専用デバイスを選択する HSRP では、グループ内の 1 つのデバイスに VIP を設定する必要があります。このアドレスは、グループ内の他デバイスによって学習されます。プライマリに割り当てられた IP アドレスは、グループの VIP として使用されま

す。HSRP アクティブルータ（「プライマリ CLB」とも呼ばれる）は IKEv2 要求を受信し、クラスタの LLG にこれらの要求をリダイレクトします。リダイレクトが IKEv2 プロトコル レベルで実行されると、以下を実行できるようになります。

- FlexVPN クライアントからのすべての要求は、VIP が FlexVPN クライアントで設定されると、プライマリ HSRP で受信される。FlexVPN クライアントが知る必要があるのは HSRP クラスタの VIP のみであるため、FlexVPN クライアントの設定は最小化される。
- プライマリ CLB はプライマリ HSRP と同じゲートウェイで実行されるため、すべての従属 CLB の負荷情報が維持される。プライマリ CLB では、要求の効率的なリダイレクトが可能なため、複数のリダイレクトやループを防ぐことができる。

プライマリ CLB

プライマリ CLB は、プライマリ HSRP またはアクティブルータ（AR）上で動作します。プライマリは、従属 CLB から更新を受信し、その負荷条件に基づいてそれらをソートし、負荷が最小のゲートウェイ（LLG）を計算します。プライマリは、LLG の IP アドレスを IKEv2（FlexVPN サーバー上）に送信します。IP アドレスは、LLG との IKEv2 セッションを開始した発信側（FlexVPN クライアント）に送信されます。プライマリは受信する IKEv2 クライアント接続を LLG にリダイレクトします。詳細については、IKEv2 リダイレクト メカニズム（3100 ページ）を参照してください。

（注） 「CLB ノード」は、プライマリ CLB と従属 CLB を指定する必要がある場所で使用します。

従属 CLB

従属 CLB は、アクティブルータ（AR）上を除いた、HSRP グループ内のすべてのデバイスで動作します。従属は、サーバーに負荷更新を定期的に送信します。従属 CLB は、プライマリ CLB に情報を提供する、フル機能の IKEv2 ゲートウェイです。更新以外にも、従属 CLB は活動管理のメッセージをプライマリ CLB に送信します。

CLB 負荷管理メカニズム

CLB 負荷管理メカニズムは、プライマリ CLB と従属 CLB 間で動作する、TCP ベースのプロトコルです。CLB 負荷管理メカニズムは、プライマリ CLB に従属 CLB の負荷について情報を提供します。この情報に基づいて、プライマリ CLB は、新しく受信する各 IKEv2 接続のセッションを処理する LLG を選択します。

IKEv2 ロード バランサの利点

- IKEv2 ロード バランサ サポート機能は、設定が簡単でコスト効率に優れています。
- FlexVPN クライアントは、クラスタ内のすべてのゲートウェイの IP アドレスを知る必要はありません。クライアントが知っておく必要があるのは、クラスタの仮想 IP アドレスのみです。

- すべての暗号化セッションは、クラスタ内のノードにリダイレクトされます。

IKEv2 リダイレクト メカニズム

IKEv2 リダイレクト メカニズムによって、VPN ゲートウェイは負荷条件およびメンテナンス要件に基づいて FlexVPN クライアント要求を別の VPN ゲートウェイにリダイレクトできます。

IKEv2 リダイレクト メカニズムは、セキュリティ アソシエーション（SA）の初期化（IKE_SA_INIT）と SA 認証（IKE_AUTH）で実行されます。

IKEv2 初期交換中のリダイレクト（SA 初期化）

FlexVPN クライアントまたは AnyConnect クライアントは、最初の IKE_SA_INIT 要求に REDIRECT_SUPPORTED 通知メッセージを含めることで、インターネット キー エクスチェンジバージョン 2（IKEv2）リダイレクト メカニズムのサポートを示します。**crypto ikev2 redirect client** コマンドを使用して、クライアントのリダイレクト メカニズムを有効にします。**crypto ikev2 redirect gateway init** コマンドを使用して、ゲートウェイの IKE_SA_INIT でのリダイレクトを有効にします。

IKEv2 要求を別の新しいゲートウェイにリダイレクトするには、IKE_SA_INIT 要求を受信するゲートウェイが、暗号ロードバランサ（CLB）モジュールのサポートによって、新しいゲートウェイ（この場合は LLG）の IP アドレスまたは完全修飾ドメイン名（FQDN）を選択します。このゲートウェイは、REDIRECT 通知メッセージを含む IKE_SA_INIT 応答で応答します。通知には、IKE_SA_INIT 要求内のペイロードからの新しいゲートウェイやナンス値などの情報が含まれます。IKE_SA_INIT 応答を受信したクライアントは、IKE_SA_INIT 要求で送信されたナンス値とリダイレクト通知で指定されたゲートウェイ情報を検証し、リダイレクト通知が設定のとおりかどうかを確認します。

（注） ナンス値が一致しない場合、クライアントはその応答を破棄して別の応答を待って、発信側のサービス妨害（DoS）攻撃を防ぎます。IKE_SA_INIT 応答内に攻撃者が不正なリダイレクト ペイロードが挿入すると、DoS 攻撃が発生する場合があります。

新しいゲートウェイとの IKE_SA_INIT 交換では、クライアント メッセージに REDIRECTED_FROM 通知ペイロードが含まれます。REDIRECTED_FROM 通知ペイロードは、クライアントにリダイレクトされる送信元 VPN ゲートウェイの IP アドレスで構成されています。IKEv2 交換は、送信元ゲートウェイでの処理と同じように処理されます。

（注） 新しいゲートウェイもクライアントの目的を果たせない場合、クライアントは新しいゲートウェイによって再度リダイレクトされることがあります。クライアントでは、リダイレクト後の新しいゲートウェイとの IKE_SA_INIT 交換に、REDIRECT_SUPPORTED ペイロードは再度含まれません。新しいゲートウェイとの IKE_SA_INIT 交換内に REDIRECTED_FROM 通知ペイロードが存在することは、クライアントが IKEv2 リダイレクト メカニズムをサポートすることを、新しいゲートウェイに示します。

IKE_AUTH 交換中のリダイレクト（SA 認証）

詳細なセキュリティ分析によって、IKE_AUTH 中のリダイレクトは IKE_INIT 中のリダイレクトと比較してより安全でも危険でもないことが示されました。ただし、パフォーマンスと拡張性の理由により、シスコは IKE_INIT 中のリダイレクトを推奨します。**crypto ikev2 redirect gateway auth** コマンドを使用して、ゲートウェイのリダイレクト メカニズムを有効にします。**redirect gateway auth** コマンドを使用して、選択した IKEv2 プロファイル認証時のリダイレクトを有効にします。

この方法では、クライアント認証ペイロードは、リダイレクト通知ペイロードを送信する前に検証されます。また、クライアントでも、リダイレクト通知に従って動作する前に、ゲートウェイ認証ペイロードが検証されます。任所ペイロードが交換され、正常に検証されると、IKEv2 セキュリティ アソシエーション（SA）が正常に検証され、要求のリダイレクトを決定する INITIAL_CONTACT が処理されます。リダイレクトが有効な場合、ゲートウェイでは IKE SA が作成され、リダイレクト通知で IKE_AUTH 応答が送信されます。

この方法では、子 SA は作成されません。IKE_AUTH には、子 SA に関連するペイロードは含まれません。IKE_AUTH 応答を受信すると、クライアントは、ゲートウェイ認証ペイロードを検証し、削除通知を送信してそのゲートウェイがある IKEv2 SA を削除します。クライアントは、リダイレクト通知ペイロードに従って動作し、新しいゲートウェイとの接続を確立します。クライアントは、削除通知の確認応答を待たずに、新しいゲートウェイとの接続を確立します。IKE_AUTH 交換で Extensible Authentication Protocol（EAP：拡張可能認証プロトコル）認証が呼び出される場合、ゲートウェイでは、リダイレクトペイロードの送信を最初と最後の IKE_AUTH 応答のどちらで送信するかを選択します。リダイレクトごとに認証情報を指定する必要がないため、EAP 認証は最初の IKE_AUTH 応答に含まれます。

互換性および相互運用性

IKEv2 リダイレクト メカニズムは、RFC 5685 に基づいています。ゲートウェイ（IKEv2 応答側）は、標準を実装するクライアント（IKEv2 発信側）と互換性があります。同様に、クライアント（発信者）の実装では、標準を実装しているサードパーティ製サーバー（応答側）との互換性が必要です。負荷管理メカニズムは Cisco 独自のもので、Cisco IOS デバイスでのみサポートされます。

リダイレクト ループ処理

クライアント要求は、正しくない設定またはサービス妨害（DoS）攻撃を理由として、順番に複数回リダイレクトできます。場合によっては、クライアントを他のゲートウェイにリダイレ

クトする複数のゲートウェイによってクライアントがループに入り、その結果クライアントへのサービスが拒否されることがあります。これを防ぐには、**max-redirects** *number* キーワード/引数ペアを指定して **crypto ikev2 redirect client** コマンドを使用し、特定の IKEv2 セキュリティ アソシエーション（SA）設定について特定数を超えるリダイレクトを受け入れないようにクライアントを設定します。

IKEv2 クラスタの再接続

IKEv2 クラスタの再接続機能によって、Cisco AnyConnect クライアントはクラスタ内のサーバーに再接続できます。**crypto ikev2 reconnect key** は、クライアントにプッシュされた不明瞭なデータを暗号化するためにサーバーに導入されています。障害を検出すると、クライアントは、認証クレデンシャルの入力を再度要求せずに新規または既存のサーバーと再接続します。

キー インデックス値は 2 つのみ（1 および 2）です。いずれかの時点で、これを使用して設定されたキーの 1 つがアクティブになります。IOS サーバーで再接続キーの CLI を使用して再接続キーが設定されている場合、Cisco IOS サーバーは再接続データを復号できます。これは、キーがバックアップ キーのみの場合にも当てはまります。

この機能は、**authentication** コマンドで IKEv2 プロファイルの認証方式として **anyconnect-eap** キーワードを指定した場合にはサポートされません。

（注） この機能は、Cisco AnyConnect サーバーとして動作するように設定された Cisco IOS デバイスで使用できます。この機能をサポートする AnyConnect クライアント ソフトウェア バージョンは、4.2 以降のリリースです。この機能は、新規導入にのみ適用できます。Cisco IOS サーバーでこの機能が有効になると、以前のリリースの Cisco AnyConnect クライアントはサポートされなくなります。

IKEv2 ロード バランサの設定方法

サーバー クラスタの設定

ロード バランシングに対する HSRP グループの設定

このタスクを実行して、単一の Hot Standby Router Protocol（HSRP）グループをクラスタ用に設定します。

Hot Standby Router Protocol（HSRP）は、プライマリ HSRP またはアクティブルータ（AR）を選択するために使用されます。専用デバイスを選択する HSRP では、グループ内の 1 つのデバイスに VIP を設定する必要があります。このアドレスは、グループ内の他デバイスによって学習されます。プライマリに割り当てられた IP アドレスは、グループの VIP として使用されます。HSRP アクティブルータ（「プライマリ CLB」とも呼ばれる）は IKEv2 要求を受信し、ク

ラスタの LLG にこれらの要求をリダイレクトします。リダイレクトが IKEv2 プロトコル レベルで実行されると、以下を実行できるようになります。

- FlexVPN クライアントからのすべての要求は、VIP が FlexVPN クライアントで設定されると、プライマリ HSRP で受信される。FlexVPN クライアントが知る必要があるのは HSRP クラスタの VIP のみであるため、FlexVPN クライアントの設定は最小化される。
- プライマリ CLB はプライマリ HSRP と同じゲートウェイで実行されるため、すべての従属 CLB の負荷情報が維持される。プライマリ CLB では、要求の効率的なリダイレクトが可能なため、複数のリダイレクトやループを防ぐことができる。

（注） このタスクでは、ロードバランシングのため、HSRP グループの設定に必要な最小限のコマンドを説明します。

手順の概要

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **ip address** *ip-address mask* [**secondary**]
5. **standby** [*group-number*] **priority** *priority*
6. **standby** *group-name*
7. **exit**
8. 手順 3 ～ 7 を繰り返して、別のクラスタに HSRP グループを設定します。

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface** *type number* 例： `Device(config)# interface GigabitEthernet 0/0/0`	インターフェイス タイプを設定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	**ip address** *ip-address mask* [**secondary**] 例：	インターフェイスのプライマリ IP アドレスまたはセカンダリ IP アドレスを指定します。

	コマンドまたはアクション	目的
	`Device(config-if)# ip address 10.0.0.1 255.255.255.0`	
ステップ 5	**standby** [*group-number*] **priority** *priority* 例： `Device(config-if)# standby 1 priority 110`	HSRP 優先度を設定します。
ステップ 6	**standby** *group-name* 例： `Device(config-if)# standby group1`	HSRP スタンバイ グループの名前を指定します。
ステップ 7	**exit** 例： `Device(config-if)# exit`	グローバル コンフィギュレーション モードに戻ります。
ステップ 8	手順 3 ～ 7 を繰り返して、別のクラスタに HSRP グループを設定します。	—

負荷管理メカニズムの設定

手順の概要

1. **enable**
2. **configure terminal**
3. **crypto ikev2 cluster**
4. **holdtime** *milliseconds*
5. **master** { **overload-limit** *percent* | **weight** { **crypto-load** *weight-number* | **system-load** *weight-number*}}
6. **port** *port-number*
7. **slave** { **hello** *milliseconds* | **max-session** *number* | **priority** *number* | **update** *milliseconds*}
8. **standby-group** *group-name*
9. **shutdown**
10. **exit**
11. **crypto ikev2 reconnect key** *key index* **active** *name*
12. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。

	コマンドまたはアクション	目的
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**crypto ikev2 cluster** 例： `Device(config)# crypto ikev2 cluster`	IKEv2 クラスタ ポリシーを定義し、IKEv2 クラスタ コンフィギュレーション モードを開始します。
ステップ 4	**holdtime** *milliseconds* 例： `Device(config-ikev2-cluster)# holdtime 10000`	（オプション）ピアからのメッセージを受信する時間をミリ秒単位で指定します。 • 設定された時間内にメッセージを受信しない場合、ピアは「死んでいる」と宣言されます。
ステップ 5	**master** { **overload-limit** *percent* | **weight** { **crypto-load** *weight-number* | **system-load** *weight-number*}} 例： `Device(config-ikev2-cluster)# master weight crypto-load 10`	HSRP クラスタのプライマリの設定を指定します。 • **overload-limit** *percent*：クラスタのしきい値負荷。デバイスがビジーなことを判断し、要求へのリダイレクトを無視するための負荷制限。 • **weight**：負荷属性の重みを指定します。範囲：0 ～ 100。デフォルトは 100 です。 • **crypto-load** *weight-number*：IKE と IPSec のセキュリティ アソシエーション（SA）の負荷。 • **system-load** *weight-number*：システムとメモリの負荷。
ステップ 6	**port** *port-number* 例： `Device(config-ikev2-cluster)# port 2000`	（任意）クラスタプライマリのリッスンポートを指定します。
ステップ 7	**slave** { **hello** *milliseconds* | **max-session** *number* | **priority** *number* | **update** *milliseconds*} 例： `Device(config-ikev2-cluster)# slave max-session 90`	HSRP グループの従属ゲートウェイ設定を指定します。 • **hello** *milliseconds*：ミリ秒単位の従属ゲートウェイの Hello インターバル。 • **max-session** *number*：従属上で許可される SA の最大数。このキーワードは必須であり、スキップできません。 • **priority** *number*：従属の優先順位。

	コマンドまたはアクション	目的
		• **update** *milliseconds*：従属ゲートウェイ用の更新メッセージ間の、ミリ秒単位のインターバル。
ステップ 8	**standby-group** *group-name* 例： `Device(config-ikev2-cluster)# standby-group group1`	従属が含まれている HSRP グループを定義します。 • *group-name*：グループ名は *group-name* 引数から派生します。これは、**standby name** コマンドで指定されます。
ステップ 9	**shutdown** 例： `Device(config-ikev2-cluster)# shutdown`	（オプション）IKEv2 クラスタ ポリシーを無効にします。
ステップ 10	**exit** 例： `Device(config-ikev2-cluster)# exit`	IKEv2 クラスタ コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードに戻ります。
ステップ 11	**crypto ikev2 reconnect key** *key index* **active** *name* 例： `Device(config)# crypto ikev2 reconnect key 1 active test123`	セッション再接続の IKEv2 不透明型データ サポートを有効にします。 （注） IKEv2 クラスタの再接続機能は、**ikev2 reconnect key active** *name key-string* に **active** キーワードが含まれている場合にのみ、暗号化に対して有効になります。クラスタの再接続機能を有効にするには、**active** キーワードは必須です。**active** キーワードを指定せずに **ikev2 reconnect key** *key-name key-string* コマンドを使用すると、ヘッドエンドでは復号化のみが可能になります。
ステップ 12	**end** 例： `Device(config-ikev2-cluster)# end`	IKEv2 クラスタ コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

サーバーでの IKEv2 リダイレクト メカニズムの有効化

手順の概要

1. **enable**
2. **configure terminal**
3. **crypto ikev2 redirect gateway init**
4. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**crypto ikev2 redirect gateway init** 例： `Device(config)# crypto ikev2 redirect gateway init`	SA 開始中に、ゲートウェイで IKEv2 リダイレクト メカニズムを有効にします。
ステップ 4	**end** 例： `Device(config)# end`	グローバル コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

クライアントでの IKEv2 リダイレクト メカニズムの有効化

手順の概要

1. **enable**
2. **configure terminal**
3. **crypto ikev2 redirect client** [**max-redirects** *number*]
4. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**crypto ikev2 redirect client** [**max-redirects** *number*] 例： `Device(config)# crypto ikev2 redirect client max-redirects 15`	FlexVPN クライアントで IKEv2 リダイレクト メカニズムを有効にします。 • **max-redirects** *number*：（オプション）リダイレクト ループ検出に対して、FlexVPN クライアン

	コマンドまたはアクション	目的
		トで設定できるリダイレクトの最大数を指定します。
ステップ 4	**end** 例： `Device(config)# end`	グローバル コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

IKEv2 ロード バランサの設定例

例：ロード バランシングに対する HSRP グループの設定

次の例では、プライオリティ 110 で Hot Standby Router Protocol（HSRP）グループのアクティブ ルータとして設定された RouterA を示します。デフォルトのプライオリティ レベルは 100 です。この HSRP グループには、group1 のグループ名が割り当てられます。グループ名は、クラスタ ポリシーに記載されています。

```
Device(config)# hostname RouterA
Device(config)# interface GigabitEthernet 0/0/0
Device(config-if)# ip address 10.0.0.1 255.255.255.0
Device(config-if)# standby 1 priority 110
Device(config-if)# standby group1
Device(config-if)# end
```

例：負荷管理メカニズムの設定

次の例は、IKEv2 で負荷管理メカニズムを設定する方法を示します。

```
Device> enable
Device# configure terminal
Device(config)# crypto ikev2 cluster
Device(config-ikev2-cluster)# holdtime 10000
Device(config-ikev2-cluster)# master crypto-load 10
Device(config-ikev2-cluster)# port 2000
Device(config-ikev2-cluster)# slave priority 90
Device(config-ikev2-cluster)# standby-group group1
Device(config-ikev2-cluster)# shutdown
Device(config-ikev2-cluster)# end
```

例：リダイレクト メカニズムの設定

次の例は、クライアント上およびゲートウェイでの開始中にリダイレクト メカニズムを有効にする方法を示します。

```
Device> enable
Device# configure terminal
Device(config)# crypto ikev2 redirect client
Device(config)# crypto ikev2 redirect gateway init
Device(config)# end
```

例：クラスタ再接続キーの設定

次の例は、サーバーで再接続キーを有効にする方法を示します。

```
Device> enable
Device# configure terminal
Device(config)# crypto ikev2 reconnect key 1 active key
Device(config)# crypto ikev2 reconnect key 2 test
Device(config)# end
```

その他の参考資料

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『Master Command List, All Releases』
セキュリティ コマンド	• 『Cisco IOS Security Command Reference Commands A to C』 • 『Cisco IOS Security Command Reference Commands D to L』 • 『Cisco IOS Security Command Reference Commands M to R』 • 『Cisco IOS Security Command Reference Commands S to Z』
HSRP コンフィギュレーション	『*Configuring HSRP*』
HSRP コマンド	『Cisco IOS First Hop Redundancy Protocols Command Reference』

標準および RFC

標準/RFC	タイトル
RFC 5685	*Redirect Mechanism for the Internet Key Exchange Protocol Version 2 (IKEv2)*

シスコのテクニカル サポート

説明	リンク
右の URL にアクセスして、シスコのテクニカル サポートを最大限に活用してください。これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

IKEv2 ロード バランサの機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *279 : IKEv2* ロード バランサの機能情報

機能名	リリース	機能情報
AnyConnect のクラスタ再接続との IKEv2 高速コンバージェンス		AnyConnect のクラスタ再接続との IKEv2 高速コンバージェンス機能では、Cisco AnyConnect クライアントはクラスタ内の任意のサーバーと再接続できます。 次のコマンドが導入または変更されました： **crypto ikev2 reconnect key**

機能名	リリース	機能情報
IKEv2 ロード バランサのサポート		IKEv2 ロード バランサ サポート機能は、要求を最低負荷ゲートウェイにリダイレクトすることで、FlexVPN クライアントから受信する IKEv2 要求を、IKEv2 FlexVPN サーバー間またはゲートウェイ間で分散します。 次のコマンドが導入または変更されました。 **crypto ikev2 cluster, crypto ikev2 redirect, holdtime, primary (IKEv2), port (IKEv2), redirect gateway, subordinate (IKEv2), standby-group, show crypto ikev2 cluster, show crypto ikev2 sa.**

第 211 章

IKEv2 フラグメンテーションの設定

RFC 機能に準拠した IKE フラグメンテーションでは、IETF の **draft-ietf-ipsecme-ikev2-fragmentation-10** ドキュメントの提案に従って、インターネット キー エクスチェンジ バージョン 2 （IKEv2）パケットのフラグメンテーションを実装しました。

IKEv2 フラグメンテーションの設定に関する情報

IKEv2 フラグメンテーション

インターネット キー エクスチェンジ バージョン 2（IKEv2）フラグメンテーション プロトコルは、大きな IKEv2 メッセージを IKE フラグメント メッセージと呼ばれる一連の小さなメッセージに分割します。IKEv2 リモート アクセスのヘッドエンド機能によって Cisco IOS ソフトウェアに実装された IKEv2 フラグメンテーション方式は、シスコ独自の方法であり、シスコ以外のピアとの相互運用性は制限されます。フラグメンテーションは、暗号化された IKEv2 パケットでのみ実行されます。そのため、ピアがすべてのフラグメントを受信するまで、ピアはメッセージを復号したり認証することはできません。RFC に準拠した IKE フラグメンテーション機能は、フラグメンテーション後にパケットを暗号化することによって IETF **draft-ietf-ipsecme-ikev2-fragmentation-10** ドキュメントを実装し、シスコ独自のフラグメンテーション方式を引き続きサポートしながらシスコ以外のピアとの相互運用性を実現します。

（注） デフォルトでは、IKEv2 フラグメンテーションは無効になっていますが、show run all により、暗号 IKEv2 フラグメンテーション MTU が 576 B であることが示されます。

ピア間のネゴシエーション

RFC 機能に準拠した IKE フラグメンテーションから有効。IETF 標準フラグメンテーション方式のサポートが通知ペイロードとして IKE_SA_INIT メッセージに追加されました。一方、シスコ独自のフラグメンテーション方式は、同じ IKE_SA_INIT メッセージ内で引き続きベンダー ID ペイロードを使用します。フラグメンテーションが有効な場合、両方の方式が **show crypto ikev2 sa detail** コマンドで適切と表示されます。最大伝送ユニット（MTU）はローカルで設定され、メッセージ間のネゴシエーションも交換も行いません。INIT 交換の後、いずれかの方式で設定されたネットワーク内のピアは、使用する必要がある認証方式と、AUTH メッセージをフラグメント化できるかどうかをを認識します。

次に、デバッグが有効で、INIT 要求メッセージでのネゴシエーション機能を表している場合のデバイスからの出力例を示します。

```
*Oct 14 08:45:24.732: IKEv2:(SESSION ID = 0,SA ID = 1):Next payload: SA, version: 2.0
Exchange type: IKE_SA_INIT, flags: INITIATOR Message id: 0, length: 524
Payload contents:
SA Next payload: KE, reserved: 0x0, length: 144
…
Security protocol id: IKE, spi size: 0, type: NAT_DETECTION_DESTINATION_IP
NOTIFY(IKEV2_FRAGMENTATION_SUPPORTED) Next payload: VID, reserved: 0x0, length: 8
Security protocol id: Unknown - 0, spi size: 0, type: IKEV2_FRAGMENTATION_SUPPORTED
VID Next payload: NONE, reserved: 0x0, length: 20
```

上記の出力では、メッセージ内の IKEV2_FRAGMENTATION_SUPPORTED および VID 値によって、IETF 標準フラグメンテーション方式とシスコ独自のフラグメンテーション方式の両方をサポートすることを示す、発信側から応答側へのメッセージが INIT 要求に含まれます。

次に、デバッグが有効で、INIT 応答メッセージでのネゴシエーション機能を表している場合のデバイスからの出力例を示します。

```
*Oct 14 08:45:24.732: IKEv2:(SESSION ID = 0,SA ID = 1):Next payload: SA, version: 2.0
Exchange type: IKE_SA_INIT, flags: INITIATOR Message id: 0, length: 524
Payload contents:
SA Next payload: KE, reserved: 0x0, length: 144
last proposal: 0x0, reserved: 0x0, length: 140
…
NOTIFY(IKEV2_FRAGMENTATION_SUPPORTED) Next payload: VID, reserved: 0x0, length: 8
Security protocol id: Unknown - 0, spi size: 0, type: IKEV2_FRAGMENTATION_SUPPORTED
<-------- Response, supporting both
VID Next payload: NONE, reserved: 0x0, length: 20 <-------- Response, supporting both
```

上記の出力では、メッセージ内の IKEV2_FRAGMENTATION_SUPPORTED および VID 値によって、IETF 標準フラグメンテーション方式とシスコ独自のフラグメンテーション方式の両方をサポートすることを示す、応答側から発信側へのメッセージが応答要求に含まれます。

以前のリリースのフラグメンテーション サポート

シスコ独自のフラグメンテーション方式を使用する以前のリリースのフラグメンテーション サポートを保証するために、IKEv2 は IETF 標準フラグメンテーション方式の IKEv2 通知ペイロード タイプと共にベンダー ID を引き続き使用します。両方のフラグメンテーション方式がサポートされている場合、IKEv2 は IETF 標準フラグメンテーション方式を優先します。

次の表に、ピアの機能に基づいてフラグメンテーションのタイプを特定する方法を示します。CISCO はシスコ独自のフラグメンテーション方式を示し、STD は IETF 標準フラグメンテーション方式を示します。

ピア 1 の機能	ピア 2 の機能	セキュリティ アソシエーションでアクティブなフラグメンテーション タイプ
STD + CISCO	STD + CISCO	STD
STD	STD	STD
CISCO	CISCO	CISCO
CISCO	STD + CISCO	CISCO
STD	STD + CISCO	STD
STD	CISCO	なし
なし	なし、STD + CISCO、または STD または CISCO	なし

フラグメントの暗号化、複合化、および再送信

フラグメンテーションおよび暗号化

パケットは、**crypto ikev2 fragmentation** コマンドで指定された最大伝送ユニット（MTU）値またはデフォルトMTU値のいずれかに基づいてフラグメント化されます。暗号化されたペイロードのみを含む IKE メッセージがフラグメント化されます。アナウンス メッセージ内の新しいペイロードタイプ（暗号化および認証されたフラグメント）は、フラグメントの合計数以上のフラグメント番号を示します。このペイロードは SKF として注釈がつけられ、値は 53 です。

発信パケットを暗号化する前に、パケット長を確認します。確立済みのセキュリティ アソシエーションは、IETF標準フラグメント方式でSAが有効になっているかどうかも確認します。次に、フラグメント化されたパケットの伝送が表示されるデバイスからの出力例を示します。

```
*Oct 16 10:31:22.221: IKEv2:(SESSION ID = 0,SA ID = 3):Next payload: SKF, version: 2.0
Exchange type: INFORMATIONAL, flags: INITIATOR Message id: 1, length: 244
Payload contents:
SKF Next payload: COOP, reserved: 0x90, length: 216
SKF Fragment number: 1 OF Total Fragments: 3
*Oct 16 10:31:22.222: IKEv2:(SESSION ID = 0,SA ID = 3):Next payload: SKF, version: 2.0
Exchange type: INFORMATIONAL, flags: INITIATOR Message id: 1, length: 244
Payload contents:
SKF Next payload: COOP, reserved: 0x90, length: 216
SKF Fragment number: 2 OF Total Fragments: 3
*Oct 16 10:31:22.222: IKEv2:(SESSION ID = 0,SA ID = 3):Next payload: SKF, version: 2.0
Exchange type: INFORMATIONAL, flags: INITIATOR Message id: 1, length: 244
Payload contents:
SKF Next payload: COOP, reserved: 0x90, length: 216
SKF Fragment number: 3 OF Total Fragments: 3
```

「SKF Next payload: COOP, reserved: 0x90, length: 216」および「SKF Fragment number: 1 OF Total Fragments: 3」は、メッセージが3つのフラグメントにフラグメント化された協調キー サーバーのアナウンスメント（ANN）パケットであることを示します。

復号と最適化

応答側で受信フラグメントが受信されると、各フラグメントは復号されて一時的に保存されます。復号（元のパックへのフラグメントのアセンブリ）時に、重複するフラグメント、フラグメントの合計数以上のフラグメント番号、およびまったく別のフラグメント番号を持つフラグメントはドロップされます。フラグメントは、受信した順ではなくフラグメント番号の昇順で追加されます。そのため、パケットアセンブリが高速化します。ただし、順序どおりではないフラグメントも許可され、処理されます。各フラグメントは、メッセージに関係するすべてのフラグメントが受信されていることを確認するために検証されます。すべてのフラグメントが受信されると、パケットはフラグメントからアセンブリされ、新しく受信したメッセージとして処理されます。確認応答（ACK）メッセージは、元のパケットがアセンブリされると送信されます。各フラグメントには送信されません。

再送信

IKEv2 再送信は、IKEv2 再送信タイマーから求められた場合に発生します。一度構成され最初に送信されたフラグメントは、リスト化され、再送信タイマーがトリガーされた場合に再送信できるよう準備されます。再送信要求を受信すると、IKEv2 は応答を再送信します。この応答は、最初のフラグメント（#1）再送信が受信されると、再送信されます。残りのフラグメント番号は無視されるため、応答のより短時間での処理が可能になります。

フラグメンテーションの有効化

セキュリティ アソシエーション（SA）ごとにフラグメンテーションをグローバルに有効にするには、**crypto ikev2 fragmentation** コマンドを使用します。両方のピアが各ピアでの INIT 交換の後に IKE_AUTH 交換に使用されるフラグメンテーションのサポートを示している場合、フラグメンテーションは SA で有効になっています。

（注） このコマンドは、IKEv2 リモート アクセス ヘッドエンド機能によって導入され、変更されていません。

mtu *mtu-size* キーワード/引数のペアを使用して、最大伝送ユニット（MTU）をバイト単位で指定できます。MTU サイズは、IP または UDP カプセル化済みの IKEv2 パケットを示します。MTU の範囲は 68 ～ 1500 バイトです。デフォルトの MTU サイズは、IPv4 パケットでは 576 バイト、IPv6 パケットでは 1280 バイトです。

RFC 機能に準拠した IKE フラグメンテーションで有効な **crypto ikev2 fragmentation** コマンドは、次のように動作します。

- 将来の SA にのみ影響し、既存の古い SA には影響しません。

- シスコ独自のフラグメンテーション方式とIETF標準のフラグメンテーション方式をサポートします。

show crypto ikev2 sa detail コマンドにより、以下の情報が表示されます。

- ピアで有効なフラグメンテーション方式。有効なフラグメンテーション方式が IETF 標準のフラグメンテーションの場合、出力には使用中の MTU が表示されます。
- フラグメンテーションが両方のピアで有効になっているか、ローカル ピアでのみ有効になっているか。

IPv6 のサポート

RFC 機能に準拠した IKE フラグメンテーションでは、IETF 標準フラグメンテーション方式を使用している場合の、IPv6 IKE エンドポイントでの IPv6 パケットの断片化のサポートを追加しました。デフォルトの MTU 値は 1280 バイトであり、**crypto ikev2 fragmentation** コマンドでMTUが指定されていない場合に使用されます。フラグメンテーションで使用されるMTUは、**show crypto ikev2 sa detail** コマンドの出力に表示されます。

IKEv2 フラグメンテーションの設定方法

IKEv2 フラグメンテーションの設定

このタスクを実行して、大規模な IKEv2 パケットのラグメンテーションを有効にします。

手順の概要

1. **enable**
2. **configure terminal**
3. **crypto ikev2 fragmentation** [**mtu** *mtu-size*]
4. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 3	**crypto ikev2 fragmentation** [**mtu** *mtu-size*] 例： `Device(config)# crypto ikev2 fragmentation mtu 100`	IKEv2 フラグメンテーションを設定します。 • MTU の範囲は 96 ～ 1500 バイトです。デフォルトの MTU サイズは、IPv4 パケットでは 576 バイト、IPv6 パケットでは 1280 バイトです。 （注） MTU のサイズは、IP または UDP でカプセル化された IKEv2 パケットを示します。
ステップ 4	**end** 例： `Device(config)# end`	グローバル コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

IKEv2 フラグメンテーションの設定例

例：設定された MTU の表示が有効な IETF フラグメンテーション

次は、IETF 標準フラグメンテーション方式が有効であることを示すサンプル出力です。このステートメントは、応答側が IETF 標準フラグメンテーション方式もサポートしている場合に表示されます。また、出力には、使用中の MTU も表示されます。

```
Device# show crypto ikev2 sa detail

IPv4 Crypto IKEv2 SA

Tunnel-id Local Remote fvrf/ivrf Status
1 10.0.8.3/848 10.0.9.4/848 none/none IN-NEG
Encr: Unknown - 0, PRF: Unknown - 0, Hash: None, DH Grp:0, Auth sign: Unknown - 0, Auth
 verify: Unknown - 0
Life/Active Time: 86400/0 sec
CE id: 0, Session-id: 0
Status Description: Initiator waiting for INIT response
Local spi: 2CD1BEADB7C20854 Remote spi: 0000000000000000
Local id: 10.0.8.3
Remote id:
Local req msg id: 0 Remote req msg id: 0
Local next msg id: 1 Remote next msg id: 0
Local req queued: 0 Remote req queued: 0
Local window: 1 Remote window: 1
DPD configured for 0 seconds, retry 0
IETF Std Fragmentation enabled.
IETF Std Fragmentation MTU in use: 272 bytes.
Extended Authentication not configured.
NAT-T is not detected
Cisco Trust Security SGT is disabled
Initiator of SA : Yes

IPv6 Crypto IKEv2 SA
```

例：発信側で設定される IETF 標準フラグメンテーション方式

次は、発信側で設定されたIETF標準フラグメンテーション方式を表示するサンプル出力です。応答側はシスコ独自のフラグメンテーション方式をサポートしています。

```
Device# show crypto ikev2 sa detail

IPv4 Crypto IKEv2 SA

Tunnel-id Local Remote fvrf/ivrf Status
1 10.0.8.3/848 10.0.9.4/848 none/none READY
Encr: AES-CBC, keysize: 256, PRF: SHA512, Hash: SHA512, DH Grp:5, Auth sign: PSK, Auth
verify: PSK
Life/Active Time: 86400/59 sec
CE id: 1001, Session-id: 1
Status Description: Negotiation done
Local spi: 84350219051DB9E3 Remote spi: 52A8BB3898E8B5CF
Local id: 10.0.8.3
Remote id: 10.0.9.4
Local req msg id: 4 Remote req msg id: 0
Local next msg id: 4 Remote next msg id: 0
Local req queued: 4 Remote req queued: 0
Local window: 5 Remote window: 5
DPD configured for 0 seconds, retry 0
IETF Std Fragmentation configured.
Extended Authentication not configured.
NAT-T is not detected
Cisco Trust Security SGT is disabled
Initiator of SA : Yes

IPv6 Crypto IKEv2 SA
```

次は、応答側の設定を表示するサンプル出力です。この出力では、シスコ独自のフラグメンテーション方式が構成されていますが、有効ではない点に注意してください。

```
Device# show crypto ikev2 sa detail

IPv4 Crypto IKEv2 SA

Tunnel-id Local Remote fvrf/ivrf Status
1 10.0.9.4/848 10.0.8.3/848 none/none READY
Encr: AES-CBC, keysize: 256, PRF: SHA512, Hash: SHA512, DH Grp:5, Auth sign: PSK, Auth
verify: PSK
Life/Active Time: 86400/52 sec
CE id: 1001, Session-id: 1
Status Description: Negotiation done
Local spi: 52A8BB3898E8B5CF Remote spi: 84350219051DB9E3
Local id: 10.0.9.4
Remote id: 10.0.8.3
Local req msg id: 0 Remote req msg id: 4
Local next msg id: 0 Remote next msg id: 4
Local req queued: 0 Remote req queued: 4
Local window: 5 Remote window: 5
DPD configured for 0 seconds, retry 0
Fragmentation configured.
Extended Authentication not configured.
NAT-T is not detected
Cisco Trust Security SGT is disabled
Initiator of SA : No

IPv6 Crypto IKEv2 SA
```

次は、発信側がIETF標準フラグメンテーション方式をサポートし、応答側はフラグメンテーションをサポートしていない例を示します。この出力は、IETF標準フラグメンテーション方式が構成されていますが、有効ではないことを示す点に注意してください。

```
Device# show crypto ikev2 sa detail
IPv4 Crypto IKEv2 SA

Tunnel-id Local Remote fvrf/ivrf Status
1 10.0.8.3/848 10.0.9.4/848 none/none READY
Encr: AES-CBC, keysize: 256, PRF: SHA512, Hash: SHA512, DH Grp:5, Auth sign: PSK, Auth
verify: PSK
Life/Active Time: 86400/44 sec
CE id: 1004, Session-id: 2
Status Description: Negotiation done
Local spi: 03534703287D9CA1 Remote spi: 146E1CFA68008A92
Local id: 10.0.8.3
Remote id: 10.0.9.4
Local req msg id: 4 Remote req msg id: 0
Local next msg id: 4 Remote next msg id: 0
Local req queued: 4 Remote req queued: 0
Local window: 5 Remote window: 5
DPD configured for 0 seconds, retry 0
IETF Std Fragmentation configured.
Extended Authentication not configured.
NAT-T is not detected
Cisco Trust Security SGT is disabled
Initiator of SA : Yes
```

次は、応答側の設定を表示するサンプル出力です。ステートメント「Fragmentation not configured.」に注意してください。

```
Device# show crypto ikev2 sa detail
IPv4 Crypto IKEv2 SA

Tunnel-id Local Remote fvrf/ivrf Status
1 10.0.9.4/848 10.0.8.3/848 none/none READY
Encr: AES-CBC, keysize: 256, PRF: SHA512, Hash: SHA512, DH Grp:5, Auth sign: PSK, Auth
verify: PSK
Life/Active Time: 86400/23 sec
CE id: 1004, Session-id: 4
Status Description: Negotiation done
Local spi: 146E1CFA68008A92 Remote spi: 03534703287D9CA1
Local id: 10.0.9.4
Remote id: 10.0.8.3
Local req msg id: 0 Remote req msg id: 3
Local next msg id: 0 Remote next msg id: 3
Local req queued: 0 Remote req queued: 3
Local window: 5 Remote window: 5
DPD configured for 0 seconds, retry 0
Fragmentation not configured.
Extended Authentication not configured.
NAT-T is not detected
Cisco Trust Security SGT is disabled
Initiator of SA : No
```

例：発信側で設定されない IETF 標準フラグメンテーション方式

次は、発信側で設定されるフラグメンテーション方式が表示されないサンプル出力です。

```
Device# show crypto ikev2 sa detail

IPv4 Crypto IKEv2 SA

Tunnel-id Local Remote fvrf/ivrf Status
2 10.0.8.3/848 10.0.9.4/848 none/none DELETE
Encr: AES-CBC, keysize: 256, PRF: SHA512, Hash: SHA512, DH Grp:5, Auth sign: PSK, Auth
verify: PSK
Life/Active Time: 86400/28 sec
CE id: 1001, Session-id: 1
Status Description: Deleting IKE SA
Local spi: 1A375C00C1D157CF Remote spi: DB50F1BC58814FFA
Local id: 10.0.8.3
Remote id: 10.0.9.4
Local req msg id: 2 Remote req msg id: 4
Local next msg id: 4 Remote next msg id: 5
Local req queued: 2 Remote req queued: 4
Local window: 5 Remote window: 5
DPD configured for 0 seconds, retry 0
Fragmentation not configured.
Extended Authentication not configured.
NAT-T is not detected
Cisco Trust Security SGT is disabled
Initiator of SA : No

IPv6 Crypto IKEv2 SA
```

例：フラグメンテーションの IPv6 サポート

次の例は、FlexVPN エンドポイント（ハブとスポーク）のフラグメンテーションを示します。次は、パケットのフラグメント化に 1300 の最大伝送ユニット（MTU）を設定したハブに関連する設定です。

```
Device# show crypto ikev2 sa detail

IPv4 Crypto IKEv2 SA

IPv6 Crypto IKEv2 SA

Tunnel-id fvrf/ivrf Status
1 none/none READY
Local 4001::2000:3/500
Remote 4001::2000:1/500
Encr: AES-CBC, keysize: 256, PRF: SHA512, Hash: SHA512, DH Grp:5, Auth sign: PSK, Auth
verify: PSK
Life/Active Time: 86400/64 sec
CE id: 1001, Session-id: 1
Status Description: Negotiation done
Local spi: 45BA0D30D0EB5FFF Remote spi: 8D7B5A8389CEB8B3
Local id: R2.cisco.com
Remote id: R1.cisco.com
Local req msg id: 3 Remote req msg id: 0
Local next msg id: 3 Remote next msg id: 0
```

```
Local req queued: 3 Remote req queued: 0
Local window: 5 Remote window: 5
DPD configured for 0 seconds, retry 0
IETF Std Fragmentation enabled.
IETF Std Fragmentation MTU in use: 1272 bytes.
Extended Authentication not configured.
NAT-T is not detected
Cisco Trust Security SGT is disabled
Initiator of SA : Yes
Remote subnets:
10.0.0.251 255.255.255.255
IPv6 Remote subnets:
3001::/112
5001::/64
```

次は、デフォルトの MTU を設定したスポークに関連する設定です。

```
Device# show crypto ikev2 sa detail

IPv4 Crypto IKEv2 SA

IPv6 Crypto IKEv2 SA

Tunnel-id fvrf/ivrf Status
1 none/none READY
Local 4001::2000:1/500
Remote 4001::2000:3/500
Encr: AES-CBC, keysize: 256, PRF: SHA512, Hash: SHA512, DH Grp:5, Auth sign: PSK, Auth
verify: PSK
Life/Active Time: 86400/58 sec
CE id: 1001, Session-id: 1
Status Description: Negotiation done
Local spi: 8D7B5A8389CEB8B3 Remote spi: 45BA0D30D0EB5FFF
Local id: R1.cisco.com
Remote id: R2.cisco.com
Local req msg id: 0 Remote req msg id: 3
Local next msg id: 0 Remote next msg id: 3
Local req queued: 0 Remote req queued: 3
Local window: 5 Remote window: 5
DPD configured for 0 seconds, retry 0
IETF Std Fragmentation enabled.
IETF Std Fragmentation MTU in use: 1232 bytes.
Extended Authentication not configured.
NAT-T is not detected
Cisco Trust Security SGT is disabled
Initiator of SA : No
Remote subnets:
10.0.0.3 255.255.255.255
```

IKEv2 フラグメンテーションの設定に関する追加情報

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『Cisco IOS Master Command List, All Releases』

関連項目	マニュアル タイトル
セキュリティ コマンド	• 『Cisco IOS Security Command Reference Commands A to C』 • 『Cisco IOS Security Command Reference Commands D to L』 • 『Cisco IOS Security Command Reference Commands M to R』 • 『Cisco IOS Security Command Reference Commands S to Z』

標準および RFC

標準/RFC	タイトル
IKEv2 フラグメンテーション	*draft-ietf-ipsecme-ikev2-fragmentation-10*

シスコのテクニカル サポート

説明	リンク
右の URL にアクセスして、シスコのテクニカル サポートを最大限に活用してください。これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

IKEv2 フラグメンテーションの機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *280 : IKEv2* フラグメンテーションの機能情報

機能名	リリース	機能情報
RFC に準拠した IKEv2 フラグメンテーション		RFC機能に準拠したIKEフラグメンテーションでは、IETFの **draft-ietf-ipsecme-ikev2-fragmentation-10** ドキュメントの提案に従って、インターネットキーエクスチェンジバージョン 2 （IKEv2）パケットのフラグメンテーションを実装しました。 **show crypto ikev2 sa** コマンドが変更されました。

第 212 章

IKEv2 再接続の設定

AnyConnect 機能の AutoReconnect 機能の IOS IKEv2 サポートは、Cisco AnyConnect でユーザーが操作しない、IKEv2 ネゴシエーションの再確立に役立ちます。

IKEv2 再接続設定の前提条件

- <BypassDownloader> 値を true に設定して、AnyConnectLocalPolicy ファイルで BypassDownloader 関数を有効にする必要があります。デバイスで SSL がサポートされていない場合、BypassDownloader 関数は動作しないため、<BypassDownloader> 値を false に設定して、この関数を無効にする必要があります。そうしないと、接続が失敗します。

IKEv2 再接続設定の制限事項

- 事前供給キー認証方式は、インターネット キー エクスチェンジ バージョン 2（IKEv2）プロファイルでは設定できません。AnyConnect 機能の AutoReconnect 機能に対する IOS IKEv2 サポートでも事前共有キー認証方式を使用するため、同じ IKEv2 プロファイル上の事前共有キーの設定によって混乱が生じる可能性があります。
- **authentication local pre-share**、**authentication remote pre-share**、**keyring**、**aaa authorization group psk**、および **aaa authorization user psk** コマンドは、IKEv2 プロファイルでは設定できません。

設定された IKEv2 フラグメンテーションに関する情報

IKEv2 および Cisco AnyConnect クライアントの再接続機能

Cisco AnyConnect クライアントの自動再接続機能によって、Cisco AnyConnect VPN クライアントは一定の期間セッションを記憶し、セキュアなチャネルの確立後に接続を再開することができます。Cisco AnyConnect クライアントはインターネット キー エクスチェンジ バージョン 2（IKEv2）と共に幅広く使用されるため、IKEv2 では Cisco IOS ソフトウェアでの自動再接続機能のサポートを AnyConnect の自動再接続機能に対する IOS IKEv2 サポートにまで拡大しています。

Cisco AnyConnect クライアントでの自動再接続は、次のシナリオで発生します。

- 中間ネットワークがダウンしています。Cisco AnyConnect クライアントは、中間ネットワークがアップするとセッションを再開しようとします。
- Cisco AnyConnect クライアント デバイスは、ネットワーク間で切り替わります。これによって送信元 IP またはポートが変わり、既存のセキュリティ アソシエーション（SA）がダウンします。そのため、Cisco AnyConnect クライアントは自動再接続機能を使用して SA を再開しようとします。
- Cisco AnyConnect クライアント デバイスは、スリープまたは休止モードから復帰した後に SA を再開しようとします。

自動再接続機能を使用する利点

- 元のセッションで使用されるコピー属性は、認証、認可、およびアカウンティング（AAA）サーバーに問い合わせることなく再使用されます。
- Cisco IOS ゲートウェイは、クライアントに再接続するために RADIUS サーバーに接続する必要はありません。
- セッションの再開時に、認証または認可のためのユーザーインタラクションは必要ありません。
- セッションを再接続する場合、認証方式は事前共有キーです。この認証方式は、他の認証方式（Rivest、Shamir、および Adelman（RSA）署名認証方式、楕円曲線デジタル署名アルゴリズム（ECDSA）署名（ECDSA-sig）認証方式、および Extensible Authentication Protocol（EAP）認証方式を含む）に比べて時間がかかりません。事前共有キー認証方式では、最小限のリソースで IOS ソフトウェアでセッションを再開できます。
- これによって、未使用のセキュリティアソシエーション（SA）が削除され、暗号化リソースが解放されます。

自動再接続および DPD

Dead Peer Detection（DPD：デッドピア検出）は、ピアにクエリを送信することによって送信されるピアの可用性を確認するように設定されます。ピアから応答がない場合、そのピアのために作成されたセキュリティアソシエーションは削除されます。両方の設定シナリオで目的は同じため、DPD が FlexVPN サーバーで設定された場合に再接続プロファイルに DPD を設定す

る必要はありません。ただし、機能が有効な場合、DPD は IKEv2 でオンデマンド DPD としてキューイングされ、SA の削除時にプラットフォーム固有のハンドルも格納します。

Cisco IOS ゲートウェイと Cisco AnyConnect 間のメッセージ交換

Cisco AnyConnect クライアントは、セキュリティ アソシエーション（SA）を確立するために、Cisco IOS ゲートウェイに問い合わせます。認証または AUTH 交換（IKE_AUTH 要求の CFGMODE_REQ ペイロード）中、IKEv2 は、**reconnect** コマンドを使用して、AnyConnect 機能の自動再接続機能に対する IOS IKEv2 サポートが IKEv2 プロファイルで有効かどうかを確認します。また、選択された IKEv2 プロファイルの IKEv2 ポリシーを選択し、セッション ID とセッション トークン属性を、IKE_AUTH 応答の CFGMODE_REPLY ペイロードで Cisco AnyConnect クライアントに送信します。認証方式は、SA 用のクライアントと Cisco IOS ソフトウェア間の事前共有キーです。

IKEv2 は、Dead Peer Detection（DPD：デッドピア検出）メッセージを Cisco AnyConnect クライアントに定期的に送信して、クライアントがアクティブかどうかを確認します。Cisco AnyConnect クライアントは、Cisco IOS ゲートウェイがアクティブ クライアントとして解釈し、そのクライアントとセキュリティ アソシエーション（SA）を作成する、DPD メッセージに応答します。ただし、クライアントがデフォルトの再接続タイムアウト期間である 30 分以内に再接続されない場合、Cisco IOS ゲートウェイはそのクライアントが非アクティブであるとみなし、そのクライアントの SA を削除します。Cisco AnyConnect クライアントは、新しい接続を開始する必要があります。

show crypto ikev2 stats reconnect コマンドを使用して接続の統計情報を表示し、**clear crypto ikev2 session** コマンドを使用してクライアントとの SA を削除します。

IKEv2 再接続の設定方法

IKEv2 再接続の有効化

このタスクを実行して、AnyConnect 機能の AutoReconnect 機能の IOS IKEv2 サポートを有効にします。

手順の概要

1. **enable**
2. **configure terminal**
3. **crypto ikev2 profile** *profile-name*
4. **reconnect** [**timeout** *seconds*]
5. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**crypto ikev2 profile** *profile-name* 例： `Device(config)# crypto ikev2 profile profile1`	IKEv2 プロファイルを定義し、IKEv2 プロファイル コンフィギュレーション モードを開始します。
ステップ 4	**reconnect** [**timeout** *seconds*] 例： `Device(config-ikev2-profile)# reconnect timeout 900`	自動再接続機能の IKEv2 サポートを有効にします。
ステップ 5	**end** 例： `Device(config-ikev2-profile)# end`	IKEv2 プロファイル コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

IKEv2 再接続設定のトラブルシューティング

AnyConnect 機能設定の AutoReconnect 機能の IOS IKEv2 サポートを確認またはクリアするには、次のコマンドを使用します。

手順の概要

1. **enable**
2. **show crypto ikev2 stats reconnect**

手順の詳細

ステップ 1 **enable**

特権 EXEC モードを有効にします。

• パスワードを入力します（要求された場合）。

例：

```
Device> enable
```

ステップ 2 **show crypto ikev2 stats reconnect**

再接続の統計情報が表示されます。

例：

```
Device# show crypto ikev2 stats reconnect

Total incoming reconnect connection:        10
Success reconnect connection:               10
Failed reconnect connection:                0
Reconnect capable active session count:     4
Reconnect capable inactive session count:   6
```

IKEv2 再接続の設定例

例：IKEv2 再接続の有効化

次の例は、AnyConnect 機能の AutoReconnect 機能の IOS IKEv2 サポートを有効にする方法を示します。

```
Device> enable
Device# configure terminal
Device(config)# crypto ikev2 profile profile1
Device(config-ikev2-profile)# reconnect timeout 600
Device(config-ikev2-profile)# end
```

IKEv2 再接続の設定に関する追加情報

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『*Cisco IOS Master Command List, All Releases*』
セキュリティ コマンド	• 『*Cisco IOS Security Command Reference Commands A to C*』 • 『*Cisco IOS Security Command Reference Commands D to L*』 • 『*Cisco IOS Security Command Reference Commands M to R*』 • 『*Cisco IOS Security Command Reference Commands S to Z*』

関連項目	マニュアル タイトル
Cisco AnyConnect VPN クライアントに関する情報	『*Cisco AnyConnect VPN Client Administrator Guide, Release 2.4*』

シスコのテクニカル サポート

説明	リンク
右の URL にアクセスして、シスコのテクニカル サポートを最大限に活用してください。これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

IKEv2 再接続の機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *281 : IKEv2* 再接続の機能情報

機能名	リリース	機能情報
AnyConnect の AutoReconnect 機能の IOS IKEv2 サポート		AnyConnect 機能の AutoReconnect 機能の IOS IKEv2 サポートは、Cisco AnyConnect でユーザーが操作しない、IKEv2 ネゴシエーションの再確立に役立ちます。 次のコマンドが導入または変更されました。 **clear crypto ikev2 stats, reconnect, show crypto ikev2 stats.**

第 213 章

MPLS over FlexVPN の設定

最新版発行日：2014 年 3 月 28 日

MPLS over FlexVPN 機能では、マルチプロトコル ラベル スイッチング（MPLS）を動的に確立された IPSec トンネルの上に実装し、それによって重複したアドレス スペースをサポートします。

MPLS over FlexVPN の前提条件

- インターネット キー エクスチェンジ バージョン 2（IKEv2）および IPSec が設定されていること。
- MPLS が設定されていること。
- NHRP リダイレクトが設定されていること。

MPLS over FlexVPN の設定に関する情報

MPLS と FlexVPN

重複するアドレッシング スペースを持つネットワーク ドメインが、VPN ルーティングおよび転送（VRF）を使用してトラフィックを分離するため、あるドメイン用のデータは別のドメインに入力されなくなります。プロバイダーエッジ（PE）デバイス間のデータ セキュリティは、すべての VRF に IPSec 保護を使用するトンネル インターフェイスを定義することで実現されます。これによって、あらゆるドメインからのトラフィックが、対応する IPSec トンネルを通過するようになります。ただし、ドメインおよびノードのメンバーがネットワーク内で成長す

ると、すべての保護ドメインに個別の IPSec トンネルとインターフェイスが必要になるため、これではスケーラブルではなくなる可能性があります。

マルチプロトコル ラベル スイッチング（MPLS）が提供する機能は、VRF あたりまたはプレフィックスあたりでラベルを割り当て、データがルーティングする必要がある正確な VRF を特定します。これは、IPSec 保護と PE 間の単一の IPsec トンネルを持つ、単一の MPLS 認識型インターフェイスのみで実現できます。

MPLS over FlexVPN 機能が提供するソリューションは、Next Hop Resolution Protocol（NHRP）を使用してリモートのカスタマー ネットワークを動的に検出し、同時に IPsec を使用して PE デバイス間のデータ トラフィックを確保する必要がある場合、カスタマー ネットワーク内で重複するアドレス間の通信を実現します。お客様が MPLS ネットワークを導入し、その MPLS ネットワークを、セキュアな方法でインターネットを介して異なるリージョンに新しく設定したネットワーク（動的に判断される）に拡張する場合は、このソリューションを使用できます。

MPLS over FlexVPN ソリューションのコンポーネントは次のとおりです。

- IPSec：リモート スポークが動的に検出された後、スポークとハブの間、およびスポーク間のデータ トラフィックを確保します。
- インターネット キー エクスチェンジ バージョン 2（IKEv2）：静的ルートを、直接接続されたルートとして、ピアのトンネル オーバーレイ アドレスに追加します。このルートは、ピアのトンネル オーバーレイ アドレスのラベル情報ベース（LIB）に暗黙的な null ラベルを追加する結果になります。

（注） あらゆる LDP NAVER との TCP トンネルの確立に LDP が関係するため、IKEv2 は LDP の代わりに使用されます。LDP を有効化することで、LDP HELLO トラフィックによりスポーク間チャネルをアクティブにし続け、スポーク間チャネルが停止しないようにします。したがって、MPLS over FlexVPN 機能の設定時は、**mpls ip** コマンドをトンネルインターフェイスまたは仮想テンプレートで実行する必要があります。

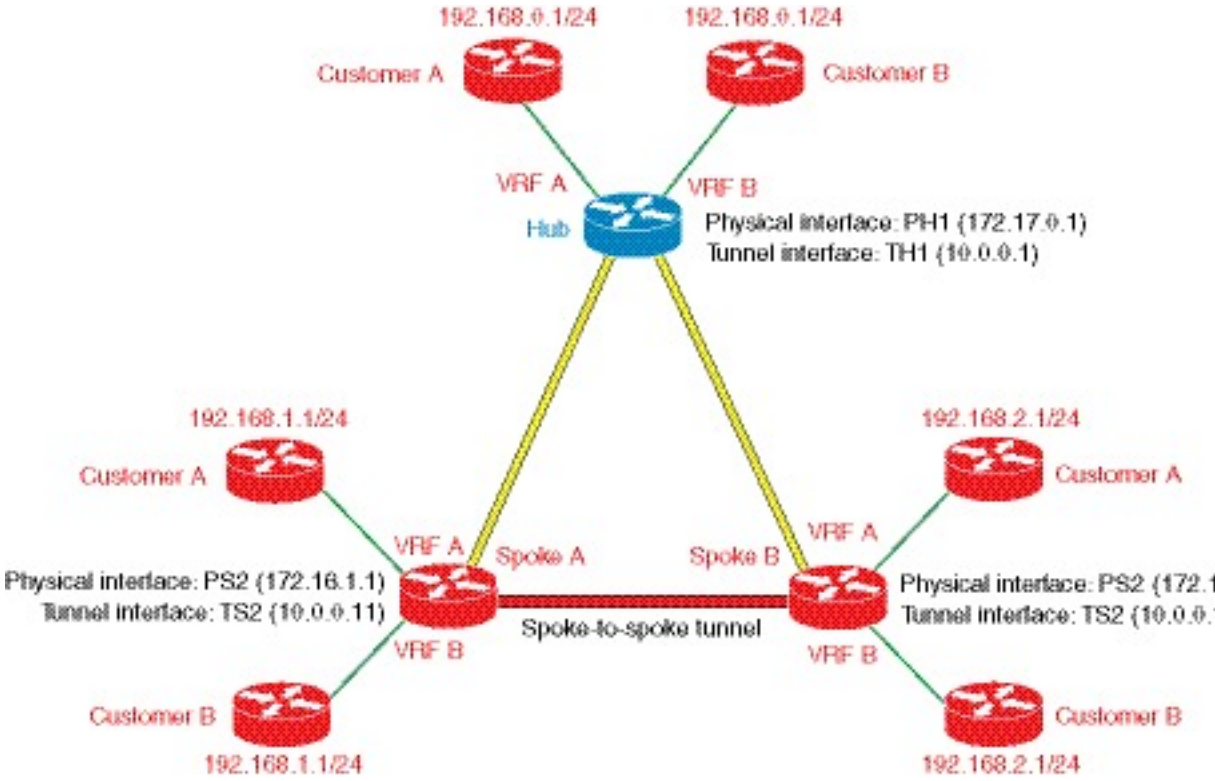
- NHRP：リモート オーバーレイ アドレスを解決し、セキュア トンネルの確立に必要なトランスポート エンド ポイントを動的に検出するために使用されます。multipoint Generic Routing Encapsulation（GRE）インターフェイスを使用する場合、トンネル エンド ポイント データベースに、オーバーレイと対応するノンブロードキャスト マルチアクセス（NBMA）アドレス間のマッピングを保存します。
- MPLS：データ パケットの MPLS タグ スイッチングを有効化します。LDP キープアライブはスポーク間のトンネルを維持し続けようとし、データ トラフィックが欠けた状態では望まれないため、デフォルトでは、Label Distribution Protocol（LDP：ラベル配布プロトコル）は有効ではなく、スポーク間でも有効ではありません。
- MPLS転送インフラストラクチャ（MFI）：アプリケーションによってラベルを割り当て、リリースします。NHRP は MFI と呼ばれるラベル管理用のアプリケーションです。

- Multiprotocol BGP（MP-BGP）：オーバーレイ ラベルを異なる VRF のネットワークに分散します。

MPLS over FlexVPN の作業

次の図と記述は、MPLS over FlexVPN ソリューションの作業を説明します。

図 *110*：スポーク～ハブ～スポークのトポロジ



MPLS over FlexVPN ソリューションには、次の前提条件があります。

- Multiprotocol BGP（MP-BGP）では、VPN ルーティングおよび転送（VRF）あたりまたはプレフィックスあたりでラベルを配布できます。
- ラベル 10 は、Hub から Spoke A に着信するパケット用 VRF A に割り当てられます。
- ラベル 20 は、Hub から Spoke B に着信するパケット用 VRF A に割り当てられます。
- ラベル 30 は、Spoke A から Hub に着信するパケット用 Hub の VRF A に割り当てられます。
- ラベル 40 は、Spoke B から Hub に着信するパケット用 Hub の VRF B に割り当てられます。

1. IKEv2 と IPSec のセキュリティ アソシエーションは、各スポークからハブに確立されます。IKEv2 は、モード構成応答とモード構成セットで受信される、スポークのオーバーレイ アドレスに対して暗黙的 NULL ラベル値をインストールします。

（注） スポークとハブは、いつでもオーバーレイ スペースで相互にネクストホップになるため、暗黙的 NULL ラベルがインストールされます。

2. MP-BGP は、VRF あたりのラベルまたはプレフィックスあたりのラベルを、すべての VRF と交換します。
3. ラベルとルートが交換された後は、データの転送が開始されます。192.168.2.1 宛ての最初のデータ パケットは、VRF A の Spoke A に到着すると、ハブに転送されます。パケットは Generic Routing Encapsulation（GRE）を使用してラベル カプセル化されますが、含まれるのはオーバーレイ ラベルのみであり、暗号化されます。
4. データ パケットは、物理（仮想アクセス）インターフェイス（172.17.0.1）またはトンネル インターフェイス（10.0.0.1）のハブに到着すると、複合化されます。オーバーレイ ラベルがハブ内で検索され、パケットは GRE を使用してカプセル化され、暗号化されて Spoke B に送信されます。
5. NHRP リダイレクト パケットはハブから Spoke A に送信されます。ラベル 30 はデータ パケットが到着する VRF を示すように、VRF 情報は NHRP に伝達されます。
6. NHRP はリダイレクト パケットを処理し、NHRP 解決要求をトリガーします。NHRP マッピング エントリが作成され、VRF A が解決される必要があるプレフィックスに関連付けられます。
7. 解決要求はハブに送信されます。そこではオーバーレイ ラベルが検索され、解決要求は適切な宛先、この場合は Spoke B に送信されます。
8. NHRP 解決要求は Spoke B に到達し、Spoke B の仮想アクセス インターフェイスまたはマルチポイント GRE（mGRE）インターフェイスを作成します。
9. IKEv2 と IPSec のセッションは、Spoke B から Spoke A に開始され、Spoke A の仮想アクセス インターフェイスまたは mGRE インターフェイスが作成されます。NHRP では、新しく作成された仮想アクセス インターフェイスを経由する Spoke A トンネルの IP アドレスへのルートが追加されます。
10. Spoke B からの NHRP 解決応答には、スポーク間トンネル経由でデータを送信するために Spoke A が使用できるラベル値が含まれます。このため、NHRP は、MPLS 転送インスタンス（MFI）からラベルを割り当て、このラベル情報をスポーク間トンネルに使用する Spoke A に送信します。

（注） MFI はラベルを追跡します。ラベルがすでに割り当て済みで、特定の VRF の MP-BGP に指定されている場合、このラベルは NHRP に返されます。MFI はこの特定のラベルを使用してアプリケーションの数を追跡し、すべてのアプリケーションにラベルがリリースされている場合のみ、このラベルをプールに戻します。

11. また、NHRP 解決応答には、Spoke B の仮想アクセス インターフェイスまたは mGRE インターフェイスの IP アドレス用の暗黙的 NULL ラベルが含まれます。この例では、応答は「192.168.2.0/24, label 40, 10.0.0.12, 172.16.2.1, [implicit-NULL]」になります。

12. NHRP 解決応答は、Spoke A の仮想アクセス インターフェイスまたは mGRE インターフェイスで受信されます。応答パケット内の NHRP 要求 ID は、Spoke A によって最初に送信された要求の要求 ID と照合され、要求が送信される VRF が取得されます。NHRP キャッシュで NHRP エントリが検索され、このエントリは「Complete」と呼ばれます。NHRP は、ラベル情報がある VRF ルーティング テーブルにルートを挿入します。
13. Spoke A と Spoke B の間にルートとラベルが設定されます。データはここでラベル カプセル化され、スポーク間で動的に確立された Spoke A と Spoke B の間のトンネルを経由して暗号化されます。

FlexVPN の IVRF サポート

FlexVPN の VPN ルーティングおよび転送（IVRF）サポートでは、トンネル インターフェイスの IVRF 設定で、次の NHRP ルーティング操作を実行する機能が提供されます。

- ルート ルックアップの実行後に、NHRP 解決要求を送信する。
- ハブの NHRP 解決要求を転送する。
- ショートカット トンネルの作成時に、IVRF での H ルートまたはネクストホップ上書き（NHO）を作成する。
- ショートカット トンネルの削除時に、IVRF から H ルートまたは NHO を削除する。

MPLS over FlexVPN の設定方法

MPLS over FlexVPN の設定

このタスクを実行して、MPLS over FlexVPN を設定します。

手順の概要

1. **enable**
2. **configure terminal**
3. **interface tunnel** *number*
4. **mpls nhrp**
5. **end**
6. **show mpls forwarding-table**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。

	コマンドまたはアクション	目的
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface tunnel** *number* 例： `Device(config)# interface tunnel 1`	FlexVPN クライアント インターフェイスを設定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	**mpls nhrp** 例： `Device(config-if)# mpls nhrp`	Label Distribution Protocol（LDP：ラベル配布プロトコル）は有効にせず、MPLS タグ スイッチングを有効にします。
ステップ 5	**end** 例： `Device(config-if)# end`	インターフェイス コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードに戻ります。
ステップ 6	**show mpls forwarding-table** 例： `Device# show mpls forwarding-table`	マルチプロトコル ラベル スイッチング（MPLS）のラベル転送情報ベース（LFIB）に関する情報が表示されます。

MPLS over FlexVPN の設定例

例：MPLS over FlexVPN の設定

次の例は、MPLS 機能を利用して FlexVPN で複数のカスタマー VRF を転送する方法を示します。次は、spoke 1 の設定です。

```
hostname R3-Spoke1
boot-start-marker
boot-end-marker
!
!
vrf definition cust1
 rd 1:1
 route-target export 1:1
 route-target import 1:1
 !
 address-family ipv4
 exit-address-family
!
vrf definition cust2
 rd 2:2
 route-target export 2:2
 route-target import 2:2
 !
 address-family ipv4
 exit-address-family
```

```
!
clock timezone CET 1 0
!
no ip domain lookup
ip domain name cisco.com
ip cef
no ipv6 cef
mpls ldp loop-detection
!
crypto pki trustpoint CA
 enrollment url http://172.16.1.1:80
 password
 fingerprint E0AFEFD7F08070BAB33C8297C97E6457
 subject-name cn=R3-spoke.cisco.com,OU=FLEX,O=Cisco
 revocation-check crl none
!
crypto pki certificate map mymap 10
 subject-name co ou = flex
!
crypto pki certificate chain CA
 certificate 03
 certificate ca 01
crypto ikev2 authorization policy default
 route set interface
!
crypto ikev2 profile default
 match certificate mymap
 identity local fqdn R3-Spoke.cisco.com
 authentication local rsa-sig
 authentication remote rsa-sig
 pki trustpoint CA
 dpd 60 2 on-demand
 aaa authorization group cert list default default
!
!
!
!
crypto ipsec profile default
 set ikev2-profile default
!
!
!
!
!
!
interface Tunnel0
 ip address negotiated
 mpls bgp forwarding
 tunnel source Ethernet0/0
 tunnel destination 172.16.0.1
 tunnel protection ipsec profile default
!
interface Ethernet0/0
 description WAN
 ip address 172.16.1.103 255.255.255.0
!
interface Ethernet0/1
 description LAN
 no ip address
 no ip unreachables
!
interface Ethernet0/1.10
 encapsulation dot1Q 10
 vrf forwarding cust1
```

```
 ip address 192.168.113.1 255.255.255.0
!
interface Ethernet0/1.20
 encapsulation dot1Q 20
 vrf forwarding cust2
 ip address 192.168.123.1 255.255.255.0
!
router bgp 100
 bgp log-neighbor-changes
 neighbor 10.0.0.1 remote-as 10
 neighbor 10.0.0.1 ebgp-multihop 255
 neighbor 10.0.0.1 update-source Tunnel0
 !
 address-family ipv4
  neighbor 10.0.0.1 activate
 exit-address-family
 !
 address-family vpnv4
  neighbor 10.0.0.1 activate
  neighbor 10.0.0.1 send-community both
 exit-address-family
 !
 address-family ipv4 vrf cust1
  redistribute connected
 exit-address-family
 !
 address-family ipv4 vrf cust2
  redistribute connected
 exit-address-family
!
ip route 10.0.0.1 255.255.255.255 Tunnel0 name workaround
ip route 172.16.0.1 255.255.255.255 172.16.1.1 name FlexHUB
```

次は、 spoke 2 の設定です。

```
hostname R4-Spoke
!
vrf definition cust1
 rd 1:1
 route-target export 1:1
 route-target import 1:1
 !
 address-family ipv4
 exit-address-family
!
vrf definition cust2
 rd 2:2
 route-target export 2:2
 route-target import 2:2
 !
 address-family ipv4
 exit-address-family
!
clock timezone CET 1 0
!
no ip domain lookup
ip domain name cisco.com
ip cef
no ipv6 cef
!
crypto pki token default removal timeout 0
!
crypto pki trustpoint CA
 enrollment url http://172.16.1.1:80
 password
```

```
 fingerprint E0AFEFD7F08070BAB33C8297C97E6457
 subject-name cn=R4-Spoke.cisco.com,OU=Flex,O=Cisco
 revocation-check crl none
!
crypto pki certificate map mymap 10
 subject-name co ou = flex
!
crypto pki certificate chain CA
 certificate 04
 certificate ca 01
!
crypto ikev2 authorization policy default
 route set interface
!
crypto ikev2 profile default
 match certificate mymap
 identity local fqdn R4.cisco.com
 authentication local rsa-sig
 authentication remote rsa-sig
 pki trustpoint CA
 dpd 60 2 on-demand
 aaa authorization group cert list default default
 virtual-template 1
!
crypto ipsec profile default
 set ikev2-profile default
!
interface Loopback100
 vrf forwarding cust1
 ip address 192.168.114.1 255.255.255.0
!
interface Loopback101
 vrf forwarding cust2
 ip address 192.168.124.1 255.255.255.0
!
interface Tunnel0
 ip address negotiated
 mpls bgp forwarding
 tunnel source Ethernet0/0
 tunnel destination 172.16.0.1
 tunnel protection ipsec profile default
!
interface Ethernet0/0
 description WAN
 ip address 172.16.1.104 255.255.255.0
!
interface Ethernet0/1
 description LAN
 ip address 192.168.104.1 255.255.255.0
!
router bgp 100
 bgp log-neighbor-changes
 neighbor 10.0.0.1 remote-as 10
 neighbor 10.0.0.1 ebgp-multihop 255
 neighbor 10.0.0.1 update-source Tunnel0
 !
 address-family ipv4
  neighbor 10.0.0.1 activate
 exit-address-family
 !
 address-family vpnv4
  neighbor 10.0.0.1 activate
  neighbor 10.0.0.1 send-community both
 exit-address-family
```

```
 !
 address-family ipv4 vrf cust1
  redistribute connected
 exit-address-family
 !
 address-family ipv4 vrf cust2
  redistribute connected
 exit-address-family
!
ip route 10.0.0.1 255.255.255.255 Tunnel0
ip route 172.16.0.1 255.255.255.255 172.16.1.1 name FlexHUB
```

次は、ハブの設定です。

```
hostname R1-HUB
aaa new-model
!
!
aaa authorization network default local
!
!
clock timezone CET 1 0
!
ip vrf cust1
 rd 1:1
 route-target export 1:1
 route-target import 1:1
!
ip vrf cust2
 rd 2:2
 route-target export 2:2
 route-target import 2:2
!
no ip domain lookup
ip domain name cisco.com
ip cef
no ipv6 cef
!
multilink bundle-name authenticated
mpls ldp loop-detection
!
crypto pki trustpoint CA
 enrollment url http://172.16.0.2:80
 password
 fingerprint E0AFEFD7F08070BAB33C8297C97E6457
 subject-name CN=R1-HUB.cisco.com,OU=FLEX,OU=VPN,O=Cisco Systems,C=US,L=Linux
 revocation-check crl none
 rsakeypair R1-HUB.cisco.com 2048
 auto-enroll 95
!
!
crypto pki certificate chain CA
 certificate 02
 certificate ca 01
!
redundancy
!
!
!
crypto ikev2 authorization policy default
 pool mypool
 banner ^C Welcome ^C
 def-domain cisco.com
!
!
```

```
!
!
crypto ikev2 profile default
 match identity remote fqdn domain cisco.com
 identity local dn
 authentication local rsa-sig
 authentication remote rsa-sig
 pki trustpoint CA
 dpd 60 2 on-demand
 aaa authorization group cert list default default
 virtual-template 1
!

crypto ipsec profile default
 set ikev2-profile default
!
!
!
!
!
!
interface Loopback0
 description VT source interface
 ip address 10.0.0.1 255.255.255.255
!
interface Ethernet0/0
 description WAN
 ip address 172.16.0.1 255.255.255.252
!
interface Ethernet0/1
 description LAN
 ip address 192.168.100.1 255.255.255.0
!
interface Ethernet0/2
 ip vrf forwarding cust1
 ip address 192.168.110.1 255.255.255.0
!
interface Ethernet0/3
 ip vrf forwarding cust2
 ip address 192.168.111.1 255.255.255.0
!
interface Virtual-Template1 type tunnel
 ip unnumbered Loopback0
 ip nhrp network-id 1
 ip nhrp redirect
 mpls bgp forwarding
 tunnel protection ipsec profile default
!
router bgp 10
 bgp log-neighbor-changes
 bgp listen range 0.0.0.0/0 peer-group mpls
 bgp listen limit 5000
 neighbor mpls peer-group
 neighbor mpls remote-as 100
 neighbor mpls transport connection-mode passive
 neighbor mpls update-source Loopback0
 !
 address-family ipv4
  redistribute static route-map global
  neighbor mpls activate
  neighbor mpls next-hop-self
 exit-address-family
 !
 address-family vpnv4
```

```
 neighbor mpls activate
 neighbor mpls send-community both
exit-address-family
!
address-family ipv4 vrf cust1
 redistribute connected
 redistribute static route-map cust1
 default-information originate
exit-address-family
!
address-family ipv4 vrf cust2
 redistribute connected
 redistribute static route-map cust2
 default-information originate
exit-address-family
!
ip local pool mypool 10.1.1.1 10.1.1.254
ip forward-protocol nd
!
!
no ip http server
no ip http secure-server
ip route 0.0.0.0 0.0.0.0 172.16.0.2 name route_to_internet
ip route vrf cust1 0.0.0.0 0.0.0.0 Null0 tag 666 name default_originate
ip route vrf cust2 0.0.0.0 0.0.0.0 Null0 tag 667 name default_originate
!
route-map cust1 permit 10
 match tag 666
!
route-map cust2 permit 10
 match tag 667
```

次は、スポークからのサンプル出力です。

```
Device# show ip cef vrf cust1 192.168.110.1

192.168.110.0/24, epoch 0, flags rib defined all labels, RIB[B], refcount 5,
per-destination sharing
  sources: RIB
  feature space:
   IPRM: 0x00018000
   LFD: 192.168.110.0/24 0 local labels
        contains path extension list
  ifnums: (none)
  path EF36CA28, path list EF36DEB4, share 1/1, type recursive, for IPv4, flags
must-be-labelled
    MPLS short path extensions: MOI flags = 0x0 label 19
  recursive via 10.0.0.1[IPv4:Default] label 19, fib F0C5926C, 1 terminal fib,
v4:Default:10.0.0.1/32
    path EF36CBE8, path list EF36DFF4, share 1/1, type attached host, for IPv4
      MPLS short path extensions: MOI flags = 0x1 label implicit-null
    attached to Tunnel0, adjacency IP midchain out of Tunnel0 F0481718
  output chain: label 19 label implicit-null TAG midchain out of Tunnel0 F1D97A90 IP adj
 out of Ethernet0/0, addr 172.16.1.1 F0481848
R4-Spoke#sh ip bgp vpnv4 all label
   Network          Next Hop      In label/Out label
Route Distinguisher: 1:1 (cust1)
   0.0.0.0          10.0.0.1        nolabel/18
   192.168.110.0    10.0.0.1        nolabel/19
   192.168.114.0    0.0.0.0         16/nolabel(cust1)
Route Distinguisher: 2:2 (cust2)
   0.0.0.0          10.0.0.1        nolabel/20
   192.168.111.0    10.0.0.1        nolabel/21
   192.168.124.0    0.0.0.0         17/nolabel(cust2)
```

次は、ハブからのサンプル出力です。

```
Device# show ip cef vrf cust1 192.168.113.1

192.168.113.0/24, epoch 0, flags rib defined all labels, RIB[B], refcount 5,
per-destination sharing
  sources: RIB, LTE
  feature space:
   IPRM: 0x00018000
   LFD: 192.168.113.0/24 1 local label
   local label info: other/25
        contains path extension list
        disposition chain 0xF1E1D9B0
        label switch chain 0xF1E1D9B0
  ifnums: (none)
  path F16ECA10, path list F16EDFBC, share 1/1, type recursive, for IPv4, flags
must-be-labelled
    MPLS short path extensions: MOI flags = 0x0 label 16
  recursive via 10.1.1.3[IPv4:Default] label 16, fib F0CCD6E8, 1 terminal fib,
v4:Default:10.1.1.3/32
    path F16ECE00, path list F16EE28C, share 1/1, type attached host, for IPv4
      MPLS short path extensions: MOI flags = 0x1 label implicit-null
    attached to Virtual-Access1, adjacency IP midchain out of Virtual-Access1 F04F35D8
 output chain: label 16 label implicit-null TAG midchain out of Virtual-Access1 F1E1DF60
 IP adj out of Ethernet0/0, addr 172.16.0.2 F04F3708
R1-HUB#sh ip bgp vpnv4 all
BGP table version is 49, local router ID is 10.0.0.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale, m multipath, b backup-path, x best-external, f
RT-Filter, a additional-path
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop            Metric LocPrf Weight Path
Route Distinguisher: 1:1 (default for vrf cust1)
*> 0.0.0.0          0.0.0.0                  0         32768 ?
*> 192.168.110.0    0.0.0.0                  0         32768 ?
*> 192.168.113.0    10.1.1.3                 0             0 100 ?
*> 192.168.114.0    10.1.1.4                 0             0 100 ?
Route Distinguisher: 2:2 (default for vrf cust2)
*> 0.0.0.0          0.0.0.0                  0         32768 ?
*> 192.168.111.0    0.0.0.0                  0         32768 ?
*> 192.168.123.0    10.1.1.3                 0             0 100 ?
*> 192.168.124.0    10.1.1.4                 0             0 100 ?
Device# show ip bgp vpnv4 all 192.168.113.1

BGP routing table entry for 1:1:192.168.113.0/24, version 48
Paths: (1 available, best #1, table cust1)
  Advertised to update-groups:
     3
  Refresh Epoch 1
  100
    10.1.1.3 from *10.1.1.3 (172.16.1.103)
      Origin incomplete, metric 0, localpref 100, valid, external, best
      Extended Community: RT:1:1
      mpls labels in/out 25/16
BGP routing table entry for 2:2:0.0.0.0/0, version 8
Paths: (1 available, best #1, table cust2)
  Advertised to update-groups:
     3
  Refresh Epoch 1
  Local
    0.0.0.0 from 0.0.0.0 (10.0.0.1)
      Origin incomplete, metric 0, localpref 100, weight 32768, valid, sourced, best
```

```
Extended Community: RT:2:2
mpls labels in/out 20/aggregate(cust2)
```

MPLS over FlexVPN の設定に関する追加情報

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『Cisco IOS Master Command List, All Releases』
セキュリティ コマンド	• 『Cisco IOS Security Command Reference Commands A to C』 • 『Cisco IOS Security Command Reference Commands D to L』 • 『Cisco IOS Security Command Reference Commands M to R』 • 『Cisco IOS Security Command Reference Commands S to Z』
推奨される暗号化アルゴリズム	『Next Generation Encryption』

標準および RFC

標準/RFC	タイトル
RFC 5586	*MPLS Generic Associated Channel*

シスコのテクニカル サポート

説明	リンク
右の URL にアクセスして、シスコのテクニカル サポートを最大限に活用してください。これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

MPLS over FlexVPN の設定の機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *282 : MPLS over FlexVPN* の設定の機能情報

機能名	リリース	機能情報
MPLS over FlexVPN		次のコマンドが導入または変更されました。 **clear ip nhrp, clear ipv6 nhrp, mpls nhrp, show dmvpn, show ip nhrp, show ipv6 nhrp.**

第 214 章

IKEv2パケットオブディスコネクトの設定

IKEv2 リモート アクセス認可変更（CoA）のパケット オブ ディスコネクト機能は、シスコがサポートするデバイスのアクティブな暗号 IKEv2 セッションを停止します。

IKEv2 パケット オブ ディスコネクトに関する情報

切断要求

パケット オブ ディスコネクト（POD）は、RADIUS disconnect_request パケットで、認証エージェント サーバーで暗号化セッションを切断する必要がある場合に使用することを目的としています。

POD が必要な場合

パケット オブ ディスコネクトは、次の状況で必要になります。

- 再認証の実行：セッションが非常に長い期間接続されている場合、ネットワーク管理者として、FlexVPN サーバー上のユーザーを解除して強制的に再認証する必要がある場合があります。
- 新しいポリシーの適用：クライアントが再接続する場合、ネットワーク管理者として、アクティブな暗号化セッションを終了して新しいポリシーをセッションに適用する必要がある場合があります。
- リソースの解放：セッションを終了して、リソースを解放し、キー再生成を終了する必要がある場合があります。

IKEv2 パケット オブ ディスコネクト

IKEv2 リモート アクセスの認可変更（CoA）：パケット オブ ディスコネクト機能は、RADIUS パケット オブ ディスコネクト（POD）機能を使用して暗号化セッションを削除します。暗号化セッションは、VPN ユーザーを AAA サーバーの新しいユーザー ポリシーまたはグループ ポリシーに更新するために削除されます。

1. AAA は、RADIUS サーバーから提供される属性キー/値ペアのリストを IKEv2 に渡します。
2. IKEv2 はリストを解析して、キーとして監査セッション ID、Cisco AV ペアを検索し、ペア値を確認します。
3. IKEv2 はセッションを検索し、特定のセッションを削除します。
4. IKEv2 は AAA に通知し、AAA は RADIUS サーバーに通知します。
5. 監査セッション ID に関係するセッションは削除されます。

IKEv2 パケット オブ ディスコネクトのパラメータ

RFC 3576 は、IKEv2 パケット オブ ディスコネクトをサポートする次の POD コードを指定します。

- 40：切断要求
- 41：切断 ACK
- 42：切断 NAK

切断 ACK コードは、監査セッション ID 用にセッションが存在し、監査セッション ID に関係するセッションが正常に終了されたことを示します。切断 NACK コードは、監査セッション ID に対応するセッションがないことを示します。ゲートウェイに応答メッセージは送信されません。

IKEv2 パケット オブ ディスコネクトの設定方法

FlexVPN サーバーでの AAA の設定

IKEv2 リモート アクセス認可変更（CoA）のパケット オブ ディスコネクト機能に対して、FlexVPN サーバーに必要な IKEv2 独自の設定はありません。FlexVPN サーバーでは、認可、およびアカウンティング（AAA）のみを設定する必要があります。AAA の設定の詳細については、『』を参照してください。

手順の概要

1. **enable**
2. **configure terminal**

3. **aaa new-model**
4. **aaa server radius dynamic-author**
5. **client** {*hostname* | *ip-address*} [**server-key** *string* | **vrf** *vrf-id*]
6. **port** *number*
7. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**aaa new-model** 例： `Device(config)# aaa new-model`	AAA をグローバルに有効にします。
ステップ 4	**aaa server radius dynamic-author** 例：	ローカル AAA サーバーでダイナミック認証サービスを設定し、ダイナミック認証ローカル サーバー コンフィギュレーション モードを開始します。 • このモードでは、RADIUS アプリケーション コマンドが設定されます。
ステップ 5	**client** {*hostname* | *ip-address*} [**server-key** *string* | **vrf** *vrf-id*] 例： `Device(config-locsvr-da-radius)# client 192.168.0.5 server-key cisco`	AAA サーバー クライアントの IP アドレスまたはホスト名を設定します。 • **server-key** キーワードと *string* 引数を使用して、クライアント レベルのサーバー キーを設定します。 （注） クライアント レベルでサーバー キーを設定すると、グローバル レベルで設定されたサーバー キーが上書きされます。
ステップ 6	**port** *number* 例： `Device(config-locsvr-da-radius)# port 1812`	UDP ポートを設定します。
ステップ 7	**end** 例： `Device(config-locsvr-da-radius)# end`	ダイナミック認証ローカル サーバー コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

IKEv2 パケット オブ ディスコネクトの設定例

例：IKEv2 セッションの終了

次に、**show aaa sessions** コマンドの出力例を示します。終了する IKEv2 セッションを特定するには、このコマンドを実行する必要があります。

```
Device# show aaa sessions

Total sessions since last reload: 32
Session Id: 3
   Unique Id: 14
   User Name: *not available*
   IP Address: 0.0.0.0
   Idle Time: 0
   CT Call Handle: 0
Session Id: 30
   Unique Id: 41
   User Name: pskuser2.g1.engdt.com
   IP Address: 0.0.0.0
   Idle Time: 0
   CT Call Handle: 0
Session Id: 32
   Unique Id: 43
   User Name: pskuser4.g2.engdt.com
   IP Address: 0.0.0.0
   Idle Time: 0
   CT Call Handle: 0
```

上記の出力では、ID 41 および 43 が IKEv2 セッションに関するものです。必要に応じて、**show aaa user** コマンドを実行して、セッションの詳細な情報を表示することができます。

```
Device# show aaa user 41

Unique id 41 is currently in use.
  No data for type 0
  No data for type EXEC
  No data for type CONN
  NET: Username=(n/a)
    Session Id=0000001E Unique Id=00000029
    Start Sent=0 Stop Only=N
    stop_has_been_sent=N
    Method List=0
    Attribute list:
      7FBD9783CCF0 0 00000001 session-id(408) 4 30(1E)
      7FBD9783CD30 0 00000001 start_time(418) 4 Nov 04 2014 00:20:23
--------
  No data for type CMD
  No data for type SYSTEM
  No data for type VRRS
  No data for type RM CALL
  No data for type RM VPDN
  No data for type AUTH PROXY
  No data for type DOT1X
  No data for type CALL
```

```
  No data for type VPDN-TUNNEL
  No data for type VPDN-TUNNEL-LINK
  IPSEC-TUNNEL: Username=pskuser2.g1.engdt.com
    Session Id=0000001E Unique Id=00000029
    Start Sent=1 Stop Only=N
    stop_has_been_sent=N
    Method List=7FBDA6E05A68 : Name = accnt_prof
    Attribute list:
      7FBD9783CCF0 0 00000001 session-id(408) 4 30(1E)
      7FBD9783CD30 0 00000001 start_time(418) 4 Nov 04 2014 00:20:23
      7FBD9783CD70 0 00000082 formatted-clid(37) 13 192.168.202.2
      7FBD9783CDB0 0 0000008A audit-session-id(819) 37
L2L433010101ZO2L4C0A8CA02ZH119404ZP37
      7FBD9783CDF0 0 00000081 isakmp-phase1-id(737) 21 pskuser2.g1.engdt.com
      7FBD9783BF80 0 00000002 isakmp-initator-ip(738) 4 192.168.202.2
--------
  No data for type MCAST
  No data for type RESOURCE
  No data for type SSG
  No data for type IDENTITY
  No data for type ConnectedApps
Accounting:
  log=0x400018041
  Events recorded :
    CALL START
    ATTR REPLACE
    INTERIM START
    INTERIM STOP
    IPSEC TNL UP
  update method(s) :
    NONE
  update interval = 0
  Outstanding Stop Records : 0
  Dynamic attribute list:
    7FBD9783BF80 0 00000001 connect-progress(75) 4 No Progress
    7FBD9783BFC0 0 00000001 pre-session-time(334) 4 0(0)
    7FBD9783C000 0 00000001 elapsed_time(414) 4 341(155)
    7FBD9783C040 0 00000001 bytes_in(146) 4 0(0)
    7FBD9783C080 0 00000001 bytes_out(311) 4 0(0)
    7FBD9783CCF0 0 00000001 pre-bytes-in(330) 4 0(0)
    7FBD9783CD30 0 00000001 pre-bytes-out(331) 4 0(0)
    7FBD9783CD70 0 00000001 paks_in(147) 4 0(0)
    7FBD9783CDB0 0 00000001 paks_out(312) 4 0(0)
    7FBD9783CDF0 0 00000001 pre-paks-in(332) 4 0(0)
    7FBD9783BA20 0 00000001 pre-paks-out(333) 4 0(0)
Debg: No data available
Radi: No data available
Interface:
  TTY Num = -1
  Stop Received = 0
  Byte/Packet Counts till Call Start:
    Start Bytes In = 0             Start Bytes Out = 0
    Start Paks  In = 0             Start Paks  Out = 0
  Byte/Packet Counts till Service Up:
    Pre Bytes In = 0             Pre Bytes Out = 0
    Pre Paks  In = 0             Pre Paks  Out = 0
  Cumulative Byte/Packet Counts :
    Bytes In = 0             Bytes Out = 0
    Paks  In = 0             Paks  Out = 0
  StartTime = 00:20:23 IST Nov 4 2014
  AuthenTime = 00:20:23 IST Nov 4 2014
  Component = VPN IPSEC
Authen: service=NONE type=NONE method=NONE
Kerb: No data available
```

```
Meth: No data available
Preauth: No Preauth data.
General:
  Unique Id = 00000029
  Session Id = 0000001E
  Session Server Key = 1771D693
  Attribute List:
PerU: No data available
Service Profile: No Service Profile data.
Unkn: No data available
Unkn: No data available
```

上記の出力では、audit-session-id、L2L433010101ZO2L4C0A8CA02ZH119404ZP37 に注意してください。次の出力例は、RADIUS サーバーで開始されるアカウンティング セッションの開始時に、FlexVPN サーバーに表示されます。

```
Nov  4 00:26:49.908 IST: RADIUS/ENCODE: Best Local IP-Address 192.168.202.1 for
Radius-Server 9.45.15.144
Nov  4 00:26:49.908 IST: RADIUS(0000002C): Send Accounting-Request to 9.45.15.144:1813
id 1646/231, len 288
Nov  4 00:26:49.908 IST: RADIUS:  authenticator 29 63 0C 79 C1 5E F2 0E - F3 CA 36 DD
A3 55 C1 DE
Nov  4 00:26:49.908 IST: RADIUS:  Acct-Session-Id     [44]  10  "00000021"
Nov  4 00:26:49.908 IST: RADIUS:  Calling-Station-Id  [31]  15  "192.168.202.2"
Nov  4 00:26:49.908 IST: RADIUS:  Vendor, Cisco       [26]  64
Nov  4 00:26:49.908 IST: RADIUS:   Cisco AVpair       [1]   58
"audit-session-id=L2L433010101ZO2L4C0A8CA02ZH11941194ZN3A"
Nov  4 00:26:49.908 IST: RADIUS:  Vendor, Cisco       [26]  46
Nov  4 00:26:49.908 IST: RADIUS:   Cisco AVpair       [1]   40
"isakmp-phase1-id=pskuser1.g1.engdt.com"
Nov  4 00:26:49.908 IST: RADIUS:  Vendor, Cisco       [26]  40
Nov  4 00:26:49.908 IST: RADIUS:   Cisco AVpair       [1]   34
"isakmp-initator-ip=192.168.202.2"
Nov  4 00:26:49.908 IST: RADIUS:  User-Name           [1]   23  "pskuser1.g1.engdt.com"
Nov  4 00:26:49.908 IST: RADIUS:  Vendor, Cisco       [26]  36
Nov  4 00:26:49.908 IST: RADIUS:   Cisco AVpair       [1]   30  "connect-progress=No
Progress"
Nov  4 00:26:49.908 IST: RADIUS:  Acct-Authentic      [45]  6   Local
   [2]
Nov  4 00:26:49.908 IST: RADIUS:  Acct-Status-Type    [40]  6   Start
   [1]
Nov  4 00:26:49.908 IST: RADIUS:  NAS-IP-Address      [4]   6   192.168.202.1

Nov  4 00:26:49.908 IST: RADIUS:  home-hl-prefix      [151] 10  "D33648D8"
Nov  4 00:26:49.908 IST: RADIUS:  Acct-Delay-Time     [41]  6   0

Nov  4 00:26:49.908 IST: RADIUS(0000002C): Sending a IPv4 Radius Packet
```

次の出力は、特定の audit-session-id のセッションを切断すると、FlexVPN サーバーに表示されます。セッション終了要求は RADIUS クライアント経由で RADIUS サーバーに送信されます。この例では、audit-session-ID が L2L433010101ZO2L4C0A8CA02ZH119404ZP37 のセッションは終了するため、出力には表示されません。

```
Nov  4 00:32:29.004 IST: RADIUS: POD  received from id 216 9.45.15.144:50567, POD Request,
 len 84
Nov  4 00:32:29.004 IST: POD: 9.45.15.144 request queued
Nov  4 00:32:29.004 IST:  ++++++ POD Attribute List ++++++
Nov  4 00:32:29.004 IST: 7FBD9783D3A8 0 00000089 audit-session-id(819) 39
L2L433010101ZO2L4C0A8CA02ZH11941194ZN3B
```

```
Nov  4 00:32:29.004 IST:
Nov  4 00:32:29.004 IST: POD: Sending ACK from port 1812 to 9.45.15.144/50567

Nov  4 00:32:29.005 IST: IKEv2:(SESSION ID = 59,SA ID = 2):Check for existing active SA
Nov  4 00:32:29.006 IST: IKEv2:in_octets 0, out_octets 0
Nov  4 00:32:29.006 IST: IKEv2:in_packets 0, out_packets 0
Nov  4 00:32:29.006 IST: IKEv2:(SA ID = 2):[IKEv2 -> AAA] Accounting stop request sent
successfully
Nov  4 00:32:29.006 IST: IKEv2:(SESSION ID = 59,SA ID = 2):Delete all IKE SAs
Nov  4 00:32:29.010 IST: RADIUS/ENCODE(0000002D):Orig. component type = VPN IPSEC
Nov  4 00:32:29.010 IST: RADIUS(0000002D): Config NAS IP: 0.0.0.0
Nov  4 00:32:29.010 IST: RADIUS(0000002D): Config NAS IPv6: ::
Nov  4 00:32:29.010 IST: RADIUS(0000002D): sending
Nov  4 00:32:29.011 IST: RADIUS/ENCODE: Best Local IP-Address 192.168.202.1 for
Radius-Server 9.45.15.144
Nov  4 00:32:29.011 IST: RADIUS(0000002D): Send Accounting-Request to 9.45.15.144:1813
id 1646/246, len 356
Nov  4 00:32:29.011 IST: RADIUS:  authenticator 52 88 5E CB 8B FA 1E C1 - CC EF 73 75
89 73 CA 95
Nov  4 00:32:29.011 IST: RADIUS:  Acct-Session-Id     [44]  10  "00000022"
Nov  4 00:32:29.011 IST: RADIUS:  Calling-Station-Id  [31]  15  "192.168.202.2"
Nov  4 00:32:29.011 IST: RADIUS:  Vendor, Cisco       [26]  64
Nov  4 00:32:29.011 IST: RADIUS:   Cisco AVpair       [1]   58
"audit-session-id=L2L433010101ZO2L4C0A8CA02ZH11941194ZN3B"
Nov  4 00:32:29.011 IST: RADIUS:  Vendor, Cisco       [26]  46
Nov  4 00:32:29.011 IST: RADIUS:   Cisco AVpair       [1]   40
"isakmp-phase1-id=pskuser1.g1.engdt.com"
Nov  4 00:32:29.011 IST: RADIUS:  Vendor, Cisco       [26]  40
Nov  4 00:32:29.011 IST: RADIUS:   Cisco AVpair       [1]   34
"isakmp-initator-ip=192.168.202.2"
Nov  4 00:32:29.011 IST: RADIUS:  User-Name           [1]   23  "pskuser1.g1.engdt.com"
Nov  4 00:32:29.011 IST: RADIUS:  Acct-Authentic      [45]  6   Local
   [2]
Nov  4 00:32:29.011 IST: RADIUS:  Vendor, Cisco       [26]  36
Nov  4 00:32:29.011 IST: RADIUS:   Cisco AVpair       [1]   30  "connect-progress=No
Progress"
Nov  4 00:32:29.011 IST: RADIUS:  Acct-Session-Time   [46]  6   56

Nov  4 00:32:29.011 IST: RADIUS:  Acct-Input-Octets   [42]  6   0

Nov  4 00:32:29.011 IST: RADIUS:  Acct-Output-Octets  [43]  6   0

Nov  4 00:32:29.011 IST: RADIUS:  Acct-Input-Packets  [47]  6   0

Nov  4 00:32:29.011 IST: RADIUS:  Acct-Output-Packets [48]  6   0

Nov  4 00:32:29.011 IST: RADIUS:  Acct-Terminate-Cause[49]  6   none
   [0]
Nov  4 00:32:29.011 IST: RADIUS:  Vendor, Cisco       [26]  32
Nov  4 00:32:29.011 IST: RADIUS:   Cisco AVpair      [1]   26  "disc-cause-ext=No Reason"
Nov  4 00:32:29.011 IST: RADIUS:  Acct-Status-Type    [40]  6   Stop
   [2]
Nov  4 00:32:29.011 IST: RADIUS:  NAS-IP-Address      [4]   6   192.168.202.1

Nov  4 00:32:29.011 IST: RADIUS:  home-hl-prefix      [151] 10  "E2F80C34"
Nov  4 00:32:29.011 IST: RADIUS:  Acct-Delay-Time     [41]  6   0

Nov  4 00:32:29.011 IST: RADIUS(0000002D): Sending a IPv4 Radius Packet
Nov  4 00:32:29.011 IST: RADIUS(0000002D): Started 5 sec timeout
```

次の出力は、特定の audit-session-ID で有効なセッションが存在しない場合に表示されます。これは、そのセッションがすでに終了していて、特定の audit-session-id に関連

するセッションが存在しない場合に発生します。FlexVPN サーバーに 送り返される メッセージに注意してください。

```
Nov  4 00:30:31.905 IST: RADIUS: POD  received from id 131 9.45.15.144:52986, POD Request,
 len 84
Nov  4 00:30:31.905 IST: POD: 9.45.15.144 request queued
Nov  4 00:30:31.905 IST:  ++++++ POD Attribute List ++++++
Nov  4 00:30:31.905 IST: 7FBD9783BA20 0 00000089 audit-session-id(819) 39
L2L433010101ZO2L4C0A8CA02ZH11941194ZN3A
Nov  4 00:30:31.905 IST:
Nov  4 00:30:31.906 IST: POD: 9.45.15.144 Unsupported attribute type 26 for component
Nov  4 00:30:31.906 IST: POD: 9.45.15.144 user  0.0.0.0i sessid 0x0 key 0x0 DROPPED
Nov  4 00:30:31.906 IST: POD: Added Reply Message: No Matching Session
Nov  4 00:30:31.906 IST: POD: Added NACK Error Cause: Invalid Request
Nov  4 00:30:31.906 IST: POD: Sending NAK from port 1812 to 9.45.15.144/52986
Nov  4 00:30:31.906 IST: RADIUS:  18  21  4E6F204D61746368696E672053657373696F6E
Nov  4 00:30:31.906 IST: RADIUS:  101 6   00000194
```

IKEv2 パケット オブ ディスコネクトに関する追加情報

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『Cisco IOS Master Command List, All Releases』
セキュリティ コマンド	• 『Cisco IOS Security Command Reference Commands A to C』 • 『Cisco IOS Security Command Reference Commands D to L』 • 『Cisco IOS Security Command Reference Commands M to R』 • 『Cisco IOS Security Command Reference Commands S to Z』
RADIUS パケット オブ ディスコネクト	『RADIUS Packet of Disconnect』 『RADIUS Packet of Disconnect』

標準および RFC

標準/RFC	タイトル
RFC 3576	*Dynamic Authorization Extensions to Remote Authentication Dial In User Service (RADIUS)*
RFC 5176	*Dynamic Authorization Extensions to Remote Authentication Dial In User Service (RADIUS)*

シスコのテクニカル サポート

説明	リンク
右の URL にアクセスして、シスコのテクニカル サポートを最大限に活用してください。これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

IKEv2 パケット オブ ディスコネクトの機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *283 : IKEv2* パケット オブ ディスコネクトの機能情報

機能名	リリース	機能情報
IKEv2 リモート アクセス認可変更（CoA）のパケット オブ ディスコネクト		IKEv2 リモート アクセス認可変更（CoA）のパケット オブ ディスコネクト機能は、シスコがサポートするデバイスのアクティブな暗号 IKEv2 セッションを停止します。 この機能によって導入されたコマンドはありません。

第 215 章

IKEv2 認可変更のサポートの設定

FlexVPN - QoS および ACL 用 IKEv2 CoA 機能は、アクティブな IKEv2 暗号セッションでの RADIUS 認可変更（CoA）をサポートしています。

IKEv2 認可変更のサポートの前提条件

- IKEv2 は、Cisco AAA コンポーネントのレジストリ エントリからコンポーネントとして登録する必要があります。

IKEv2 認可変更サポートの制限事項

- この機能では、RADIUS ベースの AAA サーバーから受信した認可変更（CoA）パケットのみをサポートしています。

IKEv2 認可変更サポートに関する情報

RADIUS 許可の変更

RADIUS 認可変更（CoA）機能は、認証、認可、およびアカウンティング（AAA）セッションの属性を、セッション認証後に変更するためのメカニズムを提供します。AAA でユーザー、またはユーザー グループのポリシーに変更がある場合、管理者は Cisco Secure Access Control

Server（ACS）などの AAA サーバーから RADIUS CoA パケットを送信して認証を再初期化し、新しいポリシーを適用することができます。

標準RADIUS インターフェイスは通常、ネットワークに接続しているデバイスから要求が送信され、クエリが送信されたサーバーが応答するプル モデルで使用されます。シスコのソフトウェアは、プッシュ モデルで使用される RFC 5176 で定義された RADIUS CoA 要求をサポートしています。このモデルでは、要求は外部サーバーからネットワークに接続されたデバイスへ発信され、外部の認証、認可、およびアカウンティング（AAA）またはポリシー サーバーからの動的なセッション再設定が可能になります。

RADIUS CoA の詳細については、『*Authentication, Authorization, and Accounting Configuration Guide, Cisco IOS Release 15M&T*』または『*Authentication, Authorization, and Accounting Configuration Guide, Cisco IOS XE Release 3S*』を参照してください。

IKEv2 認可変更の作業

FlexVPN - QoS および ACL 用 IKEv2 CoA 機能では、アクティブな IKEv2 暗号セッションの属性を変更して、新しい認証属性に適用できます。Cisco AAA コンポーネントは、AAA サーバーから認可変更（CoA）パケットを受信して、受信した CoA パケットがそれに登録された任意のコンポーネント用かどうかを確認します。CoA パケットがそれ自体のために作成されたとコンポーネントが確認した場合、以降の処理に進みます。CoA パケット内のフィールドに基づいて、パケットが IKEv2 などの任意のコンポーネントと関連している場合、そのパケットはそのコンポーネントによって使用されます。AAA はそのパケットを、リスト内の次のコンポーネントに転送しません。

この機能では、IKEv2 が CoA パケットを受信した後、IKEv2 では Cisco （AV）ペアに対してその CoA パケットを確認します。IKEv2 は、RADIUS サーバーにすでに保存されている audit-session-id に基づいてセッションを特定します。

CoA パケットに IKEv2 がサポートしていない属性が含まれる場合、IKEv2 はそのパケットを破棄し、CoA-NACK を AAA コンポーネントに送信します。

IKEv2 認可変更でサポートされる AV ペア

FlexVPN - QoS および ACL 用 IKEv2 CoA 機能は、次の Cisco AV ペアをサポートしています。

- ip:interface-config
- ip:sub-policy-In
- ip:sub-policy-Out
- ip:sub-qos-policy-in
- ip:sub-qos-policy-out
- ipsec:inacl
- ipsec:outacl

IKEv2 認可変更サポートの設定方法

FlexVPN サーバーでの認可変更の設定

IKEv2 認可変更（CoA）サポート機能に必要な、FlexVPN サーバーでの IKEv2 固有の設定はありません。FlexVPN サーバーでは、RADIUS 認可変更のみを設定する必要があります。AAA 設定の詳細については、『*Authentication, Authorization, and Accounting Configuration Guide, Cisco IOS Release 15M&T*』の「RADIUS Change of Authorization」機能モジュールを参照してください。

手順の概要

1. **enable**
2. **configure terminal**
3. **aaa new-model**
4. **aaa server radius dynamic-author**
5. **client** {*ip-address* | *name* [**vrf** *vrf-name*]} **server-key** [**0** | **7**] *string*
6. **port** *port-number*
7. **auth-type** {**any** | **all** | **session-key**}
8. **ignore session-key**
9. **ignore server-key**
10. **exit**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。プロンプトが表示されたらパスワードを入力します。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**aaa new-model** 例： `Device(config)# aaa new-model`	認証、認可、アカウンティング（AAA）をグローバルに有効化します。
ステップ 4	**aaa server radius dynamic-author** 例： `Device(config)# aaa server radius dynamic-author`	ダイナミック認可ローカル サーバー コンフィギュレーション モードを開始し、デバイスが認可変更（CoA）を受け入れ、要求を取り外す RADIUS クライアントを指定します。デバイスを AAA サー

	コマンドまたはアクション	目的
		バーとして設定し、外部ポリシー サーバーとの連携を可能にする。
ステップ 5	**client** {*ip-address* | *name* [**vrf** *vrf-name*]} **server-key** [**0** | **7**] *string* 例： `Device(config-locsvr-da-radius)# client 10.0.0.1`	RADIUS キーをデバイスと RADIUS クライアントとの間で共有されるように設定します。
ステップ 6	**port** *port-number* 例： `Device(config-locsvr-da-radius)# port 3799`	設定された RADIUS クライアントから RADIUS 要求をデバイスが受信するポートを指定します。 （注） パケットオブディスコネクトのデフォルト ポートは 1700 です。ACS 5.1 と相互運用するためには、ポート 3799 が必要です。
ステップ 7	**auth-type** {**any** | **all** | **session-key**} 例： `Device(config-locsvr-da-radius)# auth-type all`	デバイスが RADIUS クライアントに使用する認可のタイプを指定します。クライアントは、認可用に設定された属性と一致していなければなりません。
ステップ 8	**ignore session-key** 例： `Device(config-locsvr-da-radius)# ignore session-key`	（オプション）セッション キーを無視するようにデバイスを設定します。
ステップ 9	**ignore server-key** 例： `Device(config-locsvr-da-radius)# ignore server-key`	（オプション）サーバー キーを無視するようにデバイスを設定します。
ステップ 10	**exit** 例： `Device(config-locsvr-da-radius)# exit`	グローバル コンフィギュレーション モードに戻ります。

IKEv2 認可変更サポートの確認

次の show コマンドを使用して、Cisco デバイスでの認可変更（CoA）の成功を確認します。

手順の概要

1. **enable**
2. **show platform hardware qfp active feature qos all output all**
3. **show platform hardware qfp active feature qos all input all**

手順の詳細

ステップ 1 enable

例：

```
Device> enable
```

特権 EXEC モードを有効にします。

- パスワードを入力します（要求された場合）。

ステップ 2 show platform hardware qfp active feature qos all output all

例：

```
Device# show platform hardware qfp active feature qos all output all

Interface: Virtual-Access1, QFP if_h: 14, Num Targets: 1
  Target: Out, Num UIDBs: 1
    UIDB #: 0
    Hierarchy level: 0, Num matching iftgts: 1
    Policy name: aaa-out-policy, Policy id: 9679472
    Parent Class Idx: 0, Parent Class ID: 0
      IF Tgt#: 0, ifh: 14, member_ifh: 0, link_idx: 0
        PSQD specifics:
          Target Index: 0, Num Classes: 1
            Class index: 0, Class object id: 1593, Match index: 0
            Class name: class-default, Policy name: aaa-out-policy
              psqd[0-3]: 0x00000000 0x00000000 0x00000001 0x00000000
        ISQD specifics:
          Target Index: 0, Num Classes: 1
            Class index: 0, Class object id: 1593
            Class name: class-default, Policy name: aaa-out-policy
              isqd[0-3]:  0x88e78ec0 0x00000000 0x00000000 0x00000000
              (cache) isqd[0-3]: 0x88e78ec0 0x00000000 0x00000000 0x00000000
        Police specifics:
          Target Index: 0, Num Classes: 1
            Class index: 0, Class object id: 1593
            Class name: class-default, Policy name: aaa-out-policy
              Policer id: 0x20000002
              hw_policer[0-3]:       0x4000047e 0x00163ac8 0x00000000 0x00000000
              cache hw_policer[0-3]: 0x4000047e 0x00163ac8 0x00000000 0x00000000
              conform stats (paks/octets): 0x0000000000000000, : 0x0000000000000000
              exceed stats  (paks/octets): 0x0000000000000000, : 0x0000000000000000
              violate stats (paks/octets): 0x0000000000000000, : 0x0000000000000000
              police_info:           0x00000000
              cache police_info:     0x00000000
        Queue specifics:
          Target Index: 0, Num Classes: 1
            Class index: 0, Class object id: 1593
            Class name: class-default, Policy name: aaa-out-policy
              No queue configured
        Schedule specifics:
          Target Index: 0, Num Classes: 1
            Class index: 0, Class object id: 1593
            Class name: class-default, Policy name: aaa-out-policy
              No schedule info (no queue configured)
```

CoA が成功したかどうかのプラットフォーム固有情報が表示されます。

ステップ 3 show platform hardware qfp active feature qos all input all

例：

```
Device#  show platform hardware qfp active feature qos all input all

Interface: Virtual-Access1, QFP if_h: 14, Num Targets: 1
  Target: In, Num UIDBs: 1
    UIDB #: 0
    Hierarchy level: 0, Num matching iftgts: 1
    Policy name: aaa-in-policy, Policy id: 980784
    Parent Class Idx: 0, Parent Class ID: 0
      IF Tgt#: 0, ifh: 14, member_ifh: 0, link_idx: 0
        PSQD specifics:
          Target Index: 0, Num Classes: 1
            Class index: 0, Class object id: 1593, Match index: 0
            Class name: class-default, Policy name: aaa-in-policy
              psqd[0-3]: 0x00000000 0x00000000 0x00000001 0x00000000
        ISQD specifics:
          Target Index: 0, Num Classes: 1
            Class index: 0, Class object id: 1593
            Class name: class-default, Policy name: aaa-in-policy
              isqd[0-3]:  0x88d49748 0x00000001 0x00000000 0x00000000
              (cache) isqd[0-3]: 0x88d49748 0x00000001 0x00000000 0x00000000
        Police specifics:
          Target Index: 0, Num Classes: 1
            Class index: 0, Class object id: 1593
            Class name: class-default, Policy name: aaa-in-policy
              Policer id: 0x20000003
              hw_policer[0-3]:       0x10000140 0x00113a29 0x00000000 0x00000000
              cache hw_policer[0-3]: 0x10000140 0x00113a29 0x00000000 0x00000000
              conform stats (paks/octets): 0x0000000000000000, : 0x0000000000000000
              exceed stats  (paks/octets): 0x0000000000000000, : 0x0000000000000000
              violate stats (paks/octets): 0x0000000000000000, : 0x0000000000000000
              police_info:           0x00000000
              cache police_info:     0x00000000
        Queue specifics:
          Target Index: 0, Num Classes: 1
            Class index: 0, Class object id: 1593
            Class name: class-default, Policy name: aaa-in-policy
              No queue configured
        Schedule specifics:
          Target Index: 0, Num Classes: 1
            Class index: 0, Class object id: 1593
            Class name: class-default, Policy name: aaa-in-policy
              No schedule info (no queue configured)
```

機能のステータスが表示されます。

IKEv2 認可変更サポートの設定例

例：認可変更のトリガー

次の出力例は、管理者が認可変更（CoA）をトリガーすると表示されます。セッションは、audit-session-idに基づいて特定されます。このIDは動的文字列で、ピアとのセッションについて、6 タプル情報の形式にエンコードされています。

IKEv2 は、RADIUS サーバーから認可変更（CoA）パケットを受信します。セッションは、audit-session-id に基づいて特定されます。

```
*Oct  6 23:38:55.250: RADIUS: COA  received from id 125 10.106.210.176:58712, CoA Request,
 len 257
*Oct  6 23:38:55.251: COA: 10.106.210.176 request queued
*Oct  6 23:38:55.251: RADIUS:  authenticator BD 97 5E BA B2 EB C1 C5 - 1A 14 51 3D C2
C8 66 3F
*Oct  6 23:38:55.251: RADIUS:  Vendor, Cisco       [26]  62
*Oct  6 23:38:55.251: RADIUS:   Cisco AVpair       [1]   56
"audit-session-id=L2L44D010102ZO2L44D010101ZI1F401F4ZO2"
*Oct  6 23:38:55.251: RADIUS:  Vendor, Cisco       [26]  52
*Oct  6 23:38:55.251: RADIUS:   Cisco AVpair       [1]   46
"ip:interface-config=service-policy input pol"
*Oct  6 23:38:55.251: RADIUS:  Vendor, Cisco       [26]  35
*Oct  6 23:38:55.251: RADIUS:   Cisco AVpair      [1]   29  "ip:sub-qos-policy-out=2M-IN"
*Oct  6 23:38:55.251: RADIUS:  Vendor, Cisco       [26]  36
*Oct  6 23:38:55.251: RADIUS:   Cisco AVpair      [1]   30  "ip:sub-qos-policy-in=aaa-pol"
*Oct  6 23:38:55.251: RADIUS:  Vendor, Cisco       [26]  52
*Oct  6 23:38:55.251: RADIUS:   Cisco AVpair       [1]   46
"ip:interface-config=service-policy output 2M"
*Oct  6 23:38:55.251: COA: Message Authenticator missing or failed decode

*Oct  6 23:38:55.251:  ++++++ CoA Attribute List ++++++
*Oct  6 23:38:55.251: 421C9694 0 00000089 audit-session-id(819) 37
L2L44D010102ZO2L44D010101ZI1F401F4ZO2
*Oct  6 23:38:55.251: 421C9584 0 00000081 interface-config(222) 24 service-policy input
 pol
*Oct  6 23:38:55.251: 421C95B8 0 00000081 sub-qos-policy-out(423) 5 2M-IN
*Oct  6 23:38:55.251: 421C95EC 0 00000081 sub-qos-policy-in(421) 7 aaa-pol
*Oct  6 23:38:55.251: 421C9620 0 00000081 interface-config(222) 24 service-policy output
 2M
*Oct  6 23:38:55.251:
*Oct  6 23:38:55.251: COA: Added NACK Error Cause: Success
```

IKEv2 認可変更サポートに関する追加情報

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『Cisco IOS Master Command List, All Releases』
セキュリティ コマンド	• 『Cisco IOS Security Command Reference Commands A to C』 • 『Cisco IOS Security Command Reference Commands D to L』 • 『Cisco IOS Security Command Reference Commands M to R』 • 『Cisco IOS Security Command Reference Commands S to Z』

シスコのテクニカル サポート

説明	リンク
右の URL にアクセスして、シスコのテクニカル サポートを最大限に活用してください。これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

IKEv2 認可変更のサポートの機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *284 : IKEv2* 認可変更のサポートの機能情報

機能名	リリース	機能情報
FlexVPN - QoS および ACL 用 IKEv2 CoA		FlexVPN - QoS および ACL 用 IKEv2 CoA 機能は、アクティブな IKEv2 暗号セッションでの RADIUS 認可変更（CoA）をサポートしています。 この機能によって変更または更新されたコマンドはありません。

第 216 章

集約認証の設定

FlexVPN RA - Cisco AnyConnect クライアントのサポートを拡張することで、AnyConnect 機能の集約認証サポートは、集約認証方式を実装します。このクライアントでは、独自の AnyConnect EAP 認証方式を使用し、Cisco AnyConnect クライアントと FlexVPN サーバー間にインターネットを介したセキュア トンネルを確立します。

集約認証の設定の前提条件

- <BypassDownloader> 値を true に設定して、AnyConnectLocalPolicy ファイルで BypassDownloader 関数を有効にする必要があります。デバイスで SSL がサポートされていない場合、BypassDownloader 関数は動作しないため、<BypassDownloader> 値を false に設定して、この関数を無効にする必要があります。そうしないと、接続が失敗します。

集約認証の設定に関する情報

Cisco AnyConnect および FlexVPN

VPN 接続を確立するには、VPN クライアントが Extensible Authentication Protocol（EAP：拡張可能認証プロトコル）、拡張認証（XAUTH）などの認証方式を使用してユーザー クレデンシャルを取得し、Access Control Server を接続するハブにユーザー クレデンシャルを転送する必要があります。Access Control Server は、外部データベースまたは Active Directory（AD）を送信してクレデンシャルを確認します。

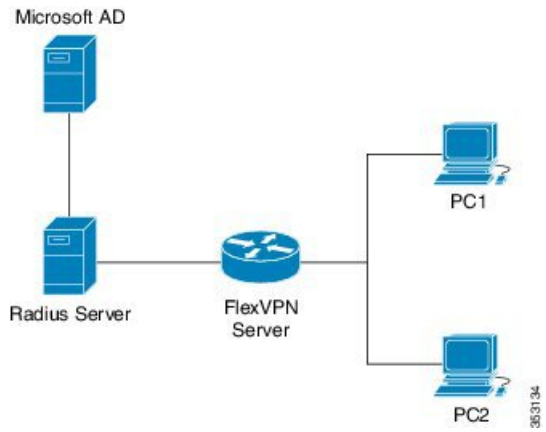
FlexVPN サーバーは（ハブとして）Cisco Secure Access Control Server と連動してユーザー クレデンシャルを確認し、VPN 接続を確立します。ただし、Cisco AnyConnect は EAP を使用してユーザー クレデンシャルを取得し、XAUTH をサポートしません。一方、Cisco Secure Access Control Server は外部データベース（ここでは AD）を使用する EAP-MD5 をサポートしません。これによって、Cisco Secure Access Control Server が EAP-MD5 をサポートする必要があるシナリオ、または FlexVPN が Cisco AnyConnect からの情報を個別に認証して、Cisco Secure Access Control Server に個別に接続する必要があるシナリオが生じます。FlexVPN は、集約認証方式を使用して、Cisco AnyConnect からの情報を認証できます。FlexVPN サーバーで集約認証方式を実装すると、Cisco IOS ソフトウェアにより多くの機能サポートを追加するためのウィンドウが提供されます。

FlexVPN RA：AnyConnect の集約認証サポート機能では、独自の AnyConnect EAP 認証方式を使用する Cisco AnyConnect クライアントのサポートを拡張することによって集約認証方式を実装し、Cisco AnyConnect サーバーや FlexVPN サーバーを使用してインターネット上にセキュアなトンネルを確立します。 これは、サーバー固有の機能で、Cisco AnyConnect と連動します。

集約認証の動作

インターネット キー エクスチェンジ バージョン 2 は、基本的な集約認証を実装することによって独自の AnyConnect EAP 認証方式を使用する Cisco AnyConnect をサポートします。ここでの認証は、リモート RADIUS サーバーを使用する認証、認可、およびアカウンティング（AAA）を介して実行されます。次に、Cisco IOS ソフトウェアでの集約認証の実装を説明するネットワーク トポロジの例を示します。

図 *111 : RADIUS* サーバーに接続された *FlexVPN* サーバー



この図は、次のことを示しています。

- Cisco Secure Access Control Server は、認証用の RADIUS サーバーとして機能します。
- クレデンシャルは、認証用の Active Directory として機能する Microsoft Active Directory に格納されます。

（注） Microsoft Active Directory は、単なる例です。クレデンシャルの格納場所は重要ではありません。

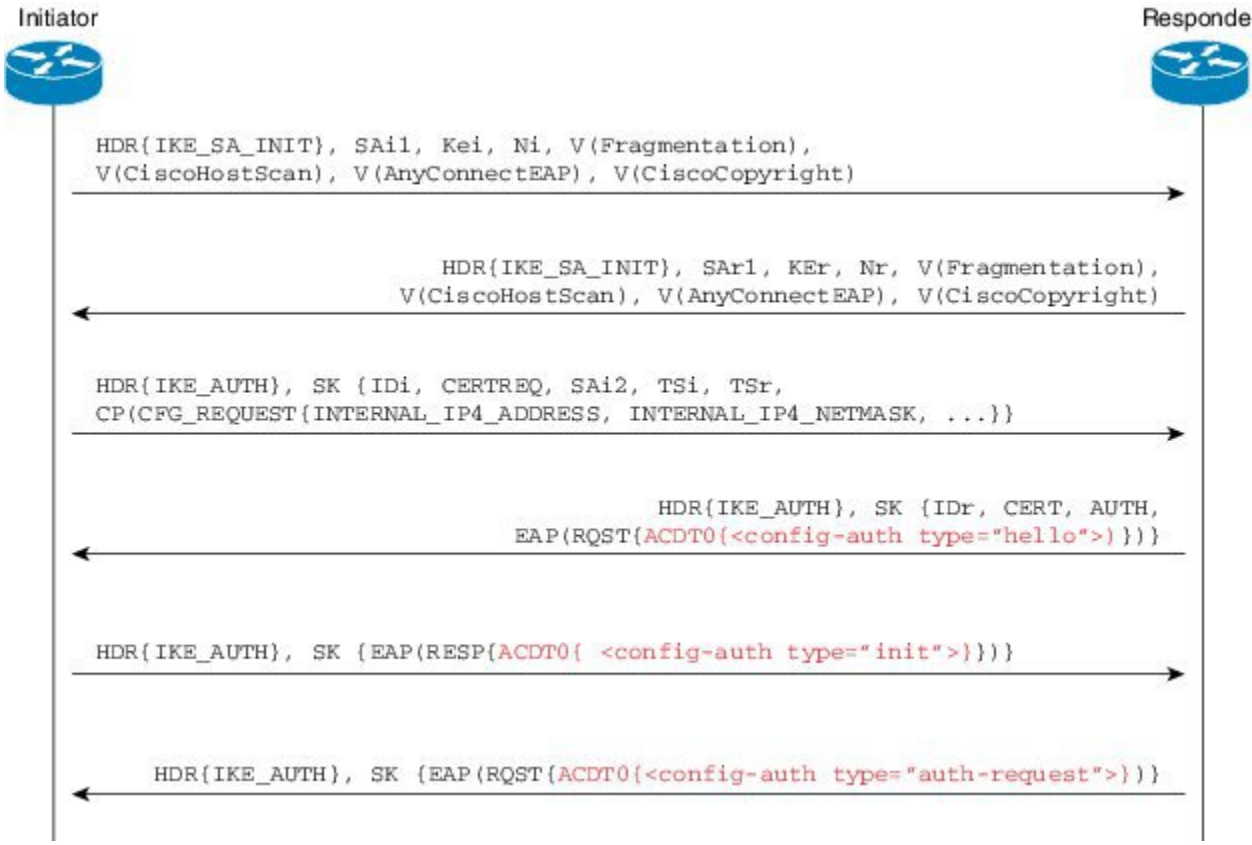
- シスコ デバイスは、FlexVPN サーバーとして機能します。
- Windows 7 PC は、Cisco AnyConnect クライアントとして機能します。

1. VPN 接続を開始するために、Cisco AnyConnect クライアントは証明書を使用して FlexVPN サーバーを確認します。
2. 証明書を確認した後、Cisco AnyConnect クライアントは Cisco AnyConnect EAP がロードしたメッセージを FlexVPN サーバーに送信します。
3. FlexVPN サーバーが Cisco AnyConnect から Cisco AnyConnect EAP がロードしたメッセージを受信すると、FlexVPN サーバーはメッセージをダウンロードして EAP のメッセージを除去します。
4. FlexVPN は認証用の RADIUS サーバーおよび認証用の Microsoft Active Directory（AD）との接続を確立して、除去されたメッセージを転送し、Cisco AnyConnect クライアントから提供されたクレデンシャルを確認します。
5. クレデンシャルが RADIUS サーバーおよび Microsoft Active Directory（AD）によって確認されて承認されると、適切な応答が FlexVPN サーバーに送信され、Cisco AnyConnect に応答し、VPN 接続が確立されます。

Cisco AnyConnect EAP を使用する IKE 交換

AnyConnect EAP を使用する IKE での認証は、RFC 3748 で説明されているように標準 EAP モデルのバリエーションです。AnyConnect EAP を使用すると、パブリック設定または認証 XML は EAP ペイロードを介して送信されます。次の図に、Cisco AnyConnect によって使用される一般的なメッセージ フローを示します。

図 *112 : AnyConnect EAP* を使用する *IKE* 交換



1. Cisco AnyConnect クライアントが、FlexVPN サーバーへの IKE 接続を開始します。クライアントは、一般的な IKE ペイロードに加えて、Cisco AnyConnect EAP のサポートを示すためのベンダー ID ペイロードを送信します。クライアントは、シスコの著作権ベンダー ID を含めることによって自身をシスコ製品として識別します。
2. サーバー ゲートウェイが、フラグメンテーションおよび AnyConnect EAP サポートを示すためのベンダー ID ペイロードを送信し、シスコの著作権ベンダー ID を含めることによって自身をシスコ製品として識別します。
3. 設定ペイロードで、トンネル設定が要求されます。クライアントは、このメッセージから AUTH ペイロードを省略することによって、Cisco AnyConnect EAP 認証の使用を希望していることを示します。
4. 集約認証および設定プロトコルが、EAP を介して伝送されます。
5. FlexVPN サーバーが、EAP の成功メッセージを送信します。
6. Cisco AnyConnect クライアントが、AUTH ペイロードを送信します。
7. FlexVPN サーバーが、AUTH ペイロードと Cisco AnyConnect クライアントが要求したトンネル設定属性を送信します。

IKEv2 でのデュアルファクタ認証のサポート

Cisco IOS ソフトウェアでの集約認証の実装は、デュアルファクタ認証に拡張できます。二重認証は、デバイス証明書情報を交換し検証する集約認証中に、新しい AnyConnect EAP 交換を導入することで実行されます。「デバイス」と同様に「ユーザー」も認証するこのメカニズムは、「二重認証」と呼ばれます。

（注） AnyConnect EAP は、AnyConnect クライアント固有の認証方式であり、他クライアントには適用されません。

集約認証の設定方法

集約認証用の FlexVPN サーバーの設定

このタスクを実行して、FlexVPN サーバーの集約認証を設定します。

手順の概要

1. **enable**
2. **configure terminal**
3. **crypto ikev2 profile** *profile-name*
4. **aaa accounting anyconnect-eap** *list-name*
5. **match identity remote key-id** *opaque-string*
6. **authentication remote anyconnect-eap aggregate** [**cert-request**]
7. **authentication local rsa-sig**
8. **pki trustpoint** *trustpoint-label*
9. **aaa authentication anyconnect-eap** *list-name*
10. **aaa authorization group anyconnect-eap list** *aaa-listname* **name-mangler** *mangler-name*
11. **aaa authorization user anyconnect-eap cached**
12. **aaa authorization user anyconnect-eap list** *aaa-listname* **name-mangler** *mangler-name*
13. **end**
14. **show crypto ikev2 session detailed**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。

	コマンドまたはアクション	目的
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**crypto ikev2 profile** *profile-name* 例： `Device(config)# crypto ikev2 profile profile1`	IKEv2プロファイル名を定義し、IKEv2プロファイル コンフィギュレーション モードを開始します。
ステップ 4	**aaa accounting anyconnect-eap** *list-name* 例： `Device(config-ikev2-profile)# aaa accounting anyconnect-eap list1`	IKEv2 リモート認証方式が AnyConnect EAP の場合、認証、認可、およびアカウンティング（AAA）のアカウンティング方式リストを有効にします。
ステップ 5	**match identity remote key-id** *opaque-string* 例： `Device(config-ikev2-profile)# match identity remote key-id aggauth_user3@abc.com`	リモート キー ID タイプの ID に基づいて、プロファイルを照合します。
ステップ 6	**authentication remote anyconnect-eap aggregate** [**cert-request**] 例： `Device(config-ikev2-profile)# authentication remote anyconnect-eap aggregate cert-request`	Cisco AnyConnect EAP に集約認証を指定します。 • **cert-request** ：二重認証用に Cisco AnyConnect クライアントに証明書を要求します。
ステップ 7	**authentication local rsa-sig** 例： `Device(config-ikev2-profile)# authentication local rsa-sig`	Rivest、Shamir、Adelman（RSA）署名をローカル認証方式として指定します。
ステップ 8	**pki trustpoint** *trustpoint-label* 例： `Device(config-ikev2-profile)# pki trustpoint CA1`	RSA 署名認証方式で使用する Public Key Infrastructure（PKI）トラストポイントを指定します。
ステップ 9	**aaa authentication anyconnect-eap** *list-name* 例： `Device(config-ikev2-profile)# aaa authentication anyconnect-eap list1`	Cisco AnyConnect EAP 認証用に、認証、認可、およびアカウンティング（AAA）認証リストを指定します。 • **anyconnect-eap**：AAA AnyConnect EAP 認証を指定します。 • *list-name*：AAA 認証リスト名。
ステップ 10	**aaa authorization group anyconnect-eap list** *aaa-listname* **name-mangler** *mangler-name* 例：	リモート認証方式が AnyConnect EAP であり、名前分割が派生する場合、各グループ ポリシーに AAA 認証を指定します。

	コマンドまたはアクション	目的
	`Device(config-ikev2-profile)# aaa authorization group anyconnect-eap list list1 name-mangler mangler1`	
ステップ 11	**aaa authorization user anyconnect-eap cached** 例： `Device(config-ikev2-profile)# aaa authorization user anyconnect-eap cached`	リモート認証方式が AnyConnect EAP であり、AnyConnect EAP 認証からキャッシュした属性を使用する場合、各ユーザーポリシーにAAA認証を指定します。
ステップ 12	**aaa authorization user anyconnect-eap list** *aaa-listname* **name-mangler** *mangler-name* 例： `Device(config-ikev2-profile)# aaa authorization user anyconnect-eap list list1 name-mangler mangler1`	リモート認証方式に AAA 方式リストを指定し、名前分割が派生します。
ステップ 13	**end** 例： `Device(config-ikev2-profile)# end`	IKEv2 プロファイル コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。
ステップ 14	**show crypto ikev2 session detailed** 例： `Device# show crypto ikev2 session detailed`	アクティブなインターネット キー エクスチェンジ バージョン 2（IKEv2）セッションのステータスを表示します。

集約認証の設定例

例：集約認証の設定

次の例は、FlexVPN サーバーで集約認証を設定する方法を示します。これによって、Cisco AnyConnect クライアントと FlexVPN サーバー間のセキュア トンネルの確立を有効にします。

```
Device> enable
Device# configure terminal
Device(config)# crypto ikev2 profile profile1
Device(config-ikev2-profile)# aaa accounting anyconnect-eap list1
Device(config-ikev2-profile)# match identity remote key-id aggauth_user1@example.com
Device(config-ikev2-profile)# authentication remote anyconnect-eap aggregate cert-request
Device(config-ikev2-profile)# authentication local rsa-sig
Device(config-ikev2-profile)# pki trustpoint CA1
Device(config-ikev2-profile)# aaa authentication anyconnect-eap list1
Device(config-ikev2-profile)# aaa authorization group anyconnect-eap list list1
name-mangler mangler1
Device(config-ikev2-profile)# aaa authorization user anyconnect-eap cached
Device(config-ikev2-profile)# aaa authorization user anyconnect-eap list list1 name-mangler
 mangler1
Device(config-ikev2-profile)# end
```

集約認証の設定に関する追加情報

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『Cisco IOS Master Command List, All Releases』
セキュリティ コマンド	• 『Cisco IOS Security Command Reference Commands A to C』 • 『Cisco IOS Security Command Reference Commands D to L』 • 『Cisco IOS Security Command Reference Commands M to R』 • 『Cisco IOS Security Command Reference Commands S to Z』

シスコのテクニカル サポート

説明	リンク
右の URL にアクセスして、シスコのテクニカル サポートを最大限に活用してください。これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

集約認証の設定に関する機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *285 :* 集約認証の設定に関する機能情報

機能名	リリース	機能情報
IKEv2 でのデュアルファクタ認証のサポート		IKEv2 でのデュアルファクタ認証のサポートは、二重認証への Cisco AnyConnect クライアントからの証明書要求をサポートします。 **authentication (IKEv2 profile)** コマンドが変更されました。
FlexVPN RA - AnyConnect の集約認証サポート		FlexVPN RA - Cisco AnyConnect クライアントのサポートを拡張することで、AnyConnect 機能の集約認証サポートは、集約認証方式を実装します。このクライアントでは、独自の AnyConnect EAP 認証方式を使用し、Cisco AnyConnect クライアントと FlexVPN サーバー間にインターネットを介したセキュア トンネルを確立します。 次のコマンドが導入または変更されました。**aaa accounting (IKEv2 profile)**、**aaa authentication (IKEv2 profile)**、**aaa authorization (IKEv2 profile)**、**authentication (IKEv2 profile)**、**show crypto ikev2 profile**、**show crypto ikev2 session**

第 217 章

付録：FlexVPN の RADIUS 属性

この章では、FlexVPN サーバーでサポートされる RADIUS 属性について説明します。

• FlexVPN RADIUS 属性 （3175 ページ）

FlexVPN RADIUS 属性

次に、FlexVPN サーバーによって使用される RADIUS 属性カテゴリを示します。

- インバウンドおよび双方向 IETF RADIUS 属性
- アウトバウンド ローカル
- アウトバウンド リモート

（注） 次のリストに含まれていない FlexVPN サーバーによって RADIUS に送信されるインバウンド属性では、値は AAA システムによって設定されます。

属性	User-Name
タイプ	IETF
書式	文字列
属性 ID	1

説明	この属性は、FlexVPN サーバーによって RADIUS に送信され、次のように取得されます。 • AAA ベースの事前共有キー：ピア IKEv2 ID • EAP 認証：ピア EAP ID • ユーザー認証またはグループ認証：name mangler の出力または IKEv2 プロファイル認証コマンドで指定された文字列。 • アカウンティング：ピア EAP ID または IKEv2 ID。 この属性は、正常な EAP 認証後に Access-Accept で RADIUS から受信されることもあります。また、認証済みのピア EAP ID を指定します。

属性	User-Password
タイプ	IETF
書式	文字列
属性 ID	2
説明	この属性は、FlexVPN サーバーによって RADIUS に送信され、次のように取得されます。 • AAA ベースの事前共有キー：「cisco」 • ユーザー/グループ認証：「cisco」

属性	Calling-Station-ID
タイプ	IETF
書式	文字列
属性 ID	31
説明	この属性は、FlexVPN サーバーによって RADIUS に送信され、次のように取得されます。 • AAA ベースの事前共有キー：IKEv2 発信側アドレス • EAP 認証：IKEv2 発信側アドレス • ユーザー/グループ認証：IKEv2 発信側アドレス

属性	Service-Type
タイプ	IETF

書式	文字列
属性 ID	6
説明	この属性は、FlexVPN サーバーによって EAP 認証に使用されており、この属性の値は「Login」に設定されています。

属性	EAP-Message
タイプ	IETF
書式	文字列
属性 ID	79
説明	この属性は、FlexVPN サーバーによって EAP 認証に使用されており、EAP サーバーとリモート アクセス クライアントの間で EAP パケットをリレーします。

属性	Message-Authenticator
タイプ	IETF
書式	文字列
属性 ID	80
説明	この属性は、FlexVPN サーバーによって EAP 認証用に送信されます。この属性の値は、AAA サブシステムによって設定されます。

属性	Framed-Pool
タイプ	IETF
書式	文字列
属性 ID	88
ローカル設定	pool name
RADIUS 設定	Framed-Pool=*pool-name*
説明	FlexVPN サーバーが IPv4 アドレスの割り当てに使用する IPv4 アドレス プールの名前を指定して、クライアントに割り当てます。割り当てられたアドレスは、IKEv2 標準設定属性の INTERNAL_IP4_ADDRESS を介してクライアントにプッシュされます。

属性	ipsec:group-dhcp-server
タイプ	Cisco AV ペア

書式	文字列
ローカル設定	dhcp server {*ipddr* | *host*}
RADIUS 設定	cisco-avpair="ipsec: group-dhcp-server=*ipaddr*"
説明	FlexVPN サーバーが IPv4 アドレスのリースに使用する IPv4 DHCP サーバーを指定して、クライアントに割り当てます。リースされたアドレスは、IKEv2 標準設定属性の INTERNAL_IP4_ADDRESS を介してクライアントにプッシュされます。

属性	ipsec:dhcp-giaddr
タイプ	Cisco AV ペア
書式	IPaddr
ローカル設定	dhcp giaddr ipaddr
RADIUS 設定	cisco-avpair="psec: dhcp-giaddr=*ipaddr*"
説明	FlexVPN サーバーが DCHP サーバーへの接続に使用する IPv4 DHCP ゲートウェイ IP アドレスを指定します。

属性	ipsec:dhcp-timeout
タイプ	Cisco AV ペア
書式	整数
ローカル設定	dhcp timeout *seconds*
RADIUS 設定	cisco-avpair="ipsec:dhcp-timeout=*seconds*"
説明	FlexVPN サーバーが DHCP サーバーからの応答をタイムアウトするのに使用する、IPv4 DHCP サーバーからの応答の待機時間を指定します。

属性	ipsec:ipv6-addr-pool
タイプ	Cisco AV ペア
書式	文字列
ローカル設定	ipv6 *pool name*
RADIUS 設定	cisco-avpair="ipsec:ipv6-addr-pool=*pool-name*"

説明	FlexVPN サーバーが IPv6 アドレスの割り当てに使用する IPv6 アドレス プールの名前を指定して、クライアントに割り当てます。割り当てられたアドレスは、IKEv2 標準設定属性の INTERNAL_IP6_ADDRESS を介してクライアントにプッシュされます。

属性	ipsec:route-set=prefix
タイプ	Cisco AV ペア
書式	文字列
ローカル設定	該当なし
RADIUS 設定	cisco-avpair="ipsec:route-set=prefix *prefix*/*length*"
例	ipsec:route-set=prefix 192.168.1.0/24
説明	FlexVPN サーバーによって保護されるサブネットを指定します。これは、IKEv2 標準設定属性の INTERNAL_IP4_SUBNET を介してクライアントにプッシュされます。 （注） この AV ペアは、Cisco IOS リリース 15.2(2)T で導入されました。

属性	ipsec:route-set=interface
タイプ	Cisco AV ペア
書式	文字列
ローカル設定	route set interface
RADIUS 設定	cisco-avpair="ipsec:route-set=interface"
説明	この属性はローカルに使用され、IKEv2 標準設定属性の INTERNAL_IP4_SUBNET を介したピアへの VPN インターフェイス IP アドレスの送信を有効にします。これによって、BGP over VPN などのルーティング プロトコルが実行されます。 （注） Cisco IOS リリース 15.2(2)T で、「ipsec:route-set-interface」AV ペアからこの AV ペアに置き換えられました。

属性	ipsec:route-accept
タイプ	Cisco AV ペア
書式	文字列
ローカル設定	route accept any [tag *tag-id*] [distance *distance*]

RADIUS 設定	cisco-avpair="ipsec:route-accept=any [tag:*tag*] [distance:*distance*]"
例	ipsec:route-accept=any tag=100
説明	この属性はローカルに使用され、IKEv2 標準設定属性の INTERNAL_IP4_SUBNET を介してピアから受信されるサブネットのフィルタを指定します。この属性は、フィルタ処理されたサブネット用に IKEv2 よって追加されるルートのタグと距離も指定します。 （注） Cisco IOS リリース 15.2(2)T で、AV ペア「ipsec:route-accept=accept acl:any」から「ipsec:route-accept=any」に置き換えられ、AV ペア「ipsec:route-accept=deny」から「ipsec:route-accept=none」に置き換えられました。

属性	ipsec:ipsec-flow-limit
タイプ	Cisco AV ペア
書式	整数
ローカル設定	ipsec flow-limit *limit*
RADIUS 設定	cisco-avpair="ipsec:ipsec-flow-limit=*limit*"
説明	この属性は FlexVPN サーバーによって使用され、IPSec dVTI セッションが使用可能な IPSec SA の最大数を指定します。デフォルトでは制限はありません。このパラメータは **crypto ipsec profile** コマンドおよび **set security-policy limit** コマンドと同様です。

属性	ip:interface-config
タイプ	Cisco AV ペア
書式	文字列
ローカル設定	aaa attribute list *list* attribute type interface-config *string*
RADIUS 設定	cisco-avpair="ip:interface-config=interface cmd string"
例	ip:interface-config=ip vrf forwarding red
説明	この属性はローカルに使用され、セッションの仮想アクセス インターフェイスに適用されるインターフェイス コンフィギュレーション モードのコマンド文字列を指定します。ローカル設定の場合、IKEv2 認証ポリシーは、interface-config 属性が必要な AAA 属性リストを示します。

属性	Tunnel-Type

タイプ	IETF
書式	整数
属性 ID	64
RADIUS 設定	Tunnel-Type=type
説明	この属性は、トンネル タイプ（ESP、AH、GRE など）を指定し、FlexVPN サーバーが RADIUS サーバーからセッションの事前共有キーを取得するときに受信されます。

属性	Tunnel-Medium-Type
タイプ	IETF
書式	整数
属性 ID	65、
RADIUS 設定	Tunnel-Medium-Type=type
説明	この属性は、トンネル転送タイプ（IPv4、IPv6 など）を指定し、FlexVPN サーバーが RADIUS サーバーからセッションの事前共有キーを取得するときに受信されます。

属性	Tunnel-Password
タイプ	IETF
書式	文字列
属性 ID	69
RADIUS 設定	Tunnel-Password=string
説明	この属性は、対称の事前共有キーを指定し、FlexVPN サーバーが RADIUS サーバーからセッションの事前共有キーを取得するときに受信されます。

属性	ipsec:ikev2-password-local
タイプ	Cisco AV ペア
書式	文字列
RADIUS 設定	cisco-avpair=“ipsec:ikev2-password-local=*string*”
説明	この属性は、ローカルの事前共有キーを指定し、FlexVPN サーバーが RADIUS サーバーからセッションの事前共有キーを取得するときに受信されます。

属性	ipsec:ikev2-password-remote
タイプ	Cisco AV ペア
書式	文字列
RADIUS 設定	cisco-avpair="ipsec:ikev2-password-remote=*string*"
説明	この属性は、リモートの事前共有キーを指定し、FlexVPN サーバーが RADIUS サーバーからセッションの事前共有キーを取得するときに受信されます。

属性	Framed-IP-Address
タイプ	IETF
書式	IPaddr
属性 ID	8
RADIUS 設定	Framed-IP-Address=*ipaddr*
説明	クライアントに割り当てられる IPv4 アドレスを指定します。これは、IKEv2 標準設定属性の INTERNAL_IP4_ADDRESS を介してクライアントにプッシュされます。

属性	Framed-IP-Netmask
タイプ	IETF
書式	IPaddr
属性 ID	9
ローカル設定	netmask *mask*
RADIUS 設定	Framed-IP-Netmask=*mask*
説明	クライアントに割り当てられる IPv4 アドレスのサブネット マスクを指定します。これは、IKEv2 標準設定属性の INTERNAL_IP4_NETMASK を介してクライアントにプッシュされます。

属性	ipsec:dns-servers
タイプ	Cisco AV ペア
書式	文字列
ローカル設定	dns *primary* [*secondary*]
RADIUS 設定	cisco-avpair="ipsec:dns-servers=*primary secondary*"

説明	クライアントのプライマリ IPv4 DNS サーバーおよびセカンダリ IPv4 DNS サーバーを指定します。これは、IKEv2 標準設定属性の INTERNAL_IP4_DNS を介してクライアントにプッシュされます。

属性	ipsec:wins-servers
タイプ	Cisco AV ペア
書式	文字列
ローカル設定	wins *primary* [*secondary*]
RADIUS 設定	cisco-avpair="ipsec:wins-servers=*primary secondary*"
説明	クライアントのプライマリ IPv4 WINS サーバーおよびセカンダリ IPv4 WINS サーバーを指定します。これは、IKEv2 標準設定属性の INTERNAL_IP4_NBNS を介してクライアントにプッシュされます。

属性	ipsec:route-set=access-list
タイプ	Cisco AV ペア
書式	文字列
ローカル設定	route set access-list {*acl-name* | *acl-number*}
RADIUS 設定	cisco-avpair="ipsec:route-set=access-list {*acl-name* | *acl-number*}"
説明	FlexVPN サーバーによって保護される IPv4 サブネットを指定します。これは、IKEv2 標準設定属性の INTERNAL_IP4_SUBNET を介してクライアントにプッシュされます。 （注） Cisco IOS リリース 15.2(2)T で、「ipsec:inacl」AV ペアからこの AV ペアに置き換えられました。

属性	ipsec:addrv6
タイプ	Cisco AV ペア
書式	文字列
RADIUS 設定	cisco-avpair="ipsec:addrv6=*ipv6-addr*"
説明	クライアントに割り当てられる IPv6 アドレスを指定します。これは、最初の 16 バイトで IKEv2 標準設定属性の INTERNAL_IP6_ADDRESS を介してクライアントにプッシュされます。

属性	ipsec:prefix-len

タイプ	Cisco AV ペア
書式	整数
ローカル設定	該当なし
RADIUS 設定	cisco-avpair="ipsec:prefix-len=*value*"
例	ipsec:prefix-len=24
説明	クライアントに割り当てられる IPv6 アドレスのプレフィックス長を指定します。これは、最後（17 番目）のバイトで IKEv2 標準設定属性の INTERNAL_IP6_ADDRESS を介してクライアントにプッシュされます。

属性	ipsec:ipv6-dns-servers-addr
タイプ	Cisco AV ペア
書式	文字列
ローカル設定	ipv6 dns *primary* [*secondary*]
RADIUS 設定	cisco-avpair="ipsec: ipv6-dns-servers-addr=ipaddr1 *ipaddr2"
説明	クライアントのプライマリ IPv6 DNS サーバーおよびセカンダリ IPv6 DNS サーバーを指定します。これは、IKEv2 標準設定属性の INTERNAL_IP6_DNS を介してクライアントにプッシュされます。

属性	ipsec:route-set=access-list ipv6
タイプ	Cisco AV ペア
書式	文字列
ローカル設定	route set access-list ipv6 acl-name
RADIUS 設定	cisco-avpair="ipsec:route-set=access-list ipv6 *acl-name*"
説明	FlexVPN サーバーによって保護される IPv6 サブネットを指定します。これは、IKEv2 標準設定属性の INTERNAL_IP6_SUBNET を介してクライアントにプッシュされます。 （注） Cisco IOS リリース 15.2(2)T で、「ipsec:ipv6-subnet-acl」AV ペアからこの AV ペアに置き換えられました。

属性	ipsec:banner
タイプ	Cisco AV ペア
書式	文字列

ローカル設定	banner *text*
RADIUS 設定	cisco-avpair="ipsec:banner=*text*"
説明	バナーテキストを指定します。これは、Cisco Unity 属性の MODECFG_BANNER を介してクライアントにプッシュされます。

属性	ipsec:default-domain
タイプ	Cisco AV ペア
書式	文字列
ローカル設定	def-domain *name*
RADIUS 設定	cisco-avpair="ipsec:default-domain=*name*"
説明	デフォルト ドメインを指定します。これは、Cisco Unity 属性の MODECFG_DEFDOMAIN を介してクライアントにプッシュされます。

属性	ipsec:split-dns
タイプ	Cisco AV ペア
書式	文字列
ローカル設定	split-dns name
RADIUS 設定	cisco-avpair="ipsec:split-dns=name"
説明	スプリット DNS 名を指定します。これは、Cisco Unity 属性の MODECFG_SPLITDNS_NAME を介してクライアントにプッシュされます。最大 10 個のスプリット DNS 名を設定できます。

属性	ipsec:ipsec-backup-gateway
タイプ	Cisco AV ペア
書式	文字列
ローカル設定	backup-gateway *name*
RADIUS 設定	cisco-avpair="ipsec:ipsec-backup-gateway=*name*"
説明	バックアップ ゲートウェイを指定します。これは、Cisco Unity 属性の MODECFG_BACKUPSERVERS を介してクライアントにプッシュされます。最大 10 のバックアップ ゲートウェイを設定できます。

属性	ipsec:pfs

タイプ	Cisco AV ペア
書式	整数
ローカル設定	pfs
RADIUS 設定	cisco-avpair="ipsec:pfs=*value*"
説明	IPsec PFS（Perfect Forward Secrecy）の有効/無効を指定します。これは、Cisco Unity 属性の MODECFG_PFS を介してクライアントにプッシュされます。値は、無効の場合は 0、有効の場合は 1 にする必要があります。

属性	ipsec:include-local-lan
タイプ	Cisco AV ペア
書式	整数
ローカル設定	include-local-lan
RADIUS 設定	cisco-avpair="ipsec:include-local-lan=*value*"
説明	ローカル LAN の包含を有効または無効にします。これは、Cisco Unity 属性の MODECFG_INCLUDE_LOCAL_LAN を介してクライアントにプッシュされます。値は、無効の場合は 0、有効の場合は 1 にする必要があります。

属性	ipsec:smartcard-removal-disconnect
タイプ	Cisco AV ペア
書式	整数
ローカル設定	smartcard-removal-disconnect
RADIUS 設定	cisco-avpair="ipsec:smartcard-removal-disconnect =*value*"
説明	スマートカードが取り外されたときの切断を有効または無効にします。これは、Cisco Unity 属性の MODECFG_SMARTCARD_REMOVAL_DISCONNECT を介してクライアントにプッシュされます。値は、無効の場合は0、有効の場合は 1 にする必要があります。

属性	ipsec:configuration-url
タイプ	Cisco AV ペア
書式	文字列
ローカル設定	configuration url *url*
RADIUS 設定	cisco-avpair="ipsec:configuration-url=*url*"

説明	設定ダウンロードの URL を指定します。これは、Cisco FlexVPN 属性の MODECFG_CONFIG_URL を介してクライアントにプッシュされます。

属性	ipsec:configuration-version
タイプ	Cisco AV ペア
書式	整数
ローカル設定	configuration version *version*
RADIUS 設定	cisco-avpair="ipsec:configuration-version=*version*"
説明	ダウンロードする設定のバージョンを指定します。これは、Cisco FlexVPN 属性の MODECFG_CONFIG_VERSION を介してクライアントにプッシュされます。

属性	Route-set remote
タイプ	Cisco AV ペア
書式	文字列
ローカル設定	route set remote {ipv4 ip-address mask | ipv6 ip-address/mask}
RADIUS 設定	cisco-avpair="ipsec:route-set=remote {ipv4 network subnet_mask | ipv6 network/subnet_mask}"
説明	FlexVPN サーバーによって保護されるサブネットを指定します。これは、IKEv2 標準設定属性の INTERNAL_IP4_SUBNET を介してクライアントにプッシュされます。ルートセットプレフィックスは 10 進数形式で表されたサブネットマスク（例：/24）で機能しますが、ルートセットリモートには標準のサブネットマスク表現（例：255.255.255.0）が必要です。 （注）　この AV ペアは、Cisco IOS リリース 3.10.0S で導入されました。

属性	Route-set local
タイプ	Cisco AV ペア
書式	文字列
ローカル設定	route set local {ipv4 ip-address mask | ipv6 ip-address/mask}
RADIUS 設定	cisco-avpair="ipsec:route-set=local {ipv4 network subnet_mask | ipv6 network/subnet_mask}"

説明	この属性は、リモートデバイスから受信したルーティング情報を信頼する必要がないエクストラネットのシナリオで役立ちます。言い換えると、この AV ペアを使用して、リモートルートを拒否し、ルートの追加をローカルに制御できます。 （注） この AV ペアは、Cisco IOS リリース 3.10.0S で導入されました。

第 218 章

付録：IKEv2 およびレガシー VPN

このモジュールでは、暗号マップ ベースの設定で IKEv2 を設定する例を示します。

（注） 暗号マップは、レガシー設定の構造と見なされます。既存の暗号マップベースの設定を移行して、トンネル保護および仮想インターフェイスを使用することをお勧めします。

例：事前共有キー認証方式を使用する暗号マップベースの IKEv2 ピアの設定

次の例に、スタティック暗号マップ IKEv2 発信側とダイナミック暗号マップ IKEv2 応答側との間で事前共有キー認証方式を使用して、暗号マップに基づく IKEv2 ピアを設定する方法を示します。発信側の設定は次のとおりです。

```
crypto ikev2 proposal prop-1
 encryption aes-cbc-128
 integrity sha1
 group 14
!
crypto ikev2 policy pol-1
 match fvrf any
 proposal prop-1
!
crypto ikev2 keyring v2-kr1
 peer abc
  address 209.165.200.231 255.255.255.224
  pre-shared-key abc
 !
```

```
!
!
crypto ikev2 profile prof
 match fvrf any
 match identity remote fqdn dmap-responder
 identity local fqdn smap-initiator
 authentication local pre-share
 authentication remote pre-share
 keyring v2-kr1
!
!
crypto ipsec transform-set trans esp-aes-cbc-128 esp-sha-hmac
!
crypto map cmap 1 ipsec-isakmp
 set peer 209.165.200.225
 set transform-set trans
 set ikev2-profile prof
 match address ikev2list
!
interface Loopback0
 ip address 209.165.200.226 255.255.255.224
!
interface Ethernet0/0
 ip address 209.165.200.227 255.255.255.224
 crypto map cmap
!
ip route 209.165.200.229 255.255.255.224 209.165.200.225
!
ip access-list extended ikev2list
 permit ip any any
!
```

応答側の設定は次のとおりです。

```
crypto ikev2 proposal prop-1
 encryption aes-cbc-128
 integrity sha1
 group 14
!
crypto ikev2 policy pol-1
 match fvrf any
 proposal prop-1
!
crypto ikev2 keyring v2-kr1
 peer abc
  address 209.165.200.228
  pre-shared-key abc
 !
!
!
crypto ikev2 profile prof
 match fvrf any
 match identity remote fqdn smap-initiator
 identity local fqdn dmap-responder
 authentication local pre-share
 authentication remote pre-share
 keyring v2-kr1
 ivrf global
!
!
crypto ipsec transform-set trans esp-aes-cbc-128 esp-sha-hmac
!
crypto dynamic-map dmap 1
 set transform-set trans
```

```
 set reverse-route tag 222
 set ikev2-profile prof
 match address ikev2list
!
crypto map cmap 1 ipsec-isakmp dynamic dmap
!
interface Loopback0
 ip address 209.165.200.230 255.255.255.224
!
interface Ethernet0/0
 ip address 209.165.200.231 255.255.255.224
 crypto map cmap
!
ip route 209.165.200.233 255.255.255.224 209.165.200.228
!
ip access-list extended ikev2list
 permit ip any any
!
```

発信側と応答側との接続を開始するには、発信側の CLI で次のコマンドを入力します。

```
ping 209.165.200.230 source 209.165.200.226
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 209.165.200.230, timeout is 2 seconds:
Packet sent with a source address of 209.165.200.226
%IKEV2-5-OSAL_INITIATE_TUNNEL: Received request to establish an IPsec tunnel; local
traffic selector = Address Range: 209.165.200.226-209.165.200.226 Protocol: 1 Port Range:
 0-65535; remote traffic selector = Address Range: 209.165.200.230-209.165.200.230
Protocol: 1 Port Range: 0-65535
%IKEV2-5-SA_UP: SA UP
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 8/11/12 ms
```

セッションの詳細を表示するには、次の **show** コマンドを入力します。

```
show crypto session
Crypto session current status
Interface: Ethernet0/0
Session status: UP-ACTIVE
Peer: 209.165.200.225 port 500
  IKEv2 SA: local 209.165.200.228/500 remote 209.165.200.231/500 Active
  IPSEC FLOW: permit ip 0.0.0.0/0.0.0.0 0.0.0.0/0.0.0.0
        Active SAs: 2, origin: crypto map
show crypto ikev2 sa detail
Tunnel-id Local                 Remote                fvrf/ivrf            Status
1   209.165.200.228/500  209.165.200.231/500           (none)/(none)        READY
      Encr: AES-CBC, Keysize: 128, Hash: SHA96, DH Grp:14, Auth sign: PSK, Auth verify:
 PSK
      Life/Active Time: 86400/21 sec
      CE id: 1002, Session-id: 2
      Status Description: Negotiation done
      Local spi: 687752902752A6FD       Remote spi: C9DCCFC65493D14F
      Local id: smap-initiator
      Remote id: dmap-responder
      Local req msg id:  2              Remote req msg id:  0
      Local next msg id: 2              Remote next msg id: 0
      Local req queued:  2              Remote req queued:  0
      Local window:      5              Remote window:      5
      DPD configured for 0 seconds, retry 0
      NAT-T is not detected
```

例：証明書認証方式を使用する暗号マップベースの IKEv2 ピアの設定

次の例は、スタティック暗号マップ IKEv2 発信側、ダイナミック暗号マップ IKEv2 応答側、および CA サーバーの間で証明書認証方式を使用して、暗号マップに基づく IKEv2 ピアを設定する方法を示します。発信側の設定は次のとおりです。

```
crypto pki trustpoint ca-server
 enrollment url http://10.1.1.3:80
 revocation-check none
!
crypto pki certificate map cmap-1 1
 subject-name eq hostname = responder
!
!
crypto pki certificate chain ca-server
 certificate 02
  308201AF 30820118 A0030201 02020102 300D0609 2A864886 F70D0101 04050030
  14311230 10060355 04031309 63612D73 65727665 72301E17 0D313030 33313031
  32353132 355A170D 31313033 31303132 35313235 5A301A31 18301606 092A8648
  86F70D01 09021609 494E4954 4941544F 52305C30 0D06092A 864886F7 0D010101
  0500034B 00304802 4100A47E 8C58BA89 8CCDC5A4 5A63BD29 C331A2A5 393F4616
  6B43FD2E 5ED4C81A 913E3B13 33A9B2DC CFC30391 24BB0DC8 B28FD6F1 C008D101
  34C10062 30F88CF7 9D630203 010001A3 4F304D30 0B060355 1D0F0404 030205A0
  301F0603 551D2304 18301680 144871D9 002C66DF D85FACB8 45D1D25F EA357455
  91301D06 03551D0E 04160414 E77C74E7 183AB530 83DC531B 1DE3DA1D 914A925D
  300D0609 2A864886 F70D0101 04050003 81810042 21934B77 7E485E6F EE717D75
  6407B361 45190CEF E1A29CF2 6FA29E9A 5ECC1CEE B273533D 1453F6CE 1FDDA747
  7E701B4B 2A2AE53F D67C2345 952325BA 30950435 0706C5EE A7A8B414 CFEEB7A2
  9CD46F8F 3F663268 A20C4CCF E75D61EF 03FBA85D EDD6B26E 63653F09 F97DAFA6
  6C76E44E C9CA3FDC 6CD85D30 169A1D9E 4E870B
        quit
 certificate ca 01
  30820201 3082016A A0030201 02020101 300D0609 2A864886 F70D0101 04050030
  14311230 10060355 04031309 63612D73 65727665 72301E17 0D313030 33313031
  32343933 385A170D 31333033 30393132 34393338 5A301431 12301006 03550403
  13096361 2D736572 76657230 819F300D 06092A86 4886F70D 01010105 0003818D
  00308189 02818100 DA4ECE09 B998F670 598F32C1 7E9FA920 1D217AC4 293B842E
  7563CE11 B2F0F822 23077930 636C8293 00F6CFDD F6C9B0F5 8348BE58 6478F631
  7D44152F 494AEBCC A507FA6B 408D6BBB FAAB0A7A 2E7546A8 CA70F9A6 0F7F6824
  554BD833 060D657D ABDF406C 69EEF449 7A4F9AFE 6F0852E7 05DEDAC1 D433191E
  712868C2 A94E642B 02030100 01A36330 61300F06 03551D13 0101FF04 05300301
  01FF300E 0603551D 0F0101FF 04040302 0186301F 0603551D 23041830 16801448
  71D9002C 66DFD85F ACB845D1 D25FEA35 74559130 1D060355 1D0E0416 04144871
  D9002C66 DFD85FAC B845D1D2 5FEA3574 5591300D 06092A86 4886F70D 01010405
  00038181 00AFC36B 8A917284 06BD51CB 83BDC4E8 9457A361 6CAAF416 3BBEF691
  04215AC5 EDBC5730 C071C2FB 8A6C90CF D6AB39C2 3BC2147F D35553D9 028B2155
  802E50DB 48CDE067 B3857447 89A1C733 D81EFEF7 1115480F 70ED2F22 F27E35A1
  F3BB597C 7C8F717B FAAD79D3 0F469702 DE9190E4 B1B0808E 46A118EB 887CEAEB
  DFE2900E D2
        quit
crypto ikev2 proposal prop-1
 encryption aes-cbc-128
 integrity sha1
 group 14
!
crypto ikev2 policy pol-1
 match fvrf any
```

```
 proposal prop-1
!
crypto ikev2 profile prof
 match fvrf any
 match certificate cmap-1
 identity local dn
 authentication local rsa-sig
 authentication remote pre-share
 authentication remote rsa-sig
 pki trustpoint ca-server
!
!
crypto ipsec transform-set trans esp-aes-cbc-128 esp-sha-hmac
!
crypto map cmap 1 ipsec-isakmp
 set peer 209.165.200.225
 set transform-set trans
 set ikev2-profile prof
 match address ikev2list
!
interface Loopback0
 ip address 209.165.200.226 255.255.255.224
!
interface Ethernet0/0
 ip address 209.165.200.227 255.255.255.224
 crypto map cmap
!
interface Ethernet1/0
 ip address 209.165.200.228 255.255.255.224
!
ip route 209.165.200.229 255.255.255.224 209.265.200.231
!
ip access-list extended ikev2list
 permit ip any any
!
```

応答側の設定は次のとおりです。

```
crypto pki trustpoint ca-server
 enrollment url http://10.1.1.3:80
 revocation-check none
!
!
!
crypto pki certificate map cmap-2 1
 subject-name eq hostname = initiator
!
crypto pki certificate chain ca-server
 certificate 03
  308201AF 30820118 A0030201 02020103 300D0609 2A864886 F70D0101 04050030
  14311230 10060355 04031309 63612D73 65727665 72301E17 0D313030 33313031
  32353231 325A170D 31313033 31303132 35323132 5A301A31 18301606 092A8648
  86F70D01 09021609 52455350 4F4E4445 52305C30 0D06092A 864886F7 0D010101
  0500034B 00304802 4100B517 EB8E64E1 B58CB014 07B3A6AF E6B69577 87486367
  9471B1DA BC66B847 DFA5073A 82121332 E787EA2D 3C433514 39033074 4095E7C7
  67A387A1 EBD24692 A76F0203 010001A3 4F304D30 0B060355 1D0F0404 030205A0
  301F0603 551D2304 18301680 144871D9 002C66DF D85FACB8 45D1D25F EA357455
  91301D06 03551D0E 04160414 DFF2401C 53276D96 89DE8C0A 786CCA71 C9EA792B
  300D0609 2A864886 F70D0101 04050003 8181002C 6E334273 CB832A95 3DDC6293
  669E416C A134D543 20952BC3 14A5C0B0 03AE011C 963AF523 C7C5C935 4FE9B2A5
  F24B3161 4D0D723A FA428BD1 85ADF172 B4007067 43C27D8A 1F74ED3D DEBE9F73
  1F515355 E77E766C AEACC303 39457991 29AB090C 99E21B5B 60DCB2C8 780B4479
  3EB3D46B B66C8C26 15311A7A B7A4ED97 32727C
        quit
```

```
 certificate ca 01
  30820201 3082016A A0030201 02020101 300D0609 2A864886 F70D0101 04050030
  14311230 10060355 04031309 63612D73 65727665 72301E17 0D313030 33313031
  32343933 385A170D 31333033 30393132 34393338 5A301431 12301006 03550403
  13096361 2D736572 76657230 819F300D 06092A86 4886F70D 01010105 0003818D
  00308189 02818100 DA4ECE09 B998F670 598F32C1 7E9FA920 1D217AC4 293B842E
  7563CE11 B2F0F822 23077930 636C8293 00F6CFDD F6C9B0F5 8348BE58 6478F631
  7D44152F 494AEBCC A507FA6B 408D6BBB FAAB0A7A 2E7546A8 CA70F9A6 0F7F6824
  554BD833 060D657D ABDF406C 69EEF449 7A4F9AFE 6F0852E7 05DEDAC1 D433191E
  712868C2 A94E642B 02030100 01A36330 61300F06 03551D13 0101FF04 05300301
  01FF300E 0603551D 0F0101FF 04040302 0186301F 0603551D 23041830 16801448
  71D9002C 66DFD85F ACB845D1 D25FEA35 74559130 1D060355 1D0E0416 04144871
  D9002C66 DFD85FAC B845D1D2 5FEA3574 5591300D 06092A86 4886F70D 01010405
  00038181 00AFC36B 8A917284 06BD51CB 83BDC4E8 9457A361 6CAAF416 3BBEF691
  04215AC5 EDBC5730 C071C2FB 8A6C90CF D6AB39C2 3BC2147F D35553D9 028B2155
  802E50DB 48CDE067 B3857447 89A1C733 D81EFEF7 1115480F 70ED2F22 F27E35A1
  F3BB597C 7C8F717B FAAD79D3 0F469702 DE9190E4 B1B0808E 46A118EB 887CEAEB
  DFE2900E D2
        quit
crypto ikev2 proposal prop-1
 encryption aes-cbc-128
 integrity sha1
 group 14
!
crypto ikev2 policy pol-1
 match fvrf any
 proposal prop-1
!
!
crypto ikev2 profile prof
 match fvrf any
 match certificate cmap-2
 identity local dn
 authentication local rsa-sig
 authentication remote pre-share
 authentication remote rsa-sig
 pki trustpoint ca-server
!
!
crypto ipsec transform-set trans esp-aes-cbc-128 esp-sha-hmac
!
crypto dynamic-map dmap 1
 set transform-set trans
 set ikev2-profile prof
!
!
crypto map cmap 1 ipsec-isakmp dynamic dmap
interface Loopback0
 ip address 209.165.200.230 255.255.255.224
!
interface Ethernet0/0
 ip address 209.165.200.231 255.255.255.224
 crypto map cmap
!
interface Ethernet1/0
 ip address 209.165.200.232 255.255.255.224
!
ip route 209.165.200.233 255.255.255.224 209.165.200.228
!
ip access-list extended ikev2list
 permit ip host 209.165.200.231 host 209.165.200.228
```

CA サーバーの設定は次のとおりです。

```
crypto pki server ca-server
 grant auto
!
crypto pki trustpoint ca-server
 revocation-check crl
 rsakeypair ca-server
!
!
crypto pki certificate chain ca-server
 certificate ca 01
  30820201 3082016A A0030201 02020101 300D0609 2A864886 F70D0101 04050030
  14311230 10060355 04031309 63612D73 65727665 72301E17 0D303930 33303831
  36333335 395A170D 31323033 30373136 33333539 5A301431 12301006 03550403
  13096361 2D736572 76657230 819F300D 06092A86 4886F70D 01010105 0003818D
  00308189 02818100 99750598 EF4AF8B4 823DEF66 2F3BBA31 81C2DC5F D9B4040B
  99FB6020 22243CD6 B9F24C84 A543D7DB DD0B3018 2E36208C D0FD4015 EAF0DA69
  C1B0302B 87CEC34B 8646593F 0185AF02 0B86A3F3 5E5C3880 A992CD4A 79F13403
  411CC61F 07CEB4D9 0E967CB2 FAE0A899 5A3B6C87 73111F06 128465DA A45291F8
  F828C5DC 657487E7 02030100 01A36330 61300F06 03551D13 0101FF04 05300301
  01FF300E 0603551D 0F0101FF 04040302 0186301F 0603551D 23041830 1680147B
  D032BFB7 B3F70F1A 597B7C1E 1B42E472 5CCD6030 1D060355 1D0E0416 04147BD0
  32BFB7B3 F70F1A59 7B7C1E1B 42E4725C CD60300D 06092A86 4886F70D 01010405
  00038181 003838FA 628804EF E9FF69D9 3D5E299C 29074B2C AE33A563 8AF75976
  78FB68D4 5EF1E27B 04936FDF 78A09432 5348849D F79E17F5 70B233C9 2C1535D0
  506F0C35 99335012 84BBA3DC 050FD3C9 6E7B1D63 41ACC2B5 2B02432D BA2CC2CF
  E379DEA0 A9C208AC 0BEBB2D8 E6488815 EB12F1E0 19072D55 D5D11A49 739144D8
  271A842E ED
        quit
!
interface Ethernet1/0
 ip address 209.165.200.232 255.255.255.224
!
ip http server
```

CA およびデバイス証明書を取得するには、**crypto pki authenticate ca-server** コマンドおよび **crypto pki enroll ca-server** コマンドを入力します。発信側と応答側との接続を開始するには、発信側の CLI で次のコマンドを入力します。

```
ping 209.165.200.230 source 209.165.200.226
```

コマンドの出力は次のようになります。

```
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 209.165.200.230, timeout is 2 seconds:
Packet sent with a source address of 209.165.200.226
%IKEV2-5-OSAL_INITIATE_TUNNEL: Received request to establish an IPsec tunnel; local
traffic selector = Address Range: 209.165.200.226-209.165.200.226 Protocol: 1 Port Range:
 0-65535; remote traffic selector = Address Range: 209.165.200.230-209.165.200.230
Protocol: 1 Port Range: 0-65535
%IKEV2-5-SA_UP: SA UP
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 8/11/12 ms
```

セッションの詳細を表示するには、応答側の CLI に次の **show** コマンドを入力します。

```
show crypto session
Crypto session current status
Interface: Ethernet0/0
Session status: UP-ACTIVE
Peer: 1.1.1.1 port 500
```

```
  IKEv2 SA: local 209.165.200.231/500 remote 209.165.200.227/500 Active
  IPSEC FLOW: permit ip 0.0.0.0/0.0.0.0 host 209.165.200.226
        Active SAs: 2, origin: dynamic crypto map
show crypto ikev2 sa detailed
Tunnel-id Local                 Remote                fvrf/ivrf            Status
1         209.165.200.231/500 209.165.200.227/500  (none)/(none)                  READY
      Encr: AES-CBC, Keysize: 128, Hash: SHA96, DH Grp:14, Auth sign: RSA, Auth verify:
 RSA
      Life/Active Time: 86400/846 sec
      CE id: 1001, Session-id: 1
      Status Description: Negotiation done
      Local spi: F79756E978ED41C7       Remote spi: 188FB9A119516D34
      Local id: hostname=RESPONDER
      Remote id: hostname=INITIATOR
      Local req msg id:  0              Remote req msg id:  2
      Local next msg id: 0              Remote next msg id: 2
      Local req queued:  0              Remote req queued:  2
      Local window:      5              Remote window:      5
      DPD configured for 0 seconds, retry 0
      NAT-T is not detected
```

例：暗号マップ ベースおよび dVTI ベースの IKEv2 ピアの設定

次の例は、スタティック クリプト マップ IKEv2 発信側と dVTI に基づく IKEv2 応答側との間に事前共有キー認証方式を使用し、クリプト マップと dVTI ベースの IKEv2 ピアを設定する方法を示します。発信側の設定は次のとおりです。

```
crypto ikev2 proposal prop-1
 encryption aes-cbc-128
 integrity sha1
 group 14
!
crypto ikev2 policy pol-1
 match fvrf any
 proposal prop-1
!
crypto ikev2 keyring v2-kr1
 peer abc
  address 0.0.0.0 0.0.0.0
  pre-shared-key abc
 !
!
!
crypto ikev2 profile prof
 match fvrf any
 match identity remote address 0.0.0.0
 authentication local pre-share
 authentication remote pre-share
 keyring v2-kr1
!
crypto ipsec transform-set trans esp-aes-cbc-128 esp-sha-hmac
!
crypto map cmap 1 ipsec-isakmp
 set peer 206.165.200.235
 set transform-set trans
 set ikev2-profile prof
 match address ikev2list
```

```
!
interface Loopback0
 ip address 206.165.200.226 255.255.255.224
!
interface Ethernet0/0
 ip address 206.165.200.227 255.255.255.224
 crypto map cmap
!
ip route 206.165.200.229 255.255.255.224 206.165.200.235
!
ip access-list extended ikev2list
 permit ip host 206.165.200.227 host 206.165.200.235
 permit ip 206.165.200.233 255.255.255.224 206.165.200.229 255.255.255.224
```

応答側の設定は次のとおりです。

```
crypto ikev2 proposal prop-1
 encryption aes-cbc-128
 integrity sha1
 group 14
!
crypto ikev2 policy pol-1
 match fvrf any
 proposal prop-1
!
crypto ikev2 keyring v2-kr1
 peer cisco
  address 0.0.0.0 0.0.0.0
  pre-shared-key cisco
 !
!
!
crypto ikev2 profile prof
 match fvrf any
 match identity remote address 0.0.0.0
 authentication local pre-share
 authentication remote pre-share
 keyring v2-kr1
 virtual-template 1
!
crypto ipsec transform-set set esp-aes-cbc-128 esp-sha-hmac
!
crypto ipsec profile vi
 set transform-set set
 set ikev2-profile prof
!
interface Loopback0
 ip address 206.165.200.230 255.255.255.224
!
interface Ethernet0/0
 ip address 206.165.200.235 255.255.255.224
!
interface Virtual-Template1 type tunnel
 ip unnumbered Ethernet0/0
 ip mtu 1000
 tunnel source Ethernet0/0
 tunnel mode ipsec ipv4
 tunnel protection ipsec profile vi
!
```

発信側と応答側との接続を開始するには、発信側の CLI で次のコマンドを入力します。

```
ping 206.165.200.230 source 206.165.200.226
```

```
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 206.165.200.230, timeout is 2 seconds:
Packet sent with a source address of 206.165.200.226
%IKEV2-5-OSAL_INITIATE_TUNNEL: Received request to establish an IPsec tunnel; local
traffic selector = Address Range: 206.165.200.226-206.165.200.226 Protocol: 1 Port Range:
 0-65535; remote traffic selector = Address Range: 206.165.200.230-206.165.200.230
Protocol: 1 Port Range: 0-65535
%IKEV2-5-SA_UP: SA UP
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 8/11/12 ms
```

次の **show** コマンドを Easy VPN サーバーに入力すると、セッションの詳細が表示されます。

```
show crypto session
Crypto session current status
Interface: Virtual-Access2
Session status: UP-ACTIVE
Peer: 206.165.200.227 port 500
  IKEv2 SA: local 206.165.200.235/500 remote 206.165.200.227/500 Active
  IPSEC FLOW: permit ip 206.165.200.229/255.255.255.224 206.165.200.233/255.255.255.224
        Active SAs: 2, origin: crypto map
show crypto ikev2 sa detail
Tunnel-id Local                 Remote                fvrf/ivrf            Status
1   206.165.200.235/500      206.165.200.227/500       (none)/(none)         READY
      Encr: AES-CBC, Keysize: 128, Hash: SHA96, DH Grp: 14, Auth sign: PSK, Auth verify:
 PSK
      Life/Active Time: 86400/8 sec
      CE id: 1001, Session-id: 1
      Status Description: Negotiation done
      Local spi: 305F610F57428834       Remote spi: D9D183B5689AEDCD
      Local id: 206.165.200.235
      Remote id: 206.165.200.227
      Local req msg id:  0              Remote req msg id:  2
      Local next msg id: 0              Remote next msg id: 2
      Local req queued:  0              Remote req queued:  2
      Local window:      5              Remote window:      5
      DPD configured for 0 seconds, retry 0
      NAT-T is not detected
show crypto route
VPN Routing Table: Shows RRI and VTI created routes
Codes: RRI - Reverse-Route, VTI- Virtual Tunnel Interface
        S - Static Map ACLs
Routes created in table GLOBAL DEFAULT
206.165.200.233/255.255.255.224 [1/0] via 206.165.200.227 tag 0
                                on Virtual-Access2 RRI
```

例： sVTI ベース IKEv2 ピアを使用した IPSec の設定

次の例は、sVTI IKEv2 発信側と sVTI IKEv2 応答側との間に事前共有キー認証方式を使用する IPsec の設定方法を示します。発信側の設定は次のとおりです。

```
crypto ikev2 proposal prop-1
 encryption aes-cbc-128
 integrity sha1
 group 14
!
crypto ikev2 policy pol-1
 match fvrf any
 proposal prop-1
```

```
!
crypto ikev2 keyring v2-kr1
 peer abc
  address 209.165.200.225
  pre-shared-key abc
 !
!
!
crypto ikev2 profile prof
 match fvrf any
 match identity remote address 209.165.200.231 255.255.255.224
 authentication local pre-share
 authentication remote pre-share
 keyring v2-kr1
!
!
crypto ipsec transform-set trans esp-aes-cbc-128 esp-sha-hmac
!
crypto ipsec profile ipsecprof
 set transform-set trans
 set ikev2-profile prof
!
interface Loopback0
 ip address 209.165.200.226 255.255.255.224
!
interface Tunnel0
 ip address 10.0.0.1 255.255.255.0
 tunnel source 209.165.200.231
 tunnel mode ipsec ipv4
 tunnel destination 209.165.200.225
 tunnel protection ipsec profile ipsecprof
!
interface Ethernet0/0
 ip address 209.165.200.231 255.255.255.224
!
ip route 209.165.200.229 255.255.255.224 Tunnel0
!
```

応答側の設定は次のとおりです。

```
crypto ikev2 proposal prop-1
 encryption aes-cbc-128
 integrity sha1
 group 14
!
crypto ikev2 policy pol-1
 match fvrf any
 proposal prop-1
!
crypto ikev2 keyring v2-kr1
 peer abc
  address 209.165.200.231
  pre-shared-key abc
 !
!
!
crypto ikev2 profile prof
 match fvrf any
 match identity remote address 209.165.200.231 255.255.255.224
 authentication local pre-share
 authentication remote pre-share
 keyring v2-kr1
!
!
```

```
crypto ipsec transform-set trans esp-aes-cbc-128 esp-sha-hmac
!
crypto ipsec profile ipsecprof
 set transform-set trans
 set ikev2-profile prof
!
crypto map cmap 1 ipsec-isakmp dynamic dmap
!
interface Loopback0
 ip address 209.165.200.230 255.255.255.224
!
interface Tunnel0
 ip address 10.0.0.2 255.255.255.0
 tunnel source 209.165.200.225
 tunnel mode ipsec ipv4
 tunnel destination 209.165.200.231
 tunnel protection ipsec profile ipsecprof
!
interface Ethernet0/0
 ip address 209.165.200.231 255.255.255.224
!
ip route 209.165.200.233 255.255.255.224 Tunnel0
```

IKEv2 ピアの sVTI では、セッションは sVTI インターフェイスが有効なときにだけ開始されます。つまり、セッションの開始のためにネットワーク トラフィックは必要ありません。発信側と応答側との間のトラフィックを確認するには、発信側の CLI で次のコマンドを入力します。

```
ping 209.165.200.230 source 209.165.200.226
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 209.165.200.230, timeout is 2 seconds:
Packet sent with a source address of 209.165.200.226
%IKEV2-5-OSAL_INITIATE_TUNNEL: Received request to establish an IPsec tunnel; local
traffic selector = Address Range: 209.165.200.226-209.165.200.226 Protocol: 1 Port Range:
 0-65535; remote traffic selector = Address Range: 209.165.200.230-209.165.200.23 Protocol:
 1 Port Range: 0-65535
%IKEV2-5-SA_UP: SA UP
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 8/11/12 ms
```

次の **show** コマンドを発信側の CLI に入力すると、セッションの詳細が表示されます。

```
show crypto session
Crypto session current status
Interface: Ethernet0/0
Session status: UP-ACTIVE
Peer: 209.165.200.225 port 500
  IKEv2 SA: local 209.165.200.231/500 remote 209.165.200.225/500 Active
  IPSEC FLOW: permit ip 0.0.0.0/0.0.0.0 0.0.0.0/0.0.0.0
        Active SAs: 2, origin: crypto map
show crypto ikev2 sa detailed
Tunnel-id Local                 Remote                fvrf/ivrf            Status
1   209.165.200.231/500  209.165.200.225/500           (none)/(none)        READY
      Encr: AES-CBC, Keysize: 128, Hash: SHA96, DH Grp: 14, Auth sign: PSK, Auth verify:
 PSK
      Life/Active Time: 86400/21 sec
      CE id: 1002, Session-id: 2
      Status Description: Negotiation done
      Local spi: 687752902752A6FD       Remote spi: C9DCCFC65493D14F
      Local id: smap-initiator
      Remote id: dmap-responder
      Local req msg id:  2              Remote req msg id:  0
      Local next msg id: 2              Remote next msg id: 0
```

```
      Local req queued:  2              Remote req queued:  0
      Local window:      5              Remote window:      5
      DPD configured for 0 seconds, retry 0
      NAT-T is not detected
```

例：DMVPN ネットワークでの IKEv2 の設定

DMVPN は、IKEv1 と IKEv2 の間で同一のトンネル保護 CLI を使用します。DMVPN トンネルに適用される IPSec プロファイルは、IKEv2 プロファイルのみを参照します。DMVPN ハブの設定は次のとおりです。

```
crypto ikev2 keyring cisco-ikev2-keyring
 peer dmvpn-node
 description symmetric pre-shared key for the hub/spoke
 address 0.0.0.0 0.0.0.0
 pre-shared-key cisco123
crypto ikev2 profile cisco-ikev2-profile
 keyring cisco-ikev2-keyring
 authentication pre-shared
 match local address 0.0.0.0
crypto ipsec profile cisco-ipsec-ikev2
 set transform-set cisco-ts
 set ikev2-profile cisco-ikev2-profile
! interface Tunnel 0
 description This is the Legacy IKEv1 facing tunnel on the hub
 ip address 1.1.1.99 255.255.255.0
 no ip redirects
 ip nhrp map multicast dynamic
 ip nhrp network-id 99
 ip nhrp redirect
 no ip split-horizon eigrp 1
 tunnel source Ethernet0/0
 tunnel mode gre multipoint
 tunnel protection ipsec profile cisco-ipsec
 !
interface Tunnel1
 description This would be the new IKEv2 facing tunnel on the hub
 ip address 2.2.2.99 255.255.255.0
 no ip redirects
 ip nhrp map multicast dynamic
 ip nhrp network-id 100
 no ip split-horizon eigrp 1
 tunnel source Ethernet0/1
 tunnel mode gre multipoint
 tunnel protection ipsec profile cisco-ipsec-ikev2
```

IKEv2 の設定は次のとおりです。

```
crypto ikev2 profile cisco-ikev2-profile
 keyring cisco-ikev2-keyring
 authentication pre-shared
 match local address 0.0.0.0
crypto ipsec profile cisco-ipsec-ikev2
 set transform-set cisco-ts
 set ikev2-profile cisco-ikev2-profile
interface Tunnel1
 ip address 2.2.2.11 255.255.255.0
 no ip redirects
 ip nhrp map 2.2.2.99 22.22.22.99
```

```
ip nhrp map multicast 22.22.22.99
ip nhrp network-id 100 ? Keep this same for all IKEv2 spokes for clarity
ip nhrp nhs 2.2.2.99 ? This points to the hub's IKEv2 facing interface
tunnel source Ethernet0/1
tunnel mode gre multipoint
tunnel protection ipsec profile cisco-ipsec-ikev2
```

第 XXII 部

Cisco Group Encrypted Transport VPN

第 219 章

Cisco Group Encrypted Transport VPN

Cisco Group Encrypted Transport VPN（GET VPN）は、Cisco IOS デバイス上で発生する、または Cisco IOS デバイス を経由するプライベート WAN 上の IP マルチキャスト トラフィック グループまたはユニキャスト トラフィックの安全を守るために必要な一連の機能です。GET VPN では、キーイング プロトコルであるグループ ドメイン オブ インタープリテーション（GDOI）と、IP セキュリティ（IPsec）暗号化が組み合されており、ユーザは、IP マルチキャスト トラフィックやユニキャスト トラフィックをセキュリティ保護するための効果的な方式を利用できます。GET VPN では、ルータによって、トンネル化されていない（つまり「ネイティブな」）IP マルチキャストおよびユニキャスト パケットに対して暗号化を適用できるので、マルチキャストおよびユニキャスト トラフィックを保護するためにトンネルを設定する必要がありません。

（注） セキュリティに対する脅威は、脅威からの保護に役立つ暗号化技術と同様に絶え間なく変化しています。シスコの暗号化に関する最新の推奨事項の詳細は、『Next Generation Encryption』（NGE）ホワイトペーパーを参照してください。

ここでは、Cisco GET VPN の設定、確認、およびトラブルシューティングの方法を説明します。

Cisco Group Encrypted Transport VPN には、次のような利点があります。

- データ セキュリティおよびトランスポート認証が利用可能で、すべての WAN トラフィックを暗号化することによって、セキュリティ適合性および内部規則を満たすことが可能。
- 大規模なネットワーク メッシュが可能であり、グループ暗号キーを使用した、複雑なピアツーピアのキー管理が不要。
- マルチプロトコル ラベル スイッチング（MPLS）ネットワークの場合でも、ネットワーク インテリジェンス（フルメッシュ接続、ナチュラル ルーティング パス、Quality of Service（QoS）など）を維持。
- 一元化されたキー サーバを使用してメンバーシップを簡単に管理可能。
- 中央集中型ハブを介した転送が不要な、サイト間におけるフルタイムの直接通信を実現することによって遅延とジッタの低減が可能。

- マルチキャスト トラフィックの複製にコア ネットワークを使用し、個々のピア サイトごとにおけるパケットの複製を不要にすることによって、宅内装置（CPE）およびプロバイダー エッジ（PE）暗号化デバイスの負荷を削減。

Cisco Group Encrypted Transport VPN の前提条件

- Cisco IOS XE リリース 2.3 以降を使用している必要があります。
- IPsec およびインターネット キー交換（IKE）に関する知識が必要です。
- Cisco IOS XE グローバル ルータにおけるマルチキャストおよびユニキャスト ルーティングの設定方法を知っている必要があります。
- IKE ポリシーを設定する際、IKE ライフタイムを最小値の 5 分に設定する必要があります。その結果、不要なリソースが、IKE セキュリティ アソシエーション（SA）のメンテナンスで無駄に使用されなくなります。登録 IKE SA が確立したら、キー再生成 SA が作成済みとなり、将来のキー再生成を受け入れるために使用されるので、登録 SA を維持する必要はなくなります。
- グループのキー再生成のライフタイムが 300 秒に設定され、ポリシーの変更による強制的なキー再生成が実行されると、ネットワークの問題が発生する可能性があります。この問題を解決するには、グループのキー再生成（KEK）に関して次のいずれかが推奨されます。
  - ライフタイムを、transform-set で設定された TEK ライフタイムの 3 倍に設定します。
  - グループのキー再生成のライフタイムをデフォルト値の 24 時間（86,400 秒）に設定します。
  - キー再生成のライフタイムを 7,200 秒（2 時間）に設定します。

Cisco Group Encrypted Transport VPN の制約事項

- カウンタ ベースのアンチ リプレイ用に高パケット レートを暗号化する場合、ライフタイムを長く設定し過ぎないようにしてください。長く設定し過ぎると、シーケンス番号のラップに数時間かかってしまう可能性があります。たとえば、パケット レートが毎秒 100

キロパケットである場合、ライフタイムは、SA がシーケンス番号のラップ前に使用されるように 11.93 時間より短く設定する必要があります。

- 仮想 PPP インターフェイスを備えた Cisco ASR 1000 シリーズ アグリゲーション ルータは、GETVPN グループメンバーとして設定できません。
- Cisco IOS XE ソフトウェアでは、ネットワークにアクセスするユーザの包含ポート範囲を **permit** コマンドを使用して拡張 ACL と照合することはできません。
- ユニキャスト トラフィックおよびカウンタベースのアンチ リプレイでは、グループ メンバーの 1 つが停止してから復帰した場合、シーケンス番号がグループ メンバー間で同期されていない状態になる可能性があります。たとえば、グループ メンバー 1 からグループ メンバー 2 へのトラフィックが存在し、最後のシーケンス番号が *n* になる場合です。Group Member 1 が停止してから復帰します。グループ メンバー 1 における SA のシーケンス番号は現在 1 で始まっていますが、グループ メンバー 2 では、前のシーケンス番号から連続する番号（*n*+1）と予測しています。このような状況の結果、Group Member 1 のシーケンス番号が *n* になるか、次のキー再生成まで、Group Member 1 からの後続のトラフィックは停止します。
- 転送モード トラフィック セレクタを設定する際、転送モードを SA にすることが可能です。パケット サイズが MTU を超え、パケットが転送できなくなると、SA が発生します。
- 転送モードは、Group Encrypted Transport VPN Mode（GM）から GM へのトラフィックだけに使用してください。
- カプセル化されたパケットの IP ヘッダー内の don't fragment bit（df-bit）設定を上書きする場合、グローバル コンフィギュレーション モードで上書きコマンドを設定する必要があります。GET VPN では、インターフェイス コンフィギュレーションは受け入れられません。この制限事項は、GET VPN にだけ当てはまります。IPsec では、グローバル コンフィギュレーション専用上書きコマンドおよびインターフェイス専用上書きコマンドの両方が受け入れられます。
- カウンタベースのアンチ リプレイは推奨できません。カウンタベースのアンチ リプレイは、1 つのグループ内に 2 つのグループ メンバーが存在している時にだけ動作します。
- GET VPN 時間ベースのアンチリプレイ機能では、Cisco ASR 1000 シリーズアグリゲーション サービス ルータと Cisco 4330 サービス統合型ルータの Encapsulating Security Payload（ESP）転送モードがサポートされていません。
- Path MTU Discovery（PMTUD）は、GET VPN に対しては動作しないので、df-bit が設定されており、中間リンクの MTU がカプセル化されたパケットのサイズより小さい場合に、カプセル化されたパケットが廃棄される可能性があります。このようなイベントが発生した場合、パケットを廃棄するルータによってパケット上の発信元 IP アドレスに対して通知が送信され、df-bit の設定のためにルータによるパケットのフラグメント化ができなかったために、パケットが廃棄されたことが通知されます。GET VPN ではヘッダー保存機能があるため、このメッセージはカプセル化を行うエンドポイントを経由しないで、直接データの発信元に送信されます。そのため、カプセル化を行うルータは、カプセル化の後で df-bit を設定する前により小さいサイズにパケットをフラグメント化しなければならないと判断できません。パケット上の df-bit 設定は継続され、中間ルータにおいて、それら

のパケットは引き続き廃棄されます（これはトラフィックの Null ルーティングと呼ばれます）。

- Cisco IOS XE リリース 3.5S 以前のリリースでは、Cisco IOS XE イメージを使用してキーサーバを設定することはできません。これらは Cisco IOS T ベースまたはメインラインベース イメージを使用して設定する必要があります。これは、Cisco IOS XE リリース 3.6S 以降のリリースの制約ではありません。
- 暗号化エンジンの最適化のために、時間ベースのアンチリプレイ（TBAR）のオーバーヘッドは 12 バイトではなく 16 バイトです。
- GET VPN は、TBAR Cisco Metadata Protocol を使用して TBAR 情報を伝送します。Cisco IOS ソフトウェアは 12 バイトのヘッダーを使用し、Cisco IOS XE は 16 バイトのヘッダーを使用します。GETVPN グループメンバーで設定され、アンチリプレイに TBAR を使用する Cisco IOS XE ソフトウェアでは、IPsec トラフィックの有効な MTU（「クリアテキスト MTU」）が、Cisco IOS ソフトウェアによって設定されるグループメンバーよりも 4 バイト小さくなります。GET VPN グループメンバーを Cisco IOS ソフトウェアから Cisco IOS XE ソフトウェアに移行する場合、4 バイトの減少により、予期しないパフォーマンスの問題が発生する可能性があります。
- Cisco ASR 1000 シリーズ アグリゲーション サービス ルータの GET VPN 設定で正常なトラフィック フローを保証するため、Cisco IOS XE リリース 3.12S 以前のリリース、Cisco IOS XE リリース 3.14S および Cisco IOS XE リリース 3.15S では 20 秒を超える TBAR ウィンドウ サイズが推奨されます。Cisco IOS XE リリース 3.13S、Cisco IOS XE リリース 3.16S 以降のリリースでは、20 秒以内の TBAR ウィンドウ サイズが許可されます。
- 暗号マップは、トンネルインターフェイスとポートチャネルインターフェイス上でサポートされません。ただし、ルールの例外として、GDOI の暗号マップはトンネルインターフェイスでサポートされます。
- 暗号マップは VLAN インターフェイスではサポートされません。
- Mediatrace で使用される RSVP は、「ルータアラート」 IP オプションフラグを設定します。Cavium N2 暗号アクセラレータは、IP オプションの使用をサポートしていません。そのため、Mediatrace は、Cavium N2 を搭載した ASR1000 での IPsec 暗号化に失敗します。Mediatrace は、Cavium N2 を搭載した ASR1000 での GETVPN 暗号化（ヘッダーが維持される IPsec）に失敗します。
- 拒否（deny）ステートメントは、ローカルでのみ GM に追加できます。許可（permit）ステートメントは、ローカルに設定されたポリシーではサポートされません。競合が発生した場合、ローカルポリシーは、KS からダウンロードされたポリシーを上書きします。
- Cisco ASR 1000 シリーズアグリゲーション サービス ルータでは、再登録に失敗した場合、実際の ACE の代わりにダミーの ACE がプッシュされるため、QFP からのアウトバウンドフローは削除されません。その結果、SA が期限切れになると、GM は、トラフィックをローカルにドロップするのではなく、期限切れの SPI を使用してアウトバウンドトラフィックを暗号化しつづけます。無効な SPI メカニズムが原因で、トラフィックは、最終的に受信側 GM でドロップされます。

- キーサーバーで IPv6 アクセスリストを設定しているときは、**permit** コマンドまたは **deny** コマンドで **ahp** オプションを使用しないでください。
- GETVPN グループメンバーとして動作している Cisco IOS XE プラットフォームは、1 つの GETVPN-ipv4 グループ メンバー インスタンスと 1 つの GETVPN-ipv6 グループ メンバー インスタンスのみをサポートできます。
- **SSO の制約事項**
- Cisco ASR 1000 シリーズ ルータは、Embedded Services Processor（ESP）スイッチオーバーでステートフル IPsec セッションをサポートします。ESP スイッチオーバー中は、すべての IPsec セッションがアップ状態のままになるので、IPsec セッションを維持するためにユーザーの操作は必要ありません。
- ESP をリロードした場合（スタンバイ ESP なし）、SA シーケンス番号は 0 から再開されます。ピア ルータは、予期されたシーケンス番号を持たないパケットをドロップします。単一の ESP を使用するシステムで ESP のリロード後にこの問題を回避するには、IPSec セッションを明示的に再確立することが必要になる場合があります。このような場合、リロード中に IPSec セッションでトラフィックの中断が発生することがあります。
- Cisco ASR 1000 シリーズ ルータは、現在、ルートプロセッサ（RP）でのステートフル スイッチオーバー（SSO）の IPsec セッションをサポートしていません。IPsec セッションはスイッチオーバーの開始時にダウンしますが、新しい RP がアクティブになるとアップ状態に戻ります。ユーザーの操作は必要ありません。セッションがアップ状態に戻るまでの間、スイッチオーバー中に IPSec セッションでトラフィックの中断が発生することがあります。
- Cisco ASR 1000 シリーズ ルータは、IPsec セッションのステートフル ISSU をサポートしていません。ISSU を実行する前に、既存のすべての IPSec セッションまたはトンネルを明示的に終了し、ISSU の実行後に再確立する必要があります。具体的には、ISSU を実行する前に、ハーフオープンまたは確立途中の IPsec トンネルが存在しないことを確認します。これを行うには、トンネルセットアップを開始する可能性のあるインターフェイス（トンネルセットアップを開始するルーティングプロトコルなど）、キープアライブが有効になっているインターフェイス、または IPsec セッションの自動トリガーが存在するインターフェイスの場合は、インターフェイスをシャットダウンすることをお勧めします。この場合、ISSU の実行中に IPsec セッションでトラフィックの中断が発生します。

Cisco Group Encrypted Transport VPN に関する情報

Cisco Group Encrypted Transport VPN の概要

音声やビデオなどのネットワークを利用するアプリケーションによって、即時に通信可能で各ブランチが相互接続された、QoS 対応 WAN の必要性が増しています。これらのアプリケーションは分散して配置されるため、スケーラビリティに対する要求も高まります。同時に、企業の WAN テクノロジーにおいては、QoS 対応ブランチ間相互接続と転送のセキュリティとの

間でトレードオフが発生します。ネットワーク セキュリティのリスクが増大し、適合認定が重要になりつつある中、次世代のWAN暗号化テクノロジーであるGET VPNを利用すれば、ネットワークのインテリジェント化とデータ プライバシとの間で折り合いをつける必要性を低下させることができます。

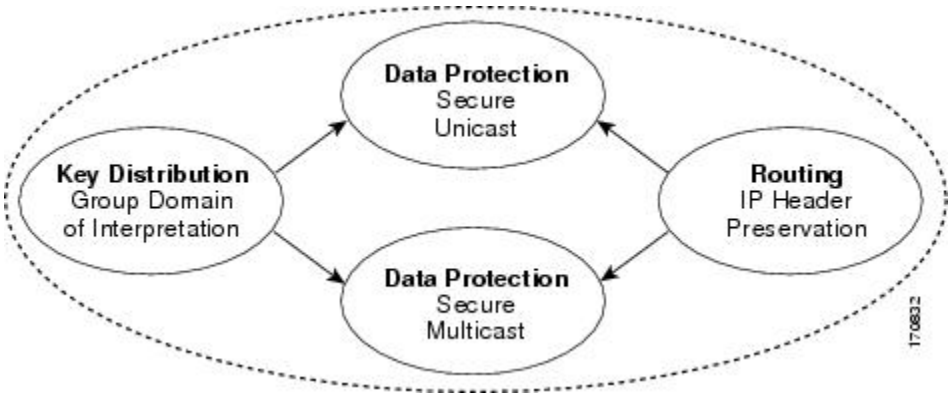
シスコでは、GET の導入に伴い、トンネルレス VPN を提供しており、これによりトンネルが不要になります。ポイントツーポイント トンネルの必要性をなくすことで、メッシュ ネットワークを大規模化すると同時に、音声やビデオの品質にとって重要なネットワークインテリジェンス機能を維持することが可能となっています。GET では、「信頼できる」グループ メンバーというコンセプトを基にした、各種の標準規格に準拠準拠したセキュリティ モデルが用意されています。信頼できるメンバーのルータでは、ポイントツーポイント IPsec トンネル関係とは独立した共通のセキュリティ方式が使用されます。ポイントツーポイント トンネルではなく信頼できるグループを使用することによって、「any-any」ネットワークを大規模化すると同時に、音声やビデオの品質にとって重要なネットワークインテリジェンス機能（QoS、ルーティング、マルチキャストなど）を維持することが可能となっています。

GET ベースのネットワークは、IP や MPLS などを含む、さまざまな WAN 環境で使用できます。この暗号化テクノロジーを使用する MPLS VPN はスケーラビリティ、管理性、コストに優れており、政府によって義務付けられている暗号化要件が満たされます。GETは柔軟であるため、セキュリティを必要とする企業では、サービス プロバイダー WAN サービスにおいて独自のネットワーク セキュリティを管理することも、暗号化サービスをプロバイダーに委託することもできます。GETによって、部分メッシュ接続または完全メッシュ接続を必要とする大規模なレイヤ 2 または MPLS ネットワークの保護が簡易化されます。

Cisco Group Encrypted Transport VPN のアーキテクチャ

GET VPN は、マルチキャスト キー再生、「ネイティブの」マルチキャスト パケットの暗号化を可能にする手段、およびプライベート WAN を介したユニキャスト キー再生成を網羅するソリューションです。マルチキャスト キー再生と GET VPN は、インターネット技術特別調査委員会（IETF）の RFC 3547 で定義されている GDOI を基盤としています。また、ヘッダー保存および SA 検索の領域においては、IPsec と各種の共通点が存在します。IPsec SA の動的配信が追加され、IPsec のトンネルが重複する特性が削除されています。次の図に、GET VPN の各概念と、概念間の関係を示します。

図 *113 : GET VPN* の概念と関係



キー配布グループ ドメイン オブ インタープリテーション（GDOI）

GDOI

GDOI は、グループ キー管理のための、Internet Security Association Key Management Protocol（ISAKMP）ドメイン オブ インタープリテーション（DOI）として定義されています。グループ管理モデルでは、GDOI プロトコルが、グループ メンバーと、グループ コントローラまたはキー サーバ（GCKS）との間で動作し、その結果、認証されているグループ メンバー間での SA が確立されます。ISAKMP では、ネゴシエーションの 2 つのフェーズが定義されています。GDOI は、フェーズ 1 の ISAKMP セキュリティ アソシエーションによって保護されます。フェーズ 2 の交換は、RFC 6407 によって定義されています。次の図に示したトポロジとそれに続く説明は、このプロトコルのしくみを説明したものです。

グループ メンバー

グループ メンバーは、グループと通信するために必要な IPsec SA または SA を取得するためのキー サーバに登録します。グループ メンバーによって、そのグループの個別のポリシーおよびキーを取得するためのキー サーバにグループ ID が提供されます。これらのキーは、現在の IPsec SA が期限切れになる前に、定期的に更新されます。その結果、トラフィックのロスがなくなります。

show crypto isakmp sa detail コマンドの出力では、GET VPN のキー暗号化キー（KEK）キー再生成認証に RSA 署名が使用されるため、セキュリティ アソシエーション（SA）認証を「rsig」として表示します。

キー サーバ

キー サーバの役割には、ポリシーの維持や、グループのキーの作成および維持などがあります。グループ メンバーが登録されると、キー サーバによってこのポリシーおよびキーが、グループ メンバーに対してダウンロードされます。また、キー サーバは、既存のキーの期限が切れる前にグループに対してキーの再生成を実行します。

（注） Cisco IOS XE リリース 3.5S 以前のリリースでは、キー サーバは Cisco ASR 1000 シリーズ ルータではサポートされていません。これらは Cisco IOS T ベースまたはメインラインベース イメージを使用して設定する必要があります。これは、Cisco IOS XE リリース 3.6S 以降のリリースの制限ではありません。

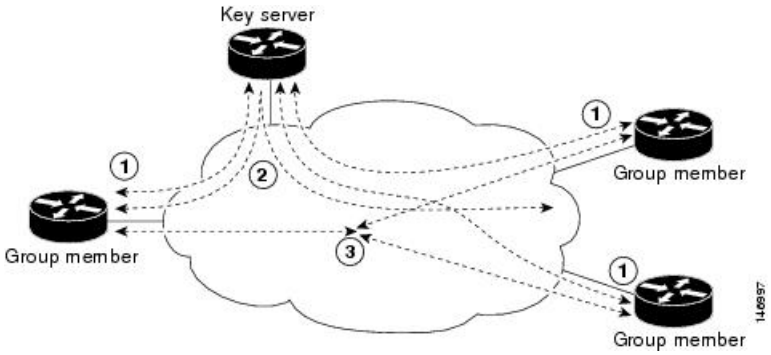
キー サーバには、登録要求の処理およびキーの再生成の送信という 2 つの機能があります。グループ メンバーはいつでも登録可能で、最新のポリシーおよびキーを受信できます。グループ メンバーがキー サーバに登録する場合、キー サーバによって、グループ メンバーが参加を試みているグループ ID が確認されます。この ID が有効なグループ ID だった場合、キー サーバによって、SA ポリシーがグループ メンバーに対して送信されます。ダウンロードされたポリシーを処理できることがグループ メンバーによって確認されると、キー サーバから各キーがダウンロードされます。

キーサーバからダウンロードされるキーには、キー暗号キー（KEK）とトラフィック暗号キー（TEK）の 2 種類があります。TEK は、同じグループ内のグループ メンバーどうしの通信で使用される IPsec SA になります。KEK は、キー再生成メッセージを暗号化します。

IPsec SA の期限切れが近づいた場合、またはキーサーバ上のポリシーが変更（コマンドライン インターフェイス [CLI] を使用）された場合、GDOI サーバによってキー再生成メッセージが送信されます。CSCti89255 では、KEK タイマーが期限切れになる前に KEK のキー再生成が行われます。グループ メンバーもタイマーを開始し、タイマーの期限が切れる前に更新されたキーを受け取ることを期待します。これらを受け取らない場合、グループ メンバーは KEK の期限切れの前にジッタが生じた再登録を開始します。KEK ライフタイムが期限切れになると、KEK は削除されます。

パケット損失に備えて、キー再生成メッセージが定期的に送信される場合もあります。パケット損失が発生する原因としては、信頼できる転送を使用することなくキー再生成メッセージが送信されることなどが考えられます。キーの再生成メカニズムがマルチキャストである場合は、受信者がキーの再生成メッセージを受信できなかったことを示す有効なフィードバック メカニズムがないため、定期的に再送信することによってすべての受信者が最新の情報を受信できるようにします。キー再生成メカニズムがユニキャストである場合、受信元によって確認応答メッセージが送信されます。

図 *114*：グループ メンバーがグループに参加するうえで必要なプロトコル フロー



上記のトポロジは、次のようにグループ メンバーがグループに参加するうえで必要なプロトコル フローを示しています。

1. グループ メンバーがキー サーバに登録されます。キー サーバによってグループ メンバーが認証および許可され、グループ メンバーが IP マルチキャスト パケットを暗号化および復号化するうえで必要な IPsec ポリシーおよびキーがダウンロードされます。
2. 必要に応じて、キー サーバからグループ メンバーに対してキーの再生成メッセージが「プッシュ」されます。キー再生成メッセージには、古い IPsec SA の期限が切れた際に使用される新しい IPsec ポリシーおよびキーが格納されています。常に有効なグループ キーが使用できるように、キーの再生成メッセージは SA の期限が切れる前に送信されます。
3. 各グループ メンバーは、キー サーバによって認証を受けてから、キー サーバから受信した IPsec SA を使用して、同じグループ内の他の認証済みグループ メンバーと通信します。

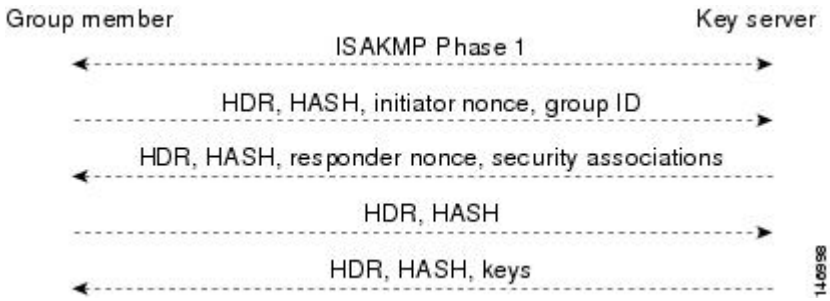
Cisco ソフトウェアでのプロトコル メッセージの動作

マルチキャスト キー再生では、グループのポリシーおよびキーを配信するためにGDOIプロトコル（RFC 6407）が使用されます。GDOI プロトコルは、キー サーバとグループ メンバーの間で使用されます。キー サーバによってポリシーとキーが作成および維持され、さらに、認証された各グループ メンバーにダウンロードされます。

GDOI プロトコルは、ISAKMP フェーズ 1 交換によって保護されます。GDOI キー サーバと GDOI グループ メンバーの ISAKMP ポリシーは同じである必要があります。このフェーズ 1 ISAKMP ポリシーは、そのポリシーに従うGDOIプロトコルを保護できる程度に強力なものである必要があります。GDOI プロトコルは、フェーズ 1 ISAKMP ポリシーに従う 4 メッセージ交換です。フェーズ 1 ISAKMP 交換は、メイン モードまたはアグレッシブ モードで発生する可能性があります。

次の図は、ISAKMP フェーズ 1 交換を示しています。

図 *115 : ISAKMP* フェーズ *1* 交換と *GDOI* 登録



上記メッセージ（ISAKMP フェーズ 1 メッセージと 4 つの GDOI プロトコル メッセージ）をGDOI登録と呼びます。上に示した交換全体は、グループ メンバーとキー サーバ間のユニキャスト交換です。

キー再生成メカニズムがマルチキャストである場合、登録中、グループ メンバーによってマルチキャスト グループのアドレスが受信され、そのグループ メンバーが、マルチキャスト キー再生成を受信するうえで必要なマルチキャスト グループに登録されます。

GDOI プロトコルでは、ユーザ データグラム プロトコル（UDP）ポート 848 が使用されます（Network Address Translation-Traversal（NAT-T）が使用されている場合、ポートは 4500 まで変化します）。

IPsec

IPsec は、IP レイヤのトラフィックのための各種セキュリティ サービスを提供するためのアーキテクチャが定義された、よく知られた RFC です。IETF RFC 2401 には、各種コンポーネントおよびそれらがどのように互いに組み合されてIP環境を形成しているかが記述されています。

IPsec SA を更新するためのキー サーバとグループ メンバー間の通信フロー

キー サーバとグループ メンバーは、GET VPN アーキテクチャを構成する 2 つのコンポーネントです。キー サーバには、グループ認証キーと IPsec SA が保存され、グループ メンバーに対して提供されます。

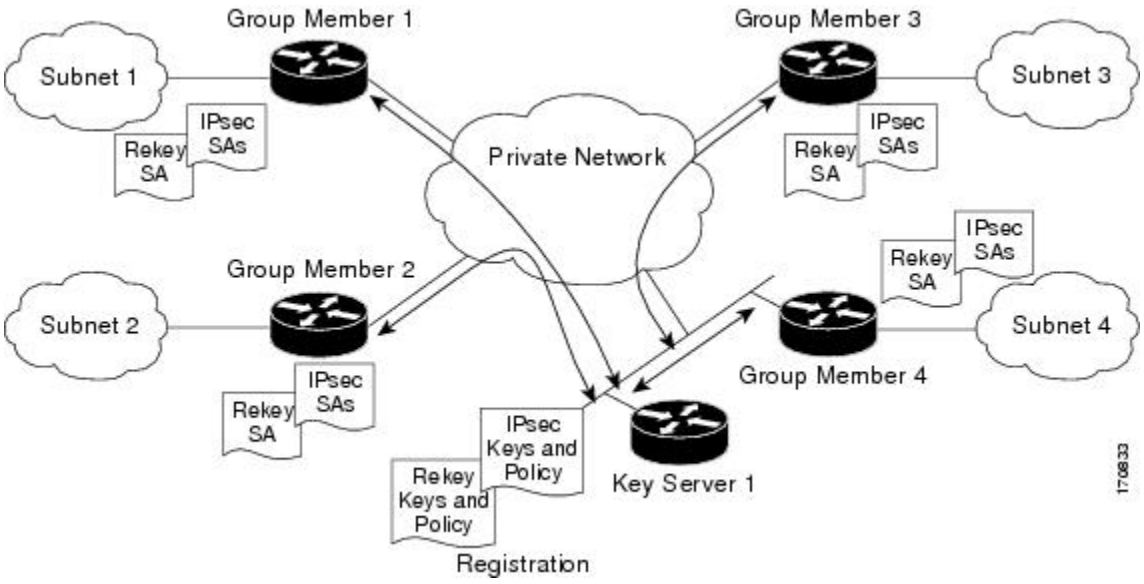
グループ メンバーでは、対象となるトラフィック（暗号化するに値し、IPsec によってセキュリティ保護されるトラフィック）に対して暗号化サービスが提供されます。

キー サーバとグループ メンバー間における通信は暗号化およびセキュリティ保護されます。GDOI には、TEK と KEK という 2 つのキーがサポートされています。TEK は、キー サーバからすべてのグループ メンバーにダウンロードされます。ダウンロードされた TEK は、グループ メンバー間で安全に通信するためにすべてのグループ メンバーで使用されます。このキーは、実質的には、すべてのグループ メンバーによって共有されるグループ キーとなります。グループ ポリシーおよび IPsec SA は、グループ メンバーへの定期的なキーの再生成メッセージを使用して、キー サーバによってリフレッシュされます。KEK もキー サーバによってダウンロードされ、グループ メンバーによって、キー サーバから受信するキーの再生成メッセージの復号化に使用されます。

キー サーバによって、GDOI グループのグループ ポリシーと IPsec SA が生成されます。キー サーバによって生成される情報には、複数の TEK 属性、トラフィック暗号化ポリシー、ライフタイム、送信元と宛先、各 TEK に関連付けられるセキュリティ パラメータ インデックス（SPI）ID、キーの再生成ポリシー（1 つの KEK）などがあります。

次の図に、グループ メンバーおよびキー サーバ間の通信フローを示します。キー サーバは、グループ メンバーからの登録メッセージを受信したあと、グループ ポリシーと新しい IPsec SA を含む情報を生成します。次に、新しい IPsec SA がグループ メンバーにダウンロードされます。キー サーバでは、グループごとに、各グループ メンバーの IP アドレスを含むテーブルが保持されます。グループ メンバーが登録されると、キー サーバはメンバーの IP アドレスを関連するグループのテーブルに追加します。これにより、キー サーバは、アクティブなグループ メンバーをモニタできるようになります。1 つのキー サーバで複数のグループをサポートできます。また、1 つのグループ メンバーは、複数のグループに属することができます。

図 *116*：グループ メンバーおよびキー サーバ間の通信フロー



IPsec と ISAKMP タイマー

IPsec と ISAKMP SA は、次のタイマーによって維持されます。

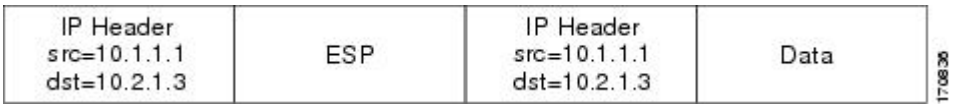
- TEK ライフタイム：IPsec SA のライフタイムを決定します。TEK ライフタイムが終了する前に、キー サーバによってキー再生成メッセージが送信されます。このメッセージには、新しい TEK 暗号キーと変換、および既存の KEK 暗号キーと変換が格納されています。TEK ライフタイムはキーサーバ上でだけ設定します。ライフタイムは、GDOI プロトコルによって各グループ メンバーに対して「プッシュ ダウン」されます。TEK ライフタイムの値はネットワークのセキュリティ ポリシーによって異なります。**set security-association lifetime** コマンドが設定されていない場合、デフォルト値である 86,400 秒が有効になります。TEK ライフタイムを設定するには、「IPsec ライフタイム タイマーの設定」セクションを参照してください。
- KEK ライフタイム：GET VPN キー再生成 SA のライフタイムを決定します。ライフタイムが終了する前に、キーサーバによってキー再生成メッセージが送信されます。このメッセージには、新しい KEK 暗号キーと変換、および新しい TEK 暗号キーと変換が格納されています。TEK ライフタイムはキー サーバ上でだけ設定します。ライフタイムは、GDOI プロトコルによって各グループ メンバーに対して動的にプッシュ ダウンされます。KEK ライフタイム値は、TEK ライフタイム値よりも大きい必要があります（KEK ライフタイム値は、TEK ライフタイム値の少なくとも 3 倍以上にすることが推奨されます）。 **rekey lifetime** コマンドが設定されていない場合、デフォルト値である 86,400 秒が有効になります。KEK ライフタイムを設定するには、「マルチキャスト キー再生成の設定」セクションを参照してください。
- ISAKMP SA ライフタイム：ISAKMP SA が期限切れになる前にどれだけの期間存在するべきかを定義します。ISAKMP SA ライフタイムは、グループ メンバーおよびキー サーバ上で設定します。グループ メンバーとキー サーバに連携可能なキー サーバがない場合、グループ メンバーの登録が終了しても ISAKMP SA は使用されません。このような（連携可能なキー サーバがない）場合、ISAKMP SA のライフタイムを短く設定できます（最小 60 秒）。連携可能なキーサーバが存在する場合は、連携可能なキーサーバの通信中に ISAKMP SA を「アップ」の状態に保つため、すべてのキー サーバのライフタイムを長く設定する必要があります。 **lifetime** コマンドが設定されていない場合、デフォルト値である 86,400 秒が有効になります。ISAKMP SA ライフタイムを設定するには、「ISAKMP ライフタイム タイマーの設定」セクションを参照してください。

アドレス保存

ここでは、GET VPN でのアドレス保存について説明します。

以下の図に示すように、IPsec で保護されたデータ パケットでは、外側の IP ヘッダーで元の送信元と宛先が伝送されます。トンネルエンドポイントのアドレスには置換されません。この技術は、IPsec Tunnel Mode with Address Preservation と呼ばれています。

図 *117*：ヘッダー保存



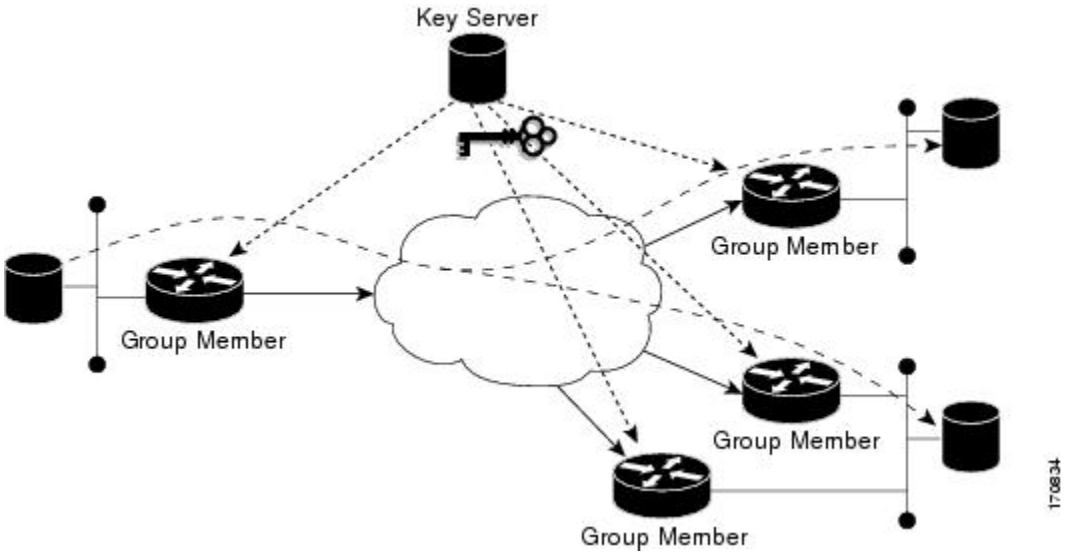
GET VPN では、アドレスが維持されるため、コア ネットワーク内のルーティング機能を使用できます。アドレスの維持によって、ネットワーク内の、宛先アドレスへのルートをアドバタイズする任意のカスタマー エッジ（CE）デバイスにパケットを配送するルーティングが可能となります。グループのポリシーに一致するすべての送信元および宛先は、同様に処理されます。アドレスの維持は、IPsec ピア間のリンクが利用できない状況では、トラフィックの「ルート不在」状況に対処するのに役立ちます。

また、ヘッダーが維持されることによって、企業のアドレス空間全体および WAN においてルーティングの継続性が維持されます。その結果、キャンパスのエンド ホスト アドレスは WAN に公開されます（MPLS では、これは WAN のエッジに適用されます）。このため、GET VPN は、WAN ネットワークが「プライベート」ネットワークとして動作する場合にだけ適用できます（MPLS ネットワークなど）。

セキュア データ プレーン マルチキャスト

マルチキャストの送信元では、キー サーバから取得される TEK が使用され、ヘッダーが保存されたマルチキャスト データ パケットが、スイッチングされる前に暗号化されます。マルチキャストパケットのレプリケーションが、マルチキャストパケット内に保持されている（S,G）ステートに基づいてコア内で実行されます。次の図に、このプロセスを示します。

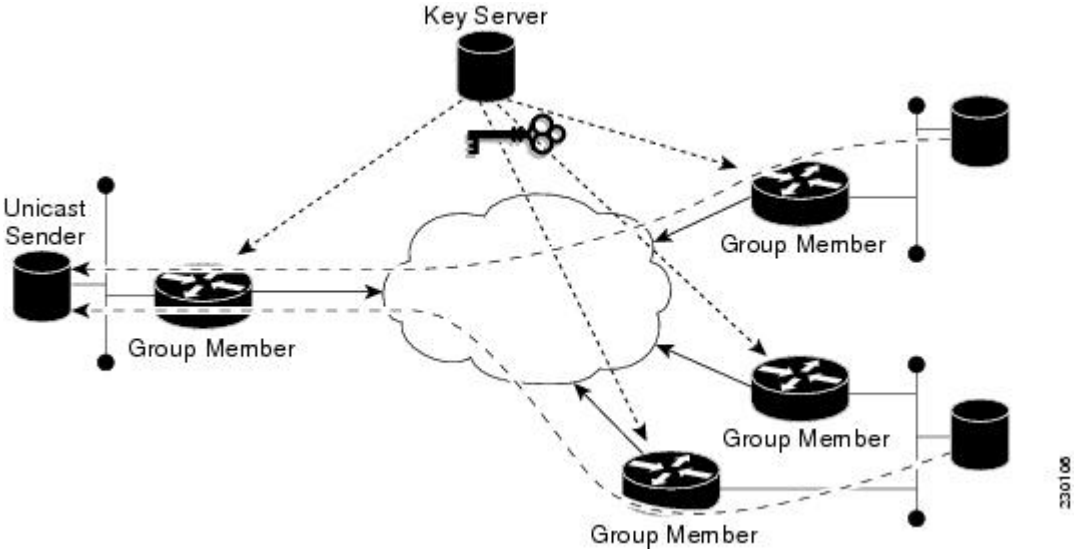
図 *118 :* セキュア データ プレーン マルチキャスト プロセス



セキュア データ プレーン ユニキャスト

ユニキャストの送信元では、キー サーバから取得される TEK が使用され、ヘッダーが保存されたユニキャスト データ パケットが、宛先にスイッチングされる前に暗号化されます。次の図に、このプロセスを示します。

図 *119* : セキュア データ プレーン ユニキャスト プロセス



Cisco Group Encrypted Transport VPN の機能

キー再生成

キー再生成は IPsec SA を更新するために使用されます。IPsec SA またはキー再生成 SA の期限切れが近づくと、特定のグループの単一のキー再生成メッセージがキー サーバ上で生成されます。キー再生成の配信のために新しいIKEセッションが生成されることはありません。キー再生成メッセージは、キー サーバによって、既存の IKE SA を介して配信されます。

キー再生成では、マルチキャスト メッセージまたはユニキャスト メッセージを使用できます。GET VPN では、ユニキャスト キー再生成とマルチキャスト キー再生成の両方がサポートされています。

CSCti89255 では、KEK タイマーが期限切れになる前に KEK のキー再生成が行われます。グループ メンバーもタイマーを開始し、タイマーの期限が切れる前に更新されたキーを受け取ることを期待します。これらを受け取らない場合、グループ メンバーは KEK の期限切れの前にジッタが生じた再登録を開始します。KEK ライフタイムが期限切れになると、KEK は削除されます。これにより以下が確保されます。

- より安全な KEK の有効期限確認メカニズム
- より安全な KEK の再登録メカニズム
- 設定されたライフタイムを超える KEK の使用の回避

次のサブセクションではキー再生成の詳細情報を提供します。

キー再生成のシーケンス番号

TEK/KEK ライフタイムが終了する前に、KS は、シーケンス番号を 1 つ増やしたキー再生成メッセージを送信します。ただし、最後のキー再生成メッセージの送信以降にセカンダリ KS がプライマリ KS になった場合、新しいプライマリ KS は、キー再生成メッセージのシーケンス番号を 10 ずつ増やします。

プライマリ KS とセカンダリ KS は、20 秒ごとにシーケンス番号を同期します。

次の例は、プライマリ KS（KS1）とセカンダリ KS（KS2）で構成される展開においてキー再生成メッセージのシーケンス番号がどのように変化するのかを示しています。この例では、シーケンス番号の初期値が 1 であると想定されています。

また、展開に多数の GM があることと、KS がキー再生成メッセージの配信を再試行する必要がある場合があることも想定されています。シーケンス番号は、再試行ごとに 1 ずつ増加します。

1. キー再生成メッセージを送信する時間になると、KS1 はシーケンス番号を 2 に増やします。
2. すべての GM がメッセージを受信するように、KS1 がキー再生成メッセージを 3 回再送信するとします。再試行ごとに、シーケンス番号が 1 ずつ増加します。そのため、このキー再生成が終わったときのシーケンス番号の値は 5 です。
3. 次のキー再生成メッセージを送信する時間になると、KS1 がキー再生成メッセージを 1 回だけ送信するとします。そのため、この 2 回目のキー再生成が終わったときのシーケンス番号は 6 です。
4. 次のキー再生成メッセージが送信される前に、KS2 がプライマリ KS になるとします。
5. キー再生成メッセージを送信する時間になると、KS2 はシーケンス番号を 10 ずつ増やします。そのため、キー再生成メッセージはシーケンス番号 16 で送信されます。
6. すべての GM がメッセージを受信するように、KS2 がキー再生成メッセージを 2 回再送信するとします。再試行ごとに、シーケンス番号が 1 ずつ増加します。そのため、このキー再生成が終わったときのシーケンス番号の値は 18 です。
7. 次のキー再生成メッセージが送信される前に、KS1 がプライマリ KS になるとします。
8. キー再生成メッセージを送信する時間になると、KS1 はシーケンス番号を 10 ずつ増やします。そのため、キー再生成メッセージはシーケンス番号 28 で送信されます。KS1 がキー再生成メッセージを 1 回だけ送信するとします。キー再生成が終わったときのシーケンス番号は 28 です。
9. 次のキー再生成メッセージを送信する時間になると、KS1 はシーケンス番号を 1 ずつ増やします。KS1 がキー再生成メッセージを 1 回だけ送信するとします。キー再生成が終わったときのシーケンス番号は 29 です。

次の表に、各キー再生成動作でのシーケンス番号の変化の概要を示します。

キー再生成番号	1（3 回の再試行）	2（0 回の再試行）	3（2 回の再試行）	4（0 回の再試行）	5（0 回の再試行）

シーケンス番号	2、3、4、5	6	16、17、18	28	29

キー再生成シーケンス番号のチェック

キー サーバとグループ メンバー間のキー再生成シーケンス番号のチェックは次のように行われます。

1. GROUPKEY-PUSH メッセージのアンチリプレーは RFC 6407 で規定されているように復元されます。
   - グループ メンバーは、最後に受信したキー再生成メッセージのシーケンス番号以下の番号のキー再生成メッセージをすべてドロップします。
   - グループ メンバーは、最後に受信したキー再生成メッセージのシーケンス番号より大きい番号のキー再生成メッセージをすべて（差がどれだけ大きくても）承認します。
2. シーケンス番号は、KEK 再生成メッセージ時ではなく、KEK 再生成キーの後の最初のキー再生成メッセージ時に 1 にリセットされます。

マルチキャスト キー再生成

マルチキャスト キー再生成は、有効なマルチキャスト キー再生成が使用されて送信されます。登録が成功すると、グループ メンバーが特定のマルチキャスト グループに登録されます。グループに登録されているすべてのグループ メンバーによって、このマルチキャスト キー再生成が受信されます。マルチキャスト キー再生成は、キー サーバに設定されているライフタイムに基づいて定期的に送信されます。IPsec またはキー再生成ポリシーがキー サーバ上で変更された場合もマルチキャスト キー再生成が送信されます。設定の変更によってトリガーされると、キー再生成によって、新しく更新されたポリシーが有効なマルチキャスト キー再生成を持つすべてのグループ メンバーに送信されます。

キー サーバによって、キー再生成の時間が次のようにプッシュ バックされます。

1. TEK のタイムアウトが 300 秒の場合：

tek_rekey_offset = 90（300 < 900 のため）

再送信が設定されている場合、キー再生成タイマーがさらに戻されます。

3 つの再送信がすべて 10 秒の場合：3 * 10

その結果、キー再生成が実際に発生するのは (300 - 90 - 30) = 180 秒

2. TEK のタイムアウトが 3600 秒の場合：

tek_rekey_offset = 3600 * 10% = 360 秒

再送信が設定されている場合、キー再生成タイマーがさらに戻されます。

3 つの再送信がすべて 10 秒の場合：3 * 10

その結果、キー再生成が実際に発生するのは (3600 - 360 - 30) = 3210 秒

KEK の期限が切れ、転送モードがマルチキャストである場合、マルチキャスト KEK キー再生成が送信されます。マルチキャスト KEK が送信されると、グループ メンバーによって古い

KEK が新しい KEK に置き換えられます。これはマルチキャスト キー再生成であり、再送信が送信されるので、古い KEK は引き続き暗号化に使用されます。このような状況が発生するのは、グループ メンバーによって新しい KEK キー再生成が受信されていないためです。そのため、マルチキャスト キー再生成を受信したグループ メンバーには古い KEK は存在せず、それらの再送信は廃棄されます。

最初に KEK キーを受信せず、現在は KEK 再送信を受信して古い KEK を新しい KEK に置き換えているグループ メンバーの場合、後の再送信は廃棄されます。たとえば、5 つの再送信が設定されており、シーケンス番号が 1 のマルチキャスト KEK キー再生成がグループ メンバー 1 で受信される場合、グループ メンバーに古い KEK がないため、シーケンス番号が 2、3、4、5、6 である他のすべての再送信は廃棄されます。

グループ メンバー 2 によってシーケンス番号が 1 の KEK キー再生成が取得されず、シーケンス番号が 2 である再送信が受信された場合、他の再送信 3、4、5、6 は廃棄されます。

マルチキャスト キー再生成の設定要件

グループ メンバーがキー サーバに登録するときは、データベースに KEK SA をインストールします。キー再生成の転送がマルチキャストのとき、グループ メンバーは IGMP を使用して、キー サーバによって定義されたマルチキャスト ストリームに参加します。IGMP 参加は、暗号マップを含むインターフェイスから送信されます。

（注） IGMP トラフィックは、キー サーバで定義された ACL またはグループ メンバーのローカル拒否 ACL による暗号化から除外する必要があります。

暗号マップを使用して設定されたものと同じインターフェイス経由でキー サーバに到達できないときは、ストリームに手動で参加する必要があります。

ユニキャスト キー再生成と SA

大型のユニキャスト グループでは、遅延問題を軽減するため、キー サーバによって一度にごく少数のグループ メンバーのキー再生成メッセージだけが生成されます。すべてのグループ メンバーによって、古い SA の期限が切れる前に新しい SA の同じキー再生成メッセージが受信されることが、キー サーバには保証されています。さらに、ユニキャスト グループでは、キー サーバからのキー再生成メッセージが受信された後、グループ メンバーによって、暗号化された確認応答（ACK）メッセージが、キー再生成メッセージの一部として受信されたキーが使用されて、キー サーバに送信されます。キー サーバによって ACK メッセージが受信されると、その受信が関連するグループのテーブルに書き込まれ、次のことが実行されます。

- キー サーバにアクティブなグループ メンバーの最新リストが保管されます。
- キー サーバによって、アクティブなメンバーにだけキー再生成メッセージが送信されます。

さらに、ユニキャストグループでは、3 回連続したキー再生成が行われて ACK メッセージが 1 つもキー サーバによって受信されなかった場合、キー サーバによってアクティブ リストからグループ メンバーが削除され、その特定のグループ メンバーに対するキー再生成メッセー

ジの送信が停止されます。3 回連続したキー再生成が行われて ACK メッセージが 1 つも受信されなくても、グループ メンバーがキー再生成メッセージを受信する必要がある場合には、現在の SA が期限切れになった後には、グループ メンバーはキー サーバに完全に再登録される必要があります。非応答グループ メンバーのイジェクトは、キー サーバがユニキャスト キー再生成モードで動作している場合にだけ行われます。マルチキャスト キー再生成モードでは、キー サーバによるグループ メンバーの排出は行われません。そのモードでは、グループ メンバーが ACK メッセージを送信できないからです。

マルチキャスト キー再生成におけるのと同様、再送信が設定されている場合、各キー再生成は、設定された回数再送信されます。

キー再生成転送モードおよび認証は、GDOI グループ下で設定できます。

ユニキャスト キー再生成転送モードが定義されていない場合、デフォルトでマルチキャストが適用されます。

TEK キー再生成が受信されなかった場合、現在の IPsec SA が期限切れになる 60 秒前にグループ メンバーがキー サーバに再登録されます。グループ メンバーの再登録が発生する前に、キー サーバによってキー再生成が送信される必要があります。再送信が設定されていない場合、SA が期限切れになる前に、キー サーバによってキー再生成 tek_rekey_offse が送信されます。tek_rekey_offset は、設定されているキー再生成ライフタイムに基づいて算出されます。TEK キー再生成のライフタイムが 900 秒より短い場合、tek_rekey_offset は 90 秒に設定されます。TEK キー再生成のライフタイムが 900 秒を超えるように設定されている場合、rekey_offset = (設定されている TEK キー再生成のライフタイム)/10 となります。再送信が設定されている場合、SA が期限切れになる 90 秒前に最新の再送信が送信されるように、tek_rekey_offset よりも前にキー再生成が発生します。

キー サーバでは、すべてのユニキャスト グループ メンバーに対するキー再生成の送信をいつ開始するか計算するために、次の例に示す数式が使用されます。キー サーバにおけるユニキャスト キー再生成処理によって、1 回のループで 50 のグループにおけるユニキャスト グループ メンバーに対してキー再生成が送信されます。このループ内でかかる時間は推定 5 秒です。

キー サーバによって、50 のグループのグループ メンバーのキー再生成が行われます。これは 2 回のループに相当します。たとえば、グループ メンバーの数が 100 の場合：

キー再生成ループの数 = (100 グループ メンバー)/50 = 2 ループ：

- 1 回のループでのキー再生成にかかる時間（推定）= 5 秒
- 50 の 2 回ループにおける 100 グループ メンバーに対するキー再生成にかかる時間：2 * 5 秒 = 10 秒

そのため、キー サーバによって、キー再生成の時間が次のようにプッシュ バックされます。

- TEK のタイムアウトが 300 の場合：300 - 10 = 290

ただし、開始は TEK が期限切れになるよりも前である必要があります（マルチキャストの場合と同じです）。

- 300 < 900 であるため、tek_rekey_offset = 90
- そのため、実際の TEK 時間から 90 秒を引いて、290 - tek_rekey_offset = 200 秒

再送信が設定されている場合、キー再生成タイマーがさらに戻されます。

- 3 つの再送信がすべて 10 秒の場合：200 - (3 * 10) = 170
- TEK のタイムアウトが 3600 秒である場合：3600 - 10 = 3590

ただし、開始は TEK が期限切れになるよりも前である必要があります（マルチキャストの場合と同じです）。

- 3600 > 900 であるため、tek_rekey_offset = 3600 * 10% = 360
- そのため、実際の TEK 時間から 360 秒を引いて、3590 - tek_rekey_offset = 3230 秒

再送信が設定されている場合、キー再生成タイマーがさらに戻されます。

- 3 つの再送信がすべて 10 秒の場合：3230 - (3 * 10) = 3200 秒

数式 tek_rekey_offset は、ユニキャストおよびマルチキャスト キー再生成に適用されます。

ポリシー変更後のキー再生成の動作

次の表に、セキュリティ ポリシーの変更に対応したキー再生成の動作の一覧を示します。

表 *286 :* セキュリティ ポリシー変更後のキー再生成の動作

ポリシーの変更	キー再生成を送信するか	ポリシー変更後のキー再生成の動作
TEK：SA ライフタイム	No	古い SA は、そのライフタイムが期限切れになるまでアクティブのままになります。新しいライフタイムは、次にスケジュールされたキー再生成の後に有効になります。
TEK：IPSEC トランスフォーム セット	Yes	古いトランスフォーム セットの SA は、そのライフタイムが期限切れになるまでアクティブのままになります。
TEK：IPSEC プロファイル	Yes	古いプロファイルの SA は、そのライフタイムが期限切れになるまでアクティブのままになります。
TEK：一致する ACL	Yes	発信パケット分類では、即座に新しいアクセス コントロール リスト（ACL）が使用されます。古い SA は SA データベース内に保存されたままになります。
TEK：リプレイ カウンタのイネーブル化	Yes	カウンタ リプレイがない古い SA は、そのライフタイムが期限切れになるまでアクティブのままになります。

ポリシーの変更	キー再生成を送信するか	ポリシー変更後のキー再生成の動作
TEK：リプレイ カウンタの変更	No	新しいリプレイ カウンタがある SA は、次にスケジュールされたキー再生成時に送信されます。
TEK：リプレイ カウンタのディセーブル化	Yes	カウンタ リプレイがイネーブルになっている古い SA は、そのライフタイムが期限切れになるまでアクティブのままになります。
TEK：受信専用のイネーブル	Yes	受信専用モードは、キー再生成後ただちにアクティブになります。
TEK：受信専用のディセーブル	Yes	受信専用モードは、キー再生成後ただちに非アクティブになります。
KEK：SA ライフタイムの動作	No	変更は次のキー再生成時に適用されます。
KEK：認証キーの変更	Yes	変更は次のキー再生成時に適用されます。
KEK：暗号アルゴリズムの変更	Yes	変更は即時に適用されます。

ポリシーの変更を即時に有効にするには、次の手順に従います。

- キーサーバーで **clear crypto gdoi** [**group**] コマンドを使用します。
- すべてのグループメンバーで **clear crypto gdoi** [**group**] コマンドを使用します。

（注） キー サーバは管理者がコンフィギュレーション モードを終了するとポリシーの更新のためのキー再生成を送信し、適切な場合にキー再生成が送信されるようにします。

（注） グループ メンバーで双方向モードに変更する前のパッシブ モードの動作は次のとおりです。

キー サーバの SA モードを「no sa receive-only」に変更し、コンフィギュレーション モードを終了する場合、キー再生成はグループ メンバーに送信され、「受信専用」から「発信オプション」にグループ メンバーの状態が変化するのを確認できます。組み込みタイマーによって設定されたインターバル（約 5 分）の後は「両方」に状態が変化します。

キー サーバはこの状態をすぐに「両方」として示します。すべてのグループ メンバーが更新される過程である可能性があるため、これは意図的に行われます。

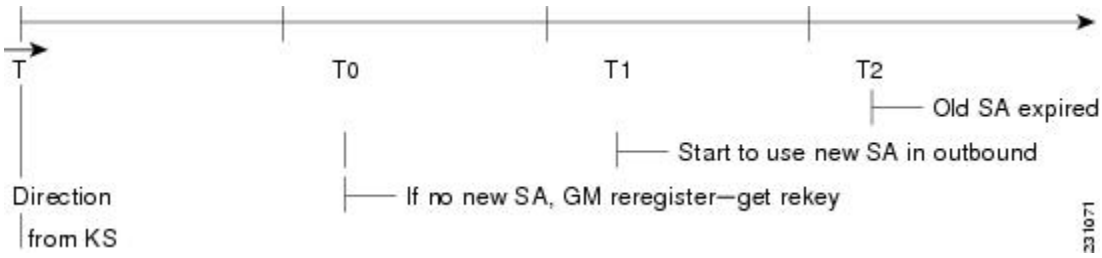
グループ メンバーにおけるIPsec SA の使用

グループ メンバー上でキー再生成が受信され、処理されると、新しい IPsec SA（SPI）がインストールされます。古い IPsec SA と新しい IPsec SA が共に使用される期間が存在します。指定された一定期間の経過後に、古い IPsec SA は削除されます。この重複によって、すべてのグループ メンバーが現在のキー再生成を受信し、新しい IPsec SA を追加できます。この動作は、キー サーバからのキー再生成のための転送モード（マルチキャストまたはユニキャスト キー再生成転送）とは無関係です。

グループ メンバー上では、古い SA が期限切れになる約 30 秒前に、グループ メンバーによって、パケットを暗号化するために発信方向で新しい SA が使用されます。古い SA が期限切れになる約 60 秒前にキー サーバからのキー再生成を介して新しい SA がグループ メンバー側で受信されていない場合、グループ メンバーが登録されます。

次の図では、時間 T2 が古い SA が期限切れになる時間です。T1 が T2 の 30 秒前で、これは、グループ メンバー（GM）によって発信方向で新しい SA の使用が開始される時間です。T0 は、T2 の 30 秒前です。T0 の時点で新しい SA が受信されない場合、グループ メンバーが登録される必要があります。T は、T0 の 30 秒前です。T の時点でキー サーバによってキー再生成が送信される必要があります。

図 *120 :* グループ メンバーにおける *IPsec SA* の使用



設定変更によってキー サーバごとのキー再生成のトリガーが可能

（注） セキュリティに対する脅威は、脅威からの保護に役立つ暗号化技術と同様に絶え間なく変化しています。最新のシスコの暗号化に関する推奨事項については、『Next Generation Encryption』（NGE）ホワイト ペーパーを参照してください。

キー サーバ上の設定変更によって、キー サーバごとの再生成のトリガーが可能です。次のサンプル設定を参照し、サンプルに記述されたもののうち、キー再生成が発生する変更と発生しない変更を確認してください。

```
crypto ipsec transform-set gdoi-p esp-aes esp-sha-hmac
!
crypto ipsec profile gdoi-p
 set security-association lifetime seconds 900
set transform-set gdoi-p
!
crypto gdoi group diffint
 identity number 3333
 server local
```

```
rekey algorithm aes 128
rekey address ipv4 121
rekey lifetime seconds 3600
no rekey retransmit
rekey authentication mypubkey rsa mykeys
sa ipsec 1
 profile gdoi-p
 match address ipv4 120
 replay counter window-size 3
```

次に示すキーサーバ上での設定変更では、キーサーバからのキー再生成がトリガーされます。

- TEK 設定におけるすべての変更（例の「sa ipsec 1」）。
  - ACL（上記例の「match address ipv4 120」）が変更された場合。ACL におけるすべての追加、削除、または変更がキー再生成の原因となります。
  - TEK リプレイがキー サーバ上でイネーブルまたはディセーブルになっている場合、キー再生成が送信されます。
  - TEK 内の IPsec プロファイルの削除または追加（例の「profile gdoi-p」）。
  - マルチキャストからユニキャスト転送への変更。
  - ユニキャストからマルチキャスト転送への変更。

次に示すキー サーバ上での設定変更は、キー サーバからのキー再生成のトリガーとはなりません。

- TEK 下におけるリプレイ カウンタ ウィンドウ サイズの変更（例の「sa ipsec 1」）。
- キー再生成再送信の設定または削除。
- キー再生成 ACL の削除または設定。
- TEK ライフタイムの変更（上記例の「set security-association lifetime seconds 300」）または KEK ライフタイムの変更（例の「rekey lifetime seconds 500」）。
- キー再生成アルゴリズムの追加、削除、または変更（例の「rekey algorithm aes 128」）。

キー再生成をトリガーするコマンド

次の表は、GET VPN コマンドによる変更の包括的な一覧です。どのコマンドがキー再生成のトリガーとなり、どのコマンドがならないのかを示しています。各コマンドは、それらのコマンドが入力されるコンフィギュレーションモードに基づいて分類しています。表には、キー再生成のトリガーになるか否かを問わず、コマンドが有効になるタイミングも示しています。

（注） GDOI グループで KEK ライフタイムが変更されると、現在の KEK が期限切れになり、新しい KEK が生成された場合にのみ変更が適用されます。キーサーバーでキー再生成コマンドの **crypto gdoi ks rekey** を発行することにより、強制的に変更を適用できます。

表 *287 :* キー再生成をトリガーするコマンド

説明	コマンド	キー再生成のトリガーとなるか	トリガーするタイミング	変更が有効になるタイミング
Mode = (config)	**configure terminal**	—	—	—
GDOI グループ内で使用される ACL の変更または削除（例：**rekey address ipv4** *access-list-number*[*options*]）	[**no**] **access-list** *access-list-number*[*options*]	非対応	—	即時
IPsec プロファイルで使用される ACL の変更または削除（例：**match address ipv4** *access-list-id* | *name*[*options*]）	[**no**] **access-list** *access-list-number*[*options*]	Yes	コンフィギュレーションモードの終了時	キーサーバー上での **show running-config** コマンドの出力は、ポリシーが不完全である、パケットがまだ既存の SA によって暗号化または復号されている、ダウンロードされた ACL は消去されたが mtree エントリがまだ存在している（**show crypto ruleset** コマンドの出力を表示することによる）、および、新しい SA がダウンロードされず、古い SA が暗号化または復号でまだアクティブであることを示します。
ISAKMP 事前共有キー（任意のキー）の追加または削除	**crypto isakmp key address** *peer-address*	非対応	—	即時

説明	コマンド	キー再生成のトリガーとなるか	トリガーするタイミング	変更が有効になるタイミング
ISAKMP事前共有キー（グループ メンバーのキー）の追加または削除	**crypto isakmp key address** *peer-address*	非対応	—	Key Encryption Key（KEK）SA が期限切れになった後（再登録）
IPsec プロファイルの追加	**crypto ipsec profile**	非対応	—	即時
ISAKMPポリシーの追加または削除	**crypto isakmp policy** *priority*	非対応	—	即時
Mode = (ipsec-profile)	**crypto ipsec profile** *name*	—	—	—
（IPsec プロファイル内の）SA ライフタイムの変更	**set security-association lifetime** *seconds*	非対応	—	次のキー再生成
トランスフォームセットの変更	**set transform-set** *transform-set-name*	Yes	コンフィギュレーション モードの終了時	古いトランスフォーム セットの SA は、ライフタイムが期限切れになるまでアクティブのままになります。
Mode = (config-gdoi-group)	**crypto gdoi group** *group-name*	—	—	—
ID 番号の変更	**identity number** *number*	非対応	—	グループ メンバー上でただちに設定する必要があります。他のグループ メンバーでは、古いグループ ID の TEK および KEK が引き続き使用されます。
Mode = (gdoi-local-server)	**server local**	—	—	—
ユニキャストからマルチキャスト転送への変更	**rekey transport unicast**	Yes	即時	キー再生成がトリガーされた後

説明	コマンド	キー再生成のトリガーとなるか	トリガーするタイミング	変更が有効になるタイミング
マルチキャストからユニキャスト転送への変更	[**no**] **rekey transport unicast**	Yes	コンフィギュレーションモードの終了時	キー再生成がトリガーされた後
キー再生成アドレスの変更	**rekey address ipv4** {*access-list-number* | *access-list-name*}	Yes	コンフィギュレーションモードの終了時	キー再生成がトリガーされた後（ただし、ACL自体を変更してもマルチキャストキー再生成はトリガーされません)
キー再生成ライフタイムの変更	**rekey lifetime seconds** *number-of-seconds*	非対応	—	次のキー再生成。ただし、コマンドが発行される（現在のライフタイムがキー再生成と共に送信される）と、ライフタイムは減少を開始します。
キー再生成再送信のイネーブル化またはディセーブル化	**rekey retransmit** *number-of-seconds* [**number** *number-of-retransmissions*]	非対応	—	次のキー再生成
キー再生成認証のイネーブル化	**rekey authentication mypubkey rsa** *key-name*	Yes	コンフィギュレーションモードの終了時	キー再生成がトリガーされた後
キー再生成認証のディセーブル化	[**no**] **rekey authentication**	非対応	—	即時

説明	コマンド	キー再生成のトリガーとなるか	トリガーするタイミング	変更が有効になるタイミング
キー再生成認証キーの変更	**rekey authentication mypubkey rsa** *key-name*	Yes	コンフィギュレーションモードの終了時	キー再生成がトリガーされた後
キー再生成暗号化の変更	**rekey algorithm** *type-of-encryption-algorithm*	Yes	コンフィギュレーションモードの終了時	新しいアルゴリズムは即座に有効になります。
Mode = (gdoi-sa-ipsec)	**sa ipsec** *sequence-number*	—	—	—
プロファイルの変更	**profile** *ipsec-profile-name*	Yes	コンフィギュレーションモードの終了時	ライフタイムが期限切れになるまで古いプロファイルの SA は有効のままです。
ACL の一致の変更	**match address** [options]	Yes	コンフィギュレーションモードの終了時	キー再生成がトリガーされた後
カウンタ リプレイのイネーブル化	**replay counter window-size** *seconds*	Yes	コンフィギュレーションモードの終了時	ライフタイムが期限切れになるまでカウンタリプレイなしの古い SA は非アクティブになります。
リプレイ カウンタ値の変更	**replay counter window-size** *seconds*	非対応	—	次のキー再生成

説明	コマンド	キー再生成のトリガーとなるか	トリガーするタイミング	変更が有効になるタイミング
時間ベースのアンチ リプレイのイネーブル化	**replay time window-size** *seconds*	Yes	コンフィギュレーション モードの終了時	時間ベースのアンチリプレイがイネーブルになった新しい SA が送信されますが、時間ベースのアンチリプレイがディセーブルになった古い SA は、ライフタイムが期限切れになるまでアクティブのままになります。
時間ベースのアンチ リプレイ ウィンドウの変更	**replay time window-size** *seconds*	非対応	—	新しい時間ベースのアンチリプレイウィンドウが有効になるのは、キーサーバーとグループメンバーの両方で **clear crypto gdoi** コマンドが入力された後だけです。
Mode = (gdoi-coop-ks-config)	**redundancy**	—	—	—
冗長性のイネーブル化	**redundancy**	非対応	—	他の各キーサーバ上でただちに設定する必要があります。
ローカル プライオリティの変更	**local priority** *number*	非対応	—	即時にですが、キーサーバに選択は強要しません。
ピア アドレスの追加または削除	[**no**] **peer address ipv4** *ip-address*	非対応	—	次の連携可能な（COOP）メッセージ

説明	コマンド	キー再生成のトリガーとなるか	トリガーするタイミング	変更が有効になるタイミング
冗長性のディセーブル化	[**no**] **redundancy**	非対応	—	他の各キーサーバ上でただちに設定する必要があります。

疑似時間同期によってタイムアウトが発生した場合、KEK タイマーまたは TEK タイマーのどちらかが次の 60 秒間に期限切れになるようにスケジュールされているかどうかがキー サーバによって確認されます。そのようにスケジュールされている場合、そのタイムアウトと疑似時間同期タイムアウトが結合されます。つまり、そのキー再生成は TEK キー再生成または KEK キー再生成と、疑似時間同期タイムアウトキー再生成の両方として動作します。疑似時間同期の詳細については、「時間ベースのアンチ リプレイ」セクションを参照してください。

キー再生成の再送信

マルチキャストキー再生成は、デフォルトで再送信されます。ユニキャストキー再生成では、キー サーバが ACK を受信しない場合にキー再生成が再送信されます。どちらの場合も、キー再生成の再送信前に、次の 120 秒間にスケジュールされている TEK キー再生成または KEK キー再生成があるかどうかがキーサーバによって確認されます。ある場合、現在の再送信は停止され、スケジュールされたキー再生成が発生するまで待機します。

グループ メンバー アクセス コントロール リスト

GET VPN の場合、保護する必要があるトラフィックは、 ACL によってキー サーバ上にスタティックに定義されます。グループ メンバーによって、キー サーバから保護対象に関する情報が取得されます。この構造によって、キーサーバによる必要に応じたポリシーの動的な選択および変更が可能となっています。Secure Multicast では、キー サーバの ACL が包括的に定義されます。ACLには、暗号化する必要があるトラフィックだけが厳密に定義されているだけでなく、暗黙の拒否によって、他のすべてのトラフィックは暗号化されない状態で許可されるようになっています（つまり、許可がない場合、他のすべてのトラフィックは許可されます）。

GET VPN では、異なる考え方が採用されています。つまり、暗号化する必要のあるパケットの定義が独立して配信されます。GET VPN でサポートしているのはスタティックに定義されたトラフィック セレクタだけです。キー サーバ上で、拒否 ACL と許可 ACL の両方を使用してポリシーを定義できます。グループ メンバー上で、手動で設定できるのは拒否 ACL だけです。キー サーバからダウンロードされるポリシーと、グループ メンバー上で設定されるポリシーは結合されます。グループ メンバー上で設定された ACL はすべて、キー サーバからダウンロードされたものよりも優先されます。

グループ メンバーによってキー サーバから ACL が取得されると、グループ メンバーによって、一時的な ACL が作成され、それがデータベースに挿入されます。何らかの理由によりグループ メンバーが GDOI グループから削除されると、この ACL は削除されます。パケットが

ACL に一致しているが、そのパケット用に IPsec SA が存在していない場合、インターフェイスから出ていくパケットは、グループ メンバーによって廃棄されます。

キー サーバによって一連のトラフィック セレクタが送信され、それらがグループ メンバー上のグループ メンバー ACL と正確には一致していない場合があります。このような違いが発生した場合、その違いを結合して解決する必要があります。グループ メンバーは、キー サーバよりもトポロジを認識するので、ダウンロードされた ACL は、グループ メンバー ACL の末尾に追加されます。グループ メンバー ACL（暗黙の拒否を除く）が最初にデータベースに挿入され、次に、ダウンロードされたキー サーバ ACL が挿入されます。このデータベースは優先化され、一致したエントリが検出された時はいつでも、データベース検索は終了します。

グループ メンバー ACL の設定方法については、「グループ メンバー ACL の設定」セクションを参照してください。

セキュリティ ポリシー変更時におけるグループ メンバーの動作

キー サーバで ACL または他のポリシーが変更されると、グループ メンバーの動作が変わります。次の 3 種類のシナリオで、グループ メンバーの動作に対するポリシーの各種変更の影響を説明します。

シナリオ 1

次の例では、ホスト A とホスト B を許可するように ACL が最初に設定されています。

```
ip access-list extended get-acl
permit ip host A host B
permit ip host B host A
```

次に、キー サーバで、ホスト C とホスト D を許可するように ACL が変更されます。

```
ip access-list extended get-acl
permit ip host C host D
permit ip host D host C
```

ACL の変更は、次の方法でグループ メンバーの動作に影響を与えます。

- キー サーバによって、ただちに、すべてのグループ メンバーに対してキー再生成が送信されます。
- キー再生成後ただちに、グループメンバーによって、ホストAとホストB間のトラフィックが暗号化されていないテキストで送信されます。
- キー再生成後ただちに、グループメンバーによって、ホストCとホストD間のトラフィックが暗号化されたテキストで送信されます。

（注） Cisco ASR 1000 シリーズ アグリゲーション サービス ルータと Cisco ISR G2 ルータの GETVPN グループメンバーは、キーサーバーでの ACL の変更またはその他のポリシー変更に続くキー再生成（トリガーまたは定期的）の後に、異なる動作をします。Cisco ISR G2 ルータのグループメンバーは、完全な再登録なしで新しいポリシーをインストールしますが、Cisco ASR 1000 シリーズ アグリゲーション サービス ルータのグループメンバーは、更新されたポリシーを取得するために再登録します。

シナリオ 2

ポリシーによってトランスフォームセットが更新され、時間ベースのアンチリプレイ（TBAR）の変更がキー サーバに対して行われると、グループ メンバーの動作が変わります。

このシナリオでは、次のことが想定されています。

- トランスフォーム セットが、ESP-3DES から ESP-AES へ変更されている。
- ポリシーの変更は、現在の TEK ライフタイムが期限切れになる 1000 秒前に発生する。

これらのポリシーの変更は、次のようにグループ メンバーの動作に影響を与えます。

- キー サーバによって、古い SA（3DES）と新しい SA（AES）の両方のキー再生成が送信されます。
- グループ メンバーでは、期限切れになるまでの 1000 秒間、古い SA（3DES）の使用が継続されます。
- 古い SA が期限切れになると、グループ メンバーによって、新しい SA（AES）に自動的に切り替えられます。

シナリオ 3

キー サーバで、ACL の変更と、トランスフォーム セットや TBAR など他の変更の両方を含むその他のポリシーの更新が行われると、グループ メンバーの動作が変わります。

このシナリオでは、次のことが想定されています。

- ACL がシナリオ 1 で指定されたとおりに更新されている。
- トランスフォーム セットが、ESP-3DES から ESP-AES へ変更されている。
- ポリシーの変更は、現在の TEK ライフタイムが期限切れになる 1000 秒前に発生する。

ACL の変更とその他のポリシーの更新は、次のようにグループ メンバーの動作に影響を与えます。

- キーサーバによって、古いSA（3DES）と新しいSA（AES）の両方で構成されているキー再生成が送信されます。
- キー再生成後ただちに、グループ メンバーによって、ホストAとホストB間のトラフィックが暗号化されていないテキストで送信されます。
- グループ メンバーによって、TEK のライフタイムが期限切れにならない限り 1000 秒間、古い SA（3DES）を使用した、ホスト C とホスト D 間の暗号化されたトラフィックが送信されます。
- 古い SA（3DES）が期限切れになると、グループ メンバーによる新しい SA への切り替えが自動的に行われ、AES におけるホスト C とホスト D 間のトラフィックが暗号化されます。

時間ベースのアンチリプレイ

アンチ リプレイは、IPSec（RFC 2401）のようなデータ暗号化プロトコルにおいて重要な機能の 1 つです。アンチ リプレイによって、第三者が IPsec カンバセーションを盗聴したり、パケットを盗んだり、さらにはそれらのパケットを後でセッションに挿入したりすることを防ぐことが可能です。時間ベースのアンチ リプレイ メカニズムを利用すれば、過去にすでに到着しているはずのリプレイ パケットを検出することによって、無効なパケットを廃棄できます。

GET VPN では、マルチセンダ トラフィック用のアンチ リプレイ保護を提供するために、同期アンチ リプレイ（SAR）が使用されています。SAR は、実社会のネットワーク タイム プロトコル（NTP）クロックや、シーケンシャル カウンタ メカニズム（パケットが送信順に受信されて処理されることを保証するメカニズム）とは独立しています。SAR クロックは、ルール正しく進みます。このクロックによって追跡される時間は、疑似時間と呼ばれます。疑似時間はキー サーバ上で維持され、キー再生成メッセージ内で指定されているグループ メンバーに対して、pseudoTimeStamp というタイムスタンプ フィールドとして定期的に送信されます。GET VPN では、Metadata というシスコ独自のプロトコルによって、psuedoTimeStamp をカプセル化しています。グループ メンバーは、定期的にキー サーバの疑似時間に再同期される必要があります。キー サーバの疑似時間は、最初のグループ メンバーが登録されたときから進み始めます。最初は、登録プロセス中に、キー サーバからグループ メンバーに対して、キー サーバの現在の疑似時間の値およびウィンドウ サイズが送信されます。時間ベースのリプレイ対応情報、ウィンドウ サイズ、キー サーバの疑似時間などの新しい属性は、SA ペイロード（TEK）で送信されます。

グループ メンバーは、疑似時間を使用して次のようにリプレイを防止します。pseudoTimeStamp には、送信者がパケットを作成したときの疑似時間の値が含まれています。受信者は、送信者の疑似時間の値と自身の疑似時間の値を比較して、パケットが再送されたパケットであるかどうかを判断します。受信元では、時間ベースのアンチリプレイ「ウィンドウ」を利用して、そのウィンドウ内のタイプスタンプ値が格納されたパケットを受信します。ウィンドウ サイズは、キー サーバで設定されて、すべてのグループ メンバーに送信されます。

（注） グループ メンバーとして Cisco VSA を使用している場合、時間ベースのアンチ リプレイは使用しないでください。

次の図は、アンチリプレイ ウィンドウを示しています。値PTrは受信者のローカルの疑似時間を、W はウィンドウ サイズを示しています。

図 *121 :* アンチリプレイ ウィンドウ

クロック同期

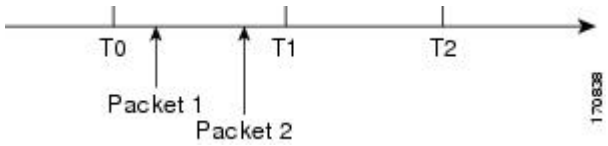
グループ メンバーのクロックとキー サーバとの同期は、ずれたり失われたりする可能性があります。クロックの同期を維持するため、キーサーバの最新の疑似時間値が格納されたキー再生成メッセージ（マルチキャストがユニキャストかは状況に応じます）が（キー再生成メッセージで、あるいは、グループメンバーに対して最小で30分ごとに）定期的に送信されます。このアンチ リプレイ チェックでパケットにエラーが発生した場合、送信元および受信元の両方の疑似時間がプリントされ、エラーメッセージが生成され、カウントの値が増分されます。

アンチリプレイの統計情報を表示するには、送信元および受信元デバイスの両方で**show crypto gdoi group** *group-name* **gm replay** コマンドを使用します。管理者がサイズ設定のリプレイ方法に影響を与えるような設定変更を行った場合、キーサーバによってキー再生成メッセージが発信されます。

インターバル期間

ティックは、SAR クロックのインターバル期間です。この期間に送信された各パケットの pseudoTimeStamp は同じものになります。またティックは、キー サーバからの疑似時間と共にグループ メンバーにダウンロードされます。たとえば、次の図に示すように、T0 と T1 の間で送信されたパケットの pseudoTimeStamp は同じ T0 になります。SAR には、ルーズなアンチ リプレイ保護が用意されています。リプレイされたパケットは、それらがウィンドウ内にリプレイされている場合は、受信されます。デフォルトのウィンドウ サイズは100秒です。パケットのリプレイを最小限に抑えるため、ウィンドウ サイズを小さく保つことを推奨します。

図 *122 : SAR* クロックのインターバル期間



アンチ リプレイ設定

アンチ リプレイ機能をキー サーバ上の IPsec SA 下でイネーブルにするには、次のコマンドを使用します。

- **replay time window-size**：非シーケンシャルまたは時間ベースモードがサポートされるリプレイ時間オプションをイネーブルにします。ウィンドウ サイズは秒単位です。このモードは、1 つのグループ内に 3 つ以上のグループ メンバーが存在している場合にだけ使用します。
- **replay counter window-size**：シーケンシャルモードをイネーブルにします。このモードは、1 つのグループ内に 2 つのグループ メンバーだけが存在している場合に便利です。
- **no replay counter window-size**：アンチリプレイをディセーブルにします。

コントロール プレーンの時間ベースのアンチリプレイ

キー再生成疑似時間のチェック

キーサーバとグループメンバー間のキー再生成疑似時間のチェックは次のように行われます。

- グループメンバーがキーサーバと自身との疑似時間の許容差を計算します。データプレーンで設定された TBAR ウィンドウ サイズ、または 30 秒の小さい方となります。
- グループメンバーは自身より疑似時間が大きいすべてのキー再生成を受け入れ、自身の疑似時間をより大きい値に更新します。計算された疑似時間の許容差よりも差が大きい場合は、次の syslog メッセージも生成されます。

```
*Jul 28 22:56:37.503: %GDOI-3-PSEUDO_TIME_LARGE: Pseudotime difference between key server
 (20008 sec) and GM (10057 sec) is larger than expected in group GET. Adjust to new
pseudotime
```

- グループメンバーが自身よりも疑似時間が小さいが許容差以内のキー再生成を受信した場合、グループメンバーはキー再生成を受け入れ、疑似時間値をそのキー再生成疑似時間値に更新します。
- グループメンバーが自身よりも疑似時間が小さいが許容差を超えているキー再生成を受信した場合、グループメンバーはキー再生成メッセージをドロップし、次の syslog メッセージを生成します。

```
*Jul 28 23:37:59.699: %GDOI-3-PSEUDO_TIME_TOO_OLD: Rekey received in group GET is too
old and fail PST check: my_pst is 22490 sec, peer_pst is 10026 sec, allowable_skew is
30 sec
```

セカンダリ キー サーバでの ANN メッセージ疑似時間の処理

連携キー サーバ間のポリシーおよびグループメンバー情報の同期には、連携キー サーバ通知（ANN）メッセージが使用されます。

セカンダリ サーバ キーは次のように ANN メッセージを処理します。

- セカンダリ キー サーバが ANN メッセージの許容疑似時間を計算します。データ プレーンで設定された TBAR ウィンドウ サイズの値、または 30 秒の小さい方となります。
- セカンダリ キーサーバが疑似時間がより大きいプライマリ キーサーバから ANN メッセージを受信した場合、次が行われます。
- 疑似時間をプライマリ キー サーバの値に更新します。
- 疑似時間の差が許容差よりも大きい場合は、次の syslog メッセージが生成されます。

```
*Jul 28 23:48:56.871: %GDOI-4-GDOI_ANN_TIMESTAMP_LARGE: COOP_KS ANN received from KS
10.0.8.1 in group GET has pseudotime bigger than myself. Adjust to new pseudotime:
my_old_pst is 23147 sec, peer_pst is 30005 sec
```

- セカンダリ キーサーバが疑似時間がより小さいプライマリ キーサーバから ANN メッセージを受信した場合、次のようになります。

- 差が許容範囲内の場合、セカンダリ キー サーバはそれを受け入れ、疑似時間をプライマリ キー サーバの値に更新します。
- 差が許容範囲を超える場合は、次の syslog メッセージが生成されます。

```
*Jul 28 23:42:12.603: %GDOI-4-GDOI_ANN_TIMESTAMP_TOO_OLD: COOP_KS ANN from KS 10.0.8.1
in group GET is too old and fail PST check:
my_pst is 22743 sec, peer_pst is 103 sec, allowable_skew is 10 sec
```

3 つの再送信要求の後、セカンダリ キー サーバが有効な疑似時間の ANN メッセージを受信していない場合は、次のように、新しいグループメンバー登録のブロックが開始されます。

```
*Jul 28 23:38:57.859: %GDOI-5-COOP_KS_VALID_ANN_TIMER_EXPIRED: This sec-KS has NOT
received an ANN with valid pseudotime for an extended period in group GET. It will block
 new group members registration temporarily until a valid ANN is received
*Jul 29 00:08:47.775: %GDOI-5-COOP_KS_BLOCK_NEW_GM_REGISTER: This key server temporarily
 blocks group member with ip-addr 10.0.0.2 from registering in group GET as it has not
received an ANN with valid pseudotime for prolonged period
```

セカンダリ キー サーバは、次のいずれかが発生するとグループ メンバー登録機能を再開します。

- プライマリ キー サーバから有効な疑似時間の ANN を受け取る。
- プライマリ キー サーバになる。
- **clear crypto gdoi group** コマンドはセカンダリキーサーバーで実行されます。

プライマリ キー サーバでの ANN メッセージ疑似時間の処理

プライマリ サーバ キーは次のように ANN メッセージを処理します。

- ANN メッセージの許容疑似時間を計算します。データ プレーンで設定された TBAR ウィンドウ サイズの値、または 30 秒の小さい方となります。
- 疑似時間が小さいが許容差以内のセカンダリ キー サーバ ANN メッセージは受け入れられます。
- 疑似時間が小さいが許容差を超えている ANN メッセージは拒否されます。

ネットワークのマージ中は、次の条件が適用されます。

- 新しいプライマリ キー サーバは 2 つのキー サーバ間で大きい方の疑似時間を常に選択します。
- 差が計算された疑似時間の許容差よりも大きい場合、新しいプライマリ キー サーバはキー再生成をすべてのグループ メンバーに対して送信し、疑似時間を更新します。また、次の syslog メッセージも生成されます。

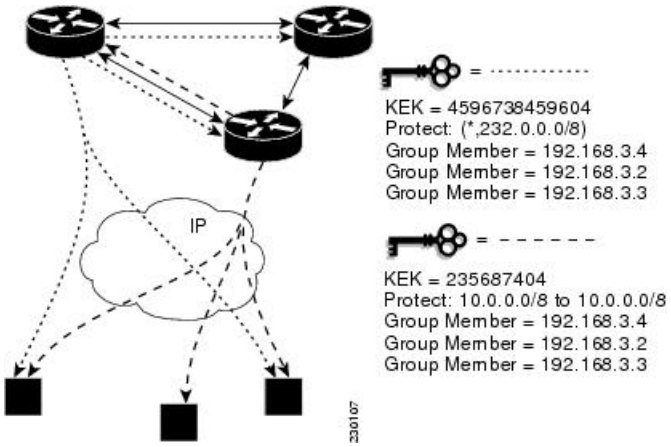
```
*Jul 28 23:42:41.311: %GDOI-5-COOP_KS_ELECTION: KS entering election mode in group GET
(Previous Primary = NONE)
*Jul 28 23:42:41.311: %GDOI-4-GDOI_ANN_TIMESTAMP_LARGE: COOP_KS ANN received from KS
10.0.9.1 in group GET has PST bigger than myself. Adjust to new pseudotime:
my_old_pst is 0 sec, peer_pst is 22772 sec
```

```
*Jul 28 23:43:16.335: %GDOI-5-COOP_KS_TRANS_TO_PRI: KS 10.0.8.1 in group GET transitioned
 to Primary (Previous Primary = NONE)
*Jul 28 23:43:16.347: %GDOI-5-KS_SEND_UNICAST_REKEY: Sending Unicast Rekey for group GET
 from address 10.0.8.1 with seq # 1
```

連携キー サーバ

次の図は、連携キー サーバのキー配布を示したものです。図の下のテキストで、連携キー サーバ機能について説明します。

図 *123 :* 連携キー サーバのキー配布



連携キー サーバを利用すると、GET VPN に冗長性が与えられます。冗長性、高可用性、およびプライマリ キー サーバに障害が発生した場合の素早いリカバリを確保するために、複数のキー サーバが GET VPN によってサポートされます。複数の連携 GDOI キー サーバによって、共同でグループの GDOI 登録が管理されます。各キー サーバはアクティブなキー サーバであり、各グループ メンバーからの GDOI 登録要求を処理します。キー サーバどうしで連携しているので、各キー サーバから、そのキー サーバに登録するグループ メンバーに対して同じ状態が配信されます。それぞれの GDOI キー サーバによって、GDOI 登録の一部を処理できるので、ロードバランスが実現します。

プライマリ キーの役割は、グループ ポリシーの作成と配信です。連携キー サーバのキー配布が発生すると、1 つのキー サーバが自身をプライマリとして宣言し、ポリシーを作成し、そのほかのセカンダリ キー サーバにポリシーを送信します。セカンダリ キー サーバは、ポリシーを取得して選択モードを終了すると、プライマリ キー サーバをプライマリ キー サーバとして宣言します。また、セカンダリ キー サーバは、連携キー サーバのキー配布が進行している間、GM 登録をブロックします。この変更により時間が短縮されるため、連携キー サーバの配布はより効率的になります。たとえば、配布時には次のような syslog の警告メッセージが表示されます。

```
00:00:16: %GDOI-5-COOP_KS_BLOCK_NEW_GM_REGISTER_ELECTION: This KS temporarily blocks GM
 with ip-addr 10.0.4.1 from registering in group diffint as the KS election is underway
```

プライマリ キー サーバによってグループ情報のアップデートが他のすべてのキー サーバに定期的に送信（またはブロードキャスト）され、その結果、これらのサーバどうしの同期が維持されます。何らかの理由によりセカンダリ キー サーバがアップデートの受信に失敗した場合、

そのセカンダリ キー サーバは、プライマリ キー サーバにアクセスして、直接情報のアップデートを要求します。延長期間にアップデートが受信されない場合、セカンダリ キー サーバによって、プライマリ サーバが到達不能（つまり「dead」）としてマーキングされます。

新しいポリシーがプライマリ キー サーバで作成されると、グループ メンバーが登録されるキー サーバがどのサーバかにかかわらず、プライマリ キー サーバの役割は、GDOI グループ メンバーに対するキー再生成メッセージの配信となります。

連携キー サーバ設定では、キー再生成のシーケンス番号がプライマリおよびセカンダリ キー サーバ間で同期されます。

ネットワーク マージでは、キー サーバは両者の大きい方のキー再生成シーケンス番号が選択されます。

連携キーサーバーの設定で 300 を超えるグループメンバーをサポートしている場合、**buffers huge size** コマンドを使用してバッファサイズを増やす必要があります。

キーサーバーの GETVPN グループ設定で使用される登録インターフェイスがシャットダウンされると、ネットワークスピットが発生します。推奨設定であるループバック インターフェイスの場合のように、インターフェイスが転送インターフェイスでない場合、キー再生成はグループ内のすべての KS から GM に送信されます。インターフェイスをシャットダウンすることによってキーサーバーをオフにすることはできません。キーサーバーを安全にオフにするには、**no crypto gdoi group** *group name* コマンドを使用します。

次の例は、キーサーバーの GETVPN グループ設定で参照される登録インターフェイスを示しています。

```
crypto gdoi group groupA
identity number 111
server local
  sa ipsec 10
   profile groupA
   match address ipv4 groupA-crypto-policy
   no replay
  no tag
  address ipv4 a.b.c.d
  redundancy
   local priority 250
   peer address ipv4 a.b.c.d
   peer address ipv4 a.b.c.d
```

通知メッセージ

通知メッセージは IKE フェーズ 1 によってセキュリティ保護され、IKE 通知メッセージとして送信されます。IKE によって提供される認証および機密保持は、キー サーバ間のメッセージをセキュリティ保護するために使用されます。通知メッセージ内のシーケンス番号によって、アンチ リプレイ保護が提供されます。通知メッセージは定期的にプライマリ キー サーバからセカンダリ キー サーバに送信されます。

通知メッセージには、現在の状態を維持するための次のコンポーネントが含まれます。

キー サーバの送信元プライオリティ

この値は送信元のプライオリティを示します。CLIによって設定可能です。最も高いプライオリティを持つキー サーバがプライマリ キー サーバとなります。プライオリティの値が同じ場合、最も高いIPアドレスを持つキー サーバがプライマリ キー サーバになります。

送信元のロールの維持

同期期間中、各キー サーバが地理的に分散した場所にある場合、それらのキー サーバにネットワーク分割イベントが発生する可能性があります。ネットワーク分割イベントが発生した場合、一定の期間中、複数のキーサーバがプライマリ キーサーバになる可能性があります。ネットワークが再び正常に動作し、すべてのキー サーバが互いに検知したら、各キー サーバがそれぞれの正しいロールを維持できるように、それらのサーバに対して、送信元の現在のロールを通知する必要があります。

リターン パケット フラグの要求

すべてのメッセージは一方向のメッセージとして定義されています。必要に応じて、キーサーバによってピアから現在の状態を要求し、そのロールを検出するか、グループの現在の状態を要求するかを行うことができます。

グループ ポリシー

グループ ポリシーは、任意のグループのために維持されるポリシーです。グループ メンバーの情報、IPsec SA、およびキーなどがあります。

アンチリプレイ機能および組み込まれた連携通知メッセージがサポートされています。プライマリ キー サーバによって疑似時間値が更新され、その値がグループ内のすべてのセカンダリ キーサーバに送信されます。セカンダリ キーサーバによって、それらのサーバのSARクロックとこの更新された値とが同期されます。

連携キー サーバ間の ANN メッセージ シーケンス番号のチェック

次に、連携キー サーバ間のシーケンス番号のチェックについて説明します。

- 連携キーサーバは、最後に受信したANNメッセージのシーケンス番号以下の番号のANNメッセージをすべてドロップします。
- ANNメッセージは、その差が大きくても、最後に受信したキー再生成メッセージよりシーケンス番号が大きい場合に承認されます。
- キー サーバがリロードされると、新しいIKEセッションがピア間に作成され、リロードされたキー サーバのANNシーケンス番号はゼロから開始します。この場合、もう一方ではどのシーケンス番号のANNメッセージも受け入れます。

キー サーバのロールの変更

連携キー サーバのネットワークでは、プライマリ サーバが、選択時における最も高いプライオリティに基づいて選択されます。他のキーサーバのステータスはセカンダリになります。プ

ライマリキーサーバーが停止状態として検知されたり、そのロールが変更されたりした場合、**clear crypto gdoi ks coop role** コマンドを使用すれば、プライマリキーサーバーの連携ロールをリセットできます。

clear crypto gdoi ks coop role コマンドがセカンダリキーサーバー上で実行されると、選択がそのセカンダリキーサーバー上でトリガーされますが、すでに選択されているプライマリキーサーバーが存在しているため、たいていの場合そのサーバーはセカンダリキーサーバーのままとなります。しかし、**clear crypto gdoi ks coop role** コマンドがプライマリキーサーバー上で実行された場合、そのプライマリキーサーバーはセカンダリロールに再割り当てされ、その結果、すべてのキーサーバーが関わる新しい選択がトリガーされます。前のプライマリ サーバのプライオリティが（すべてのキーサーバの中で）最も高い場合、そのサーバが再びプライマリサーバになります。前のプライマリ サーバがプライオリティの最も高いサーバではない場合、プライオリティが最も高いサーバが新しいプライマリ サーバとして選択されます。

受信専用 SA

マルチキャスト トラフィックで GDOI プロトコルが使用されている場合、双方向 SA がインストールされます。受信専用機能を利用すれば、段階的な導入が可能となり、ネットワーク全体を稼働させる前にごく少数のサイトを確認できます。サイトをテストするには、グループ メンバーの 1 つが他のすべてのグループ メンバーに暗号化されたトラフィックを送信し、トラフィックを復号化してトラフィックを「暗号化せずに」転送させる必要があります。受信専用 SA モードでは、期間の受信方向のみで暗号化できます。（受信専用 SA プロセスの手順を参照してください）。キーサーバーで **sa receive-only** コマンドを設定する場合、ステップ 2 および 3 は自動的に発生します。

1. GDOI キー サーバ上で IPsec SA を「受信専用」としてマーキングします。

これにより、グループ メンバーによる着信方向だけの SA のインストールが可能となります。受信専用 SA は、暗号グループの下で設定できます（「グループ ID、サーバ タイプ、および SA タイプの設定」セクションを参照してください）。

1. GDOI TEK ペイロードを「受信専用」としてマーキングします。

sa receive-only コマンドが設定されている場合、このグループ下のすべての TEK は、グループ メンバーへの送信時に、キーサーバーによって「受信専用」としてマーキングされます。

1. 一方向の IPsec フローのインストール

GDOI グループ メンバーによって、「受信専用」としてマーキングされているキー サーバからの IPsec SA が受信される度に、グループ メンバーによって、着信方向と発信方向の両方ではなく、着信方向だけでこの IPsec SA がインストールされます。

1. 次のローカル変換コマンドを使用して個々のグループ メンバーをテストします。
2. **crypto gdoi gm ipsec direction inbound optional**
3. **crypto gdoi gm ipsec direction both**

最初に、個々のグループ メンバーを個別に passive モード（この変換により、発信チェックに対して有効な SA が存在することが通知されます）に変換してから、次に、双方向モードに変換します。

1. 「受信専用」から「受信および送信」にグローバルに変換します。

テスト フェーズが終了し「受信専用」SA を双方向 SA に変換しなければならない時には、次の方式を使用できます。

グローバル変換

グループ下の **sa receive-only** コマンドを削除します。**sa receive-only** コマンドを削除すると、このグループの新しい IPsec SA が作成され、キー再生成が開始されます。受信と同時に、グループ メンバーによって、双方向で SA が再インストールされ、その SA の passive モードでの使用が開始されます。SA が永続的に passive モードでいることはできないので、5 分間キー再生成がなかった場合、グループ メンバーによって、これらの SA が受信モードまたは送信モードに変更されます。passive モードから双方向暗号化モードへの変換は自動で行われるので、管理者は何もする必要はありません。

パッシブ SA

パッシブ SA 機能によって、グループ メンバーを、永続的に passive モードにするように設定できます。パッシブ SA 機能を使用すれば、**crypto gdoi gm ipsec direction inbound optional** 特権 EXEC コマンドを使用する必要はなくなります。ただし、ルータのリロード後にこれが永続するわけではなく、キー再生成からのキーサーバー設定によって無効にできます。passive モードのグループ メンバーがあると、GET VPN への移行中におけるネットワーク テストやデバッグに利点があります。移行中に完全な暗号化保護を利用できるからです。グループ メンバーの passive モード設定は、キー サーバ設定よりも高いプライオリティを持ちます。**crypto gdoi gm ipsec direction inbound optional** 特権 EXEC コマンドは、グループメンバーとキーサーバーの設定を元に戻す次のキー再生成まで設定を無効にすることができます。

パッシブ SA 機能を設定するには、「パッシブ SA の設定」セクションを参照してください。

拡張ソリューションの管理性

機能の確認を支援するために、複数の **show** コマンドおよび **debug** コマンドがサポートされています。詳細については、「Fail-Close モードのアクティブ化」セクションを参照してください。

VRF-Lite インターフェイスによるサポート

VRF-Lite アプリケーションでは、ルーティング テーブルをユーザ グループ（または VPN）ごとに分離することによって、コントロール プレーンおよびフォワーディング プレーンでのトラフィックのセグメンテーションがサポートされています。また、各ユーザ グループの関連インターフェイスまたは専用インターフェイス上のトラフィックが転送されます。

MPLS VPN ネットワークに接続されているリモート サイトによって、セグメンテーションをキャンパスから WAN へ拡張する導入シナリオがあります。このような拡張されたセグメンテーションの場合、CE（グループ メンバーまたはキー サーバ）デバイス上の CE-PE インター

フェイスが、関連する Virtual Routing and Forwarding（VRF）に「バインド」されます。この VRF インターフェイスは、MPLS PE デバイスに接続されます。MPLS PE デバイスでは、VRF インターフェイスが関連するボーダー ゲートウェイ プロトコル（BGP）VRF プロセスにマッピングされています。このような場合、クリプト マップが VRF インターフェイスに適用されます。他の設定変更は必要ありません。

GM 登録の認証ポリシー

GM は、事前共有キーまたは公開キー インフラストラクチャ（PKI）を使用して登録時にキー サーバに認証できます。事前共有キーは、展開が容易ですが、プロアクティブに管理する必要があります。シスコはネットワーク内のすべてのデバイスに対してデフォルト キー（0.0.0.0 のアドレスで定義されるキー）を定義するのではなく、ピアベースの事前共有キーを展開することをお勧めします。事前共有キーは定期的に更新する必要があります（数ヵ月ごと）。

（注） キー再生成は KEK を使用してセキュリティが確保されるため、事前共有キーは暗号化データ プレーンまたはコントロール プレーンに影響を与えずにキー サーバ グループ メンバー（KS-GM）ピアごとに更新できます。新しく割り当てられた事前共有キーを使用して、発注済みの一連のキー サーバごとに GM を再登録できるようにすることが重要です。

PKI では、事前共有キーを使用するときに直面するキー管理の困難を克服するためにインフラストラクチャを使用します。PKI インフラストラクチャは認証局（CA）として機能し、ここでルータ証明書が発行され、維持されます。ただし、IKE 認証中に PKI を使用することは計算負荷が集中します。PKI の展開では、キー サーバのキャパシティ、設計、および配置が重要になります。

セキュリティを強化するため、GET VPN では事前共有キーまたは PKI を使用する GM 認証もサポートします。詳細については、「GET VPN 認証」セクションを参照してください。

GET VPN GM 認証

GET VPN GM 認証は、事前共有キーまたは PKI を使用して実行できます。GET VPN 認証をオンにすることはベスト プラクティスです。キー サーバが複数の GDOI グループに使用される際、あるグループの GM が別のグループからキーとポリシーを要求するのを防ぐには、キー サーバ認証が必要です。ISAKMP 認証では GM がキー サーバから GDOI 属性を要求できることが確認され、GDOI 認証では GM がキー サーバに設定された特定のグループから GDOI 属性を要求できることが確認されます。

GDOI 認証は、GM から送信された ISAKMP ID に基づきます。GM が ID として IP アドレスを送信すると、認証アドレスのみが認証に使用されます。GM が識別名（DN）またはホスト名を送信すると、認証 ID が使用されます。ID として IP アドレスを使用すると、DN またはホスト名と照合する認証がバイパスされます。逆も同様です。特定の DN の GM だけが接続できる（別の ID を使用する GM が接続できない）ようにするには、認証アドレスで **deny any** を指定する必要があります。

事前共有キーを使用する GM 認証

事前共有キーを使用するとき、GET VPN では IP アドレスを使用する GM 認証がサポートされます。GM の WAN アドレス（またはサブネット）を照合する ACL は、GET VPN グループ設定に定義し、適用することができます。ACL と一致する IP アドレスを持つ GM は認証が成功し、キー サーバに登録できます。GM IP アドレスが ACL と一致しない場合、キー サーバは GM の登録要求を拒否します。

認証失敗の場合、次の syslog メッセージが生成されます。

```
%GDOI-1-UNAUTHORIZED_IPADDR: Group getvpn received registration from
unauthorized ip address: 10.1.1.9
```

PKI を使用する GM 認証

PKI を使用する場合、GET VPN では一般的に使用される DN または完全修飾ドメイン名（FQDN）を使用する GM 認証がサポートされます。GM 認証をアクティブにするには、**authorization identity** コマンドを使用します。GM 証明書の特定のフィールド（通常、組織ユニット（OU））と一致する暗号 ID は、GET VPN グループ設定に定義し、適用することができます。暗号 ID を定義するには、**crypto identity** コマンドを使用します。

証明書クレデンシャルが ISAKMP ID と一致する GM は認証され、キー サーバに登録できます。たとえば、すべての GM 証明書に OU=GETVPN が発行される場合、すべての GM が OU=GETVPN を持つ証明書を提示することをチェック（認証）するようにキー サーバを設定できます。GM が提示する証明書の OU がそれ以外に設定されている場合、GM のキー サーバへの登録は認証されません。

認証が失敗した場合、次の syslog メッセージが生成されます。

```
%GDOI-1-UNAUTHORIZED_IDENTITY: Group getvpn received registration from
unauthorized identity: Dist.name: hostname=GroupMember-1, ou=TEST
```

Protocol Independent Multicast-Sparse Mode でのキー再生成機能

マルチキャスト キー再生成は、マルチキャストのすべてのモードで使用できます。継続するトラフィックが受信されないと PIM-SM Shortest Path Tree（SPT）が廃棄される可能性があるため、Protocol Independent Multicast-Sparse Mode（PIM-SM）を設定するときは必ず、**rekey retransmit** コマンドを使用する必要があります。トラフィックが再開すると、PIM-SM によって SPT が必ず確立されます。キー再生成パケットを再送信すると、PIM-SM による SPT の設定時にグループ メンバーによってキー再生成が受信される可能性が高くなります。

Fail-Close モード

グループ メンバーがキー サーバに登録されないと、そのグループ メンバーを通過するトラフィックが暗号化されません。この状態は「フェール オープン」と呼ばれます。グループ メンバーが登録される前に暗号化されていないトラフィックがそのグループ メンバーを通過することを防ぐには、Fail-Close 機能を設定します。この機能を設定すると、暗黙的な「permit ip any any」ポリシーがインストールされ、そのグループ メンバーを通過する暗号化されていないトラフィックはすべて廃棄されます（この状態を Fail-Close モードと呼びます）。

Fail-Close 機能は、インターフェイス ACL を設定することによっても実現可能です。ただし、Fail-Close 機能は、ACL リストよりも管理しやすく、実装も簡単です。

Fail-Close 機能を設定している場合でも、 **match address** コマンド（**match address** {*access-list-number* | *access-list-name*}）を設定することによって、特定の暗号化されていないトラフィックがグループメンバーを通過することを許可することが可能です。この明示的な「deny」ACL は、暗黙的な「permit ip any any」によって、拒否された（暗号化されていない）トラフィックがグループ メンバーの通過を許可される前に追加されます。

グループ メンバーの登録が正常終了したら、Fail-Close ポリシーが明示的であるか暗黙的であるかを問わず削除され、グループ メンバーの動作が、Fail-Close 機能が設定される以前のものと同じになります。

Fail-Close 機能の使用上の注意事項

Fail-Close モードで作業するためにクリプト マップを設定する場合、注意しなければならないことがあります。Fail-Close ACL を正しく定義しないと、自分自身をロックアウトしてしまう可能性があります。たとえば、セキュアシェル（SSH）を使用して暗号マップが適用されたインターフェイス経由でルータにログインする場合、**deny tcp any eq** *port* **host** *address* コマンドラインを Fail-Close ACL 下に含める必要があります。キーサーバーへのパスを検索する場合は、ルータが使用しているルーティングプロトコル（**deny ospf any any** など）も含める必要がある場合もあります。最初に Fail-Close とその ACL を設定し、次に **show crypto map gdoi fail-close** *map-name* コマンドを使用して Fail-Close ACL を確認します。Fail-Close ACL を確認し、それが正しいと確信したら、**activate** コマンドを設定して、Fail-Close モードで暗号マップを動作させることができます。**activate** コマンドを設定しない限り、Fail-Close はアクティブになりません。

Fail-Close ACL はグループ メンバーの視点で設定します。Fail-Close ACL は、グループ メンバー上で次のように設定されます。

access-list 125 deny ip host *host1-ip-addr host2-ip-addr*

Fail-Close モードでは、host1 から host2 へのすべての IP トラフィックが、Group Member 1 によって、暗号化されていないテキストで送信されます。さらに、着信ミラートラフィック（つまり、host2 から host1 への IP トラフィック）も、GM1 によって暗号化されていないテキストで受信されます。

（注） deny エントリに一致するすべての IP トラフィックは、グループ メンバーによって、暗号化されていないテキストで送信されます。

着信トラフィックは、ミラー アクセス リストに対応付けられます。

Fail-Close アクセス リストは、グループ メンバー アクセス リストと同じルールに従います。詳細は、「グループ メンバー アクセス コントロール リスト」のセクションを参照してください。

GDOI 登録を行うために **deny udp any eq 848 any eq 848** コマンドを設定する必要はありません。コード自体によって、そのコードの設定対象となっているキー サーバからの、特定のグ

ループ メンバーの GDOI パケットであるかどうかが判断されます。そのグループ メンバーの GDOI パケットだった場合、そのパケットは処理されます。ただし、キーサーバーがグループメンバー 1 の後になるシナリオでは、グループメンバー 1 がキーサーバーに正常に登録できない場合、グループメンバー 1 に対して明示的に **deny udp any eq 848 any eq 848** コマンドラインが設定されていない限り、他のグループメンバーも登録できなくなります。しかし、Fail-Close 機能が正しく設定されている場合は、グループ メンバーがキーサーバへの登録に失敗しても、望まないトラフィックが「暗号化されずに」出ていくことがないようにすることができます。ただし、他のグループ メンバーからの登録パケットが、登録に失敗した場合でもグループ メンバー 1 経由でキー サーバに到達できる場合、指定されたトラフィックが暗号化されずに出ていくことを許可することができます。

Fail-Close モードの設定の詳細については、「Fail-Close モードのアクティブ化」セクションを参照してください。

Fail-Close モードがアクティブになっているか確認するには、**show crypto map gdoi fail-close** コマンドを使用します。

フェールクローズ復帰

フェールクローズモードでは、フェールクローズモードで登録する前は、グループメンバーはそのローカル フェールクローズ ポリシーを適用し、それに応じてトラフィックを管理します。登録後は、グループメンバーはキーサーバーからダウンロードされたポリシーを適用し、それに応じてトラフィックを処理します。

キー再生成がない場合またはグループメンバーがキーサーバーに再登録できない場合、グループメンバーは、キーサーバーからダウンロードされた同じポリシーを使用します。暗号化または復号のためのキーがないため、パケットのドロップが発生します。フェールクローズ復帰により、グループメンバーは、フェールクローズモードに戻り、ダウンロードしたキーサーバー ポリシーを削除することができます。これは、グループメンバーでフェールクローズ復帰が有効になっている場合にのみ発生します。

このフェールクローズ復帰は、すべてのアクティブな SA が期限切れになり、再登録のために到達できるキーサーバーがない場合にトリガーされます。clear crypto sa コマンドを使用して IPsec SA を手動でクリアすると、機能の意図した動作が得られません。ただし、キーサーバーに到達できない場合、clear crypto gdoi コマンドを使用するとフェールクローズモードに戻ります。

この機能の設定手順については、「フェールクローズ復帰の設定」のセクションを参照してください。

GDOI 登録成功を追跡する MIB オブジェクトの作成

Null ルートを回避するため、GET VPN のルーティングプレーンと暗号プレーンは同期される必要があります。GET VPN Null ルートは、次の状況で発生します。

- アクティブな TEK がない KS に GM が登録できず、トラフィックを暗号化または復号化できない。
- GM TEK SA の期限が切れたがキー再生成または再登録によって KS から新しいキーを受け取っていない。

- GM は KS からキー再生成を受け取ったが、SA を暗号エンジンにインストールするときにエラーが発生する。

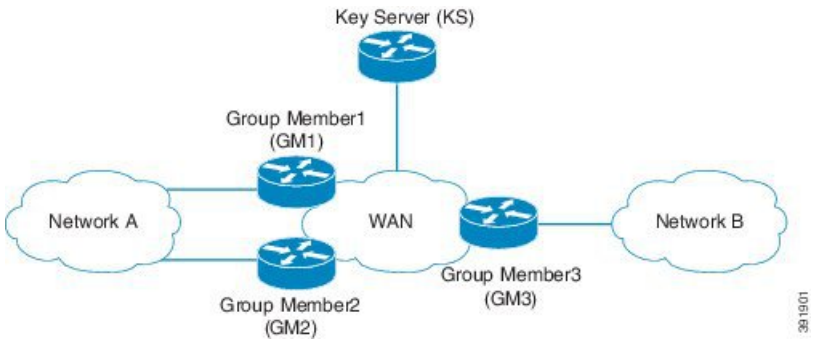
GDOI 登録成功を追跡する MIB オブジェクトの作成機能では、グループ内のアクティブな TEK 数を示すため、GDOI MIB に新しい MIB オブジェクトが導入されています。

BGP の GET VPN ルーティング認識

Null ルートを回避するため、GET VPN のルーティングプレーンと暗号プレーンは同期する必要があります。グループ メンバー（GM）がキー サーバ（KS）に正常に登録される場合、セキュリティ ポリシーまたはキーは GM にインストールされません。ただし、GM は他の GM に対して保護されたネットワークのルートをアドバタイズできます。

次の図は、Null ルートの生成について説明しています。

図 *124 : Null* ルートの生成



1. グループ メンバー 1、グループ メンバー 2、グループ メンバー 3 が起動し、WAN とルーティング アジャセンシー関係を確立します。
2. グループ メンバー 1 およびグループ メンバー 2 は、ネットワーク A のプレフィックスを WAN にアドバタイズします。ネットワーク B からネットワーク A へのトラフィックの優先パスは、グループ メンバー 1 経由です。
3. グループ メンバー 3 はネットワーク B を WAN にアドバタイズします。トラフィック ネットワーク A からネットワーク B への優先パスは、グループ メンバー 1 経由です。
4. KS は、ネットワーク A とネットワーク B の間のすべてのトラフィックを保護するためのセキュリティを定義します。
5. グループ メンバー 1 とグループ メンバー 3（およびグループ メンバー 2）は正常に KS からセキュリティ キーを取得し、ネットワーク A とネットワーク B 間のすべてのトラフィックを保護します。
6. グループ メンバー 2 およびグループ メンバー 3 が正常にキーを取得する一方、グループ メンバー 1 は更新されたキーまたはポリシーの受信に失敗し、KS への再登録に失敗します。
7. ルーティング プロトコルは、ネットワーク A とネットワーク B 間のすべてのトラフィックに対してグループ メンバー 1 経由のパスを優先し続けます。

8. グループ メンバー 1 は、ポリシーまたはキーが無効なため、ネットワーク A とネットワーク B の間に流れるトラフィックすべてをドロップします。

ネットワーク B のホストがネットワーク A のホストにトラフィックを送信する際、トラフィックはグループ メンバー 3 によって暗号化され、グループ メンバー 1 経由（優先パス）でネットワーク A に送信されます。ただし、グループ メンバー 1 はトラフィックを復号するためのポリシーまたは現在のキーを持たないため、パケットをドロップします。その結果、トラフィックはドロップされ、Null ルートが生成されます。同様に、ネットワーク A のホストがネットワーク B のホストにトラフィックを送信する際、トラフィックはグループ メンバー 1（優先パス）に転送され、グループ メンバー 1 にポリシーまたは現在のキーがないためにドロップされます。グループ メンバー 1 にポリシーまたはキーがない場合、適切な動作としてトラフィックはグループ メンバー 2 経由で転送および再ルーティングされます。

BGP の GET VPN ルーティング認識機能では、GETVPN GM の暗号化状態を追跡し、追跡情報を適用して GM で双方向条件付きルートフィルタリングを実行することにより、ルーティングが存在しない状態を回避します。

双方向条件付きルート フィルタリング

双方向条件付きルート フィルタリングでは、BGP、OSPF、EIGRP、RIPv2 などのさまざまなルーティング プロトコルをサポートしています。EOT は GET VPN GM 暗号化状態を追跡し、EOT 値に基づいて条件により特定のルートマップ エントリを有効または無効にします。次に、GET VPN GM 暗号化状態をモニタする設定例を示します。

```
route-map bgp-policy-out permit 10
 match ip address register-int-Only
route-map bgp-policy-out permit 20
 match track 99
 match ip address orig_route_map_acl_out
route-map bgp-policy-out deny 30

route-map bgp-policy-in permit 10
 match ip address noc
route-map bgp-policy-in permit 20
 match track 99
 match ip address orig_route_map_acl_in
route-map bgp-policy-in deny 30

ip access-list standard noc
 permit 1.1.1.0                                  <---- NOC subnet with Keyserver (KS)
ip access-list standard register-int-Only
 permit 2.2.2.2                                 <---- registration interface ip of the
 GM itself
ip access-list standard orig_route_map_acl_in      <---- original inbound route-map ACL

 permit a.b.c.d
 permit .......
ip access-list standard orig_route_map_acl_out     <---- original outbound route-map
ACL
 permit e.f.g.h
 permit .......

router bgp 64600
 no synchronization
 bgp router-id xxxxxxxx
 bgp log-neighbor-changes
 network xxxxxxxxxx mask 255.255.255.255
```

```
network xxxxxxxxxx mask 255.255.255.252
neighbor xxxxxxxxxx remote-as 65000
neighbor xxxxxxxxxx description PE
neighbor xxxxxxxxxx route-map bgp-policy-in in
neighbor xxxxxxxxxx route-map bgp-policy-out out
```

上記の例では、GET VPN GM 暗号化状態をモニタするために **match track 99** コマンドが指定されています。GM が適切に機能する場合、**match track 99** コマンドは値 *true* を返し、GM は次のルートをアドバタイズまたは受信します。

- 発信：GM 登録インターフェイスに到達するルート、および着信ルートマップのアクセスコントロール リスト（ACL）「orig_route_map_acl_out」によって許可されたルート。
- 着信：NOC に到達するルート、およびルーティングは、ピアから受信した発信ルートマップ ACL「orig_route_map_acl_in」によって許可されたルート。

一方、GM が正しく機能しない場合、**match track 99** コマンドは値 *false* を返し、GM は次のルートのみをアドバタイズまたは受信します。

- 発信：GM 登録インターフェイスに到達するルート。
- 着信：NOC サブネットに到達するルート。

Cisco Group Encrypted Transport VPN システム ロギング メッセージ

次の表に、GET VPN システム ロギング（syslog とも呼ばれます）メッセージと説明を示します。

表 *288 : GET VPN* システム ロギング メッセージ

メッセージ	説明
COOP_CONFIG_MISMATCH	プライマリ KS とセカンダリ KS 間の設定が一致しません。
COOP_KS_ADD	グループ内の連携 KS のリストに KS が追加されました。
COOP_KS_ELECTION	ローカル KS によってグループ内の選択プロセスが開始されました。
COOP_KS_REACH	設定済み連携 KS 間の到達可能性は回復しています。
COOP_KS_REMOVE	グループ内の連携 KS のリストから KS が削除されました。
COOP_KS_TRANS_TO_PRI	ローカル KS が、グループ内のセカンダリ サーバからプライマリ ロールに移行しました。

メッセージ	説明
COOP_KS_UNAUTH	認証されていないリモートサーバーによって、グループ内のローカル KS へのアクセスが試行されました。敵対的なイベントの可能性があります。
COOP_KS_UNREACH	設定済み連携 KS 間の到達可能性が失われています。敵対的なイベントの可能性があります。
COOP_KS_VER_MISMATCH	各 KS が、異なるバージョンの Cisco IOS コードを実行しています。
COOP_PACKET_DROPPED	ドライババッファ サイズに設定されたハード制限によって、このサイズ以上のパケットの送信はできません。
GDOI-3-GDOI_REKEY_SEQ_FAILURE	シーケンス番号のアンチ リプレイ チェックが失敗したため、キー再生成メッセージが拒否されています。
GDOI-3-GM_NO_CRYPTO_ENGINE	リソースが不足しているかサポートされていない機能が要求されたために暗号化エンジンが検出できません。
GDOI-3-PSEUDO_TIME_LARGE	キー再生成に、計算された許容される疑似時間の差を超える大きな疑似時間があります。
GDOI-3-PSEUDO_TIME_TOO_OLD	キー再生成に、計算された許容される疑似時間の差を超える小さな疑似時間があります。
GDOI-4-GDOI_ANN_TIMESTAMP_ LARGE	セカンダリ KS が、プライマリ KS から計算された許容される疑似時間の差を超える大きな疑似時間がある ANN を受信しています。
GDOI-4-GDOI_ANN_TIMESTAMP_ TOO_OLD	セカンダリ KS が、プライマリ KS から計算された許容される疑似時間の差を超える小さな疑似時間がある ANN を受信しています。
GDOI-5-COOP_KS_BLOCK_NEW_GM_REGISTER	セカンダリ KS がプライマリ KS から有効な疑似時間を受信していないため、GM のグループへの登録を一時的にブロックしています。

メッセージ	説明
GDOI-5-COOP_KS_VALID_ANN_ TIMER_EXPIRED	セカンダリ KS が 3 つの再送信後に無効な疑似時間のある ANN を受信し続けています。セカンダリ KS は有効な ANN が受信されるまで一時的に新しいグループ メンバー登録をブロックします。
GDOI_ACL_NUM	ACL のエントリが多すぎます。GDOI は、指定された最初の 100 個の ACL エントリだけを受け入れます。
GDOI_REKEY_FAILURE	GDOI キー再生成中に、KS からのペイロード構文解析が、この GM 上で失敗しました。
GM_ACL_MERGE	GM と KS 間における ACL の違いは解決され、結合が実行されました。
GM_ACL_PERMIT	GM は「拒否」の ACL のみをサポートできます。「許可」エントリと一致するすべてのトラフィックがドロップされます。
GM_CLEAR_REGISTER	ローカル GM によって、**clear crypto gdoi** コマンドが実行されました。
GM_CM_ATTACH	このローカル GM 用の暗号マップが追加されました。
GM_CM_DETACH	このローカル GM 用の暗号マップが削除されました。
GM_CONV_SA_DUPLEX	IPsec SA が、GM 上のグループ内で双方向モードに変換されました。
GM_CONV_SA_DUPLEX_LOCAL	CLI コマンドによって、GM 上のグループ内で、IPsec SA が双方向モードに変換されました。
GM_DELETE	グループ内の GM が KS から削除されました。
GM_ENABLE_GDOI_CM	GM に、KS を持つグループ内の GDOI 暗号マップ上のイネーブルにされた ACL があります。
GM_HASH_FAIL	GDOI 登録プロトコル中に KS によって送信されたメッセージに不具合があるか、ハッシュがありません。

メッセージ	説明
GM_INCOMPLETE_CFG	GDOI グループ設定で、グループ ID、サーバID、またはその両方が見つからないために、登録が完了できません。
GM_NO_IPSEC_FLOWS	IPsec フロー 制限に関するハードウェアの制限に達しました。IPsec SA をこれ以上作成できません。
GM_RE_REGISTER	あるグループのために作成された IPsec SA が期限切れか、消去された可能性があります。KS に再登録する必要があります。
GM_RECV_DELETE	GM を削除するために KS によって送信されたメッセージを受信しました。
GM_RECV_REKEY	キー再生成を受信しました。
GM_REGS_COMPL	Registration complete.
GM_REJECTING_SA_PAYLOAD	GDOI 登録プロトコル中に、KS によって送信された提案が、ローカル GM によって拒否されました。
GM_REKEY_NOT_RECD	GMによって、グループ内のKSからのキー再生成メッセージが受信されませんでした。現在実装されていません。
GM_REKEY_TRANS_2_MULTI	GM が、ユニキャスト キー再生成メカニズムの使用から、マルチキャスト メカニズムの使用へと移行しました。
GM_REKEY_TRANS_2_UNI	GM が、マルチキャスト キー再生成メカニズムの使用から、ユニキャスト メカニズムの使用へと移行しました。
GM_SA_INGRESS	グループ内の KS からの受信専用 ACL が、GM によって受信されました。
GM_UNREGISTER	GM がグループから去りました。
KS_BAD_ID	GDOI 登録プロトコル中に、ローカル KS と GM との間で設定の不一致が発生しました。
KS_BLACKHOLE_ACK	KS が、GM からの Null ルートメッセージの状態になりました。敵対的なイベントの可能性があります。

メッセージ	説明
KS_CLEAR_REGISTER	ローカル KS によって、**clear crypto gdoi** コマンドが実行されました。
KS_CONV_SAS_DUPLEX	IPsec SA が、グループ内で双方向モードに変換されました。
KS_CONV_SAS_INGRESS	IPsec SA が、グループ内で受信専用モードに変換されました。
KS_FIRST_GM, GDOI, LOG_INFO	ローカル KS がグループに参加している最初の GM を受信しました。
KS_GM_REJECTS_SA_PAYLOAD	GDOI 登録プロトコル中に、KS によって送信された提案が、GM によって拒否されました。
KS_GM_REVOKED	キー再生成プロトコル中に、認証されていないメンバーによるグループへの加入が試行されました。敵対的なイベントの可能性があります。
KS_GROUP_ADD	コンフィギュレーション コマンドが実行され、グループ内に KS が追加されました。
KS_GROUP_DELETE	コンフィギュレーション コマンドが実行され、グループから KS が削除されました。
KS_HASH_FAIL	GDOI 登録プロトコル中に GM によって送信されたメッセージに不具合があるか、ハッシュがありません。
KS_LAST_GM	最後の GM がローカル KS でグループを去りました。
KS_NACK_GM_EJECT	KS が、GM からの ACK メッセージを受信しない状態になり、イジェクトされました。
KS_NO_RSA_KEYS	RSA キーが作成されなかったか、失われています。
KS_REGS_COMPL	KS による、グループ内における登録が正常終了しました。
KS_REKEY_TRANS_2_MULTI	グループが、ユニキャスト キー再生成メカニズムの使用から、マルチキャスト メカニズムへと移行しました。

メッセージ	説明
KS_REKEY_TRANS_2_UNI	グループが、マルチキャスト キー再生成メカニズムの使用から、ユニキャスト メカニズムの使用へと移行しました。
KS_SEND_MCAST_REKEY	マルチキャスト キー再生成を送信中です。
KS_SEND_UNICAST_REKEY	ユニキャスト キー再生成を送信中です。
KS_UNAUTHORIZED	GDOI 登録プロトコル中に、認証されていないメンバーによるグループへの加入が試行されました。敵対的なイベントの可能性があります。
KS_UNSOL_ACK	KS によって、過去の GM からの非送信請求 ACK メッセージが受信されたか、DoS 攻撃を受けています。敵対的なイベントの可能性があります。
PSEUDO_TIME_LARGE	GM によって、その GM の疑似時間とは大きく異なる値を持つ疑似時間が受信されました。
REPLAY_FAILED	GM または KS のアンチ リプレイ チェックが失敗しました。
UNAUTHORIZED_IDENTITY	登録要求が、要求を行っているデバイスがグループの参加を許可されなかったために廃棄されました。
UNAUTHORIZED_IPADDR	登録要求が、要求を行っているデバイスがグループの参加を許可されなかったために廃棄されました。
UNEXPECTED_SIGKEY	予期しないシグニチャ キーが検出されました。このシグニチャ キーを解除します。
UNREGISTERED_INTERFACE	未登録のインターフェイスからの登録を受信中です。処理を停止してください。
UNSUPPORTED_TEK_PROTO	予期しない TEK プロトコルです。

Cisco Group Encrypted Transport VPN の設定方法

キー サーバの設定

前提条件

GDOI グループを作成する前に、最初に IKE および IPsec トランスフォーム セットを設定してから、IPsec プロファイルを作成する必要があります。IKE と IPsec トランスフォーム セットの設定方法、および IPsec プロファイルの作成方法については、「その他の関連資料」セクションの「関連資料」の項を参照してください。

キー再生成メッセージに署名するための RSA キーの設定

（注） セキュリティに対する脅威は、脅威からの保護に役立つ暗号化技術と同様に絶え間なく変化しています。最新のシスコの暗号化に関する推奨事項については、『Next Generation Encryption（NGE）ホワイト ペーパー』を参照してください。

キー再生成メッセージに署名するために使用される RSA キーを設定するには、次の手順を実行します。キー再生成が使用中でない場合、このサブ作業はスキップしてください。

手順の概要

1. **enable**
2. **configure terminal**
3. **crypto key generate rsa general-keys label** *name-of-key*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**crypto key generate rsa general-keys label** *name-of-key* 例：	キー再生成メッセージに署名するために使用される RSA キーを生成します。生成されるキーの長さ（ビット単位）を確認するプロンプトが表示されま

	コマンドまたはアクション	目的
	`Router(config)# crypto key generate rsa general-keys label mykeys`	す。2048 未満の長さを指定することは推奨されません。

次の作業

グループ ID、サーバ タイプ、および SA タイプを設定します（「グループ ID、サーバ タイプ、および SA タイプの設定」セクションを参照してください）。

グループ ID、サーバ タイプ、および SA タイプの設定

サイトが大量にある場合、特にあるサイトが Dual Multipoint VPN（DMVPN）のような他の暗号化ソリューションから移行する場合は、予防措置を取り、段階的に機能を追加する必要があります。たとえば、すべての CPE デバイスを、トラフィックが双方向で暗号化されるように設定するのではなく、1 つまたは少数のグループだけが暗号化されたトラフィックの送信を許可されるように、一方向の暗号化を設定することが可能です。その他のデバイスは暗号化されたトラフィックだけを受信することが許可されます。1 つまたは少数のメンバーに関する一方向の暗号化の検証が終わったら、すべてのメンバーに対して双方向の暗号化をオンにできます。この「着信専用」トラフィックは、暗号グループ下で **sa receive only** コマンドを使用して制御可能です。

グループ ID、サーバ タイプ、および SA タイプを設定するには、次の手順を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **crypto gdoi group** *group-name*
4. 次のいずれかのコマンドを入力します。
   - **identity number** *number*
   - **identity address ipv4** *address*
5. **server local**
6. **sa receive-only**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例：	グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
	`Router# configure terminal`	
ステップ 3	**crypto gdoi group** *group-name* 例： `Router(config)# crypto gdoi group gdoigroupname`	GDOI グループを指定し、GDOI グループ コンフィギュレーション モードを開始します。

ステップ 4	次のいずれかのコマンドを入力します。
	• **identity number** *number*
	• **identity address ipv4** *address*
	例：
	`Router(config-gdoi-group)# identity number 3333`
	例：
	`Router(config-gdoi-group)# identity address ipv4 209.165.200.225`
		GDOI グループ番号またはアドレスを指定します。

ステップ 5	**server local** 例： `Router(config-gdoi-group)# server local`	デバイスを GDOI キー サーバとして指定し、GDOI ローカル サーバ コンフィギュレーション モードを開始します。
ステップ 6	**sa receive-only** 例： `Router(config-local-server)# sa receive-only`	IPsec SA がグループ メンバーによって「着信専用」としてインストールされるように指定します。

次の作業

グループ メンバーが双方向の受信および送信モードで動作するように、キー サーバ上の受信専用設定を削除します。

キー再生成の設定

ここでは、次のオプションの作業について説明します。

キー再生成は、グループのポリシーと IPsec SA を定期的に更新するために、キー サーバによってコントロール プレーンで使用されます。グループ メンバー側では、他の何らかの理由によりタイマーが満了するときに完全に登録するのではないので、キー再生成への登録の更新がより効率的になります。最初の登録は常にユニキャスト登録です。

キー サーバは、ユニキャストまたはマルチキャスト モードでキー再生成を送信するように設定できます。キー再生成の転送モードは、キー サーバによって IP マルチキャストが使用されてキー再生成が配信できるかどうかによって決まります。マルチキャスト機能がカスタマーの

ネットワーク内に存在しない場合、キー サーバを、ユニキャスト メッセージを使用してキー再生成を送信するように設定する必要があります。

キー再生成の追加オプションでは、**rekey authentication**、**rekey retransmit**、および **rekey address ipv4** コマンドを使用します。ユニキャスト転送モードが設定されている場合、このユニキャストキー再生成メッセージの送信元アドレスが指定されるように **source address** コマンドを指定する必要があります。

マルチキャストは、キー再生成メッセージのデフォルトの転送タイプです。次の箇条書きでは、キー再生成転送タイプにどのような場合にマルチキャストにするか、あるいはユニキャストにするかを説明します。

- グループ内のすべてのメンバーがマルチキャストに対応している場合は、**rekey transport unicast** コマンドを設定しません。マルチキャストキー再生成はデフォルトでオンになっているので、このグループ下でキー再生成転送タイプ「ユニキャスト」が過去に設定されていない場合、**no rekey transport unicast** コマンドは必要ありません。
- グループ内のすべてのメンバーがユニキャストである場合、**rekey transport unicast** コマンドを使用します。
- グループ内に混合されたメンバーがある場合（つまり、大多数がマルチキャストで、少数がユニキャスト）、**rekey transport unicast** コマンドは設定しません。キー再生成は、グループ メンバーの大多数に対して、マルチキャストで配信されます。マルチキャスト メッセージを受信しない残りのグループ メンバー（ユニキャスト グループ メンバー）は、そのポリシーが期限切れになった時にキー サーバに再登録する必要があります。混合モード（つまり、ユニキャストとマルチキャスト キー再生成モード）は現在サポートされていません。

no rekey transport unicast コマンドが使用されている場合、マルチキャストキー再生成メッセージを受信できないGDOIグループ内のメンバーを、最新のグループポリシーを取得するようにキーサーバーに再登録する必要があります。再登録すると、デフォルトの転送タイプが強制的にマルチキャストになります。過去に転送タイプが設定されていない場合、マルチキャスト転送タイプがデフォルトで適用されます。

前提条件

rekey authentication コマンドを設定する前に、**crypto key generate rsa** コマンドおよび **general-keys** キーワードと **label** キーワードを使用して RSA キーが生成されるようにルータを設定しておく必要があります（例：「crypto key generate rsa general-key label my keys」）。

ユニキャスト キー再生成の設定

次の設定作業表では、アドレス「ipv4 10.0.5.2」は、ユニキャストまたはマルチキャスト キー再生成メッセージを送信するキー サーバ上のインターフェイスを示しています。このアドレスは、ユニキャスト キー再生成では必須ですが、マルチキャスト キー再生成では任意です。マルチキャスト キー再生成の場合、キー サーバの送信元アドレスを、キー再生成 ACL から取得できます。

ユニキャスト キー再生成を設定するには、次の手順を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **crypto gdoi group** *group-name*
4. 次のいずれかのコマンドを入力します。
   - **identity number** *number*
   - **identity address ipv4** *address*
5. **server local**
6. **rekey transport unicast**
7. **rekey lifetime seconds** *number-of-seconds*
8. **rekey retransmit** *number-of-seconds* **number** *number-of-retransmissions*
9. **rekey authentication mypubkey rsa** *key-name*
10. **address ipv4** *ipv4-address*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**crypto gdoi group** *group-name* 例： `Router(config)# crypto gdoi group gdoigroupname`	GDOI グループを指定し、GDOI グループ コンフィギュレーション モードを開始します。

ステップ 4	次のいずれかのコマンドを入力します。
	• **identity number** *number*
	• **identity address ipv4** *address*
	例：
	`Router(config-gdoi-group)# identity number 3333`
	例：
	`Router(config-gdoi-group)# identity address ipv4 209.165.200.225`
		GDOI グループ番号またはアドレスを指定します。

	コマンドまたはアクション	目的
ステップ 5	**server local** 例： `Router(config-gdoi-group)# server local`	デバイスを GDOI キー サーバとして指定し、GDOI ローカル サーバ コンフィギュレーション モードを開始します。
ステップ 6	**rekey transport unicast** 例： `Router(config-local-server)# rekey transport unicast`	グループ メンバーに対するキー再生成メッセージのユニキャスト配信を設定します。
ステップ 7	**rekey lifetime seconds** *number-of-seconds* 例： `Router(gdoi-local-server)# rekey lifetime seconds 300`	（任意）任意の暗号キーが使用される秒数を制限します。 • このコマンドが設定されていない場合、デフォルト値の 86,400 秒が有効になります。
ステップ 8	**rekey retransmit** *number-of-seconds* **number** *number-of-retransmissions* 例： `Router(gdoi-local-server)# rekey retransmit 10 number 3`	（任意）キー再生成メッセージが再送信される回数を指定します。 • このコマンドが設定されていない場合、再送信は行われません。
ステップ 9	**rekey authentication mypubkey rsa** *key-name* 例： `Router(gdoi-local-server)# rekey authentication mypubkey rsa mykeys`	（任意）GDOI グループ メンバーに対するキー再生成に使用されるキーを指定します。 • キー再生成が不要な場合、このコマンドは任意です。キー再生成が必須の場合、このコマンドは必須です。
ステップ 10	**address ipv4** *ipv4-address* 例： `Router(gdoi-local-server)# address ipv4 209.165.200.225`	（任意）ユニキャスト キー再生成メッセージの送信元情報を指定します。 • キー再生成が不要な場合、このコマンドは任意です。キー再生成が必須の場合、このコマンドは必須です。

マルチキャスト キー再生成の設定

マルチキャスト キー再生成を設定するには、次の手順を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **crypto gdoi group** *group-name*

4. 次のいずれかのコマンドを入力します。
   - **identity number** *number*
   - **identity address ipv4** *address*
5. **server local**
6. **rekey address ipv4** {*access-list-name* | *access-list-number*}
7. **rekey lifetime seconds** *number-of-seconds*
8. **rekey retransmit** *number-of-seconds* **number** *number-of-retransmissions*
9. **rekey authentication** {**mypubkey** | **pubkey**} **rsa** *key-name*
10. **exit**
11. **exit**
12. **access-list** *access-list-number* {**deny** | **permit**} **udp host** *source* [*operator*[*port*]] **host** *source* [*operator*[*port*]]
13. **interface** *type slot/ port*
14. **ip igmp join-group** *group-address* [**source** *source-address*]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**crypto gdoi group** *group-name* 例： `Router(config)# crypto gdoi group gdoigroupname`	GDOI グループを指定し、GDOI グループ コンフィギュレーション モードを開始します。

ステップ 4	次のいずれかのコマンドを入力します。
	• **identity number** *number*
	• **identity address ipv4** *address*
	例：
	`Router(config-gdoi-group)# identity number 3333`
	例：
	`Router(config-gdoi-group)# identity address ipv4 209.165.200.225`
		GDOI グループ番号またはアドレスを指定します。

	コマンドまたはアクション	目的
ステップ 5	**server local** 例： `Router(config-gdoi-group)# server local`	デバイスを GDOI キー サーバとして指定し、GDOI ローカル サーバ コンフィギュレーション モードを開始します。
ステップ 6	**rekey address ipv4** {*access-list-name* | *access-list-number*} 例： `Router(gdoi-local-server)# rekey address ipv4 121`	登録するマルチキャスト サブアドレス範囲グループ メンバーを定義します。
ステップ 7	**rekey lifetime seconds** *number-of-seconds* 例： `Router(gdoi-local-server)# rekey lifetime seconds 300`	（任意）任意の暗号キーが使用される秒数を制限します。 • このコマンドが設定されていない場合、デフォルト値の 86,400 秒が有効になります。
ステップ 8	**rekey retransmit** *number-of-seconds* **number** *number-of-retransmissions* 例： `Router(gdoi-local-server)# rekey retransmit 10 number 3`	（任意）キー再生成メッセージが再送信される回数を指定します。 • このコマンドが設定されていない場合、再送信は行われません。
ステップ 9	**rekey authentication** {**mypubkey** | **pubkey**} **rsa** *key-name* 例： `Router(gdoi-local-server)# rekey authentication mypubkey rsa mykeys`	（任意）GDOI グループ メンバーに対するキー再生成に使用されるキーを指定します。 • キー再生成が不要な場合、このコマンドは任意です。キー再生成が必須の場合、このコマンドは必須です。
ステップ 10	**exit** 例： `Router(gdoi-local-server)# exit`	GDOI サーバ ローカル コンフィギュレーション モードを終了します。
ステップ 11	**exit** 例： `Router(config-gdoi-group)# exit`	GDOI グループ コンフィギュレーション モードを終了します。
ステップ 12	**access-list** *access-list-number* {**deny** | **permit**} **udp** **host** *source* [*operator*[*port*]] **host** *source* [*operator*[*port*]] 例：	拡張 IP アクセス リストを定義します。

	コマンドまたはアクション	目的
	`Router(config)# access-list 121 permit udp host 10.0.5.2 eq 848 host 239.0.1.2 eq 848`	
ステップ 13	**interface** *type slot/ port* 例： `Router(config)# interface gigabitethernet 0/0`	インターフェイス タイプを設定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 14	**ip igmp join-group** *group-address* [**source** *source-address*] 例： `Router(config-if)# ip igmp join-group 232.2.2.2 source 10.1.1.1`	指定したグループまたはチャネルに参加するようにルータのインターフェイスを設定します。 （注） 暗号マップが設定されているものと同じインターフェイスでキー サーバに到達できない場合に手動でストリームに参加するには、このコマンドを使用します。

グループ メンバー ACL の設定

deny エントリに一致するすべての IP トラフィックは、グループ メンバーによって、暗号化されていないテキストで送信されます。着信トラフィックは、ミラー アクセス リストに対応付けられます。

（注） グループ メンバー ACL にエントリを追加または削除するために推奨の方法として、最初に既存のグループ メンバー ACL のコピーを異なる名前で作成してから、この新しい ACL のエントリに追加または削除します。その後 GDOI 暗号マップ下の既存のグループ メンバー ACL を新しく作成したグループ メンバー ACL で置き換える必要があります。この推奨の方法に従わない場合、予期しない動作が発生する可能性があります。

グループ メンバー ACL を設定するには、このタスクを実行します（グループ メンバーのアクセス リストに拒否ステートメントが含まれている場合があることに注意してください）。

手順の概要

1. **enable**
2. **configure terminal**
3. **access-list** *access-list-number* **deny ip host** *source* **host** *source*
4. **access-list** *access-list-number* **permit ip** *source*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**access-list** *access-list-number* **deny ip host** *source* **host** *source* 例： `Router(config)# access-list 101 deny ip host 10.0.0.1 host 10.0.0.2`	拒否される IP アクセス リストを定義します。
ステップ 4	**access-list** *access-list-number* **permit ip** *source* 例： `Router(config)# access-list 103 permit ip 209.165.200.225 0.255.255.255 10.20.0.0 0.255.255.255`	許可される IP アクセス リストを定義します。

次の作業

手順4で定義したアクセス リストは、SAの設定に使用する必要があるものと同じです。「IPsec SA の設定」のセクションを参照してください。

IPsec ライフタイム タイマーの設定

プロファイルのIPsec ライフタイム タイマーを設定するには、次の手順を実行します。この設定作業を実行しない場合、デフォルトは最大IPsec SA ライフタイムの3600秒になります。TEK ライフタイム値は 900 秒を超える値にする必要があります。

手順の概要

1. **enable**
2. **configure terminal**
3. **crypto ipsec profile** *name*
4. **set security-association lifetime seconds** *seconds*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**crypto ipsec profile** *name* 例： `Router(config)# crypto ipsec profile profile1`	2 つの IPsec ルータ間における IPsec 暗号化で使用される IPsec パラメータを定義し、暗号化 IPsec プロファイル コンフィギュレーション モードを開始します。
ステップ 4	**set security-association lifetime seconds** *seconds* 例： `Router(ipsec-profile)# set security-association lifetime seconds 2700`	IPsec SA をネゴシエーションするときに使用されるグローバル ライフタイム値を上書きします（特定のクリプト マップ エントリの場合）。

次の作業

IPsec SA を設定します。「IPsec SA の設定」のセクションを参照してください。

ISAKMP ライフタイム タイマーの設定

ISAKMP ライフタイム タイマーを設定するには、次の手順を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **crypto isakmp policy** *priority*
4. **lifetime** *seconds*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。

	コマンドまたはアクション	目的
ステップ 2	**configure terminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**crypto isakmp policy** *priority* 例： `Router(config)# crypto isakmp policy 1`	IKE ポリシーを定義し、ISAKMP ポリシー コンフィギュレーション モードを開始します。
ステップ 4	**lifetime** *seconds* 例： `Router(config-isakmp-policy)# lifetime 86400`	IKE SA のライフタイムを指定します。

IPsec SA の設定

時間ベースのアンチ リプレイがキー サーバ上で設定されているが、それに対応する機能がグループ メンバーにない場合、GDOI-3-GM_NO_CRYPTO_ENGINE syslog メッセージがグループ メンバーに記録されます。システム エラー メッセージの一覧については、「Cisco Group Encrypted Transport VPN システム ロギング メッセージ」セクションを参照してください。

（注） セキュリティに対する脅威は、脅威からの保護に役立つ暗号化技術と同様に絶え間なく変化しています。最新のシスコの暗号化に関する推奨事項については、『Next Generation Encryption（NGE）ホワイト ペーパー』を参照してください。

IPsec SA を設定するには、次の手順を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **crypto ipsec transform-set** *transform-set-name transform* [*transform2...transform4*]
4. **crypto ipsec profile** *ipsec-profile-name*
5. **set transform-set** *transform-set-name*
6. **exit**
7. **crypto gdoi group** *group-name*
8. 次のいずれかのコマンドを入力します。
   - **identity number** *number*
   - **identity address ipv4** *address*
9. **server local**
10. **sa ipsec** *sequence-number*

11. **profile** *ipsec-profile-name*
12. **match address ipv4** {*access-list-number* | *access-list-name*}
13. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**crypto ipsec transform-set** *transform-set-name transform* [*transform2...transform4*] 例： `Router(config)# crypto ipsec transform-set gdoi-trans esp-aes esp-sha-hmac`	トランスフォーム セット（セキュリティ プロトコルとセキュリティ アルゴリズムの受け入れ可能な組み合わせ）を定義します。
ステップ 4	**crypto ipsec profile** *ipsec-profile-name* 例： `Router(config)# crypto ipsec profile profile1`	IPsec プロファイルを定義し、暗号 ipsec プロファイル コンフィギュレーション モードを開始します。
ステップ 5	**set transform-set** *transform-set-name* 例： `Router(ipsec-profile)# set transform-set transformset1`	クリプト マップ エントリで使用可能なトランスフォーム セットを指定します。
ステップ 6	**exit** 例： `Router(ipsec-profile)# exit`	IPSec プロファイル コンフィギュレーション モードを終了します。
ステップ 7	**crypto gdoi group** *group-name* 例： `Router(config)# crypto gdoi group gdoigroupname`	GDOI グループを指定し、GDOI グループ コンフィギュレーション モードを開始します。
ステップ 8	次のいずれかのコマンドを入力します。 • **identity number** *number*	GDOI グループ番号またはアドレスを指定します。

	コマンドまたはアクション	目的

	• **identity address ipv4** *address*
	例：
	`Router(config-gdoi-group)# identity number 3333`
	例：
	`Router(config-gdoi-group)# identity address ipv4 209.165.200.225`	

ステップ 9	**server local** 例： `Router(config-gdoi-group)# server local`	デバイスを GDOI キー サーバとして指定し、GDOI ローカル サーバ コンフィギュレーション モードを開始します。
ステップ 10	**sa ipsec** *sequence-number* 例： `Router(gdoi-local-server)# sa ipsec 1`	GDOI グループに使用される IPsec SA ポリシー情報を指定し、GDOI SA IPsec コンフィギュレーション モードを開始する。
ステップ 11	**profile** *ipsec-profile-name* 例： `Router(gdoi-sa-ipsec)# profile gdoi-p`	GDOI グループ用の IPsec SA ポリシーを定義します。
ステップ 12	**match address ipv4** {*access-list-number* | *access-list-name*} 例： `Router(gdoi-sa-ipsec)# match address ipv4 102`	GDOI 登録の IP 拡張アクセス リストを指定します。
ステップ 13	**end** 例： `Router(gdoi-sa-ipsec)# end`	GDOI SA IPsec コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

次の作業

リプレイを設定する必要があります。リプレイを設定しない場合、デフォルトはカウンタ モードになります。

GDOI グループ用の時間ベースのアンチリプレイの設定

GDOI グループ用の時間ベースのアンチ リプレイを設定するには、次の手順を実行します。

手順の概要

1. **enable**

2. **configure terminal**
3. **crypto gdoi group** *group-name*
4. **identity number** *policy-name*
5. **server local**
6. **address** *ip-address*
7. **sa ipsec** *sequence-number*
8. **profile** *ipsec-profile-name*
9. **match address** {**ipv4** *access-list-number* | *access-list-name*}
10. **replay counter window-size** *seconds*
11. **replay time window-size** *seconds*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**crypto gdoi group** *group-name* 例： `Router(config)# crypto gdoi group gdoigroup1`	GDOI グループを指定し、GDOI グループ コンフィギュレーション モードを開始します。
ステップ 4	**identity number** *policy-name* 例： `Router(config-gdoi-group)# identity number 1234`	GDOI グループ番号を指定します。
ステップ 5	**server local** 例： `Router(config-gdoi-group)# server local`	デバイスを GDOI キー サーバとして指定し、GDOI ローカル サーバ コンフィギュレーション モードを開始します。
ステップ 6	**address** *ip-address* 例： `Router(config-server-local)# address 209.165.200.225`	送信元アドレスを設定します。このアドレスは、ローカル キー サーバによって送信されるパケットの送信元として使用されます。
ステップ 7	**sa ipsec** *sequence-number* 例：	IPsec SA を指定し、GDOI SA IPsec コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
	`Router(config-server-local)# sa ipsec 1`	
ステップ 8	**profile** *ipsec-profile-name* 例： `Router(gdoi-sa-ipsec)# profile test1`	GDOI グループ用の IPsec SA ポリシーを定義します。
ステップ 9	**match address** {**ipv4** *access-list-number* | *access-list-name*} 例： `Router(gdoi-sa-ipsec)# match address ipv4 101`	GDOI 登録の IP 拡張アクセス リストを指定します。
ステップ 10	**replay counter window-size** *seconds* 例： `Router(gdoi-sa-ipsec)# replay counter window-size 512`	1 つのグループ内に 2 つのグループ メンバーだけが存在している場合、GDOI を使用して、アクセス リスト内に定義されたトラフィックのカウンタ ベースのアンチ リプレイ保護をオンにします。 （注） このコマンドによる動作と **replay time window-size** コマンドによる動作は、相互に排他的な関係にあります。設定できるのはどちらか一方だけです。
ステップ 11	**replay time window-size** *seconds* 例： `Router(gdoi-sa-ipsec)# replay time window-size 1`	1 つのグループ内に 3 つ以上のグループ メンバーが存在している場合、GDOI を使用して、アンチリプレイ保護のウィンドウ サイズを設定します。 （注） このコマンドによる動作と **replay counter window-size** コマンドによる動作は、相互に排他的な関係にあります。設定できるのはどちらか一方だけです。

パッシブ SA の設定

（グループ メンバーを passive モードにするために）パッシブ SA を設定するには、次の手順を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **crypto gdoi group** *group-name*
4. **identity** *name*
5. **passive**
6. **server address ipv4** {*address* | *hostname*}

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**crypto gdoi group** *group-name* 例： `Router(config)# crypto gdoi group group1`	GDOI グループを指定し、GDOI グループ コンフィギュレーション モードを開始します。
ステップ 4	**identity** *name* 例： `Router(config-gdoi-group)# identity 2345`	クリプト マップに対して ID を設定します。
ステップ 5	**passive** 例： `Router(config-gdoi-group)# passive`	グループ メンバーを passive モードにします。
ステップ 6	**server address ipv4** {*address* | *hostname*} 例： `Router(config-gdoi-group)# server address ipv4 209.165.200.225`	GDOI グループが到達しようとするサーバのアドレスを指定します。

キー サーバのロールのリセット

プライマリ サーバの連係可能なロールをリセットするには、次の手順を実行します。

手順の概要

1. **enable**
2. **clear crypto gdoi ks coop role**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**clear crypto gdoi ks coop role** 例： `Router# clear crypto gdoi ks coop role`	キー サーバの連携ロールをリセットします。

グループ メンバーの設定

グループ メンバーを設定するには、次のサブ作業を実行します。

グループ名、ID、キー サーバ IP アドレス、およびグループ メンバー登録の設定

グループ名、ID、キー サーバ IP アドレス、およびグループ メンバー登録を設定するには、次の手順を実行します。キー サーバ アドレスは 8 個まで設定できます。

手順の概要

1. **enable**
2. **configure terminal**
3. **crypto gdoi group** *group-name*
4. 次のいずれかを実行します。
   - **identity number** *number*
   - **identity address ipv4** *address*
5. **server address ipv4** *address*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 3	**crypto gdoi group** *group-name* 例： `Router(config)# crypto gdoi group gdoigroupone`	GDOI グループを指定し、GDOI グループ コンフィギュレーション モードを開始します。

ステップ 4	次のいずれかを実行します。
	• **identity number** *number*
	• **identity address ipv4** *address*
	例：
	`Router(config-gdoi-group)# identity number 3333`
	例：
	`Router(config-gdoi-group)# identity address ipv4 209.165.200.225`
		GDOI グループ番号またはアドレスを指定します。

ステップ 5	**server address ipv4** *address* 例： `Router(config-gdoi-group)# server address ipv4 209.165.200.225`	GDOI グループが到達しようとするサーバのアドレスを指定します。 • アドレスを無効にするには、このコマンドの **no** 形式を使用します。

次の作業

クリプト マップを設定します。「暗号マップ エントリの作成」セクションを参照してください。

暗号マップ エントリの作成

クリプト マップ エントリを作成し、それに GDOI グループを関連付けるには、次の手順を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **crypto map** *map-name seq-num* **gdoi**
4. **set group** *group-name*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例：	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。

	コマンドまたはアクション	目的
	`Router> enable`	
ステップ 2	**configure terminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**crypto map** *map-name seq-num* **gdoi** 例： `Router(config)# crypto map mymap 10 gdoi`	クリプト マップ コンフィギュレーション モードを開始して、クリプト マップ エントリを作成または変更します。
ステップ 4	**set group** *group-name* 例： `Router(config-crypto-map)# set group group1`	GDOI グループをクリプト マップに関連付けます。

次の作業

トラフィックを暗号化する必要があるインターフェイスにクリプトマップを適用します。「トラフィックを暗号化する必要があるインターフェイスへの暗号マップの適用」セクションを参照してください。

トラフィックを暗号化する必要があるインターフェイスへの暗号マップの適用

トラフィックを暗号化する必要があるインターフェイスに暗号マップを適用するには、次の手順を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **interface** *type slot* / *port*
4. **crypto map** *map-name* **redundancy** *standby-group-name* **stateful**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例：	グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
	`Router# configure terminal`	
ステップ 3	**interface** *type slot* / *port* 例： `Router(config)# interface gigabitethernet 0/0`	インターフェイスタイプを設定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	**crypto map** *map-name* **redundancy** *standby-group-name* **stateful** 例： `Router(config-if)# crypto map map1`	クリプトマップをインターフェイスに適用します。

Fail-Close モードのアクティブ化

Fail-Close モードは、グループ メンバーがキー サーバに登録される前に暗号されていないトラフィックがそのグループ メンバーを通過しないようにします。

クリプト マップを Fail-Close モードで動作するように設定するには、次の手順を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **crypto map** *map-name* **gdoi fail-close**
4. **match address** {*access-list-number* | *access-list-name*}
5. **activate**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**crypto map** *map-name* **gdoi fail-close** 例： `Router(config)# crypto map map1 gdoi fail-close`	暗号マップが Fail-Close モードで動作するように指定して暗号マップ Fail-Close コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 4	**match address** {*access-list-number* | *access-list-name*} 例： `Router(crypto-map-fail-close)# match address 133`	（オプション）GDOI 登録用の ACL を指定します。
ステップ 5	**activate** 例： `Router(crypto-map-fail-close)# activate`	Fail-Close モードをアクティブ化します。

フェールクローズ復帰の設定

（注） フェールクローズ復帰機能では、フェールクローズモードをアクティブにする必要があります。

手順の概要

1. **enable**
2. **configure terminal**
3. **crypto gdoi group** *group-name*
4. 次のいずれかのコマンドを入力します。
   - **identity number** *number*
   - **identity address ipv4** *address*
5. **server address ipv4** *address*
6. **client fail-close revert**
7. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 3	**crypto gdoi group** *group-name* 例： `Router(config)# crypto gdoi group gdoigroupone`	GDOI グループを指定し、GDOI グループ コンフィギュレーション モードを開始します。

ステップ 4	次のいずれかのコマンドを入力します。
	• **identity number** *number*
	• **identity address ipv4** *address*
	例：
	`Router(config-gdoi-group)# identity number 3333`
	例：
	`Router(config-gdoi-group)# identity address ipv4 10.2.2.2`
		GDOI グループ番号またはアドレスを指定します。

ステップ 5	**server address ipv4** *address* 例： `Router(config-gdoi-group)# server address ipv4 10.0.5.2`	GDOI グループが到達しようとするサーバのアドレスを指定します。 • アドレスを無効にするには、このコマンドの **no** 形式を使用します。
ステップ 6	**client fail-close revert** 例： `Router(config-gdoi-group)# client fail-close revert`	クライアント フェール クローズ復帰機能を有効にします。
ステップ 7	**end** 例： `Router(config-gdoi-group)# end`	GDOI グループ コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

KEK の許容可能な暗号化アルゴリズムまたはハッシュ アルゴリズムの設定

（注） セキュリティに対する脅威は、脅威からの保護に役立つ暗号化技術と同様に絶え間なく変化しています。最新のシスコの暗号化に関する推奨事項については、『Next Generation Encryption』（NGE）ホワイト ペーパーを参照してください。

GM によって許可される KEK の暗号化およびハッシュ アルゴリズムを設定するには、次のステップを実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **crypto gdoi group** *group-name*
4. 次のいずれかのコマンドを入力します。
   - **identity number** *number*
   - **identity address ipv4** *address*
5. **server address ipv4** *address*
6. **client rekey encryption** *cipher* [*... [cipher*]]
7. **client rekey hash** *hash*
8. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**crypto gdoi group** *group-name* 例： `Router(config)# crypto gdoi group gdoigroupone`	GDOI グループを指定し、GDOI グループ コンフィギュレーション モードを開始します。

ステップ 4	次のいずれかのコマンドを入力します。
	• **identity number** *number*
	• **identity address ipv4** *address*
	例：
	`Router(config-gdoi-group)# identity number 3333`
	例：
	`Router(config-gdoi-group)# identity address ipv4 10.2.2.2`
		GDOI グループ番号またはアドレスを指定します。

ステップ 5	**server address ipv4** *address* 例：	GDOI グループが到達しようとするサーバのアドレスを指定します。

	コマンドまたはアクション	目的
	`Router(config-gdoi-group)# server address ipv4 10.0.5.2`	• アドレスを無効にするには、このコマンドの **no** 形式を使用します。
ステップ 6	**client rekey encryption** *cipher* [*... [cipher]*] 例： `Router(config-gdoi-group)# client rekey encryption aes 128 aes 192 aes 256`	KEK のクライアント受け入れ可能キー再生成暗号化を設定します。
ステップ 7	**client rekey hash** *hash* 例： `Router(config-gdoi-group)# client rekey hash sha`	KEK のクライアント受け入れ可能ハッシュを設定します。
ステップ 8	**end** 例： `Router(config-gdoi-group)# end`	GDOI グループ コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

TEK の受け入れ可能トランスフォーム セットの設定

GM によって許可されるデータ暗号化または認証のために TEK が使用するトランスフォーム セットを設定するには、次のステップを実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **crypto ipsec transform-set** *transform-set-name transform* [*transform2...transform4*]
4. **exit**
5. **crypto gdoi group** *group-name*
6. **client transform-sets** *transform-set-name1* [*... [transform-set-name6*]]
7. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例：	グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
	`Router# configure terminal`	
ステップ 3	**crypto ipsec transform-set** *transform-set-name transform* [*transform2...transform4*] 例： `Router(config)# crypto ipsec transform-set g1 esp-aes 192 esp-sha-hmac`	トランスフォーム セット（セキュリティ プロトコルおよびアルゴリズムの受け入れ可能な組み合わせ）を定義し、暗号化トランスフォーム コンフィギュレーション モードを開始します。
ステップ 4	**exit** 例： `Router(cfg-crypto-trans)# exit`	暗号化トランスフォーム コンフィギュレーション モードを終了します。
ステップ 5	**crypto gdoi group** *group-name* 例： `Router(config)# crypto gdoi group gdoigroupone`	GDOI グループを指定し、GDOI グループ コンフィギュレーション モードを開始します。
ステップ 6	**client transform-sets** *transform-set-name1* [*... [transform-set-name6*]] 例： `Router(config-gdoi-group)# client transform-sets g1`	データの暗号化および認証のためにTEKによって使用される受け入れ可能トランスフォーム タグを指定します。 • トランスフォーム セット タグは 6 個まで指定できます。
ステップ 7	**end** 例： `Router(config-gdoi-group)# end`	GDOI グループ コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

グループ メンバーの暗号状態の追跡

設定済みの拡張オブジェクト トラッカー（EOT）のスタブオブジェクト ID を使用してグループ メンバー（GM）の暗号化状態を追跡するには、この作業を実行します。

始める前に

スタブオブジェクトを作成し、このオブジェクトにトラッキング ID を割り当てて GDOI MIB をモニタすることにより、拡張オブジェクト トラッキング（EOT）を設定する必要があります。次に、トラッキング ID 99 をスタブオブジェクトに割り当てる設定例を示します。

```
event manager applet test1
 event snmp oid <new GDOI MIB object> .....
 action 2.0 track set 99 state up

track 99 stub-object
 delay up 60
```

手順の概要

1. **enable**
2. **configure terminal**
3. **crypto gdoi group** *group-name*
4. **client status active-sa track** *tracking-number*
5. **exit**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**crypto gdoi group** *group-name* 例： `Device(config)# crypto gdoi group gdoigroupone`	GDOI グループを指定し、GDOI グループ コンフィギュレーション モードを開始します。
ステップ 4	**client status active-sa track** *tracking-number* 例： `Device(config-gdoi-group)# client status active-sa track 99`	スタブオブジェクトの追跡を有効化します。この例では、GM がキー サーバ（KS）から有効なトラフィック暗号キー（TEK）を受信すると、スタブオブジェクト 99 の状態を「UP」に設定します。一方、登録失敗やキー再生成の前に TEK の期限が切れた場合などのエラーのために有効な TEK がない場合、GM はスタブオブジェクト 99 の状態を「DOWN」に設定します。
ステップ 5	**exit** 例： `Device(config-gdoi-group)# exit`	GDOI グループ コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

GET VPN GM 認証の設定

GET VPN GM 認証は、事前共有キーまたは PKI を使用して実行できます。GET VPN 認証をオンにすることはベスト プラクティスです。キー サーバが複数の GDOI グループに使用される際、あるグループの GM が別のグループからキーとポリシーを要求するのを防ぐには、キー サーバ認証が必要です。ISAKMP 認証では GM がキー サーバから GDOI 属性を要求できることが確認され、GDOI 認証では GM がキー サーバに設定された特定のグループから GDOI 属性を要求できることが確認されます。

GET VPN GM 認証を設定するには、次のいずれかのタスクを実行します。

事前共有キーを使用する GM 認証の設定

事前共有キーを使用する GM の認証を設定するには、次のステップを実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **crypto gdoi group** *group-name*
4. **server local**
5. **authorization address ipv4 {** *access-list-name* | *access-list-number* **}**
6. **exit**
7. **exit**
8. **access-list** *access-list-number* [**dynamic** *dynamic-name* [**timeout** *minutes*]] {**deny** | **permit**} *protocol source source-wildcard destination destination-wildcard* [**precedence** *precedence*] [**tos** *tos*] [**time-range** *time-range-name*] [**fragments**] [**log** [*word*] | **log-input** [*word*]]
9. **exit**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**crypto gdoi group** *group-name* 例： `Router(config)# crypto gdoi group getvpn`	GDOI を指定し、GDOI グループ コンフィギュレーション モードを開始します。
ステップ 4	**server local** 例： `Router(config-gdoi-group)# server local`	デバイスを GDOI キー サーバとして指定し、GDOI ローカル サーバ コンフィギュレーション モードを開始します。
ステップ 5	**authorization address ipv4 {** *access-list-name* | *access-list-number* **}** 例：	GDOI のアドレスのリストを指定します。

	コマンドまたはアクション	目的
	`Router(gdoi-local-server)# authorization address ipv4 50`	
ステップ 6	**exit** 例： `Router(gdoi-local-server)# exit`	GDOI ローカル コンフィギュレーション モードを終了して GDOI グループ コンフィギュレーション モードに戻ります。
ステップ 7	**exit** 例： `Router(config-gdoi-group)# exit`	GDOI グループ コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードに戻ります。
ステップ 8	**access-list** *access-list-number* [**dynamic** *dynamic-name* [**timeout** *minutes*]] {**deny** | **permit**} *protocol source source-wildcard destination destination-wildcard* [**precedence** *precedence*] [**tos** *tos*] [**time-range** *time-range-name*] [**fragments**] [**log** [*word*] | **log-input** [*word*]] 例： `Router(config)# access-list 50 permit ip 209.165.200.225 0.0.0.0 209.165.200.254 0.0.0.0`	許可される IP アクセス リストを定義します。 • この例では、アクセス リスト番号 50 のアクセス リストが定義され、送信元 IP アドレス 209.165.200.225 から宛先 IP アドレス 209.165.200.254 に送信されるパケットが許可されます。
ステップ 9	**exit** 例： `Router(config)# exit`	グローバル コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

PKI を使用する GM 認証の設定

PKI を使用する GM の認証を設定するには、次のステップを実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **crypto isakmp identity** {**address** | **dn** | **hostname**}
4. **crypto pki trustpoint** *name*
5. **subject-name** [*x.500-name*]
6. **exit**
7. **crypto gdoi group** *group-name*
8. **server local**
9. **authorization identity** *name*
10. **exit**
11. **exit**

12. **crypto identity** *name*
13. **dn** *name=string* [, *name=string*]
14. **exit**
15. **crypto isakmp identity** {**address** | **dn** | **hostname** }
16. **crypto pki trustpoint** *name*
17. **subject-name** [*x.500-name*]
18. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**crypto isakmp identity** {**address**	**dn**	**hostname**} 例： `Router(config)# crypto isakmp identity dn`	ルータがインターネットキー交換（IKE）プロトコルに参加する際にルータが使用するアイデンティティを定義します。
ステップ 4	**crypto pki trustpoint** *name* 例： `Router(config)# crypto pki trustpoint GETVPN`	ルータで使用するトラストポイントを宣言し、CA トラストポイント コンフィギュレーション モードを開始します。
ステップ 5	**subject-name** [*x.500-name*] 例： `Router(ca-trustpoint)# subject-name OU=GETVPN`	証明書要求の所有者名を指定します。
ステップ 6	**exit** 例： `Router(ca-trustpoint)# exit`	CA トラストポイント コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードに戻ります。
ステップ 7	**crypto gdoi group** *group-name* 例： `Router(config)# crypto gdoi group getvpn`	GDOI グループを指定し、GDOI グループ コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 8	**server local** 例： `Router(config-gdoi-group)# server local`	デバイスを GDOI キー サーバとして指定し、GDOI ローカル サーバ コンフィギュレーション モードを開始します。
ステップ 9	**authorization identity** *name* 例： `Router(gdoi-local-server)# authorization identity GETVPN_FILTER`	GDOI グループのアイデンティティを指定します。
ステップ 10	**exit** 例： `Router(gdoi-local-server)# exit`	GDOI ローカル サーバ コンフィギュレーション モードを終了して GDOI グループ コンフィギュレーション モードに戻ります。
ステップ 11	**exit** 例： `Router(config-gdoi-group)# exit`	GDOI グループ コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードに戻ります。
ステップ 12	**crypto identity** *name* 例： `Router(config)# crypto identity GETVPN_FILTER`	ルータの証明書内にある指定 DN リストを使用してルータのアイデンティティを設定し、暗号アイデンティティ コンフィギュレーション モードを開始します。
ステップ 13	**dn** *name=string* [, *name=string*] 例： `Router(config-crypto-identity)# dn ou=GETVPN`	ルータの証明書内にある DN に、ルータのアイデンティティを関連付けます。
ステップ 14	**exit** 例： `Router(config-crypto-identity)# exit`	GDOI グループ コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードに戻ります。
ステップ 15	**crypto isakmp identity** {**address** | **dn** | **hostname** } 例： `Router(config)# crypto isakmp identity dn`	IKE プロトコルに参加する際にルータが使用するアイデンティティを定義します。
ステップ 16	**crypto pki trustpoint** *name* 例： `Router(config)# crypto pki trustpoint GETVPN`	ルータで使用するトラストポイントを宣言し、CA トラストポイント コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 17	**subject-name** [*x.500-name*] 例： `Router(ca-trustpoint)# subject-name ou=getvpn`	証明書要求の所有者名を指定します。
ステップ 18	**end** 例： `Router(ca-trustpoint)# exit`	GDOI グループ コンフィギュレーション モードを終了し、設定を保存して、特権 EXEC モードに戻ります。

Cisco Group Encrypted Transport VPN 設定の確認とトラブルシューティング

GET VPN の設定を確認およびトラブルシューティングするには、次の作業を行います。これらの作業は任意であり、トラブルシューティング中に情報を収集するために行います。

（注） CSCsi82594 では、時間ベースのアンチリプレイ（TBAR）を有効にした場合、キー再生成の期間は 2 時間（7200 秒）に設定されます。このシナリオでは、キー サーバは 2 時間（7200 秒）ごとにグループ メンバーに定期的にキー再生成を送信します。次の例では、トラフィック暗号キー（TEK）のライフタイムが 28800 秒（8 時間）に設定されていますが、キー再生成タイマーは依然として 2 時間です。TBAR 情報を表示する show 出力の場合は、**show crypto gdoi gm replay** コマンドおよび **show crypto gdoi ks replay** コマンドを使用します。

```
crypto ipsec profile atm-profile
set security-association lifetime seconds 28800
!
crypto gdoi group ATM-DSL
server local
   sa ipsec 1
      !
      replay time window-size 100
```

キー サーバ上のアクティブなグループ メンバーの確認

キー サーバ上のアクティブなグループ メンバーを確認するには、次の手順を実行します。

手順の概要

1. **enable**
2. **show crypto gdoi ks members**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**show crypto gdoi ks members** 例： `Router# show crypto gdoi ks members`	キー サーバ メンバーに関する情報を表示します。

キー再生成関連統計情報の確認

キー再生成関連統計情報を確認するには、次の手順を実行します。

手順の概要

1. **enable**
2. **show crypto gdoi ks rekey**
3. **show crypto gdoi [gm]**

手順の詳細

ステップ 1 **enable**

例：

```
Device> enable
```

特権 EXEC モードを有効にします。

• パスワードを入力します（要求された場合）。

ステップ 2 **show crypto gdoi ks rekey**

例：

```
Device# show crypto gdoi ks rekey

For group diffint (handle: 2147483650) server 10.0.8.1 (handle: 2147483650):

# of teks : 1 Seq num : 0
KEK POLICY (transport type : Unicast)
spi : 0xA8110DE7CC8B0FB201F2A8BFAA0F2D90
management alg : disabled encrypt alg : 3DES
crypto iv length : 8 key size : 24
orig life(sec): 300 remaining life(sec): 296 <------- ticking down
sig hash algorithm : enabled sig key length : 94
```

```
sig size : 64
sig key name : mykeys
```

キーサーバ上でこのコマンドを実行すると、キーサーバから送信されるキー再生成に関する情報が表示されます。出力は、KEK の残りのライフタイムの経過を表示します。

ステップ 3 show crypto gdoi [gm]

例：

```
Device# show crypto gdoi
GROUP INFORMATION

Group Name : diffint
Group Identity : 3333
Rekeys received : 0
IPSec SA Direction : Both

Group Server list : 10.0.8.1

Group member : 10.0.3.1 vrf: None
Version : 1.0.2
Registration status : Registered
Registered with : 10.0.8.1
Re-registers in : 93 sec <-----------re-registration time for TEK or KEK
Succeeded registration: 1
Attempted registration: 1
Last rekey from : 0.0.0.0
Last rekey seq num : 0
Unicast rekey received: 0
Rekey ACKs sent : 0
Rekey Received : never
allowable rekey cipher: any
allowable rekey hash : any
allowable transformtag: any ESP

Rekeys cumulative
Total received : 0
After latest register : 0
Rekey Acks sents : 0

ACL Downloaded From KS 10.0.8.1:
access-list permit ip host 10.0.1.1 host 239.0.1.1
access-list permit ip host 10.0.100.2 host 238.0.1.1

KEK POLICY:
Rekey Transport Type : Unicast
Lifetime (secs) : 255 <-----------lifetime ticking
Encrypt Algorithm : 3DES
Key Size : 192
Sig Hash Algorithm : HMAC_AUTH_SHA
Sig Key Length (bits) : 512
```

グループメンバー上でこのコマンドを実行すると、キーサーバから送信されるキー再生成に関する情報が表示されます。出力の「re-registers in」フィールドは、その後にグループ メンバーが TEK または KEK に再登録する、より短い方の期間を表示します。

グループ メンバー上で GDOI によって作成された IPsec SA の確認

グループ メンバー上で GDOI によって作成された IPsec SA を確認するには、次の手順を実行します。

手順の概要

1. **enable**
2. **show crypto gdoi group** *group-name* **ipsec sa**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**show crypto gdoi group** *group-name* **ipsec sa** 例： `Router# show crypto gdoi group diffint ipsec sa`	グループ メンバー上で GDOI によって作成された IPsec SA に関する情報を表示します。 • この場合、表示されるのは、グループ「diffint」に関する情報だけです。 • すべてのグループの IPsec SA に関する情報を表示するには、**group** キーワードおよび *group-name* 引数を省略します。

キー サーバ上で GDOI によって作成された IPsec SA の確認

キー サーバ上で GDOI によって作成された IPsec SA を確認するには、次の手順を実行します。

手順の概要

1. **enable**
2. **show crypto ipsec sa**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**show crypto ipsec sa** 例：	現在の SA によって使用されている設定を表示します。

	コマンドまたはアクション	目的
	`Device# show crypto ipsec sa`	

グループ メンバーが最後にキー サーバから受信した TEK の確認

GM が最後に KS から受信した TEK を確認するには、GM で次のステップを実行します。

手順の概要

1. **enable**
2. **show crypto gdoi**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**show crypto gdoi** 例： `Router# show crypto gdoi`	現在の GDOI 構成、および KS からダウンロードされたポリシーを表示します。TEK は TEK POLICY セクションに表示されます。デバッグを有効にせずに、次のコマンドを使用することで、TEK が実際に最後に受信した GM を KS から IPsec コントロールプレーンにダウンロードした TEK（**show crypto ipsec sa** コマンドを使用して表示可能）と比較できます。

連携キー サーバの状態と統計情報の確認

連携キーサーバーの状態と統計情報を確認するには、**debug** および **show** コマンドのうち 1 つまたは両方を使用して、次の手順を実行します。

手順の概要

1. **enable**
2. **debug crypto gdoi ks coop**
3. **show crypto gdoi group** *group-name* **ks coop** [**version**]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例：	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。

	コマンドまたはアクション	目的
	`Router> enable`	
ステップ 2	**debug crypto gdoi ks coop** 例： `Router# debug crypto gdoi ks coop`	連携キー サーバに関する情報を表示します。
ステップ 3	**show crypto gdoi group** *group-name* **ks coop** [**version**] 例： `Router# show crypto gdoi group diffint ks coop version`	グループ「diffint」に関する情報と、連携キー サーバに関するバージョン情報を表示します。

アンチリプレイ疑似時間関連の統計情報の確認

アンチリプレイ疑似時間関連の統計情報を確認するには、**clear**、**debug**、および **show** コマンドのうち 1 つまたはすべてを使用して、次の手順を実行します。

手順の概要

1. **enable**
2. **clear crypto gdoi group** *group-name* **replay**
3. **debug crypto gdoi replay**
4. **show crypto gdoi group** *group-name*
5. **show crypto gdoi group** *group-name* **ks replay**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**clear crypto gdoi group** *group-name* **replay** 例： `Router# clear crypto gdoi group diffint replay`	リプレイ カウンタを消去します。
ステップ 3	**debug crypto gdoi replay** 例： `Router# debug crypto gdoi replay`	パケット内に格納されている疑似時間スタンプに関する情報を表示します。

	コマンドまたはアクション	目的
ステップ 4	**show crypto gdoi group** *group-name* 例： `Router# show crypto gdoi group diffint`	グループ メンバーの現在の疑似時間に関する情報を表示します。 • このグループのアンチ リプレイに関連する各種カウントも表示します。
ステップ 5	**show crypto gdoi group** *group-name* **ks replay** 例： `Router# show crypto gdoi group diffint ks replay`	キー サーバの現在の疑似時間に関する情報を表示します。

暗号マップの Fail-Close モードの状態の確認

クリプト マップの Fail-Close モードの状態を確認するには、次の手順を実行します。

手順の概要

1. **enable**
2. **show crypto map gdoi fail-close**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**show crypto map gdoi fail-close** 例： `Router# show crypto map gdoi fail-close`	Fail-Close モードの状態に関する情報を表示します。

Cisco Group Encrypted Transport VPN の設定例

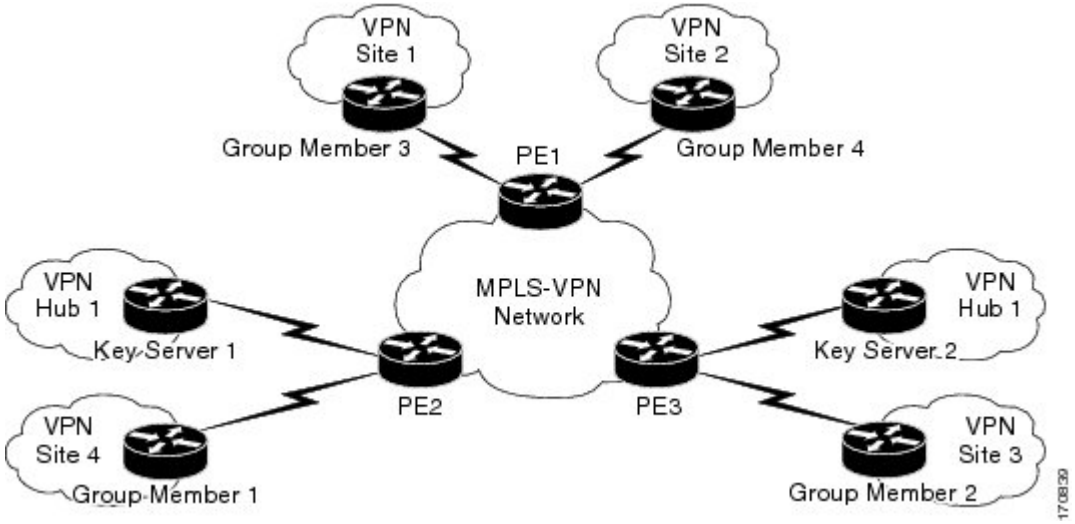
例：キー サーバとグループ メンバーのケース スタディ

次のケース スタディでは、MPLS VPN 環境における CE 間のトラフィックを暗号化します。

MPLS VPN コアによって、下図に示すとおりに各 VPN サイトを相互接続します。Group Member 1 から Group Member 4 までの VPN サイト CPE を、これらのサイトがその一部となっている VPN と関連付けられた単一の GDOI グループにグループ化します。このシナリオは、インター

ネット VPN のシナリオです。すべてのキー サーバおよびグループ メンバーは同じ VPN の一部です。Key Server 1 と Key Server 2 は連携キー サーバであり、VPN メンバーである Group Member 1 から Group Member 4 までがサポートされています。Key Server 1 はプライマリ キー サーバであり、Key Server 2 はセカンダリ キー サーバです。

図 *125* : キー サーバとグループ メンバーのシナリオ



次の設定例は上図のケース スタディに基づいています。

キー サーバ 1 の例

Key server 1 はプライマリ キー サーバです。

```
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
service internal
!
hostname KS1
!
logging buffered 100000 debugging
no logging console
!
no aaa new-model
!
resource policy
!
clock timezone EST 0
ip subnet-zero
no ip domain lookup
ip domain name cisco.com
!
crypto isakmp policy 1
 encr 3des
 authentication pre-share
 group 2
 lifetime 400
crypto isakmp key cisco address 10.1.1.13
```

```
crypto isakmp key cisco address 10.1.1.9
crypto isakmp key cisco address 10.1.1.1
crypto isakmp key cisco address 10.1.1.5
crypto isakmp key cisco address 10.1.1.21
!
crypto ipsec transform-set gdoi-trans-group1 esp-3des esp-sha-hmac
!
crypto ipsec profile gdoi-profile-group1
 set security-association lifetime seconds 1800
 set transform-set gdoi-trans-group1
!
crypto gdoi group group1
 identity number 1
 server local
  rekey lifetime seconds 86400
  rekey retransmit 10 number 2
  rekey authentication mypubkey rsa group1-export-general
  rekey transport unicast
  sa ipsec 1
   profile gdoi-profile-group1
   match address ipv4 101
   replay counter window-size 64
  address ipv4 209.165.200.225
  redundancy
   local priority 10
   peer address ipv4 209.165.200.225
   !
interface Ethernet0/0
 ip address 209.165.200.225 255.255.255.252
!
ip classless
ip route 0.0.0.0 0.0.0.0 10.1.1.18
!
access-list 101 permit ip 10.1.0.0 0.0.255.255 10.1.0.0 0.0.255.255
!
end
```

キー サーバ 2 の例

Key Server 2はセカンダリ キー サーバです。

```
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
service internal
!
hostname KS2
!
logging buffered 100000 debugging
no logging console
!
no aaa new-model
!
resource policy
!
clock timezone EST 0
ip subnet-zero
no ip domain lookup
ip domain name cisco
!
crypto isakmp policy 1
```

```
 encr 3des
 authentication pre-share
 group 2
 lifetime 400
crypto isakmp key cisco address 10.1.1.9
crypto isakmp key cisco address 10.1.1.1
crypto isakmp key cisco address 10.1.1.5
crypto isakmp key cisco address 10.1.1.17
crypto isakmp key cisco address 10.1.1.13
!
crypto ipsec transform-set gdoi-trans-group1 esp-3des esp-sha-hmac
!
crypto ipsec profile gdoi-profile-group1
 set security-association lifetime seconds 1800
 set transform-set gdoi-trans-group1
!
crypto gdoi group group1
 identity number 1
 server local

  rekey lifetime seconds 86400
  rekey retransmit 10 number 2
  rekey authentication mypubkey rsa group1-export-general
  rekey transport unicast
  sa ipsec 1
   profile gdoi-profile-group1
   match address ipv4 101
   replay counter window-size 64
  address ipv4 10.1.1.21
  redundancy
   local priority 1
   peer address ipv4 10.1.1.17
   !
interface Ethernet0/0
 ip address 209.165.200.225 255.255.255.252
!
ip classless
ip route 0.0.0.0 0.0.0.0 10.1.1.22
!
access-list 101 permit ip 10.1.0.0 0.0.255.255 10.1.0.0 0.0.255.255
!
end
```

例：グループ メンバー 1 の設定

Group Member 1 は、これらのサイトがその一部となっている VPN と関連付けられた GDOI グループの一部です。

```
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname GM1
!
resource policy
!
clock timezone EST 0
ip subnet-zero
!
crypto isakmp policy 1
 encr aes
```

```
 authentication pre-share
 group 14
 lifetime 3600
crypto isakmp key cisco address 209.165.200.225
crypto isakmp key cisco address 209.165.201.1
!
crypto gdoi group group1
 identity number 1
 server address ipv4 209.165.200.225
 server address ipv4 209.165.201.1
!
crypto map map-group1 10 gdoi
 set group group1
!
interface Ethernet0/0
 ip address 209.165.200.225 255.255.255.252
 crypto map map-group1
!
router bgp 1000
 no synchronization
 bgp log-neighbor-changes
 network 10.1.1.0 mask 255.255.255.0
 neighbor 10.1.1.2 remote-as 5000
 no auto-summary
!
ip classless
!
End
```

The same GDOI group cannot be applied to multiple interfaces. The following examples show unsupported cases:

例 1

```
crypto map map-group1
  group g1
 interface ethernet 1/0
  crypto map map-group1
 interface ethernet 2/0
  crypto map map-group1
```

例 2

```
crypto map map-group1 10 gdoi
  set group group1
crypto map map-group2 10 gdoi
  set group group1
 interface ethernet 1/0
  crypto map map-group1
 interface ethernet 2/0
```

例：グループ メンバー 2 の設定

Group Member 2 は、これらのサイトがその一部となっている VPN と関連付けられた GDOI グループの一部です。

```
service timestamps debug datetime msec
service timestamps log datetime msec
!
```

```
hostname GM2
!
resource policy
!
clock timezone EST 0
ip subnet-zero
!
crypto isakmp policy 1
 encr aes
 authentication pre-share
 group 14
 lifetime 3600
crypto isakmp key cisco address 209.165.200.225
crypto isakmp key cisco address 209.165.201.1
!
crypto gdoi group group1
 identity number 1
 server address ipv4 209.165.201.1
 server address ipv4 209.165.200.225
!
crypto map map-group1 10 gdoi
 set group group1
!
interface Ethernet0/0
 ip address 209.165.200.225 255.255.255.252
 crypto map map-group1
!
router bgp 2000
 no synchronization
 bgp log-neighbor-changes
 network 10.1.2.0 mask 255.255.255.0
 neighbor 10.1.1.6 remote-as 5000
 no auto-summary
!
ip classless
!
end
```

例：グループ メンバー 3 の設定

Group Member 3 は、これらのサイトがその一部となっている VPN と関連付けられた GDOI グループの一部です。

```
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname GM3
!
resource policy
!
clock timezone EST 0
ip subnet-zero
!
crypto isakmp policy 1
 encr aes
 authentication pre-share
 group 14
 lifetime 3600
crypto isakmp key cisco address 209.165.200.225
crypto isakmp key cisco address 209.165.201.1
```

```
!
crypto ipsec transform-set gdoi-trans-group1 esp-aes esp-sha-hmac
crypto gdoi group group1
 identity number 1
 server address ipv4 209.165.200.225
 server address ipv4 209.165.201.1
!
crypto map map-group1 10 gdoi
 set group group1
!
interface Ethernet0/0
 ip address 209.165.201.1 255.255.255.252
 crypto map map-group1
!
router bgp 3000
 no synchronization
 bgp log-neighbor-changes
 network 10.1.3.0 mask 255.255.255.0
 neighbor 10.1.1.10 remote-as 5000
 no auto-summary
!
ip classless
!
end
```

例：グループ メンバー 4 の設定

Group Member 4 は、これらのサイトがその一部となっている VPN と関連付けられた GDOI グループの一部です。

```
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname GM4
!
clock timezone EST 0
ip subnet-zero
!
crypto isakmp policy 1
 encr aes
 authentication pre-share
 group 14
 lifetime 3600
crypto isakmp key cisco address 209.165.200.225
crypto isakmp key cisco address 209.165.201.1
!
crypto gdoi group group1
 identity number 1
 server address ipv4 209.165.200.225
 server address ipv4 209.165.201.1
!
crypto map map-group1 10 gdoi
 set group group1
!
interface Ethernet0/0
 ip address 209.165.201.1 255.255.255.252
 crypto map map-group1
!
router bgp 4000
 no synchronization
```

```
 bgp log-neighbor-changes
 network 10.1.4.0 mask 255.255.255.0
 neighbor 10.1.1.14 remote-as 5000
 no auto-summary
!
ip classless
!
end
```

例：グループ メンバー 5 の設定

グループ メンバーの複数のインターフェイスが同じGDOIグループの一部である場合、ループバック インターフェイスを使用して暗号化を行う必要があります。ループバック インターフェイスを使用しない場合、暗号化されたトラフィックが処理される各インターフェイスを個別にキー サーバに登録する必要があります。

キー サーバではこれらが別個の要求と判断されるので、同一のグループ メンバーの複数のレコードが保管されます。これは、複数のキー再生成が送信されることも意味します。暗号化がループバック インターフェイスから行われる場合は、グループ メンバーを一度だけキー サーバに登録します。

次の設定は、どのようにグループ メンバーを一度だけキー サーバに登録するのかを示しています。

```
!


interface GigabitEthernet0/1
 description *** To AGG-1 ***
 crypto map dgvpn
!
interface GigabitEthernet0/2
 description *** To AGG-2 ***
 crypto map dgvpn
!
interface Loopback0
 ip address 209.165.201.1 255.255.255.255
!
 crypto map dgvpn local-address Loopback0
!
```

例：グループ メンバーが最後にキー サーバから受信した TEK の確認

次の例は、現在の GDOI 構成、および KS からダウンロードされたポリシーを表示する方法を示します。

```
Device# show crypto gdoi

GROUP INFORMATION

    Group Name               : GETV6
.
.
.
KEK POLICY:
.
```

```
.
.
TEK POLICY for the current KS-Policy ACEs Downloaded:
  Ethernet2/0:
    IPsec SA:
        spi: 0x627E4B84(1652444036)
        transform: esp-aes
        sa timing:remaining key lifetime (sec): (3214)
        Anti-Replay(Time Based) : 10 sec interval
        tag method : cts sgt
        alg key size: 24 (bytes)
        sig key size: 20 (bytes)
        encaps: ENCAPS_TUNNEL


GROUP INFORMATION

    Group Name               : GETV4
.
.
.
KEK POLICY:
.
.
.
TEK POLICY for the current KS-Policy ACEs Downloaded:
  Ethernet2/0:
    IPsec SA:
        spi: 0xF6E6B597(4142314903)
        transform: esp-aes
        sa timing:remaining key lifetime (sec): (3214)
        Anti-Replay : Disabled
        tag method : cts sgt
        alg key size: 24 (bytes)
        sig key size: 20 (bytes)
        encaps: ENCAPS_TUNNEL
```

TEK は TEK POLICY セクションに表示されます。デバッグを有効にせずに、次のコマンドを使用することで、TEK が実際に最後に受信した GM を KS から IPsec コントロールプレーンにダウンロードした TEK（**show crypto ipsec sa** コマンドを使用して表示可能）と比較できます。

タグ メソッド フィールドは、GET VPN インライン タギングに使用するメソッドを示します。可能な値は cts sgt（Cisco TrustSec セキュリティ グループ タグ用）または無効です。alg キー サイズ フィールドは、TEK ポリシーで設定されている暗号化アルゴリズムのキーの長さを示します。sig キー サイズ フィールドは、TEK ポリシーで設定されている署名のキーの長さを示します。encaps フィールドは、TEK ポリシーで設定されている IPsec カプセル化のタイプ（トンネルまたはトランスポート）を示します。

このコマンドの出力は、TEK が KS から受け取った時刻から期限切れになったことを示す場合があります。

パッシブ SA の例

次の例は、発信パケットに関する暗号化ルールに関する情報を示しています。

```
Router# show crypto ruleset
```

```
Ethernet0/0:
  59 ANY ANY DENY
  11 ANY/848 ANY/848 DENY
 IP ANY ANY IPSec SA Passive
 IP ANY ANY IPSec Cryptomap
```

次の例は、IPsec SA の方向モードを示しています。

```
Router# show crypto ruleset detail
Ethernet0/0:
 20000001000019  59 ANY ANY DENY -> 20000001999999
20000001000029  11 ANY/848 ANY/848 DENY -> 20000001999999
 20000001000035 IP ANY ANY IPSec SA Passive
 20000001000039 IP ANY ANY IPSec Cryptomap
```

Fail-Close モードの例

次の例は、Fail-Close モードがすでにアクティブになっていて、グループ メンバーが登録される前のアクセス リスト 102 からの暗号化されていないトラフィックが許可されていることを示しています。

```
crypto map map1 gdoi fail-close
 match address 102
 activate
crypto map map1 10 gdoi
 set group ks1_group
 match address 101
!
access-list 101 deny ip 10.0.1.0 0.0.0.255 10.0.1.0 0.0.0.255
access-list 102 deny tcp any eq telnet any
```

次の **show crypto map gdoi fail-close** コマンドの出力は、Fail-Close モードがすでにアクティブになっていることを示しています。

```
Router# show crypto map gdoi fail-close

Crypto Map: "svn"
        Activate: yes
        Fail-Close Access-List: (Deny = Forward In Clear, Permit = Drop)
            access-list 105 deny tcp any port = 23 any
            access-list 105 deny ospf any any
```

例：フェールクローズ復帰の確認

```
Device#show cry gdoi group GDOI_GROUP_1 | i Fail|Policy
       Fail-Close Revert : Enabled
       KS Policy Removal in : 697 sec
```

Cisco Group Encrypted Transport VPN の追加の制約事項

標準

標準	タイトル
新しい標準または変更された標準はサポートされていません。また、既存の標準に対するサポートに変更はありません。	—

MIB

MIB	MIB のリンク
CISCO-GDOI-MIB	選択したプラットフォーム、Cisco ソフトウェア リリース、およびフィーチャ セットの MIB を検索してダウンロードする場合は、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

RFC

RFC	タイトル
RFC 2401	『*Security Architecture for the Internet Protocol*』
RFC 6407	『*The Group Domain of Interpretation*』

シスコのテクニカル サポート

説明	リンク
右の URL にアクセスして、シスコのテクニカル サポートを最大限に活用してください。これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

Cisco Group Encrypted Transport VPN の機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *289 : Cisco Group Encrypted Transport VPN* の機能情報

機能名	リリース	機能情報
Cisco Group Encrypted Transport VPN	Cisco IOS XE Release 2.3	Cisco Group Encrypted Transport VPN は、any-to-any の接続を必要とする大規模な IP または MPLS サイトに対する最適な暗号化ソリューションであり、コンバージェンスに要する時間が最短に抑えられ、処理、プロビジョニング、管理、トラブルシューティングの低いオーバヘッドを実現しています。 次のコマンドが導入または変更されました。**address ipv4 (GDOI)**、**clear crypto gdoi**、**crypto gdoi gm**、 **debug crypto gdoi**、 **local priority**、 **peer address ipv4**、 **redundancy**、 **rekey address ipv4**、 **rekey transport unicast**、 **replay counter window-size**、 **replay time window-size**、 **sa receive-only**、**show crypto gdoi**。
GDOI 登録成功を追跡する MIB オブジェクトの作成	Cisco IOS XE リリース 3.12S	GDOI 登録成功を追跡する MIB オブジェクトの作成機能では、グループ内のアクティブな TEK 数を示すため、GDOI MIB に新しい MIB オブジェクトが導入されています。
GET VPN の強化	Cisco IOS XE Release 3.9S	この機能は GET VPN の復元力を改善します。復元力を強化することで、次のいずれかの方法を使用してデータ トラフィックの中断を防止または最小化します。 • トラフィックの中断の原因となる状態が検出された場合に修正を行います。 • 障害が検出された場合に迅速に回復機能を実行します。 次のコマンドが変更されました。**show crypto gdoi**、**show crypto ipsec sa**、**show tech-support**。

機能名	リリース	機能情報
GET VPN IKEv1 の分離	Cisco IOS XE Release 3.11S	この機能は、メンテナンスやトラブルシューティングに役立ちます。 次のコマンドが変更されました。**show tech-support**、**show crypto gdoi**、および **show crypto ipsec sa**。
GET VPN フェーズ 1.2	Cisco IOS XE Release 2.3	これらの機能拡張には、次の機能があります。 • キー サーバのロールの変更 この機能を使用すれば、キー サーバのロールをプライマリからセカンダリに変更できます。 この機能により、次のコマンドが導入または変更されました。**clear crypto gdoi ks coop role** • Fail-Close モード この機能によって、グループ メンバーが登録される前に、暗号化されていないトラフィックがそのグループ メンバーを通過することを防止できます。 この機能により、次のコマンドが導入または変更されました。**activate**、**crypto map**、**match address**、および **show crypto map**。 • パッシブ SA この機能を使用すれば、グループ メンバーを passive モードに永続的に設定できます。 次のコマンドが導入されました：**passive**
BGP 向けの GETVPN ルーティング対応	Cisco IOS XE リリース 3.13S	次のコマンドが導入または変更されました。**client status active-sa track**。

機能名	リリース	機能情報
GET VPN の復元力	Cisco IOS XE Release 3.9S	この機能は、エラーが発生したときのデータ トラフィックの中断が防止または最小化されるように GET VPN の復元力を向上します。 この機能は、長い SA ライフタイムの機能を導入しています。これにより、キー暗号キーとトラフィック暗号キーのライフタイムを最大 24 時間から 30 日に延長して設定できます。また、この機能により、最後にスケジュールされたキー再生成の確認応答で応答しなかったグループ メンバーに、定期的にリマインダ キー再生成を送信し続けるようにキー サーバを設定することができます。 長いSAライフタイムを定期的なリマインダ キー再生成と組み合わせて使用することで、キーがロールオーバーする前にグループ メンバーがスケジュールされたキー再生成を行わない場合、キー サーバがグループ メンバーを効果的に同期できます。 次のコマンドが変更されました。**rekey lifetime**、**rekey retransmit**、**set security-association lifetime**、**show crypto gdoi**。
Cisco TrustSec の IPsec インライン タギングの GET VPN サポート	Cisco IOS XE Release 3.9S	Cisco TrustSec（CTS）は、認証時に取得したユーザとデバイスの ID 情報を使用して、ネットワークに進入するパケットを分類します。CTS では、CTS ネットワークへの進入時にセキュリティ グループ タグ（SGT）でパケットにタグを付けることで各パケットの分類が維持されます。これにより、パケットはデータパス全体を通じて識別され、セキュリティおよびその他のポリシー基準が適用されます。タグにより、スイッチやファイアウォールなどの中継ネットワークは分類に基づいてアクセス コントロール ポリシーを適用することができます。Cisco TrustSec の IPsec インライン タギングの GET VPN サポート機能では、GET VPN インライン タギングを使用してプライベート WAN 経由で SGT 情報を伝送します。 次のコマンドが導入または変更されました。**show crypto gdoi**、**show crypto ipsec sa**、**tag cts sgt**
GET VPN 時間ベースのアンチリプレイ	Cisco IOS XE Release 2.3	時間ベースのアンチリプレイのサポートが Cisco VSA に追加されました。

機能名	リリース	機能情報
GET VPN のトラブルシューティング	Cisco IOS XE Release 3.8S	この機能では、エラー状態のログとそのトレースバック、および条件付きデバッグを保存（これはキー サーバから個々のグループ メンバーをデバッグする機能を提供します）するために、デバッグ レベル（これによりデバッグ メッセージを機能ごとに有効にできます）、イベント ロギング、トレース終了の機能の向上を提供します。条件付きデバッグ機能は、GM またはそのほかの連携キー サーバに基づいてフィルタリングできるように、キー サーバの条件付きデバッグを実行する能力を提供します。イベント ロギング機能は、イベントの最後のセットを記録する機能を提供します。 次のコマンドが導入または変更されました。**clear crypto gdoi**、**debug crypto condition unmatched**、**debug crypto gdoi**、**debug crypto gdoi condition**、**monitor event-trace gdoi**、**show crypto gdoi**、および **show monitor event-trace gdoi**。
Group Encrypted Transport VPN キー サーバ	Cisco IOS XE Release 3.6S	キー サーバとして Cisco IOS XE を実行するデバイスを設定するためのサポートが追加されました。 この機能は、Cisco IOS XE リリース 3.6S で Cisco ASR 1000 シリーズ アグリゲーション サービス ルータに導入されました。 Cisco IOS XE リリース 3.13S では、シスコ クラウド サービス ルータ（CSR）1000V シリーズのサポートが追加されました。
GET VPN の VSA サポート	Cisco IOS XE Release 2.3	Cisco VSA（高性能暗号化エンジン）サポートが、GDOI および GET VPN に対して追加されました。

用語集

DOI：Domain of Interpretation（ドメイン オブ インタープリテーション）。Internet Security Association Key Management Protocol（ISAKMP）の場合、キー管理メッセージが送信されるコンテキスト内に記述されるセキュリティ アソシエーション（SA）のペイロード内の値です（IPsec または グループ ドメイン オブ インタープリテーション）。

GDOI：Group Domain of Interpretation（グループ ドメイン オブ インタープリテーション）。ISAKMP の場合、相互に信頼し合うシステムのグループのキーを配信および管理する手段です。

group member：グループに登録されるデバイス（Cisco IOS ルータ）。他のグループメンバーと通信するためにキーサーバーによって制御されます。

group security association：グループ内のすべてのグループメンバーによって共有される SA です。

IPsec：IP security（IP セキュリティ）。一連の RFC（IETF RFC 2401 を参照）で定義されている IP パケット用データ暗号化プロトコル。

ISAKMP：Internet Security Association and Key Management Protocol。暗号キー管理プロトコルのためのフレームワークを提供するプロトコルです。

KEK：Key Encryption Key（キー暗号化キー）。キー サーバとグループ メンバー間のキー再生成を保護するために使用されるキーです。

key server：グループメンバーに対してキーおよびポリシーを配信するデバイス（Cisco IOS ルータ）。

MTU：Maximum Transmission Unit（最大伝送単位）。通信プロトコルの特定のレイヤによって宛先に渡すことが可能な最大パケットまたはフレーム サイズ（バイト単位）です。

SA：Security Association（セキュリティ アソシエーション）。グループ内のすべてのグループメンバーによって共有される SA です。

Simple Network Management Protocol (SNMP)：SNMP エージェントからの管理対象デバイスの外部モニタリングを可能にする、相互運用可能な標準ベースのプロトコルです。

TEK：Traffic Encryption Key（トラフィック暗号化キー）。グループ メンバー間のキー再生成を保護するために使用されるキーです。

第 220 章

GET VPN GM の削除とポリシー トリガー

GET VPN GM の削除とポリシー トリガー機能では、グループ暗号化トランスポート（GET）VPN ネットワークから不要なグループ メンバー（GM）を簡単に削除できます。新しいセキュリティ アソシエーション（SA）をインストールし、古い SA を削除するキー再生成トリガーの方法を提供します。また、デバイスがこれらの機能をサポートする GET VPN ソフトウェアのバージョンを実行しているかどうかを確認することができます。

GM の削除とポリシー トリガーに関する情報

GET VPN のソフトウェア バージョン

GET VPN のソフトウェア バージョンは次の形式です。

major-version.minor-version.mini-version

値は次のとおりです。

- *major-version* は、すべての GET VPN デバイスの互換性を定義します。
- *minor-version* は、キー サーバ（KS）/KS 間（連携キー サーバ）の関係と GM/GM 間の相互運用性に関する互換性を定義します。
- *mini-version* は、互換性に影響しない機能変更を追跡します。

たとえば、基本バージョン（以前のすべての GET VPN 機能）は 1.0.1 です。また、たとえば GM の削除機能とポリシー交換機能が含まれるバージョンは 1.0.2 である場合、これらの機能は（トリガーされるキー再生成でのこれらの機能の動作導入に関係なく）基本バージョンと完全な後方互換性があることを意味します。

GM はインターネット キー エクスチェンジ（IKE）フェーズ 1 ネゴシエーション（RFC 2408、『*Internet Security Association and Key Management Protocol [ISAKMP]*』で定義されています）の間にベンダー ID ペイロードで KS に GET VPN ソフトウェア バージョンを送信します。KS は、連携 KS 通知（ANN）メッセージのバージョン フィールドで他の連携 KS にソフトウェア バージョンを送信します。連携 KS も、各 GM が使用しているバージョンのリストを同期します。

GM 削除機能とポリシー交換機能はそれぞれ、その機能をサポートしていないグループのデバイスを検出するために KS（またはプライマリ KS）で実行するコマンドを提供しています。

GM の削除

GM の削除とポリシー交換機能がないとき、グループから不要な GM を削除するには、次の手順を実行する必要があります。

1. フェーズ 1 のクレデンシャル（たとえば、事前共有キーまたは 1 つ以上の PKI 証明書）を失効にします。
2. KS のトラフィック暗号キー（TEK）および Key Encryption Key（KEK）データベースをクリアします。
3. 各 GM で TEK および KEK データベースを個別にクリアし、強制的に各 GM を再登録します。

GET VPN グループが数千の GM にサービスを提供しているとき、機能させるとき、3 番目のステップには時間がかかります。また、実稼動ネットワークのグループ全体をクリアすると、ネットワーク中断を引き起こす可能性があります。GET VPN GM 削除機能とポリシー トリガー機能では、KS（またはプライマリ KS）で入力したコマンドを使用して新たな一連の TEK および KEK キーを作成し、それらを GM に伝播することによって、このプロセスを自動化します。

他の GET VPN ソフトウェア バージョンとの GM 削除の互換性

GET VPN の GM 削除およびポリシー トリガー機能は、GET VPN ネットワークのすべてのデバイスがこの機能をサポートする GET VPN ソフトウェア バージョンにアップグレードされた後にのみ使用する必要があります。そうしないと、古いソフトウェアを実行しているセカンダリ KS または GM が GM の削除メッセージを無視し、古い SA を使用してトラフィックの暗号化と復号化を続行します。この動作により、ネットワーク トラフィックの中断が発生します。

この機能には、ネットワークのすべてのデバイスが GM の削除をサポートするバージョンを実行しているかどうかを確認するために KS（またはプライマリ KS）で使用するコマンドが用意されています。プライマリ KS が GM の削除をサポートしていないデバイスを含むネットワークの GM を削除しようとすると、警告メッセージが表示されます。詳細については、「GM の削除をサポートするソフトウェア バージョンを GM が実行していることを確認する」セクションを参照してください。

一時的な IPsec SA による GM の削除

GET VPN GM の削除とポリシー トリガー機能には、一時的な IPsec SA により GM の削除をトリガーするためにKS（またはプライマリKS）で使用するコマンドが用意されています。この動作により、すべてのGMのキーのライフタイムが短縮され、キーの有効期限が切れる前に再登録します。GM の削除の間、ライフタイムが期限切れになるまで一時的なIPsec SA を使用してトラフィックの暗号化と復号化が継続されるため、ネットワーク中断は発生しません。詳細については、「一時的な IPsec SA による GM の削除」セクションを参照してください。

即時の IPsec SA 削除による GM の削除

GET VPN GM の削除とポリシー トリガー機能では、GM が強制的に古い TEK と KEK を（一時的な SA を使用せず）即座に削除し、再登録するために KS（またはプライマリ KS）で使用できるオプションのキーワードを提供します。ただし、この動作により、データプレーンに中断が引き起こされる可能性があります。そのため、重大なセキュリティ上の理由がある場合のみこの方式を使用する必要があります。詳細については、「GMの削除とIPSecSAの即座の削除」セクションを参照してください。

ポリシーの交換とキー再生成のトリガー

GET VPN GM 削除およびポリシー トリガー機能では、古い SA を削除し、新しい SA をインストールするための新しいキー再生成トリガー方法を提供します。

キー再生成をトリガーする TEK および KEK ポリシー変更に関する不整合

この機能なしでは、キー再生成をトリガーする TEK および KEK ポリシー変更に関して不整合があります。

- セキュリティ ポリシーの更新中に複数のキー再生成が送信される可能性があります。
- 一部のポリシー変更は（たとえば、トランスフォームセット、プロファイル、ライフタイム、およびアンチリプレイ）新しい SA を GM にインストールしますが、既存のポリシーからの SA はライフタイムが期限切れになるまでアクティブのままになります。
- 一部のポリシー変更（たとえば、TEK のアクセス コントロール エントリ/アクセス コントロール リスト（ACE/ACL）の変更）は新しい SA を GM にインストールし、即座に有効になります。ただし、古い SA は各 GM のデータベースで維持されます（ライフタイムが期限切れになるまで **show crypto ipsec sa** コマンドを使用して表示できます）。

たとえば、KS が Data Encryption Standard（DES）から Advanced Encryption Standard（AES）にポリシーを変更する場合、GM がこのトリガーされたキー再生成を受け取ると、新しい SA（例：AES）がインストールされ、古いSA（例：DES）のライフタイムは短縮されます。GM は短縮されたライフタイムが期限切れになるまで古い SA を使用してトラフィックの暗号化と復号化を継続します。

次に、短縮されたライフタイムを計算する式を示します。

TEK_SLT = MIN(TEK_RLT, MAX(90s, MIN(5%(TEK_CLT), 3600s)))

値は次のとおりです。

- TEK_SLT は TEK の短縮されたライフタイムです。
- TEK_RLT は TEK の残りのライフタイムです。
- TEK_CLT は TEK の設定されたライフタイムです。

次の表は、キー再生成に関する不整合をまとめたものです。

表 *290* : セキュリティ ポリシー変更後のキー再生成の動作

ポリシーの変更	キー再生成を送信するか	ポリシー変更後のキー再生成の動作
TEK：SA ライフタイム	No	古い SA は、そのライフタイムが期限切れになるまでアクティブのままになります。新しいライフタイムは、次にスケジュールされたキー再生成の後に有効になります。**clear crypto sa** コマンドを入力しても、古いライフタイムを使用して再登録され、古い SA が再度ダウンロードされます。
TEK：IPSEC トランスフォーム セット	Yes	古いトランスフォーム セットの SA は、そのライフタイムが期限切れになるまでアクティブのままになります。
TEK：IPSEC プロファイル	Yes	古いプロファイルの SA は、そのライフタイムが期限切れになるまでアクティブのままになります。
TEK：一致する ACL	Yes	発信パケット分類ですぐに ACL が使用されます。ただし、古い SA は SA データベースに残ります（**show crypto ipsec sa** コマンドを使用して表示できます）。
TEK：リプレイ カウンタのイネーブル化	Yes	ただし、カウンタ リプレイがない古い SA は、そのライフタイムが期限切れになるまでアクティブのままになります。
TEK：リプレイ カウンタ値の変更	No	新しいリプレイ カウンタがある SA は、次にスケジュールされたキー再生成時に送信されます。
TEK：リプレイ カウンタのディセーブル化	Yes	ただし、カウンタ リプレイがイネーブルになっている古い SA は、そのライフタイムが期限切れになるまでアクティブのままになります。
TEK：TBAR の有効化	Yes	ただし、時間ベースのアンチリプレイ（TBAR）が無効になった古い SA は、そのライフタイムが期限切れになるまでアクティブのままになります。

ポリシーの変更	キー再生成を送信するか	ポリシー変更後のキー再生成の動作
TEK：TBAR ウィンドウの変更	No	新しい TBAR ウィンドウがある SA は、次にスケジュールされたキー再生成時に送信されます。
TEK：TBAR の無効化	Yes	ただし、TBAR がイネーブルになっている古い SA は、そのライフタイムが期限切れになるまでアクティブのままになります。
TEK：受信専用のイネーブル	Yes	受信専用モードは、キー再生成後ただちにアクティブになります。
TEK：受信専用のディセーブル	Yes	受信専用モードは、キー再生成後ただちに非アクティブになります。
KEK：SA ライフタイムの動作	No	変更は次のキー再生成時に適用されます。
KEK：認証キーの変更	Yes	変更は即時に適用されます。
KEK：暗号アルゴリズムの変更	Yes	変更は即時に適用されます。

この機能では、一貫性を確保することで、これらの問題を解決します。この機能によって、GET VPN ポリシーの変更単独ではキー再生成がトリガーされなくなります。ポリシー（およびグローバル コンフィギュレーション モードの終了）を変更すると、ポリシーが変更され、キー再生成が必要であることを示す syslog メッセージがプライマリ KS に表示されます。この機能には、（実行コンフィギュレーションの最新のセキュリティポリシーに基づく）キー再生成を送信するためにKS（またはプライマリKS）で入力する新しいコマンドが用意されています。

この機能ではまた、古い TEK および KEK を即座に削除し、新しい TEK および KEK をインストールするようにキー再生成を受信するGMに強制する追加のキーワードを新しいコマンドに用意しています。そのため、新しいポリシーは古い SA ポリシーが期限切れになるのを待たずにただちに反映されます。（ただし、すべてのGMが同時にキー再生成メッセージを受信しない場合があるため、このキーワードを使用すると、一時的なトラフィックの切断が発生する可能性があります）。

ポリシーの交換およびキー再生成のトリガーの他の GET VPN ソフトウェア バージョンとの互換性

キー再生成のトリガーは、GET VPN ネットワーク内のすべてのデバイスをこの機能をサポートする GET VPN ソフトウェア バージョンにアップグレードしてから使用する必要があります。**crypto gdoi ks** コマンドをまだサポートしていない古いバージョンを実行している GM では、プライマリ KS はソフトウェアバージョン管理機能を使用してこれらのバージョンを検出し、ポリシー交換のための命令を送信せずにキー再生成のトリガーのみ実行します。したがっ

て、GM がキー再生成を受信すると、新しい SA をインストールしますが、古い SA の有効期間は短縮しません。（この動作は以前のキー再生成メソッドと同様であり、ポリシーの交換をサポートしないデバイスの後方互換性が確保されます。）

この機能は、ネットワークのすべてのデバイスがポリシーの交換をサポートするバージョンを実行しているかどうかを確認するためにKS（またはプライマリ KS）で使用するコマンドを提供します。詳細については「GM がポリシーの交換をサポートするソフトウェア バージョンを実行していることを確認する」セクションを参照してください。

GET VPN GM 削除およびポリシー トリガーの設定方法

GM の削除をサポートするソフトウェア バージョンを GM が実行していることを確認する

GET VPN の GM 削除およびポリシー トリガー機能は、GET VPN ネットワークのすべてのデバイスがこの機能をサポートする GET VPN ソフトウェア バージョンにアップグレードされた後にのみ使用する必要があります。そうしないと、古いソフトウェアを実行しているセカンダリ KS または GM が GM 削除メッセージを無視して、古い SA を使用するトラフィックの暗号化および復号化を継続します。この動作により、ネットワーク トラフィックの中断が発生します。

ネットワーク内のすべてのデバイスが GM 削除をサポートすることを確認するには、KS（またはプライマリ KS）でこの作業を実行します。

手順の概要

1. **enable**
2. **show crypto gdoi feature gm-removal**
3. **show crypto gdoi feature gm-removal | include No**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**show crypto gdoi feature gm-removal** 例： `Device# show crypto gdoi feature gm-removal`	GET VPN ネットワーク内の各 KS および GM で実行されている GET VPN ソフトウェアのバージョンを表示し、そのデバイスが GM 削除をサポートしているかどうかを表示します。

	コマンドまたはアクション	目的
ステップ 3	**show crypto gdoi feature gm-removal | include No** 例： `Device# show crypto gdoi feature gm-removal | include No`	（オプション）GM 削除をサポートしないデバイスのみ表示します。

一時的な IPsec SA による GM の削除

一時的な IPsec SA の GM の削除をトリガーするには、KS（またはプライマリ KS）でこの作業を実行します。

手順の概要

1. **enable**
2. **clear crypto gdoi** [**group** *group-name*] **ks members**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**clear crypto gdoi** [**group** *group-name*] **ks members** 例： `Device# clear crypto gdoi ks members`	新しい TEK および KEK キーのセットを作成します。またこのコマンドは、すべての GM に古い TEK および KEK データベースをクリーンアップするための GM 削除メッセージも送信します。

例

KS に次のようにメッセージが表示されます。

```
Device# clear crypto gdoi ks members

% This GM-Removal message will shorten all GMs' key lifetimes and cause them to
re-register before keys expiry.
Are you sure you want to proceed? ? [yes/no]: yes
Sending GM-Removal message to group GET...
```

各 GM が GM 削除メッセージを受信すると、次の syslog メッセージが各 GM に表示されます。

```
*Jan 28 08:37:03.103: %GDOI-4-GM_RECV_DELETE: GM received delete-msg from KS in group
GET.
TEKs lifetime are reduced and re-registration will start before SA expiry
```

各 GM は KEK を即時削除し、次のように古い TEK のライフタイムを短縮します。

```
TEK_SLT = MIN(TEK_RLT, MAX(90s, MIN(5%(TEK_CLT), 3600s)))
TEK_SLT: TEK shortened lifetime
TEK_RLT: TEK Remaining LIfeTime
TEK_CLT: TEK Configured LIfeTime
```

また GM は、従来の再登録タイマーに従いジッター（ランダムな遅延）が適用された新しい TEK と KEK を取得するために KS への再登録を開始します。ジッターは、すべての GM が同時に再登録してキーサーバの CPU に過負荷を与えることを防ぎます。KS にインストールされた新しいクレデンシャルに基づいて認証を通す GM だけが新しい TEK と KEK を受信します。

トラフィックはライフタイムが期限切れになるまで一時的な IPsec SA を使用して暗号化と復号化を続けるため、GM 削除によってネットワークの中断が発生することはありません。

セカンダリ KS でこのコマンドを使用しようとすると、次のように拒否されます。

```
Device# clear crypto gdoi ks members

ERROR for group GET: can only execute this command on Primary KS
```

GM の削除と IPSec SA の即時削除

古い TEK と KEK を即時削除して再登録するように GM に強制するには KS（またはプライマリ KS）でこの作業を実行します。

手順の概要

1. **enable**
2. **clear crypto gdoi** [**group** *group-name*] **ks members now**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**clear crypto gdoi** [**group** *group-name*] **ks members now** 例： `Device# clear crypto gdoi ks members now`	新しい TEK および KEK キーのセットを作成します。またこのコマンドは、すべての GM に古い TEK および KEK データベースをクリーンアップするための GM 削除メッセージも送信します。 （注） **now** キーワードの使用により、データプレーンにネットワーク中断が発生することがあります。セキュリティに関する問題が中断よりも重要である場合にのみ、GM 削除を進めます。

例

KS に次のようにメッセージが表示されます。

```
Device# clear crypto gdoi ks members now

% This GM-Removal immediate message will cleanup all GMs downloaded policies
% This will cause all GMs to re-register.
Are you sure you want to proceed? ? [yes/no]: yes
Sending GM-Removal message to group GET...
```

上記のコマンドの入力後、KS は、各 GM の次のアクションをトリガーするために「remove now」メッセージを各 GM に送信します。

1. ダウンロードされた TEK および KEK ならびにそのポリシーがすぐにクリーンアップされ、（明示的にフェールクローズ モードが設定されていない限り）フェールオープン モードに戻ります。
2. 設定されている TEK ライフタイムの 2 パーセント以内のランダムに選択された期間でタイマーを設定します。
3. ステップ 2 のタイマーの期限が切れると、GM は新しい TEK および KEK をダウンロードするために KS への再登録を開始します。

各 GM では、GM がランダムな期間内に再登録されることを示すために次の syslog メッセージが表示されます。

```
*Jan 28 08:27:05.627: %GDOI-4-GM_RECV_DELETE_IMMEDIATE: GM receive REMOVAL-NOW in group

GET to cleanup downloaded policy now. Re-registration will start in a randomly chosen
period of 34 sec
```

GM 削除をサポートしていないデバイスを含むネットワークの GM を削除しようとすると、警告メッセージが表示されます。

```
Device# clear crypto gdoi ks members now

% This GM-Removal immediate message will cleanup all GMs downloaded policies
% This will cause all GMs to re-register.
Are you sure you want to proceed? ? [yes/no]: yes
WARNING for group GET: some devices cannot support GM-REMOVAL and can cause network
disruption. Please check 'show crypto gdoi feature'.
Are you sure you want to proceed ? [yes/no]: no
```

GM がポリシーの交換をサポートするソフトウェア バージョンを実行していることを確認する

ネットワーク内のすべてのデバイスがポリシーの交換をサポートするかどうかを確認するには、KS（またはプライマリ KS）でこの作業を実行します。

手順の概要

1. **enable**

2. **show crypto gdoi feature policy-replace**
3. **show crypto gdoi feature policy-replace | include No**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**show crypto gdoi feature policy-replace** 例： `Device# show crypto gdoi feature policy-replace`	GET VPN ネットワーク内の各 KS および GM で実行されている GET VPN ソフトウェアのバージョンを表示し、そのデバイスがポリシーの交換をサポートしているかどうかを表示します。
ステップ 3	**show crypto gdoi feature policy-replace | include No** 例： `Device# show crypto gdoi feature policy-replace | include No`	（オプション）ポリシーの交換をサポートしないデバイスのみ検索します。これらのデバイスでは、プライマリ KS はポリシー交換に関する手順なしでトリガーされるキー再生成のみを送信します。したがって、GM がキー再生成を受信すると、新しい SA をインストールしますが、古い SA の有効期間は短縮しません。この動作は既存のキー再生成メソッドと同じであり後方互換性があります。

キー再生成のトリガー

KS（またはプライマリ KS）でセキュリティ ポリシーを変更し（たとえば、DES から AES）、グローバル コンフィギュレーション モードを終了すると、ポリシーが変更され、キー再生成が必要であることを示す syslog メッセージが KS に表示されます。実行コンフィギュレーションの最新のポリシーに基づくキー再生成を送信するために、次のようにキー再生成をトリガーするコマンドを入力します。

キー再生成をトリガーするには KS（プライマリ KS）でこの作業を実行します。

手順の概要

1. **enable**
2. **crypto gdoi ks** [**group** *group-name*] **rekey** [**replace-now**]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例：	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。

	コマンドまたはアクション	目的
	`Device> enable`	
ステップ 2	**crypto gdoi ks** [**group** *group-name*] **rekey** [**replace-now**] 例： `Device# crypto gdoi ks group mygroup rekey`	すべての GM のキー再生成をトリガーします。 オプションの **replace-now** キーワードは、各 GM の古い TEK および KEK を即時に置き換え、SA が期限切れになる前に新しいポリシーを有効にします。 （注） **replace-now** キーワードを使用すると、一時的なトラフィックの不連続を引き起こすことがあります。

例

KS に次のようにメッセージが表示されます。

```
Device# crypto gdoi ks rekey
Device#
*Jan 28 09:17:44.363: %GDOI-5-KS_SEND_UNICAST_REKEY: Sending Unicast Rekey with
policy-replace for group GET from address 10.0.8.1 with seq # 2
```

ポリシーの変更後、各 GM がこのトリガーされたキー再生成を受信すると、新しい SA（たとえば、AES 用）をインストールして、古い SA（たとえば、DES 用）のライフタイムを短縮します。各 GM はこの短縮されたライフタイムが期限切れになるまで古い SA を使用してトラフィックの暗号化および復号化を続けます。

セカンダリ KS のキー再生成をトリガーしようとすると、次のようにコマンドが拒否されます。

```
Device# crypto gdoi ks rekey
ERROR for group GET: This command must be executed on Pri-KS
```

GET VPN GM の削除とポリシーのトリガーの設定例

例：GET VPN ネットワークからの GM の削除

GM の削除をサポートするソフトウェア バージョンを GM が実行していることを確認する

次の例は、ネットワーク内のすべてのデバイスが GM 削除機能をサポートしているかどうかを確認するために KS（またはプライマリ KS）で GET VPN ソフトウェア バージョン管理コマンドを使用する方法を示します。

```
Device# show crypto gdoi feature gm-removal
```

```
Group Name: GET
 Key Server ID       Version   Feature Supported
    10.0.8.1         1.0.2          Yes
    10.0.9.1         1.0.2          Yes
    10.0.10.1        1.0.2          Yes
    10.0.11.1        1.0.2          Yes
 Group Member ID     Version   Feature Supported
    10.0.0.2         1.0.2          Yes
    10.0.0.3         1.0.1          No
```

次の例は、GMの削除をサポートしていないデバイスのみを検索する方法を示します。

```
Device# show crypto gdoi feature gm-removal | include No

       10.0.0.3          1.0.1          No
```

上記の例では、IP アドレス 10.0.0.3 の GM は（GM の削除をサポートしない）古いソフトウェア バージョン 1.0.1 を実行中であり、アップグレードする必要があることを示しています。

一時的な IPsec SA による GM の削除

次の例では、一時的な IPsec SA を使用する GM の削除をトリガーする方法を示します。KS（またはプライマリ KS）でこのコマンドを使用します。

```
Device# clear crypto gdoi ks members

% This GM-Removal message will shorten all GMs' key lifetimes and cause them to
re-register before keys expiry.
Are you sure you want to proceed? ? [yes/no]: yes
Sending GM-Removal message to group GET...
```

GM の削除と IPSec SA の即時削除

次の例は、古い TEK と KEK を即座に削除して再登録するために GM を強制適用する方法を示しています。KS（またはプライマリ KS）でこのコマンドを使用します。

```
Device# clear crypto gdoi ks members now

% This GM-Removal immediate message will cleanup all GMs downloaded policies
% This will cause all GMs to re-register.
Are you sure you want to proceed? ? [yes/no]: yes
Sending GM-Removal message to group GET...
```

例：グループ メンバーのキー再生成のトリガー

GM がキー再生成のトリガーをサポートするソフトウェア バージョンを実行していることを確認する

次の例は、GET VPN ネットワークのデバイスのソフトウェアのバージョンを表示し、またポリシー変更後のキー再生成のトリガーをサポートするかどうかを表示するために、KS（またはプライマリ KS）で GET VPN ソフトウェア バージョン管理コマンドを使用する方法を示します。

```
Device# show crypto gdoi feature policy-replace

Key Server ID       Version  Feature Supported
  10.0.8.1         1.0.2          Yes
  10.0.9.1         1.0.2          Yes
  10.0.10.1        1.0.2          Yes
  10.0.11.1        1.0.2          Yes
 Group Member ID     Version  Feature Supported
  5.0.0.2          1.0.2          Yes
  9.0.0.2          1.0.1          No
```

次の例は、ポリシー交換後のキー再生成のトリガーをサポートしていないデバイスのみを検索する方法を示します。

```
Device# show crypto gdoi feature policy-replace  | include No

       9.0.0.2          1.0.1          No
```

これらのデバイスでは、プライマリ KS はポリシー交換に関する手順なしでトリガーされるキー再生成のみを送信します。したがって、GM がキー再生成を受信すると、新しい SA をインストールしますが、古い SA の有効期間は短縮しません。

キー再生成のトリガー

次の例では、ポリシー変更の実行後にキー再生成をトリガーする方法を示します。この例では、**profile gdoi-p2** コマンドで IPSec ポリシーの変更（たとえば、DES から AES）が発生します。

```
Device# configure terminal
Device(config)# crypto gdoi group GET
Device(config-gdoi-group)# server local
Device(gdoi-local-server)# sa ipsec 1
Device(gdoi-sa-ipsec)# no profile gdoi-p
Device(gdoi-sa-ipsec)# profile gdoi-p2
Device(gdoi-sa-ipsec)# end
Device#

*Jan 28 09:15:15.527: %SYS-5-CONFIG_I: Configured from console by console
*Jan 28 09:15:15.527: %GDOI-5-POLICY_CHANGE: GDOI group GET policy has changed. Use
'crypto gdoi ks rekey' to send a rekey, or the changes will be send in the next scheduled
```

```
rekey
Device# crypto gdoi ks rekey
Device#
*Jan 28 09:17:44.363: %GDOI-5-KS_SEND_UNICAST_REKEY: Sending Unicast Rekey with
policy-replace for group GET from address 10.0.8.1 with seq # 2
```

次の例では、セカンダリ KS のキー再生成をトリガーしようとすると表示されるエラーメッセージを示します。

```
Device# crypto gdoi ks rekey

ERROR for group GET: This command must be executed on Pri-KS
```

（注） 時間ベースのアンチリプレイ（TBAR）が設定されると、キー サーバは 2 時間（7200 秒）ごとに定期的にキー再生成をグループ メンバーに送信します。次の例では、有効期間が 8 時間（28800 秒）に設定されていますが、キー再生成タイマーは 2 時間に設定されています。

```
Device(config)# crypto ipsec profile atm-profile
Device(ipsec-profile)# set security-association lifetime seconds 28800
!
Device(ipsec-profile)# exit
Device(config)# crypto gdoi group ATM-DSL
Device(config-gdoi-group)# server local
Device(gdoi-sa-ipsec)# sa ipsec 1
!
Device(gdoi-sa-ipsec)# replay time window-size 100
```

show crypto gdoi gm replay コマンドおよび **show crypto gdoi ks replay** コマンドにより TBAR 情報が表示されます。

GET VPN GM の削除とポリシーのトリガーのその他の参考資料

関連資料

関連項目	マニュアル タイトル
Cisco IOS セキュリティ コマンド	『*Cisco IOS Security Command References*』

シスコのテクニカル サポート

説明	リンク
右の URL にアクセスして、シスコのテクニカル サポートを最大限に活用してください。これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

GET VPN GM の削除とポリシーのトリガーの機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *291 : GET VPN GM* の削除とポリシーのトリガーの機能情報

機能名	リリース	機能情報
GET VPN GM の削除とポリシー トリガー		この機能は、GET VPN ネットワークから不要な GM を効率的に削除するコマンド、新しい SA をインストールして古い SA を削除するためにキー再生成をトリガーするコマンド、およびネットワーク デバイスがこれらの機能をサポートする GET VPN ソフトウェアのバージョンを実行しているかどうかを表示するコマンドを提供します。 次のコマンドが導入または変更されました。**clear crypto gdoi, crypto gdoi ks, show crypto gdoi.**

第 221 章

GET VPN の GDOI MIB サポート

暗号化された既存の MIB はインターネット キー エクスチェンジ（IKE）および IP Security（IPsec）MIB であり、Group Domain of Interpretation（GDOI）には不十分です。GET VPN の GDOI MIB サポート機能では、RFC 6407、『The Group Domain of Interpretation』に MIB のサポートが追加されます。GDOI MIB IETF 標準規格に関連するオブジェクトのみがサポートされます。GDOI MIB .my ファイルは SNMP 管理ステーションにインポートして解析することにより、テーブル オブジェクトと階層情報を取得することができます。

GDOI MIB は、（トラップと呼ばれていた）オブジェクトおよび通知で構成されます。これには、GDOI グループ、グループ メンバー（GM）とキー サーバ（KS）のピア、および作成またはダウンロードされるポリシーに関する情報が含まれます。「get」操作のみが GDOI でサポートされます。

GET VPN の GDOI MIB のサポートを設定するには、「GET VPN の GDOI MIB サポートの設定」セクションを参照してください。

GET VPN の GDOI MIB サポートに関する情報

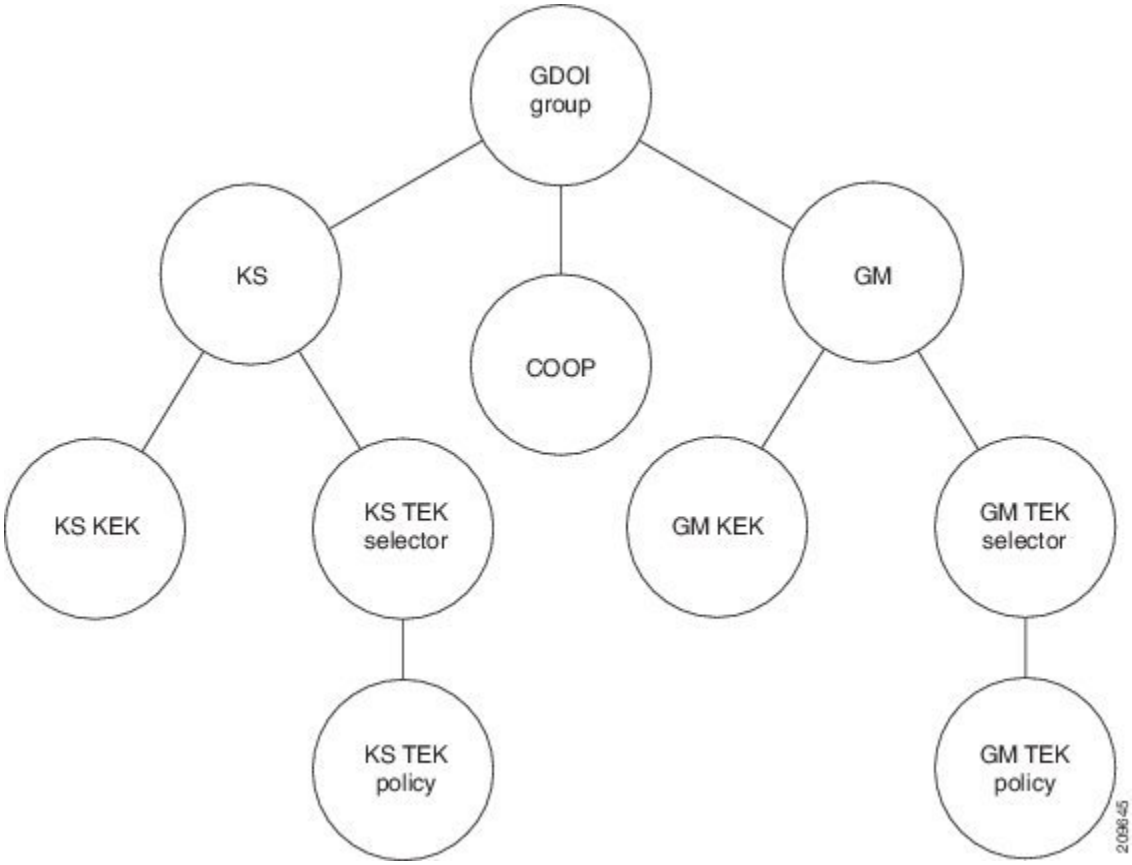
他の GET VPN ソフトウェア バージョンとの GDOI MIB の互換性

GET VPN の GDOI MIB サポート機能には、ネットワークのすべてのデバイスが GDOI MIB をサポートするバージョンを実行しているかどうかを確認するために KS（プライマリ KS）で使用するコマンドが用意されています。詳細については、「GDOI MIB をサポートするソフトウェア バージョンを GM が実行していることを確認する」セクションを参照してください。

GDOI MIB テーブル階層

GDOI MIB オブジェクトは次の GDOI MIB テーブルで構成されます。次に、テーブル間の関係（階層）を示します。

図 *126 : GDOI MIB* テーブル階層



GDOI MIB テーブル オブジェクト

次は、MIB テーブル オブジェクトのリストです（グループごとにリスト）。

グループ テーブル オブジェクト：

- Group ID type：グループ ID が IP アドレス、グループ番号、ホスト名などのいずれであるかを指定します。
- Group ID length：グループ ID 値のオクテット数。
- Group ID value：グループ番号、IP アドレス、またはホスト名。
- Group name：文字列の値。
- Group member count：このグループに登録済みの KS 数を指定します。

- Group active peer KS count：このグループに対するアクティブな KS 数を指定します。
- Group last rekey retransmits：最後のキー再生成操作の一部として送信されたキー再生成メッセージと再送信メッセージの累積数を指定します。
- Group last rekey time taken：最後のキー再生成操作の完了に KS が費やした時間を指定します。

KS テーブル オブジェクト：

- KS ID type
- KS ID length
- KS ID value
- Active KEK：キー再生成メッセージを暗号化するために KS によって現在使用されている Key Encryption Key（KEK）の SPI。
- Last rekey sequence number：グループに KS から送信された最後のキー再生成番号。
- KS Role：プライマリまたはセカンダリ。
- Number of registered GMs：この KS に登録された GM の数。

COOP テーブル オブジェクト：

- COOP peer ID type
- COOP peer ID length
- COOP peer ID value
- COOP peer ID role：プライマリまたはセカンダリ
- COOP peer status：アライブ、デッド、または不明
- Number of registered GMs：この COOP ピアに登録された GM の数

GM テーブル：

- GM ID type
- GM ID length
- GM ID value
- Registered KS ID type：GM が登録されている KS の ID タイプ。
- Registered KS ID length
- Registered KS ID value
- Active KEK：キー再生成メッセージの復号化に GM が現在使用している KEK の SPI。
- Last rekey seq number：GM が受信した最後のキー再生成番号。

- Count of active TEKs：データプレーン トラフィックの暗号化/復号化/認証のために GM によって使用されるアクティブな TEK の数。

KS KEK テーブル：

- KEK index
- KEK SPI
- KEK source ID information：送信元 ID のタイプ、ID の長さ、および ID の値。
- KEK source ID port：送信元 ID に関連付けられたポート。
- KEK destination ID information：宛先 ID のタイプ、ID の長さ、および ID の値。
- KEK destination ID port：宛先 ID に関連付けられたポート。
- IP protocol ID：UDP または TCP。
- キー管理アルゴリズム（未使用）。
- 暗号化アルゴリズムとキーの長さ（ビット）
- SIG ペイロード ハッシュ アルゴリズム、SIG ペイロード署名アルゴリズム、および SIG ペイロード キーの長さ（ビット）。
- ハッシュ アルゴリズム（IPsec MIB から再利用されます）
- Diffie-Hellman グループ
- KEK original lifetime (seconds)：KEK が有効である最長時間。
- KEK remaining lifetime (seconds)

KS TEK セレクタ テーブル（KS で GDOI グループ設定の IPsec SA の一部として設定された ACL に対応）：

- TEK selector index：トラフィック暗号キー（TEK）の整数のインデックス。
- TEK source ID information：送信元 ID のタイプ、ID の長さ、および ID の値。
- TEK source ID port：送信元 ID に関連付けられたポート。
- TEK destination ID information：宛先 ID のタイプ、ID の長さ、および ID の値。
- TEK destination ID port：宛先 ID に関連付けられたポート。
- TEK Security protocol：SA TEK ペイロードの GDOI_PROTO_IPSEC_ESP プロトコル ID 値（RFC 6407 を参照）。

KS TEK ポリシー テーブル：

- TEK policy index：整数のインデックス。
- TEK SPI：4 つのオクテット

- Encapsulation mode：トンネルまたは転送。
- 暗号化アルゴリズムとキーの長さ（ビット）
- 整合性および認証アルゴリズムとキーの長さ（ビット）
- TBAR window size (seconds)
- TEK original lifetime (seconds)：TEK が有効である最長時間。
- TEK remaining lifetime (seconds)
- TEK Status：着信、発信、または不使用。

GM KEK テーブル：

- KEK index：整数のインデックス。
- KEK SPI
- KEK source ID information：送信元 ID のタイプ、ID の長さ、および ID の値。
- KEK source ID port：送信元 ID に関連付けられたポート。
- KEK destination ID information：宛先 ID のタイプ、ID の長さ、および ID の値。
- KEK destination ID port：宛先 ID に関連付けられたポート。
- IP protocol ID：UDP または TCP。
- Key Management アルゴリズム（未使用）
- 暗号化アルゴリズムとキーの長さ（ビット）
- SIG ペイロード ハッシュ アルゴリズム、SIG ペイロード署名アルゴリズム、および SIG ペイロード キーの長さ（ビット）
- Hash algorithm
- Diffie-Hellman グループ
- KEK original lifetime (seconds)：KEK が有効である最長時間。
- KEK remaining lifetime (seconds)

GM TEK セレクタ テーブル（KS から TEK ポリシーの一部として GM にダウンロードされる ACL に対応）：

- TEK selector index：整数のインデックス。
- TEK source ID information：送信元 ID のタイプ、ID の長さ、および ID の値。
- TEK source ID port：送信元 ID に関連付けられたポート。
- TEK destination ID information：宛先 ID のタイプ、ID の長さ、および ID の値。
- TEK destination ID port：宛先 ID に関連付けられたポート。

- TEK Security protocol：SA TEK ペイロードの GDOI_PROTO_IPSEC_ESP プロトコル ID 値（RFC 6407 を参照）。

GM TEK ポリシー テーブル：

- TEK policy index：整数のインデックス。
- TEK SPI：4 つのオクテット。
- Encapsulation mode：トンネルまたは転送。
- 暗号化アルゴリズムとキーの長さ（ビット）
- 整合性および認証アルゴリズムとキーの長さ（ビット）
- TBAR window size (seconds)
- TEK original lifetime (seconds)：TEK が有効である最長時間。
- TEK remaining lifetime (seconds)
- TEK Status：着信、発信、または不使用。

GDOI MIB 通知

GDOI MIB は次の表の Simple Network Management Protocol（SNMP）通知をサポートしています。GDOI MIB には、KS によって生成された通知と各 GM によって生成された通知の 2 種類の通知があります。任意の組み合わせの通知（またはすべての通知）を有効にできます。

表 *292 : GDOI MIB* にサポートされる *SNMP* 通知

通知	説明
KS New Registration	KS が GM から最初に登録要求を受信した。
KS Registration Complete	GM が KS への登録を完了した。
KS Rekey Pushed	キー再生成メッセージが KS によって送信された。
KS No RSA Keys	RSA キーが見つからないために KS からエラー通知が受信された。
GM Register	GM が KS に最初の登録要求を送信した。
GM Registration Complete	GM が KS への登録を完了した。
GM Re-Register	GM が KS への登録プロセスを開始した。
GM Rekey Received	キー再生成メッセージが GM で受信された。
GM Incomplete Config	GM が設定の不足によるエラー通知を送信した。

通知	説明
GM Rekey Failure	GM がキー再生成の処理とインストールができないため、エラー通知を送信した。
KS Role Change	KS がプライマリとセカンダリ ロールを切り替えた。
KS GM Deleted	GM が KS から削除されると生成されます。
KS Peer Reachable	到達不能な COOP ピアが到達可能になると KS によって生成されます。
KS Peer Unreachable	到達可能な COOP ピアが到達不能になると KS によって生成されます。

詳細については、「GDOI MIB 通知の有効化」セクションを参照してください。

GDOI MIB の制限

GDOI MIB には RFC 6407 にリストされているオブジェクトのみが含まれ、GDOI のシスコ実装に固有の機能のためのオブェクトは含まれません。リストでは次の演算を使用します。

- 連携キー サーバ
- GM ACL
- 受信専用 SA
- Fail-Close またはフェール オープン
- 暗号マップ オブジェクト
- 他の Cisco GET VPN 固有の機能

GET VPN の GDOI MIB サポートの設定方法

GDOI MIB をサポートするソフトウェア バージョンを GM が実行していることを確認する

GET VPN ネットワーク内のすべてのデバイスが GDOI MIB をサポートすることを確認するには、KS（またはプライマリ KS）でこの作業を実行します。

手順の概要

1. **enable**
2. **show crypto gdoi feature gdoi-mib**

3. **show crypto gdoi feature gdoi-mib | include No**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**show crypto gdoi feature gdoi-mib** 例： `Device# show crypto gdoi feature gdoi-mib`	ネットワーク内の各 KS および GM で実行されている GET VPN ソフトウェアのバージョンを表示し、そのデバイスが GDOI MIB をサポートしているかどうかを表示します。
ステップ 3	**show crypto gdoi feature gdoi-mib	include No** 例： `Device# show crypto gdoi feature gdoi-mib	include No`	（オプション）GDOI MIB をサポートしないデバイスのみ検索します。

SNMP コミュニティのアクセス コントロールの作成

SNMP へのアクセスを許可するために、KS または GM 上の SNMP マネージャと SNMP エージェント間の関係を定義する SNMP コミュニティ アクセス文字列を指定します。このコミュニティ アクセス文字列は、デバイス上のエージェントへのアクセスを制御するパスワードのように機能します。

コミュニティ アクセス文字列を指定するにはこの作業を行います。

手順の概要

1. **enable**
2. **configure terminal**
3. **snmp-server community** *community-string* [**view** *view-name*] [**ro** | **rw**] [**ipv6** *nacl*] [*access-list-number* | *extended-access-list-number* | *access-list-name*]
4. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。

	コマンドまたはアクション	目的
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**snmp-server community** *community-string* [**view** *view-name*] [**ro** | **rw**] [**ipv6** *nacl*] [*access-list-number* | *extended-access-list-number* | *access-list-name*] 例： `Device(config)# snmp-server community mycommunity`	コミュニティ アクセス文字列を指定します。
ステップ 4	**end** 例： `Device(config)# end`	グローバル コンフィギュレーション モードを終了し、設定を保存して、特権 EXEC モードに戻ります。

コミュニティ アクセス文字列の指定に関する詳細については、『*SNMP Configuration Guide*』の「Configuring SNMP Support」モジュールを参照してください。**snmp-server community** コマンドに関する詳細（シンタックスと使用法に関するガイドラインを含む）については、『Cisco IOS SNMP Support Command Reference』を参照してください。

SNMP マネージャとの通信の有効化

KS の SNMP エージェントまたは GM と SNMP マネージャ間の通信を有効にするには、このタスクを実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **snmp-server host** {*hostname* | *ip-address*} **version** {**1** | **2c** | **3**} *community-string*
4. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例：	グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
	`Device# configure terminal`	
ステップ 3	**snmp-server host** {*hostname* | *ip-address*} **version** {**1** | **2c** | **3**} *community-string* 例： `Device(config)# snmp-server host 209.165.200.225 version 2c mycommunity`	ホストがSNMP通知を受信するように指定します。 • 2c は通常 SNMP バージョンとして使用されます。
ステップ 4	**end** 例： `Device(config)# end`	グローバル コンフィギュレーション モードを終了し、設定を保存して、特権 EXEC モードに戻ります。

SNMP マネージャとの通信を有効にする方法についての詳細は、『*SNMP Configuration Guide*』の「Configuring SNMP Support」モジュールを参照してください。**snmp-server host** コマンドに関する詳細（シンタックスと使用法に関するガイドラインを含む）については、『Cisco IOS SNMP Support Command Reference』を参照してください。

GDOI MIB 通知の有効化

KS または GM の GDOI MIB 通知を有効にするには、次の作業を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **snmp-server enable traps gdoi** [*notification-type*]
4. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 3	**snmp-server enable traps gdoi** [*notification-type*] 例： `Device(config)# snmp-server enable traps gdoi gm-registration-complete gm-rekey-rcvd ks-new-registration ks-reg-complete`	有効にする特定のSNMP通知を指定します。任意の順序で次の種類を組み合わせて指定できます。次のキーワードなしでコマンドを入力すると、すべてのGDOI MIB 通知が有効になります。 • **gm-incomplete-cfg**：設定が見つからないためGM がエラー通知を送信しました。 • **gm-re-register**：GM が KS で登録プロセスを開始しました。 • **gm-registration-complete**：GM が KS への登録を完了しました。 • **gm-rekey-fail**：キー再生成を正常に処理およびインストールできないため、GM がエラー通知を送信しました。 • **gm-rekey-rcvd**：GM がキー再生成メッセージを受信しました。 • **gm-start-registration**：GM が最初の登録要求をKS に送信しました。 • **ks-new-registration**：KS が最初の登録要求をGMから受信しました。 • **ks-no-rsa-keys**：RSA キーが見つからないためKS からのエラー通知を受信しました。 • **ks-reg-complete**：GM が KS への登録を完了しました。 • **ks-rekey-pushed**：KS からキー再生成メッセージが送信されました。 • **ks-gm-deleted**：GM が KS によって削除されます。 • **ks-peer-reachable**：到達不能な COOP ピアが到達可能になります。 • **ks-peer-unreachable**：到達可能な COOP ピアが到達不能になります。 • **ks-role-change**：KS の役割がプライマリからセカンダリ（またはその逆）に変更されます。

	コマンドまたはアクション	目的
ステップ 4	**end** 例： `Device(config)# end`	グローバル コンフィギュレーション モードを終了し、設定を保存して、特権 EXEC モードに戻ります。

GET VPN 用の GDOI MIB サポートの設定例

例：GDOI MIB をサポートするソフトウェア バージョンを GM が実行していることを確認する

次の例は、ネットワーク内のすべてのデバイスが GDOI MIB をサポートしているかどうかを確認するために KS（またはプライマリ KS）で GET VPN ソフトウェア バージョン管理コマンドを使用する方法を示します。

```
Device# show crypto gdoi feature gdoi-mib

Group Name: GET
 Key Server ID       Version   Feature Supported
    10.0.8.1         1.0.2          Yes
    10.0.9.1         1.0.2          Yes
    10.0.10.1        1.0.2          Yes
    10.0.11.1        1.0.2          Yes
 Group Member ID     Version   Feature Supported
    10.0.11.2          1.0.2          Yes
    10.0.11.3          1.0.1          No
```

次の例は、GDOI MIB をサポートしていないデバイスのみを検索する方法を示します。

```
Device# show crypto gdoi feature gdoi-mib | include No

       10.0.11.3          1.0.1          No
```

例：SNMP コミュニティのアクセス コントロールの作成

次の例では、SNMP へのアクセスを許可するために、KS または GM 上の SNMP マネージャと SNMP エージェント間の関係を定義するために mycommunity という名前の SNMP コミュニティ文字列を指定する方法を示します。

```
Device> enable
Device# configure terminal
Device(config)# snmp-server community mycommunity
Device(config)# end
```

例：SNMP マネージャとの通信の有効化

次に、SNMP マネージャとの通信を有効化する例を示します。この例では、すでに作成されている mycommunity という名前のコミュニティ文字列を使用します。

```
Device> enable
Device# configure terminal
Device(config)# snmp-server host 209.165.200.225 version 2c mycommunity
Device(config)# end
```

例：GDOI MIB 通知の有効化

次に、GDOI MIB 通知を有効化する例を示します。

```
Device> enable
Device# configure terminal
Device(config)# snmp-server enable traps gdoi gm-registration-complete gm-rekey-rcvd
ks-new-registration ks-reg-complete
Device(config)# end
```

GET VPN 用の GDOI MIB サポートのその他の参考資料

関連資料

関連項目	マニュアル タイトル
Cisco IOS セキュリティ コマンド	『*Cisco IOS Security Command References*』
SNMP の設定	• 『SNMP Configuration Guide, Cisco IOS Release 15.2M&T』の「Configuring SNMP Support」モジュール • 『Cisco IOS SNMP Support Command Reference』

MIB

MIB	MIB のリンク
CISCO-GDOI-MIB	選択したプラットフォーム、Cisco ソフトウェア リリース、およびフィーチャ セットの MIB を検索してダウンロードする場合は、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

シスコのテクニカル サポート

説明	リンク
右の URL にアクセスして、シスコのテクニカル サポートを最大限に活用してください。これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

GET VPN 用の GDOI MIB サポートの機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *293 : GET VPN* 用の *GDOI MIB* サポートの機能情報

機能名	リリース	機能情報
GET VPN の GDOI MIB サポート		この機能は、IETF RFC 6407『The Group Domain of Interpretation』用の MIB サポートを追加します。この機能は、GDOI MIB の IETF 標準に関連したオブジェクトのみをサポートします。またこの機能は、ネットワーク上のデバイスが GDOI MIB をサポートする GET VPN ソフトウェアのバージョンを実行しているかどうかを表示するコマンドも提供します。 GDOI MIB は、GDOI グループ、GM と KS ピア、および作成またはダウンロードされたポリシーに関する情報が含まれるオブジェクトと通知から構成されます。 次のコマンドが導入されました。 **snmp-server enable traps gdoi.**
XE 3.16 GETVPN GDOI/COOP MIBS		次のコマンドが変更されました。 **snmp-server enable traps gdoi.**

第 222 章

GET VPN の復元力

GET VPN の復元力機能では、Cisco Group Encrypted Transport（GET）VPN の復元力を改善し、エラーが発生したときのデータ トラフィックの中断を防止したり最小化したりします。

GET VPN の復元力の前提条件

この機能を有効にするすべてのキー サーバ（KS）およびグループ メンバー（GM）で、GET VPN ソフトウェア バージョン 1.0.4 以降を実行している必要があります。この機能は、GET VPN ネットワーク内のすべてのデバイスをこの機能をサポートする GET VPN ソフトウェア バージョンにアップグレードしてから使用する必要があります。この機能は、ネットワークのすべてのデバイスがこの機能をサポートするバージョンを実行しているかどうかを確認するために KS（またはプライマリ KS）で使用するコマンドを提供します。詳細については「*GM* が長い *SA* ライフタイムをサポートするソフトウェア バージョンを実行していることを確認する」セクションを参照してください。

GET VPN の復元力の制約事項

- すべてキー サーバ（KS）およびグループ メンバー（GM）は、長い SA ライフタイム向けにアップグレードする必要があります。

GET VPN の復元力に関する情報

長い SA ライフタイム

長いセキュリティアソシエーション（SA）ライフタイム機能では、Key Encryption Key（KEK）およびトラフィック暗号キー（TEK）の最大ライフタイムを 24 時間から 30 日に延長します。この機能により、スケジュールされた最後のキー再生成時に確認応答に応答しないグループメンバー（GM）に対して定期的なリマインダキー再生成を送信し続けるようにキーサーバ（KS）を設定することもできます。

定期的なリマインダキー再生成と長い SA ライフタイムを組み合わせて使用することにより、キーがロールオーバーする前にスケジュールされたキー再生成に失敗した場合、KS が効果的に GM を同期することができます。

（注） 24 時間より長いライフタイムでは、暗号化アルゴリズムを、128 ビット以上の AES キーを使用する Advanced Encryption Standard-Cipher Block Chaining（AES-CBC）または Advanced Encryption Standard-Galois/Counter Mode（AES-GCM）にする必要があります。

長い SA ライフタイム機能は GETVPN スイート B 機能とともに使用すると、GCM-AES と GMAC-AES でカプセル化されたパケットのグループでトラフィック暗号キー（TEK）ポリシーがトランスフォームされるときに AES-GSM および Galois Message Authentication Code-Advanced Encryption Standard（GMAC-AES）を使用できます。

長い SA ライフタイムへの移行

長い SA ライフタイム機能（1 日以上）に移行するときには、次のルールが適用されます。

- 長い SA ライフタイムが暗号 IPsec プロファイルに設定されているとき、GETVPN は非 Group Domain of Interpretation（GDOI）グループに対して IPsec プロファイルを使用しないように警告メッセージを表示します。
- グループメンバーが短い SA ライフタイムでキーサーバーに登録され、キーサーバーがポリシーを長い SA ライフタイムに変更する場合、GETVPN は **crypto gdoi ks rekey** コマンドを設定してポリシー変更を開始するときにすべての GM のソフトウェアバージョンをチェックします。KS に登録されている GM が長い SA ライフタイムをサポートしていない場合、すべての GM がアップグレードされるまでポリシーの変更を推奨しないというメッセージが表示されます。
- 長い SA 機能が KS で有効になると、この機能をサポートしていない古い Cisco IOS リリースを実行している GM からの登録がブロックされます。

クロック スキューの軽減

セキュリティアソシエーション（SA）のライフタイムが長いとき、グループメンバー（GM）は長期間、キーサーバから更新を受信しないことがあります。これにより、グループメンバーはKey Encryption Key（KEK）ライフタイム、トラフィック暗号キー（TEK）ライフタイム、および時間ベースアンチリプレイ（TBAR）疑似時間の間クロックスキューを経験することがあります。更新のキー再生成と新しい発信IPsec SAへのロールオーバーによってGMはクロックスキューの問題を軽減することができます。

更新のキー再生成

トラフィック暗号キー（TEK）のライフタイムが2日以上の期間に設定され、時間ベースのアンチリプレイ（TBAR）が無効である場合、キーサーバは24時間ごとに更新のキー再生成を送信し、すべてのグループメンバー（GM）のKey Encryption Key（KEK）ライフタイム、TEKライフタイム、およびTBAR疑似時間を更新します。簡単に言うと、更新のキー再生成は、最後のユニキャスト確認応答（ACK）の受信状態に関係ない、すべてのGMへの現在のKEKポリシー、TEKポリシー、およびTBAR疑似時間（有効な場合）の再送信です。TBARが有効な場合、更新のキー再生成は疑似時間を同期するために2時間ごとに送信され、追加の更新のキー再生成は必要ありません。

新しい発信 IPsec SA へのロールオーバー

長いSAライフタイム（1日を超える）が設定されている場合、トラフィック暗号キー（TEK）の残りのライフタイムが、下限が30秒のライフタイムに設定された古いTEKの1%に達し、古いTEKの残りのライフタイムの30秒でないとき、ロールオーバーが発生します。これにより、（他のGMが古いTEKを削除してから）1つのGMから新しいTEK遅延にロールオーバーされるトラフィックが破棄されるまで、グループメンバー（GM）間のより大きなクロックスキューが可能になります。これによって、長期間GMが「オフライン」（KSからの切断）になり、クロックスキューを軽減するための更新のキー再生成を受信できない問題が緩和されます。

定期的なリマインダ同期キー再生成

キーサーバ（KS）の定期的なリマインダ同期キー再生成機能を使用すると、スケジュールされている直前のキー再生成時に確認応答（ACK）に応答しないグループメンバー（GM）に対して定期的なリマインダキー再生成を送信できます。長いSAライフタイム機能とこの機能の組み合わせは、キーのロールオーバーの前にスケジュールされたキー再生成に失敗したGMとKSが同期するために有効です。KSグループ設定で、キー再生成の再送信を設定するときの**rekey retransmit**コマンドに新しいキーワード**periodic**が追加されています。

キー再生成の再送信と同様に、定期的な再送信はそれぞれシーケンス番号を増加させます。スケジュールされた3回のキー再生成（再送信ではない）でGMがACKを送信しないと、GMはKSのデータベースから削除されます。

事前配置されたキー再生成

長い SA ライフタイム（1 日を超える）が設定されているとき、事前配置されたキー再生成機能を使用すると、キーサーバー（KS）はSAライフタイムの半分の期間より先にキー再生成を送信できます。キー再生成の送信の通常な動作は短い SA ライフタイムに使用されます。グループ メンバー（GM）はこの早いキー再生成を受信すると、新しい TEK が発信としてロールオーバーされるまで、引き続き古い TEK を発信として使用します。事前配置されたキー再生成機能と長い SA ライフタイム機能の組み合わせはキーのロールオーバーの安定性を向上させます。この機能により、定期的なリマインダ キー再生成や同期キー再生成などのキー再生成エラーを回復するための十分な時間（KS）が確保されます。

GET VPN の復元力の設定方法

GM が長い SA ライフタイムをサポートするソフトウェア バージョンを実行していることを確認する

長いSAライフタイムは、GET VPNネットワーク内のすべてのデバイスをこの機能をサポートする GET VPN ソフトウェア バージョンにアップグレードしてから使用する必要があります。

ネットワーク内のすべてのデバイスが長い SA ライフタイムをサポートしていることを確認するには、キー サーバ（またはプライマリ キー サーバ）でこの作業を実行します。

手順の概要

1. **enable**
2. **show crypto gdoi feature long-sa-lifetime**
3. **show crypto gdoi feature long-sa-lifetime | include No**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**show crypto gdoi feature long-sa-lifetime** 例： `Device# show crypto gdoi feature long-sa-lifetime`	GET VPN ネットワーク内の各 KS および GM で実行されている GET VPN ソフトウェアのバージョンを表示し、そのデバイスが長い SA ライフタイムをサポートしているかどうかを表示します。
ステップ 3	**show crypto gdoi feature long-sa-lifetime | include No** 例： `Device# show crypto gdoi feature long-sa-lifetime | include No`	（オプション）長い SA ライフタイムをサポートしないデバイスのみ表示します。

長い SA ライフタイムの設定

TEK の長い SA ライフタイムの設定

トラフィック暗号キー（TEK）の長い SA ライフタイムを設定するには、次のステップを実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **crypto ipsec profile** *name*
4. **set security-association lifetime days** *days*
5. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**crypto ipsec profile** *name* 例： `Device(config)# crypto ipsec profile gdoi-p`	2 つの IPsec デバイス間における IPsec 暗号化で使用される IPsec パラメータを定義し、暗号化 IPsec プロファイル コンフィギュレーション モードを開始します。
ステップ 4	**set security-association lifetime days** *days* 例： `Device(ipsec-profile)# set security-association lifetime days 15`	セキュリティ アソシエーション（SA）のライフタイムを 1 日に設定します。 • 最大日数は 30 日です。
ステップ 5	**end** 例： `Device(ipsec-profile)# end`	暗号 IPsec プロファイル ピア コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

KEK の長い SA ライフタイムの設定

キー暗号キー（TEK）の長い SA ライフタイムを設定するには、次のステップを実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **crypto gdoi group** *group-name*
4. **identity number** *number*
5. **server local**
6. **rekey lifetime days** *days*
7. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**crypto gdoi group** *group-name* 例： `Device(config)# crypto gdoi group GET`	GDOI グループを指定し、GDOI グループ コンフィギュレーション モードを開始します。
ステップ 4	**identity number** *number* 例： `Device(config-gdoi-group)# identity number 3333`	GDOI グループ番号を指定します。
ステップ 5	**server local** 例： `Device(config-gdoi-group)# server local`	デバイスを GDOI キー サーバとして指定し、GDOI ローカル サーバ コンフィギュレーション モードを開始します。
ステップ 6	**rekey lifetime days** *days* 例： `Device(gdoi-local-server)# rekey lifetime days 20`	KEK の日数または秒数を制限します。
ステップ 7	**end** 例： `Device(gdoi-local-server)# end`	GDOI ローカル サーバ コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

定期的なリマインダ同期キー再生成の設定

定期的なリマインダ同期キー再生成を設定するには、次のステップを実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **crypto gdoi group** *group-name*
4. **identity number** *number*
5. **server local**
6. **rekey retransmit** *number-of-seconds* **periodic**
7. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**crypto gdoi group** *group-name* 例： `Device(config)# crypto gdoi group group1`	GDOI グループを指定し、GDOI グループ コンフィギュレーション モードを開始します。
ステップ 4	**identity number** *number* 例： `Device(config-gdoi-group)# identity number 3333`	GDOI グループ番号を指定します。
ステップ 5	**server local** 例： `Device(config-gdoi-group)# server local`	デバイスを GDOI キー サーバとして指定し、GDOI ローカル サーバ コンフィギュレーション モードを開始します。
ステップ 6	**rekey retransmit** *number-of-seconds* **periodic** 例： `Device(gdoi-local-server)# rekey retransmit 10 periodic`	キー再生成メッセージが定期的に再送信される回数を指定します。 • このコマンドが設定されていない場合、再送信は行われません。
ステップ 7	**end** 例： `Device(gdoi-local-server)# end`	GDOI ローカル サーバ コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

GET VPN の復元力の確認とトラブルシューティング

キー サーバの GET VPN の復元力の確認とトラブルシューティング

キーサーバー（KS）で実行されている設定を表示するには、**show running-config** コマンドと次のコマンドを使用します。

手順の概要

1. **enable**
2. **show crypto gdoi**
3. **show crypto gdoi ks rekey**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device# enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**show crypto gdoi** 例： `Device# show crypto gdoi`	現在の GDOI 構成、および KS からダウンロードされたポリシーを表示します。
ステップ 3	**show crypto gdoi ks rekey** 例： `Device#  show crypto gdoi ks rekey`	KS から送信されるキー再生成に関する情報を表示します。

グループ メンバーの GET VPN の復元力の確認とトラブルシューティング

グループメンバー（GM）で実行されている設定を表示するには、**show running-config** コマンドと次のコマンドを使用します。

手順の概要

1. **enable**
2. **show crypto gdoi ks rekey**
3. **show crypto gdoi ks policy**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device# enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。

	コマンドまたはアクション	目的
ステップ 2	**show crypto gdoi ks rekey** 例： `Device# show crypto gdoi ks rekey`	KS から送信されるキー再生成に関する情報を表示します。
ステップ 3	**show crypto gdoi ks policy** 例： `Device# show crypto gdoi ks policy`	次のキー再生成までの時間を表示します。

GET VPN 復元力の設定例

例：GMが長いSAライフタイムをサポートするソフトウェアバージョンを実行していることを確認する

次の例は、各グループ内のすべてのデバイスが長い SA ライフタイムをサポートしているかどうかを確認するために KS（またはプライマリ KS）で GET VPN ソフトウェア バージョン管理コマンドを使用する方法を示します。

```
Device# show crypto gdoi feature long-sa-lifetime

Group Name: GETVPN
    Key Server ID       Version   Feature Supported
        10.0.5.2         1.0.4          Yes
        10.0.6.2         1.0.4          Yes
        10.0.7.2         1.0.3          No
        10.0.8.2         1.0.2          No

    Group Member ID     Version   Feature Supported
        10.0.1.2         1.0.2          No
        10.0.2.5         1.0.3          No
        10.0.3.1         1.0.4          Yes
        10.0.3.2         1.0.4          Yes
```

また、上記のコマンドは GM でも入力できます（その GM の情報を表示します。KS や他の GM には使用できません）。

次の例は、KS（プライマリ KS）で長い SA ライフタイムをサポートしていない GET VPN ネットワークのデバイスのみ検索するコマンドを入力する方法を示しています。

```
Device# show crypto gdoi feature long-sa-lifetime | include No

        10.0.7.2         1.0.3          No
        10.0.8.2         1.0.2          No
        10.0.1.2         1.0.2          No
        10.0.2.5         1.0.3          No
```

例：長い SA ライフタイムの設定

例：TEK の長い SA ライフタイムの設定

次に、トラフィック暗号キー（TEK）の長い SA ライフタイムの設定方法の例を示します。

```
Device> enable
Device# configure terminal
Device(config)# crypto ipsec profile gdoi-p
Device(ipsec-profile)# set security-association lifetime days 15
Device(ipsec-profile)# end
```

例：KEK の長い SA ライフタイムの設定

次に、キー暗号キー（KEK）の長い SA ライフタイムの設定方法の例を示します。

```
Device> enable
Device# configure terminal
Device(config)# crypto gdoi group GET
Device(config-gdoi-group)# identity number 3333
Device(config-gdoi-group)# server local
Device(gdoi-local-server)# rekey lifetime days 20
Device(gdoi-local-server)# end
```

例：定期的なリマインダ同期キー再生成の設定

次に、定期的なリマインダ同期キー再生成の設定方法の例を示します。

```
Device> enable
Device# configure terminal
Device(config)# crypto gdoi group group1
Device(config-gdoi-group)# identity number 3333
Device(config-gdoi-group)# server local
Device(gdoi-local-server)# rekey retransmit 10 periodic
Device(gdoi-local-server)# end
```

GET VPN の復元力のその他の参考資料

関連資料

関連項目	マニュアル タイトル

関連項目	マニュアル タイトル
Cisco IOS セキュリティ コマンド	• 『*Cisco IOS Security Command Reference Commands A to C*』 • 『*Cisco IOS Security Command Reference Commands D to L*』 • 『*Cisco IOS Security Command Reference Commands M to R*』 • 『*Cisco IOS Security Command Reference Commands S to Z*』
エンタープライズ ネットワークの GET VPN の有効化のための基本的な導入ガイドライン	『*Cisco IOS GET VPN Solutions Deployment Guide*』
GET VPN ネットワークの設計と実装	『*Group Encrypted Transport VPN (GETVPN) Design and Implementation Guide*』

標準および RFC

標準/RFC	タイトル
RFC 2401	『*Security Architecture for the Internet Protocol*』
RFC 6407	『*The Group Domain of Interpretation*』

シスコのテクニカル サポート

説明	リンク
右の URL にアクセスして、シスコのテクニカル サポートを最大限に活用してください。これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

GET VPN の復元力の機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだ

けを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *294 : GET VPN* の復元力の機能情報

機能名	リリース	機能情報
GET VPN の復元力		次のコマンドが導入または変更されました。 **rekey lifetime, rekey retransmit, set security-association lifetime, show crypto gdoi.**

第 223 章

GETVPN 復元力 GM - エラー検出

GETVPN 復元力 - GM エラー検出機能では、無効なステートフル パケット インスペクション（SPI）または時間ベースのアンチリプレイ（TBAR）エラーなど、各グループ ドメイン オブ インタープリテーション（GDOI）のデータ プレーンで異常なパケットを検出します。これらのエラーは追跡され、パケットの外部送信元 IP アドレスが記録されます。

GETVPN の復元力：GM のエラー検出に関する情報

エラー処理

エラー処理を機能させるには、GM と KS の両方で GETVPN の復元力（GM のエラー検出の機能）を有効にする必要があります。KS は、SPI（セキュリティ パラメータ インデックス）のグループ情報をエンコードし、TEK ポリシーを介してそれを GM にダウンロードします。

GETVPN 復元力 - GM エラー検出機能によって障害が検出されると、異常なパケットの送信元 IP アドレスを示す syslog メッセージが生成されます。

```
 *Feb 10 21:01:56.043:
%GDOI-4-TIMEBASED_REPLAY_FAILED: An anti replay check has failed in
group GETVPN from sourceip-address
100.0.0.9.
 my_pseudotime is 600006.78 secs,
peer_pseudotime is 500033.34 secs, replay_window is 100
(second)
 *Feb 10 21:01:56.043:
%CRYPTO-4-PKT_REPLAY_ERR: decrypt: replay check failed
 connection id=29, sequence
number=11
```

show crypto gdoi gm コマンドは、直近の 50 個の時間ベースのアンチリプレイ（TBAR）エラーの履歴を表示します。これらの送信元 IP アドレス レコードを使用すると、送信者グループ メ

ンバー（GM）を突き止め、既存のハードウェアまたはソフトウェアの問題を調査することができます。次の統計情報もコマンドで利用できます。

- GM リカバリ機能のオン/オフ
- リカバリの間隔
- 適用される GM リカバリの再登録の数

エラーが発生すると、GM は次に使用可能なキー サーバ（KS）に再登録し、最新のポリシーとキーを取得し、登録が完了するまで以前にダウンロードされたすべてのグループ ポリシーとキーを維持します。

たとえば、連携キー サーバ（COOP KS）の分割が発生すると、レベルを上げられた各 KS が独自の Key Encryption Key（KEK）とトラフィック暗号化キー（TEK）を生成します。GM は、無効な SPI パケットを受信すると、それをデコードします（KS は SPI のグループ情報をエンコードし、TEK ポリシーを介してそれを GM にダウンロードします）。それが現在の GETVPN グループに属していることが判明した場合は、リカバリ登録を開始します。

無効な SPI は、次の 2 つのカテゴリのいずれかに属している可能性があります。

- 正の無効な SPI：現在のグループに属しており、GM リカバリ登録が必要な、無効な SPI。
- 負の無効な SPI：リカバリ登録を必要としない無効な SPI。

正の無効な SPI の場合、リスト内の次のキーサーバー（KS）へのリカバリ登録が実行されます。このリカバリ登録は、リスト内の次の KS への各クライアント リカバリ間隔で、無効なステートフル パケット インスペクション（SPI）パケットまたは TBAR エラーごとに繰り返されます。リスト内のすべての KS が回復され、無効な SPI が含まれなくなると、その SPI は誤検出としてマークされ、それ以上のリカバリ登録は実行されません。KS は TBAR エラーに対して常にリカバリ登録を実行します。ただし、無効な SPI のために GM がリストのすべての KS を回復し、SPI がある KS がなくなると、その SPI は誤検出としてマークされ、その SPI のためにさらにリカバリ登録が実行されることはなくなります。

この GM リカバリの再登録機能がトリガーされたことを通知するため、syslog メッセージが生成されます。たとえば、GM が 300 秒ごとにコントロール プレーンのエラーをモニタするように設定している場合、リカバリ登録が発生すると、次の syslog が生成されます。

```
*Feb 23 19:06:28.600: %GDOI-5-GM_RECOVERY_REGISTER: received invalid GDOI packets;
register to KS to refresh policy, keys, and PST.
```

GETVPN の復元力：GM のエラー検出の設定方法

GETVPN の復元力：GM のエラー検出の設定

手順の概要

1. **crypto gdoi group** *group-name*
2. **identity number** *number*

3. **server address ipv4** *address*
4. **client recovery-check interval** *interval*
5. **exit**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**crypto gdoi group** *group-name* 例： `Device(config)# crypto gdoi group GETVPN`	グループ ドメイン オブ インタープリテーション（GDOI）グループを作成し、GDOI グループ コンフィギュレーション モードを開始します。
ステップ 2	**identity number** *number* 例： `Device(config-gdoi-group)# identity number 1111`	GDOI グループ番号を指定します。
ステップ 3	**server address ipv4** *address* 例： `Device(config-gdoi-group)# server address ipv4 1.0.0.2`	GDOI グループが到達しようとするサーバの IP アドレスを指定します。
ステップ 4	**client recovery-check interval** *interval* 例： `Device(config-gdoi-group)# client recovery-check interval 300`	コントロール プレーンを監視するクライアント グループ メンバー（GM）の時間間隔を設定します。
ステップ 5	**exit** 例： `Device(config-gdoi-group)# exit`	GDOI グループ コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードに戻ります。

GETVPN の復元力：GM のエラー検出の設定例

例：GETVPN の復元力：GM のエラー検出の設定

次の例は、グループ メンバー（GM）が 300 秒ごとにコントロール プレーンのエラーを監視できるようにする方法を示します。

```
crypto gdoi group GETVPN
 identity number 1111
 server address ipv4 1.0.0.2
 client recovery-check interval 300
```

GETVPN の復元力：GM のエラー検出その他の参考資料

関連資料

関連項目	マニュアル タイトル
Cisco IOS セキュリティ コマンド	『*Cisco IOS Security Command References*』
エンタープライズ ネットワークの GET VPN の有効化のための基本的な導入ガイドライン	『*Cisco IOS GET VPN Solutions Deployment Guide*』
GET VPN ネットワークの設計と実装	『*Group Encrypted Transport VPN (GETVPN) Design and Implementation Guide*』

標準および RFC

標準/RFC	タイトル
RFC 6407	『*The Group Domain of Interpretation*』

シスコのテクニカル サポート

説明	リンク
右の URL にアクセスして、シスコのテクニカル サポートを最大限に活用してください。これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

GETVPN の復元力：GM のエラー検出の機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *295 : GETVPN* の復元力：*GM* のエラー検出の機能情報

機能名	リリース	機能情報
GETVPN の復元力：GM のエラー検出		各 GDOI グループのデータ プレーンのエラー パケットを検出します。 次のコマンドが導入されました。 **client recovery-check interval.**

第 224 章

GETVPN CRL チェック

Group Encrypted Transport VPN（GET VPN）プロセスの間、証明書は認証局（CA）から受信され、アイデンティティの証明として使用されます。証明書は、キーのセキュリティ侵害や証明書の喪失など、さまざまな理由により失効する可能性があります。失効した証明書はリポジトリに定期的に発行される証明書失効リスト（CRL）に配置されます。このリストは設定済みの CRL ライフタイムで指定された期間、リポジトリに格納されます。数時間から数日の任意の期間にすることができます。

GETVPN CRL チェックに関する情報

インターネット キー エクスチェンジ（IKE）では、証明書は 2 台のピア間でセッションが確立されるときに検証されます。現在のセッションは証明書失効の影響を受けません。ただし、新しいセッションを確立することはできず、グループ メンバーがキー サーバ（KS）に再登録しない限り証明書は再検証されません。

GETVPN CRL チェック機能では、設定されたトラストポイントで新しい CRL が利用可能なときに公開キー インフラストラクチャ（PKI）がグループ ドメイン オブ インタープリテーション（GDOI）KS に通知することができます。その後 KS は新しい Key Encryption Key（KEK）を作成し、グループ メンバーデバイスに再認証メッセージを送信します。これにより、syslog メッセージが出力され、現在の KEK が削除され、KS に再登録されます。

連携キー サーバのプロトコル統合

連携キー サーバのプロトコル（COOP）は、VPN ネットワークに複数のキー サーバ（KS）を設定できるようにする GET VPN の機能です。KS 冗長性のために使用されます。

すべての KS でグループ メンバー（GM）の再認証を有効にすることで、GETVPN CRL チェックは COOP と統合されます。ただし、連携 KS 間で一時的に接続が失われる場合、COOP 分割が発生する可能性は常にあります。

再認証がトリガーされたときの COOP 分割なし

COOP 分割が発生しない場合、プライマリ GM デバイスはセカンダリ KS の Key Encryption Key（KEK）を削除し、GM に再認証メッセージを送信します。セカンダリ KS は GM が再登録を開始する前に現在のポリシーをプライマリ ポリシーと同期させます。すべての GM が使用可能な KS に再登録して再認証され、新しい KEK を受信します。

再認証がトリガーされたときの COOP 分割

再認証がトリガーされる前に COOP 分割が発生し、2 つのプライマリ KS しかない場合、両者が再認証メッセージを送信します。それぞれのプライマリ KS は異なる新しい KEK を作成します。GM は、メッセージを受信するとすぐに既存の KEK をすべて削除するため、受信する最初の再認証メッセージだけを理解します。GM は使用可能な KS に再登録し、CRL チェックが行われます。再登録のとき、GM が登録した KS に応じて GM は最初のプライマリの KEK または 2 番目のプライマリの KEK のいずれかを受け取ります。GM はその KEK をインストールし、そのプライマリ KS からのみ今後のキー再生成を受信します。COOP マージが発生すると、KS はポリシーを同期し、キー再生成を送信して、すべての GM が最新の KEK とトラフィック暗号キー（TEK）を持つようにします。

異なる KEK の作成の回避

COOP 分割中に再認証がトリガーされる場合も、再認証と CRL チェックは依然として発生します。ただし、KS での異なる KEK の作成をトリガーすることは、再認証を遅らすことによって回避できます。プライマリ KS はすべての COOP KS に到達可能な（分割されない）場合にのみ、再認証を開始します。1 つの COOP KS に到達できない場合、プライマリ KS はすべての COOP KS が到達可能になるまで再認証メッセージの送信を遅らせます。

GETVPN CRL チェックの設定方法

GETVPN CRL チェック機能を有効にする前に、複数のコンポーネントを設定する必要があります。次の作業を行います。

- グループ メンバーとキー サーバが PKI クライアントとなるために定義された公開キー インフラストラクチャ（PKI）認証局（CA）（証明書を取得するように登録する必要があります）。
- PKI での証明書失効リスト（CRL）チェックを有効にするように設定されたキー サーバ（KS）。
- CA で利用可能であり、最初に必要なときに CRL をダウンロードするように設定された KS。これは、新しい CRL が利用可能になった後に最初のグループ メンバー（GM）登録に続いて KS が CRL をダウンロードすることを意味します。「GETVPN CRL チェックのためのキー サーバの設定」セクションを参照してください。

- PKI のグループ メンバー デバイスで無効化された CRL チェック。「グループ メンバーでの CRL チェックの無効化」セクションを参照してください。
- 証明書に対して設定されたインターネット キー エクスチェンジ（IKE）認証。「証明書の IKE 認証の設定」セクションを参照してください。

GETVPN CRL チェックのためのキー サーバの設定

新しい CRL が認証局（CA）で利用可能になった後に最初のグループ メンバー（GM）登録が発生した場合にキー サーバ（KS）が証明書失効リスト（CRL）をダウンロードするように設定するには、次のステップを実行します。

手順の概要

1. **ip domain name** *name*
2. **ip http server**
3. **crypto pki trustpoint** *name*
4. **enrollment url** *url*
5. **revocation-check** *method*
6. **exit**
7. **crypto identity** *method*
8. **fqdn** *domain*
9. **fqdn** *domain*
10. **exit**
11. **crypto gdoi group** *group-name*
12. **server local**
13. **authorization identity** *name*
14. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**ip domain name** *name* 例： `Device(config)# ip domain name cisco.com`	Cisco IOS ソフトウェアが未修飾ホスト名（ドット付き 10 進ドメイン名を含まない名前）を作成するときに使用するデフォルトのドメイン名を定義します。
ステップ 2	**ip http server** 例： `Device(config)# ip http server`	IP または IPv6 システム上の HTTP サーバを有効化します。

	コマンドまたはアクション	目的
ステップ 3	**crypto pki trustpoint** *name* 例： `Device(config)# crypto pki trustpoint mycert`	デバイスで使用するトラストポイントを定義し、CA トラストポイント コンフィギュレーション モードを開始します。
ステップ 4	**enrollment url** *url* 例： `Device(config-ca-trustpoint)# enrollment url http://10.1.3.1:80`	CA の登録 URL を指定します。
ステップ 5	**revocation-check** *method* 例： `Device(config-ca-trustpoint)# revocation-check crl`	CRL による証明書チェックが行われることを確認します。
ステップ 6	**exit** 例： `Device(config-ca-trustpoint)# exit`	CA トラストポイント コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードに戻ります。
ステップ 7	**crypto identity** *method* 例： `Device(config)# crypto identity abcd`	デバイスの証明書内にある指定の識別名（DN）リストを使用してデバイスのアイデンティティを設定し、暗号アイデンティティ コンフィギュレーション モードを開始します。 （注） 特定の証明書、特に特定の DN の証明書を使用して、ピアが指定された暗号化インターフェイスにアクセスしないようにするデバイス構成の制限を設定できます。
ステップ 8	**fqdn** *domain* 例： `Device(config-crypto-identity)# fqdn ut01-unix5.cisco.com`	GM の完全修飾ドメイン名（FQDN）のリモート アイデンティティからネーム マングラーを取得します。
ステップ 9	**fqdn** *domain* 例： `Device(config-crypto-identity)# fqdn ut01-unix6.cisco.com`	次の GM の FQDN のリモート アイデンティティからネーム マングラーを取得します。

	コマンドまたはアクション	目的
ステップ 10	**exit** 例： `Device(config-crypto-identity)# exit`	暗号アイデンティティ コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードに戻ります。
ステップ 11	**crypto gdoi group** *group-name* 例： `Device(config)# crypto gdoi group gdoi-group1`	グループ ドメイン オブ インタープリテーション（GDOI）グループを作成し、GDOI グループ コンフィギュレーション モードを開始します。
ステップ 12	**server local** 例： `Device(config-gdoi-group)# server local`	デバイスを GDOI キー サーバとして指定し、GDOI ローカル サーバ コンフィギュレーション モードを開始します。
ステップ 13	**authorization identity** *name* 例： `Device(config-gdoi-local-server)# authorization identity abcd`	識別名（DN）または FQDN に基づいて GDOI グループの認証アイデンティティを指定します。
ステップ 14	**end** 例： `Device(config-gdoi-local-server)# end`	GDOI ローカル サーバ コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

グループ メンバーでの CRL チェックの無効化

Public Key Infrastructure（PKI）のグループ メンバー（GM）をチェックする証明書失効リスト（CRL）を無効にするには、次のステップを実行してください。

手順の概要

1. **ip domain name** *name*
2. **ip http server**
3. **crypto pki trustpoint** *name*
4. **enrollment url** *url*
5. **revocation-check** *method*
6. **exit**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**ip domain name** *name* 例： `Device(config)# ip domain name cisco.com`	Cisco IOS ソフトウェアが未修飾ホスト名（ドット付き 10 進ドメイン名を含まない名前）を作成するときに使用するデフォルトのドメイン名を定義します。
ステップ 2	**ip http server** 例： `Device(config)# ip http server`	IP または IPv6 システム上の HTTP サーバを有効化します。
ステップ 3	**crypto pki trustpoint** *name* 例： `Device(config)# crypto pki trustpoint mycert`	デバイスで使用するトラストポイントを定義し、CA トラストポイント コンフィギュレーション モードを開始します。
ステップ 4	**enrollment url** *url* 例： `Device(config-ca-trustpoint)# enrollment url http://10.1.3.1:80`	認証局（CA）の登録 URL を指定します。
ステップ 5	**revocation-check** *method* 例： `Device(config-ca-trustpoint)# revocation-check none`	GM の証明書チェックを無効にします。
ステップ 6	**exit** 例： `Device(config-ca-trustpoint)# exit`	CA トラストポイント モードを終了し、グローバル コンフィギュレーション モードに戻ります。

証明書の IKE 認証の設定

手順の概要

1. **crypto isakmp policy** *priority*
2. **no authentication pre-share**
3. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**crypto isakmp policy** *priority* 例： `Router(config)# crypto isakmp policy 1`	インターネット キー エクスチェンジ（IKE）ポリシーを定義して、ISAKMP ポリシー コンフィギュレーション モードを開始します。
ステップ 2	**no authentication pre-share** 例： `Router(config-isakmp)# no authentication pre-share`	IKE ポリシー内の認証方式をデフォルト値にリセットします。
ステップ 3	**end** 例： `Router(config)# end`	特権 EXEC モードに戻ります。

キー サーバでの GETVPN CRL チェックの有効化

新しい証明書失効リスト（CRL）が設定されているトラストポイント認証局（CA）で利用可能になったときに Public Key Infrastructure（PKI）がドメイン オブ インタープリテーション（GDOI）キー サーバ（KS）に通知するように設定するには、次のステップを実行します。

手順の概要

1. **crypto gdoi group** *group-name*
2. **server local**
3. **registration periodic crl trustpoint** *trustpoint-name*
4. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**crypto gdoi group** *group-name* 例： `Device(config)# crypto gdoi group gdoi_group1`	GDOI グループを作成し、GDOI グループ コンフィギュレーション モードを開始します。
ステップ 2	**server local** 例： `Device(config-gdoi-group)# server local`	デバイスを GDOI キー サーバとして指定し、GDOI ローカル サーバ コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 3	**registration periodic crl trustpoint** *trustpoint-name* 例： `Device(config-gdoi-local-server)# registration periodic crl trustpoint mycert`	設定されている PKI トラストポイント認証局で新しい CRL が使用可能になったときに GDOI KS の定期的な登録を有効にします。
ステップ 4	**end** 例： `Device(config-gdoi-local-server)# end`	GDOI ローカル サーバ モードを終了し、特権 EXEC モードに戻ります。

GETVPN CRL チェックの設定例

例：GETVPN CRL チェックの有効化

次の例は、すべての必須の事前設定を含めた、GETVPN CRL チェック機能を有効にする方法を示します。

例：GETVPN CRL チェックのためのキー サーバの設定

次の例では、新しい CRL が mycert という名前のトラストポイントの認証局（CA）で利用可能になった後に最初のグループ メンバー登録が発生すると、キー サーバ（KS）が証明書失効リスト（CRL）をダウンロードするように設定されます。

```
ip domain name cisco.com
ip http server
crypto pki trustpoint mycert
 enrollment url http://10.1.3.1:80
 revocation-check crl

crypto identity abcd
 fqdn ut01-unix5.cisco.com
 fqdn ut01-unix6.cisco.com

crypto gdoi group gdoi-group1
 server local
 authorization identity abcd
```

例：グループ メンバーでの CRL チェックの無効化

次の例では、Public Key Infrastructure（PKI）のグループ メンバー（GM）の CRL チェックが無効化されます。

```
ip domain name cisco.com
ip http server
crypto pki trustpoint mycert
```

```
 enrollment url http://10.1.3.1:80
 revocation-check none
```

例：証明書の IKE 認証の設定

```
crypto isakmp policy 1
 no authentication pre-share
```

例：キー サーバの GETVPN CRL チェックの有効化

次の例では、新しい CRL が mycert という名前のトラストポイント CA で利用可能になると、PKI が group1 という名前の GDOI KS に通知するように設定されます。

```
Crypto gdoi group gdoi_group1
 Server local
  registration periodic crl trustpoint mycert
```

GETVPN CRL チェックに関する追加情報

関連資料

関連項目	マニュアル タイトル
Cisco IOS セキュリティ コマンド	『*Cisco IOS Security Command References*』
エンタープライズ ネットワークの GET VPN の有効化のための基本的な導入ガイドライン	『*Cisco IOS GETVPN Solution Deployment Guide*』
GET VPN ネットワークの設計と実装	『*Group Encrypted Transport VPN (GETVPN) Design and Implementation Guide*』

標準および RFC

標準/RFC	タイトル
RFC 2401	『*Security Architecture for the Internet Protocol*』
RFC 6407	『*The Group Domain of Interpretation*』

シスコのテクニカル サポート

説明	リンク
右の URL にアクセスして、シスコのテクニカル サポートを最大限に活用してください。これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

GETVPN CRL チェックに関する機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *296 : GETVPN CRL* チェックに関する機能情報

機能名	リリース	機能情報
GETVPN CRL チェック		新しい証明書失効リスト（CRL）が設定されているトラストポイントで利用可能になったときに Public Key Infrastructure（PKI）がドメイン オブ インタープリテーション（GDOI）キー サーバ（KS）に通知できるようにします。 次のコマンドが導入されました。 **registration periodic crl trustpoint.**

第 225 章

スイート B での GET VPN のサポート

スイート B での GET VPN のサポート機能では、Cisco Group Encrypted Transport（GET）VPN に対してスイート B の暗号方式セットのサポートが追加されます。スイート B は、Galois Counter Mode Advanced Encryption Standard（GCM-AES）を含む暗号化アルゴリズムとハッシュ、デジタル署名、キー交換用のアルゴリズムのセットです。

IP Security（IPsec）VPN のスイート B は、RFC 4869、『Suite B Cryptographic Suites for IPsec』でその使用が定義されている標準規格です。スイート B は Cisco IPsec VPN に包括的なセキュリティ拡張機能を提供し、大規模な展開に対して追加のセキュリティを有効にします。スイート B は、リモート サイト間のワイドエリア ネットワーク（WAN）に高度な暗号化セキュリティを必要とする組織に対して推奨されるソリューションです。

スイート B での GET VPN のサポートの前提条件

この機能を有効にするすべてのキー サーバ（KS）およびグループ メンバー（GM）で、GET VPN ソフトウェア バージョン 1.0.4 以降を実行している必要があります。この機能は、GET VPN ネットワーク内のすべてのデバイスをこの機能をサポートする GET VPN ソフトウェア バージョンにアップグレードしてから使用する必要があります。この機能は、ネットワークのすべてのデバイスがスイート B をサポートするバージョンであるかどうかを確認するために KS（またはプライマリ KS）で使用するコマンドを提供します。詳細については「GM がスイート B をサポートするソフトウェア バージョンを実行していることを確認する」セクションを参照してください。

スイート B での GET VPN のサポートの制約事項

これらが GCM ポリシーまたはガロア メッセージ認証コード（GMAC）トラフィック暗号キー（TEK）ポリシーを使用している場合、グループのすべての連携 KS で同一順序の同一の ACL エントリ（ACE）を持つアクセス コントロール リスト（ACL）を使用する必要があります。そうでない場合、別の KS に登録する GM は、ポリシーのダウンロード後は正しく暗号化および復号化することができません。これは、スイート B では、SPI（TEK に関連付けられているセキュリティ パラメータ インデックス ID）が各 ACL エントリに対して生成され、各 ACL エントリに対して一意であるためです。

既存の ACL のエントリの順序を変更することはできません。したがって、GCM または GMAC TEK ポリシーを使用していて、各 KS に同一順序の同一エントリを持つように各 KS の ACL を更新する必要がある場合は、各セカンダリ KS から ACL を削除し、プライマリ KS で新しい ACL を作成し、セカンダリ KS にそれをコピーしてから、プライマリ KS で **crypto gdoi ks rekey** コマンドを入力して GET VPN ネットワーク全体のキー再生成をトリガーする必要があります。

ip access-list コマンドの **no** 形式（IPv6 を使用している場合は **ipv6 access-list** コマンドの **no** 形式）を使用して ACL を削除します。

Cisco Catalyst 8000 シリーズ エッジ プラットフォームは、GET VPN の Suite B をサポートしていません。Suite B は、次の Cisco ASR 1000 シリーズ アグリゲーション サービス ルータおよび Cisco 4000 シリーズ サービス統合型ルータでのみサポートされています。

表 *297 : GET VEPN Suite B* のサポート

プラットフォーム	モデル	GET VPN Suite B
Cisco ASR 1000 シリーズ アグリゲーション サービス ルータ	ASR1001-X	対応
	ASR1002-X	対応
	ASR1001-HX	対応
	ASR1002-HX	対応
	ESP100	対応
	ESP200	対応
Cisco 4000 シリーズ サービス統合型ルータ	ISR 4461	対応
	ISR4451-X	対応
	ISR4431	対応

スイート B での GET VPN のサポートに関する情報

スイート B

スイート B は国家安全保障局（NSA）と国立標準技術研究所（NIST）によって標準化されています。スイート B での GET VPN のサポート機能では、これらの暗号化アルゴリズムが GDOI および GET VPN とさまざまな方法（SHA-2/HMAC-SHA-2 と AEC-GCM/AES-GMAC の使用など）で使用できるようにします。

セキュア ハッシュ アルゴリズム 2（SHA-2）は、米国の連邦情報処理標準（FIPS）として NSA により設計され、NIST によって公開された一連の暗号ハッシュ関数（SHA-224、SHA-256、SHA-384、および SHA-512）です。SHA-2 には旧モデル SHA-1 からの多数の変更が含まれます。SHA-2 は 224、256、384、または 512 ビットのダイジェストを含む 4 つのハッシュ関数のセットで構成されます。

HMAC は反復暗号ハッシュ関数を使用するメッセージ認証のメカニズムです。HMAC-SHA-2 は、IPsec の秘密共有キーと組み合わせた SHA-2 バージョン（SHA-224、SHA-256、SHA-384 および SHA-512）反復暗号ハッシュ関数と組み合わせて使用される HMAC です。これらの組み合わせにより、HMAC-SHA-224、HMAC-SHA-256、HMAC-SHA-384、HMAC-SHA-512 と呼ばれます。これらのアルゴリズムは、認証ヘッダー（AH）（ただし GET VPN でサポートされていません）、Encapsulating Security Payload（ESP）、IKE、および IKEv2 プロトコルのデータ発信元の認証および整合性の基礎として、および IKE および IKEv2 の Pseudo-Random Function（PRF）としても使用できます。

GCM を使用する AES（AES-GCM）は、IPsec の暗号化アルゴリズムです。Galois メッセージ認証コードを使用する AES（AES-GMAC）もまた、IPsec に使用されるメッセージの整合性アルゴリズムです。

SHA-2 および HMAC-SHA-2

スイート B での GET VPN のサポート機能では、ハッシュおよび署名アルゴリズムとして SHA-2 および HMAC-SHA-2（HMAC-SHA-256、384、および 512）を使用することができます。256、384、および 512 ビット キーによる SHA-2 および HMAC-SHA-2 は次に使用されます。

- RFC 6407、『The Group Domain of Interpretation』の セクション 3.2（KS と GM 間の認証）で説明されているハッシュアルゴリズムとして IKEv1 を使用する GDOI 登録。
- KS からのキー再生成メッセージの認証および GM からの確認応答メッセージの認証のためのキー再生成メッセージをハッシュ化する Key Encryption Key（KEK）キー再生成ポリシー。
- IPsec SA 整合性チェックのための HMAC-SHA-2 の TEK IPsec ポリシー。

AES-GCM と AEC-GMAC

256、384、および 512 ビット キーによる AES-GCM（AES-GCM-128、192、および 256）および AES-GMAC（AES-GMAC-128、192、および 256）暗号化アルゴリズムは、IPsec SA 暗号化および整合性アルゴリズムとして TEK IPsec ポリシーで使用されます。GCM は暗号化および整合性に使用され、GMAC は整合性のみに使用されます。

スイート B に準拠する暗号化アルゴリズムのセット

RFC 4869 には IKE および IPsec を使用する 4 セットの暗号化アルゴリズムが定義されています。設定すると、これらのいずれかのセットがスイート B に準拠します。各セットは、暗号化アルゴリズム、デジタル署名アルゴリズム、キー アグリーメント アルゴリズム、およびハッシュまたはメッセージ ダイジェスト アルゴリズムで構成されます。

- Suite-B-GCM-128：128 ビット AES-GCM を使用して ESP の整合性の保護と機密性を提供します（RFC 4106、『The Use of Galois/Counter Mode (GCM) in IPsec Encapsulating Security Payload (ESP)』を参照してください）。ESP の整合性の保護および暗号化が両方必要な場合はこのスイートまたは Suite-B-GCM-256 を使用します。
- Suite-B-GCM-256：256 ビット AES-GCM を使用して ESP の整合性の保護と機密性を提供します（RFC 4106、『The Use of Galois/Counter Mode (GCM) in IPsec Encapsulating Security Payload (ESP)』を参照してください）。ESP の整合性の保護および暗号化が両方必要な場合はこのスイートまたは Suite-B-GCM-128 を使用します。
- Suite-B-GMAC-128：128 ビット AES-GMAC を使用して ESP の整合性の保護を提供します（RFC 4543、『The Use of Galois Message Authentication Code (GMAC) in IPsec ESP and AH』を参照してください）が、機密性は提供しません。ESP 暗号化の必要がない場合にのみこのスイートまたは Suite-B-GMAC-256 を使用します。
- Suite-B-GMAC-256：256 ビット AES-GMAC を使用して ESP の整合性の保護を提供します（RFC 4543、『The Use of Galois Message Authentication Code (GMAC) in IPsec ESP and AH』を参照してください）が、機密性は提供しません。ESP 暗号化の必要がない場合にのみこのスイートまたは Suite-B-GMAC-128 を使用します。

シスコのソフトウェアでは、これらのどのアルゴリズムも設定できます。スイート B での GET VPN のサポート機能では、GET VPN でこれらのアルゴリズムを使用できます。

SID 管理

GET VPN のカウンタ ベースの動作モード（ESP-GCM-AES など）では、初期化ベクトル（IV）をグループ キーで再利用しない必要があります。そのため、この機能では KS が IV 作成のための一意の送信者 ID（SID）を各 GM（インターフェイスごと）に割り当てることができる方法が提供されています。

スイート B の IPsec SA 暗号化および整合性アルゴリズムとして使用される TEK IPsec ポリシーには、GM にこれらの一意の SID 値（GMSID）を配布するため、KS で一意の SID 値のプールの管理が必要です。それぞれの連携 KS には割り当てる GMSID の個別のプールが必要です。各 KS はこれらの SID プールを設定するために一意の KS SID（KSSID）を設定します。

SID の領域は、KSSID 部と GMSID 部の 2 部に分けられます。したがって、SID は KSSID と GMSID の連結であり、KSSID は SID の KS 部、GMSID は SID の GM 部です。SID は次のビットによって形成されます。

```
 0                   1                   2
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3  (bits)
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|    KSSID    |            GMSID                |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

この例では、各 KSSID（0 ～ 127）に 2^{17}（131,072）の GMSID があり、登録する各 GM に動的に割り当てられます。

GM は GMSID を使用して、AES-GCM または AES-GMAC を使用するときに指定したキーで送信される各パケットに対して一意の 64 ビット IV を形成します。IV は次のバイトで形成されます。

```
  0   1   2   3   4   5   6   7   (bytes)
+---+---+---+---+---+---+---+---+
|    SID    |       SSIV       |
+---+---+---+---+---+---+---+---+
```

送信者固有の IV（SSIV）は、パケット カウンタです。

グループ サイズ

グループ サイズは、GM への配布のため KS に予約されている KSSID および GMSID の SID スペース割り当ての長さです。使用可能なグループサイズには、小（8、12、または16ビット）、中（24 ビット、デフォルト）、大（32 ビット）があります。中は、ほぼすべてのネットワークに適しています。

大のグループサイズは、マニュアル『 Implementation Guidance for FIPS PUB 140-2 and the Cryptographic Module Validation Program 』のセクション A.5 「Key/IV Pair Uniqueness Requirements from SP 800-38D」の要件（Suite B と組み合わせて使用される GET VPN に 2^{32} 以上の使用可能な固有の「モジュール名」（SID）がある必要がある）に厳密に準拠する必要がある場合にのみ使用する必要があります。このマニュアルは、NIST および Communications Security Establishment Canada（CSEC）によって発行および管理されています。

たとえば、KS 1 台の大のグループ サイズで SID は 32 ビットであり、512 個の KSSID 値（0 ～ 511 の範囲）があり、それぞれに GM の登録に配布する GMSID が 8,388,607 個あります。大のグループ サイズでは、次の KSSID 割り当てのガイドラインを使用して、KSSID の範囲を設定します。

表 *298* : グループ サイズ大に推奨される *KSSID* 範囲

KS	1 台の KS（連携 KS なし）	2 台の連携 KS	3 台の連携 KS	4 台の連携 KS
KS1	0 - 511	0 - 255	0 - 127	0 - 63
KS2	—	256 - 511	128 - 255	64 - 127

KS	1 台の KS（連携 KS なし）	2 台の連携 KS	3 台の連携 KS	4 台の連携 KS
KS3	—	—	256 - 383	128 - 191
KS4	—	—	384 - 511	192 - 255
KS5	—	—	—	256 - 319
KS6	—	—	—	320 - 383
KS7	—	—	—	384 - 447
KS8	—	—	—	448 - 511

最初に元の KS を設定し、より多くの KS を含めるように連携 KS ネットワークを拡張する予定の場合、上の表の列にはネットワークで予想される KS の数を使用し、後で新しい KS を追加できるようにします。

小（8、12、または 16 ビット）のグループサイズは、RFC 6054、『Using Counter Modes with Encapsulating Security Payload (ESP) and Authentication Header (AH) to Protect Group Traffic』に従って、8、12、および16 ビットの SID 長さで厳格な相互運用性が要求される、よく理解されている状況でのみ使用する必要があります。このような相互運用性が必要な場合、グループごとの SID の数が厳しく制限される（これにより KS および GM の数が厳しく制限される）ため、ネットワークの設計時は注意が必要です。小グループ サイズの制限を次に示します。

表 *299* : グループ サイズ小の制限

SID 長さ	KSSID（合計 KS）	KSSID ごとの GMSID	GMSID（合計 GM）	KS 1 台に可能な GM 登録数（すべての KS に KSSID を均等に割り当てた後）			
—	—	—	—	1 KS	2 KS	4 KS	8 KS
8 ビット	2	128	255	320	96	—	—
12 ビット	4	1,024	4,095	3,840	1,792	768	—
16 ビット	16	4,096	65,535	64,512	31,744	15,360	7,168

連携キー サーバへの KSSID 割り当て

設定されたグループ サイズ、KS の数、GM の数、KS ごとの GM の数、および KS または GM（または両方）の将来の拡張に基づいて、最初の GDOI KS ID（KSSID）の数を各 KS に割り当てるよう前もって計画する必要があります。

GDOI グループに複数の連携 KS があるときは、各 KS が固有の KSSID 値のセットを持つようにして、登録する GM が、グループ内の登録する別の GM と同じ SID を受け取らないようにする必要があります。このため、連携 KS の数と、連携 KS を後で追加するかどうかを考慮しつつ、連携 KS 全体に KSSID をどのように割り当てるのかを前もって計画する必要がありま

す。何も追加しない場合、すべてのKSで利用可能なすべてのKSSIDを割り当てることができます。連携KSを追加する場合、一部のKSSIDを予約し、それらのKSをネットワークに追加するときに割り当てる必要があります。

KSSIDは再割り当てできます。ただし、GMSIDを配布するためにKSによってすでに使用されているKSSIDをKSから削除する場合、グループはトラフィックを損失することなく再初期化されます（つまり、すべてのGMが強制的に再登録を行い、TEK IPsec SAのキー再生成が行われて使用済みのKSSIDがリセットされます）。このグループの再初期化を回避するには、（中のデフォルト グループ サイズを使用する）次の表のガイドラインを使用します。

表 *300 :* 連携 *KS*（グループ サイズ中）の推奨される *KSSID* 割り当て範囲

	1 台の KS（連携 KS なし）	**2 台の連携 KS**	**3 台の連携 KS**	**4 台の連携 KS**
KS1	0 - 127	0 - 63	0 - 31	0 - 15
KS2	—	64 - 127	32 - 63	16 - 31
KS3	—	—	64 - 95	32 - 47
KS4	—	—	96 - 127	48 - 64
KS5	—	—	—	65 - 80
KS6	—	—	—	81 - 95
KS7	—	—	—	96 - 112
KS8	—	—	—	113 - 127

より多くのKSを含めるように連携KSネットワークを拡張する予定の場合、最初に元のKSを設定するときは、上の表の列には拡張したネットワークで予定されるKSの数を使用し、後で新しいKSを追加できるようにします。

次に、KSにKSSIDを割り当てるための追加のガイドラインを示します。

- KS全体のKSSIDの連続するブロックのみを設定します（例：KS1 = 0-9 + 40-49、KS2 = 10-19 + 50-59、KS3 = 20-29、KS4 = 30-39など）。
- 任意の1台のKSには、（他のKSがGM登録をすべて失敗した場合）グループからすべてのGM登録を受信するために十分なKSSIDのスペースがある必要があります。
- グループの再初期化を回避するには、新しいKSSIDの値または範囲だけを追加します。必要な場合を除き、これらは削除しないでください。
- ネットワーク分割（連携KS間の接続の損失）の間は、KSSIDの割り当てを変更しないでください。これにより、マージ時（連携KS間の接続の回復時）に再初期化を引き起こす可能性があるKSSIDの重複を防ぎます。
- グループが *n* とおりの分割（セカンダリKSが計画されるがまだ設定されていないという意味）を開始する場合は、すべてのKSSIDをグループが分割されていないかのように設定します。

使用可能な KSSID の数は、次の表のように、グループ サイズの設定に依存します。

表 *301* : グループ サイズに基づく使用可能な *KSSID* の範囲

設定されたグループサイズ	使用可能な KSSID の数
小（8 ビット）	0 ～ 1
小（12 ビット）	0 ～ 3
小（16 ビット）	0 ～ 15
中	0 ～ 127
大	0 ～ 511

グループの再初期化

グループの再初期化は、KSSID を廃棄するプロセスです。グループの再初期化は、すべての KS にわたって発生します（プライマリおよびセカンダリ）。どの KS もグループの再初期化をトリガーでき、次のときに発生します。

- 非 GCM から GCM に TEK ポリシーを変更する。
- グループ サイズを変更する。
- 以前に使用した KSSID を削除する。
- グループの KS が KSSID と GMSID の両方を使い果たした。
- 連携 KS によって検出された KSSID の重複が解決された。

再初期化では、すべての KS が使用済みの KSSID を古い（使用済みの）KSSID に移動します（それにより廃棄されます）。次に、再初期化によって新しい KEK と新しい TEK が作成され、既存の TEK ライフタイムが短くなり、既存の TEK が削除され、すべての GM が再登録します（**clear crypto gdoi ks members** コマンドによって決定される期間内）。この期間は残りのライフタイムの 5 % であり、90 秒から 1 時間の間です。既存の TEK のライフタイムが期限切れになると、各 KS は古い（使用済み）KSSID をリセットするため、すべての KSSID が再度使用可能になります。

再初期化により GM でトラフィックが中断されることはありません。すべての GM は登録時に新しい TEK を含む新しい GMSID を受信します。

スイート B の Cisco GET VPN システム ロギング メッセージ

次の表では、スイート B に関連する GET VPN システム ロギング（syslog とも呼ばれます）メッセージについて説明します。

表 *302 : KS* および連携 *KS* メッセージ

メッセージ	説明
%GDOI-5-KS_REINIT_GROUP: *reason* for group *group-name* and will re-initialize the group.	KS はグループを再初期化します。表示される可能性のある *reason* の文字列は、次のとおりです。 • KS configured Suite-B transform requiring SIDs • KS configured Suite-B transform requiring SIDs during scheduled rekey • KS is running out of SIDs • KS changed Group Size • KS removed used KSSIDs • KS issued 'clear crypto gdoi ks members' • KS issued re-init test cmd • KSSID overlap was resolved • Pri KS peer changed used Group Size • Pri KS peer sent re-init request • Sec KS peer sent re-init request
%GDOI-5-KS_REINIT_FINISH: Re-initialization of group *group-name* completed.	グループの再初期化が完了しました。一部の操作は再初期化中（グループ サイズの変更時や使用する KSSID の削除時など）にブロックされるため、再初期化がいつ完了したのかを確認するのに役立ちます。再初期化は、古い（使用した）TEK がクリアされるまで終了しません。これは、再初期化が再度チェックされるか（**show** コマンドの実行時、グループ サイズまたは KSSID の設定時、または連携 KS の更新時など）、次の GM が登録するまで発生しないことがあります。
%GDOI-3-KS_NO_SID_AVAILABLE: GMs for group *group-name* need SIDs but this KS has no KS SIDs configured or no more SIDs available.	（GCM の使用時と GM が登録を開始した後）グループの GM は SID を必要としますが、KS に設定された KSSID がないか、それ以上使用可能な SID がありません。

メッセージ	説明
%GDOI-3-COOP_KS_KSSID_OVERLAP: Overlapping KS Sender Identifier(s) (KSSID) {*KSSID*|*KSSID-Range*} with COOP-KS peer *ip-address* in group *group-name* blocking GM registration (MISCONFIG).	別のグループの連携 KS ピアと重複する KSSID または KSSID 範囲が GM 登録をブロックしています。重複する KSSID 設定は CLI によって連携 KS でブロックされますが、GET VPN ネットワークの分割シナリオ（1 つ以上の連携 KS が一時的に使用できなかったがオンラインに戻った場合）や保存済みの設定を使用するとこれが生じることがあります。
%GDOI-5-COOP_KS_KSSID_OVERLAP_RESOLVED: Resolved overlapping KS Sender Identifier(s) (KSSID) with COOP-KS peer allowing GM registrations once again.	連携 KS ピアと重複する KSSID が解決されました（GM 登録を再開できます）。

表 *303 : GM* メッセージ

メッセージ	説明
%GDOI-5-GM_IV_EXHAUSTED: GM for group *group-name* exhausted its IV space for interface *interface-name* and will re-register.	グループの GM が特定の SA の IV スペース（固有の IV のセットの意味）を使い尽くしたため、再登録します。
%GDOI-5-GM_REJECTING_SA_PAYLOAD: Registration: Policy in SA payload sent by KS *ip-address* rejected by GM in the group *group-name* reason: client rekey hash algorithm (*kek-policy*) is unacceptable by this GM.	クライアントのキー再生成ハッシュ アルゴリズム（指定された KEK ポリシー）が指定されたグループの GM によって承認されませんでした。登録時に GM が KEK ポリシーを拒否しました。
%GDOI-5-GM_REJECTING_SA_PAYLOAD: Registration: Policy in SA payload sent by KS *ip-address* rejected by GM in the group *group-name* reason : client rekey transform-sets (*tek-policy*) for data-protection are unacceptable by this GM.	データ保護のクライアントのキー再生成トランスフォーム セット（指定された TEK ポリシー）が GM によって承認されませんでした。登録時に GM が TEK ポリシーを拒否しました。
%GDOI-5-GM_REKEY_TRANSFORMSET_CHECK_FAIL: The transform set (*transform-set*) for data protection in group *group-name* is unacceptable by this client.	グループのデータ保護のトランスフォーム セットがクライアントによって承認されませんでした。GM がキー再生成を受け取り、TEK ポリシーを拒否しました。

メッセージ	説明
%GDOI-3-KS_REKEY_AUTH_KEY_LENGTH_INSUFFICIENT: Rejected rekey sig-hash algorithm change: using sig-hash algorithm HMAC_AUTH_SHA*bits* requires an authentication key length of at least *number-of-bits* bits (*number-of-blocks* blocks in bytes) - current RSA key "360-bit" is only 45 blocks in bytes.	RSA キーのモジュラス長が十分にないため、キー再生成のシグニチャ ハッシュ アルゴリズムの設定が拒否されました。HMAC-SHA-384 は少なくとも 465 ビット（バイトの 59 ブロック）のモジュラスを必要とし、HMAC-SHA-512 は 593 ビット（バイトの 75 ブロック）のモジュラスを必要とします。

スイート B での GET VPN のサポートの設定方法

スイート B での GET VPN のサポート機能セットの各機能は個別に設定可能です。しかし、スイート B の標準に準拠するため、特定の組み合わせでこれらの機能を設定する必要があります。これらの組み合わせの詳細については、RFC 4869、『 Suite B Cryptographic Suites for IPsec 』を参照してください。

GM がスイート B をサポートするソフトウェア バージョンを実行していることを確認する

GET VPN はグループに基づいた技術であるため、（プライマリ KS、連携 KS、および GM を含めた）同じグループ内のすべてのデバイスは、機能を有効化するためにスイート B の機能をサポートする必要があります。グループの機能を有効にするには、グループ内のすべてのデバイスが GET VPN ソフトウェアの互換性のあるバージョンを実行していることを確認する必要があります。

GET VPN ネットワークのすべてのデバイスがスイート B をサポートしていることを確認するには、KS（またはプライマリ KS）で次のステップを実行します。

手順の概要

1. **enable**
2. **show crypto gdoi feature suite-b**
3. **show crypto gdoi feature suite-b | include No**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例：	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。

	コマンドまたはアクション	目的
	`Device> enable`	
ステップ 2	**show crypto gdoi feature suite-b** 例： `Device# show crypto gdoi feature suite-b`	ネットワーク内の各 KS および GM で実行されている GET VPN ソフトウェアのバージョンを表示し、そのデバイスがスイート B をサポートしているかどうかを表示します。
ステップ 3	**show crypto gdoi feature suite-b | include No** 例： `Device# show crypto gdoi feature suite-b | include No`	（オプション）スイート B をサポートしないデバイスのみ検索します。

GET VPN スイート B でのキー サーバの設定

KEK の署名ハッシュ アルゴリズムの設定

KEK の署名ハッシュ アルゴリズムを設定するにはこの作業を行います。

始める前に

この作業には次の前提条件があります。

- デバイスに関連付けられている RSA キー ペアを使用するキー再生成認証が有効になっていることを確認します。これを行うには、**rekey authentication** コマンドを **mypubkey rsa** *key-name* キーワードと引数で使用します。
- RSA キー ペアに十分な長さのモジュラスがあることを確認します。HMAC-SHA-384 は少なくとも 465 ビット（バイトの 59 ブロック）のモジュラスを必要とし、HMAC-SHA-512 は 593 ビット（バイトの 75 ブロック）のモジュラスを必要とします。キー再生成の署名ハッシュ アルゴリズムが不十分なモジュラス長のキー ペアを使用する SHA-384 または SHA-512 に変更されると、設定拒否メッセージがコンソールに表示され、システム ログ メッセージが生成されます。同様に、キー再生成の署名ハッシュ アルゴリズムがすでに SHA-384 または SHA-512 であり、キーペアが不十分なモジュラス長の 1 つに変更されると、同様のメッセージがコンソールに表示され、同じシステム ログ メッセージが生成されます。
- キー再生成メッセージを受信した後の GM から KS への確認応答の認証に SHA-2/HMAC-SHA-2 を使用するには、GM へのキー再生成メッセージのユニキャスト配信を有効にする必要があります。これを実行するには、**rekey transport unicast** コマンドを使用します。

手順の概要

1. **enable**

2. **configure terminal**
3. **crypto gdoi group** [**ipv6**] *group-name*
4. **server local**
5. **rekey sig-hash algorithm** *algorithm*
6. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**crypto gdoi group** [**ipv6**] *group-name* 例： `Device(config)# crypto gdoi group mygroup`	GDOI グループを指定し、GDOI グループ コンフィギュレーション モードを開始します。 • データプレーン内で IPv6 で GET VPN を使用する場合、**ipv6** キーワードを使用する必要があります。
ステップ 4	**server local** 例： `Device(config-gdoi-group)# server local`	デバイスを GDOI KS として指定し、GDOI ローカル サーバ コンフィギュレーション モードを開始します。
ステップ 5	**rekey sig-hash algorithm** *algorithm* 例： `Device(gdoi-local-server)# rekey sig-hash algorithm sha512`	KEK の署名ハッシュ アルゴリズムを設定します。Suite B の場合は、**sha256**、**sha384**、または **sha512** を指定する必要があります。
ステップ 6	**end** 例： `Device(gdoi-local-server)# end`	GDOI ローカル サーバ コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

グループ サイズの設定

このタスクはオプションです。ほぼすべての展開で、メディアのデフォルト グループ サイズ（送信者識別子の長さ）が推奨されます。スイート B のグループ サイズを設定するにはこの作業を行います。

スイート B（つまり ESP-GCM または ESP-GMAC）が設定され、スイート B のポリシーが生成された後で、連携 KS を使用するグループのグループ サイズを変更する場合、プライマリ KS で変更する前にすべてのセカンダリ KS でグループ サイズを変更する必要があります。

グループ サイズを変更すると（新しい SID 長が使用できるように）グループが初期化されます。KS 全体で競合するグループ サイズ設定があると GM 登録がブロックされます。

手順の概要

1. **enable**
2. **configure terminal**
3. **crypto gdoi group** [**ipv6**] *group-name*
4. **server local**
5. **group size** {**small** {**8** | **12** | **16**} | **medium** | **large**}
6. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**crypto gdoi group** [**ipv6**] *group-name* 例： `Device(config)# crypto gdoi group mygroup`	GDOI グループを指定し、GDOI グループ コンフィギュレーション モードを開始します。 • データプレーン内で IPv6 で GET VPN を使用する場合、**ipv6** キーワードを使用する必要があります。
ステップ 4	**server local** 例： `Device(config-gdoi-group)# server local`	デバイスを GDOI KS として指定し、GDOI ローカル サーバ コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 5	**group size** {**small** {**8** | **12** | **16**} | **medium** | **large**} 例： `Device(gdoi-local-server)# group size small 16`	グループ サイズを設定します。
ステップ 6	**end** 例： `Device(gdoi-local-server)# end`	GDOI ローカル サーバ コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

キー サーバ識別子の設定

スイート B では、それぞれの GM に固有の GMSID の割り当てが必要です。これは GM が以前同じキーに（その GM または別の GM が）使用した SID を再利用できないことを意味します。したがって、GET VPN が重複する SID 値を許可しないように設計されていても、KS ごとに固有のセットを持つように KS 間の KSSID 値を正しく設定する必要があります。（KS 間の KSSID が重複すると再初期化されます。）

KS に SID のプールを割り当てるには少なくとも 1 つの KSSID を設定する必要があります。TEK IPSec ポリシーとして GCM または GMAC を設定する前に KS でこれを行います。

この作業を行って KS に KSSID または KSSID の範囲を割り当てます。各 KS は、GCM または GMAC を使用する際には少なくとも 1 つの KSSID を割り当てる必要があります。単一の KSSID、KSSID の範囲、またはその両方を設定できます。メディアのデフォルト グループ サイズとして、0 ～ 127 の範囲の 128 個の利用可能な KSSID 値があります。

KSSID 値は、GDOI ローカル サーバ ID コンフィギュレーション モードを終了するまで KS に割り当てられません（KS から使用もできません）。

手順の概要

1. **enable**
2. **configure terminal**
3. **crypto gdoi group** [**ipv6**] *group-name*
4. **server local**
5. **identifier**
6. **range** *lowest-kssid* **-** *highest-kssid*
7. **value** *kssid*
8. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**crypto gdoi group** [**ipv6**] *group-name* 例： `Device(config)# crypto gdoi group mygroup`	GDOI グループを指定し、GDOI グループ コンフィギュレーション モードを開始します。 • データプレーン内で IPv6 で GET VPN を使用する場合、**ipv6** キーワードを使用する必要があります。
ステップ 4	**server local** 例： `Device(config-gdoi-group)# server local`	デバイスを GDOI KS として指定し、GDOI ローカル サーバ コンフィギュレーション モードを開始します。
ステップ 5	**identifier** 例： `Device(gdoi-local-server)# identifier`	GDOI ローカル サーバ ID コンフィギュレーション モードを開始します。
ステップ 6	**range** *lowest-kssid - highest-kssid* 例： `Device(gdoi-local-server-id)# range 10 - 20`	KSSID の範囲を割り当てます。 • この範囲は、グループ全体で一意である必要があります。
ステップ 7	**value** *kssid* 例： `Device(gdoi-local-server-id)# value 0`	KSSID を割り当てます。 • この KSSID は、グループ全体で一意である必要があります。 • **value 0** コマンドは、KSSID 値 0 で始まる SID のプールを KS に割り当てます（つまり 0x0 で始まり 0x1FFFF で終わる SID 値のプールが割り当てられます）。

	コマンドまたはアクション	目的
ステップ 8	**end** 例： `Device(gdoi-local-server-id)# end`	GDOI ローカル サーバ ID コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

すでに別の KSSID が割り当てられている KS に 1 つ以上の KS を設定しようとすると（かつ連携 KS ネットワークが分割されていないと）、設定は拒否され、GDOI ローカル サーバ ID コンフィギュレーション モードを終了すると次のメッセージが表示されます。

```
% Key Server SID Configuration Denied:
%   The following Key Server SIDs being added overlap:
%   2, 200-250  (COOP-KS Peer: 10.0.9.1)
```

連携 KS ネットワークが分割されている場合、重複する KSSID を設定する必要はありません。ネットワークのマージで KSSID の重複が検出されると、GM の登録は重複が解決するまでブロックされます。次のシステム ログ メッセージが両方の KS に表示されます。

```
%GDOI-3-COOP_KSSID_OVERLAP: Overlapping KS Sender Identifier(s) (KSSID) {2, 200-250}
with COOP-KS peer 10.0.9.1 in group diffint blocking GM registration (MISCONFIG)
```

KS が重複する KSSID を構成解除すると、グループはトラフィックを損失することなく再初期化します（つまり、すべての GM が再登録を強制され、TEK IPSec SA は使用された KSSID をリセットするためにキー再生成されます）。次のシステム ログ メッセージが KS に表示されます。

```
%SYS-5-CONFIG_I: Configured from console by console
%GDOI-5-COOP_KSSID_OVERLAP_RESOLVED: Resolved overlapping KS Sender Identifier(s) (KSSID)
 with COOP-KS peer allowing GM registrations once again
%GDOI-5-KS_REINIT_GROUP: KSSID overlap was resolved for group diffint and will
re-initialize the group.
%GDOI-5-KS_SEND_UNICAST_REKEY: Sending Unicast Rekey for group diffint from address
10.0.8.1 with seq # 11
%GDOI-4-GM_DELETE: GM 10.0.3.1 deleted from group diffint.
%GDOI-4-GM_DELETE: GM 10.65.9.2 deleted from group diffint.
```

%GDOI-5-KS_SEND_UNICAST_REKEY システム ログ メッセージは、これがプライマリ KS である場合にのみ表示されます。KSSID が重複しているピア KS でも %GDOI-5-COOP_KSSID_OVERLAP_RESOLVED システム ログ メッセージが表示されます。

スイート B の IPsec SA の設定

スイート B の IPsec SA を設定するには、次のステップを実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **crypto ipsec transform-set** *transform-set-name* {**esp-gcm** | **esp-gmac**} [**128** | **192** | **256**]
4. **crypto ipsec profile** *ipsec-profile-name*

5. **set transform-set** *transform-set-name*
6. **exit**
7. **crypto gdoi group** [**ipv6**] *group-name*
8. 次のいずれかのコマンドを入力します。
   - **identity number** *number*
   - **identity address ipv4** *address*
9. **server local**
10. **sa ipsec** *sequence-number*
11. **profile** *ipsec-profile-name*
12. **match address** {**ipv4** | **ipv6**} {*access-list-number* | *access-list-name*}
13. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**crypto ipsec transform-set** *transform-set-name* {**esp-gcm** | **esp-gmac**} [**128** | **192** | **256**] 例： `Device(config)# crypto ipsec transform-set g1 esp-gcm 192`	トランスフォーム セット（セキュリティ プロトコルおよびアルゴリズムの受け入れ可能な組み合わせ）を定義し、暗号化トランスフォーム コンフィギュレーション モードを開始します。 • スイート B では、ESP-GCM または ESP-GMAC を使用するトランスフォーム セットを指定する必要があります。（別のコマンドラインにコマンドをもう一度入力して、複数のトランスフォーム セットを定義できます。） • オプションで 128、192、または 256 のキー サイズを指定できます。デフォルトのキーのサイズは 128 です。
ステップ 4	**crypto ipsec profile** *ipsec-profile-name* 例： `Device(config)# crypto ipsec profile profile1`	IPsec プロファイル（2 つの IPsec ルータ間の IPsec 暗号化に使用されるパラメータ）を定義して、IPsec プロファイル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 5	**set transform-set** *transform-set-name* 例： `Device(ipsec-profile)# set transform-set transformset1`	クリプト マップ エントリで使用可能なトランスフォーム セットを指定します。
ステップ 6	**exit** 例： `Device(ipsec-profile)# exit`	IPSec プロファイル コンフィギュレーション モードを終了します。
ステップ 7	**crypto gdoi group** [**ipv6**] *group-name* 例： `Device(config)# crypto gdoi group gdoigroupname`	GDOI グループを指定し、GDOI グループ コンフィギュレーション モードを開始します。 • データプレーン内で IPv6 で GET VPN を使用する場合、**ipv6** キーワードを使用する必要があります。

ステップ 8	次のいずれかのコマンドを入力します。
	• **identity number** *number*
	• **identity address ipv4** *address*
	例：
	`Device(config-gdoi-group)# identity number 3333`
	例：
	`Device(config-gdoi-group)# identity address ipv4 209.165.200.225`
		GDOI グループ番号またはアドレスを指定します。
		• **identity number** *number* コマンドは IPv4 および IPv6 の構成に適用されます。
		• **identity address ipv4** *address* コマンドは、IPv4 構成のみに適用されます。

ステップ 9	**server local** 例： `Device(config-gdoi-group)# server local`	デバイスを GDOI KS として指定し、GDOI ローカル サーバ コンフィギュレーション モードを開始します。
ステップ 10	**sa ipsec** *sequence-number* 例： `Device(gdoi-local-server)# sa ipsec 1`	GDOI グループに使用される IPsec SA ポリシー情報を指定し、GDOI SA IPsec コンフィギュレーション モードを開始する。
ステップ 11	**profile** *ipsec-profile-name* 例： `Device(gdoi-sa-ipsec)# profile gdoi-p`	GDOI グループ用の IPsec SA ポリシーを定義します。
ステップ 12	**match address** {**ipv4** | **ipv6**} {*access-list-number* | *access-list-name*} 例：	GDOI 登録の IP 拡張アクセス リスト（ACL）を選択します。

	コマンドまたはアクション	目的

	`Device(gdoi-sa-ipsec)# match address ipv4 102`	• IPv4 グループに対しては **ipv4** キーワード、IPv6 グループに対しては **ipv6** キーワードを使用する必要があります。
		• IPv6 構成には（番号付きではなく）名前付きアクセス リストを使用する必要があります。
		（注） 必ずグループのすべての連携 KS の中で同一順序で同一エントリを持つ ACL を選択してください。そうでない場合、別の KS に登録する GM は、ポリシーのダウンロード後は正しく暗号化および復号化することができません。
		（注） IPv6 グループに IPv4 のポリシーを割り当てようとするると、アクセス リスト名が無効であるか、リストはすでに存在するが誤った種類であることを示すエラー メッセージが表示されます。
		`Access-list type conflicts with prior definition`
		`% ERROR: access-list-name is either an invalid name or the list already exists but is the wrong type.`

ステップ 13	**end** 例： `Device(gdoi-sa-ipsec)# end`	GDOI SA IPsec コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

GET VPN スイート B でのグループ メンバーの設定

スイート B の KEK の許容可能な暗号化アルゴリズムまたはハッシュ アルゴリズムの設定

GM によって許可される KEK 用の スイート B 暗号化およびハッシュ アルゴリズムを設定するには、次のステップを実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **crypto gdoi group** [**ipv6**] *group-name*
4. 次のいずれかのコマンドを入力します。

- **identity number** *number*
- **identity address ipv4** *address*

5. **server address ipv4** *address*
6. **client rekey encryption** *cipher* [... [*cipher*]]
7. **client rekey hash** *hash*
8. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**crypto gdoi group** [**ipv6**] *group-name* 例： `Device(config)# crypto gdoi group gdoigroupone`	GDOI グループを指定し、GDOI グループ コンフィギュレーション モードを開始します。 • データプレーン内で IPv6 で GET VPN を使用する場合、**ipv6** キーワードを使用する必要があります。

ステップ 4	次のいずれかのコマンドを入力します。
	• **identity number** *number*
	• **identity address ipv4** *address*
	例：
	`Device(config-gdoi-group)# identity number 3333`
	例：
	`Device(config-gdoi-group)# identity address ipv4 10.2.2.2`
		GDOI グループ番号またはアドレスを指定します。

ステップ 5	**server address ipv4** *address* 例： `Device(config-gdoi-group)# server address ipv4 10.0.5.2`	GDOI グループが到達しようとするサーバのアドレスを指定します。 • アドレスを無効にするには、このコマンドの **no** 形式を使用します。
ステップ 6	**client rekey encryption** *cipher* [... [*cipher*]] 例：	KEK のクライアント受け入れ可能キー再生成暗号化を設定します。

	コマンドまたはアクション	目的
	`Device(config-gdoi-group)# client rekey encryption 3des-cbc aes 192 aes 256`	
ステップ 7	**client rekey hash** *hash* 例： `Device(config-gdoi-group)# client rekey hash sha384`	KEK のクライアント受け入れ可能ハッシュを設定します。 • Suite B の場合は、**sha256**、**sha384**、または **sha512** のいずれかを指定する必要があります。
ステップ 8	**end** 例： `Device(config-gdoi-group)# end`	GDOI グループ コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

スイート B の TEK の受け入れ可能トランスフォーム セットの設定

GM によって許可されるデータ暗号化または認証のために TEK が使用するトランスフォーム セットを設定するには、次のステップを実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **crypto ipsec transform-set** *transform-set-name* {**esp-gcm** | **esp-gmac**} [**128** | **192** | **256**]
4. **exit**
5. **crypto gdoi group** [**ipv6**] *group-name*
6. **client transform-sets** *transform-set-name1* [... [*transform-set-name6*]]
7. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**crypto ipsec transform-set** *transform-set-name* {**esp-gcm**	**esp-gmac**} [**128**	**192**	**256**] 例：	トランスフォーム セット（セキュリティ プロトコルおよびアルゴリズムの受け入れ可能な組み合わせ）

	コマンドまたはアクション	目的
	`Device(config)# crypto ipsec transform-set g1 esp-gcm 192`	を定義し、暗号化トランスフォーム コンフィギュレーション モードを開始します。 • スイート B では、ESP-GCM または ESP-GMAC を使用するトランスフォームセットを指定する必要があります。 • 別のコマンドラインにコマンドをもう一度入力して、複数のトランスフォームセットを定義できます。 • オプションで 128、192、または 256 のキー サイズを指定できます。デフォルトのキーのサイズは 128 です。
ステップ 4	**exit** 例： `Device(cfg-crypto-trans)# exit`	暗号化トランスフォーム コンフィギュレーション モードを終了します。
ステップ 5	**crypto gdoi group** [**ipv6**] *group-name* 例： `Device(config)# crypto gdoi group gdoigroupone`	GDOI グループを指定し、GDOI グループ コンフィギュレーション モードを開始します。 • データプレーン内で IPv6 で GET VPN を使用する場合、**ipv6** キーワードを使用する必要があります。
ステップ 6	**client transform-sets** *transform-set-name1* [*...* [*transform-set-name6*]] 例： `Device(config-gdoi-group)# client transform-sets g1`	データの暗号化および認証のために TEK によって使用される受け入れ可能トランスフォームセット タグを指定します。 • トランスフォーム セット タグは 6 個まで指定できます。
ステップ 7	**end** 例： `Device(config-gdoi-group)# end`	GDOI グループ コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

スイート B での GET VPN のサポートの確認とトラブルシューティング

キー サーバ上のスイート B での GET VPN のサポートの確認とトラブルシューティング

KS で実行されている設定を表示するには、**show running-config** コマンドを使用します。

手順の概要

1. **show crypto gdoi ks identifier** [**detail**]
2. **show crypto gdoi ks coop identifier** [**detail**]
3. **show crypto gdoi feature suite-b**
4. **show crypto gdoi ks policy**

手順の詳細

ステップ 1 **show crypto gdoi ks identifier** [**detail**]

例：

```
Device# show crypto gdoi ks identifier detail

KS Sender ID (KSSID) Information for Group diffint:

    Transform Mode           : Counter (Suite B)
    reinitializing          : No
    SID Length (Group Size)  : 24 bits (medium)
    Current KSSID In-Use     : 0
    Last GMSID Used          : 1

    KSSID (or SIDS)Assigned        : 0-15
    KSSID (or SIDS)Used            : 0
    KSSID (or SIDS) Used  (Old)      : none
    Available KSSID (or SIDS): 1-15

    REMAINING SIDs:
      KSSID to reinitialize at         : 15
      GMSID to reinitialize at         : 6291456
      # of SIDs Remaining for Cur KSSID : 8388606
      # of SIDs Remaining until Re-init : 132120575
```

このコマンドは、スイート B の SID 管理の状態を表示します。Transform Mode フィールドは SID 管理およびスイート B のポリシーがグループ内で現在使用されているかどうかを確認するために非カウンタ（非スイート B）またはカウンタ（スイート B）のいずれかにできます。グループが現在再初期化（つまり、すべての GM が再登録を強制され、TEK IPsec SA がキー再生成されて使用済みの KSSID をリセットする）を行っている場合は、reinitializing フィールドに Yes が表示されます。SID Length (Group Size) フィールドは、グループで現在使用されているグループ サイズを決定します。デフォルトは 24 ビット（中）です。

Current KSSID In-Use フィールドおよび Last GMSID Used フィールドは、次の登録 GM に分配される SID（または SIDS）に対応します。KSSID (or SIDS) Assigned フィールドは、連携 KS と同期した、ローカルに設定されている KSSID に対応します。Available KSSID (or SIDS) フィールドは、最後の再初期化以降まだ使用されていない KSSID に対応します。新しい KSSID を使用するたびに KSSID (or SIDS) Used フィールドに追加され、再初期化時に、これらの使用された KSSID が KSSID (or SIDS) Used (Old) フィールドに移動されます。再初期化期間の終わりに、古い使用済みの KSSID がクリアされて再び Available KSSID プールに加えられます。

（注） # of SIDs Remaining until Re-init フィールドの値が 0 に近づくと、GM が再登録を継続している場合はすぐに再初期化が発生します。再初期化によってトラフィックの中断やネットワークの問題が発生することはありませんが、すべての GM がの再登録が発生します。

ステップ 2 **show crypto gdoi ks coop identifier** [**detail**]

例：

```
Device# show crypto gdoi ks coop identifier detail

COOP-KS Sender ID (SID) Information for Group diffint:

    Local KS Role: Primary   , Local KS Status: Alive
        Local Address                : 10.0.8.1
        Next SID Client Operation    : NOTIFY
        reinitializing              : No
        KSSID Overlap                : No
        SID Length (Group Size) Cfg  : 24 bits (medium)
        SID Length (Group Size) Used : 24 bits (medium)
        Current KSSID In-Use         : 0
        KSSID (or SIDS)Assigned            : 0-15
        KSSID (or SIDS)Used                : 0
        Old KSSID (or SIDS)Used            : none

    Peer KS Role:  Secondary , Peer KS Status:  Alive
        Peer Address                 : 10.0.9.1
        Next SID Client Operation    : NOTIFY
        reinitializing              : No
        KSSID Overlap                : No
        SID Length (Group Size) Cfg  : 24 bits (medium)
        SID Length (Group Size) Used : 24 bits (medium)
        Current KSSID In-Use         : 16
        KSSID (or SIDS)Assigned            : 16-31
        KSSID (or SIDS)Used                : 16
        Old KSSID (or SIDS)Used            : none
```

このコマンドは、連携 KS 全体で同期化された SID のステータス情報を表示します。

KSSID Overlap フィールドに Yes が表示されると、KSSID の重複（ネットワークの分割時に発生することがあります）が解決するまで GM 登録がブロックされます。GM 登録を再開するには、1 つの連携 KS またはほかの KS から重複している KSSID を構成解除する必要があります。重複する KSSID が解決すると、再初期化が発生します。

グループ サイズを変更すると（ほとんどの導入では推奨されません）、すべてのセカンダリ KS で最初に新しいグループ サイズを設定する必要があります。次にプライマリ KS で、SID Length (Group Size) Cfg フィールドに、すべての連携 KS ピアの新しいグループ サイズが表示されます。プライマリ KS で新しいグループ サイズを設定したときのみ、すべての KS が新しいグループ サイズの使用を開始し、SID Length (Group Size) Used フィールドを更新して新しいグループ サイズを表示します。

ステップ 3 **show crypto gdoi feature suite-b**

例：

```
Device# show crypto gdoi feature suite-b

Group Name: diffint
    Key Server ID       Version   Feature Supported
        10.0.8.1         1.0.4          Yes
        10.0.9.1         1.0.4          Yes

    Group Member ID     Version   Feature Supported
        10.0.3.1         1.0.4          Yes
```

```
        10.0.4.1         1.0.4          Yes
```

このコマンドは、KS および GM がスイート B 機能セット（つまり、AES-GCM、AES-GMAC、SHA-2、および HMAC-SHA2）を使用できるかどうかを表示します。Version フィールドが 1.0.4 またはそれ以上を表示し、Feature Supported フィールドが連携 KS グループ内のすべての KS、および登録されている GM について Yes を表示する必要があります。

ステップ 4 show crypto gdoi ks policy

例：

```
Device# show crypto gdoi ks policy

Key Server Policy:
For group diffint (handle: 2147483650) server 10.0.8.1 (handle: 2147483650):

  # of teks : 4  Seq num : 0
  KEK POLICY (transport type : Unicast)
    spi : 0x80474E999FE8F60364B7F51809E28C84
    management alg     : disabled    encrypt alg       : 3DES
    crypto iv length   : 8           key size          : 24
    orig life(sec): 86400       remaining life(sec): 85586
    sig hash algorithm : enabled     sig key length    : 162
    sig size           : 128
    sig key name       : mykeys

  TEK POLICY (encaps : ENCAPS_TUNNEL)
    spi                : 0x9C666FA7
    access-list        : gcm-acl
    Selector           : permit ip host 10.0.1.1 host 239.0.1.1
    transform          : esp-gcm
    alg key size       : 20            sig key size          : 0
    orig life(sec)     : 900           remaining life(sec)   : 87
    tek life(sec)      : 900           elapsed time(sec)     : 813
    override life (sec): 0             antireplay window size: 64


  TEK POLICY (encaps : ENCAPS_TUNNEL)
    spi                : 0x54E8D5D3
    access-list        : gcm-acl
    Selector           : permit ip host 10.0.100.2 host 238.0.1.1
    transform          : esp-gcm
    alg key size       : 20            sig key size          : 0
    orig life(sec)     : 900           remaining life(sec)   : 87
    tek life(sec)      : 900           elapsed time(sec)     : 813
    override life (sec): 0             antireplay window size: 64



  TEK POLICY (encaps : ENCAPS_TUNNEL)
    spi                : 0xC8B4DE6D
    access-list        : gcm-acl
    Selector           : permit ip host 10.0.1.1 host 10.0.100.2
    transform          : esp-gcm
    alg key size       : 20            sig key size          : 0
    orig life(sec)     : 900           remaining life(sec)   : 87
    tek life(sec)      : 900           elapsed time(sec)     : 813
    override life (sec): 0             antireplay window size: 64
```

```
TEK POLICY (encaps : ENCAPS_TUNNEL)
  spi                : 0x1C908AF3
  access-list        : gcm-acl
  Selector           : permit ip host 10.0.100.2 host 10.0.1.1
  transform          : esp-gcm
  alg key size       : 20            sig key size          : 0
  orig life(sec)     : 900           remaining life(sec)   : 87
  tek life(sec)      : 900           elapsed time(sec)     : 813
```

このコマンドは、TEK および IPSec SA が ESP-GCM または ESP-GMAC の TEK ポリシーの access-list フィールド内の ACL から（Selector フィールドに表示される）ACE ごとに生成されているかどうかを表示します。またこのコマンドは、KEK ポリシーが署名ハッシュ アルゴリズムとして SHA-2/HMAC-SHA-2 を使用しているかどうかも表示します。

GM 上のスイート B での GET VPN のサポートの確認とトラブルシューティング

GM で実行されている設定を表示するには、**show running-config** コマンドを使用します。

手順の概要

1. **show crypto gdoi gm identifier** [**detail**]
2. **show crypto gdoi feature suite-b**
3. **show crypto gdoi**

手順の詳細

ステップ 1 **show crypto gdoi gm identifier** [**detail**]

例：

```
Device# show crypto gdoi gm identifier detail

GM Sender ID (SID) Information for Group diffint:

  Group Member: 10.65.9.2        vrf: None
    Transform Mode                 : Counter (Suite B)
    # of SIDs Last Requested       : 3

    CURRENT SIDs:
      Shared Across Interfaces?    : Yes
      SID Length (Group Size)      : 24 bits (medium)
      # of SIDs Downloaded         : 3
      First SID Downloaded         : 0x08000007
      Last SID Downloaded          : 0x08000009

      CM Interface   B/W (Kbps) MTU (B)  # Req # Rx  Installed SID Range
      ============== ========== ======== ===== ===== ======================
      Et2/0          10000      1500     1     3     0x08000007 - 0x08000009
      Et3/0          10000      1500     1     3     0x08000007 - 0x08000009
      Et4/0          10000      1500     1     3     0x08000007 - 0x08000009

    NEXT SID REQUEST:
```

```
      TEK Lifetime                 : 900 sec
      SID Length (Group Size)      : 32 bits (LARGE)
```

このコマンドは、GM が GCM-AES または GMAC-AES を TEK IPsec SA ポリシーとして使用しているときに受信してインストールされた SID のステータスを表示します。Transform Mode フィールドでは、SID がダウンロードされ、インストールされているかどうか、およびスイート B のポリシーがグループで使用されているかどうかを確認するために、非カウンタ（非スイート B）またはカウンタ（スイート B）を表示できます。# of SIDs Last Requested フィールドは、主にこの登録されている（つまり、ローカル アドレスまたはクライアント登録インターフェイスを使用している）GM のために暗号マップが適用されるインターフェイスの数に依存します。SID は、ローカル アドレスを使用している場合は Shared Across Interfaces フィールドであり、各 CM の Installed SID Range フィールドも同じになります。このコマンドは、主に各 CM インターフェイスにインストールされている SID があることを確認するために使用します。

ステップ 2 show crypto gdoi feature suite-b

例：

```
Device# show crypto gdoi feature Suite B

       Version    Feature Supported
        1.0.4           Yes
```

このコマンドは、この GM がスイート B 機能セット（つまり、GCM-AES、GMAC-AES、SHA-2、および HMAC-SHA-2）を使用できるかどうかを表示します。Version フィールドが 1.0.4 またはそれ以上を表示し、Feature Supported フィールドが Yes を表示する必要があります。

ステップ 3 show crypto gdoi

例：

```
Device# show crypto gdoi

GROUP INFORMATION

    Group Name               : diffint
    Group Identity           : 1234
    Crypto Path              : ipv4
    Key Management Path      : ipv4
    Rekeys received          : 0
    IPSec SA Direction       : Both

     Group Server list       : 10.0.8.1

    Group member             : 10.0.3.1         vrf: None
       Version               : 1.0.4
       Registration status   : Registered
       Registered with       : 10.0.8.1
.
.
.
ACL Downloaded From KS 10.0.8.1:
   access-list   permit ip host 10.0.1.1 host 239.0.1.1
   access-list   permit ip host 10.0.100.2 host 238.0.1.1
   access-list   permit ip host 10.0.1.1 host 10.0.100.2
```

```
   access-list   permit ip host 10.0.100.2 host 10.0.1.1

KEK POLICY:
    Rekey Transport Type     : Unicast
    Lifetime (secs)          : 85740
    Encrypt Algorithm        : 3DES
    Key Size                 : 192
    Sig Hash Algorithm       : HMAC_AUTH_SHA256
    Sig Key Length (bits)    : 1024

TEK POLICY for the current KS-Policy ACEs Downloaded:
  Ethernet3/0:
    IPsec SA:
        spi: 0x318846DE(831014622)
        transform: esp-gcm
        sa timing:remaining key lifetime (sec): (86350)
        Anti-Replay(Counter Based) : 64

    IPsec SA:
        spi: 0xF367AEA0(4083658400)
        transform: esp-gcm
        sa timing:remaining key lifetime (sec): (86350)
        Anti-Replay(Counter Based) : 64

    IPsec SA:
        spi: 0xE583A3F5(3850609653)
        transform: esp-gcm
        sa timing:remaining key lifetime (sec): (86350)
        Anti-Replay(Counter Based) : 64

    IPsec SA:
        spi: 0xE9AC04C(245022796)
        transform: esp-gcm
        sa timing:remaining key lifetime (sec): (86350)
        Anti-Replay(Counter Based) : 64
```

複数の IPsec SA のプレゼンスは、GCM または GMAC が設定されていることを示します（各 IPSec SA にはダウンロードした各 ACE の固有の SPI があることに注意してください）。TEK POLICY for the current KS-Policy ACEs Downloaded セクションの TEK POLICY に記載されている各 ACE に関して、このコマンドは、TEK ポリシーおよび IPsec SA が ACL Downloaded From KS に記載されている ACL からダウンロード（およびインストール）されているかどうかを表示します。またこのコマンドは、KEK ポリシーが署名ハッシュ アルゴリズム（たとえば、HMAC_AUTH_SHA256）に SHA-2/HMAC-SHA-2 を使用しているかどうかも表示します。

スイート B での GET VPN のサポートの設定例

例：GM がスイート B をサポートするソフトウェア バージョンを実行していることを確認する

次の例は、各グループ内のすべてのデバイスがスイート B 暗号化をサポートしているかどうかを確認するために KS（またはプライマリ KS）で GET VPN ソフトウェア バージョン管理コマンドを使用する方法を示します。

```
Device# show crypto gdoi feature suite-b

Group Name: GETVPN
    Key Server ID       Version   Feature Supported
        10.0.5.2         1.0.4          Yes
        10.0.6.2         1.0.4          Yes
        10.0.7.2         1.0.3          No
        10.0.8.2         1.0.2          No

    Group Member ID     Version   Feature Supported
        10.0.1.2         1.0.2          No
        10.0.2.5         1.0.3          No
        10.0.3.1         1.0.4          Yes
        10.0.3.2         1.0.4          Yes
```

また、上記のコマンドは GM でも入力できます（その GM の情報を表示します。KS や他の GM には使用できません）。

次の例は、KS（プライマリ KS）でスイート B をサポートしていない GET VPN ネットワークのデバイスのみ検索するコマンドを入力する方法を示しています。

```
Device# show crypto gdoi feature suite-b | include No

        10.0.7.2         1.0.3          No
        10.0.8.2         1.0.2          No
        10.0.1.2         1.0.2          No
        10.0.2.5         1.0.3          No
```

例：GET VPN スイート B のキー サーバの設定

KEK の署名ハッシュ アルゴリズムの設定

次に、KEK の署名ハッシュ アルゴリズムを設定する方法の例を示します。

```
Device> enable
Device# configure terminal
Device(config)# crypto gdoi group mygroup
```

```
Device(config-gdoi-group)# server local
Device(gdoi-local-server)# rekey sig-hash algorithm sha512
Device(gdoi-local-server)# end
```

スイート B のグループ サイズの設定

メディアのデフォルトのグループ サイズはほとんどの導入に十分であるため、スイート B のグループ サイズの設定はオプションです。次の例は、スイート B にグループ サイズを設定する方法を示しています。

```
Device> enable
Device# configure terminal
Device(config)# crypto gdoi group mygroup
Device(config-gdoi-group)# server local
Device(gdoi-local-server)# group size small 16
Device(gdoi-local-server)# end
```

キー サーバ識別子の設定

次の例では、KS に KSSID および KSSID の範囲を割り当てる方法を示します。

```
Device> enable
Device# configure terminal
Device(config)# crypto gdoi group mygroup
Device(config-gdoi-group)# server local
Device(gdoi-local-server)# identifier
Device(gdoi-local-server-id)# range 10 - 20
Device(gdoi-local-server-id)# value 0
Device(gdoi-local-server-id)# end
```

スイート B の IPsec SA の設定

次の例では、スイート B の IPsec SA を設定する方法を示します。この例では、アイデンティティ アドレスではなくアイデンティティ番号を使用します。

```
Device> enable
Device# configure terminal
Device(config)# crypto ipsec transform-set g1 esp-gcm 192
Device(config)# crypto ipsec profile profile1
Device(ipsec-profile)# set transform-set transformset1
Device(ipsec-profile)# exit
Device(config)# crypto gdoi group gdoigroupname
Device(config-gdoi-group)# identity number 3333
Device(config-gdoi-group)# server local
Device(gdoi-local-server)# sa ipsec 1
Device(gdoi-sa-ipsec)# profile gdoi-p
Device(gdoi-sa-ipsec)# match address ipv4 102
Device(gdoi-sa-ipsec)# end
```

例：GET VPN スイート B のグループ メンバーの設定

スイート B の KEK の暗号化アルゴリズムまたはハッシュ アルゴリズムの設定

次の例は、GM によって許可される KEK のスイート B 暗号化およびハッシュ アルゴリズムの設定方法について説明します。この例では、アイデンティティ アドレスを使用します（IPv4データ プレーン構成とのみ互換性）。代わりにアイデンティティ番号を使用できます（IPv4 および IPv6 データ プレーン構成と互換性）。

```
Device> enable
Device# configure terminal
Device(config)# crypto gdoi group gdoigroupone
Device(config-gdoi-group)# identity address ipv4 10.2.2.2
Device(config-gdoi-group)# server address ipv4 10.0.5.2
Device(config-gdoi-group)# client rekey encryption 3des-cbc aes 192 aes 256
Device(config-gdoi-group)# client rekey hash sha384
Device(config-gdoi-group)# end
```

スイート B の TEK の受け入れ可能トランスフォーム セットの設定

次の例は、データ暗号化または認証のために TEK が使用する受け入れ可能トランスフォーム セットを設定する方法を示します。

```
Device> enable
Device# configure terminal
Device(config)# crypto ipsec transform-set g1 esp-gcm 192
Device(cfg-crypto-trans)# exit
Device(config)# crypto gdoi group gdoigroupone
Device(config-gdoi-group)# client transform-sets g1
Device(config-gdoi-group)# end
```

その他の参考資料

関連資料

関連項目	マニュアル タイトル
Cisco IOS セキュリティ コマンド	『*Cisco IOS Security Command References*』
IKE および IKE ポリシーの設定作業 IPsec トランスフォームの設定作業	『Internet Key Exchange for IPsec VPNs Configuration Guide, Cisco IOS Release 15.2M&T』の「Configuring Internet Key Exchange for IPsec VPNs」モジュール

関連項目	マニュアル タイトル
エンタープライズ ネットワークの GET VPN の有効化のための基本的な導入ガイドライン	『Cisco IOS GET VPN Solutions Deployment Guide』

標準および RFC

標準/RFC	タイトル
連邦情報処理標準（FIPS）パブリケーション 140-2	『Security Requirements for Cryptographic Modules』
RFC 2401	『Security Architecture for the Internet Protocol』
RFC 4106	『The Use of Galois/Counter Mode (GCM) in IPsec Encapsulating Security Payload (ESP)』
RFC 4543	『The Use of Galois Message Authentication Code (GMAC) in IPsec ESP and AH』
RFC 4869	『Suite B Cryptographic Suites for IPsec』
RFC 6054	『Using Counter Modes with Encapsulating Security Payload (ESP) and Authentication Header (AH) to Protect Group Traffic』
RFC 6407	『The Group Domain of Interpretation』

シスコのテクニカル サポート

説明	リンク
右の URL にアクセスして、シスコのテクニカル サポートを最大限に活用してください。これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

スイート B での GET VPN のサポートの機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだ

けを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *304* : スイート *B* での *GET VPN* のサポートの機能情報

機能名	リリース	機能情報
スイート B での GET VPN のサポート		スイート B での GET VPN のサポート機能では、Cisco Group Encrypted Transport（GET）VPN に対してスイート B の暗号方式セットのサポートが追加されます。スイート B は、Galois Counter Mode Advanced Encryption Standard（GCM-AES）を含む暗号化アルゴリズムとハッシュ、デジタル署名、キー交換用のアルゴリズムのセットです。IP Security（IPsec）VPN 用のスイート B は、RFC 4869 で使用法が定義されている標準です。スイート B は Cisco IPsec VPN に包括的なセキュリティ拡張機能を提供し、大規模な展開に対して追加のセキュリティを有効にします。スイート B は、リモート サイト間のワイドエリア ネットワーク（WAN）に高度な暗号化セキュリティを必要とする組織に対して推奨されるソリューションです。 次のコマンドが導入または変更されました。 **client rekey hash, crypto key export ec, crypto key generate ec keysize, crypto key import ec, group size, identifier, rekey sig-hash algorithm, show crypto gdoi.**

第 226 章

Cisco TrustSec の IPsec インライン タギングの GET VPN サポート

Cisco TrustSec（CTS）アーキテクチャは、信頼できるネットワーク デバイスのドメインを確立することによってネットワークを保護します。ネットワーク デバイスがネットワークに認証されると、クラウド内のデバイス間のリンクを使用する通信は、暗号化、メッセージ整合性チェック、およびリプレイ保護メカニズムを組み合わせることで保護されます。

CTS は認証時に取得したユーザとデバイスの ID 情報を使用して、ネットワークに進入するパケットを分類します。CTS では、ネットワークへの進入時にセキュリティ グループ タグ（SGT）でパケットまたはフレームにタグを付けることで各パケットまたはフレームの分類が維持されます。これにより、パケットはデータ パス全体を通じて識別され、セキュリティおよびその他のポリシー基準が適用されます。タグにより、スイッチやファイアウォールなどの中継ネットワークは分類に基づいてアクセス コントロール ポリシーを適用することができます。

Cisco TrustSec の IPsec インライン タギングの GET VPN サポート機能では、GET VPN インライン タギングを使用してプライベート WAN 経由で SGT 情報を伝送します。

Cisco TrustSec 用の IPsec インライン タギングの GET VPN のサポートの前提条件

この機能を有効にするすべてのキー サーバ（KS）およびグループ メンバー（GM）で、GET VPN ソフトウェア バージョン 1.0.5 以降を実行している必要があります。この機能は、GET VPN ネットワーク内のすべてのデバイスをこの機能をサポートする GET VPN ソフトウェア バージョンにアップグレードしてから使用する必要があります。

この機能は、ネットワークのすべてのデバイスが Cisco TrustSec の IPsec インライン タギングをサポートするバージョンを実行しているかどうかを確認するために KS（またはプライマリ KS）で使用するコマンドを提供します。詳細については「GM が Cisco TrustSec の IPsec インライン タギングをサポートするソフトウェア バージョンを実行していることを確認する」セクションを参照してください。

Cisco TrustSec 用の IPsec インライン タギングの GET VPN のサポートの制約事項

- この機能は、IPv6 トラフィックをサポートしません。
- この機能は、Cisco ASR 1000 シリーズ アグリゲーション サービス ルータ、または第 2 世代シスコ サービス統合型ルータ（ISR G2）用の Cisco VPN 内部サービス モジュールのトランスポート モードをサポートしません。

Cisco TrustSec の IPsec インライン タギングの GET VPN サポートに関する情報

セキュリティ グループ タギング機能のグループ メンバー登録

KS はグループ メンバー（GM）からセキュリティ アソシエーション（SA）登録要求を受信するか、連携 KS から接続確立要求を受信すると、グループ SA が SGT インライン タギングを有効にしているかどうかを確認します。有効にしている場合、承認を得るためには、すべての GM と連携 KS が GET VPN ソフトウェア バージョン 1.0.5 以降を使用して登録する必要があります。そうでない場合、登録要求または確立要求は拒否され、KS はネットワーク管理者に通知する syslog メッセージを生成します。

セキュリティ グループ タギングが有効な SA の作成

（**tag cts sgt** コマンドを使用して）グループ SA で IPsec インラインタギングの GET VPN サポートを有効にして、（**crypto gdoi ks rekey** コマンドを使用して）キー再生成をトリガーすると、KS は互換性のあるソフトウェアバージョンを使用しないグループ内の GM および連携 KS をチェックします。見つかると、警告メッセージが表示されます。

```
WARNING for group GETVPN: some devices cannot support SGT inline tagging. Rekey can cause
 traffic disruption and GM registration failures. Please check 'show crypto gdoi feature
 sgt'.
Are you sure you want to proceed ? [yes/no]:
```

グループ メンバー データ プレーンのセキュリティ グループ タグの処理

出力トラフィックとは、GM の GDOI 保護インターフェイスから送信されるトラフィックです。次の表は、出力パスにおける GM の動作を示したものです。

表 *305*：セキュリティ グループ タグの出力処理

セキュリティ グループ タギングが SA で有効	CTS が SGT を提供	GM データ プレーンの動作
対応	対応	SGT を Cisco メタデータに追加し、暗号化
対応	非対応	SGT なしで暗号化
非対応	はい	SGT なしで暗号化
非対応	非対応	SGT なしで暗号化

入力トラフィックとは、GM の GDOI 保護インターフェイスが受信するトラフィックです。次の表は、入力パスにおける GM の動作を示したものです。

表 *306*：セキュリティ グループ タグの入力処理

セキュリティ グループ タギングが SA で有効	CTS が SGT を提供	GM データ プレーンの動作
対応	対応	CTS の SGT を復号して抽出
対応	非対応	SGT の処理なしで復号
非対応	はい	復号して SGT を無視
非対応	非対応	SGT の処理なしで復号

セキュリティ グループ タギング使用時のパケットのオーバーヘッドとフラグメンテーション

各 GDOI パケットに SGT 情報を含む Cisco メタデータが追加されるため、SGT インライン タギングではパケットのオーバーヘッドが 8 バイト（または、時間ベースのアンチリプレイを有効にすると 16 バイト）増加します。

パケットが GDOI の暗号化の前に分割される場合、各フラグメントはそれに応じた SGT 情報とともにインライン タギングされます。パケットが GDOI 暗号化の後で分割される場合、最初のフラグメントのみが SGT 情報とともにインライン タギングされます。

2 つの方法を使用してフラグメンテーションを処理できます。1 つ目の方法は、Cisco メタデータを介した SGT 情報の伝達に使用される追加分のバイトを収容して暗号化を処理しているインターフェイスで **ip mtu** コマンドを使用することです。2 つ目の方法は、GM の LAN インターフェイスで **ip tcp adjst-mss 1352** コマンドを使用することです。このコマンドにより、LAN セグメントの最終的な IP パケットは 1392 バイト未満となり、それによって SGT を伝送するための任意のオーバーヘッドと Cisco メタデータに対して 108 バイトが提供されます。

MTU の問題に関する設計の詳細については、『Group Encrypted Transport VPN (GETVPN) Design and Implementation Guide』の「Designing Around MTU Issues」のセクションを参照してください。

Cisco TrustSec の IPsec インライン タギングの GET VPN サポートの設定方法

GM が Cisco TrustSec の IPsec インライン タギングをサポートするソフトウェア バージョンを実行していることを確認する

Cisco TrustSec の IPsec インライン タギング機能は、GET VPN ネットワーク内のすべてのデバイスをこの機能をサポートする GET VPN ソフトウェア バージョンにアップグレードしてから使用する必要があります。

ネットワーク内のすべてのデバイスが Cisco TrustSec の IPsec インライン タギングをサポートすることを確認するには、KS（またはプライマリ KS）でこの作業を実行します。

手順の概要

1. **enable**
2. **show crypto gdoi feature cts-sgt**
3. **show crypto gdoi feature cts-sgt | include No**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**show crypto gdoi feature cts-sgt** 例： `Device# show crypto gdoi feature cts-sgt`	GET VPN ネットワーク内の各 KS および GM で実行されている GET VPN ソフトウェアのバージョンを表示し、そのデバイスが Cisco TrustSec の IPsec インラインタギングをサポートしているかどうかを表示します。
ステップ 3	**show crypto gdoi feature cts-sgt | include No** 例： `Device# show crypto gdoi feature cts-sgt | include No`	（オプション）Cisco TrustSec の IPsec インライン タギングをサポートしていないデバイスのみ表示します。

Cisco TrustSec の IPsec インライン タギングの設定

Cisco TrustSec の IPsec インライン タギングを設定するには、次のステップを実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **crypto gdoi group** *group-name*
4. 次のいずれかのコマンドを入力します。
   - **identity number** *number*
   - **identity address ipv4** *address*
5. **server local**
6. **sa ipsec** *sequence-number*
7. **tag cts sgt**
8. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。

	コマンドまたはアクション	目的
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**crypto gdoi group** *group-name* 例： `Device(config)# crypto gdoi group GET-SGT`	GDOI グループを指定し、GDOI グループ コンフィギュレーション モードを開始します。

ステップ 4	次のいずれかのコマンドを入力します。
	• **identity number** *number*
	• **identity address ipv4** *address*
	例：
	`Device(config-gdoi-group)# identity number 3333`
	例：
	`Device(config-gdoi-group)# identity address ipv4 10.2.2.2`
		GDOI グループ番号またはアドレスを指定します。

ステップ 5	**server local** 例： `Device(config-gdoi-group)# server local`	デバイスを GDOI KS として指定し、GDOI ローカル サーバ コンフィギュレーション モードを開始します。
ステップ 6	**sa ipsec** *sequence-number* 例： `Device(gdoi-local-server)# sa ipsec 1`	GDOI グループに使用される IPsec SA ポリシー情報を指定し、GDOI SA IPsec コンフィギュレーション モードを開始する。
ステップ 7	**tag cts sgt** 例： `Device(gdoi-sa-ipsec)# tag cts sgt`	Cisco TrustSec の IPSec インライン タギングを有効化します。
ステップ 8	**end** 例： `Device(gdoi-sa-ipsec)# end`	GDOI SA IPsec コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

IPsec インライン タギングを有効にした後、キー再生成をトリガーする必要があります。詳細については「キー再生成のトリガー」セクションを参照してください。

キー再生成のトリガー

KS（またはプライマリ KS）でセキュリティ ポリシーを変更し（たとえば、DES から AES）、グローバル コンフィギュレーション モードを終了すると、ポリシーが変更され、キー再生成が必要であることを示す syslog メッセージが KS に表示されます。実行コンフィギュレーションの最新のポリシーに基づくキー再生成を送信するために、次のようにキー再生成をトリガーするコマンドを入力します。

キー再生成をトリガーするには KS（プライマリ KS）でこの作業を実行します。

手順の概要

1. **enable**
2. **crypto gdoi ks** [**group** *group-name*] **rekey** [**replace-now**]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**crypto gdoi ks** [**group** *group-name*] **rekey** [**replace-now**] 例： `Device# crypto gdoi ks group mygroup rekey`	すべての GM のキー再生成をトリガーします。 オプションの **replace-now** キーワードは、各 GM の古い TEK および KEK を即時に置き換え、SA が期限切れになる前に新しいポリシーを有効にします。 （注） **replace-now** キーワードを使用すると、一時的なトラフィックの不連続を引き起こすことがあります。

例

KS に次のようにメッセージが表示されます。

```
Device# crypto gdoi ks rekey
Device#
*Jan 28 09:17:44.363: %GDOI-5-KS_SEND_UNICAST_REKEY: Sending Unicast Rekey with
policy-replace for group GET from address 10.0.8.1 with seq # 2
```

ポリシーの変更後、各 GM がこのトリガーされたキー再生成を受信すると、新しい SA（たとえば、AES 用）をインストールして、古い SA（たとえば、DES 用）のライフタイムを短縮します。各 GM はこの短縮されたライフタイムが期限切れになるまで古い SA を使用してトラフィックの暗号化および復号化を続けます。

セカンダリ KS のキー再生成をトリガーしようとすると、次のようにコマンドが拒否されます。

```
Device# crypto gdoi ks rekey
ERROR for group GET: This command must be executed on Pri-KS
```

Cisco TrustSec 用の IPsec インライン タギングの GET VPN のサポートの確認とトラブルシューティング

GM で実行されている設定を表示するには、**show running-config** コマンドを使用します。

SGT でタグ付けされたパケットの数を表示するには、次のコマンドを入力します。

```
Device# show crypto ipsec sa detail

interface: Ethernet0/0
   Crypto map tag: GET, local addr 5.0.0.2
   protected vrf: (none)
   local  ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
   remote ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
   Group: GET-SGT
.
.
.
#pkts tagged (send): 0, #pkts untagged (rcv): 5
```

pkts tagged (send) フィールドは、アウトバウンド方向の SGT でタグ付けされたパケットを表示します。pkts untagged (rcv) フィールドは、インバウンド方向の SGT でタグ付けされていないパケットを表示します。

Cisco TrustSec の IPsec インライン タギングの GET VPN サポートの設定例

例：GM が Cisco TrustSec の IPsec インライン タギングをサポートするソフトウェア バージョンを実行していることを確認する

次の例は、各グループ内のすべてのデバイスが Cisco TrustSec の IPsec インライン タギングをサポートしているかどうかを確認するために KS（またはプライマリ KS）で GET VPN ソフトウェア バージョン管理コマンドを使用する方法を示します。

```
Device# show crypto gdoi feature cts-sgt

Group Name: GETVPN
    Key Server ID       Version   Feature Supported
        10.0.5.2         1.0.5          Yes
        10.0.6.2         1.0.5          Yes
        10.0.7.2         1.0.3          No
        10.0.8.2         1.0.2          No
```

```
    Group Member ID     Version   Feature Supported
        10.0.1.2         1.0.2          No
        10.0.2.5         1.0.3          No
        10.0.3.1         1.0.5          Yes
        10.0.3.2         1.0.5          Yes
```

また、上記のコマンドは GM でも入力できます（その GM の情報を表示します。KS や他の GM には使用できません）。

次の例は、KS（プライマリ KS）で Cisco TrustSec の IPsec インライン タギングをサポートしていない GET VPN ネットワークのデバイスのみ検索するコマンドを入力する方法を示しています。

```
Device# show crypto gdoi feature cts-sgt | include No

        10.0.7.2         1.0.3          No
        10.0.8.2         1.0.2          No
        10.0.1.2         1.0.2          No
        10.0.2.5         1.0.3          No
```

例：Cisco TrustSec の IPsec インライン タギングの設定

次に、単一の GDOI グループを提供する KS 用の IPsec SA の CTS SGT インライン タギングを設定する方法の例を示します。

```
Device> enable
Device# configure terminal
Device(config)# ip access-list extended ACL-SGT
Device(config-ext-nacl)# permit ip any any
Device(config-ext-nacl)# exit
Device(config)# crypto gdoi group GET-SGT
Device(config-gdoi-group)# identity number 1
Device(config-gdoi-group)# server local
Device(gdoi-local-server)# sa ipsec 1
Device(gdoi-sa-ipsec)# tag cts sgt
Device(gdoi-sa-ipsec)# profile gdoi-p2
Device(gdoi-sa-ipsec)# match address ipv4 ACL-SGT
Device(gdoi-sa-ipsec)# replay time window-size 100
Device(gdoi-sa-ipsec)# end
```

次に、GET VPN バージョン 1.0.5 以降 にアップグレードした GM を使用する（したがって CTS SGT インライン タギングをサポートしている）グループと、まだアップグレードしていない GM を使用するグループの、2 つのグループを設定する方法の例を示します。アップグレード済みの GM は、グループ番号 1111（小さい暗号マップ シーケンス番号）にグループ番号 2222（大きい暗号マップ シーケンス番号）とともに登録します。アップグレードしていない GM はグループ番号 2222 にのみ登録します。

この例では、2 つのサイト間のトラフィックに対して SGT タギングを設定します。**permit ip** コマンドは、2 つのサイト間の通信を許可するアクセス制御リスト（ACL）にアクセス制御エントリ（ACE）を追加します。

```
Device> enable
Device# configure terminal
Device(config)# ip access-list extended ACL_NET_AB
Device(config-ext-nacl)# permit ip 10.1.0.0 0.0.255.255 10.2.0.0 0.0.255.255
Device(config-ext-nacl)# permit ip 10.2.0.0 0.0.255.255 10.1.0.0 0.0.255.255
Device(config-ext-nacl)# exit
Device(config)# ip access-list extended ACL_ALL
Device(config-ext-nacl)# permit ip any any
Device(config-ext-nacl)# exit
Device(config)# crypto gdoi group GET1
Device(config-gdoi-group)# identity number 1111
Device(config-gdoi-group)# server local
Device(gdoi-local-server)# rekey authentication mypubkey rsa mykey
Device(gdoi-local-server)# rekey transport unicast
Device(gdoi-local-server)# sa ipsec 1
Device(gdoi-sa-ipsec)# tag cts sgt
Device(gdoi-sa-ipsec)# profile gdoi-p2
Device(gdoi-sa-ipsec)# match address ipv4 ACL_NET_AB
Device(gdoi-sa-ipsec)# replay time window-size 100
Device(gdoi-sa-ipsec)# exit
Device(gdoi-local-server)# exit
Device(config-gdoi-group)# exit
Device(config)# crypto gdoi group GET2
Device(config-gdoi-group)# crypto gdoi group GET2
Device(config-gdoi-group)# server local
Device(gdoi-local-server)# rekey authentication mypubkey rsa mykey
Device(gdoi-local-server)# rekey transport unicast
Device(gdoi-local-server)# sa ipsec 1
Device(gdoi-sa-ipsec)# profile gdoi-p2
Device(gdoi-sa-ipsec)# match address ipv4 ACL_ALL
Device(gdoi-sa-ipsec)# replay time window-size 100
Device(gdoi-sa-ipsec)# end
```

（注） GET VPN は、ACL あたり最大 100 の ACE をサポートします。

例：グループ メンバーのキー再生成のトリガー

GM がキー再生成のトリガーをサポートするソフトウェア バージョンを実行していることを確認する

次の例は、GET VPN ネットワークのデバイスのソフトウェアのバージョンを表示し、またポリシー変更後のキー再生成のトリガーをサポートするかどうかを表示するために、KS（またはプライマリ KS）で GET VPN ソフトウェア バージョン管理コマンドを使用する方法を示します。

```
Device# show crypto gdoi feature policy-replace

Key Server ID       Version  Feature Supported
  10.0.8.1         1.0.2          Yes
  10.0.9.1         1.0.2          Yes
  10.0.10.1        1.0.2          Yes
  10.0.11.1        1.0.2          Yes
```

```
 Group Member ID     Version  Feature Supported
  5.0.0.2          1.0.2          Yes
  9.0.0.2          1.0.1          No
```

次の例は、ポリシー交換後のキー再生成のトリガーをサポートしていないデバイスのみを検索する方法を示します。

```
Device# show crypto gdoi feature policy-replace  | include No

       9.0.0.2          1.0.1          No
```

これらのデバイスでは、プライマリ KS はポリシー交換に関する手順なしでトリガーされるキー再生成のみを送信します。したがって、GM がキー再生成を受信すると、新しい SA をインストールしますが、古い SA の有効期間は短縮しません。

キー再生成のトリガー

次の例では、ポリシー変更の実行後にキー再生成をトリガーする方法を示します。この例では、**profile gdoi-p2** コマンドで IPSec ポリシーの変更（たとえば、DES から AES）が発生します。

```
Device# configure terminal
Device(config)# crypto gdoi group GET
Device(config-gdoi-group)# server local
Device(gdoi-local-server)# sa ipsec 1
Device(gdoi-sa-ipsec)# no profile gdoi-p
Device(gdoi-sa-ipsec)# profile gdoi-p2
Device(gdoi-sa-ipsec)# end
Device#

*Jan 28 09:15:15.527: %SYS-5-CONFIG_I: Configured from console by console
*Jan 28 09:15:15.527: %GDOI-5-POLICY_CHANGE: GDOI group GET policy has changed. Use
'crypto gdoi ks rekey' to send a rekey, or the changes will be send in the next scheduled

rekey
Device# crypto gdoi ks rekey
Device#
*Jan 28 09:17:44.363: %GDOI-5-KS_SEND_UNICAST_REKEY: Sending Unicast Rekey with
policy-replace for group GET from address 10.0.8.1 with seq # 2
```

次の例では、セカンダリ KS のキー再生成をトリガーしようとすると表示されるエラーメッセージを示します。

```
Device# crypto gdoi ks rekey

ERROR for group GET: This command must be executed on Pri-KS
```

（注） 時間ベースのアンチリプレイ（TBAR）が設定されると、キー サーバは 2 時間（7200 秒）ごとに定期的にキー再生成をグループ メンバーに送信します。次の例では、有効期間が 8 時間（28800 秒）に設定されていますが、キー再生成タイマーは 2 時間に設定されています。

```
Device(config)# crypto ipsec profile atm-profile
Device(ipsec-profile)# set security-association lifetime seconds 28800
!
Device(ipsec-profile)# exit
Device(config)# crypto gdoi group ATM-DSL
Device(config-gdoi-group)# server local
Device(gdoi-sa-ipsec)# sa ipsec 1
!
Device(gdoi-sa-ipsec)# replay time window-size 100
```

show crypto gdoi gm replay コマンドおよび **show crypto gdoi ks replay** コマンドにより TBAR 情報が表示されます。

Cisco TrustSec 用の IPsec インライン タギングの GET VPN のサポートのその他の参考資料

関連資料

関連項目	マニュアル タイトル
Cisco IOS セキュリティ コマンド	『*Cisco IOS Security Command References*』
エンタープライズ ネットワークの GET VPN の有効化のための基本的な導入ガイドライン	『Cisco IOS GET VPN Solutions Deployment Guide』
Cisco TrustSec の設定	『Cisco TrustSec Configuration Guide, Cisco IOS Release 15M&T』
MTU の問題の迂回設計	『Group Encrypted Transport VPN (GETVPN) Design and Implementation Guide』

標準および RFC

標準/RFC	タイトル
RFC 2401	『Security Architecture for the Internet Protocol』
RFC 6407	『The Group Domain of Interpretation』

シスコのテクニカル サポート

説明	リンク
右の URL にアクセスして、シスコのテクニカル サポートを最大限に活用してください。これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

Cisco TrustSec 用の IPsec インライン タギングの GET VPN のサポートの機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *307 : Cisco TrustSec* 用の *IPsec* インライン タギングの *GET VPN* のサポートの機能情報

機能名	リリース	機能情報
Cisco TrustSec の IPsec インライン タギングの GET VPN サポート		

機能名	リリース	機能情報
		Cisco TrustSec（CTS）アーキテクチャは、信頼できるネットワーク デバイスのドメインを確立することによってネットワークを保護します。ネットワーク デバイスがネットワークに認証されると、クラウド内のデバイス間のリンクを使用する通信は、暗号化、メッセージ整合性チェック、およびリプレイ保護メカニズムを組み合わせることで保護されます。 CTS は認証時に取得したユーザとデバイスの ID 情報を使用して、ネットワークに進入するパケットを分類します。CTS では、ネットワークへの進入時にセキュリティ グループ タグ（SGT）でパケットまたはフレームにタグを付けることで各パケットまたはフレームの分類が維持されます。これにより、パケットはデータ パス全体を通じて識別され、セキュリティおよびその他のポリシー基準が適用されます。タグにより、スイッチやファイアウォールなどの中継ネットワークは分類に基づいてアクセス コントロール ポリシーを適用することができます。 Cisco TrustSec の IPsec インライン タギングの GET VPN サポート機能では、GET VPN インライン タギングを使用してプライベート WAN 経由で SGT 情報を伝送します。 次のコマンドが導入または変更されました。 **show crypto gdoi, show crypto ipsec sa, tag cts sgt.**

第 227 章

GETVPN GDOI バイパス

GETVPN GDOI バイパス機能では、デフォルトのグループ ドメイン オブ インタープリテーション（GDOI）バイパス暗号化ポリシーの有効化と無効化をサポートします。また、有効にすると、デフォルト GDOI バイパス暗号化ポリシーの強化もサポートされます。

GETVPN GDOI バイパスの制約事項

キー サーバ（KS）がグループ メンバー（GM）の後ろに配置されるときは、ローカルの拒否アクセス コントロール リスト（ACL）を明示的に設定し、トランスポート プロトコルとして UDP を、送信元または宛先のいずれかとしてポート 848 を使用するトラフィック（UDP 848 トラフィック）が通過できるようにする必要があります。

GETVPN GDOI バイパスに関する情報

GDOI バイパス暗号化ポリシー

Cisco IOS の Group Encrypted Transport VPN（GETVPN）は、グループはキー管理プロトコルとしてグループ ドメイン オブ インタープリテーション（GDOI）を使用します。

グループ メンバー（GM）は暗号化と復号を担当するデバイスです。つまり、GET VPN データ プレーンを処理するデバイスです。

キー サーバ（KS）は、GET VPN コントロール プレーンを作成し、維持するデバイスです。トラフィック、暗号化プロトコル、セキュリティ アソシエーション、キー再生成タイマーなどの

すべての暗号化ポリシーは KS で一元的に定義され、登録時にすべての GM にプッシュされます。

デフォルト GDOI バイパス暗号化ポリシーの有効化と無効化

新しいグループ メンバー（GM）設定では、GM ローカル アクセス コントロール リスト（ACL）を明示的に設定することによって、ユーザはグループ ドメイン オブ インタープリテーション（GDOI）バイパス暗号化ポリシーを無効にし、トラフィックの例外を制御することができます。

デフォルト GDOI バイパス暗号化ポリシーの強化

セキュリティを強化するため、デフォルトのグループ ドメイン オブ インタープリテーション（GDOI）バイパス暗号化ポリシーを適用する一方、次の変更が実施されています。

- デフォルト GDOI バイパス暗号化ポリシーは、Group Encrypted Transport VPN（GETVPN）保護インターフェイス（GDOI 暗号マップが適用されるインターフェイス）にのみインストールされます。登録またはキー再生成に使用するグループ メンバー（GM）のアドレス宛ての UDP848 トラフィックのみが許可されます。
- GM VRF 認識型機能を使用して GDOI データ プレーンとコントロール プレーンが異なる VRF にあることを指定する場合、デフォルト GDOI バイパス暗号化ポリシーの自動挿入は GDOI 保護インターフェイスに適用されません。
- UDP をトランスポート プロトコルとして、ポート 848 を送信元または宛先（UDP 848 トラフィック）として使用するトラフィックが他の非 GDOI 保護インターフェイスに着信すると予想される場合は、非 GDOI 暗号マップの例外を明示的に設定する必要があります。
- 複数グループの暗号マップ セットを設定する場合、インストールされる全体の GDOI バイパス暗号化ポリシーは、セキュリティ アソシエーション データベース（SADB）内の各グループの GDOI バイパス暗号化ポリシーすべての統合です。

以下に説明する条件のいずれかにより、GETVPN 保護インターフェイスに適用されるデフォルト GDOI バイパス暗号化ポリシーの再計算がトリガーされます。

- **no client bypass-policy** コマンドを使用して **client bypass-policy** 設定を削除。
- インターフェイスの GDOI バイパス暗号マップの適用または削除。
- 暗号マップ セットの GDOI バイパス暗号マップの適用または削除。
- GDOI 保護インターフェイスの IP アドレスの変更（**no client registration interface** が使用される場合）。
  - **client registration interface** が使用される場合、次の場合に GETVPN 保護インターフェイスに適用されるデフォルト GDOI バイパス暗号化ポリシーの再計算がトリガーされます。
    - **no client registration interface** から **client registration interface** に変更

- クライアント登録インターフェイスに対する変更（たとえば、ループバック 0 からループバック 1）
- クライアント登録インターフェイス アドレスの変更

GETVPN GDOI バイパスの設定方法

デフォルト GDOI バイパス暗号化ポリシーの有効化

手順の概要

1. **enable**
2. **configure terminal**
3. **crypto gdoi group** *group-name*
4. **client bypass-policy**
5. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**crypto gdoi group** *group-name* 例： `Device(config)# crypto gdoi group GETVPN`	GDOI グループを指定し、GDOI グループ コンフィギュレーション モードを開始します。
ステップ 4	**client bypass-policy** 例： `Device(config-gdoi-group)# client bypass-policy`	デフォルト GDOI バイパス暗号化ポリシーを有効化します。
ステップ 5	**end** 例： `Device(config-gdoi-group)# end`	GDOI グループ コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

デフォルト GDOI バイパス暗号化ポリシーの無効化

手順の概要

1. **enable**
2. **configure terminal**
3. **crypto gdoi group** *group-name*
4. **no client bypass-policy**
5. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**crypto gdoi group** *group-name* 例： `Device(config)# crypto gdoi group GETVPN`	GDOI グループを指定し、GDOI グループ コンフィギュレーション モードを開始します。
ステップ 4	**no client bypass-policy** 例： `Device(config-gdoi-group)# no client bypass-policy`	デフォルト GDOI バイパス暗号化ポリシーを無効にします。
ステップ 5	**end** 例： `Device(config-gdoi-group)# end`	GDOI グループ コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

デフォルト GDOI バイパス暗号化ポリシーの有効性と無効性の確認

手順の概要

1. **enable**
2. **show crypto gdoi gm acl**
3. **show crypto gdoi gm acl**

手順の詳細

ステップ 1 enable

特権 EXEC モードを有効にします。

- パスワードを入力します（要求された場合）。

例：

```
Device> enable
```

ステップ 2 show crypto gdoi gm acl

デフォルト GDOI バイパス暗号化ポリシーの有効性を確認します。

（注） VRF は、非グローバルである場合にのみ表示されます。

例：

```
Device# show crypto gdoi gm acl

Group Name: GETVPN
 ACL Downloaded From KS 10.0.0.2:
   access-list   deny eigrp any any
   access-list   permit ip any any
 ACL Configured Locally:
 ACL of default GDOI bypass policy:
   Ethernet1/0: deny udp host 10.0.0.9 eq 848 any eq 848 vrf RED*
```

ステップ 3 show crypto gdoi gm acl

デフォルト GDOI バイパス暗号化ポリシーの無効性を確認します。

例：

```
Device# show crypto gdoi gm acl

Group Name: GETVPN
 ACL Downloaded From KS 10.0.0.2:
   access-list   deny eigrp any any
   access-list   permit ip any any
 ACL Configured Locally:
 ACL of default GDOI bypass policy: Disabled
```

GETVPN GDOI バイパスの設定例

例：デフォルト GDOI バイパス暗号化ポリシーの有効化

```
Device> enable
Device# configure terminal
Device(config)# crypto gdoi group getvpn
```

```
Device(config-gdoi-group)# client bypass-policy
Device(config-gdoi-group)# end
```

例：デフォルト GDOI バイパス暗号化ポリシーの無効化

```
Device> enable
Device# configure terminal
Device(config)# crypto gdoi group getvpn
Device(config-gdoi-group)# no client bypass-policy
Device(config-gdoi-group)# end
```

GETVPN GDOI バイパスのその他の参考資料

関連資料

関連項目	マニュアル タイトル
Cisco IOS セキュリティ コマンド	『*Cisco IOS Security Command References*』
エンタープライズ ネットワークの GET VPN の有効化のための基本的な導入ガイドライン	『*Cisco IOS GET VPN Solutions Deployment Guide*』
GET VPN ネットワークの設計と実装	『*Group Encrypted Transport VPN (GETVPN) Design and Implementation Guide*』

標準および RFC

標準/RFC	タイトル
RFC 6407	『*The Group Domain of Interpretation*』

シスコのテクニカル サポート

説明	リンク
シスコのサポート Web サイトでは、シスコの製品やテクノロジーに関するトラブルシューティングにお役立ていただけるように、マニュアルやツールをはじめとする豊富なオンライン リソースを提供しています。 お使いの製品のセキュリティ情報や技術情報を入手するために、Cisco Notification Service（Field Notice からアクセス）、Cisco Technical Services Newsletter、Really Simple Syndication（RSS）フィードなどの各種サービスに加入できます。 シスコのサポート Web サイトのツールにアクセスする際は、Cisco.com のユーザ ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

GETVPN GDOI バイパスの機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *308 : GETVPN GDOI* バイパスの機能情報

機能名	リリース	機能情報
GETVPN GDOI バイパス		次のコマンドが導入されました。**client bypass-policy** および **show crypto gdoi gm acl**。

第 228 章

GETVPN G-IKEv2

Cisco Group Encrypted Transport VPN（GET VPN）には、シスコ デバイス上で発生する、またはシスコ デバイスを経由するエンタープライズ プライベート WAN 上の IP マルチキャスト トラフィック グループまたはユニキャスト トラフィックの安全を守るために必要な一連の機能が含まれます。GETVPN G-IKEv2 機能は GETVPN にインターネット キー エクスチェンジ バージョン 2（IKEv2）プロトコルを実装するため、GETVPN は IKEv2 のメリットを享受できます。

GETVPN G-IKEv2 の制約事項

- キー サーバ（KS）には Group Key Management（GKM）と Group Domain of Interpretation（GDOI）の両方を設定できますが、グループ メンバー（GM）には GKM と GDOI のいずれかを設定できます。
- COOP 用の IKEv2 はサポートされていません。G-IKEv2 セットアップではキーサーバー間の COOP に IKEv1 を使用してください。
- EAP は現在、G-IKEv2 ではサポートされていません。
- GETVPN G-IKEv2 は IP-D3P をサポートしていません。G-IKEv2 を使用した IP-D3P は、引き続き GETVPN グループメンバー（GM）でサポートされています。

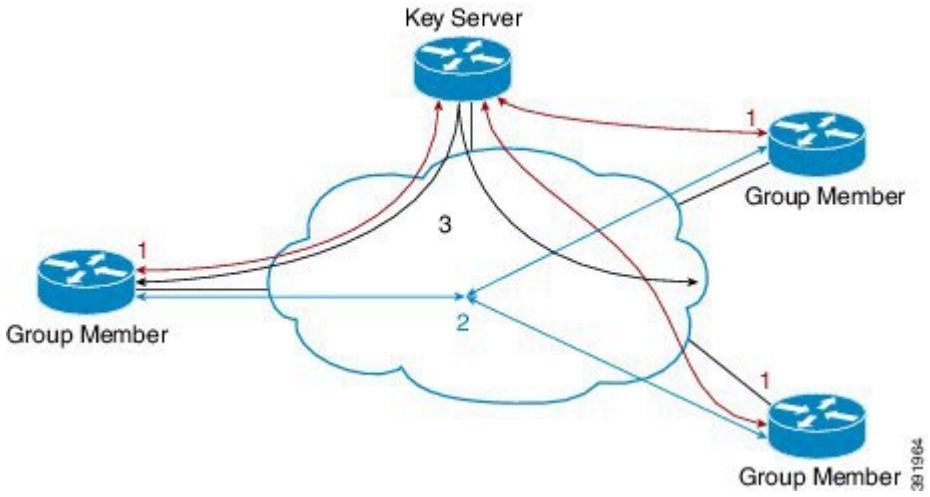
GETVPN G-IKEv2 に関する情報

GETVPN G-IKEv2 の概要

Cisco Group Encrypted Transport バーチャル プライベート ネットワーク（GETVPN）アーキテクチャは、Group Domain of Interpretation（GDOI）プロトコルに基づいています。GETVPN では、Internet Security Exchange and Key Management Protocol（ISAKMP）を使用して、新しいグループ メンバーの認証、暗号化ポリシーのダウンロード、およびグループ メンバーへのトラフィック暗号キー（TEK）と Key Encryption Key（KEK）の配信を行います。ただし、インターネット キー エクスチェンジ バージョン 2（IKEv2）は置き換えられます。IKEv2 は、ネットワーク遅延を軽減し、メッセージ交換の複雑さを軽減し、相互運用性と信頼性を向上させ、ハッシュ認証の暗号化の問題を修正します。GET VPN は IKEv2 プロトコルと IPsec を組み合わせ、GETVPN G-IKEv2 機能によって IP マルチキャスト トラフィックまたはユニキャスト トラフィックを保護する効果的な方法を提供します。この機能では、シスコのすべての VPN Technologies を利用して完全な IKEv2 ソリューションを提供します。

G-IKEv2 プロトコルは、グループ メンバー（GM）に対し、キー サーバ（KS）からポリシーおよびキーをダウンロードするメカニズムを提供します。これらのポリシーおよびキーは、グループ内の GM 間の通信を保護するために使用されます。G-IKEv2 は、企業のプライベート WAN におけるリモート ロケーション間のグループ通信を保護する新しいモデルです。次の図は、G-IKEv2 を使用して GM を KS に登録し、KS から GM にキーおよびポリシーをダウンロードする GETVPN の基本システム アーキテクチャを示しています。

図 *127 : G-IKEv2* プロトコルを使用する *GETVPN* アーキテクチャ



インターネット キー エクスチェンジ バージョン 2（IKEv2）

RFC 4306 に基づく次世代のキー管理プロトコルであるインターネット キー エクスチェンジ バージョン 2（IKEv2）は、IKE プロトコルの機能拡張です。IKEv2 は、相互認証を実行して

SA を確立および管理するために使用します。IKEv2 の詳細については、『*FlexVPN and Internet Key Exchange Version 2 Configuration Guide*』を参照してください。

次の表では、IKE と IKEv2 間のトンネル パフォーマンスを比較します。

プロトコル	1 秒あたりのトンネル数	最大同時トンネル数
IKE	45	60
IKEv2	89	200

IKEv2 の利点は次のとおりです。

デッド ピア検出とネットワーク アドレス変換トラバーサル

インターネット キー エクスチェンジ バージョン 2（IKEv2）にはデッド ピア検出（DPD）とネットワーク アドレス変換トラバーサル（NAT-T）のサポートが組み込まれています。

証明書の URL

証明書はIKEv2パケット内で送信されるのではなくURLとハッシュを通じて参照できるため、フラグメンテーションを回避できます。

DoS 攻撃の復元力

IKEv2は、要求者を確認するまで要求を処理しません。これにより、偽の場所から大量の暗号化（高コスト）処理を実行するようにスプーフィングされる可能性があるIKEv1でのサービス妨害（DoS）の問題にある程度対処しています。

EAP のサポート

IKEv2 では認証に Extensible Authentication Protocol（EAP）を使用できます。

複数の暗号エンジン

ネットワークに IPv4 と IPv6 の両方のトラフィックがあり、複数の暗号エンジンがある場合、次のいずれかの設定オプションを選択します。

- 1 つのエンジンで IPv4 トラフィックを処理し、他方のエンジンで IPv6 トラフィックを処理する。
- 1 つのエンジンで IPv4 と IPv6 の両方のトラフィックを処理する。

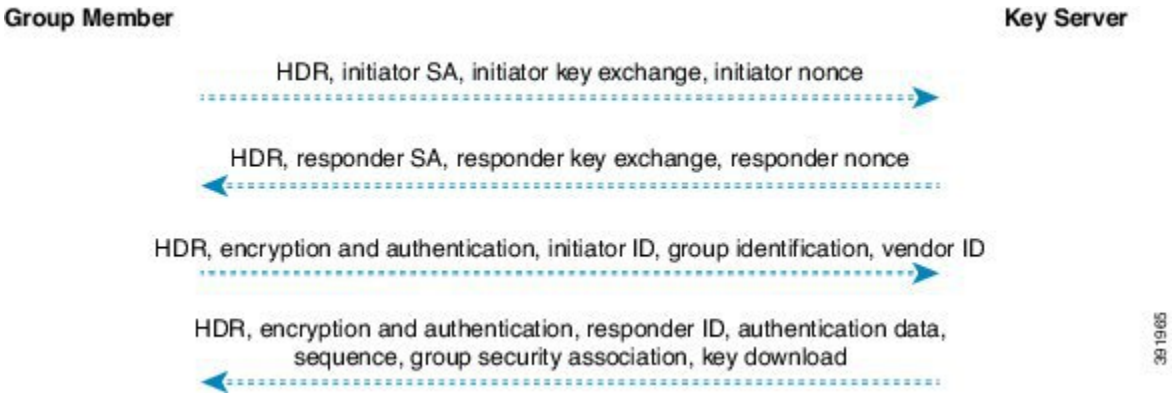
信頼性と状態管理（ウィンドウイング）

IKEv2 では、信頼性を提供するためにシーケンス番号と確認が使用され、エラー処理ロジスティックと共有状態管理が要求されます。

GETVPN G-IKEv2 の交換

GM と KS 間のメッセージ交換は、IKEv2 の標準ドラフトを使用する Internet Engineering Task Force（IETF）のグループ キー管理に準拠しています。

図 *128 : G-IKEv2* メッセージ交換



1. グループ メンバーは、優先される暗号化アルゴリズム（SAi ペイロード）、発信側のキー交換（KE）フェーズ 1 ペイロードの Diffie-Hellman 公開番号、および発信側のナンス ペイロードの存在を保証するための乱数であるナンスを送信することによってキー サーバへの登録要求を開始します。
2. キー サーバはネゴシエート済みの暗号化アルゴリズム（応答側の SA フェーズ 1 ペイロード）、Diffie-Hellman 公開番号（応答側の KE ペイロード）、ナンス（応答側のナンス ペイロード）を使用して応答します。オプションで、認証方式として Rivest、Shamir、Adleman（RSA）デジタル署名を使用するようにキー サーバが設定されている場合、キー サーバも証明書要求を送信します。
3. 登録要求に対するキー サーバの応答を受信すると、グループ メンバーは SAr1 ペイロードの暗号化アルゴリズムと Diffie-Hellman 値を使用してキーを作成し、キー サーバに送信されるメッセージを暗号化します。RSA デジタル署名が認証方式として使用される場合、暗号化されたメッセージには、発信側の ID と、オプションで証明書および証明書要求が含まれます。スイート B の実装の場合、Galois/Counter Mode（GCM）–Advanced Encryption Standard（AES）または Galois Message Authentication Code（GMAC）–Advanced Encryption Standard（AES）トランスフォームとともに使用される送信者 ID を要求するために通知ペイロードが送信されます。

（注） グループ メンバーは、1 日のライフタイムの間、インターフェイスに適用可能な一連の送信元 ID を要求します。登録（長い SA ライフタイムの場合）またはキー再生成（短い SA ライフタイムの場合）のメッセージでライフタイムを受け取ると、グループ メンバーは将来の登録のため送信者 ID の数を計算するためにライフタイムを保存します。

4. グループ マネージャの認証後、キー サーバはグループ マネージャを登録する前にグループ メンバーを承認します。登録後、キー サーバはグループ マネージャにグループ ポリ

シー（GSA ペイロード）およびグループのキーイング マテリアル（KD ペイロード）を送信します。SEQ ペイロードはオプションであり、キー サーバでキー再生成メッセージの現在のシーケンス番号をグループ マネージャに通知する場合に送信されます。これらのペイロードは、GSA_AUTH 応答メッセージに含められます。

グループ メンバーの通信

グループ メンバーは相互に IPsec トンネルを確立するのではなく、IPsec ポリシーおよびキーを使用してグループ内のグループ メンバー間の通信を保護します。

将来の登録

セキュアな登録チャネルがグループ マネージャとキー サーバとの間に確立されると、そのほかのグループの追加のグループ メンバー登録は、確立されたセキュアな登録チャネルを通じて行われます。そのようなシナリオでは、グループ メンバーはグループ ID（IDg）を含む GSA_CLIENT_SERVER 交換を使用して、キー サーバから Key Encryption Key（KEK）またはトラフィック暗号キー（TEK）のいずれかを要求します。

キー サーバのキー再生成

キー サーバはユニキャストまたはマルチキャスト通信を介して G-IKEv2 グループ メンテナンス チャネルを使用するグループ メンバーに新しいグループ キーを配布します。キー再生成は G-IKEv2 のオプションです。キー再生成を使用すると、KS はグループ メンバーにキー再生成メッセージを送信します。このメッセージはキー サーバの設定に応じてユニキャストまたはマルチキャストにできます。キー サーバでは、登録時にグループ メンバーに送信される KEK を使用してキー再生成メッセージを暗号化します。キー再生成メッセージを受信したら、グループ メンバーは、キー再生成メッセージの SEQ 番号が最後に受信した SEQ 番号より大きいことを確認する必要があります。グループ メンバーは、どちらが後でも、登録メッセージまたはキー再生成メッセージのいずれかから SEQ 番号を受け取っているはずです。GDOI（IKEv1）と G-IKEv2 の両方のグループとしてキー サーバ グループが設定されている場合、マルチキャスト キー再生成のため、2 つのキー再生成メッセージ（GDOI 用に 1 つと G-IKEv2 用に 1 つ）が送信されます。ユニキャスト キー再生成の場合、キー サーバはグループ メンバーのモードまたはタイプに応じて GDOI または G-IKEv2 のキー再生成のみを送信します。

（注） キー再生成がユニキャストの場合、グループ メンバーはキー サーバに確認応答を送信する必要があります。

サポートされる機能と GKM のバージョン

GETVPN G-IKEv2 機能では、次のような既存の GETVPN 機能がサポートされています。

- キー再生成と再送信
- GM アクセス コントロール リスト（ACL）

- Fail-Close モード
- 受信専用モード
- アンチリプレイ
- グループ メンバー登録の認証ポリシー
- GDOI MIB
- VRF 認識型グループ メンバー
- グループ メンバーの削除とポリシー交換
- 連携キー サーバ
- GETVPN IPv6 データプレーン
- IPsec インライン タギングのサポート
- GETVPN の復元力のフェーズ 1 とフェーズ 2
- 連携通知メッセージの最適化

GETVPN G-IKEv2 機能は、GKM バージョン 1.0.12 以降のリリースでサポートされています。キーサーバーでサポートされる GKM のバージョンは 1.0.13 で、グループメンバーでサポートされる GKM のバージョンは 1.0.12 です。キーサーバーとグループメンバーのバージョンの違いは、GETVPN キーサーバーでの IP D3P サポートと Cisco GETVPN キーサーバーのインターネットドラフト ACK の機能が、 1.0.13 以降のキーサーバーでのみ使用できるためです。

GDOI から G-IKEv2 への移行

長期にわたって、キー サーバとグループ メンバーを G-IKEv2 にアップグレードして移行することを希望している場合があります。GETVPN グループ全体の GDOI から G-IKEv2 への移行には、慎重な計画が必要です。すべてのグループ メンバーを同時に移行することはできません。移行では、GDOI グループ メンバーと G-IKEv2 グループ メンバーが、GDOI と G-IKEv2 の異なるコントロール プレーン プロトコルを使用する一方で、同じトラフィック暗号キー（TEK）を使用した通信を可能にする必要があります。GDOI から G-IKEv2 への移行の順番は次のとおりです。

- 後方互換性：GETVPN G-IKEv2 機能を含む新しい Cisco IOS ソフトウェア イメージでは既存の GDOI 機能をサポートしている必要があり、Cisco IOS ソフトウェアの以前のリリースの GDOI 機能との互換性が必要です。
- サービス アップグレード：Cisco IOS ソフトウェア イメージを変更する推奨順序は、セカンダリ キー サーバ、プライマリ キー サーバ、およびグループ メンバーです。
- サービス ダウングレード：Cisco IOS ソフトウェア イメージを変更する推奨順序は、グループ メンバー、セカンダリ キー サーバ、プライマリ キー サーバです。

サービス アップグレード手順

1. 既存のキー サーバとグループ メンバーの GDOI 設定を保存します。詳細については、『*Managing Configuration Files Configuration Guide*』の「Configuration Replace and Configuration Rollback」機能モジュールを参照してください。
2. キー サーバの移行中のネットワーク分割およびマージを防ぐため、すべてのキー サーバで Key Encryption Key（KEK）とトラフィック暗号キー（TEK）のライフタイムを設定します。新しいライフタイムを設定するには、crypto gdoi ks rekey コマンドを使用します。
3. 新しい Cisco IOS ソフトウェア イメージにキー サーバをアップグレードします。上記の順序に従います。セカンダリ キー サーバから開始し、プライマリ キー サーバに続きます。キーワード **gdoi** を使用するすべての既存の設定がキーワード **gkm** に変換されます。たとえば、グローバル コンフィギュレーション コマンド **crypto gdoi group** は **crypto gkm group** コマンドに変換されます。ただし、再登録とキー再生成にはグループは引き続き GDOI を使用します。
4. キーサーバーで、GDOI および G-IKEv2 グループメンバーをサポートするグループに対してサーバーローカルコマンドの **gikev2** コマンドを実行します。
5. 新しい Cisco IOS ソフトウェア イメージにグループ メンバーをアップグレードします。キーワード「**gdoi**」を使用するすべての既存の設定がキーワード **gkm** に変換されます。たとえば、グローバル コンフィギュレーション コマンド **crypto gdoi group** と **crypto map gdoi** は、「**crypto gkm group**」と **crypto map gkm** にそれぞれ変換されます。これらのグループは再登録とキー再生成には GDOI を引き続き使用し、**client protocol gdoi** コマンドを含めます。
6. グループメンバーで G-IKEv2 を使用するには、**client protocol gikev2** コマンドを設定します。
7. GDOI グループメンバーへのサービスを停止するには、サーバーのローカルコマンドの **no gdoi** コマンドを設定します。

G-IKEv2 へのアップグレード後に GDOI を使用するグループメンバーに対して、グループメンバーグループ設定の **client protocol gdoi** コマンドを設定します。グループ メンバーは G-IKEv2 の代わりに GDOI を使用してキー サーバに再度登録します。

（注） グループ メンバーを変換する前に、グループ メンバーの登録先のキー サーバが GDOI ローカル サーバ コンフィギュレーション モードの gdoi コマンドで設定されていることを確認します。

サービス ダウングレード手順

以前に保存（アップグレード手順の前に保存）した GDOI 設定を使用し、各グループ メンバーの Cisco IOS ソフトウェアをダウングレードします。次に、キー サーバをダウングレードします。セカンダリ キー サーバから開始し、プライマリ キー サーバに続きます。詳細について

は、『*Managing Configuration Files Configuration Guide*』の「Configuration Replace and Configuration Rollback」機能モジュールを参照してください。

移行例

このセクションでは、GDOI から G-IKEv2 への移行の例を示します。次に、G-IKEv2 Cisco IOS ソフトウェア イメージにアップグレードした後に GDOI グループ g1 を GKM グループに変換する例を示します。Cisco IOS ソフトウェアのアップグレードの前のキー サーバ設定の例を次に示します。

```
crypto gdoi group g1
 identity 1111
 server local
  .
  .
  .
  sa ipsec 1
   profile getvpn_profile
   match address getvpn_acl
   .
   .
   .
   redundancy
   .
   .
   .
```

Cisco IOS ソフトウェアのアップグレードの後のキー サーバ設定の例を次に示します。この例では、コマンド **gdoi**、**no gikev2**、および **gikev2** が自動的に追加されます。**gikev2** コマンドは G-IKEv2 登録の受け入れを開始します。

```
crypto gkm group g1
 identity 1111
 server local
  gdoi
  no gikev2
  gikev2 ikev2_profile1
  .
  .
  .
  sa ipsec 1
   profile getvpn_profile
   match address getvpn_acl
   .
   .
   .
   redundancy
   .
   .
   .
```

Cisco IOS ソフトウェアのアップグレードの前のグループ メンバー設定の例を次に示します。

```
crypto gdoi group g1
 identity 1111
 server address ipv4 ks1
 server address ipv4 ks2

crypto map GETVPN_CM 10 gdoi
```

```
 set group g1

interface g0/0/0
 crypto map GETVPN_CM
```

Cisco IOS ソフトウェアのアップグレードの後のグループ メンバー設定の例を次に示します。この例では、コマンド **client protocol gdoi** および **client protocol gikev2** が自動的に追加されます。**client protocol gikev2** コマンドは G-IKEv2 の使用を開始します。

```
crypto gkm group g1
 identity 1111
 server address ipv4 ks1
 server address ipv4 ks2
 client protocol gdoi
 client protocol gikev2 ikev2_profile1 ] - Configure this to start using G-IKEv2

crypto map GETVPN_CM 10 gdoi
 set group g1

interface g0/0/0
 crypto map GETVPN_CM
```

GETVPN G-IKEv2 の設定

すべての GETVPN コマンド（EXEC およびグローバル コンフィギュレーション コマンド）にはキーワード **gdoi** が含まれます。G-IKEv2 にはドメイン オブ インタープリテーションが含まれていないため、登録およびキー再生成に GDOI と G-IKEv2 のいずれかのプロトコルを使用できるグループではグループ キー管理を指す全般的な短縮形 **gkm** が使用されます。現時点では、**crypto gdoi** コマンドと **crypto gkm** コマンドの両方を使用できます。ただし、**GDOI** キーワードは廃止されるため、今後は **gkm** キーワードに置き換わります。たとえば、キーサーバーグループを設定する場合、GDOI コマンドは **crypto gdoi group** *group-name* ですが、GKM コマンドは **crypto gkm group** *group-name* になります。

GETVPN G-IKEv2 の設定方法

IKEv2 プロファイルの設定

手順の概要

1. **enable**
2. **configure terminal**
3. **crypto ikev2 profile** *profile-name*
4. **authentication** {**local** {**rsa-sig** | **pre-share** [**key** {**0** | **6**} *password*}] | **ecdsa-sig** | **eap** [**gtc** | **md5** | **ms-chapv2**] [**username** *username*] [**password** {**0** | **6**} *password*}]} | **remote** {**eap** [**query-identity** | **timeout** *seconds*] | **rsa-sig** | **pre-share** [**key** {**0** | **6**} *password*}] | **ecdsa-sig**}}
5. **identity local** {**address** {*ipv4-address* | *ipv6-address*} | **dn** | **email** *email-string* | **fqdn** *fqdn-string* | **key-id** *opaque-string*}

6. **keyring** {**local** *keyring-name* | **aaa** *list-name* [**name-mangler** *mangler-name* | **password** *password*] }
7. **match** {**address local** {*ipv4-address* | *ipv6-address* | **interface** *name*} | **certificate** *certificate-map* | **fvrf** {*fvrf-name* | **any**} | **identity remote address** {*ipv4-address* [*mask*] | *ipv6-address prefix*} | {**email** [*domain string*] | **fqdn** [*domain string*]} *string* | **key-id** *opaque-string*}
8. **pki trustpoint** *trustpoint-label* [**sign** | **verify**]
9. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**crypto ikev2 profile** *profile-name* 例： `Device(config)# crypto ikev2 profile gkm-gikev2`	IKEv2 プロファイルを定義し、IKEv2 プロファイル コンフィギュレーション モードを開始します。
ステップ 4	**authentication** {**local** {**rsa-sig**	**pre-share** [**key** {**0**	**6**} *password*}]	**ecdsa-sig**	**eap** [**gtc**	**md5**	**ms-chapv2**] [**username** *username*] [**password** {**0**	**6**} *password*}]}	**remote** {**eap** [**query-identity**	**timeout** *seconds*]	**rsa-sig**	**pre-share** [**key** {**0**	**6**} *password*}]	**ecdsa-sig**}} 例： `Device(config-ikev2-profile)# authentication local ecdsa-sig`	ローカルまたはリモートの認証方式を指定します。 • **rsa-sig**：認証方式として RSA-sig を指定します。 • **pre-share**：認証方式として事前共有キーを指定します。 • **ecdsa-sig**：認証方式として ECDSA-sig を指定します。 • **eap**：リモート認証方式として EAP を指定します。 • **query-identity**：ピアに EAP ID を問い合わせます。 • **timeout** *seconds*：最初の IKE_AUTH 応答を返してから次の IKE_AUTH 要求を受け取るまでの期間を秒単位で指定します。 （注） ローカル認証方式は 1 つしか指定できませんが、リモート認証方式は複数指定できます。

	コマンドまたはアクション	目的
ステップ 5	**identity local** {**address** {*ipv4-address* | *ipv6-address*} | **dn** | **email** *email-string* | **fqdn** *fqdn-string* | **key-id** *opaque-string*} 例： `Device(config-ikev2-profile)# identity local email abc@example.com`	この手順は任意です。（任意）ローカル IKEv2 アイデンティティタイプを指定します。 （注） ローカル認証方式が事前共有キーの場合は、デフォルトのローカル ID が IP アドレスになります。ローカル認証方式が Rivest、Shamir、および Adleman（RSA）署名の場合は、デフォルトのローカル ID が識別名になります。
ステップ 6	**keyring** {**local** *keyring-name* | **aaa** *list-name* [**name-mangler** *mangler-name* | **password** *password*] } 例： `Device(config-ikev2-profile)# keyring aaa keyring1 name-mangler mangler1`	ローカルまたはリモートの事前共有キー認証方式で使用する必要があるローカルまたは AAA ベースのキーリングを指定します。 （注） 1 つのキーリングしか指定することができません。ローカル AAA は AAA ベースの事前共有キーに対してサポートされません。 （注） リリースによっては、**local** キーワードと **name-mangler** *mangler-name* キーワード引数ペアを使用する必要があります。 （注） AAA を使用する場合、Radius アクセス要求のデフォルトパスワードは「cisco」です。パスワードを変更するには、**keyring** コマンド内で **password** キーワードを使用します。
ステップ 7	**match** {**address local** {*ipv4-address* | *ipv6-address* | **interface** *name*} | **certificate** *certificate-map* | **fvrf** {*fvrf-name* | **any**} | **identity remote address** {*ipv4-address* [*mask*] | *ipv6-address prefix*} | {**email** [*domain string*] | **fqdn** [*domain string*]} *string* | **key-id** *opaque-string*} 例： `Device(config-ikev2-profile)# match address local interface Ethernet 2/0`	match ステートメントを使用して、ピア用の IKEv2 プロファイルを選択します。
ステップ 8	**pki trustpoint** *trustpoint-label* [**sign** | **verify**] 例： `Device(config-ikev2-profile)# pki trustpoint tsp1 sign`	RSA 署名認証方式で使用する Public Key Infrastructure（PKI）トラストポイントを指定します。 （注） **sign** または **verify** キーワードが指定されていない場合、トラストポイントは署名と検証に使用されます。

	コマンドまたはアクション	目的
		（注） IKEv1 とは対照的に、証明書ベースの認証を成功させるためにトラストポイントを IKEv2 プロファイル内で設定する必要があります。このコマンドが設定内に存在しない場合は、グローバルに設定されたトラストポイントのフォールバックが存在しません。トラストポイント設定は IKEv2 イニシエータおよびレスポンダに適用されます。
ステップ 9	**end** 例： `Device(config-ikev2-profile)# end`	IKEv2 プロファイル コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

キーサーバーでの GKM ポリシーの設定

手順の概要

1. **enable**
2. **configure terminal**
3. **crypto gkm group** [**ipv6**] *group-name*
4. **server local**
5. **gikev2** *IKEv2-profile-name*
6. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**crypto gkm group** [**ipv6**] *group-name* 例： `Device(config)# crypto gkm group gkm-grp1`	GKM ポリシーを設定し、GKM グループ コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 4	**server local** 例： `Device(config-gkm-group)# server local`	デバイスを GKM キーサーバーとして指定し、GKM ローカル サーバー コンフィギュレーション モードを開始します。
ステップ 5	**gikev2** *IKEv2-profile-name* 例： `Device(gkm-local-server)# gikev2 gkm-gikev2`	キーサーバーでの登録およびキー再生成のために G-IKEv2 プロファイルを有効にします。
ステップ 6	**end** 例： `Device(gkm-local-server)# end`	GKM ローカル サーバー コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

グループメンバーでの GKM ポリシーの設定

手順の概要

1. **enable**
2. **configure terminal**
3. **crypto gkm group** [**ipv6**] *group-name*
4. **client protocol gikev2** *gkm-gikev2*
5. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**crypto gkm group** [**ipv6**] *group-name* 例： `Device(config)# crypto gkm group gkm-grp2`	GKM ポリシーを設定し、GKM グループ コンフィギュレーション モードを開始します。
ステップ 4	**client protocol gikev2** *gkm-gikev2* 例： `Device(config-gkm-group)# client protocol gikev2 gkm-gikev2`	グループメンバーでの登録およびキー再生成のために G-IKEv2 プロファイルを有効にします。

	コマンドまたはアクション	目的
ステップ 5	**end** 例： `Device(config-gkm-group)# end`	GKM グループ コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

GETVPN G-IKEv2 のその他の参考資料

関連資料

関連項目	マニュアル タイトル
セキュリティ コマンド	• 『*Cisco IOS Security Command Reference: Commands A to C*』 • 『*Cisco IOS Security Command Reference: Commands D to L*』 • 『*Cisco IOS Security Command Reference: Commands M to R*』 • 『*Cisco IOS Security Command Reference: Commands S to Z*』

標準および RFC

標準/RFC	タイトル
RFC 4306	*Internet Key Exchange (IKEv2) Protocol*
IKEv2 を使用したグループ キー管理	『*draft-yeung-g-ikev2-07*』

シスコのテクニカル サポート

説明	リンク
右の URL にアクセスして、シスコのテクニカル サポートを最大限に活用してください。これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

GETVPN G-IKEv2 の機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *309 : GETVPN G-IKEv2* の機能情報

機能名	リリース	機能情報
GETVPN G-IKEv2		次のコマンドが導入または変更されました。**client protocol**、**crypto gkm group**、**gikev2**、**show crypto gkm**

第 229 章

8K GM スケールの改善

8K GM スケールの改善機能では、グループ メンバー（GM）の数を 8000 まで増やすことにより、Cooperative Protocol（COOP）通知メッセージの最適化をサポートします。

8K GM スケールの改善の前提条件

特定のプロトコル バージョンをアップグレードまたはダウングレードするには、グループ メンバー（GM）間で中断のない通信を確保するため、同じポリシー、キー、および GM データベースを維持します。

8K GM スケールの改善に関する情報

8K GM スケールの改善

Cooperative Protocol Announcement（COOP ANN）メッセージには複数のクライアントがあり、各クライアントはプロトコル バージョンに関連付けられます。COOP ANN メッセージは、最大 8000 のグループ メンバー（GM）を保留にし、続いて GM ヘッダーのプロトコル バージョンが上がるように最適化されています。

この機能はまた、GM ヘッダー プロトコル バージョンのアップグレードとダウングレードもサポートします。

8K GM スケールの改善の設定方法

グループ メンバー ヘッダーのプロトコル バージョンのアップグレードとダウングレード

始める前に

- すべてのキー サーバ（KS）が、ネットワークを 4000 GM 以上に拡張する前に「最適化」プロトコル バージョンにアップグレードされることを確認します。
- すべてのアップグレードされた KS が、最大で 4000 GM をサポートするネットワークに縮小する前に「基本」プロトコル バージョンにダウングレードされる必要があることを確認します。

手順の概要

1. **enable**
2. **configure terminal**
3. **crypto gdoi group** *group-name*
4. **server local**
5. **redundancy**
6. **protocol version** {**base** | **optimize**}
7. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**crypto gdoi group** *group-name* 例： `Device(config)# crypto gdoi group GETVPN`	GDOI グループを指定し、GDOI グループ コンフィギュレーション モードを開始します。
ステップ 4	**server local** 例： `Device(config-gdoi-group)# server local`	ローカルに定義されているグループ サーバを特定し、GDOI のローカル サーバのコンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 5	**redundancy** 例： `Device(gdoi-local-server)# redundancy`	GDOI COOP KS コンフィギュレーション モードを開始します。 （注） ローカル サーバの送信元アドレスが定義されていることを確認します。
ステップ 6	**protocol version** {**base** | **optimize**} 例： `Device(gdoi-coop-ks-config)# protocol version optimize`	GM ヘッダーのプロトコル バージョンをアップグレードまたはダウングレードします。 • **base**： 4000 GM までの COOP ANN メッセージをサポートします。 • **optimize**： 8000 GM までの COOP ANN メッセージをサポートします。
ステップ 7	**end** 例： `Device(gdoi-coop-ks-config)# end`	COOP KS コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

8K GM スケールの改善の設定例

例：グループ メンバー ヘッダーのプロトコル バージョンのアップグレード

```
Device> enable
Device# configure terminal
Device(config)# crypto gdoi group getvpn
Device(config-gdoi-group)# server local
Device(gdoi-local-server)# redundancy
Device(gdoi-coop-ks-config)# protocol version optimize
Device(gdoi-coop-ks-config)# end
```

例：グループ メンバー ヘッダーのプロトコル バージョンのダウングレード

```
Device> enable
Device# configure terminal
Device(config)# crypto gdoi group getvpn
Device(config-gdoi-group)# server local
Device(gdoi-local-server)# redundancy
Device(gdoi-coop-ks-config)# protocol version base
Device(gdoi-coop-ks-config)# end
```

GETVPN での IPSEC 暗号化および復号

GETVPN IPsec フローでは、予期される IPsec フローレコーダで着信トラフィックが復号されない場合があります。復号されたトラフィックは、任意の IPsec SA に記録できます（使用可能な場合）。復号は、ランダムな IPsec フローレコーダで行われる可能性があります。次に、例を示します。

```
Device# ping vrf cust1 48.1.1.1 so 38.1.1.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 48.1.1.1, timeout is 2 seconds:
Packet sent with a source address of 38.1.1.1
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms

Device# show crypto session ivrf cust1  detail | sec permit ip 38.0.0.0
  IPSEC FLOW: permit ip 38.0.0.0/255.0.0.0 48.0.0.0/255.0.0.0
        Active SAs: 2, origin: crypto map
        Inbound:  #pkts dec'ed 0 drop 0 life (KB/Sec) KB Vol Rekey Disabled/1 hours, 16
 mins
        Outbound: #pkts enc'ed 5 drop 0 life (KB/Sec) KB Vol Rekey Disabled/1 hours, 16
 mins

Device# show crypto session ivrf cust1  detail | sec permit ip 48.0.0.0
  IPSEC FLOW: permit ip 48.0.0.0/255.0.0.0 38.0.0.0/255.0.0.0
        Active SAs: 2, origin: crypto map
        Inbound:  #pkts dec'ed 0 drop 0 life (KB/Sec) KB Vol Rekey Disabled/1 hours, 16
 mins
        Outbound: #pkts enc'ed 0 drop 0 life (KB/Sec) KB Vol Rekey Disabled/1 hours, 16
 mins

Device# show crypto session ivrf cust1  detail | sec permit ip 45.0.0.0
  IPSEC FLOW: permit ip 45.0.0.0/255.0.0.0 35.0.0.0/255.0.0.0
        Active SAs: 2, origin: crypto map
        Inbound:  #pkts dec'ed 5 drop 0 life (KB/Sec) KB Vol Rekey Disabled/1 hours, 15
 mins
        Outbound: #pkts enc'ed 0 drop 0 life (KB/Sec) KB Vol Rekey Disabled/1 hours, 15
 mins
```

上記の例では、フロー着信トラフィックは、予期される IPsec フローで復号されません。

この問題を解決し、暗号化されたパケットと復号されたパケットの数を表示するには、次の **show** コマンドを使用します。次に、**show** コマンドの出力例を示します。

```
Device# show crypto gdoi group v6-cust-gdoi1 gm dataplane counters

Data-plane statistics for group v6-cust-gdoi1:
   #pkts encrypt            : 1912   #pkts decrypt            : 1914
    #pkts tagged (send)      : 1841     #pkts untagged (rcv)     : 1834
    #pkts no sa (send)       : 0        #pkts invalid sa (rcv)   : 0
    #pkts encaps fail (send) : 0        #pkts decap fail (rcv)   : 0
    #pkts invalid prot (rcv) : 0        #pkts verify fail (rcv)  : 0
    #pkts not tagged (send)  : 0        #pkts not untagged (rcv) : 0
    #pkts internal err (send): 0        #pkts internal err (rcv) : 0
```

8K GM スケールの改善のその他の参考資料

関連資料

関連項目	マニュアル タイトル
Cisco IOS セキュリティ コマンド	『*Cisco IOS Security Command References*』
エンタープライズ ネットワークの GET VPN の有効化のための基本的な導入ガイドライン	『*Cisco IOS GET VPN Solutions Deployment Guide*』
GET VPN ネットワークの設計と実装	『*Group Encrypted Transport VPN (GETVPN) Design and Implementation Guide*』

標準および RFC

標準/RFC	タイトル
RFC 6407	『*The Group Domain of Interpretation*』

シスコのテクニカル サポート

説明	リンク
シスコのサポート Web サイトでは、シスコの製品やテクノロジーに関するトラブルシューティングにお役立ていただけるように、マニュアルやツールをはじめとする豊富なオンライン リソースを提供しています。 お使いの製品のセキュリティ情報や技術情報を入手するために、Cisco Notification Service（Field Notice からアクセス）、Cisco Technical Services Newsletter、Really Simple Syndication（RSS）フィードなどの各種サービスに加入できます。 シスコのサポート Web サイトのツールにアクセスする際は、Cisco.com のユーザ ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *310 :* 機能情報

機能名	リリース	機能情報
8K GM スケールの改善		8K GM スケールの改善機能では、グループ メンバー（GM）の数を 8000 まで増やすことにより、Cooperative Protocol（COOP）通知メッセージの最適化をサポートします。 **protocol** コマンドが変更されました。

第 230 章

GET VPN 相互運用性

GETVPN キーサーバーでの D3P サポートの機能、アクティブ化時間遅延の機能、および Cisco GETVPN キーサーバーの GDOI 相互運用 ACK の機能により、キーサーバーとグループメンバーの間の相互運用性が強化されます。

GET VPN 相互運用性の前提条件

- グループの機能を有効にするには、グループ内のすべてのデバイスで互換性のあるバージョンの Cisco IOS ソフトウェアおよび Group Domain of Interpretation（GDOI）が実行されている必要があります。
- Cisco GETVPN キーサーバーのインターネットドラフト ACK とアクティブ化時間遅延の機能を設定する前に、GDOI グループでユニキャストキー再生成機能を有効にします。

GET VPN 相互運用性に関する制約事項

- GETVPN キーサーバー機能での IP-D3P サポートは、GETVPN の復元力（GM のエラー検出および Cisco TrustSec 用の IPsec インラインタギングの GET VPN サポートの機能）と共存できません。後者の機能は、GET VPN キーサーバーで IP-D3P サポートを有効にする前に無効にする必要があります。また、GETVPN キーサーバーで GETVPN の復元力のサポートを有効にする前に IP-D3P を無効にする必要があります。
- アクティブ化時間遅延機能は、IPsec セキュリティ アソシエーションでのみサポートされます。複数の IPsec SA を設定しないでください。

- Cisco-Metdata と IP-D3P は共存できません。CMD 機能と IP-D3P を切り替える場合、キーサーバーは、すべての GM に対して **crypto gdoi ks rekey replace** を実行して、これら 2 つの機能が同時に有効になっていないことを確認する必要があります。
- ASR1K は、GETVPN IPv4 トンネルモードでのみ IP-D3P をサポートします。

GET VPN 相互運用性に関する情報

IP 配信遅延検出プロトコル（IP-D3P）の概要

IPデータグラムは、ホストまたはゲートウェイが最新ではないデータグラムを受信する配信遅延攻撃の対象となる可能性があります。最新のデータグラムは、「プロトコルの以前のインタラクションから再生されたのではなく、最近生成されたデータグラム」として定義されます。IP-D3P データグラムは、ヘッダーと IP ペイロードで構成されます。IP-D3P ヘッダーには、パケットが最近生成されたかどうかを判断するためにパケットの受信者が使用するタイムスタンプが含まれています。受信者は、IPパケットで配信されたタイムスタンプをローカル時間と比較し、パケットを受け入れるかどうかを決定します。

IP-D3P は、グループメンバーのシステムクロックを使用して、IP-D3P データグラムのタイムスタンプを作成および確認します。ほとんどの場合、システムクロックは、送信者と受信者のシステムクロックを同期するために、Network Time Protocol（NTP）などの外部プロトコルから設定されます。

GETVPN キーサーバーでの D3P サポートの機能により、GET VPN での IP-D3P のサポートが有効になります。

キーサーバーの IP-D3P サポート

GDOI ローカル サーバー コンフィギュレーション モードで新しい コンフィギュレーション コマンドの **d3p** を使用すると、キーサーバーで IP-D3P を有効にできます。D3P コマンドを有効にすると、プライマリキーサーバーは、D3P 属性を持つグループ関連ポリシー（GAP）ペイロードがあるすべてのグループメンバーにキー再生成を発行します。GAPペイロードのキー再生成メッセージには次の属性が含まれます。

- D3P-TYPE：Portable Operating System Interface（POSIX）時間（ミリ秒単位）。
- D3P-WINDOWSIZE：IP-D3P ウィンドウサイズ（ミリ秒単位）。

show crypto gkm ks コマンドは、キーサーバーで有効になっている IP-D3P パラメータを表示します。

連携キーサーバーの IP-D3P サポート

GET VPN グループに複数のキーサーバーがある場合は、すべてのキーサーバーで IP-D3P を有効にする必要があります。プライマリキーサーバーは、アナウンスメッセージを介して、IP-D3P

属性を含む GAP ペイロードをセカンダリキーサーバーに送信します。これにより、すべての連携キーサーバーに、IP-D3P がグループ内で適用されるようになったことが通知されます。

GAP ペイロードを受信すると、連携キーサーバーは、IP-D3P 属性をグループ設定と照合します。不一致がある場合、連携キーサーバーは、次に示すように、ネットワーク管理者に誤った設定または不適切な設定を警告する Syslog メッセージを生成します。

```
%GDOI-3-COOP_CONFIG_MISMATCH: WARNING: IP-D3P configuration between Primary KS and
Secondary KS are mismatched
```

グループメンバーの IP-D3P サポート

グループメンバーは、キー再生成メッセージに含まれる IP-D3P パラメータを受信します。グループメンバーは、新しい GAP ペイロード属性（D3P-TYPE および D3P-WINDOWSIZE）を処理します。グループメンバーの IP-D3P で使用する必要があるウィンドウサイズは、GDOI グループ設定で **client d3p** コマンドを使用して上書きできます。たとえば、キーサーバーの設定が **d3p window msec 1000** であり、グループメンバーの設定が **client d3p window sec 50** である場合、グループメンバーは、次のパラメータを使用して、キーサーバーから受信したパラメータを上書きし、IP-D3P を有効にすることができます。

```
D3P-TYPE = POSIX-TIME-MSEC
D3P-WINDOWSIZE = 50000
```

グループメンバーの IP-D3P 設定と、発生した IP-D3P エラー（ある場合）を表示するには、**show crypto gdoi gm** コマンドを使用します。

（注） IP-D3P は、キーサーバーから送信されたパラメータを使用する Cisco ASR 9000 シリーズ アグリゲーション サービス ルータでは有効にできません。Cisco ASR 9000 シリーズ アグリゲーション サービス ルータ上のキーサーバーから送信されたパラメータを表示するには、**show crypto gdoi group** コマンドを使用します。

アクティブ化時間遅延

GET VPN は、アクティブ化時間遅延（ATD）機能をサポートします。この機能では、キーサーバーがグループメンバーに対して、トラフィック暗号化のための新しいセキュリティ アソシエーション（SA）の使用を遅らせるように指示します。キーサーバーは、ユニキャストキー再生成メッセージをグループメンバーに送信するときに、グループ関連ポリシー（GAP）ペイロードに ATD 値を含めます。遅延時間の値は、ユーザーが設定できません。SA の有効期限が切れる 30 秒前に固定されています。ATD 値を計算する式は、次のとおりです。

ATD = Max((Max(old-SA-remaining-lifetime_sec, 30sec) – 30sec), 1sec)

（注） ATD のサポートは、Cisco ASR 9000 シリーズ アグリゲーション サービス ルータおよび非 Cisco デバイスで設定されているグループメンバーに限定されます。そのため、キーサーバーは、Cisco ASR 9000 シリーズ アグリゲーション サービス ルータおよび非 Cisco デバイス以外のデバイスに ATD 情報を送信しません。

.

キー再生成確認応答

キーサーバーが、グループのキーとポリシーを更新するために、グループメンバーにキー再生成メッセージを送信する場合、すべてのグループメンバーがキー再生成メッセージを受信して、新しいキーおよびポリシーが正常に処理され、インストールされ、応答されたかどうかが分かると便利です。

シスコのユニキャストキー再生成確認応答メッセージ

ユニキャストキー再生成が設定されている場合、キーサーバーはキー再生成メッセージを送信し、グループメンバーはそれに対して確認応答キー再生成メッセージを送信することで応答します。

（注） マルチキャストキー再生成が設定されている場合、確認応答メッセージは存在しません。

キーサーバーが、応答確認されていないユニキャストキー再生成をグループメンバーに3回連続して送信し、そのユニキャストキー再生成がそのグループメンバーによって確認応答されなかった場合、そのグループメンバーはキーサーバーのグループ メンバー データベースから削除され、以降のユニキャストキー再生成はそのグループメンバーに送信されません。

GDOI I-D キー再生成確認応答メッセージ

Cisco キーサーバーの GDOI 相互運用 ACK の機能は、シスコ製ではないグループメンバーとキーサーバーの間で、RFC-8263（GROUPKEY-PUSH 確認応答メッセージ）で定義されているキー再生成確認応答メッセージの標準規格を実装します。

GDOI GROUPKEY-PUSH 確認応答メッセージ（「GDOI I-D キー再生成 ACK」と呼ばれる）では、シスコのユニキャストキー再生成確認応答メッセージとは異なり、グループメンバーがグループ内の任意のキーサーバーにキー再生成確認応答を送信するための相互運用可能な方式が定義されています。

キーサーバーの GDOI I-D キー再生成 ACK サポート

rekey acknowledgement コマンドを使用すると、キーサーバーは、 コマンドで選択されているキーワードに応じて、グループメンバーにキー再生成の確認応答を要求できます。

- **cisco**：シスコ独自のキー再生成 ACK（暗号化）メッセージを受け入れます。

- **interoperable**：対応するインターネットドラフトに従って、キー再生成ACK（暗号化されていない）メッセージを要求して受け入れます。
- **any**：グループキーメンバーのバージョンに基づいて、サポートされているすべてのACKメッセージを受け入れます。

rekey acknowledgement コマンドを有効にすると、キーサーバーは、新しいポリシー属性 **KEK_ACK_REQUESTED** を送信します。これは、登録およびキー再生成のためにキー暗号化キー（KEK）SA ペイロードに含まれる新しいポリシー属性です。

連携キーサーバーの GDOI I-D キー再生成 ACK サポート

GET VPN グループに複数のキーサーバーがある場合は、すべてのキーサーバーで **rekey acknowledgement** コマンドを設定する必要があります。プライマリキーサーバーがセカンダリキーサーバーにアナウンスメッセージを送信する場合、プライマリキーサーバーには、**KEK_ACK_REQUESTED** 属性を伝送する **KEK SA** ペイロードも含まれます。これにより、すべての連携キーサーバーに、それらの下に登録されているグループメンバーに **KEK_ACK_REQUESTED** 属性を送信するように通知されます。

KEK_ACK_REQUESTED 属性を持つ **KEK SA** ペイロードを受信すると、連携キーサーバーは、グループ設定を確認します。不一致がある場合、連携キーサーバーは、次に示すように、ネットワーク管理者に誤った設定または不適切な設定を警告するメッセージを生成します。

```
%GDOI-3-COOP_CONFIG_MISMATCH: WARNING: Interoperable Rekey ACK configuration between
Primary KS and Secondary KS are mismatched
```

（注） キー再生成メッセージを送信するのはプライマリキーサーバーであるため、キー再生成確認応答はプライマリキーサーバーにのみ送信されます。キー再生成確認応答は、連携キーサーバーがプライマリキーサーバーとして昇格され、古いプライマリキーサーバーがキー暗号化キー（KEK）またはトラフィック暗号化キー（TEK）ポリシーを作成しなかった場合にのみ、連携サーバーに送信されます。

グループメンバーの GDOI I-D キー再生成サポート

グループメンバーが、KEK SA ペイロードに KEK_ACK_REQUESTED 属性を含むキー再生成メッセージを受信し、確認応答メッセージを介してキーサーバーに GDOI ID キー再生成 ACK を送信する場合、そのグループメンバーは、Cisco GETVPN キーサーバーのインターネットドラフト ACK の機能をサポートしていると見なされます。

キーサーバーとグループメンバーの通信

キーサーバーが KEK SA ペイロードで KEK_ACK_REQUESTED 属性を送信すると、対応するキーサーバーから別の通知がないかぎり、グループメンバーは、後続のキー再生成メッセージに GDOI ID キー再生成 ACK で応答する必要があります。キーサーバーとグループメンバーの間の通信は、次のとおりです。

1. キーサーバーによって送信されるすべてのGROUPKEY-PUSHメッセージに対して、グループメンバーはGROUP-PUSH-KEY ACKメッセージで応答する必要があります。
2. キーサーバーは、メッセージの形式とペイロードを検証して妥当性を確認します。検証に失敗すると、メッセージはドロップされます。
3. 検証に成功すると、キーサーバーは、SEQペイロードとIDペイロードを処理して、IDに関連付けられたグループメンバーの最新の確認応答済みシーケンス番号を記録します。シーケンス番号は、最後に送信されたシーケンス番号と同じである必要があります。それ以外の場合、SEQペイロードとIDペイロードは記録されません。

（注） Ciscoキーサーバーの場合、グループメンバーがキー再生成メッセージに対して3回連続して確認応答を送信しない場合、そのグループメンバーはデータベースから削除されます。グループメンバーにユニキャストキー再生成機能が設定されており、特定のKEKセキュリティパラメータインデックス（SPI）に対してKEK_ACK_REQUESTED属性が送信されない場合、グループメンバーは、Ciscoユニキャストキー再生成ACKメッセージをキーサーバーに送信する必要があります。

次の表で、KEK SAペイロードで送信される属性と、キーサーバーで設定された各確認応答オプションに対して送信される値について説明します。

表 *311* : 各確認応答オプションの *KEK SA* ペイロード

確認応答オプション	新しいシスコグループメンバー	Cisco ASR 9000 グループメンバー	シスコ製以外のグループメンバー
Cisco	属性なし	属性なし	属性なし
相互運用可能	KEK_ACK_REQ REKEY_ACK_KEK_SHA256	KEK_ACK_REQ REKEY_ACK_KEK_SHA256	KEK_ACK_REQ REKEY_ACK_KEK_SHA256
いずれか	属性なし	KEK_ACK_REQ REKEY_ACK_KEK_SHA256	KEK_ACK_REQ REKEY_ACK_KEK_SHA256

（注） **no rekey acknowledgement** コマンドを使用してキー再生成確認応答をデフォルト値の「Cisco」に設定すると、キーサーバーは、KEK SAペイロードにKEK_ACK_REQUESTED属性を含めません。

次の表で、キーサーバーにおいて **rekey acknowledgement** コマンドでキーワードを使用して設定された各確認応答タイプの確認手法について説明します。

表 *312 :* 確認応答の方法論

確認応答オプション	キーサーバーが I-D ACK を受け入れる	キーサーバーが Cisco ACK を受け入れる
Cisco	いいえ（エラーになります）	対応
相互運用可能	対応	いいえ（エラーになります）
いずれか	対応	対応

GET VPN 相互運用性の設定方法

キーサーバー上の正しい GDOI バージョンの確認

手順の概要

1. **enable**
2. **show crypto gkm feature** *feature name*
3. **show crypto gkm feature** *feature-name* | **include no**

手順の詳細

ステップ 1 **enable**

特権 EXEC モードを有効にします。

- パスワードを入力します（要求された場合）。

```
Device> enable
```

ステップ 2 **show crypto gkm feature** *feature name*

ネットワーク内の各キーサーバーおよびグループメンバーで実行されている GDOI バージョンと、デバイスが GET VPN 相互運用性機能（つまり、GETVPN キーサーバーでの D3P サポートと Cisco GETVPN キーサーバーのインターネットドラフト ACK）をサポートしているかどうかに関する情報を表示します。

例：

```
Device# show crypto gkm feature ip-d3p
Group Name: GET VPN1
    Key Server ID       Version   Feature Supported
        10.0.8.1         1.0.11         Yes
        10.0.9.1         1.0.10         No
    Group Member ID     Version   Feature Supported
        10.0.3.1         1.0.11         Yes
        10.65.9.2        1.0.10         No
```

例：

```
Device# show crypto gkm feature gdoi-interop-ack
Group Name: GET VPN2
    Key Server ID       Version   Feature Supported
        10.0.8.1         1.0.11         Yes
        10.0.9.1         1.0.10         No
    Group Member ID     Version   Feature Supported
        10.0.3.1         1.0.11         Yes
        10.65.9.2        1.0.10         No
```

ステップ 3 **show crypto gkm feature** *feature-name* | **include no**

（任意）機能をサポートしていないデバイスを検索します。

例：

```
Device# show crypto gkm feature gdoi-interop-ack | include no
```

グループメンバー上の正しい GDOI バージョンの確認

手順の概要

1. **enable**
2. **show crypto gkm feature** *feature name*

手順の詳細

ステップ 1 **enable**

特権 EXEC モードを有効にします。

- パスワードを入力します（要求された場合）。

ステップ 2 **show crypto gkm feature** *feature name*

ネットワーク内のグループメンバーで実行されている GDOI バージョンと、デバイスが GET VPN 相互運用性機能（つまり、GETVPN キーサーバーでの D3P サポートと Cisco GETVPN キーサーバーのインターネットドラフト ACK）をサポートしているかどうかに関する情報を表示します。

例：

```
Device# show crypto gkm feature ip-d3p
       Version    Feature Supported
        1.0.11           Yes
```

例：

```
Device# show crypto gkm feature gdoi-interop-ack
       Version    Feature Supported
        1.0.10           No
```

キーサーバーでの IP-D3P の有効化

手順の概要

1. **enable**
2. **configure terminal**
3. **crypto gkm group GETVPN**
4. **server local**
5. **sa d3p window**{**sec** *seconds* | **msec** *milliseconds*}
6. **exit**
7. **show crypto gkm ks replay**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**crypto gkm group GETVPN** 例： `Device(config)# crypto gkm group GETVPN`	グループキー管理（GKM）グループを設定し、GKM グループ コンフィギュレーション モードを開始します。
ステップ 4	**server local** 例： `Device(config-gkm-group)# server local`	デバイスをキーサーバーとして指定し、GDOI ローカル サーバー コンフィギュレーション モードを開始します。
ステップ 5	**sa d3p window**{**sec** *seconds* | **msec** *milliseconds*} 例： `Device(gdoi-local-server)# sa d3p window msec 5000`	グループ内のすべてのセキュリティ アソシエーションで IP 配信遅延検出プロトコル（IP-D3P）を有効にします。 • **sec** *seconds*：ウィンドウサイズ（秒単位）。範囲は 1 ～ 100 です。 • **msec** *milliseconds*：ウィンドウサイズ（ミリ秒単位）。範囲は 100 ～ 10000 です。
ステップ 6	**exit** 例： `Device(gdoi-local-server)# exit`	GDOI ローカル サーバ コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

	コマンドまたはアクション	目的
ステップ 7	**show crypto gkm ks replay** 例： `Device# show crypto gkm ks replay`	時間ベースのアンチリプレイのキーサーバーグループ情報を表示します。

例

次に、**show crypto gkm ks replay** コマンドの出力例を示します。

```
Device# show crypto gkm ks replay
Anti-replay Information For Group GETVPN:
    IP-D3P: Type = POSIX-TIME-MSEC, Window-size = 5000 msec
```

グループメンバーでの IP-D3P の有効化

手順の概要

1. **enable**
2. **configure terminal**
3. **crypto gkm group GET**
4. **client d3p window** {**sec** *seconds* | **msec** *milliseconds*}
5. **exit**
6. **show crypto gkm gm replay**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**crypto gkm group GET** 例： `Device(config)# crypto gkm group GETVPN`	グループキー管理（GKM）グループを設定し、GKM グループ コンフィギュレーション モードを開始します。
ステップ 4	**client d3p window** {**sec** *seconds* | **msec** *milliseconds*} 例： `Device(config-gkm-group)# client d3p window sec 50`	クライアントが許容できるIP配信遅延検出プロトコル（IP-D3P）を有効にします。 • **sec** *seconds*：ウィンドウサイズ（秒単位）。範囲は 1 ～ 100 です。

	コマンドまたはアクション	目的
		• **msec** *milliseconds*：ウィンドウサイズ（ミリ秒単位）。範囲は 100 ～ 10000 です。
ステップ 5	**exit** 例： `Device(gdoi-local-server)# exit`	GDOI ローカルサーバコンフィギュレーションモードを終了し、特権 EXEC モードに戻ります。
ステップ 6	**show crypto gkm gm replay** 例： `Device# show crypto gkm gm replay`	時間ベースのアンチリプレイのグループメンバー情報を表示します。

例

次に、**show crypto gkm gm replay** コマンドの出力例を示します。

```
Device# show crypto gkm gm replay
Anti-replay Information For Group GET:
   IP-D3P:
     Posix-time-msec           : 502764.17
     Input Packets            : 5        Output Packets           : 5
     Input Error Packets      : 5        Output Error Packets     : 0

IP-D3P Error History (sampled at 10pak/min):
     xx:xx:xx.xxx PST Tue Feb 25 2014: src=5.0.0.2; my_time=502729.95; peer_time=33.46;
 win=10
     yy:yy:yy.yyy PST Tue Feb 25 2014: src=5.0.0.2; my_time=502723.95; peer_time=27.45;
 win=10
```

キー再生成確認応答の有効化

手順の概要

1. **enable**
2. **configure terminal**
3. **crypto gkm group GET**
4. **server local**
5. **rekey acknowledgement**{**cisco** | **interoperable** | **any**}
6. **exit**
7. **show crypto gkm ks replay**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例：	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。

	コマンドまたはアクション	目的
	`Device> enable`	
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**crypto gkm group GET** 例： `Device(config)# crypto gkm group GET`	グループキー管理（GKM）グループを設定し、GKM グループ コンフィギュレーション モードを開始します。
ステップ 4	**server local** 例： `Device(config-gkm-group)# server local`	デバイスをキーサーバーとして指定し、GDOI ローカル サーバー コンフィギュレーション モードを開始します。
ステップ 5	**rekey acknowledgement**{**cisco** | **interoperable** | **any**} 例： `Device(gdoi-local-server)# rekey acknowledgment interoperable`	グループメンバーがキー再生成を確認応答できるようにします。 • **cisco**：Cisco Rekey ACK（暗号化）メッセージを受け入れます。 • **interoperable**：相互運用可能なキー再生成 ACK（非暗号化）メッセージを要求して受け入れます。 • **any**：グループキーメンバーのバージョンに基づいて、サポートされている ACK メッセージを受け入れます。
ステップ 6	**exit** 例： `Device(gdoi-local-server)# exit`	GDOI ローカルサーバコンフィギュレーションモードを終了し、特権 EXEC モードに戻ります。
ステップ 7	**show crypto gkm ks replay** 例： `Device# show crypto gkm ks replay`	キーサーバーでのキー再生成確認応答の設定を表示します。

例

次に、キー再生成確認応答の設定を表示する **show** コマンドの出力例を示します。

```
Device# show crypto gkm

GROUP INFORMATION
    Group Name               : GETVPN (Unicast)
 .
 .
 .
```

```
    Group Rekey Lifetime     : 86400 secs
    Group Rekey
        Remaining Lifetime   : 44710 secs
        Time to Rekey        : 44485 secs
        Acknowledgement Cfg  : {Cisco|Interoperable|Any}
 .
 .
 .

Device# show crypto gkm ks

Total group members registered to this box: 0
Key Server Information For Group GETVPN:
    Group Name               : GETVPN
Group Name               : GETVPN (Unicast)
 .
 .
 .
    Group Members            : 0
      GDOI Group Members     : 0
      G-IKEv2 Group Members  : 0
    Rekey Acknowledgement Cfg: {Cisco|Interoperable|Any}
    IPSec SA Direction       : Both
 .
 .
 .
Device# show crypto gkm ks rekey

Group GETVPN (Unicast)
    Acknowledgement Type In-Use         : {Cisco|Interoperable|Any}
    Number of Rekeys sent               : 20
 .
 .
 .
Device# show crypto gkm ks rekey

Group GETVPN (Multicast)
    Acknowledgement Type In-Use         : None
    Number of Rekeys sent               : 20
 .
 .
 .
Device# show crypto gkm ks policy

Key Server Policy:
For group diffint (handle: 2147483650) server 10.0.8.1 (handle: 2147483650):
  # of teks : 2  Seq num : 7
  KEK POLICY (transport type : Unicast)
    spi : 0x7D32D2052B87CEFE14060B58B0176129
    management alg     : disabled    encrypt alg       : AES
    crypto iv length   : 16          key size          : 16
    orig life(sec): 86400       remaining life(sec): 44699
    time to rekey (sec): 44474
    sig hash algorithm : enabled     sig key length    : 162
    sig size           : 128
    sig key name       : mykeys
    acknowledgement    : {cisco|interoperable|any}

Device# show crypto gkm ks policy

Key Server Policy:
For group diffint (handle: 2147483650) server 10.0.8.1 (handle: 2147483650):
  # of teks : 2  Seq num : 7
  KEK POLICY (transport type : Multicast)
```

```
spi : 0x7D32D2052B87CEFE14060B58B0176129
management alg     : disabled    encrypt alg       : AES
crypto iv length   : 16          key size          : 16
orig life(sec): 86400       remaining life(sec): 44699
time to rekey (sec): 44474
sig hash algorithm : enabled     sig key length    : 162
sig size           : 128
sig key name       : mykeys
acknowledgement    : none
```

GET VPN 相互運用性の設定例

例：キーサーバーでの IP-D3P の有効化

```
Device> enable
Device# configure terminal
Device(config)# crypto gkm group GETVPN
Device(config-gkm-group)# server local
Device(gdoi-local-server)# sa d3p window msec 5000
Device(gdoi-local-server)# exit
```

例：グループメンバーでの IP-D3P の有効化

```
Device> enable
Device# configure terminal
Device(config-gkm-group)# client d3p window sec 50
Device(gdoi-local-server)# exit
```

例：キー再生成確認応答の有効化

```
Device> enable
Device# configure terminal
Device(config)# crypto gkm group GET
Device(config-gkm-group)# server local
Device(gdoi-local-server)# rekey acknowledgment interoperable
Device(gdoi-local-server)# exit
```

GET VPN の相互運用性に関する追加情報

関連資料

関連項目	マニュアル タイトル

関連項目	マニュアル タイトル
セキュリティ コマンド	• 『Cisco IOS Security Command Reference: Commands A to C』 • 『Cisco IOS Security Command Reference Commands D to L』 • 『Cisco IOS Security Command Reference: Commands M to R』 • 『Cisco IOS Security Command Reference: Commands S to Z』
GET VPN の設定	*Cisco Group Encrypted Transport VPN*
ユニキャストキー再生成	*GET VPN* モジュールの「Unicast Rekeying」セクション

標準および RFC

標準/RFC	タイトル
draft-weis-delay-detection-00	『*IP Delivery Delay Detection Protocol*』
draft-weis-gdoi-rekey-ack-01	『*GDOI GROUPKEY-PUSH Acknowledgement Message*』
RFC 5374 - セクション 5.4：グループ関連ポリシー	『*Multicast Extensions to the Security Architecture for the Internet Protocol*』
RFC 6407 - セクション 4.2.1：アクティブ化時間遅延	『*The Group Domain of Interpretation*』

シスコのテクニカル サポート

説明	リンク
右の URL にアクセスして、シスコのテクニカル サポートを最大限に活用してください。これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

GET VPN 相互運用性の機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *313 : GET VPN* 相互運用性の機能情報

機能名	リリース	機能情報
GETVPN キーサーバーでの D3P サポート		GETVPN キーサーバーでの D3P サポートの機能は、GET VPN ネットワークでの IP-D3P のサポートを有効にします。 次のコマンドが導入または変更されました。**client d3p**、**sa d3p**、**show crypto gkm gm replay**、**show crypto gkm ks replay**
Cisco GETVPN キーサーバーのインターネットドラフト ACK		Cisco GETVPN キーサーバーのインターネットドラフト ACK は、シスコ製ではないグループメンバーとキーサーバーの間で、GDOI GROUPKEY-PUSH 確認応答メッセージドラフトで定義されているキー再生成確認応答メッセージの標準規格を実装します。 次のコマンドが導入または変更されました。 **rekey acknowledgement**、**show crypto gkm**。
RFC 8263 ID Ack の実装		Group Domain of Interpretation（GDOI）には、現在の一連のデバイスに追加のセキュリティアソシエーションを提供するキーサーバーの機能が含まれています。たとえば、期限切れのセキュリティ アソシエーションのキーを再生成できます。この機能により、グループデバイスがキー再生成メッセージの受信確認応答を返すように要求するキーサーバーの機能が追加され、確認応答の方式が指定されます。

第 231 章

GETVPN の Perfect Forward Secrecy

グループメンバー（GM）が侵害された場合、攻撃者は保存された長期キーとメッセージにアクセスする可能性があります。GETVPN の Perfect Forward Secrecy（PFS）により、攻撃者はキーとメッセージを使用して過去または将来のセッションのキーを取得することができなくなります。そのため、攻撃者は、侵害されたトラフィック暗号化キー（TEK）を使用して現在のセッションの通信を復号することは可能ですが、録音された通信や将来の通信は復号できません。

GETVPN の PFS に関する機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *314 : GETVPN* の *PFS* に関する機能情報

機能名	リリース	機能情報
GETVPN の Perfect Forward Secrecy	Cisco IOS XE Gibraltar 16.12.1	次のコマンドが導入または変更されました。**show crypto gkm feature pfs**、**pfs**、**show crypto gdoi**、および **client pfs**。

GETVPN の PFS に関する情報

GETVPN の PFS の概要

仮に、デバイスが侵害され、攻撃者が、デバイスに保存されている長期キーにアクセスしたとします。Perfect Forward Secrecy（PFS）では、攻撃者が長期キーを使用してキーを取得し、過去のセッションの記録された通信を復号することを防止します。関連するセキュリティ対策に、「Perfect Backward Secrecy（PBS）」と呼ばれるものがあります。PBS では、攻撃者が長期キーを使用してキーを取得し、将来のセッションの通信を復号することを防止します。

GM が侵害された場合、攻撃者は保存された長期キーとメッセージにアクセスする可能性があります。それにより、攻撃者は、Diffie-Hellman（DH）の結果および登録メッセージ、またはキー暗号化キー（KEK）と過去のキー再生成メッセージを取得する可能性があります。GETVPN の PFS では、攻撃者は、キーとメッセージを使用して過去のセッションの TEK を取得することができません。さらに、攻撃者は、KEK を使用して将来のキー再生成メッセージを復号できないため、将来のセッションの TEK を取得できません。そのため、攻撃者は、現在のセッションの TEK にのみアクセスできます。キーが侵害されても、記録された通信や将来の通信は安全なままです。

GETVPN の PFS には、次の変更点が含まれています。

- キー再生成プロセスが変更されています。GM 登録メカニズムは変更されていません。
- GETVPN の PFS を有効にすると、GM-KS IKEv2 チャネルのデフォルトのライフタイムが 1 日から 600 秒に変更されます。

  ただし、カスタマイズされたライフタイムを設定している場合は、GETVPN の PFS を有効にした後もライフタイムは変更されません。
- GETVPN の PFS をサポートするキーサーバー（KS）とグループメンバー（GM）には、新しいバージョン番号があります。このバージョン番号は、サードパーティの GM との後方互換性およびインタラクションをサポートします。

GETVPN の PFS に関する制約事項

- キーサーバー（KS）とグループメンバー（GM）は、IKEv2 プロトコルを使用して通信する必要があります。KS と GM が IKEv1 プロトコルを使用して通信する場合、GETVPN の PFS はサポートされません。
- COOP 内のすべての KS で PFS を有効にしてください。GM では、PFS はデフォルトで有効になっています。
- スケジュールされたキー再生成と手動でトリガーされたキー再生成の両方によって、GM が KS に再登録されます。この再登録により、特に大規模な場合に、KS で顕著なオーバーヘッドが発生する可能性があります。

- キー再生成を強制すると、GM 間のキーの不一致が原因でトラフィックが失われる可能性があります。
- RSA キーサイズが 4096 の場合は、キーのサイズが大きいために、暗号化エンジンによるキー再生成の署名にかなりの時間がかかります。キー再生成の署名中に受信した登録要求が多すぎると、暗号化エンジンが過負荷状態になる可能性があります。オーバーロードされた暗号化エンジンは、次のエラーメッセージをログに記録します。

```
%ACE-3-TRANSERR: IOSXE-ESG(9): IKEA trans 0x11A8; opcode 0x23; param 0x0; error 0xC;
 retry cnt 0
```

このエラーメッセージは、4096 の RSA キーサイズを使用しており、100 を超える GM があり、PFS が有効になっている GETVPN 展開において、より頻繁に表示される可能性があります。頻度が増加するのは、PFS が有効になっている場合、キー再生成のたびに再登録がトリガーされ、100 を超える GM では、暗号化エンジンがキー再生成の署名中に複数の登録要求を受信する可能性が高くなり、過負荷状態になる可能性があるためです。

同様に、そのような展開では、**crypto gdoi ks rekey replace-now** コマンドを繰り返し実行すると、このコマンドによってトリガーされる登録要求のために、このエラーメッセージがより頻繁に表示される可能性があります。

PFS が有効になっている GETVPN 展開では、2048 の RSA キーサイズを使用することをお勧めします。キー再生成メッセージには TEK/KEK キーが含まれないため、4096 の RSA キーサイズを使用する必要はありません。

変更されたキー再生成プロセス

GETVPN の PFS は、攻撃者が侵害された GM からの KEK を使用して過去または将来のキー再生成メッセージを復号できないようにします。そのため、攻撃者は、過去または将来の KEK や TEK を取得できません。この目的のために、GETVPN の PFS は、キー再生成メカニズムを変更して、キー再生成メッセージに KEK または TEK が含まれないようにします。キー再生成メッセージの内容は、キー再生成のタイプによって異なります。

スケジュールされたキー再生成

1. KEK または TEK のキー再生成タイマーが切れると、KS はそれぞれ新しい KEK または TEK を生成します。
2. KS は、キー再生成メッセージの GSA ペイロードにプライベート属性を設定し、現在の KEK でメッセージを暗号化します。キー再生成メッセージには、新しい KEK または TEK は含まれません。KS は、GM にキー再生成メッセージを送信します。
3. GM は、キー再生成メッセージを受信し、現在の KEK を使用してメッセージを復号します。GM は、スケジュールされたキー再生成を識別し、0 ～ 6 秒の範囲のランダムな時間間隔で再登録タイマーを開始します。
4. 再登録タイマーが切れると、GM は KS への再登録を開始します。
5. 再登録後、KS は、IKEv2 チャネルを介して KEK または TEK を GM に送信します。

6. 新しい KEK を受信すると、GM は、古い KEK を新しい KEK に置き換えます。
7. 新しい TEK を受信すると、GM は、TEK のアクティブ化時間遅延（ATD）を確認します。ATD が 0 以外の場合、GM は、データプレーンに TEK をインストールする前にタイマーを開始して ATD を適用します。

   ATD は、KS で次のように計算されます。

   1. 長い SA ライフタイムが設定されている場合、ATD タイマーは、次のように計算される秒単位の値に初期化されます。ATD =（古い TEK の残りのライフタイム）-（古い TEK の残りのライフタイムの 1%）- 75

      新しい TEK は、（古い TEK の残りのライフタイムの 1%）時にロールオーバーされます。

   2. 長い SA ライフタイムが設定されていない場合、ATD タイマーは、次のように計算される秒単位の値に初期化されます。ATD =（古い TEK の残りのライフタイム）- 75

      新しい TEK は、古い TEK の有効期限が切れる 30 秒前にロールオーバーされます。

同期キー再生成

1. KS は、pseudoTimeStamp（PST）値のみを含むキー再生成メッセージを GM に送信します。

   このメッセージに KEK または TEK は含まれません。
2. キー再生成メッセージを受信すると、GM は、疑似時間値を更新し、再登録をトリガーしません。KS から受信した pseudoTimeStamp 値と GM で設定された 時間ベースアンチリプレイ（TBAR）ウィンドウに応じて、GM が Syslog メッセージを生成する場合があります。

手動でトリガーされるキー

1. **crypto gdoi ks** または **clear crypto gdoi ks members** を使用してキー再生成動作をトリガーすると、KS は、キー再生成タイプに基づいて GAP/DELETE ペイロードを送信します。
   - ポリシー変更のないキー再生成メッセージ

表 *315*：ポリシー変更のないキー再生成メッセージの *GAP/DELETE* ペイロード

Type	KEK	TEK	キー再生成のプライベート属性	KD	GAP	DELETE
`crypto gdoi ks rekey`	非対応	非対応	非対応	非対応	非対応	非対応
`crypto gdoi ks rekey replace-now`	非対応	非対応	はい	非対応	ATD 1 秒	未対応
`clear crypto gdoi ks members`	非対応	非対応	非対応	非対応	ATD TEK の 5%	対応

Type	KEK	TEK	キー再生成のプライベート属性	KD	GAP	DELETE
clear crypto gdoi ks members now	非対応	非対応	はい	非対応	ATD 1 秒	対応

• ポリシー変更のある再生成メッセージ

表 *316 :* ポリシー変更のあるキー再生成メッセージの *GAP/DELETE* ペイロード

Type	KEK	TEK	キー再生成のプライベート属性	KD	GAP	DELETE
crypto gdoi ks rekey	非対応	非対応	はい	非対応	ATD TEK の 5%	未対応
crypto gdoi ks rekey replace-now	非対応	非対応	はい	非対応	ATD 1 秒	未対応
clear crypto gdoi ks members	非対応	非対応	非対応	非対応	ATD TEK の 5%	対応
clear crypto gdoi ks members now	非対応	非対応	はい	非対応	ATD 1 秒	対応

2. キー再生成メッセージを受信した GM は、KS への再登録を開始します。
3. 再登録の一環として、KS は、IKEv2 チャネルを介して KEK または TEK を GM に送信します。
4. GM は、古いキーのライフタイムを、KS から送信されたアクティブ化時間遅延（ATD）値に設定します。ATD の後、GM は、古いキーを削除し、新しいキーをインストールします。

Suite B のサポート

GM の初回登録時に、KS は、一意の送信者識別子（SID）と初期化ベクトル（IV）範囲を GM に割り当てます。GM がキー再生成メッセージに応答して KS に再登録する場合、GM は、KS が登録時に割り当てた SID を提供します。KS は、新しい SID または初期化ベクトル（IV）範囲を GM に割り当てません。

GETVPN の PFS の KS バージョンおよび GM バージョン

Cisco IOS XE Gibraltar 16.12.1 以降のリリースが GM にインストールされている場合、GETVPN の PFS はデフォルトで有効になります。コマンドラインインターフェイスを使用して、GETVPN の PFS を無効にできます。GM のバージョンは、次の表に示すように、PFS が有効になっているかどうかによって異なります。

	Suite B サポートなし	Suite B サポートあり	ASR 1000 シリーズ
PFS が無効	16	17	19
PFS が有効	21	22	20

Cisco IOS XE Gibraltar 16.12.1 以降のリリースが KS にインストールされている場合、GETVPN の PFS はデフォルトで無効になり、KS のバージョンは 1.0.18 です。CLI を使用して、GETVPN の PFS を有効にできます。GETVPN の PFS が有効になっている場合、KS のバージョンは 1.0.23 です。すべての連携 KS で GETVPN の PFS を有効にします。

KS は、GM のバージョンに基づいて、キー再生成メッセージを GM に送信します。

- GETVPN の PFS が無効になっており、1.0.17 や 1.0.19 などのバージョン番号を送信する GM に対して、KS は、KEK または TEK を含むキー再生成メッセージを送信します。

  KS は、GETVPN の PFS が無効になっている GM およびシスコ以外の GM に、KEK または TEK を含むキー再生成メッセージを送信します。GETVPN の PFS が無効になっている GM は、1.0.17 や 1.0.19 などのバージョン番号を KS に送信します。シスコ以外の GM は、KS に不明なバージョン番号を送信します。

- KS は、GETVPN の PFS が有効になっている GM に、KEK または TEK を含まない、変更されたキー再生成メッセージを送信します。GETVPN の PFS が有効になっている GM は、1.0.20 や 1.0.22 などのバージョン番号を送信します。

GETVPN の PFS のKS および GM の更新

GETVPN の PFS を有効にするには、ネットワーク内のすべての KS および GM で PFS を有効にします。GM で GETVPN の PFS を有効にしていない場合、GM が侵害されると、侵害されたキーにより、ネットワーク全体のセキュリティが妨げられる可能性があります。

次のように、ネットワーク内の KS をアップグレードします。

（注） KEK と TEK の有効期限が切れるまでに十分な時間がある間に KS をアップグレードすることをお勧めします。

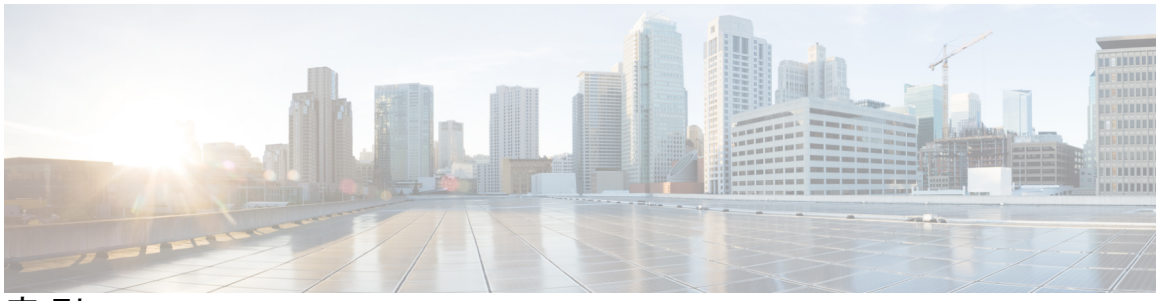
1. セカンダリ KS をアップグレードし、COOP の選択が完了するまで待ちます。
2. COOP の各セカンダリ KS について、手順 1 を繰り返します。

   セカンダリ KS が再起動してプライマリ KS と同期し、セカンダリ KS の役割を担います。
3. プライマリ KS をアップグレードします。

   セカンダリ KS の 1 つが新しいプライマリ KS として選択されます。アップグレードされた KS が再起動し、セカンダリ KS の役割を担います。

4. すべての KS で PFS を有効にします。

アップグレード後、KS は、GM が送信するバージョン番号に基づいてキー再生成メッセージを送信します。GM バージョン番号に基づいて、KS は、KEK または TEK を含むキー再生成メッセージか、KEK または TEK を含まない変更されたキー再生成メッセージを送信します。



索 引

A

C

D

E

F

G

H

K

L

M

N

O

P

R

S

T

U

V

あ

か

さ

す

せ

そ

と

な

は

ふ

へ

ほ

め

も

り

ろ

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。