CLI ブック 1：Cisco ASA シリーズ 9.4 CLI コンフィギュレーション ガイド（一般的な操作）

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

目 次

このマニュアルについて

ここでは、このガイドを使用する方法について説明します。

本書の目的

このマニュアルは、コマンドライン インターフェイスを使用して Cisco ASA シリーズの一般的な操作を設定する際に役立ちます。このマニュアルは、すべての機能を網羅しているわけではなく、ごく一般的なコンフィギュレーションの事例を紹介しています。

また、Web ベースの GUI アプリケーションである適応型セキュリティ デバイス マネージャ（ASDM）を使用して ASA を設定、監視することもできます。ASDM では、コンフィギュレーション ウィザードを使用して、いくつかの一般的なコンフィギュレーションを設定できます。また、あまり一般的ではない事例には、オンラインのヘルプが用意されています。

このマニュアルを通じて、「ASA」という語は、特に指定がない限り、サポートされているモデルに一般的に適用されます。

関連資料

詳細については、『*Navigating the Cisco ASA Series Documentation*』（http://www.cisco.com/go/asadocs）を参照してください。

表記法

このマニュアルでは、文字、表示、および警告に関する次の規則に準拠しています。

文字表記法

表記法	説明
boldface	コマンド、キーワード、ボタン ラベル、フィールド名、およびユーザ入力テキストは、**boldface**で示しています。メニューベース コマンドの場合は、メニュー項目を [ ] で囲み、コマンドのフル パスを示しています。
italic	ユーザが値を指定する変数は、イタリック体で示しています。 イタリック体は、マニュアル タイトルと一般的な強調にも使用されています。
等幅	システムが表示するターミナル セッションおよび情報は、等幅文字で記載されます。
{x | y | z}	どれか1つを選択しなければならない必須キーワードは、波カッコで囲み、縦棒で区切って示しています。
[ ]	角カッコの中の要素は、省略可能です。
[x | y | z]	いずれか 1 つを選択できる省略可能なキーワードは、角カッコで囲み、縦棒で区切って示しています。
[ ]	システム プロンプトに対するデフォルトの応答も、角カッコで囲んで記載されます。
< >	パスワードなどの出力されない文字は、山カッコ（< >）で囲んで示しています。
!、#	コードの先頭に感嘆符（!）または番号記号（#）がある場合は、コメント行であることを示します。

読者への警告

このマニュアルでは、読者への警告に以下を使用しています。

（注） 「注釈」です。役立つ情報やこのマニュアルに記載されていない参照資料を紹介しています。

ヒント 「問題解決に役立つ情報」です。

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

ワンポイント アドバイス	時間を節約する方法です。ここに紹介している方法で作業を行うと、時間を短縮できます。
警告	「警告」の意味です。人身事故を予防するための注意事項が記述されています。

通信、サービス、およびその他の情報

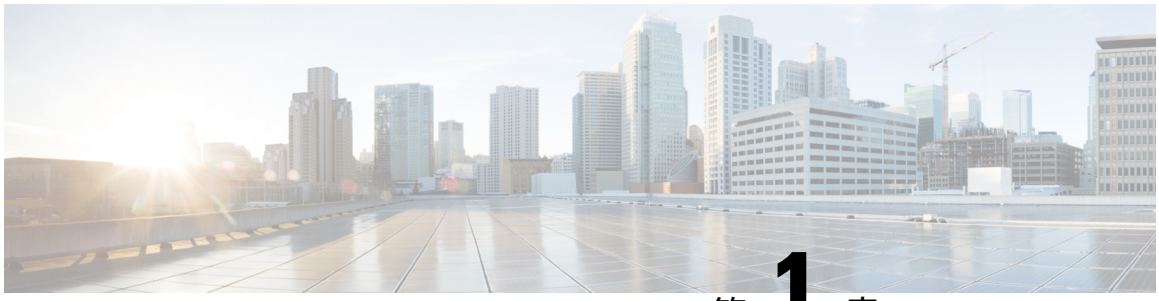
- シスコからタイムリーな関連情報を受け取るには、Cisco Profile Manager でサインアップしてください。
- 重要な技術によりビジネスに必要な影響を与えるには、シスコ サービスにアクセスしてください。
- サービス リクエストを送信するには、シスコ サポートにアクセスしてください。
- 安全で検証済みのエンタープライズクラスのアプリケーション、製品、ソリューション、およびサービスを探して参照するには、Cisco Marketplace にアクセスしてください。
- 一般的なネットワーク、トレーニング、認定関連の出版物を入手するには、Cisco Press にアクセスしてくださ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

Cisco バグ検索ツール

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

第 部

ASA の開始



第 1 章

Cisco ASA の概要

Cisco ASA は、追加モジュールとの統合サービスに加え、高度なステートフル ファイアウォールおよび VPN コンセントレータ機能を 1 つのデバイスで提供します。ASA は、複数のセキュリティコンテキスト（仮想ファイアウォールに類似）、クラスタリング（複数のファイアウォールを 1 つのファイアウォールに統合）、トランスペアレント（レイヤ 2）ファイアウォールまたはルーテッド（レイヤ3）ファイアウォール オペレーション、高度なインスペクション エンジン、IPsec VPN、SSL VPN、クライアントレス SSL VPN サポートなど、多数の高度な機能を含みます。

ハードウェアとソフトウェアの互換性

サポートされるすべてのハードウェアおよびソフトウェアの一覧は、『Cisco ASA Compatibility（Cisco ASA の互換性）』[英語] を参照してください。

VPN の互換性

『Supported VPN Platforms, Cisco ASA Series』[英語] を参照してください。

新機能

このセクションでは、各リリースの新機能を示します。

（注） 『syslog メッセージ ガイド』に、新規、変更済み、および廃止された syslog メッセージを記載しています。

ASA 9.4(4.5) の新機能

リリース：2017年4月3日

（注） バージョン 9.4(4) は、バグ CSCvd78303 のため、Cisco.com から削除されました。

このリリースに新機能はありません。

ASA 9.4(3) の新機能

リリース：2016年4月25日

機能	説明
ファイアウォール機能	
ルートの収束に対する接続ホールドダウン タイムアウト。	接続で使用されているルートがもう存在していない、または非アクティブになったときに、システムが接続を保持する時間を設定できるようになりました。このホールドダウン期間内にルートがアクティブにならない場合、接続は解放されます。ルートの収束がさらに迅速に行われるようにホールドダウンタイマーを短縮することができます。ただし、ほとんどのネットワークでは、ルートのフラッピングを防止するためにデフォルトの 15 秒が適切です。 次のコマンドが追加されました。**timeout conn-holddown**
リモート アクセス機能	
設定可能な SSH 暗号機能と HMAC アルゴリズム	ユーザはSSH暗号化を管理するときに暗号化モードを選択し、さまざまなキー交換アルゴリズムに対して HMAC と暗号化を設定できます。 次のコマンドが導入されました。**ssh cipher encryption**、**ssh cipher integrity**。 *9.1(7)* でも使用可能です。
IPv6 の HTTP リダイレクト サポート	ASDM アクセスまたはクライアントレス SSL VPN 用の HTTPS に HTTP リダイレクトを有効にすると、IPv6 アドレスへ送信されるトラフィックもリダイレクトできるようになりました。 次のコマンドに機能が追加されました。**http redirect** *9.1(7)* でも使用可能です。

機能	説明
モニタリング機能	
フェールオーバーの SNMP engineID の同期	フェールオーバー ペアでは、一対の ASA の SNMP engineID は両方のユニットで同期されます。ASA ごとに、同期された engineID、ネイティブ engineID、およびリモート engineID による engineID が 3 セット維持されます。 SNMPv3 ユーザは、ローカライズされた **snmp-server user** 認証とプライバシー オプションを保存するためのプロファイルを作成するときに ASA の engineID も指定できます。ユーザがネイティブ engineID を指定しない場合、**show running config** 出力に engineID がユーザごとに 2 つずつ表示されます。 次のコマンドが変更されました。**snmp-server user**
show tech support の強化	**show tech support** コマンドは現在次のとおりです。 • **dir all-filesystems** の出力が含まれます。この出力は次の場合に役立つことがあります。 • SSL VPN コンフィギュレーション：必要なリソースが ASA にあるかどうかを確認します。 • クラッシュ：クラッシュ ファイルの日付のタイムスタンプと存在を確認します。 • **show kernel cgroup-controller detail** の出力の削除：このコマンド出力は **show tech-support detail** の出力内に残されます。 次のコマンドが変更されました。**show tech support** *9.1(7)* でも使用可能です。
CISCO-ENHANCED-MEMPOOL-MIB の cempMemPoolTable のサポート	CISCO-ENHANCED-MEMPOOL-MIB の cempMemPoolTable がサポートされました。これは、管理型システムのすべての物理エンティティのメモリプールモニタリング エントリのテーブルです。 （注） CISCO-ENHANCED-MEMPOOL-MIB は 64 ビットのカウンタを使用して、プラットフォーム上の 4 GB 以上のメモリのレポーティングをサポートします。 追加または変更されたコマンドはありません。 *9.1(7)* でも使用可能です。

ASA 9.4(2.145) の新機能

リリース：**2015年11月13日**

このリリースに新機能はありません。

（注） このリリースは Firepower 9300 ASA セキュリティ モジュールのみをサポートします。

ASA 9.4(2) の新機能

リリース：**2015年9月24日**

このリリースに新機能はありません。

（注） ASAv 9.4(1.200) の各機能はこのリリースには含まれません。

（注） このバージョンは ISA 3000 をサポートしません。

ASA 9.4(1.225) の新機能

リリース：**2015年9月17日**

（注） このリリースは Cisco ISA 3000 のみをサポートします。

機能	説明
プラットフォーム機能	

機能	説明
Cisco ISA 3000 サポート	Cisco ISA 3000 は、DIN レールにマウントされた高耐久型の産業用セキュリティ アプライアンスです。ギガビットイーサネットと専用管理ポートを備えた、低消費電型ファンレス デバイスです。このモデルには ASA Firepower モジュールが事前にインストールされています。このモデルの特別な機能として、カスタマイズされたトランスペアレントモードのデフォルト設定と、電源喪失時もトラフィックがアプライアンスを通過することを可能にするハードウェア バイパス機能があります。 次のコマンドが導入されました。**hardware-bypass**、**hardware-bypass manual**、**hardware-bypass boot-delay**、**show hardware-bypass** この機能は、バージョン *9.5(1)* では使用できません。

ASA 9.4(1.152) の新機能

リリース：**2015年7月13日**

（注） このリリースは、Firepower 9300 の ASA のみをサポートします。

機能	説明
プラットフォーム機能	
Firepower 9300 の ASA セキュリティ モジュール	Firepower 9300 の ASA セキュリティ モジュールに ASA を導入しました。 （注） Firepower Chassis Manager 1.1.1 は Firepower 9300 の ASA セキュリティ モジュールの VPN 機能（サイト間またはリモート アクセス）を一切サポートしません。
ハイ アベイラビリティ機能	
Firepower 9300用シャーシ内 ASA クラスタリング	FirePOWER 9300 シャーシ内では、最大 3 つセキュリティ モジュールをクラスタ化できます。シャーシ内のすべてのモジュールは、クラスタに属している必要があります。 次のコマンドを導入しました。**cluster replication delay**、**debug service-module**、**management-only individual**、**show cluster chassis**
ライセンシング機能	
Firepower 9300 の ASA のシスコ スマート ソフトウェア ライセンシング	FirePOWER 9300 に ASA のシスコ スマート ソフトウェア ライセンシングが導入されました。 次のコマンドが導入されました。**feature strong-encryption**、**feature mobile-sp**、**feature context**

ASAv 9.4(1.200) の新機能

リリース：**2015年5月12日**

（注） このリリースは、ASAv のみをサポートします。

機能	説明
プラットフォーム機能	
VMware 上の ASAv では vCenter サポートは不要になりました。	vCenter なしで、vSphere クライアントまたは OVFTool のデイゼロ設定を使用して ASAv を VMware 上にインストールできるようになりました。
Amazon Web Services（AWS）の ASAv	Amazon Web Services（AWS）とデイゼロ設定で ASAv を使用できるようになりました。 （注） Amazon Web Services は ASAv10 と ASAv30 のモデルのみをサポートします。

ASA 9.4(1) の新機能

リリース：**2015年3月30日**

機能	説明
プラットフォーム機能	
ASA 5506W-X、ASA 5506H-X、ASA 5508-X、ASA 5516-X	ワイヤレスアクセスポイントを内蔵した ASA 5506W-X、強化された ASA 5506H-X、ASA 5508-X、ASA 5516-X の各モデルが導入されました。 **hw-module module wlan recover image**、**hw-module module wlan recover image** の各コマンドが導入されました。
認定機能	

機能	説明
国防総省（DoD）統一機能規則（UCR）2013 証明書	ASA は、DoD UCR 2013 規則を遵守するように更新されています。この証明書に追加された次の機能については、この表の行を参照してください。 • 定期的な証明書認証 • 証明書有効期限のアラート • 基本制約 CA フラグの適用 • 証明書コンフィギュレーションの ASDM ユーザ名 • ASDM 管理認証 • IKEv2 無効セレクタの通知設定 • 16 進数の IKEv2 事前共有キー
FIPS 140-2 認証のコンプライアンス更新	ASA で FIPS モードを有効にすると、ASA が FIPS 140-2 に準拠するように追加制限が設定されます。次の制限があります。 • RSA および DH キー サイズの制限：RSA および DH キー 2K（2048 ビット）以上のみが許可されます。DH の場合、これはグループ 1（768 ビット）、2（1024 ビット）、5（1536 ビット）が許可されないことを意味します。 （注） キー サイズの制限により、FIPS での IKEv1 の使用が無効になります。 • デジタル署名のハッシュ アルゴリズムの制限：SHA 256 以上のみが許可されます。 • SSH 暗号の制限：許可された暗号は aes128-cbc または aes256-cbc です。MAC は SHA1 です。 ASA の FIPS 認証ステータスを表示するには、次の URL を参照してください。 http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140InProcess.pdf この PDF は毎週更新されます。 詳細については、Computer Security Division Computer Security Resource Center のサイトを参照してください。 http://csrc.nist.gov/groups/STM/cmvp/inprocess.html **fips enable** コマンドが変更されました。
ファイアウォール機能	

機能	説明
複数のコアを搭載した ASA での SIP インスペクションのパフォーマンスが向上。	複数のコアで ASA を通過する SIP シグナリングチングが複数存在する場合の SIP インスペクション パフォーマンスが向上しました。ただし、TLS、電話、または IME プロキシを使用する場合、パフォーマンスの向上は見られません。 変更されたコマンドはありません。
電話プロキシおよび UC-IME プロキシに対する SIP インスペクションのサポートが削除されました。	SIP インスペクションを設定する際、電話プロキシまたは UC-IME プロキシは使用できなくなります。暗号化されたトラフィックを検査するには、TLS プロキシを使用します。 **phone-proxy**、**uc-ime** の各コマンドが削除されました。**inspect sip** コマンドから **phone-proxy** キーワードと **uc-ime** キーワードが削除されました。
ISystemMapper UUID メッセージ RemoteGetClassObject opnum3 の DCERPC インスペクションのサポート。	ASA は、リリース 8.3 で EPM 以外の DCERPC メッセージのサポートを開始し、ISystemMapper UUID メッセージ RemoteCreateInstance opnum4 をサポートしています。この変更により、RemoteGetClassObject opnum3 メッセージまでサポートが拡張されます。 変更されたコマンドはありません。
コンテキストごとに無制限の SNMP サーバ トラップ ホスト	ASA では、コンテキストごとに SNMP サーバのトラップ ホスト数の制限がありません。**show snmp-server host** コマンドの出力には ASA をポーリングしているアクティブなホストと、静的に設定されたホストのみが表示されます。 **show snmp-server host** コマンドが変更されました。
VXLAN パケット インスペクション	ASA は、標準形式に準拠するために VXLAN ヘッダーを検査できます。 **inspect vxlan** コマンドが導入されました。
IPv6 の DHCP モニタリング	IPv6 の DHCP 統計情報および DHCP バインディングをモニタできます。
ESMTP インスペクションの TLS セッションでのデフォルトの動作が変更されました。	ESMTP インスペクションのデフォルトが、検査されない、TLS セッションを許可するように変更されました。ただし、このデフォルトは新しい、または再イメージングされたシステムに適用されます。**no allow-tls** を含むシステムをアップグレードする場合、このコマンドは変更されません。 デフォルトの動作の変更は、古いバージョンでも行われました：8.4（7.25）、8.5（1.23）、8.6（1.16）、8.7（1.15）、9.0（4.28）、9.1（6.1）、9.2（3.2）、9.3（1.2）、9.3（2.2）。
ハイ アベイラビリティ機能	
スタンバイ ASA での syslog 生成のブロック	スタンバイ装置で特定の syslog の生成をブロックできます。 **no logging message** *syslog-id* **standby** コマンドが導入されました。

機能	説明
インターフェイスごとに ASA クラスタのヘルス モニタリングをイネーブルまたはディセーブル	ヘルス モニタリングは、インターフェイスごとにイネーブルまたはディセーブルにすることができます。デフォルトでは、ポートチャネル、冗長、および単一のすべての物理インターフェイスでヘルス モニタリングがイネーブルになっています。ヘルス モニタリングは VLAN サブインターフェイス、または VNI や BVI などの仮想インターフェイスでは実行されません。クラスタ制御リンクのモニタリングは設定できません。このリンクは常にモニタされています。たとえば、管理インターフェイスなど、必須以外のインターフェイスのヘルス モニタリングをディセーブルにすることができます。 **health-check monitor-interface** コマンドが導入されました。
DHCP リレーの ASA クラスタリングのサポート	ASA クラスタで DHCP リレーを設定できます。クライアントの DHCP 要求は、クライアントの MAC アドレスのハッシュを使用してクラスタ メンバにロードバランスされます。DHCP クライアントおよびサーバ機能はサポートされていません。 **debug cluster dhcp-relay** コマンドが導入されました。
ASA クラスタリングでの SIP インスペクションのサポート	ASA クラスタで SIP インスペクションを設定できます。制御フローは、任意のユニットで作成できますが（ロード バランシングのため）、その子データ フローは同じユニットに存在する必要があります。TLS プロキシ設定はサポートされていません。 **show cluster service-policy** コマンドが導入されました。
ルーティング機能	
Policy Based Routing：ポリシーベース ルーティング	ポリシーベース ルーティング（PBR）は、ACL を使用して指定された QoS でトラフィックが特定のパスを経由するために使用するメカニズムです。ACL では、パケットのレイヤ 3 および レイヤ4 ヘッダーの内容に基づいてトラフィックを分類できます。このソリューションにより、管理者は区別されたトラフィックに QoS を提供し、低帯域幅、低コストの永続パス、高帯域幅、高コストのスイッチドパスの間でインタラクティブ トラフィックとバッチ トラフィックを分散でき、インターネット サービス プロバイダーとその他の組織は明確に定義されたインターネット接続を介して一連のさまざまなユーザから送信されるトラフィックをルーティングできます。 **set ip next-hop verify-availability**、**set ip next-hop**、**set ip next-hop recursive**、**set interface**、**set ip default next-hop**、**set default interface**、**set ip df**、**set ip dscp**、**policy-route route-map**、**show policy-route**、**debug policy-route** の各コマンドが導入されました。
インターフェイス機能	

機能	説明
VXLAN のサポート	VXLAN のサポートが追加されました（VXLAN トンネルエンドポイント（VTEP）のサポートを含む）。ASA またはセキュリティ コンテキストごとに 1 つの VTEP 送信元インターフェイスを定義できます。 次のコマンドが導入されました。**debug vxlan**、**default-mcast-group**、**encapsulation vxlan**、**inspect vxlan**、**interface vni**、**mcast-group**、**nve**、**nve-only**、**peer ip**、**segment-id**、**show arp vtep-mapping**、**show interface vni**、**show mac-address-table vtep-mapping**、**show nve**、**show vni vlan-mapping**、**source-interface**、**vtep-nve**、**vxlan port**
モニタリング機能	
EEM のメモリ トラッキング	メモリの割り当てとメモリの使用状況をログに記録してメモリ ロギングのラップ イベントに応答するための新しいデバッグ機能が追加されました。 次のコマンドが導入または変更されました。**memory logging**、**show memory logging**、**show memory logging include**、**event memory-logging-wrap**
トラブルシューティングのクラッシュ	**show tech-support** コマンドの出力と **show crashinfo** コマンドの出力には、生成された syslog の最新 50 行が含まれます。これらの結果を表示できるようにするには、**logging buffer** コマンドをイネーブルにする必要があります。
リモート アクセス機能	
ECDHE-ECDSA 暗号のサポート	TLSv1.2 では、次の暗号のサポートが追加されています。 • ECDHE-ECDSA-AES256-GCM-SHA384 • ECDHE-RSA-AES256-GCM-SHA384 • DHE-RSA-AES256-GCM-SHA384 • AES256-GCM-SHA384 • ECDHE-ECDSA-AES256-SHA384 • ECDHE-RSA-AES256-SHA384 • ECDHE-ECDSA-AES128-GCM-SHA256 • ECDHE-RSA-AES128-GCM-SHA256 • DHE-RSA-AES128-GCM-SHA256 • RSA-AES128-GCM-SHA256 • ECDHE-ECDSA-AES128-SHA256 • ECDHE-RSA-AES128-SHA256 （注） 優先度が最も高いのは ECDSA 暗号および DHE 暗号です。 **ssl ecdh-group** コマンドが導入されました。

機能	説明
クライアントレス SSL VPN セッション Cookie アクセスの制限	クライアントレス SSL VPN セッション Cookie が JavaScript などのクライアント側のスクリプトを介してサードパーティからアクセスされないようにすることができます。 （注） この機能は、Cisco TAC から使用を推奨された場合のみ使用してください。このコマンドをイネーブルにすると、次のクライアントレス SSL VPN 機能が警告なしで動作しなくなるため、セキュリティ上のリスクが発生します。 • Java プラグイン • Java リライタ • ポート フォワーディング。 • ファイル ブラウザ • デスクトップ アプリケーション（Microsoft Office アプリケーションなど）を必要とする Sharepoint 機能 • AnyConnect Web 起動 • Citrix Receiver、XenDesktop、および Xenon • その他の非ブラウザ ベース アプリケーションおよびブラウザ プラグイン ベースのアプリケーション **http-only-cookie** コマンドが導入されました。 この機能は、*9.2(3)* にもあります。
セキュリティ グループ タギングを使用した仮想デスクトップのアクセス制御	ASA では、内部アプリケーションおよび Web サイトへのクライアントレス SSL リモートアクセス用にセキュリティ グループ タギングベースのポリシー制御をサポートしています。この機能では、配信コントローラおよび ASA のコンテンツ変換エンジンとして XenDesktop による Citrix の仮想デスクトップ インフラストラクチャ（VDI）を使用します。 詳細については、次の Citrix 製品のマニュアルを参照してください。 • XenDesktop および XenApp のポリシー：http://support.citrix.com/proddocs/topic/infocenter/ic-how-to-use.html • XenDesktop 7 でのポリシーの管理：http://support.citrix.com/proddocs/topic/xendesktop-7/cds-policies-wrapper-rho.html • XenDesktop 7 のポリシー用のグループ ポリシー エディタの使用：http://support.citrix.com/proddocs/topic/xendesktop-7/cds-policies-use-gpmc.html

機能	説明
クライアントレスSSL VPN に OWA 2013 機能のサポートを追加	クライアントレス SSL VPN では、以下を除き、OWA 2013 の新機能をサポートしています。 • タブレットおよびスマートフォンのサポート • オフライン モード • Active Directory Federation Services（AD FS）2.0. ASA および AD FS 2.0 は、暗号化プロトコルをネゴシエートできません。 変更されたコマンドはありません。
クライアントレスSSL VPN に Citrix XenDesktop 7.5 および StoreFront 2.5 のサポートを追加	クライアントレス SSL VPN では、XenDesktop 7.5 および StoreFront 2.5 のアクセスをサポートしています。 XenDesktop 7.5 の機能の完全なリストと詳細については、http://support.citrix.com/proddocs/topic/xenapp-xendesktop-75/cds-75-about-whats-new.html を参照してください。 StoreFront 2.5 の機能の完全なリストと詳細については、http://support.citrix.com/proddocs/topic/dws-storefront-25/dws-about.html を参照してください。 変更されたコマンドはありません。
定期的な証明書認証	定期的な証明書認証を有効にすると、ASA は、VPN クライアントから受信した証明書チェーンを保存し、それらを定期的に再認証します。 **periodic-authentication certificate**、**revocation-check, show vpn-sessiondb** の各コマンドが導入または変更されました。
証明書有効期限のアラート	ASA は、トラスト ポイントですべての CA および ID の証明書の有効期限について 24 時間ごとにチェックします。証明書の有効期限がまもなく切れる場合は、syslog がアラートとして発行されます。リマインダおよび繰り返しの間隔を設定できます。デフォルトでは、リマインダは有効期限の 60 日前に開始し、7 日ごとに繰り返されます。 **crypto ca alerts expiration** コマンドが導入または変更されました。
基本制約 CA フラグの適用	デフォルトでは、CA フラグのない証明書を CA 証明書として ASA にインストールできなくなりました。基本制約拡張は、証明書のサブジェクトが CA で、この証明書を含む有効な認証パスの最大深さかどうかを示すものです。必要に応じて、これらの証明書のインストールを許可するように ASA を設定できます。 **ca-check** コマンドが導入されました。

機能	説明
IKEv2 無効セレクタの通知設定	現在、ASA が SA 上で着信パケットを受信し、そのパケットのヘッダー フィールドが SA 用のセレクタに適合しなかった場合、ASA はそのパケットを廃棄します。ピアへの IKEv2 通知の送信をイネーブルまたはディセーブルにすることができます。この通知の送信はデフォルトで無効になっています。 （注） この機能は、AnyConnect 3.1.06060 以降でサポートされています。 **crypto ikev2 notify invalid-selectors** コマンドが導入されました。
16 進数の IKEv2 事前共有キー	16 進数の IKEv2 事前共有キーを設定できます。 **ikev2 local-authentication pre-shared-key hex**、**ikev2 remote-authentication pre-shared-key hex** の各コマンドが導入されました。
管理機能	
ASDM 管理認証	HTTP アクセスと Telnet および SSH アクセス別に管理認証を設定できるようになりました。 次のコマンドが導入されました。 **aaa authorization http console**
証明書コンフィギュレーションの ASDM ユーザ名	ASDM の証明書認証（**http authentication-certificate**）を有効にすると、ASDM が証明書からユーザ名を抽出する方法を設定できます。また、ログイン プロンプトでユーザ名を事前に入力して表示できます。 次のコマンドが導入されました。**http username-from-certificate**
CLI で **?** の入力時にヘルプを有効または無効にするための **terminal interactive** コマンド	通常、ASA CLI で **?** を入力すると、コマンド ヘルプが表示されます。コマンド内にテキストとして **?** を入力できるようにするには（たとえば、URL の一部として ? を含めるには）、**no terminal interactive** コマンドを使用してインタラクティブなヘルプを無効にします。 次のコマンドが導入されました。terminal interactive
REST API の機能	
REST API バージョン 1.1	REST API バージョン 1.1 のサポートが追加されました。
トークンベース認証が（既存の基本認証に加えて）サポートされるようになりました。	クライアントは特定の URL にログイン要求を送信でき、成功すると、（応答ヘッダーに）トークンが返されます。クライアントはさらなる API コールを送信するために、（特別な要求ヘッダー内で）このトークンを使用します。トークンは明示的に無効にするまで、またはアイドル/セッション タイムアウトに到達するまで有効です。

機能	説明
マルチ コンテキスト モードの限定的なサポート	REST API エージェントをマルチ コンテキスト モードで有効にできるようになりました。CLI コマンドはシステム コンテキスト モードでのみ発行できます（シングル コンテキスト モードと同じコマンド）。 次のようにパススルー CLI の API コマンドを使用して、コンテキストを設定できます。 `https://<asa_admin_context_ip>/api/cli?context=<context_name>` **context** パラメータがない場合、要求は **admin** コンテキストに向けられたものとみなされます。
高度な（粒状の）インスペクション	次のプロトコルの詳細なインスペクションをサポートします。 • DNS over UDP • HTTP • ICMP • ICMP ERROR • RTSP • SIP • FTP • DCERPC • IP オプション • NetBIOS Name Server over IP • SQL*Net

ファイアウォール機能の概要

ファイアウォールは、外部ネットワーク上のユーザによる不正アクセスから内部ネットワークを保護します。また、ファイアウォールは、人事部門ネットワークをユーザ ネットワークから分離するなど、内部ネットワーク同士の保護も行います。Web サーバまたはFTP サーバなど、外部のユーザが使用できるようにする必要のあるネットワーク リソースがあれば、ファイアウォールで保護された別のネットワーク（非武装地帯（DMZ）と呼ばれる）上に配置します。ファイアウォールによってDMZに許可されるアクセスは限定されますが、DMZにあるのは公開サーバだけのため、この地帯が攻撃されても影響を受けるのは公開サーバに限定され、他の内部ネットワークに影響が及ぶことはありません。また、特定アドレスだけに許可する、認証または認可を義務づける、または外部の URL フィルタリング サーバと協調するといった手段

によって、内部ユーザが外部ネットワーク（インターネットなど）にアクセスする機会を制御することもできます。

ファイアウォールに接続されているネットワークに言及する場合、外部ネットワークはファイアウォールの手前にあるネットワーク、内部ネットワークはファイアウォールの背後にある保護されているネットワーク、そして *DMZ* はファイアウォールの背後にあるが、外部ユーザに制限付きのアクセスが許されているネットワークです。ASA を使用すると、数多くのインターフェイスに対してさまざまなセキュリティポリシーが設定できます。このインターフェイスには、多数の内部インターフェイス、多数の DMZ、および必要に応じて多数の外部インターフェイスが含まれるため、ここでは、このインターフェイスの区分は一般的な意味で使用するだけです。

セキュリティ ポリシーの概要

他のネットワークにアクセスするために、ファイアウォールを通過することが許可されるトラフィックがセキュリティポリシーによって決められます。デフォルトでは、内部ネットワーク（高セキュリティ レベル）から外部ネットワーク（低セキュリティ レベル）へのトラフィックは、自由に流れることが ASA によって許可されます。トラフィックにアクションを適用してセキュリティ ポリシーをカスタマイズすることができます。

アクセス ルールによるトラフィックの許可または拒否

アクセス ルールを適用することで、内部から外部に向けたトラフィックを制限したり、外部から内部に向けたトラフィックを許可したりできます。ブリッジグループ インターフェイスでは、EtherType アクセス ルールを適用して、非 IP トラフィックを許可できます。

NAT の適用

NAT の利点のいくつかを次に示します。

- 内部ネットワークでプライベート アドレスを使用できます。プライベート アドレスは、インターネットにルーティングできません。
- NAT はローカル アドレスを他のネットワークから隠蔽するため、攻撃者はホストの実際のアドレスを取得できません。
- NAT は、重複 IP アドレスをサポートすることで、IP ルーティングの問題を解決できます。

IP フラグメントからの保護

ASA は、IP グラグメント保護を提供します。この機能は、すべての ICMP エラー メッセージの完全なリアセンブリと、ASA 経由でルーティングされる残りの IP フラグメントの仮想リアセンブリを実行します。セキュリティ チェックに失敗したフラグメントは、ドロップされログに記録されます。仮想リアセンブリはディセーブルにできません。

HTTP、HTTPS、または FTP フィルタリングの適用

アクセス リストを使用して、特定の Web サイトまたは FTP サーバへの発信アクセスを禁止できますが、このような方法で Web サイトの使用方法を設定し管理することは、インターネットの規模とダイナミックな特性から、実用的とはいえません。

ASA でクラウド Web セキュリティを設定したり、URL およびその他のフィルタリング サービス（ASA CX や ASA FirePOWER など）を提供する ASA モジュールをインストールすることができます。ASA は、Cisco Web セキュリティ アプライアンス（WSA）などの外部製品とともに使用することも可能です。

アプリケーション インスペクションの適用

インスペクション エンジンは、ユーザのデータ パケット内に IP アドレッシング情報を埋め込むサービスや、ダイナミックに割り当てられるポート上でセカンダリ チャネルを開くサービスに必要です。これらのプロトコルは、ASA によるディープ パケット インスペクションの実行を必要とします。

サポート対象のハードウェアモジュールまたはソフトウェアモジュールへのトラフィックの送信

一部の ASA モデルでは、ソフトウェア モジュールの設定、またはハードウェア モジュールのシャーシへの挿入を行うことで、高度なサービスを提供することができます。これらのモジュールを通じてトラフィック インスペクションを追加することにより、設定済みのポリシーに基づいてトラフィックをブロックできます。また、これらのモジュールにトラフィックを送信することで、高度なサービスを利用することができます。

QoS ポリシーの適用

音声やストリーミング ビデオなどのネットワーク トラフィックでは、長時間の遅延は許容されません。QoS は、この種のトラフィックにプライオリティを設定するネットワーク機能です。QoS とは、選択したネットワーク トラフィックによりよいサービスを提供するネットワークの機能です。

接続制限と TCP 正規化の適用

TCP 接続、UDP 接続、および初期接続を制限することができます。接続と初期接続の数を制限することで、DoS 攻撃（サービス拒絶攻撃）から保護されます。ASA では、初期接続の制限を利用して TCP 代行受信を発生させます。代行受信によって、TCP SYN パケットを使用してインターフェイスをフラッディングする DoS 攻撃から内部システムを保護します。初期接続とは、送信元と宛先の間で必要になるハンドシェイクを完了していない接続要求のことです。

TCP 正規化は、正常に見えないパケットをドロップするように設計された高度な TCP 接続設定で構成される機能です。

脅威検出のイネーブル化

スキャン脅威検出と基本脅威検出、さらに統計情報を使用して脅威を分析する方法を設定できます。

基本脅威検出は、DoS 攻撃などの攻撃に関係している可能性のあるアクティビティを検出し、自動的にシステム ログ メッセージを送信します。

典型的なスキャン攻撃では、あるホストがサブネット内の IP アドレスにアクセスできるかどうかを 1 つずつ試します（サブネット内の複数のホストすべてを順にスキャンするか、1 つのホストまたはサブネットの複数のポートすべてを順にスイープする）。スキャン脅威検出機能は、いつホストがスキャンを実行するかを判別します。トラフィック署名に基づく IPS スキャン検出とは異なり、ASA のスキャニング脅威検出機能は、スキャン アクティビティに関して分析できるホスト統計を含む膨大なデータベースを維持します。

ホスト データベースは、不審なアクティビティを追跡します。このようなアクティビティには、戻りアクティビティのない接続、閉じているサービス ポートへのアクセス、脆弱な TCP 動作（非ランダム IPID など）、およびその他の多くの動作が含まれます。

攻撃者に関するシステム ログ メッセージを送信するように ASA を設定できます。または、自動的にホストを排除できます。

ファイアウォール モードの概要

ASA は、次の 2 つのファイアウォール モードで動作します。

- ルーテッド
- Transparent

ルーテッド モードでは、ASA は、ネットワークのルータ ホップと見なされます。

トランスペアレント モードでは、ASA は「Bump In The Wire」または「ステルス ファイアウォール」のように動作し、ルータ ホップとは見なされません。ASA は「ブリッジグループ」の内部および外部インターフェイスと同じネットワークに接続します。

トランスペアレント ファイアウォールは、ネットワーク コンフィギュレーションを簡単にするために使用できます。トランスペアレント モードは、攻撃者からファイアウォールが見えないようにする場合にも有効です。トランスペアレント ファイアウォールは、他の場合にはルーテッド モードでブロックされるトラフィックにも使用できます。たとえば、トランスペアレント ファイアウォールでは、EtherType アクセス リストを使用するマルチキャスト ストリームが許可されます。

ステートフル インスペクションの概要

ASA を通過するトラフィックはすべて、アダプティブ セキュリティ アルゴリズムを使用して検査され、通過が許可されるか、またはドロップされます。単純なパケット フィルタは、送信元アドレス、宛先アドレス、およびポートが正しいかどうかはチェックできますが、パケット

シーケンスまたはフラグが正しいかどうかはチェックしません。また、フィルタはすべてのパケットをフィルタと照合してチェックするため、処理が低速になる場合があります。

（注） TCP ステート バイパス機能を使用すると、パケット フローをカスタマイズできます。

ただし、ASA のようなステートフル ファイアウォールは、パケットの次のようなステートについて検討します。

- 新規の接続かどうか。

  新規の接続の場合、ASA は、パケットをアクセス リストと照合してチェックする必要があり、これ以外の各種のタスクを実行してパケットの許可または拒否を決定する必要があります。このチェックを行うために、セッションの最初のパケットは「セッション管理パス」を通過しますが、トラフィックのタイプに応じて、「コントロール プレーン パス」も通過する場合があります。

  セッション管理パスで行われるタスクは次のとおりです。

  - アクセス リストとの照合チェック
  - ルート ルックアップ
  - NAT 変換（xlates）の割り当て
  - 「ファスト パス」でのセッションの確立

  ASA は、TCP トラフィックのファスト パスに転送フローとリバース フローを作成します。ASA は、高速パスも使用できるように、UDP、ICMP（ICMP インスペクションがイネーブルの場合）などのコネクションレス型プロトコルの接続状態の情報も作成するので、これらのプロトコルもファスト パスを使用できます。

  （注） SCTP などの他の IP プロトコルの場合、ASA はリバース パス フローを作成しません。そのため、これらの接続を参照する ICMP エラー パケットはドロップされます。

  レイヤ7インスペクションが必要なパケット（パケットのペイロードの検査または変更が必要）は、コントロール プレーン パスに渡されます。レイヤ 7 インスペクション エンジンは、2 つ以上のチャネルを持つプロトコルで必要です。2 つ以上のチャネルの 1 つは周知のポート番号を使用するデータ チャネルで、その他はセッションごとに異なるポート番号を使用するコントロール チャネルです。このようなプロトコルには、FTP、H.323、および SNMP があります。

- 確立済みの接続かどうか。

  接続がすでに確立されている場合は、ASA でパケットの再チェックを行う必要はありません。一致するパケットの大部分は、両方向で「ファースト」パスを通過できます。高速パスで行われるタスクは次のとおりです。

- IP チェックサム検証
- セッション ルックアップ
- TCP シーケンス番号のチェック
- 既存セッションに基づく NAT 変換
- レイヤ 3 ヘッダー調整およびレイヤ 4 ヘッダー調整

レイヤ7インスペクションを必要とするプロトコルに合致するデータ パケットも高速パスを通過できます。

確立済みセッション パケットの中には、セッション管理パスまたはコントロール プレーン パスを引き続き通過しなければならないものがあります。セッション管理パスを通過するパケットには、インスペクションまたはコンテンツ フィルタリングを必要とする HTTP パケットが含まれます。コントロール プレーン パスを通過するパケットには、レイヤ 7 インスペクションを必要とするプロトコルのコントロール パケットが含まれます。

VPN 機能の概要

VPN は、TCP/IP ネットワーク（インターネットなど）上のセキュアな接続で、プライベートな接続として表示されます。このセキュアな接続はトンネルと呼ばれます。ASA は、トンネリング プロトコルを使用して、セキュリティ パラメータのネゴシエート、トンネルの作成および管理、パケットのカプセル化、トンネルを通したパケットの送信または受信、パケットのカプセル化の解除を行います。ASA は、双方向トンネルのエンドポイントとして機能します。たとえば、プレーンパケットを受信してカプセル化し、それをトンネルのもう一方のエンドポイントに送信することができます。そのエンドポイントで、パケットはカプセル化を解除され、最終的な宛先に送信されます。また、セキュリティ アプライアンスは、カプセル化されたパケットを受信してカプセル化を解除し、それを最終的な宛先に送信することもできます。ASA は、これらの機能を実行するためにさまざまな標準プロトコルを起動します。

ASA は、次の機能を実行します。

- トンネルの確立
- トンネル パラメータのネゴシエーション
- ユーザの認証
- ユーザ アドレスの割り当て
- データの暗号化と復号化
- セキュリティ キーの管理
- トンネルを通したデータ転送の管理
- トンネル エンドポイントまたはルータとしての着信と発信のデータ転送の管理

ASA は、これらの機能を実行するためにさまざまな標準プロトコルを起動します。

セキュリティ コンテキストの概要

単一の ASA は、セキュリティ コンテキストと呼ばれる複数の仮想デバイスにパーティション化できます。各コンテキストは、独自のセキュリティ ポリシー、インターフェイス、および管理者を持つ独立したデバイスです。マルチ コンテキストは、複数のスタンドアロン デバイスを使用することに似ています。マルチ コンテキスト モードでは、ルーティング テーブル、ファイアウォール機能、IPS、管理など、さまざまな機能がサポートされています。ただし、サポートされていない機能もあります。詳細については、機能に関する各章を参照してください。

マルチ コンテキスト モードの場合、ASA には、セキュリティ ポリシー、インターフェイス、およびスタンドアロン デバイスで設定できるほとんどのオプションを識別するコンテキストごとのコンフィギュレーションが含まれます。システム管理者がコンテキストを追加および管理するには、コンテキストをシステム コンフィギュレーションに設定します。これが、シングル モード設定と同じく、スタートアップ コンフィギュレーションとなります。システム コンフィギュレーションは、ASA の基本設定を識別します。システム コンフィギュレーションには、ネットワーク インターフェイスやネットワーク設定は含まれません。その代わりに、ネットワーク リソースにアクセスする必要が生じたときに（サーバからコンテキストをダウンロードするなど）、システムは管理コンテキストとして指定されているコンテキストのいずれかを使用します。

管理コンテキストは、他のコンテキストとまったく同じです。ただし、ユーザが管理コンテキストにログインすると、システム管理者権限を持つので、システム コンテキストおよび他のすべてのコンテキストにアクセス可能になる点が異なります。

ASA クラスタリングの概要

ASA クラスタリングを利用すると、複数の ASA をグループ化して、1 つの論理デバイスにすることができます。クラスタは、単一デバイスのすべての利便性（管理、ネットワークへの統合）を備える一方で、複数デバイスによって高いスループットおよび冗長性を達成します。

すべてのコンフィギュレーション作業（ブートストラップ コンフィギュレーションを除く）は、マスター ユニット上でのみ実行します。コンフィギュレーションは、メンバ ユニットに複製されます。

特殊なサービスおよびレガシー サービス

一部のサービスのマニュアルは、主要な設定ガイドおよびオンライン ヘルプとは別の場所にあります。

特殊なサービスに関するガイド

特殊なサービスを利用して、たとえば、電話サービス（Unified Communications）用のセキュリティ プロキシを提供したり、ボットネット トラフィック フィルタリングを Cisco アップデート サーバのダイナミック データベースと組み合わせて提供したり、Cisco Web セキュリティ アプライアンス用の WCCP サービスを提供したりすることにより、ASA と他のシスコ製品の相互運用が可能になります。これらの特殊なサービスの一部については、別のガイドで説明されています。

- 『Cisco ASA Botnet Traffic Filter Guide』
- 『Cisco ASA NetFlow Implementation Guide』
- 『Cisco ASA Unified Communications Guide』
- 『Cisco ASA WCCP Traffic Redirection Guide』
- 『SNMP Version 3 Tools Implementation Guide』

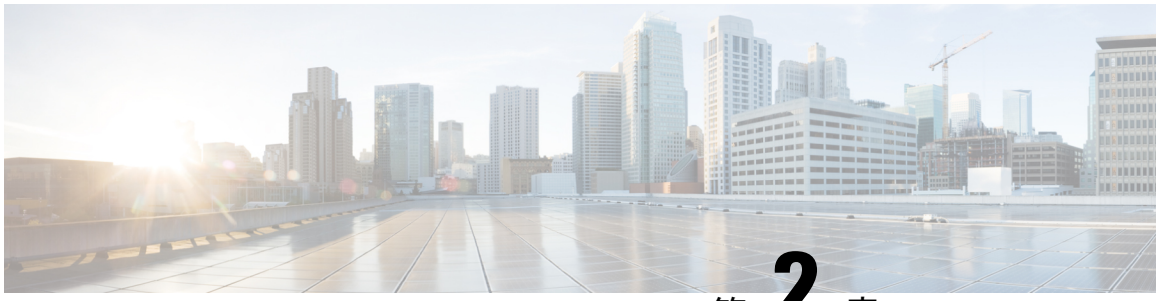
レガシー サービス ガイド

レガシー サービスは現在も ASA でサポートされていますが、より高度なサービスを代わりに使用できる場合があります。レガシー サービスについては別のガイドで説明されています。

『Cisco ASA Legacy Feature Guide』

このマニュアルの構成は、次のとおりです。

- RIP の設定
- ネットワーク アクセスの AAA 規則
- IP スプーフィングの防止などの保護ツールの使用（**ip verify reverse-path**）、フラグメント サイズの設定（**fragment**）、不要な接続のブロック（**shun**）、TCP オプションの設定（ASDM 用）、および基本 IPS をサポートする IP 監査の設定（**ip audit**）。
- フィルタリング サービスの設定



第 2 章

使用する前に

この章では、Cisco ASA の使用を開始する方法について説明します。

コマンドラインインターフェイス（CLI）のコンソールへのアクセス

初期設定を行うには、コンソール ポートから直接 CLI にアクセスします。その後、#unique_39 に従って Telnet または SSH を使用して、リモート アクセスを設定できます。システムがすでにマルチ コンテキスト モードで動作している場合は、コンソール ポートにアクセスするとシステムの実行スペースに入ります。

（注） ASAv のコンソール アクセスについては、ASAv のクイック スタート ガイドを参照してください。

アプライアンス コンソールへのアクセス

アプライアンス コンソールにアクセスするには、次の手順に従います。

手順

ステップ 1 付属のコンソール ケーブルを使用してコンピュータをコンソール ポートに接続します。ターミナル エミュレータを回線速度 9600 ボー、データ ビット 8、パリティなし、ストップ ビット 1、フロー制御なしに設定して、コンソールに接続します。

コンソール ケーブルの詳細については、ASA のハードウェア ガイドを参照してください。

ステップ 2 **Enter** キーを押して、次のプロンプトが表示されることを確認します。

```
ciscoasa>
```

このプロンプトは、ユーザ EXEC モードで作業していることを示します。ユーザ EXEC モードでは、基本コマンドのみを使用できます。

ステップ 3 特権 EXEC モードにアクセスします。

enable

パスワードを入力するように求められます。デフォルトではパスワードは空白に設定されているため、**Enter** キーを押して先に進みます。イネーブル パスワードを変更するには、ホスト名、ドメイン名、およびイネーブル パスワードと Telnet パスワードの設定 （583 ページ）を参照してください。

例：

```
ciscoasa> enable
Password:
ciscoasa#
```

設定以外のすべてのコマンドは、特権 EXEC モードで使用できます。特権 EXEC モードからコンフィギュレーション モードに入ることもできます。

特権モードを終了するには、**disable** コマンド、**exit** コマンド、または **quit** コマンドを入力します。

ステップ 4 グローバル コンフィギュレーション モードにアクセスします。

configure terminal

例：

```
ciscoasa# configure terminal
ciscoasa(config)#
```

グローバル コンフィギュレーション モードから ASA の設定を開始できます。グローバル コンフィギュレーション モードを終了するには、**exit** コマンド、**quit** コマンド、または **end** コマンドを入力します。

Firepower 9300 シャーシ 上の ASA コンソールへのアクセス

初期設定の場合、Firepower 9300 シャーシ スーパバイザに（コンソール ポートに、あるいは Telnet または SSH を使用してリモートで）接続してコマンドライン インターフェイスにアクセスし、ASA セキュリティ モジュールに接続します。

手順

ステップ 1 Firepower 9300 シャーシ スーパバイザ CLI（コンソールまたは SSH）に接続し、次に ASA にセッション接続します。

connect module *slot* **console**

初めてモジュールにアクセスするときは、FXOS モジュールの CLI にアクセスします。その後 ASA アプリケーションに接続する必要があります。

connect asa

例：

```
Firepower# connect module 1 console
Firepower-module1> connect asa

asa>
```

ステップ 2 最高の特権レベルである特権 EXEC モードにアクセスします。

enable

パスワードを入力するように求められます。デフォルトではパスワードは空白に設定されているため、**Enter** キーを押して先に進みます。イネーブル パスワードを変更するには、ホスト名、ドメイン名、およびイネーブル パスワードと Telnet パスワードの設定（583 ページ）を参照してください。

例：

```
asa> enable
Password:
asa#
```

設定以外のすべてのコマンドは、特権 EXEC モードで使用できます。特権 EXEC モードからコンフィギュレーション モードに入ることもできます。

特権モードを終了するには、**disable** コマンド、**exit** コマンド、または **quit** コマンドを入力します。

ステップ 3 グローバル コンフィギュレーション モードを開始します。

configure terminal

例：

```
asa# configure terminal
asa(config)#
```

グローバル コンフィギュレーション モードを終了するには、**disable**、**exit**、または **quit** コマンドを入力します。

ステップ 4 **Ctrl-a、d** と入力し、アプリケーション コンソールを終了して FXOS モジュール CLI に移動します。

トラブルシューティングのために FXOS モジュールの CLI を使用する場合があります。

ステップ 5 FXOS CLI のスーパバイザ レベルに戻ります。

a) ~ と入力

Telnet アプリケーションに切り替わります。

b) Telnet アプリケーションを終了するには、次を入力します。

telnet>**quit**

ASA サービス モジュール コンソールへのアクセス

初期設定の場合、スイッチに（コンソール ポートに、あるいは Telnet または SSH を使用してリモートで）接続してコマンドライン インターフェイス（CLI）にアクセスし、ASASM に接続します。ここでは、ASASM CLI にアクセスする方法について説明します。

接続方法について

スイッチ CLI から ASASM に接続するには、次の 2 つの方法が使用できます。

- 仮想コンソール接続：**service-module session** コマンドを使用して、ASASM への仮想コンソール接続を作成します。仮想コンソール接続には、実際のコンソール接続のすべての利点と制限があります。

  利点を次に示します。

  - 接続はリロード中も持続し、タイムアウトしません。
  - ASASM リロード中も接続を維持でき、スタートアップ メッセージを閲覧できます。
  - ASASM がイメージをロードできない場合、ROMMON にアクセスできます。
  - 初期パスワードの設定は必要ではありません。

  制限を次に示します。

  - 接続が低速です（9600 ボー）。
  - 一度にアクティブにできるコンソール接続は 1 つだけです。

- このコマンドは、Ctrl+Shift+6、x がターミナル サーバ プロンプトに戻るためのエスケープ シーケンスであるターミナル サーバとともに使用することはできません。**Ctrl+Shift+6**、**x** は、ASASM コンソールをエスケープして、スイッチ プロンプトに戻るためのシーケンスでもあります。したがって、この状況で ASASM を終了しようとすると、代わりにターミナル サーバ プロンプトに戻ります。スイッチにターミナル サーバを再接続した場合、ASASM コンソール セッションがアクティブのままです。スイッチ プロンプトを終了することはできません。コンソールをスイッチ プロンプトに戻すには、直接シリアル接続を使用する必要があります。この場合、Cisco IOS でターミナル サーバまたはスイッチ エスケープ文字を変更するか、または Telnet **session** コマンドを使用します。

（注） コンソール接続の永続性のため、ASASM を正しくログ アウトしないと、意図よりも長く接続が存在する可能性があります。他の人がログインする場合は、既存の接続を終了する必要があります。

- Telnet 接続：**session** コマンドを使用して、ASASM への Telnet 接続を作成します。

（注） 新しい ASASM に対してはこの方式を使用して接続できません。この方式では、ASASM 上での Telnet ログイン パスワードの設定が必要です（デフォルトのパスワードはありません）。**passwd** コマンドを使用してパスワードを設定した後に、この方式を使用できます。

利点を次に示します。

- ASASM への複数のセッションを同時に使用できます。
- Telnet セッションは、高速接続です。

制限を次に示します。

- Telnet セッションは、ASASM リロード時に終了し、タイムアウトします。
- ASASM が完全にロードするまで ASASM にはアクセスできません。したがって、ROMMON にアクセスできません。
- 最初に Telnet ログイン パスワードを設定する必要があります。デフォルトのパスワードはありません。

ASA サービス モジュールへのログイン

初期設定の場合、スイッチに（スイッチのコンソール ポートに、あるいは Telnet または SSH を使用してリモートで）接続してコマンドライン インターフェイスにアクセスし、ASASM に接続します。

システムがすでにマルチ コンテキスト モードで動作している場合は、スイッチ環境から ASASM にアクセスするとシステムの実行スペースに入ります。

その後は、Telnet または SSH を使用してリモート アクセスを ASASM に直接設定できます。

手順

ステップ 1 スイッチから、次のいずれかを実行します。

- 最初のアクセスで使用可能：スイッチ CLI からこのコマンドを入力し、ASASM にコンソール アクセスします。

  service-module session [**switch** {**1** | **2**}] **slot** *number*

  例：

  ```
  Router# service-module session slot 3
  ciscoasa>
  ```

  VSS 内のスイッチの場合、**switch** 引数を入力します。

  モジュールのスロット番号を表示するには、スイッチ プロンプトで **show module** コマンドを入力します。

  ユーザ EXEC モードにアクセスします。

- ログイン パスワードの設定後に使用可能：スイッチ CLI からこのコマンドを入力し、バックプレーンを介して ASASM に Telnet 接続します。

  session [**switch** {**1** | | **2**}] **slot** *number* **processor 1**

  ログイン パスワードの入力が求められます。

  ```
  ciscoasa passwd:
  ```

  例：

  ```
  Router# session slot 3 processor 1
  ciscoasa passwd: cisco
  ciscoasa>
  ```

  VSS 内のスイッチの場合、**switch** 引数を入力します。

  session *slot* **processor 0** コマンドは、他のサービス モジュールではサポートされていますが、ASASM ではサポートされていません。ASASM にはプロセッサ 0 がありません。

モジュールのスロット番号を表示するには、スイッチ プロンプトで **show module** コマンドを入力します。

ASADM へのログイン パスワードを入力します。**passwd** コマンドを使用してパスワードを設定します。デフォルトのパスワードはありません。

ユーザ EXEC モードにアクセスします。

ステップ 2 最高の特権レベルである特権 EXEC モードにアクセスします。

enable

パスワードを入力するように求められます。デフォルトではパスワードは空白に設定されているため、**Enter** キーを押して先に進みます。イネーブル パスワードを変更するには、ホスト名、ドメイン名、およびイネーブル パスワードと Telnet パスワードの設定 （583 ページ）を参照してください。

例：

```
ciscoasa> enable
Password:
ciscoasa#
```

設定以外のすべてのコマンドは、特権 EXEC モードで使用できます。特権 EXEC モードからコンフィギュレーション モードに入ることもできます。

特権モードを終了するには、**disable** コマンド、**exit** コマンド、または **quit** コマンドを入力します。

ステップ 3 グローバル コンフィギュレーション モードにアクセスします。

configure terminal

グローバル コンフィギュレーション モードを終了するには、**disable** コマンド、**exit** コマンド、または **quit** コマンドを入力します。

関連トピック

管理アクセスのガイドライン
ホスト名、ドメイン名、およびイネーブル パスワードと Telnet パスワードの設定 （583 ページ）

コンソール セッションのログアウト

ASASM からログアウトしない場合、コンソール接続は維持され、タイムアウトはありません。ASASM コンソール セッションを終了してスイッチの CLI にアクセスするには、次の手順を実行します。

意図せずに開いたままになっている可能性のある、別のユーザのアクティブな接続を終了するには、アクティブなコンソール接続の終了 （30 ページ）を参照してください。

手順

スイッチ CLI に戻るには、次を入力します。

Ctrl+Shift+6、x

スイッチ プロンプトに戻ります。

```
asasm# [Ctrl-Shift-6, x]
Router#
```

（注） 米国および英国キーボードの Shift+6 はキャレット記号（^）を出力します。別のキーボードを使用しており、単独の文字としてキャレット記号（^）を出力できない場合、一時的または永続的に、エスケープ文字を別の文字に変更できます。**terminal escape-character** *ascii_number* コマンド（このセッションで変更する）、または **default escape-character** *ascii_number* コマンド（永続的に変更する）を使用します。たとえば、現在のセッションのシーケンスを **Ctrl-w**、**x** に変更するには、**terminal escape-character 23** を入力します。

アクティブなコンソール接続の終了

コンソール接続の永続性のために、ASASM を正しくログアウトしないと、意図したよりも長い時間にわたって接続が存在する可能性があります。他の人がログインする場合は、既存の接続を終了する必要があります。

手順

ステップ 1 スイッチ CLI から、**show users** コマンドを使用して、接続されたユーザを表示します。コンソール ユーザは「con」と呼ばれます。ホスト アドレスは、127.0.0.*slot*0 と表示されます（*slot* はモジュールのスロット番号です）。

show users

たとえば、次のコマンド出力は、スロット 2 にあるモジュールのライン 0 のユーザ「con」を示しています。

```
Router# show users
Line       User       Host(s)              Idle       Location
*  0       con 0     127.0.0.20           00:00:02
```

ステップ 2 コンソール接続のあるラインをクリアするには、次のコマンドを入力します。

clear *line number*

次に例を示します。

```
Router# clear line 0
```

Telnet セッションのログアウト

Telnet セッションを終了してスイッチ CLI にアクセスするには、次の手順を実行します。

手順

スイッチ CLI に戻るには、ASASM 特権モードまたはユーザ EXEC モードから **exit** を入力します。コンフィギュレーション モードに入っている場合は、Telnet セッションが終了するまで繰り返し **exit** を入力します。

スイッチ プロンプトに戻ります。

```
asasm# exit
Router#
```

（注） 代わりに、エスケープ シーケンス Ctrl+Shift+6、x を使用して、Telnet セッションをエスケープすることができます。このエスケープ シーケンスを使用すると、スイッチ プロンプトで Enter キーを押すことで、Telnet セッションを再開できます。スイッチから Telnet セッションを切断するには、スイッチ CLI で **disconnect** を入力します。セッションを切断しない場合、ASASM 設定に従って最終的にタイムアウトします。

ソフトウェア モジュール コンソールへのアクセス

ASA 5506-X に ASA FirePOWER などのソフトウェア モジュールをインストールしている場合、モジュール コンソールへのセッションを実行できます。

（注） **session** コマンドを使用して ASA バックプレーンを介してハードウェア モジュール CLI にアクセスすることはできません。

手順

ASA CLI から、モジュールへのセッションを実行します。

session {**sfr** | **cxsc** | **ips**} **console**

例：

```
ciscoasa# session sfr console
Opening console session with module sfr.
Connected to module sfr. Escape character sequence is 'CTRL-^X'.

Cisco ASA SFR Boot Image 5.3.1
asasfr login: admin
Password: Admin123
```

ASA 5506W-X ワイヤレス アクセス ポイント コンソールへのアクセス

ワイヤレス アクセス ポイント コンソールにアクセスするには、次の手順を実行します。

手順

ステップ 1 ASA CLI から、アクセス ポイントへのセッションを実行します。

session wlan console

例：

```
ciscoasa# session wlan console
opening console session with module wlan
connected to module wlan. Escape character sequence is 'CTRL-^X'

ap>
```

ステップ 2 アクセス ポイント CLI については、『Cisco IOS Configuration Guide for Autonomous Aironet Access Points』[英語] を参照してください。

ASDM アクセスの設定

ここでは、デフォルト コンフィギュレーションで ASDM にアクセスする方法、およびデフォルト設定がない場合にアクセスを設定する方法について説明します。

ASDM アクセス（アプライアンス、ASAv）に対する工場出荷時のデフォルト コンフィギュレーションの使用

工場出荷時のデフォルト コンフィギュレーションでは、ASDM 接続はデフォルトのネットワーク設定で事前設定されています。

手順

次のインターフェイスおよびネットワーク設定を使用して ASDM に接続します。

- 管理インターフェイスは、ご使用のモデルによって異なります。
  - Firepower 9300：展開時に定義された管理タイプインターフェイスと IP アドレス。管理ホストは任意のネットワークからアクセスできます。
  - ASA 5506-X、ASA 5508-X および ASA 5516-X：内部 GigabitEthernet 1/2（192.168.1.1）および ASA 5506W-X、Wi-Fi GigabitEthernet 1/9（192.168.10.1）用。内部ホストは 192.168.1.0/24 ネットワークに限定され、Wi-Fi ホストは 192.168.10.0/24 に限定されます。
  - ASA 5512-X 以降：管理 0/0（192.168.1.1）。管理ホストは 192.168.1.0/24 ネットワークに限定されます。
  - ASA：管理 0/0（導入時に設定）。管理ホストは管理ネットワークに限定されます。
  - ISA 3000：管理 1/1（192.168.1.1）。管理ホストは 192.168.1.0/24 ネットワークに限定されます。

（注） マルチ コンテキスト モードに変更すると、上記のネットワーク設定を使用して管理コンテキストから ASDM にアクセスできるようになります。

関連トピック

工場出荷時のデフォルト設定 （40 ページ）
マルチ コンテキスト モードの有効化またはディセーブル化 （215 ページ）
ASDM の起動 （38 ページ）

ASDM アクセスのカスタマイズ

この手順は、ASA サービス モジュールを除くすべてのモデルに適用されます。

次の条件に *1* つ以上当てはまる場合は、この手順を使用します。

- 工場出荷時のデフォルト コンフィギュレーションがない。
- 管理 IP アドレスを変更したい。
- トランスペアレント ファイアウォール モードに変更したい。
- マルチ コンテキスト モードに変更したい。

シングル ルーテッド モードの場合、ASDM に迅速かつ容易にアクセスするために、独自の管理IPアドレスを設定できるオプションを備えた工場出荷時のデフォルトコンフィギュレーションを適用することを推奨します。この項に記載されている手順は、特別なニーズ（トランスペ

アレント モードやマルチ コンテキスト モードの設定など）がある場合や、他の設定を維持する必要がある場合にのみ使用してください。

（注） ASAv の場合、導入時にトランスペアレント モードを設定できるため、この手順は、設定をクリアする必要がある場合など、導入後に特に役立ちます。

手順

ステップ 1 コンソール ポートで CLI にアクセスします。

ステップ 2 （オプション）トランスペアレント ファイアウォール モードをイネーブルにします。

このコマンドは、設定をクリアします。

firewall transparent

ステップ 3 管理インターフェイスを設定します。

```
interface interface_id
   nameif name
   security-level level
   no shutdown
   ip address ip_address mask
```

例：

```
ciscoasa(config)# interface management 0/0
ciscoasa(config-if)# nameif management
ciscoasa(config-if)# security-level 100
ciscoasa(config-if)# no shutdown
ciscoasa(config-if)# ip address 192.168.1.1 255.255.255.0
```

security-level は、1 ～ 100 の数字です。100 が最も安全です。

ステップ 4 （直接接続された管理ホスト用）管理ネットワークの DHCP プールを設定します。

```
dhcpd address ip_address-ip_address interface_name
dhcpd enable interface_name
```

例：

```
ciscoasa(config)# dhcpd address 192.168.1.2-192.168.1.254 management
ciscoasa(config)# dhcpd enable management
```

その範囲にインターフェイス アドレスが含まれていないことを確認します。

ステップ 5 （リモート管理ホスト用）管理ホストへのルートを設定します。

route *management_ifc management_host_ip mask gateway_ip* **1**

例：

```
ciscoasa(config)# route management 10.1.1.0 255.255.255.0 192.168.1.50 1
```

ステップ 6 ASDM の HTTP サーバをイネーブルにします。

http server enable

ステップ 7 管理ホストの ASDM へのアクセスを許可します。

http *ip_address mask interface_name*

例：

```
ciscoasa(config)# http 192.168.1.0 255.255.255.0 management
```

ステップ 8 設定を保存します。

write memory

ステップ 9 （オプション）モードをマルチ モードに設定します。

mode multiple

プロンプトが表示されたら、既存の設定を管理コンテキストに変換することを承認します。ASA をリロードするよう求められます。

例

次の設定では、ファイアウォール モードがトランスペアレント モードに変換され、Management 0/0 インターフェイスが設定され、管理ホストに対して ASDM がイネーブルにされます。

```
firewall transparent
interface management 0/0

ip address 192.168.1.1 255.255.255.0
nameif management
security-level 100
no shutdown

dhcpd address 192.168.1.2-192.168.1.254 management
dhcpd enable management
http server enable
http 192.168.1.0 255.255.255.0 management
```

関連トピック

工場出荷時のデフォルト設定の復元 （41 ページ）
ファイアウォール モードの設定 （184 ページ）
アプライアンス コンソールへのアクセス （23 ページ）

ASDM の起動 （38 ページ）

ASA サービス モジュールの ASDM アクセスの設定

ASASM には物理インターフェイスがないため、ASDM アクセスが事前設定されていません。ASASM の CLI を使用して ASDM アクセスを設定する必要があります。ASDM アクセス用に ASASM を設定するには、次の手順を実行します。

始める前に

ASASM のクイック スタート ガイドに従って、ASASM に VLAN インターフェイスを割り当てます。

手順

ステップ 1 ASASM に接続し、グローバル コンフィギュレーション モードにアクセスします。

ステップ 2 （オプション）トランスペアレント ファイアウォール モードをイネーブルにします。

firewall transparent

このコマンドは、設定をクリアします。

ステップ 3 ご使用のモードに応じて、次のいずれかの操作を行って管理インターフェイスを設定します。

- ルーテッド モード：インターフェイスをルーテッド モードで設定します。

```
interface vlan number
   ip address ip_address [mask]
   nameif name
   security-level level
```

例：

```
ciscoasa(config)# interface vlan 1
ciscoasa(config-if)# ip address 192.168.1.1 255.255.255.0
ciscoasa(config-if)# nameif inside
ciscoasa(config-if)# security-level 100
```

security-level は、1 ～ 100 の数字です。100 が最も安全です。

- トランスペアレント モード：ブリッジ仮想インターフェイスを設定し、ブリッジ グループに管理 VLAN を割り当てます。

```
interface bvi number
   ip address ip_address [mask]

interface vlan number
   bridge-group bvi_number
   nameif name
   security-level level
```

例：

```
ciscoasa(config)# interface bvi 1
ciscoasa(config-if)# ip address 192.168.1.1 255.255.255.0

ciscoasa(config)# interface vlan 1
ciscoasa(config-if)# bridge-group 1
ciscoasa(config-if)# nameif inside
ciscoasa(config-if)# security-level 100
```

security-level は、1 ～ 100 の数字です。100 が最も安全です。

ステップ 4 （直接接続された管理ホスト用）管理インターフェイス ネットワーク上の管理ホストの DHCP をイネーブルにします。

dhcpd address *ip_address-ip_address interface_name*
dhcpd enable *interface_name*

例：

```
ciscoasa(config)# dhcpd address 192.168.1.2-192.168.1.254 inside
ciscoasa(config)# dhcpd enable inside
```

この範囲内には管理アドレスを含めないでください。

ステップ 5 （リモート管理ホスト用）管理ホストへのルートを設定します。

route *management_ifc management_host_ip mask gateway_ip* **1**

例：

```
ciscoasa(config)# route management 10.1.1.0 255.255.255.0 192.168.1.50
```

ステップ 6 ASDM の HTTP サーバをイネーブルにします。

http server enable

ステップ 7 管理ホストの ASDM へのアクセスを許可します。

http *ip_address mask interface_name*

例：

```
ciscoasa(config)# http 192.168.1.0 255.255.255.0 management
```

ステップ 8 設定を保存します。

write memory

ステップ 9 （オプション）モードをマルチ モードに設定します。

mode multiple

プロンプトが表示されたら、既存の設定を管理コンテキストに変換することを承認します。ASASM をリロードするよう求められます。

例

次のルーテッド モードの設定では、VLAN 1 のインターフェイスを設定し、管理ホストの ASDM のイネーブルにします。

```
interface vlan 1
nameif inside
ip address 192.168.1.1 255.255.255.0
security-level 100

dhcpd address 192.168.1.3-192.168.1.254 inside
dhcpd enable inside
http server enable
http 192.168.1.0 255.255.255.0 inside
```

次の設定では、ファイアウォール モードをトランスペアレント モードに変換し、VLAN 1 インターフェイスを設定して BVI 1 に割り当てた後、管理ホストの ASDM をイネーブルにします。

```
firewall transparent
interface bvi 1

ip address 192.168.1.1 255.255.255.0
interface vlan 1
bridge-group 1
nameif inside
security-level 100

dhcpd address 192.168.1.3-192.168.1.254 inside
dhcpd enable inside
http server enable
http 192.168.1.0 255.255.255.0 inside
```

関連トピック

ASA サービス モジュール コンソールへのアクセス （26 ページ）
接続方法について （26 ページ）
コンソール セッションのログアウト （29 ページ）
アクティブなコンソール接続の終了 （30 ページ）
Telnet セッションのログアウト （31 ページ）
ファイアウォール モードの設定 （184 ページ）

ASDM の起動

ASDM は、次の 2 つの方法で起動できます。

- ASDM-IDM ランチャ：ランチャは、ASA から Web ブラウザを使用してダウンロードされるアプリケーションです。これを使用すると、任意の ASA IP アドレスに接続できます。他の ASA に接続する場合、ランチャを再度ダウンロードする必要はありません。
- Java Web Start：管理する ASA ごとに Web ブラウザで接続して、Java Web Start アプリケーションを保存または起動する必要があります。任意でコンピュータにショートカットを保存できます。ただし、ASA IP アドレスごとにショートカットを分ける必要があります。

（注） Web Start を使用する場合は、Java キャッシュをクリアしてください。クリアしない場合、Hostscan などのログイン前ポリシーに対する変更が失われる可能性があります。この問題は、ランチャを使用している場合には発生しません。

ASDM では、管理のために別の ASA IP アドレスを選択できます。ランチャと Java Web Start の機能の違いは、主に、ユーザが最初にどのように ASA に接続し、ASDM を起動するかにあります。

ここでは、まず ASDM に接続する方法について説明します。次にランチャまたは Java Web Start を使用して ASDM を起動する方法について説明します。

ASDM はローカルの \Users\<user_id>\.asdm ディレクトリ内にキャッシュ、ログ、および設定などのファイルを保存し、Temp ディレクトリ内にも AnyConnect プロファイルなどのファイルを保存します。

手順

ステップ 1 ASDM クライアントとして指定したコンピュータで次の URL を入力します。

https://*asa_ip_address*/**admin**

次のボタンを持つ ASDM 起動ページが表示されます。

- **Install ASDM Launcher and Run ASDM**
- **Run ASDM**
- **Run Startup Wizard**

ステップ 2 ランチャをダウンロードするには、次の手順を実行します。

a) [Install ASDM Launcher and Run ASDM] をクリックします。

b) ユーザ名とパスワードのフィールドを空のままにし（新規インストールの場合）、[OK] をクリックします。HTTPS 認証が設定されていない場合は、ユーザ名および**イネーブル** パスワード（デフォルトで空白）を入力しないで ASDM にアクセスできます。**注**：HTTPS 認証をイネーブルにした場合、ユーザ名と関連付けられたパスワードを入力します。認証が有効でない場合でも、ログイン画面で（ユーザ名をブランクのままにしないで）ユーザ名とパスワードを入力すると、ASDM によってローカルデータベースで一致がチェックされます。

c) インストーラをコンピュータに保存して、インストーラを起動します。インストールが完了すると、ASDM-IDM ランチャが自動的に開きます。
d) 管理 IP アドレス、および同じユーザ名とパスワード（新規インストールの場合は空白）を入力し、[OK] をクリックします。

ステップ 3 Java Web Start を使用するには：

a) [Run ASDM] または [Run Startup Wizard] をクリックします。
b) プロンプトが表示されたら、ショートカットをコンピュータに保存します。オプションで、アプリケーションを保存せずに開くこともできます。
c) ショートカットから Java Web Start を起動します。
d) 表示されたダイアログボックスに従って、任意の証明書を受け入れます。Cisco ASDM-IDM Launcher が表示されます。
e) ユーザ名とパスワードのフィールドを空のままにし（新規インストールの場合）、[OK] をクリックします。HTTPS 認証が設定されていない場合は、ユーザ名および**イネーブル** パスワード（デフォルトで空白）を入力しないで ASDM にアクセスできます。**注**：HTTPS 認証をイネーブルにした場合、ユーザ名と関連付けられたパスワードを入力します。認証が有効でない場合でも、ログイン画面で（ユーザ名をブランクのままにしないで）ユーザ名とパスワードを入力すると、ASDM によってローカルデータベースで一致がチェックされます。

工場出荷時のデフォルト設定

工場出荷時のデフォルト設定とは、シスコが新しい ASA に適用したコンフィギュレーションです。

- ASA 5506-X、5508-X および 5516-X：工場出荷時のデフォルト設定により、機能内部/外部設定が有効になります。ASA は、内部インターフェイスから ASDM を使用して管理できます。
- ASA 5512-X ～ ASA 5585-X：管理用のインターフェイスは工場出荷時のデフォルト設定によって設定されるため、ASDM を使用してこのインターフェイスに接続して設定を完了できます。
- Firepower 9300 シャーシ：ASA のスタンドアロンまたはクラスタを展開する場合、管理用のインターフェイスは工場出荷時のデフォルト設定によって設定されるため、ASDM を使用してこのインターフェイスに接続して設定を完了できます。
- ASAv：ハイパーバイザによっては、導入の一環として、管理用のインターフェイス導入設定（初期の仮想導入設定）によって設定されるため、ASDM を使用してこのインターフェイスに接続して設定を完了できます。フェールオーバー IP アドレスも設定できます。また、必要に応じて、「工場出荷時のデフォルト」コンフィギュレーションを適用することもできます。

- ASASM：デフォルト設定はありません。コンフィギュレーションを開始するには、ASA サービス モジュール コンソールへのアクセス （26 ページ）を参照してください。
- ISA 3000：工場出荷時のデフォルト設定は、同じネットワーク上のすべての内部および外部インターフェイスを使用した、ほぼ完全なトランスペアレント ファイアウォール モード設定です。ASDM を使用して管理インターフェイスに接続し、ネットワークの IP アドレスを設定できます。ハードウェアバイパスは2つのインターフェイスペアに対して有効になっており、すべてのトラフィックはインラインタップモニタ専用モードで ASA FirePOWER モジュールに送信されます。このモードでは、モニタリング目的でのみトラフィックの重複ストリームが ASA Firepower モジュールに送信されます。

アプライアンス および Firepower 9300 シャーシの場合、工場出荷時のデフォルト設定は、ルーテッドファイアウォールモードとシングルコンテキストモードのみで使用できます。ASAvの場合、導入時にトランスペアレントモードまたはルーテッドモードを選択できます。

（注） イメージ ファイルと（隠された）デフォルト コンフィギュレーションに加え、log/、crypto_archive/、および coredumpinfo/coredump.cfg がフラッシュ メモリ内の標準のフォルダとファイルです。フラッシュ メモリ内で、これらのファイルの日付は、イメージ ファイルの日付と一致しない場合があります。これらのファイルは、トラブルシューティングに役立ちますが、障害が発生したことを示すわけではありません。

工場出荷時のデフォルト設定の復元

この項では、工場出荷時のデフォルトコンフィギュレーションを復元する方法について説明します。ASAv では、この手順を実行することで導入設定が消去され、ASA 5525-X の場合と同じ工場出荷時のデフォルト設定が適用されます。

（注） ASASM で出荷時のデフォルト コンフィギュレーションを復元すると、設定は消去されます。工場出荷時のデフォルト コンフィギュレーションはありません。

Firepower 9300 では、工場出荷時のデフォルト設定を復元すると単に設定が消去されるだけです。デフォルト設定を復元するには、スーパバイザから ASA をもう一度展開する必要があります。

始める前に

この機能は、ルーテッド ファイアウォール モードでのみ使用できます。トランスペアレントモードの場合、インターフェイスの IP アドレスがサポートされません。さらに、この機能はシングル コンテキスト モードでのみ使用できます。コンフィギュレーションがクリアされた ASA には、この機能を使用して自動的に設定する定義済みコンテキストがありません。

手順

ステップ 1 工場出荷時のデフォルト コンフィギュレーションを復元します。

configure factory-default [*ip_address* [*mask*]]

例：

```
ciscoasa(config)# configure factory-default 10.1.1.1 255.255.255.0
```

ip_address を指定する場合は、デフォルトの IP アドレスを使用する代わりに、お使いのモデルに応じて、内部または管理インターフェイスの IP アドレスを設定します。*ip_address* オプションで設定されているインターフェイスについては、次のモデルのガイドラインを参照してください。

- Firepower 9300：効果はありません。
- ASAv：**管理**インターフェイスの IP アドレスを設定します。
- ASA 5506-X：**内部**インターフェイスの IP アドレスを設定します。
- ASA 5508-X および 5516-X：**内部**インターフェイスの IP アドレスを設定します。
- ASA 5512-X、5515-X、5525-X、5545-X、5555-X：**管理**インターフェイスの IP アドレスを設定します。
- ASA 5585-X：**管理**インターフェイスの IP アドレスを設定します。
- ISA 3000：**管理**インターフェイスの IP アドレスを設定します。
- ASASM：効果はありません。

http コマンドでは、ユーザが指定するサブネットが使用されます。同様に、**dhcpd address** コマンドの範囲は、指定したサブネット内のアドレスで構成されます。

Firepower 2100 の場合：このモデルでは、**boot system** コマンドは使用されません。パッケージは FXOS によって管理されます。

その他すべてのモデルの場合：このコマンドは、残りの設定とともに **boot system** コマンドをクリアします（存在する場合）。**boot system** コマンドを使用すると、特定のイメージから起動できます。出荷時の設定に戻した後、次回 ASA をリロードすると、内部フラッシュ メモリの最初のイメージからブートします。内部フラッシュ メモリにイメージがない場合、ASA はブートしません。

ステップ 2 デフォルト コンフィギュレーションをフラッシュ メモリに保存します。

write memory

このコマンドでは、事前に **boot** config コマンドを設定して、別の場所を設定していた場合でも、実行コンフィギュレーションはスタートアップ コンフィギュレーションのデフォルトの場所に保存されます。コンフィギュレーションがクリアされると、このパスもクリアされます。

ASAv 導入設定の復元

この項では、ASAv の導入（第 0 日）設定を復元する方法について説明します。

手順

ステップ 1 フェールオーバーを行うために、スタンバイ装置の電源を切ります。

スタンバイ ユニットがアクティブになることを防ぐために、電源をオフにする必要があります。電源を入れたままにした場合、アクティブ装置の設定を消去すると、スタンバイ装置がアクティブになります。以前のアクティブ ユニットをリロードし、フェールオーバー リンクを介して再接続すると、古い設定は新しいアクティブ ユニットから同期し、必要な導入コンフィギュレーションが消去されます。

ステップ 2 リロード後に導入設定を復元します。フェールオーバーを行うために、アクティブ装置で次のコマンドを入力します。

write erase

（注） ASAv が現在の実行イメージをブートするため、元のブート イメージには戻りません。元のブート イメージを使用するには、**boot image** コマンドを参照してください。

コンフィギュレーションは保存しないでください。

ステップ 3 ASAv をリロードし、導入設定をロードします。

reload

ステップ 4 フェールオーバーを行うために、スタンバイ装置の電源を投入します。

アクティブ装置のリロード後、スタンバイ装置の電源を投入します。導入設定がスタンバイ装置と同期されます。

ASA 5506-X、5508-X、および 5516-X のデフォルト設定

ASA 5506-X シリーズ、5508-X、および 5516-X の工場出荷時のデフォルト設定は、次のとおりです。

- 内部 --> 外部へのトラフィック フロー：GigabitEthernet 1/1（外部）、GigabitEthernet 1/2（内部）

- DHCP の外部 IP アドレス、内部 IP アドレス：192.168.1.1
- （ASA 5506W-X）WiFi<--> 内部のトラフィック フロー、WiFi --> 外部へのトラフィック フロー：GigabitEthernet 1/9（WiFi）
- （ASA 5506W-X）WiFi の IP アドレス：192.168.10.1
- 内部および WiFi 上のクライアントに対する DHCP。アクセス ポイント自体とそのすべてのクライアントが ASA を DHCP サーバとして使用します。
- 管理 1/1 インターフェイスが稼働しているが、そうでない場合は未設定。ASA FirePOWER モジュールは、このインターフェイスを使用して ASA 内部ネットワークに接続し、内部インターフェイスをインターネットへのゲートウェイとして使用できます。
- ASDM アクセス：内部ホストおよび WiFi ホストに許可されます。
- NAT：内部、WiFi、および管理から外部へのすべてのトラフィックのインターフェイス PAT。

このコンフィギュレーションは次のコマンドで構成されています。

```
interface Management1/1
  management-only
  no nameif
  no security-level
  no ip address
  no shutdown
interface GigabitEthernet1/1
  nameif outside
  security-level 0
  ip address dhcp setroute
  no shutdown
interface GigabitEthernet1/2
  nameif inside
  security-level 100
  ip address 192.168.1.1 255.255.255.0
  no shutdown
!
object network obj_any
  subnet 0.0.0.0 0.0.0.0
  nat (any,outside) dynamic interface
!
http server enable
http 192.168.1.0 255.255.255.0 inside
!
dhcpd auto_config outside
dhcpd address 192.168.1.5-192.168.1.254 inside
dhcpd enable inside
!
logging asdm informational
```

ASA 5506W-X の場合は、次のコマンドも含まれます。

```
same-security-traffic permit inter-interface
!
interface GigabitEthernet 1/9
  security-level 100
  nameif wifi
```

```
  ip address 192.168.10.1 255.255.255.0
  no shutdown
!
http 192.168.10.0 255.255.255.0 wifi
!
dhcpd address 192.168.10.2-192.168.10.254 wifi
dhcpd enable wifi
```

ASA 5512-X ～ ASA 5585-X デフォルト設定

ASA 5512-X ～ ASA 5585-X の工場出荷時のデフォルト設定は、次のとおりです。

- 管理インターフェイス：Management 0/0（管理）。
- IP アドレス：管理アドレスは 192.168.1.1/24 です。
- DHCP サーバ：管理ホストでは DHCP サーバがイネーブルにされているため、管理インターフェイスに接続するコンピュータには、192.168.1.2 ～ 192.168.1.254 の間のアドレスが割り当てられます。
- ASDM アクセス：管理ホストに許可されます。

このコンフィギュレーションは次のコマンドで構成されています。

```
interface management 0/0
  ip address 192.168.1.1 255.255.255.0
  nameif management
  security-level 100
  no shutdown
!
asdm logging informational
asdm history enable
!
http server enable
http 192.168.1.0 255.255.255.0 management
!
dhcpd address 192.168.1.2-192.168.1.254 management
dhcpd enable management
```

Firepower 9300 シャーシ デフォルト設定

Firepower 9300 シャーシ 上に ASA を展開した場合、ASDM を使用して管理インターフェイスへの接続が可能になる多くのパラメータを事前設定できます。一般的な構成には次の設定があります。

- 管理インターフェイス：
  - Firepower 9300 シャーシ スーパバイザ上で定義された任意の管理タイプ インターフェイス
  - 名前は「management」
  - 任意の IP アドレス

- セキュリティ レベル 0
- 管理専用

- 管理インターフェイス内のデフォルト ルート
- ASDM アクセス：すべてのホストが許可されます。

スタンドアロン ユニットの設定は、次のコマンドで構成されます。クラスタ ユニットの追加の設定については、ASA クラスタの作成 （428 ページ） を参照してください。

```
interface <management_ifc>
  management-only
  ip address <ip_address> <mask>
  ipv6 address <ipv6_address>
  ipv6 enable
  nameif management
  security-level 0
  no shutdown
!
http server enable
http 0.0.0.0 0.0.0.0 management
http ::/0 management
!
route management 0.0.0.0 0.0.0.0 <gateway_ip> 1
ipv6 route management ::/0 <gateway_ipv6>
```

ISA 3000 のデフォルト設定

ISA 3000 の工場出荷時のデフォルト設定は、次のとおりです。

- トランスペアレント ファイアウォール モード：トランスペアレント ファイアウォールは、「Bump In The Wire」または「ステルス ファイアウォール」のように動作するレイヤ 2 ファイアウォールであり、接続されたデバイスへのルータ ホップとしては認識されません。
- 1 ブリッジ仮想インターフェイス：すべてのメンバー インターフェイスは同じネットワーク内に存在しています（**IP アドレスは事前設定されていません。ネットワークと一致するように設定する必要があります**）：GigabitEthernet 1/1 （outside1）、GigabitEthernet 1/2（inside1）、GigabitEthernet 1/3（outside2）、GigabitEthernet 1/4（inside2）
- すべての内部および外部インターフェイスは相互通信できます。
- 管理 1/1インターフェイス：ASDM アクセスの 192.168.1.1/24。
- 管理上のクライアントに対する DHCP。
- ASDM アクセス：管理ホストに許可されます。
- ハードウェア バイパスは、次のインターフェイス ペアで有効になっています。GigabitEthernet 1/1 および 1/2。GigabitEthernet 1/3 および 1/4

（注） ISA 3000 への電源が切断され、ハードウェア バイパス モードに移行すると、通信できるのは上記のインターフェイス ペアのみになります。inside1 と inside2 および outside1 と outside2 は通信できなくなります。これらのインターフェイス間の既存の接続がすべて失われます。電源が再投入されると、ASA がフローを引き継ぐため、接続が短時間中断されます。

- ASA Firepower モジュール：すべてのトラフィックが、Inline Tap Monitor-Only モードのモジュールに送信されます。このモードでは、モニタリング目的でのみトラフィックの重複ストリームが ASA Firepower モジュールに送信されます。

このコンフィギュレーションは次のコマンドで構成されています。

```
firewall transparent

interface GigabitEthernet1/1
  bridge-group 1
  nameif outside1
  security-level 0
  no shutdown
interface GigabitEthernet1/2
  bridge-group 1
  nameif inside1
  security-level 100
  no shutdown
interface GigabitEthernet1/3
  bridge-group 1
  nameif outside2
  security-level 0
  no shutdown
interface GigabitEthernet1/4
  bridge-group 1
  nameif inside2
  security-level 100
  no shutdown
interface Management1/1
  management-only
  no shutdown
  nameif management
  security-level 100
  ip address 192.168.1.1 255.255.255.0
interface BVI1
  no ip address

access-list allowAll extended permit ip any any
access-group allowAll in interface outside1
access-group allowAll in interface outside2

same-security-traffic permit inter-interface

hardware-bypass GigabitEthernet 1/1-1/2
hardware-bypass GigabitEthernet 1/3-1/4

http server enable
http 192.168.1.0 255.255.255.0 management
```

```
dhcpd address 192.168.1.5-192.168.1.254 management
dhcpd enable management


access-list sfrAccessList extended permit ip any any
class-map sfrclass
  match access-list sfrAccessList
policy-map global_policy
  class sfrclass
  sfr fail-open monitor-only
service-policy global_policy global
```

ASAv 導入設定

ASAv 上に ASA を展開した場合、ASDM を使用して管理 0/0 インターフェイスへの接続が可能になる多くのパラメータを前もって設定できます。一般的な構成には次の設定があります。

- ルーテッド ファイアウォール モードまたはトランスペアレント ファイアウォール モード
- Management 0/0 インターフェイス：
  - 名前は「management」
  - IP アドレスまたは DHCP
  - セキュリティ レベル 0
  - 管理専用
- 管理ホスト IP アドレスのスタティック ルート（管理サブネット上にない場合）
- HTTP サーバの有効または無効
- 管理ホスト IP アドレス用の HTTP アクセス
- （オプション）GigabitEthernet 0/8 用のフェールオーバー リンク IP アドレス、Management0/0 のスタンバイ IP アドレス
- DNS サーバ
- スマート ライセンス ID トークン
- スマート ライセンスのスループット レベルおよび標準機能ティア
- （オプション）Smart Call Home HTTP プロキシ URL およびポート
- （オプション）SSH 管理設定：
  - クライアント IP アドレス
  - ローカル ユーザ名とパスワード
  - ローカル データベースを使用する SSH に必要な認証
- （オプション）REST API の有効または無効

（注） Cisco 認証局に正常に登録するには、ASAv をインターネット アクセスが必要です。インターネットアクセスを実行して正常にライセンス登録するには、導入後に追加の設定が必要になることがあります。

スタンドアロン ユニットについては、次の設定例を参照してください。

```
interface Management0/0
  nameif management
  security-level 0
  ip address ip_address
  management-only
  no shutdown
http server enable
http managemment_host_IP mask management
route management management_host_IP mask gateway_ip 1
dns server-group DefaultDNS
  name-server ip_address
call-home
  http-proxy ip_address port port
license smart
  feature tier standard
  throughput level {100M | 1G | 2G}
  license smart register idtoken id_token
aaa authentication ssh console LOCAL
username username password password
ssh source_IP_address mask management
rest-api image boot:/path
rest-api agent
```

フェールオーバー ペアのプライマリ ユニットについては、次の設定例を参照してください。

```
nameif management
  security-level 0
  ip address ip_address standby standby_ip
  management-only
  no shutdown
route management management_host_IP mask gateway_ip 1
http server enable
http managemment_host_IP mask management
dns server-group DefaultDNS
  name-server ip_address
call-home
  http-proxy ip_address port port
license smart
  feature tier standard
  throughput level {100M | 1G | 2G}
  license smart register idtoken id_token
aaa authentication ssh console LOCAL
username username password password
ssh source_IP_address mask management
rest-api image boot:/path
rest-api agent
failover
failover lan unit primary
failover lan interface fover gigabitethernet0/8
```

```
failover link fover gigabitethernet0/8
failover interface ip fover primary_ip mask standby standby_ip
```

コンフィギュレーション作業

この項では、コンフィギュレーションを処理する方法について説明します。ASAは、スタートアップ コンフィギュレーションと呼ばれるコンフィギュレーションをテキスト ファイルからロードします。このファイルは、デフォルトでは隠しファイルとして内部フラッシュ メモリに常駐しています。ただし、ユーザはスタートアップ コンフィギュレーションに異なるパスを指定することができます

コマンドを入力すると、メモリ上の実行コンフィギュレーションに対してだけ変更が適用されます。変更内容をリブート後も維持するには、実行コンフィギュレーションを手動でスタートアップ コンフィギュレーションに保存する必要があります。

この項で説明する内容は、特に指定がない限り、シングル モードとマルチ モードの両セキュリティ コンテキストに適用されます。

コンフィギュレーションの変更の保存

この項では、コンフィギュレーションを保存する方法について説明します。

シングル コンテキスト モードでのコンフィギュレーションの変更の保存

実行コンフィギュレーションをスタートアップ コンフィギュレーションに保存するには、次の手順を実行します。

手順

実行コンフィギュレーションをスタートアップ コンフィギュレーションに保存します。

write memory

（注） **copy running-config startup-config** コマンドは、**write memory** コマンドに相当します。

マルチ コンテキスト モードでのコンフィギュレーションの変更の保存

各コンテキスト（およびシステム）コンフィギュレーションを個別に保存することも、すべてのコンテキスト コンフィギュレーションを同時に保存することもできます。

各コンテキストとシステムの個別保存

システムまたはコンテキストのコンフィギュレーションを保存するには、次の手順を使用します。

手順

コンテキストまたはシステム内から、実行コンフィギュレーションをスタートアップ コンフィギュレーションに保存します。

write memory

マルチ コンテキスト モードでは、コンテキストのスタートアップ コンフィギュレーションを外部サーバに置くことができます。この場合、ASA は、コンテキスト URL で指定したサーバにコンフィギュレーションを戻して保存します。ただし HTTP URL および HTTPS URL の場合は例外で、サーバにコンフィギュレーションを保存できません。

（注） **copy running-config startup-config** コマンドは、**write memory** コマンドに相当します。

すべてのコンテキスト コンフィギュレーションの同時保存

すべてのコンテキスト コンフィギュレーションとシステム コンフィギュレーションを同時に保存するには、次の手順を使用します。

手順

システム実行スペースから、すべてのコンテキストとシステム コンフィギュレーションの実行コンフィギュレーションをスタートアップ コンフィギュレーションに保存します。

write memory all [**/noconfirm**]

/noconfirm キーワードを入力しない場合、次のプロンプトが表示されます。

```
Are you sure [Y/N]:
```

Y を入力すると、ASA によってシステム コンフィギュレーションと各コンテキストが保存されます。コンテキストのスタートアップ コンフィギュレーションは、外部サーバに配置できます。この場合、ASA は、コンテキスト URL で指定したサーバにコンフィギュレーションを戻して保存します。ただし HTTP URL および HTTPS URL の場合は例外で、サーバにコンフィギュレーションを保存できません。

ASA によって各コンテキストが保存された後、次のメッセージが表示されます。

```
‘Saving context ‘b’ ... ( 1/3 contexts saved ) ’
```

エラーのためにコンテキストが保存されない場合もあります。エラーについては、次の情報を参照してください。

- メモリ不足のためにコンテキストが保存されない場合は、次のメッセージが表示されます。

```
The context 'context a' could not be saved due to Unavailability of resources
```

- リモートの宛先に到達できないためにコンテキストが保存されない場合は、次のメッセージが表示されます。

```
The context 'context a' could not be saved due to non-reachability of destination
```

- コンテキストがロックされているために保存されない場合は、次のメッセージが表示されます。

```
Unable to save the configuration for the following contexts as these contexts are
locked.
context ‘a’ , context ‘x’ , context ‘z’ .
```

  コンテキストがロックされるのは、別のユーザがすでにコンフィギュレーションを保存している場合、またはコンテキストを削除している場合のみです。

- スタートアップ コンフィギュレーションが読み取り専用であるために（たとえば、HTTP サーバで）コンテキストが保存されない場合は、他のすべてのメッセージの最後に次のメッセージ レポートが出力されます。

```
Unable to save the configuration for the following contexts as these contexts have
read-only config-urls:
context ‘a’ , context ‘b’ , context ‘c’ .
```

- フラッシュ メモリのセクターが壊れているためコンテキストを保存できない場合は、次のメッセージが表示されます。

```
The context 'context a' could not be saved due to Unknown errors
```

スタートアップコンフィギュレーションの実行コンフィギュレーションへのコピー

新しいスタートアップ コンフィギュレーションを実行コンフィギュレーションにコピーするには、次のいずれかのコマンドを使用します。

- **copy startup-config running-config**

  スタートアップ コンフィギュレーションを実行コンフィギュレーションとマージします。マージによって、新しいコンフィギュレーションから実行コンフィギュレーションに新しいコマンドが追加されます。コンフィギュレーションが同じ場合、変更は発生しません。コマンドが衝突する場合、またはコマンドがコンテキストの実行に影響を与える場合、

マージの結果はコマンドによって異なります。エラーが発生することも、予期できない結果が生じることもあります。

- **reload**

  ASA をリロードします。その結果、スタートアップ コンフィギュレーションがロードされ、実行コンフィギュレーションが破棄されます。

- **clear configure all**、続いて then**copy startup-config running-config**

  スタートアップ コンフィギュレーションをロードし、実行コンフィギュレーションを破棄します。リロードは不要です。

設定の表示

実行コンフィギュレーションとスタートアップ コンフィギュレーションを表示するには、次のコマンドを使用します。

- **show running-config**

  実行コンフィギュレーションを表示します。

- **show running-config** *command*

  特定のコマンドの実行コンフィギュレーションを表示します。

- **show startup-config**

  スタートアップ コンフィギュレーションを表示します。

コンフィギュレーション設定のクリアおよび削除

設定を消去するには、次のいずれかのコマンドを入力します。

- **clear configure** *configurationcommand* [*level2configurationcommand*]

  指定されたコマンドのすべてのコンフィギュレーションをクリアします。コマンドの特定バージョンのコンフィギュレーションだけをクリアする場合は、*level2configurationcommand* に値を入力します。

  たとえば、すべての **aaa** コマンドのコンフィギュレーションをクリアするには、次のコマンドを入力します。

  ```
  ciscoasa(config)# clear configure aaa
  ```

  aaa authentication コマンドのコンフィギュレーションだけをクリアするには、次のコマンドを入力します。

  ```
  ciscoasa(config)# clear configure aaa authentication
  ```

- **no** *configurationcommand* [*level2configurationcommand*] *qualifier*

コマンドの特定のパラメータまたはオプションをディセーブルにします。この場合、**no** コマンドを使用して、*qualifier* で識別される特定のコンフィギュレーションを削除します。

たとえば、特定の **access-list** コマンドを削除するには、それを一意に特定するのに十分なコマンドを入力します。コマンド全体を入力しなければならない場合もあります。

```
ciscoasa(config)# no access-list abc extended permit icmp any any object-group
obj_icmp_1
```

- **write erase**

  スタートアップ コンフィギュレーションを消去します。

  （注） ASAv の場合、このコマンドはリロード後に導入構成を復元します。コンフィギュレーションを完全に消去するには、**clear configure all** コマンドを使用します。

- **clear configure all**

  実行コンフィギュレーションを消去します。

  （注） マルチコンテキストモードでは、システム コンフィギュレーションから **clear configure all** を入力すると、すべてのコンテキストを削除し、実行中のコンフィギュレーションを停止することにもなります。コンテキスト コンフィギュレーション ファイルは消去されず、元の場所に保持されます。

  （注） Firepower 2100 の場合：このモデルでは、**boot system** コマンドは使用されません。パッケージは FXOS によって管理されます。

  その他すべてのモデルの場合：このコマンドは、残りの設定とともに **boot system** コマンドをクリアします（存在する場合）。**boot system** コマンドは、外部フラッシュ メモリ カードのイメージを含む、特定のイメージからの起動を可能にします。ASA を次回リロードすると、内部フラッシュ メモリの最初のイメージから起動します。内部フラッシュ メモリにイメージがない場合、ASA は起動しません。

オフラインでテキスト コンフィギュレーション ファイルの作成

このガイドは、CLIを使用したASAの設定方法について説明します。コマンドを保存すると、変更がテキスト ファイルに書き込まれます。一方、CLI を使用する代わりに、テキスト ファイルをコンピュータで直接編集して、コンフィギュレーション モードのコマンドライン プロンプトから、コンフィギュレーションを全部または1行ずつペーストすることができます。別の方法として、ASA 内部フラッシュ メモリにテキスト ファイルをダウンロードします。ASA への設定ファイルのダウンロードについては、ソフトウェアおよびコンフィギュレーション（1003 ページ） を参照してください。

ほとんどの場合、このマニュアルで説明するコマンドには、CLIプロンプトが先行します。次の例でのプロンプトは「ciscoasa(config)#」です。

```
ciscoasa(config)# context a
```

コマンドの入力が要求されないテキスト コンフィギュレーション ファイルの場合は、プロンプトは次のように省略されます。

```
context a
```

ファイルのフォーマットの詳細については、コマンドライン インターフェイスの使用 （1203 ページ）を参照してください。

接続の設定変更の適用

コンフィギュレーションに対してセキュリティ ポリシーの変更を加えた場合は、すべての新しい接続で新しいセキュリティ ポリシーが使用されます。既存の接続は、接続の確立時に設定されたポリシーを引き続き使用します。古い接続の **show** コマンド出力には古い設定が反映され、古い接続に関するデータを含まない場合があります。

たとえば、インターフェイスから QoS **service-policy** を削除し、修正バージョンを再度追加する場合、**show service-policy** コマンドには、新しいサービス ポリシーと一致する新規接続と関連付けられている QoS カウンタのみ表示されます。古いポリシーの既存の接続はコマンド出力には表示されません。

すべての接続が新しいポリシーを確実に使用するように、現在の接続を解除し、新しいポリシーを使用して再度接続できるようにします。

接続を解除するには、次のいずれかのコマンドを入力します。

- **clear local-host** [*ip_address*] [**all**]

  このコマンドは、接続制限値や初期接続の制限など、クライアントごとのランタイム ステートを再初期化します。これにより、このコマンドは、これらの制限を使用しているすべての接続を削除します。ホストごとの現在のすべての接続を表示するには、**show local-host all** コマンドを参照してください。

引数を指定しないと、このコマンドは、影響を受けるすべての through-the-box 接続をクリアします。to-the-box 接続もクリアするには（現在の管理セッションを含む）、**all** キーワードを使用します。特定の IP アドレスへの、または特定の IP アドレスからの接続をクリアするには、*ip_address* 引数を使用します。

- **clear conn**[**all**] [**protocol** {**tcp** |**udp**}] [**address** *src_ip* [-*src_ip*] [**netmask** *mask*] [**port** *src_port* [-*src_port*] [**address** *dest_ip* [-*dest_ip*] [**netmask** *mask*] [**port** *dest_port* [-*dest_port*]

  このコマンドは、すべての状態の接続を終了します。現在のすべての接続を表示するには、**show conn** コマンドを参照してください。

  引数を指定しないと、このコマンドはすべての through-the-box 接続をクリアします。to-the-box 接続もクリアするには（現在の管理セッションを含む）、**all** キーワードを使用します。送信元 IP アドレス、宛先 IP アドレス、ポート、プロトコルに基づいて特定の接続をクリアするには、必要なオプションを指定できます。

ASA のリロード

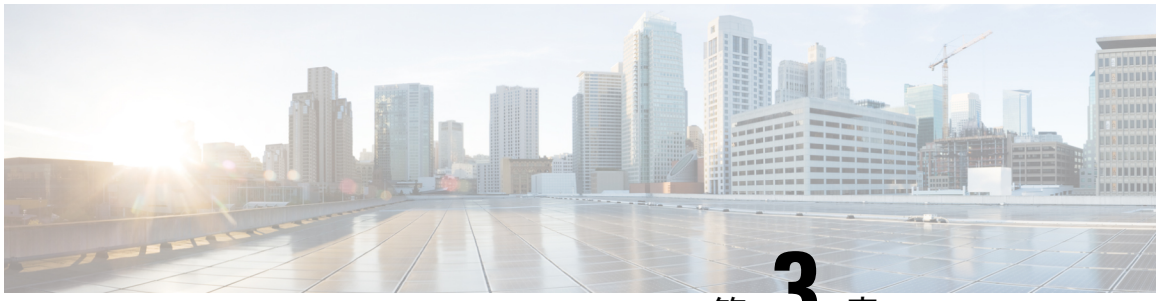
ASA をリロードするには、次の手順を実行します。

手順

ASA をリロードします。

reload

（注） マルチ コンテキスト モードでは、システム実行スペース以外からはリロードできません。



第 3 章

ライセンス：製品認証キー ライセンス

ライセンスでは、特定の Cisco ASA 上でイネーブルにするオプションを指定します。このマニュアルでは、すべての物理ASAの製品認証キー（PAK）のライセンスについて説明します。ASAvについては、ライセンス：スマート ソフトウェア ライセンス（ASAv、ASA on Firepower）（131 ページ）を参照してください。

PAK ライセンスについて

ライセンスでは、特定のASA上でイネーブルにするオプションを指定します。ライセンスは、160 ビット（32 ビットのワードが 5 個、または 20 バイト）値であるアクティベーション キーで表されます。この値は、シリアル番号（11 文字の文字列）とイネーブルになる機能とを符号化します。

事前インストール済みライセンス

デフォルトでは、ASAは、ライセンスがすでにインストールされた状態で出荷されます。このライセンスは、注文した内容およびベンダーがインストールした内容に応じて、ライセンスを追加できる基本ライセンスの場合と、すべてのライセンスがすでにインストールされている場合があります。

関連トピック

PAK ライセンスのモニタリング （108 ページ）

永続ライセンス

永続アクティベーション キーを 1 つインストールできます。永続アクティベーション キーは、1 つのキーにすべてのライセンス機能を格納しています。時間ベース ライセンスもインストールすると、ASA は永続ライセンスと時間ベース ライセンスを 1 つの実行ライセンスに結合します。

関連トピック

永続ライセンスと時間ベース ライセンスの結合 （59 ページ）

時間ベース ライセンス

永続ライセンスに加えて、時間ライセンスを購入したり、時間制限のある評価ライセンスを入手したりできます。たとえば、SSL VPN の同時ユーザの短期増加に対処するために時間ベースの AnyConnect Premium ライセンスを購入したり、1 年間有効なボットネット トラフィック フィルタ時間ベース ライセンスを注文したりできます。

（注） ASA 5506-X および ASA 5506W-X は、時間ベース ライセンスをサポートしません。

時間ベース ライセンス有効化ガイドライン

- 複数の時間ベース ライセンスをインストールし、同じ機能に複数のライセンスを組み込むことができます。ただし、一度にアクティブ化できる時間ベース ライセンスは、1 機能につき 1 つだけです。非アクティブのライセンスはインストールされたままで、使用可能な状態です。たとえば、1000 セッション AnyConnect Premium ライセンスと 2500 セッション AnyConnect Premium ライセンスをインストールした場合、これらのライセンスのうちいずれか 1 つだけをアクティブにできます。
- キーの中に複数の機能を持つ評価ライセンスをアクティブにした場合、そこに含まれている機能のいずれかに対応する時間ベース ライセンスを同時にアクティブ化することはできません。たとえば、評価ライセンスにボットネット トラフィック フィルタと 1000 セッション AnyConnect Premium ライセンスが含まれる場合、スタンドアロンの時間ベース 2500 セッション AnyConnect Premium ライセンスをこの評価ライセンスと同時にアクティブ化することはできません。

時間ベース ライセンス タイマーの動作

- 時間ベース ライセンスのタイマーは、ASA 上でライセンスをアクティブにした時点でカウント ダウンを開始します。
- タイムアウト前に時間ベース ライセンスの使用を中止すると、タイマーが停止します。時間ベース ライセンスを再度アクティブ化すると、タイマーが再開します。
- 時間ベース ライセンスがアクティブになっているときに ASA をシャットダウンすると、タイマーはカウント ダウンを停止します。時間ベース ライセンスでは、ASA が動作して

いる場合にのみカウント ダウンします。システム クロック設定はライセンスに影響しません。つまり、ASA 稼働時間ではライセンス継続期間に対してのみカウントします。

永続ライセンスと時間ベース ライセンスの結合

時間ベース ライセンスをアクティブにすると、永続ライセンスと時間ベース ライセンスに含まれる機能を組み合わせた実行ライセンスが作成されます。永続ライセンスと時間ベース ライセンスの組み合わせ方は、ライセンスのタイプに依存します。次の表に、各機能ライセンスの組み合わせルールを示します。

（注） 永続ライセンスが使用されていても、時間ベース ライセンスがアクティブな場合はカウントダウンが続行されます。

表 *1*：時間ベース ライセンスの組み合わせルール

時間ベース機能	結合されたライセンスのルール
AnyConnect Premium セッション	時間ベース ライセンスまたは永続ライセンスのうち、値の高い方が使用されます。たとえば、永続ライセンスが 1000 セッション、時間ベース ライセンスが 2500 セッションの場合、2500 セッションがイネーブルになります。通常は、永続ライセンスよりも機能の低い時間ベース ライセンスをインストールすることはありませんが、そのようなインストールが行われた場合は永続ライセンスが使用されます。
Unified Communications Proxy セッション	時間ベースライセンスのセッションは、プラットフォームの制限数まで永続セッションに追加されます。たとえば、永続ライセンスが 2500 セッション、時間ベース ライセンスが 1000 セッションの場合、時間ベース ライセンスがアクティブである限り、3500 セッションがイネーブルになります。
セキュリティ コンテキスト	時間ベース ライセンスのコンテキストは、プラットフォームの制限数まで永続コンテキストに追加されます。たとえば、永続ライセンスが 10 コンテキスト、時間ベース ライセンスが 20 コンテキストの場合、時間ベース ライセンスがアクティブである限り、30 コンテキストがイネーブルになります。

時間ベース機能	結合されたライセンスのルール
Botnet Traffic Filter	使用可能な永続ボットネット トラフィック フィルタ ライセンスはありません。時間ベース ライセンスが使用されます。
その他	時間ベース ライセンスまたは永続ライセンスのうち、値の高い方が使用されます。ライセンスのステータスがイネーブルまたはディセーブルの場合、イネーブル ステータスのライセンスが使用されます。数値ティアを持つライセンスの場合、高い方の値が使用されます。通常は、永続ライセンスよりも機能の低い時間ベース ライセンスをインストールすることはありませんが、そのようなインストールが行われた場合は永続ライセンスが使用されます。

関連トピック

PAK ライセンスのモニタリング （108 ページ）

時間ベース ライセンスのスタッキング

多くの場合、時間ベース ライセンスは更新の必要があり、旧ライセンスから新しいライセンスへシームレスに移行する必要があります。時間ベース ライセンスだけで使用される機能では、新しいライセンスが適用される前に、ライセンスの有効期限が切れてしまわないことが特に重要です。ASA では時間ベース ライセンスをスタックできるので、ライセンスの有効期限が切れたり、新しいライセンスを早めにインストールしたために時間が無駄になったりする心配はありません。

すでにインストールされているのと同じ時間ベース ライセンスをインストールすると、それらのライセンスは結合され、有効期間は両者を合わせた期間になります。

次に例を示します。

1. 52 週のボットネット トラフィック フィルタ ライセンスをインストールし、このライセンスを 25 週間使用します（残り 27 週）。
2. 次に、別の 52 週ボットネット トラフィック フィルタ ライセンスを購入します。2 つめのライセンスをインストールすると、ライセンスが結合され、有効期間は 79 週（52＋27 週）になります。

同様の例を示します。

1. 8 週 1000 セッションの AnyConnect Premium ライセンスをインストールし、これを 2 週間使用します（残り 6 週）。

2. 次に、別の 8 週 1000 セッションのライセンスをインストールすると、これらのライセンスは結合され、14 週（8 + 6 週）1000 セッションのライセンスになります。

これらのライセンスが同一でない場合（たとえば、1000 セッション AnyConnect Premium ライセンスと 2500 セッション ライセンス）、これらのライセンスは結合されません。1 つの機能につき時間ベース ライセンスを 1 つだけアクティブにできるので、ライセンスのうちいずれか 1 つだけをアクティブにすることができます。

同一でないライセンスは結合されませんが、現在のライセンスの有効期限が切れた場合、同じ機能のインストール済みライセンスが使用可能であれば、ASA はそのライセンスを自動的にアクティブにします。

関連トピック

キーのアクティブ化または非アクティブ化 （77 ページ）
時間ベース ライセンスの有効期限 （61 ページ）

時間ベース ライセンスの有効期限

機能に対応する現在のライセンスが期限切れになると、同じ機能のインストール済みライセンスが使用可能であれば、ASA はそのライセンスを自動的にアクティブにします。その機能に使用できる時間ベース ライセンスが他にない場合は、永続ライセンスが使用されます。

その機能に対して複数の時間ベース ライセンスを追加でインストールした場合、ASA は最初に検出されたライセンスを使用します。どのライセンスを使用するかは、ユーザが設定することはできず、内部動作に依存します。ASA がアクティブ化したライセンスとは別の時間ベース ライセンスを使用するには、目的のライセンスを手動でアクティブにする必要があります。

たとえば、2500 セッションの時間ベース AnyConnect Premium ライセンス（アクティブ）、1000 セッションの時間ベース AnyConnect Premium ライセンス（非アクティブ）、500 セッションの永続 AnyConnect Premium ライセンスを所有しているとします。2500 セッション ライセンスの有効期限が切れた場合、ASA は 1000 セッション ライセンスを有効化します。1000 セッション ライセンスの有効期限が切れた後、ASA は 500 セッション永久ライセンスを使用します。

関連トピック

キーのアクティブ化または非アクティブ化 （77 ページ）

ライセンスに関する注意事項

次の項で、ライセンスに関する追加情報について説明します。

AnyConnect Plus および Apex ライセンス

AnyConnect Plus および Apex ライセンスは、ライセンスが指定するユーザ プールを共有するすべての複数の ASA に適用できる同時使用ライセンスです。https://www.cisco.com/go/license [英語] を参照し、各 ASA に個別に PAK を割り当てます。ASA に取得したアクティベーション キーを適用すると、VPN 機能が最大許容数に切り替わりますが、ライセンスを共有するすべて

の ASA 上の実際の一意のユーザ数はライセンス限度を超えることはできません。詳細については、以下を参照してください。

- 『Cisco AnyConnect Ordering Guide』
- AnyConnect Licensing Frequently Asked Questions (FAQ)

その他の VPN ライセンス

その他の VPN セッションには、次の VPN タイプが含まれています。

- IKEv1 を使用した IPsec リモート アクセス VPN
- IKEv1 を使用した IPsec サイトツーサイト VPN
- IKEv2 を使用した IPsec サイトツーサイト VPN

このライセンスは基本ライセンスに含まれています。

合計 VPN セッション、全タイプ

- VPN セッションの最大数の合計が、VPN AnyConnect とその他の VPN セッションの最大数よりも多くなっても、組み合わせたセッション数が VPN セッションの制限を超えることはできません。VPN の最大セッション数を超えた場合、ASA をオーバーロードして、適切なネットワークのサイズに設定してください。
- クライアントレス SSL VPN セッションを開始した後、ポータルから AnyConnect クライアントセッションを開始した場合は、合計 1 つのセッションが使用されています。これに対して、最初に AnyConnect クライアントを（スタンドアロン クライアントなどから）開始した後、クライアントレス SSL VPN ポータルにログインした場合は、2 つのセッションが使用されています。

VPN ロード バランシング

VPN ロード バランシングには、強力な暗号化（3DES/AES）ライセンスが必要です。

レガシー VPN ライセンス

ライセンスに関するすべての関連情報については、「AnyConnect の補足エンド ユーザ ライセンス契約書（Supplemental end User License Agreement for AnyConnect）」を参照してください。

暗号化ライセンス

DES ライセンスはディセーブルにできません。3DES ライセンスをインストールしている場合、DES は引き続き使用できます。強力な暗号化だけを使用したい場合に DES の使用を防止するには、強力な暗号化だけを使用するようにすべての関連コマンドを設定する必要があります。

合計 UC プロキシ セッション

Encrypted Voice Inspection の各 TLS プロキシ セッションは、TLS ライセンスの制限に対してカウントされます。

TLS プロキシセッションを使用するその他のアプリケーション（ライセンスが不要な Mobility Advantage Proxy など）では、TLS 制限に対してカウントしません。

アプリケーションによっては、1 つの接続に複数のセッションを使用する場合があります。たとえば、プライマリとバックアップの Cisco Unified Communications Manager を電話に設定した場合は、TLS プロキシ接続は 2 つ使用されます。

TLS プロキシの制限は、**tls-proxy maximum-sessions** コマンドまたは ASDM で [Configuration] > [Firewall] > [Unified Communications] > [TLS Proxy] ペインを使用して個別に設定できます。モデルの制限を表示するには、**tls-proxy maximum-sessions ?** コマンドを入力します。デフォルトの TLS プロキシ制限よりも高い TLS プロキシライセンスを適用する場合、ASA では、そのライセンスに一致するように TLS プロキシの制限が自動的に設定されます。ライセンスの制限よりも TLS プロキシ制限が優先されます。TLS プロキシ制限をライセンスよりも少なく設定すると、ライセンスですべてのセッションを使用できません。

（注） 「K8」で終わるライセンス製品番号（たとえばユーザ数が 250 未満のライセンス）では、TLS プロキシセッション数は 1000 までに制限されます。「K9」で終わるライセンス製品番号（たとえばユーザ数が 250 以上のライセンス）では、TLS プロキシの制限はコンフィギュレーションに依存し、モデルの制限が最大数になります。K8 と K9 は、エクスポートについてそのライセンスが制限されるかどうかを示します。K8 は制限されず、K9 は制限されます。

（たとえば **clear configure all** コマンドを使用して）コンフィギュレーションをクリアすると、TLS プロキシ制限がモデルのデフォルトに設定されます。このデフォルトがライセンスの制限よりも小さいと、**tls-proxy maximum-sessions** コマンドを使用したときに、再び制限を高めるようにエラー メッセージが表示されます（ASDM の [TLS Proxy] ペインを使用）。フェールオーバーを使用して、**write standby** コマンドを入力するか、または ASDM でプライマリ装置に対して [File] > [Save Running Configuration to Standby Unit] を使用して強制的にコンフィギュレーションの同期を行うと、セカンダリ装置で **clear configure all** コマンドが自動的に生成され、セカンダリ装置に警告メッセージが表示されることがあります。コンフィギュレーションの同期によりプライマリ装置の TLS プロキシ制限の設定が復元されるため、この警告は無視できます。

接続には、SRTP 暗号化セッションを使用する場合もあります。

- K8 ライセンスでは、SRTP セッション数は 250 までに制限されます。
- K9 ライセンスでは、制限はありません。

（注） メディアの暗号化/復号化を必要とするコールだけが、SRTP 制限に対してカウントされます。コールに対してパススルーが設定されている場合は、両方のレッグが SRTP であっても、SRTP 制限に対してカウントされません。

VLAN、最大

VLAN 制限の対象としてカウントするインターフェイスに、VLAN を割り当てます。 次に例を示します。

```
interface gigabitethernet 0/0.100
vlan 100
```

ボットネット トラフィック フィルタ ライセンス

ダイナミック データベースをダウンロードするには、強力な暗号化（3DES/AES）ライセンスが必要です。

IPS モジュールのライセンス

IPS モジュール ライセンスがあると、ASA で IPS ソフトウェア モジュールを実行することができます。また、IPS 側の IPS シグニチャ サブスクリプションが必要です。

次のガイドラインを参照してください。

- IPS シグニチャ サブスクリプションを購入するには、IPS がプリインストールされた ASA が必要です（製品番号に、たとえば ASA5515-IPS-K9 のように「IPS」が含まれている必要があります）。IPS ではない製品番号の ASA に IPS シグニチャ サブスクリプションを購入することはできません。
- フェールオーバーについては、両方のユニットで IPS シグネチャ サブスクリプションが必要です。このサブスクリプションは ASA ライセンスでないため、フェールオーバー時に共有されません。
- フェールオーバーについて、IPS シグニチャ サブスクリプションには、装置ごとに個別の IPS モジュール ライセンスが必要です。他の ASA のライセンスと同様に、IPS モジュール ライセンスも技術的にはフェールオーバー クラスタ ライセンスで共有されます。しかし、IPS シグニチャ サブスクリプションの要件によって、フェールオーバーの装置ごとに個別の IPS モジュール ライセンスを購入する必要があります。

AnyConnect Premium 共有ライセンス（AnyConnect 3 以前）

（注） ASAの共有ライセンス機能は、AnyConnect 4 以降のライセンスではサポートされていません。AnyConnect ライセンスが共有されているため、共有サーバまたは参加ライセンスは不要になりました。

共有ライセンスを使用すると、多数の AnyConnect Premium セッションを購入し、それらのセッションを ASA のグループ間で必要に応じて共有できます。そのためには、いずれかの ASA を共有ライセンス サーバとして、残りを共有ライセンス参加システムとして設定します。

フェールオーバーまたは ASA クラスタ ライセンス

いくつかの例外を除き、フェールオーバーおよびクラスタ ユニットは、各ユニット上で同一のライセンスを必要としません。以前のバージョンについては、お使いのバージョンに該当するライセンシング マニュアルを参照してください。

フェールオーバー ライセンスの要件および例外

フェールオーバーユニットは、各ユニット上で同一のライセンスを必要としません。両方のユニット上にライセンスがある場合、これらのライセンスは単一の実行フェールオーバー クラスタ ライセンスに結合されます。このルールには、いくつかの例外があります。フェールオーバーの正確なライセンス要件については、次の表を参照してください。

モデル	ライセンス要件
ASA 5506-X および ASA 5506W-X	• アクティブ/スタンバイ：Security Plus ライセンス。 • アクティブ/アクティブ：サポートなし。 （注） 各ユニットに同じ暗号化ライセンスが必要です。

モデル	ライセンス要件
ASA 5512-X ～ ASA 5555-X	• ASA 5512：Security Plus ライセンス。 • その他のモデル：基本ライセンス。 （注） • 各ユニットに同じ暗号化ライセンスが必要です。 • マルチ コンテキスト モードでは、各ユニットに同じ AnyConnect Apex ライセンスが必要です。 • 各ユニットに同じ IPS モジュール ライセンスが必要です。両方の装置の IPS 側で IPS シグニチャ サブスクリプションも必要です。次のガイドラインを参照してください。 • IPS シグニチャ サブスクリプションを購入するには、IPS がプリインストールされた ASA が必要です（ASA5525-IPS-K9 のように、製品番号に「IPS」が含まれている必要があります）。IPS 以外の製品番号の ASA に IPS シグニチャ サブスクリプションを購入することはできません。 • 両方の装置に IPS シグニチャ サブスクリプションが必要です。このサブスクリプションは ASA ライセンスではないため、フェールオーバー間で共有されません。 • IPS シグニチャ サブスクリプションには、装置ごとに個別の IPS モジュール ライセンスが必要です。他の ASA のライセンスと同様に、IPS モジュール ライセンスも技術的にはフェールオーバー クラスタ ライセンスで共有されます。しかし、IPS シグニチャ サブスクリプションの要件によって、装置ごとに個別の IPS モジュール ライセンスを購入する必要があります。
ASAv	ASAv のフェールオーバー ライセンス （138 ページ）を参照してください。

モデル	ライセンス要件
Firepower 9300	Firepower 9300 シャーシ の ASA のフェールオーバー ライセンス （138 ページ）を参照してください。
他のすべてのモデル	基本ライセンスまたは標準ライセンス。 （注） • 各ユニットに同じ暗号化ライセンスが必要です。 • マルチ コンテキスト モードでは、各ユニットに同じ AnyConnect Apex ライセンスが必要です。

（注） 有効な永続キーが必要です。まれに、PAK 認証キーを削除できることもあります。キーがすべて 0 の場合は、フェールオーバーを有効化するには有効な認証キーを再インストールする必要があります。

ASA クラスタ ライセンスの要件および例外

クラスタ ユニットは、各ユニット上で同じライセンスを必要としません。一般的には、マスター ユニット用のライセンスのみを購入します。スレーブ ユニットはマスターのライセンスを継承します。複数のユニットにライセンスがある場合は、これらが統合されて単一の実行 ASA クラスタ ライセンスとなります。

このルールには、例外があります。クラスタリングの正確なライセンス要件については、次の表を参照してください。

モデル	ライセンス要件
ASA 5585-X	クラスタ ライセンス、最大 16 ユニットをサポートします。 （注） 各ユニットに、同じ暗号化ライセンスが必要です。各ユニットに同じ 10 GE I/O/Security Plus ライセンスが必要です（ASA 5585-X と SSP-10 および SSP-20）。
ASA 5512-X	Security Plus ライセンス、2 ユニットをサポートします。 （注） 各ユニットに同じ暗号化ライセンスが必要です。
ASA 5515-X、ASA 5525-X、ASA 5545-X、ASA 5555-X	基本ライセンス、2 ユニットをサポートします。 （注） 各ユニットに同じ暗号化ライセンスが必要です。

モデル	ライセンス要件
Firepower 9300 シャーシ	Firepower 9300 シャーシ 上の ASA の ASA クラスタ ライセンス （139 ページ）を参照してください。
他のすべてのモデル	サポートしない

フェールオーバーまたは ASA クラスタ ライセンスの結合方法

フェールオーバー ペアまたは ASA クラスタでは、各ユニットのライセンスが結合されて 1 つの実行クラスタ ライセンスとなります。ユニットごとに別のライセンスを購入した場合は、結合されたライセンスには次のルールが使用されます。

- 数値ティアを持つライセンスの場合は（セッション数など）、各ユニットのライセンスの値が合計されます。ただし、プラットフォームの制限を上限とします。使用されているライセンスがすべて時間ベースの場合は、ライセンスのカウント ダウンは同時に行われます。

  たとえば、フェールオーバーの場合は次のようになります。

  - 2 つの ASA があり、それぞれに 10 個の TLS プロキシ セッションが設定されている場合、ライセンスは結合され、合計で 20 個の TLS プロキシ セッションになります。
  - 1000 個の TLS プロキシ セッションを設定した ASA 5545-X と、2000 個のセッションを設定した ASA 5545-X がある場合、プラットフォームの制限が 2000 であるため、結合されたライセンスでは 2000 個の TLS プロキシ セッションを使用できます。
  - 2 つの ASA 5545-X ASA があり、一方は 20 コンテキスト、もう一方は 10 コンテキストである場合、結合されたライセンスでは30コンテキストを使用できます。アクティブ/アクティブ フェールオーバーの場合は、コンテキストが 2 つのユニットに分配されます。たとえば、一方のユニットが 18 コンテキストを使用し、他方が 12 コンテキストを使用します（合計 30 の場合）。

  たとえば、ASA クラスタリングの場合は次のようになります。

  - デフォルトの 2 コンテキストの 2 つの ASA 5516-X ASA があります。プラットフォームの制限が 5 であるため、結合されたライセンスでは最大 4 のコンテキストが許容されます。したがって、プライマリ ユニット上で最大 4 のコンテキストを設定できます。各セカンデリ ユニットも、コンフィギュレーションの複製経由で4のコンテキストを持つことになります。
  - 4 つの ASA 5516-X ASA があります。これは、それぞれが 5 コンテキストの 3 つのユニットと、デフォルトの 2 コンテキストの 1 つのユニットです。プラットフォームの制限が 5 であるため、ライセンスは合計で 5 コンテキストに結合されます。したがって、プライマリ ユニット上で最大 5 のコンテキストを設定できます。各セカンデリ ユニットも、コンフィギュレーションの複製経由で 5 のコンテキストを持つことになります。

- ライセンスのステータスがイネーブルまたはディセーブルの場合、イネーブル ステータスのライセンスが使用されます。
- イネーブルまたはディセーブル状態（かつ数値ティアを持たない）の時間ベース ライセンスの場合、有効期間はすべてのライセンスの期間の合計となります。最初にプライマリ/マスター ユニットのライセンスがカウント ダウンされ、期限切れになると、セカンダリ/スレーブ ユニットのライセンスのカウント ダウンが開始し、以下も同様です。このルールは、アクティブ/アクティブ フェールオーバーと ASA クラスタリングにも適用されます（すべてのユニットがアクティブに動作していても適用されます）。

  たとえば、2 つのユニットのボットネット トラフィック フィルタ ライセンスの有効期間が 48 週残っている場合は、結合された有効期間は 96 週です。

関連トピック

PAK ライセンスのモニタリング （108 ページ）

フェールオーバーまたは ASA クラスタ ユニット間の通信の途絶

ユニットの通信が途絶えてからの期間が 30 日を超えた場合は、各ユニットにはローカルにインストールされたライセンスが適用されます。30 日の猶予期間中は、結合された実行ライセンスが引き続きすべてのユニットで使用されます。

30 日間の猶予期間中に通信が復旧した場合は、時間ベース ライセンスについては、経過した時間がプライマリ/マスター ライセンスから差し引かれます。プライマリ/マスター ライセンスが期限切れになるまでは、セカンダリ/スレーブ ライセンスのカウント ダウンが開始することはありません。

30 日間の期間が終了しても通信が復旧しなかった場合は、時間ベース ライセンスについては、その時間がすべてのユニットのライセンスから差し引かれます（インストールされている場合）。これらはそれぞれ別のライセンスとして扱われ、ライセンスの結合によるメリットはありません。経過時間には 30 日の猶予期間も含まれます。

次に例を示します。

1. 52 週のボットネット トラフィック フィルタ ライセンスが 2 つのユニットにインストールされています。結合された実行ライセンスでは、合計期間は 104 週になります。
2. これらのユニットが、1 つのフェールオーバー ユニット/ASA クラスタとして 10 週間動作すると、結合ライセンスの期間の残りは 94 週となります（プライマリ/マスターに 42 週、セカンダリ/スレーブに 52 週）。
3. ユニットの通信が途絶えた場合（たとえば、プライマリ/マスター ユニットが停止した場合）は、セカンダリ/スレーブ ユニットは結合されたライセンスを引き続き使用し、94 週からカウント ダウンを続行します。
4. 時間ベース ライセンスの動作は、通信がいつ復元されるかによって次のように異なります。
   - 30 日以内：経過した時間がプライマリ/マスター ユニットのライセンスから差し引かれます。この場合、通信は 4 週間後に復元されます。したがって、4 週がプライマリ/

マスター ライセンスから差し引かれて、残りは合計 90 週となります（プライマリに 38 週、セカンダリに 52 週）。

- 30 日経過以降：経過時間が両方の装置から差し引かれます。この場合、通信は 6 週間後に復元されます。したがって、6 週がプライマリ/マスターとセカンダリ/スレーブの両方のライセンスから差し引かれて、残りは合計 84 週となります（プライマリ/マスターに 36 週、セカンダリ/スレーブに 46 週）。

フェールオーバー ペアのアップグレード

フェールオーバーペアでは、両方の装置に同一のライセンスがインストールされている必要はないので、ダウンタイムなしに各装置に新しいライセンスを適用できます。リロードが必要な永続ライセンスを適用する場合、リロード中に他の装置へのフェールオーバーを実行できます。両方の装置でリロードが必要な場合は、各装置を個別にリロードするとダウンタイムは発生しません。

関連トピック

キーのアクティブ化または非アクティブ化 （77 ページ）

ペイロード暗号化機能のないモデル

ペイロード暗号化機能のないモデルを購入することができます。輸出先の国によっては、Cisco ASA シリーズでペイロード暗号化をイネーブルにできません。ASA ソフトウェアは、ペイロード暗号化なしモデルを検出し、次の機能をディセーブルにします。

- ユニファイド コミュニケーション
- [VPN]

このモデルでも管理接続用に高度暗号化（3DES/AES）ライセンスをインストールできます。たとえば、ASDM HTTPS/SSL、SSHv2、Telnet、および SNMPv3 を使用できます。ボットネット トラフィック フィルタ（SSL を使用）用のダイナミック データベースをダウンロードすることもできます。

ライセンスを表示すると、VPN およびユニファイド コミュニケーションのライセンスはリストに示されません。

関連トピック

PAK ライセンスのモニタリング （108 ページ）

ライセンスの FAQ

AnyConnect Premium とボットネット トラフィック フィルタなど、複数の時間ベース ライセンスをアクティブにできますか。

はい。一度に使用できる時間ベース ライセンスは、1 機能につき 1 つです。

複数の時間ベース ライセンスを「スタック」し、時間制限が切れると自動的に次のライセンスが使用されるようにできますか。

はい。ライセンスが同一の場合は、複数の時間ベース ライセンスをインストールすると、時間制限が結合されます。ライセンスが同一でない場合（1000 セッション AnyConnect Premium ライセンスと 2500 セッション ライセンスなど）、ASA はその機能に対して検出された次の時間ベース ライセンスを自動的にアクティブにします。

アクティブな時間ベース ライセンスを維持しながら、新しい永続ライセンスをインストールできますか。

はい。永続ライセンスをアクティブ化しても、時間ベース ライセンスには影響しません。

フェールオーバーのプライマリ装置として共有ライセンス サーバを、セカンダリ装置として共有ライセンス バックアップ サーバを使用できますか。

いいえ。セカンダリ装置は、プライマリ装置と同じ実行ライセンスを使用します。共有ライセンス サーバには、サーバ ライセンスが必要です。バックアップ サーバには、参加ライセンスが必要です。バックアップ サーバは、2 つのバックアップ サーバの別々のフェールオーバー ペアに配置できます。

フェールオーバー ペアのセカンダリ装置用に、同じライセンスを購入する必要がありますか。

いいえ。バージョン 8.3(1) から、両方の装置に同一のライセンスをインストールする必要はなくなりました。一般的に、ライセンスはプライマリ装置で使用するために購入されます。セカンダリ装置は、アクティブになるとプライマリ ライセンスを継承します。セカンダリ装置に別のライセンスを持っている場合は（たとえば、8.3 よりも前のソフトウェアに一致するライセンスを購入した場合）、ライセンスは実行フェールオーバー クラスタ ライセンスに結合されます。ただし、モデルの制限が最大数になります。

AnyConnect Premium（共有）ライセンスに加えて、時間ベースまたは永続の AnyConnect Premium ライセンスを使用できますか。

はい。ローカルにインストールされたライセンス（時間ベース ライセンスまたは永続ライセンス）のセッション数を使い果たした後、共有ライセンスが使用されます。

（注） 共有ライセンス サーバでは、永続 AnyConnect Premium ライセンスは使用されません。ただし、共有ライセンス サーバ ライセンスと同時に時間ベース ライセンスを使用することはできます。この場合、時間ベース ライセンスのセッションは、ローカルの AnyConnect Premiumセッションにだけ使用できます。共有ライセンス プールに追加して参加システムで使用することはできません。

PAK ライセンスのガイドライン

コンテキスト モードのガイドライン

マルチ コンテキスト モードでシステム実行スペース内にアクティベーション キーを適用します。

フェールオーバーのガイドライン

フェールオーバーまたは ASA クラスタ ライセンス （65 ページ）を参照してください。

モデルのガイドライン

- スマート ライセンスは、ASAv でのみサポートされます。
- 共有ライセンスは、ASAv、ASA 5506-X、ASA 5508-X および ASA 5516-X ではサポートされません。
- ASA 5506-X および ASA 5506W-X は、時間ベース ライセンスをサポートしません。

アップグレードとダウングレードのガイドライン

任意の旧バージョンから最新バージョンにアップグレードした場合、アクティベーション キーの互換性は存続します。ただし、ダウングレード機能の維持には問題が生じる場合があります。

- バージョン 8.1 以前にダウングレードする場合：アップグレード後に、*8.2* よりも前に導入された機能のライセンスを追加でアクティブ化すると、ダウングレードした場合でも旧バージョンに対するアクティベーション キーの互換性は存続します。ただし、*8.2* 以降で導入された機能ライセンスをアクティブ化した場合は、アクティベーション キーの下位互換性がなくなります。互換性のないライセンス キーがある場合は、次のガイドラインを参照してください。
  - 以前のバージョンでアクティベーション キーを入力した場合は、ASA はそのキーを使用します（バージョン 8.2 以降でアクティブ化した新しいライセンスがない場合）。
  - 新しいシステムで、以前のアクティベーション キーがない場合は、旧バージョンと互換性のある新しいアクティベーション キーを要求する必要があります。
- バージョン 8.2 以前にダウングレードする場合：バージョン 8.3 では、よりロバストな時間ベース キーの使用およびフェールオーバー ライセンスの変更が次のとおり導入されました。
  - 複数の時間ベースのアクティベーション キーがアクティブな場合、ダウングレード時には一番最近アクティブ化された時間ベース キーのみがアクティブになれます。他のキーはすべて非アクティブ化されます。最後の時間ベース ライセンスが 8.3 で導入された機能に対応している場合、そのライセンスは旧バージョンでの使用はできなくて

も、アクティブ ライセンスのままです。永続キーまたは有効な時間ベース キーを再入力してください。

- フェールオーバーペアに不一致のライセンスがある場合、ダウングレードによりフェールオーバーはディセーブルになります。キーが一致した場合でも、使用するライセンスは、結合されたライセンスではなくなります。
- 1 つの時間ベース ライセンスをインストールしているが、それが 8.3 で導入された機能に対応している場合、ダウングレードの実行後、その時間ベース ライセンスはアクティブなままです。この時間ベース ライセンスをディセーブルにするには、永続キーを再入力する必要があります。

その他のガイドライン

- アクティベーション キーは、コンフィギュレーション ファイルには保存されません。隠しファイルとしてフラッシュ メモリに保存されます。
- アクティベーション キーは、デバイスのシリアル番号に関連付けられます。機能ライセンスは、デバイス間で転送できません（ハードウェア障害の発生時を除く）。ハードウェア障害が発生したためにデバイスを交換する必要があり、このことが Cisco TAC によってカバーされている場合は、シスコのライセンス チームに連絡して、既存のライセンスを新しいシリアル番号に転送するよう依頼してください。シスコのライセンス チームから、製品認証キーの参照番号と既存のシリアル番号を求められます。
- ライセンシングで使うシリアル番号は、 **show version** 出力。このシリアル番号は、ハードウェアの外側に印刷されているシャーシのシリアル番号とは異なります。シャーシのシリアル番号は、テクニカル サポートで使用され、ライセンスには使用されません。
- 購入後に、返金またはアップグレードしたライセンスのためにライセンスを返却できません。
- 1 つのユニット上で、同じ機能の 2 つの別個のライセンスを加算することはできません。たとえば、25 セッション SSL VPN ライセンスを購入した後で 50 セッション ライセンスを購入しても、75 個のセッションを使用できるわけではなく、使用できるのは最大 50 個のセッションです。（アップグレード時に、数を増やしたライセンスを購入できることがあります。たとえば 25 セッションから 75 セッションへの増加です。このタイプのアップグレードは、2 つのライセンスの加算とは別のものです）。
- すべてのライセンス タイプをアクティブ化できますが、機能によっては、機能どうしの組み合わせができないものがあります。AnyConnect Essentials ライセンスの場合、次のライセンスとは互換性がありません。AnyConnect Premium ライセンス、AnyConnect Premium（共有）ライセンス、および Advanced Endpoint Assessment ライセンス。デフォルトでは、AnyConnect Essentials ライセンスをインストールした場合（使用中のモデルで利用できる場合）、このライセンスが前述のライセンスの代わりに使用されます。 **webvpn**、次に **no anyconnect-essentials** コマンドを使用して、設定で AnyConnect Essentials ライセンスを無効にし、他のライセンスを使用できます。

PAK ライセンスの設定

この項では、アクティベーションキーを取得する方法とそれをアクティブ化する方法について説明します。また、キーを非アクティブ化することもできます。

ライセンスの PAK の注文とアクティベーション キーの取得

ASA にライセンスをインストールするには製品認証キーが必要です。その後、それを Cisco.com に登録してアクティベーション キーを取得することができます。次に、ASA のアクティベーション キーを入力できます。機能ライセンスごとに個別の製品認証キーが必要になります。PAK が組み合わせられて、1 つのアクティベーションキーになります。デバイス発送時に、すべてのライセンス PAK が提供されている場合もあります。ASA には基本ライセンスまたは Security Plus ライセンスがプリインストールされ、ご使用資格を満たしている場合には Strong Encryption（3DES/AES）ライセンスも提供されます。無料の Strong Encryption ライセンスを手動でリクエストする必要がある場合は、http://www.cisco.com/go/license を参照してください。

始める前に

デバイスの 1 つ以上のライセンスを購入する場合は、Cisco Smart Software Manager で管理します。

https://software.cisco.com/#module/SmartLicensing

まだアカウントをお持ちでない場合は、このリンクをクリックして新しいアカウントをセットアップしてください。Smart Software Manager では、組織のマスター アカウントを作成できます。

手順

ステップ 1 追加ライセンスを購入するには、http://www.cisco.com/go/ccw を参照してください。次の AnyConnect 発注ガイドおよび FAQ を参照してください。

- 『Cisco AnyConnect Ordering Guide』
- AnyConnect Licensing Frequently Asked Questions (FAQ)

ライセンスを購入した後、製品認証キー（PAK）が記載された電子メールを受け取ります。AnyConnect ライセンスの場合、ユーザ セッションの同じプールを使用する複数の ASA に適用できるマルチユース PAK を受け取ります。場合によっては、PAK が記載された電子メールを受け取るまで数日かかることがあります。

ASA FirePOWER モジュールは、ASA とは別のライセンス メカニズムを使用します。詳しくは、ご使用のモデルのクイック スタート ガイドを参照してください。

ステップ 2 次のコマンドを入力して、ASA のシリアル番号を取得します。

show version | grep Serial

ライセンスに使用されるシリアル番号は、ハードウェアの外側に印刷されているシャーシのシリアル番号とは異なります。シャーシのシリアル番号は、テクニカルサポートで使用され、ライセンスには使用されません。

ステップ 3 アクティベーション キーを取得するには、以下のライセンス Web サイトに移動します。

http://www.cisco.com/go/license

ステップ 4 プロンプトが表示されたら、次の情報を入力します。

- Product Authorization Key（キーが複数ある場合は、まず 1 つを入力します。キーごとに個別のプロセスとして入力する必要があります）
- ASA のシリアル番号
- 電子メール アドレス

アクティベーション キーが自動的に生成され、指定した電子メールアドレスに送信されます。このキーには、永続ライセンス用にそれまでに登録した機能がすべて含まれています。時間ベース ライセンスの場合は、ライセンスごとに個別のアクティベーション キーがあります。

ステップ 5 さらに追加の製品認証キーがある場合は、製品認証キーごとにこの手順を繰り返します。すべての Product Authorization Key を入力した後、最後に送信されるアクティベーション キーには、登録した永続機能がすべて含まれています。

ステップ 6 キーのアクティブ化または非アクティブ化 （77 ページ）に基づいて、アクティベーション キーをインストールします。

高度暗号化ライセンスの取得

ASDM（および他の多数の機能）を使用するには、高度暗号化（3DES/AES）ライセンスをインストールする必要があります。ASA に高度暗号化ライセンスがプリインストールされていない場合は、ライセンスを無料で入手できます。高度暗号化ライセンスに関するそれぞれ国の資格を満たす必要があります。

手順

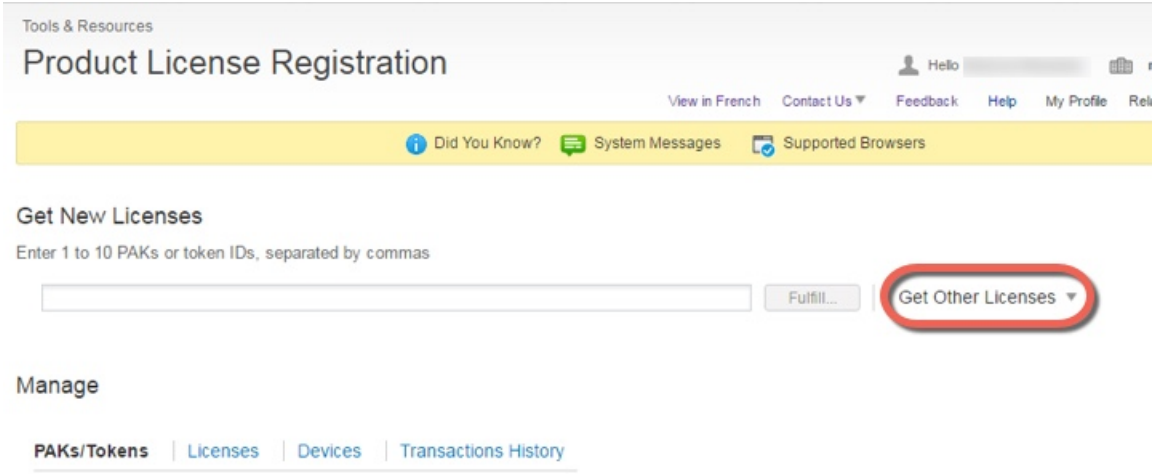
ステップ 1 次のコマンドを入力して、ASA のシリアル番号を取得します。

show version | grep Serial

このシリアル番号は、ハードウェアの外側に印刷されているシャーシのシリアル番号とは異なります。シャーシのシリアル番号は、テクニカルサポートで使用され、ライセンスには使用されません。

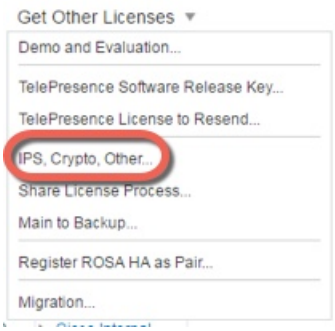
ステップ 2 Https://www.cisco.com/go/license を参照し、**[Get Other Licenses]** をクリックしてください。

図 *1*：他のライセンスの取得



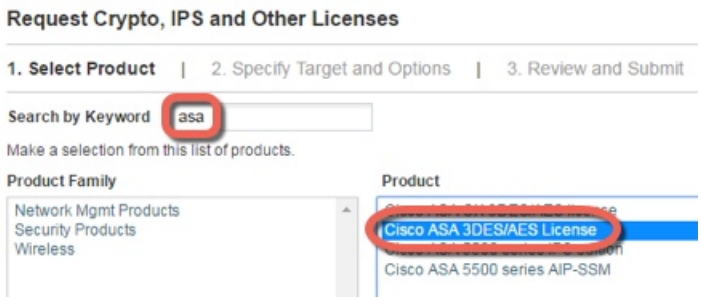
ステップ 3 [IPS, Crypto, Other] を選択します。

図 *2*：*IPS*、*Crypto*、その他



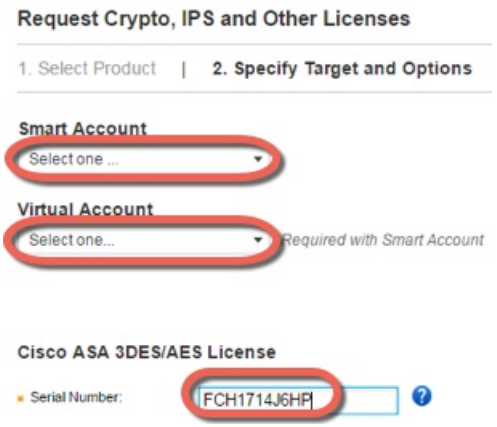
ステップ 4 [Search by Keyword] フィールドに **asa** と入力し、[Cisco ASA 3DES/AES License] を選択します。

図 *3*：*Cisco ASA 3DES/AES* ライセンス



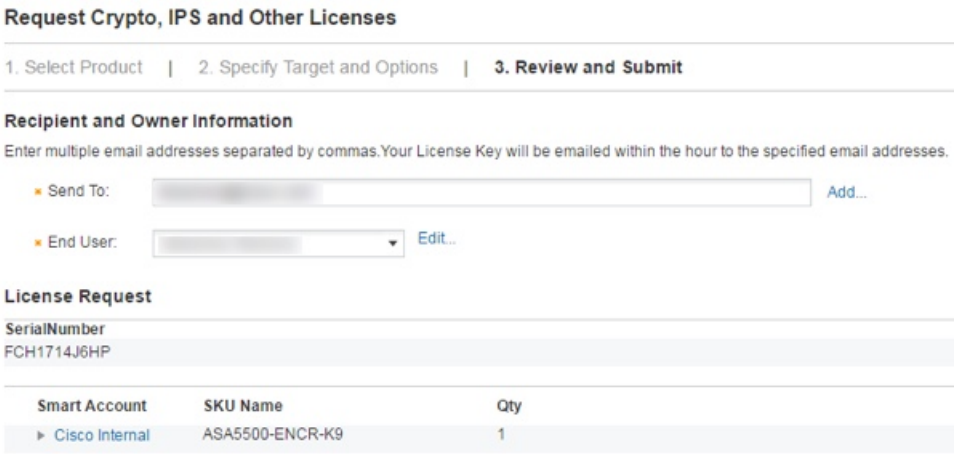
ステップ 5 [Smart Acfcount] 、[Virtual Account] を選択し、ASA の [Serial Number] を入力して、[Next] をクリックします。

図 *4*：スマート アカウント、バーチャル アカウント、シリアル番号



ステップ 6 送信先の電子メールアドレスとエンドユーザ名は自動的に入力されます。必要に応じて追加の電子メール アドレスを入力します。[I Agree] チェックボックスをオンにして、[Submit] をクリックします。

図 *5*：送信



ステップ 7 その後、アクティベーション キーの記載された電子メールが届きますが、**[Manage]** > **[Licenses]** エリアからキーをすぐにダウンロードすることもできます。

ステップ 8 キーのアクティブ化または非アクティブ化（77 ページ）に基づいて、アクティベーションキーを適用します。

キーのアクティブ化または非アクティブ化

この項では、新しいアクティベーション キーの入力と、時間ベース キーのアクティブ化および非アクティブ化の方法について説明します。

始める前に

- すでにマルチ コンテキスト モードに入っている場合は、システム実行スペースにこのアクティベーション キーを入力します。
- 一部の永続ライセンスでは、アクティブ化後に ASA をリロードする必要があります。次の表に、リロードが必要なライセンスを示します。

表 *2:* 永続ライセンスのリロード要件

モデル	リロードが必要なライセンス アクション
すべてのモデル	暗号化ライセンスのダウングレード

手順

ステップ 1 アクティベーション キーを ASA に適用します。

activation-key *key* [**activate** | **deactivate**]

例：

```
ciscoasa# activation-key 0xd11b3d48 0xa80a4c0a 0x48e0fd1c 0xb0443480 0x843fc490
```

キーは、5 つのエレメントからなる 16 進文字列です。各エレメントは 1 つのスペースで区切られます。先頭の 0x 指定子は任意です。すべての値が 16 進数と見なされます。

1 つの永続キーおよび複数の時間ベース キーをインストールできます。新しい永続キーを入力した場合、すでにインストール済みのキーが上書きされます。

activate および **deactivate** キーワードは、時間ベース キーだけに使用できます。値を入力しない場合は、**activate** がデフォルトです。特定の機能に対して最後にアクティブ化した時間ベース キーがアクティブになります。アクティブな時間ベース キーを非アクティブにするには、**deactivate** キーワードを入力します。キーの初回入力時で、**deactivate** を指定した場合、キーは ASA に非アクティブ ステートでインストールされます。

ステップ 2 （場合によって必須）ASA をリロードします。

reload

永続ライセンスによっては、新しいアクティベーション キーの入力後に ASA をリロードする必要があります。リロードが必要な場合は、次のメッセージが表示されます。

```
WARNING: The running activation key was not updated with the requested key.
The flash activation key was updated with the requested key, and will become
active after the next reload.
```

関連トピック

時間ベース ライセンス （58 ページ）

共有ライセンスの設定（AnyConnect 3 以前）

（注） ASAの共有ライセンス機能は、AnyConnect 4 以降のライセンスではサポートされていません。AnyConnect ライセンスが共有されているため、共有サーバまたは参加ライセンスは不要になりました。

この項では、共有ライセンス サーバと参加システムを設定する方法について説明します。

共有ライセンスについて

共有ライセンスを使用すると、多数の AnyConnect Premium セッションを購入し、それらのセッションを ASA のグループ間で必要に応じて共有できます。そのためには、いずれかの ASA を共有ライセンス サーバとして、残りを共有ライセンス参加システムとして設定します。

共有ライセンスのサーバと参加システムについて

次に、共有ライセンスの動作手順を示します。

1. いずれの ASA を共有ライセンス サーバとするかを決定し、デバイス シリアル番号を使用する共有ライセンス サーバのライセンスを購入します。
2. いずれの ASA を共有ライセンス バックアップ サーバを含む共有ライセンス参加者とするかを決定し、各デバイス シリアル番号を使用して各デバイスに対して共有ライセンス参加ライセンスを取得します。
3. （オプション）別の ASA を共有ライセンス バックアップ サーバとして指定します。バックアップ サーバには 1 台のみ指定できます。

（注） 共有ライセンス バックアップ サーバに必要なのは参加ライセンスのみです。

4. 共有ライセンス サーバ上に共有秘密を設定します。共有秘密を保持する参加者であればいずれも共有ライセンスを使用できます。
5. ASA を参加者として設定する場合、ローカル ライセンスおよびモデル情報を含む自身の情報を送信することで共有ライセンス サーバに登録します。

（注） 参加者は IP ネットワークを経由してサーバと通信できる必要がありますが、同じサブネット上にある必要はありません。

6. 共有ライセンス サーバは、参加者がサーバにポーリングするべき頻度の情報で応答します。
7. 参加者がローカル ライセンスのセッションを使い果たした場合、参加者は共有ライセンス サーバに 50 セッション単位で追加セッションの要求を送信します。
8. 共有ライセンス サーバは、共有ライセンスで応答します。1 台の参加者が使用する合計セッション数は、プラットフォーム モデルの最大セッション数を超えられません。

（注） 共有ライセンス サーバは、共有ライセンス プールに参加することもできます。参加には参加ライセンスもサーバ ライセンスも必要ありません。

   1. 参加者に対して共有ライセンス プールに十分なセッションがない場合、サーバは使用可能な限りのセッション数で応答します。
   2. 参加者はさらなるセッションを要求するリフレッシュ メッセージの送信をサーバが要求に適切に対応できるまで続けます。

9. 参加者の負荷が減少した場合、参加者はサーバに共有セッションを解放するようにメッセージを送信します。

（注） ASA は、サーバと参加者間のすべての通信の暗号化に SSL を使用します。

参加者とサーバの間の通信問題

参加者とサーバ間の通信問題については、次のガイドラインを参照してください。

- 参加者が更新の送信に失敗して更新間隔 3 倍の時間が経過した後で、サーバはセッションを解放して共有ライセンス プールに戻します。
- 参加者が更新を送信するためにライセンス サーバに到達できない場合、参加者はサーバから受信した共有ライセンスを最大 24 時間使用し続けられます。
- 24 時間を経過しても参加者がまだライセンス サーバと通信できない場合、参加者はセッションがまだ必要であっても共有ライセンスを解放します。参加者は既存の確立している接続を維持しますが、ライセンス制限を超えて新しい接続を受け入れられません。
- 参加者が 24 時間経過前にサーバに再接続したが、サーバが参加セッションを期限切れにした後である場合、参加者はセッションに対する新しい要求を送信する必要があります。サーバは、参加者に再割り当てできる限りのセッション数で応答します。

共有ライセンス バックアップ サーバについて

共有ライセンス バックアップ サーバは、バックアップの役割を実行する前にメインの共有ライセンス サーバへの登録に成功している必要があります。登録時には、メインの共有ライセン

スサーバは共有ライセンス情報に加えてサーバ設定もバックアップと同期します。情報には、登録済み参加者の一覧および現在のライセンス使用状況が含まれます。メインサーバとバックアップ サーバは、10 秒間隔でデータを同期します。初回同期の後で、バックアップ サーバはリロード後でもバックアップの役割を実行できます。

メインサーバがダウンすると、バックアップサーバがサーバ動作を引き継ぎます。バックアップサーバは継続して最大30日間動作できます。30日を超えると、バックアップ サーバは参加者へのセッション発行を中止し、既存のセッションはタイムアウトします。メインサーバをこの 30 日間中に確実に復旧するようにします。クリティカル レベルの syslog メッセージが 15 日めに送信され、30 日めに再送信されます。

メイン サーバが復旧した場合、メイン サーバはバックアップ サーバと同期してから、サーバ動作を引き継ぎます。

バックアップ サーバがアクティブでないときは、メインの共有ライセンス サーバの通常の参加者として動作します。

（注） メインの共有ライセンス サーバの初回起動時には、バックアップ サーバは独立して 5 日間のみ動作できます。動作制限は 30 日に到達するまで日ごとに増加します。また、メイン サーバがその後短時間でもダウンした場合、バックアップサーバの動作制限は日ごとに減少します。メイン サーバが復旧した場合、バックアップ サーバは再び日ごとに増加を開始します。たとえば、メインサーバが20日間ダウンしていて、その期間中バックアップサーバがアクティブであった場合、バックアップ サーバには、10 日間の制限のみが残っています。バックアップサーバは、非アクティブなバックアップとしてさらに20日間が経過した後で、最大の30日間まで「充電」されます。この充電機能は共有ライセンスの誤使用を防ぐために実装されています。

フェールオーバーと共有ライセンス

ここでは、共有ライセンスとフェールオーバーの相互作用について説明します。

フェールオーバーと共有ライセンス サーバ

この項では、メイン サーバおよびバックアップ サーバと、フェールオーバーとの相互作用について説明します。共有ライセンスサーバでは、VPNゲートウェイやファイアウォールなど、ASA としての通常機能も実行されます。このため、メインとバックアップの共有ライセンスサーバにフェールオーバーを設定して、信頼性を高めることをお勧めします。

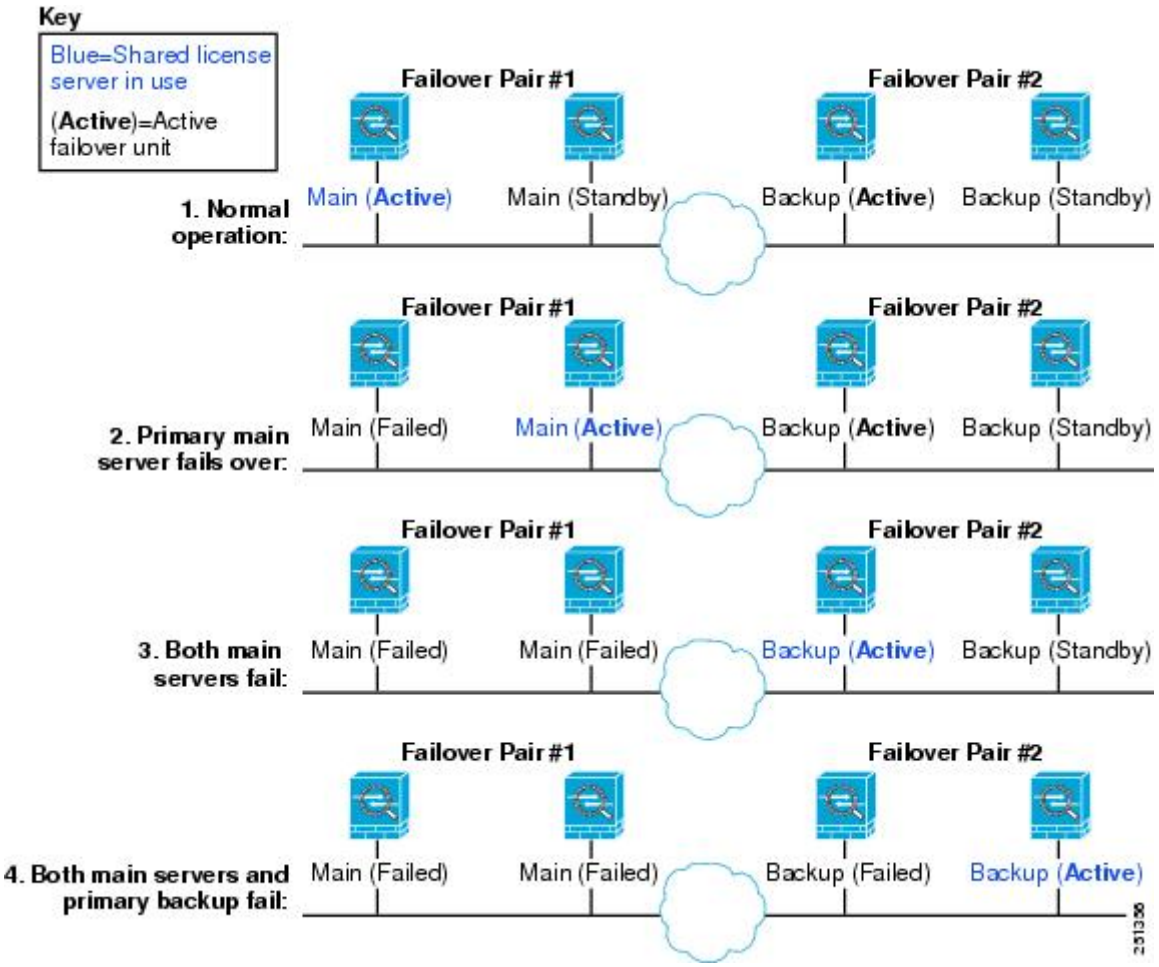
（注） バックアップ サーバ メカニズムとフェールオーバーは異なりますが、両者には互換性があります。

共有ライセンスはシングル コンテキスト モードでだけサポートされるため、アクティブ/アクティブ フェールオーバーはサポートされません。

アクティブ/スタンバイ フェールオーバーでは、プライマリ装置が主要な共有ライセンス サーバとして機能し、スタンバイ装置はフェールオーバー後に主要な共有ライセンス サーバとして機能します。スタンバイ装置は、バックアップの共有ライセンス サーバとしては機能しません。必要に応じて、バックアップ サーバとして機能する装置のペアを追加します。

たとえば、2 組のフェールオーバー ペアがあるネットワークを使用するとします。ペア #1 にはメインのライセンス サーバが含まれます。ペア #2 にはバックアップ サーバが含まれます。ペア #1 のプライマリ装置がダウンすると、ただちに、スタンバイ装置が新しくメイン ライセンス サーバになります。ペア #2 のバックアップ サーバが使用されることはありません。ペア #1 の装置が両方ともダウンした場合だけ、ペア #2 のバックアップ サーバが共有ライセンス サーバとして使用されるようになります。ペア #1 がダウンしたままで、ペア #2 のプライマリ装置もダウンした場合は、ペア #2 のスタンバイ装置が共有ライセンス サーバとして使用されるようになります（次の図を参照）。

図 *6:* フェールオーバーと共有ライセンス サーバ



スタンバイ バックアップ サーバは、プライマリ バックアップ サーバと同じ動作制限を共有します。スタンバイ装置がアクティブになると、その時点からプライマリ装置のカウントダウンを引き継ぎます。

関連トピック

共有ライセンス バックアップ サーバについて （80 ページ）

フェールオーバーと共有ライセンス参加システム

参加システムのペアについては、両方の装置を共有ライセンス サーバに登録します。登録時には、個別の参加システム ID を使用します。アクティブ装置の参加システム ID は、スタンバイ装置と同期されます。スタンバイ装置は、アクティブに切り替わるときに、この ID を使用して転送要求を生成します。この転送要求によって、以前にアクティブだった装置から新しくアクティブになる装置に共有セッションが移動します。

参加者の最大数

ASA では、共有ライセンスの参加システム数に制限がありません。ただし、共有ネットワークの規模が非常に大きいと、ライセンス サーバのパフォーマンスに影響する場合があります。この場合は、参加システムのリフレッシュ間隔を長くするか、共有ネットワークを 2 つ作成することをお勧めします。

共有ライセンス サーバの設定

この項では、ASA を共有ライセンス サーバとして設定する方法について説明します。

始める前に

サーバが共有ライセンス サーバ キーを持っている必要があります。

手順

ステップ 1 共有秘密を設定します。

license-server secret *secret*

例：

```
ciscoasa(config)# license-server secret farscape
```

secret は、4 ～ 128 文字の ASCII 文字の文字列です。この秘密を持つ参加システムが、ライセンス サーバを使用できます。

ステップ 2 （オプション）更新間隔を設定します。

license-server refresh-interval *seconds*

例：

```
ciscoasa(config)# license-server refresh-interval 100
```

間隔は 10 ～ 300 秒です。この値が、サーバと通信する頻度として参加システムに設定されます。デフォルトは 30 秒です。

ステップ 3 （オプション）サーバが参加ユニットからの SSL 接続をリッスンするポートを設定します。

license-server port *port*

例：

```
ciscoasa(config)# license-server port 40000
```

port は 1 ～ 65535 です。デフォルトは、TCP ポート 50554 です。

ステップ 4 （オプション）バックアップ サーバの IP アドレスとシリアル番号を指定します。

license-server backup *address* **backup-id** *serial_number* [**ha-backup-id** *ha_serial_number*]

例：

```
ciscoasa(config)# license-server backup 10.1.1.2 backup-id JMX0916L0Z4 ha-backup-id
JMX1378N0W3
```

バックアップ サーバがフェールオーバー ペアの一部である場合は、スタンバイ装置のシリアル番号も指定します。1つのバックアップ サーバとそのオプションのスタンバイ ユニットのみを指定できます。

ステップ 5 このユニットを共有ライセンス サーバとしてイネーブルにします。

license-server enable *interface_name*

例：

```
ciscoasa(config)# license-server enable inside
```

参加システムがサーバと通信するインターフェイスを指定します。このコマンドは必要なインターフェイスの数だけ繰り返せます。

例

次に、共有秘密を設定し、更新間隔とポートを変更し、バックアップ サーバを設定し、このユニットを inside インターフェイスおよび dmz インターフェイスで共有ライセンス サーバとしてイネーブルにする例を示します。

```
ciscoasa(config)# license-server secret farscape
ciscoasa(config)# license-server refresh-interval 100
ciscoasa(config)# license-server port 40000
ciscoasa(config)# license-server backup 10.1.1.2 backup-id JMX0916L0Z4 ha-backup-id
JMX1378N0W3
ciscoasa(config)# license-server enable inside
ciscoasa(config)# license-server enable dmz
```

共有ライセンス バックアップ サーバの設定（オプション）

この項では、共有ライセンスのメイン サーバがダウンした場合にバックアップ サーバとして機能する参加システムをイネーブルにします。

始める前に

バックアップ サーバには、共有ライセンス参加キーが必要です。

手順

ステップ 1 共有ライセンス サーバの IP アドレスと共有秘密を指定します。

license-server address *address* **secret** *secret* [**port** *port*]

例：

```
ciscoasa(config)# license-server address 10.1.1.1 secret farscape
```

デフォルト ポートをサーバ コンフィギュレーションで変更した場合は、同じポートをバックアップ サーバにも設定します。

ステップ 2 このユニットを共有ライセンス バックアップ サーバとしてイネーブルにします。

license-server backup enable *interface_name*

例：

```
ciscoasa(config)# license-server backup enable inside
```

参加システムがサーバと通信するインターフェイスを指定します。このコマンドは必要なインターフェイスの数だけ繰り返せます。

例

次に、ライセンス サーバと共有秘密を指定し、このユニットを内部インターフェイスとdmzインターフェイス上のバックアップ共有ライセンス サーバとしてイネーブルにする例を示します。

```
ciscoasa(config)# license-server address 10.1.1.1 secret farscape
ciscoasa(config)# license-server backup enable inside
ciscoasa(config)# license-server backup enable dmz
```

共有ライセンス パーティシパントの設定

この項では、共有ライセンス サーバと通信する共有ライセンス参加システムを設定します。

始める前に

参加システムが共有ライセンス参加キーを持っている必要があります。

手順

ステップ 1 共有ライセンス サーバの IP アドレスと共有秘密を指定します。

license-server address *address* **secret** *secret* [**port** *port*]

例：

```
ciscoasa(config)# license-server address 10.1.1.1 secret farscape
```

デフォルト ポートをサーバ コンフィギュレーションで変更した場合は、同じポートを参加システムにも設定します。

ステップ 2 （オプション）バックアップ サーバを設定した場合は、バックアップ サーバのアドレスを入力します。

license-server backup address *address*

例：

```
ciscoasa(config)# license-server backup address 10.1.1.2
```

例

次に、ライセンス サーバの IP アドレスおよび共有秘密、ならびにバックアップ ライセンス サーバの IP アドレスの設定例を示します。

```
ciscoasa(config)# license-server address 10.1.1.1 secret farscape
ciscoasa(config)# license-server backup address 10.1.1.2
```

モデルごとにサポートされている機能のライセンス

この項では、各モデルに使用できるライセンスと、ライセンスに関する特記事項について説明します。

モデルごとのライセンス

この項では、各モデルに使用できる機能のライセンスを示します。

イタリック体で示された項目は、基本ライセンス（または Security Plus など）ライセンス バージョンを置換できる個別のオプション ライセンスです。オプション ライセンスは、混在させることも統一することもできます。

（注） 一部の機能は互換性がありません。互換性情報については、個々の機能の章を参照してください。

ペイロード暗号化機能のないモデルの場合は、次に示す機能の一部がサポートされません。サポートされない機能のリストについては、ペイロード暗号化機能のないモデル （70 ページ）を参照してください。

ライセンスの詳細については、ライセンスに関する注意事項 （61 ページ）を参照してください。

ASA 5506-X および ASA 5506W-X のライセンス機能

次の表に、ASA 5506-X および ASA 5506W-X のライセンス機能を示します。

ライセンス	基本ライセンス	Security Plus ライセンス
ファイアウォール ライセンス		
Botnet Traffic Filter	サポートなし	サポートなし （注） ライセンス情報は、このライセンスが有効になっていることを示すことがあります。このライセンスがサポートされていないため、ディスプレイは無視するべきです。
ファイアウォールの接続、同時	20,000	50,000
GTP/GPRS	サポートなし	サポートなし

ライセンス	基本ライセンス		Security Plus ライセンス	
合計 UC プロキシセッション	160		160	
VPN ライセンス				
AnyConnect ピア	ディセーブル	オプションの *AnyConnect Plus* または *Apex* ライセンス：最大 *50*	ディセーブル	オプションの *AnyConnect Plus* または *Apex* ライセンス：最大 *50*
その他の VPN ピア	10		50	
合計 VPN ピア。全タイプの合計	50		50	
VPN ロードバランシング	サポートなし		サポートなし	
一般ライセンス				
暗号化	基本（DES）	オプション ライセンス：強化（*3DES/AES*）	基本（DES）	オプション ライセンス：強化（*3DES/AES*）
フェールオーバー	サポートなし		アクティブ/スタンバイ	
セキュリティコンテキスト	サポートなし		サポートなし	
クラスタ	サポートなし		サポートなし	
VLAN、最大	5		30	

ASA 5506H-X ライセンスの各機能

次の表に、ASA 5506H-X のライセンス機能を示します。

ライセンス	基本ライセンス	
ファイアウォール ライセンス		
Botnet Traffic Filter	サポートなし （注） ライセンス情報は、このライセンスが有効になっていることを示すことがあります。このライセンスがサポートされていないため、ディスプレイは無視するべきです。	
ファイアウォールの接続、同時	50,000	
GTP/GPRS	サポートなし	
合計 UC プロキシ セッション	160	
VPN ライセンス		
AnyConnect Plus または Apex ライセンス（個別に購入）、最大プレミアム ピア	50	
合計 VPN ピア。全タイプの合計	50	
その他の VPN ピア	50	
VPN ロード バランシング	イネーブル	
一般ライセンス		
暗号化	基本（DES）	オプション ライセンス：強化（*3DES/AES*）
フェールオーバー	Active/Standby または Active/Active	
セキュリティ コンテキスト	サポートなし	

ライセンス	基本ライセンス
クラスタ	サポートなし
VLAN、最大	30

ASA 5508-X ライセンスの各機能

次の表に、ASA 5508-X のライセンス機能を示します。

ライセンス	基本ライセンス	
ファイアウォール ライセンス		
Botnet Traffic Filter	サポートなし （注） ライセンス情報は、このライセンスが有効になっていることを示すことがあります。このライセンスがサポートされていないため、ディスプレイは無視するべきです。	
ファイアウォールの接続、同時	100,000	
GTP/GPRS	サポートなし	
合計 UC プロキシ セッション	320	
VPN ライセンス		
AnyConnect ピア	ディセーブル	オプションの *AnyConnect Plus* または *Apex* ライセンス：最大 *100*
合計 VPN ピア。全タイプの合計	100	
その他の VPN ピア	100	
VPN ロード バランシング	イネーブル	
一般ライセンス		
暗号化	基本（DES）	オプション ライセンス：強化（*3DES/AES*）
フェールオーバー	Active/Standby または Active/Active	

ライセンス	基本ライセンス		
セキュリティ コンテキスト	2	オプション ライセンス：	*5*
クラスタ	サポートなし		
VLAN、最大	50		

ASA 5512-X ライセンスの機能

次の表に、ASA 5512-X のライセンス機能を示します。

ライセンス	基本ライセンス					Security Plus ライセンス					
ファイアウォール ライセンス											
Botnet Traffic Filter	ディセーブル	オプションの時間ベース ライセンス：使用可能				ディセーブル	オプションの時間ベース ライセンス：使用可能				
ファイアウォールの接続、同時	100,000					250,000					
GTP/GPRS	サポートなし					サポートなし					
合計 UC プロキシ セッション	2	オプション ライセンス：				2	オプション ライセンス：				
		24	*50*	*100*	*250*	*500*	*24*	*50*	*100*	*250*	*500*
VPN ライセンス											
AnyConnect ピア	ディセーブル	オプションの *AnyConnect Plus* または *Apex* ライセンス：最大 *250*				ディセーブル	オプションの *AnyConnect Plus* または *Apex* ライセンス：最大 *250*				
その他の VPN ピア	250					250					

ライセンス	基本ライセンス		Security Plus ライセンス	
合計 VPN ピア。全タイプの合計	250		250	
VPN ロードバランシング	サポートなし		イネーブル	
一般ライセンス				
暗号化	基本（DES）	オプション ライセンス：強化（*3DES/AES*）	基本（DES）	オプション ライセンス：強化（*3DES/AES*）
フェールオーバー	サポートなし		Active/Standby または Active/Active	
セキュリティ コンテキスト	サポートなし		2	オプション ライセンス：*5*
クラスタ	サポートなし		2	
IPS モジュール	ディセーブル	オプション ライセンス：使用可能	ディセーブル	オプション ライセンス：使用可能
VLAN、最大	50		100	

ASA 5515-X ライセンスの機能

次の表に、ASA 5515-X のライセンス機能を示します。

ライセンス	基本ライセンス
ファイアウォール ライセンス	

ライセンス	基本ライセンス						
Botnet Traffic Filter	ディセーブル	オプションの時間ベース ライセンス：使用可能					
ファイアウォールの接続、同時	250,000						
GTP/GPRS	サポートなし						
合計 UC プロキシ セッション	2	オプション ライセンス：	*24*	*50*	*100*	*250*	*500*
VPN ライセンス							
AnyConnect ピア	ディセーブル	オプションの *AnyConnect Plus* または *Apex* ライセンス：最大 *250*					
その他の VPN ピア	250						
合計 VPN ピア。全タイプの合計	250						
VPN ロードバランシング	イネーブル						
一般ライセンス							
暗号化	基本（DES）	オプション ライセンス：強化（*3DES/AES*）					
フェールオーバー	Active/Standby または Active/Active						

ライセンス	基本ライセンス		
セキュリティコンテキスト	2	オプション ライセンス：	*5*
クラスタ	2		
IPS モジュール	ディセーブル	オプション ライセンス：使用可能	
VLAN、最大	100		

ASA 5516-X ライセンスの機能

次の表に、ASA 5516-X のライセンス機能を示します。

ライセンス	基本ライセンス	
ファイアウォール ライセンス		
Botnet Traffic Filter	サポートなし （注） ライセンス情報は、このライセンスが有効になっていることを示すことがあります。このライセンスがサポートされていないため、ディスプレイは無視するべきです。	
ファイアウォールの接続、同時	250,000	
GTP/GPRS	サポートなし	
合計 UC プロキシ セッション	1000	
VPN ライセンス		
AnyConnect ピア	ディセーブル	オプションの *AnyConnect Plus* または *Apex* ライセンス：最大 *300*
その他の VPN ピア	300	

ライセンス	基本ライセンス		
合計 VPN ピア。全タイプの合計	300		
VPN ロードバランシング	イネーブル		
一般ライセンス			
暗号化	基本（DES）	オプション ライセンス：強化（*3DES/AES*）	
フェールオーバー	Active/Standby または Active/Active		
セキュリティ コンテキスト	2	オプション ライセンス：	*5*
クラスタ	サポートなし		
VLAN、最大	150		

ASA 5525-X ライセンスの各機能

次の表に、ASA 5525-X のライセンス機能を示します。

ライセンス	基本ライセンス	
ファイアウォール ライセンス		
Botnet Traffic Filter	ディセーブル	オプションの時間ベース ライセンス：使用可能
ファイアウォールの接続、同時	500,000	
GTP/GPRS	ディセーブル	オプション ライセンス：使用可能

ライセンス	基本ライセンス								
合計 UC プロキシセッション	2	オプション ライセンス：	*24*	*50*	*100*	*250*	*500*	*750*	*1000*
VPN ライセンス									
AnyConnect ピア	ディセーブル	オプションの *AnyConnect Plus* または *Apex* ライセンス：最大 *750*							
その他の VPN ピア	750								
合計 VPN ピア。全タイプの合計	750								
VPN ロードバランシング	イネーブル								
一般ライセンス									
暗号化	基本（DES）	オプション ライセンス：強化（*3DES/AES*）							
フェールオーバー	Active/Standby または Active/Active								
セキュリティコンテキスト	2	オプション ライセンス：	*5*	*10*	*20*				
クラスタ	2								
IPS モジュール	ディセーブル	オプション ライセンス：使用可能							

ライセンス	基本ライセンス
VLAN、最大	200

ASA 5545-X ライセンスの機能

次の表に、ASA 5545-X のライセンス機能を示します。

ライセンス	基本ライセンス								
ファイアウォール ライセンス									
Botnet Traffic Filter	ディセーブル	オプションの時間ベース ライセンス：使用可能							
ファイアウォールの接続、同時	750,000								
GTP/GPRS	ディセーブル	オプション ライセンス：使用可能							
合計 UC プロキシ セッション	2	オプション ライセンス：	*24*	*50*	*100*	*250*	*500*	*750*	*1000*	*2000*
VPN ライセンス									
AnyConnect ピア	ディセーブル	オプションの *AnyConnect Plus* または *Apex* ライセンス：最大 *2500*							
その他の VPN ピア	2500								
合計 VPN ピア。全タイプの合計	2500								

ライセンス	基本ライセンス					
VPN ロードバランシング	イネーブル					
一般ライセンス						
暗号化	基本（DES）	オプション ライセンス：強化（*3DES/AES*）				
フェールオーバー	Active/Standby または Active/Active					
セキュリティコンテキスト	2	オプション ライセンス：	*5*	*10*	*20*	*50*
クラスタ	2					
IPS モジュール	ディセーブル	オプション ライセンス：使用可能				
VLAN、最大	300					

ASA 5555-X ライセンスの機能

次の表に、ASA 5555-X のライセンス機能を示します。

ライセンス	基本ライセンス	
ファイアウォール ライセンス		
Botnet Traffic Filter	ディセーブル	オプションの時間ベース ライセンス：使用可能

ライセンス	基本ライセンス								
ファイアウォールの接続、同時	1,000,000								
GTP/GPRS	ディセーブル	オプション ライセンス：使用可能							
合計 UC プロキシセッション	2	オプション ライセンス：							
		24	*50*	*100*	*250*	*500*	*750*	*1000*	*2000*	*3000*
VPN ライセンス									
AnyConnect ピア	ディセーブル	オプションの *AnyConnect Plus* または *Apex* ライセンス：最大 *5000*							
その他の VPN ピア	5000								
合計 VPN ピア。全タイプの合計	5000								
VPN ロードバランシング	イネーブル								
一般ライセンス									
暗号化	基本（DES）	オプション ライセンス：強化（*3DES/AES*）							
フェールオーバー	Active/Standby または Active/Active								

ライセンス	基本ライセンス						
セキュリティ コンテキスト	2	オプション ライセンス：	*5*	*10*	*20*	*50*	*100*
クラスタ	2						
IPS モジュール	ディセーブル	オプション ライセンス：使用可能					
VLAN、最大	500						

ASA 5585-X（SSP-10）ライセンスの各機能

次の表に、ASA 5585-X（SSP-10）のライセンス機能を示します。

同一のシャーシで同じレベルの 2 つの SSP を使用できます。レベルが混在した SSP はサポートされていません（たとえば、SSP-10 と SSP-20 の組み合わせはサポートされていません）。各 SSP は個別のコンフィギュレーションおよび管理を持つ独立したデバイスとして動作します。必要に応じて 2 つの SSP をフェールオーバー ペアとして使用できます。

ライセンス	基本ライセンスと Security Plus ライセンス	
ファイアウォール ライセンス		
Botnet Traffic Filter	ディセーブル	オプションの時間ベース ライセンス：使用可能
ファイアウォールの接続、同時	1,000,000	
GTP/GPRS	ディセーブル	オプション ライセンス：使用可能

ライセンス	基本ライセンスと Security Plus ライセンス								
合計 UC プロキシセッション	2	オプション ライセンス：							
		24	*50*	*100*	*250*	*500*	*750*	*1000*	*2000*	*3000*
VPN ライセンス									
AnyConnect ピア	ディセーブル	オプションの *AnyConnect Plus* または *Apex* ライセンス：最大 *5000*							
その他の VPN ピア	5000								
合計 VPN ピア。全タイプの合計	5000								
VPN ロードバランシング	イネーブル								
一般ライセンス									
10 GE I/O	**基本ライセンス**：ディセーブル。ファイバ ifcs は 1 GE で動作します					**Security Plus ライセンス**：イネーブル。ファイバ ifcs は 10 GE で動作します			
暗号化	基本（DES）	オプション ライセンス：強化（*3DES/AES*）							
フェールオーバー	Active/Standby または Active/Active								
セキュリティコンテキスト	2	オプション ライセンス：	*5*	*10*	*20*	*50*	*100*		
クラスタ	ディセーブル	オプション ライセンス*: 16* 単位で利用可能							

ライセンス	基本ライセンスと Security Plus ライセンス
VLAN、最大	1024

ASA 5585-X（SSP-20）ライセンスの機能

次の表に、ASA 5585-X（SSP-20）のライセンス機能を示します。

同一のシャーシで同じレベルの 2 つの SSP を使用できます。レベルが混在した SSP はサポートされていません（たとえば、SSP-20 と SSP-40 の組み合わせはサポートされていません）。各 SSP は個別のコンフィギュレーションおよび管理を持つ独立したデバイスとして動作します。必要に応じて 2 つの SSP をフェールオーバー ペアとして使用できます。

（注） 10,000 セッション UC ライセンスの場合、組み合わせたセッション数は合計 10,000 までですが、電話プロキシ セッションの最大数は 5000 です。

ライセンス	基本ライセンスと Security Plus ライセンス										
ファイアウォール ライセンス											
Botnet Traffic Filter	ディセーブル	オプションの時間ベース ライセンス：使用可能									
ファイアウォールの接続、同時	2,000,000										
GTP/GPRS	ディセーブル	オプション ライセンス：使用可能									
合計 UC プロキシ セッション	2	オプション ライセンス：									
		24	*50*	*100*	*250*	*500*	*750*	*1000*	*2000*	*3000*	*5000*	*10,000*
VPN ライセンス											
AnyConnect ピア	ディセーブル	オプションの *AnyConnect Plus* または *Apex* ライセンス：最大 *10,000*									

ライセンス	基本ライセンスと Security Plus ライセンス
その他の VPN ピア	10,000
合計 VPN ピア。全タイプの合計	10,000
VPN ロードバランシング	イネーブル

一般ライセンス

10 GE I/O	**基本ライセンス**：ディセーブル。ファイバ ifcs は 1 GE で動作します				**Security Plus ライセンス**：イネーブル。ファイバ ifcs は 10 GE で動作します			
暗号化	基本（DES）	オプション ライセンス：強化（*3DES/AES*）						
フェールオーバー	Active/Standby または Active/Active							
セキュリティ コンテキスト	2	オプション ライセンス：	*5*	*10*	*20*	*50*	*100*	*250*
クラスタ	ディセーブル	オプション ライセンス*: 16* 単位で利用可能						
VLAN、最大	1024							

ASA 5585-X（SSP-40 および -60）ライセンスの機能

次の表に、ASA 5585-X（SSP-40 および -60）のライセンス機能を示します。

同一のシャーシで同じレベルの 2 つの SSP を使用できます。レベルが混在した SSP はサポートされていません（たとえば、SSP-40 と SSP-60 の組み合わせはサポートされていません）。各 SSP は個別のコンフィギュレーションおよび管理を持つ独立したデバイスとして動作します。必要に応じて 2 つの SSP をフェールオーバー ペアとして使用できます。

（注） 10,000 セッション UC ライセンスの場合、組み合わせたセッション数は合計 10,000 までですが、電話プロキシ セッションの最大数は 5000 です。

ライセンス	基本ライセンス										
ファイアウォール ライセンス											
Botnet Traffic Filter	ディセーブル	オプションの時間ベース ライセンス：使用可能									
ファイアウォールの接続、同時	**5585-X（SSP-40）**：4,000,000					**5585-X（SSP-60）**：10,000,000					
GTP/GPRS	ディセーブル	オプション ライセンス：使用可能									
合計 UC プロキシ セッション	2	オプション ライセンス：									
		24	*50*	*100*	*250*	*500*	*750*	*1000*	*2000*	*3000*	*5000*	*10,000*
VPN ライセンス											
AnyConnect ピア	ディセーブル	オプションの *AnyConnect Plus* または *Apex* ライセンス：最大 *10,000*									
その他の VPN ピア	10,000										
合計 VPN ピア。全タイプの合計	10,000										
VPN ロードバランシング	イネーブル										

ライセンス	基本ライセンス							
一般ライセンス								
10 GE I/O	イネーブル。ファイバ インターフェイスは 10 GE で動作							
暗号化	基本（DES）	オプション ライセンス：強化（*3DES/AES*）						
フェールオーバー	Active/Standby または Active/Active							
セキュリティ コンテキスト	2	オプション ライセンス：	*5*	*10*	*20*	*50*	*100*	*250*
クラスタ	ディセーブル	オプション ライセンス*: 16* 単位で利用可能						
VLAN、最大	1024							

ASASM ライセンスの機能

次の表に、ASA サービス モジュールのライセンス機能を示します。

（注） 10,000 セッション UC ライセンスの場合、組み合わせたセッション数は合計 10,000 までですが、電話プロキシ セッションの最大数は 5000 です。

ライセンス	基本ライセンス	
ファイアウォール ライセンス		
Botnet Traffic Filter	ディセーブル	オプションの時間ベース ライセンス：使用可能

ライセンス	基本ライセンス										
ファイアウォールの接続、同時	10,000,000										
GTP/GPRS	ディセーブル	オプション ライセンス：使用可能									
合計 UC プロキシセッション	2	オプション ライセンス：									
		24	*50*	*100*	*250*	*500*	*750*	*1000*	*2000*	*3000*	*5000*	*10,000*
VPN ライセンス											
AnyConnect ピア	ディセーブル	オプションの *AnyConnect Plus* または *Apex* ライセンス：最大 *10,000*									
その他の VPN ピア	10,000										
合計 VPN ピア。全タイプの合計	10,000										
VPN ロードバランシング	イネーブル										
一般ライセンス											
暗号化	基本（DES）	オプション ライセンス：強化（*3DES/AES*）									
フェールオーバー	Active/Standby または Active/Active										

ライセンス	基本ライセンス					
セキュリティコンテキスト	2	オプション ライセンス：				
		5	*10*	*20*	*50*	*100*	*250*
クラスタ	サポートなし					
VLAN、最大	1000					

ISA 3000 ライセンスの各機能

次の表に、ISA 3000 のライセンス機能を示します。

ライセンス	基本ライセンス		Security Plus ライセンス	
ファイアウォール ライセンス				
Botnet Traffic Filter	サポートなし		サポートなし	
ファイアウォールの接続、同時	20,000		50,000	
GTP/GPRS	サポートなし		サポートなし	
合計 UC プロキシセッション	160		160	
VPN ライセンス				
AnyConnect ピア	ディセーブル	オプションの *AnyConnect Plus* または *Apex* ライセンス：最大 *25*	ディセーブル	オプションの *AnyConnect Plus* または *Apex* ライセンス：最大 *25*

ライセンス	基本ライセンス		Security Plus ライセンス	
その他の VPN ピア	10		50	
合計 VPN ピア。全タイプの合計	25		50	
VPN ロードバランシング	サポートなし		サポートなし	
一般ライセンス				
暗号化	基本（DES）	オプション ライセンス：強化（*3DES/AES*）	基本（DES）	オプション ライセンス：強化（*3DES/AES*）
フェールオーバー	サポートなし		アクティブ/スタンバイ	
セキュリティ コンテキスト	サポートなし		サポートなし	
クラスタ	サポートなし		サポートなし	
VLAN、最大	5		25	

PAK ライセンスのモニタリング

この項では、ライセンス情報の表示方法について説明します。

現在のライセンスの表示

この項では、現在のライセンスと、時間ベース アクティベーション キーの残り時間を表示する方法について説明します。

始める前に

ペイロード暗号化機能のないモデルでライセンスを表示すると、VPN および Unified Communications ライセンスは一覧に示されません。詳細については、「ペイロード暗号化機能のないモデル （70 ページ）」を参照してください。

手順

永続ライセンス、アクティブな時間ベース ライセンス、および実行ライセンスを表示します。実行ライセンスとは、永続ライセンスとアクティブな時間ベース ライセンスの組み合わせです。

show activation-key [**detail**]

detail キーワードを使用すると、非アクティブな時間ベース ライセンスも表示されます。

フェールオーバーまたはクラスタ ユニットでは、このコマンドは、すべてのユニットの結合キーである「クラスタ」ライセンスも示します。

例

例 1：show activation-key コマンドのスタンドアロン ユニットの出力

次に、実行ライセンス（永続ライセンスと時間ベース ライセンスの組み合わせ）、およびアクティブな各時間ベース ライセンスを示す、スタンドアロン ユニットの **show activation-key** コマンドの出力例を示します。

```
ciscoasa# show activation-key

Serial Number:  JMX1232L11M
Running Permanent Activation Key: 0xce06dc6b 0x8a7b5ab7 0xa1e21dd4 0xd2c4b8b8 0xc4594f9c
Running Timebased Activation Key: 0xa821d549 0x35725fe4 0xc918b97b 0xce0b987b 0x47c7c285
Running Timebased Activation Key: 0xyadayad2 0xyadayad2 0xyadayad2 0xyadayad2 0xyadayad2

Licensed features for this platform:
Maximum Physical Interfaces       : Unlimited      perpetual
Maximum VLANs                     : 150            perpetual
Inside Hosts                      : Unlimited      perpetual
Failover                          : Active/Active  perpetual
VPN-DES                           : Enabled        perpetual
VPN-3DES-AES                      : Enabled        perpetual
Security Contexts                 : 10             perpetual
GTP/GPRS                          : Enabled        perpetual
AnyConnect Premium Peers          : 2              perpetual
AnyConnect Essentials             : Disabled       perpetual
Other VPN Peers                   : 750            perpetual
```

```
Total VPN Peers                   : 750           perpetual
Shared License                    : Enabled       perpetual
  Shared AnyConnect Premium Peers : 12000         perpetual
AnyConnect for Mobile             : Disabled      perpetual
AnyConnect for Cisco VPN Phone    : Disabled      perpetual
Advanced Endpoint Assessment      : Disabled      perpetual
UC Phone Proxy Sessions           : 12            62 days
Total UC Proxy Sessions           : 12            62 days
Botnet Traffic Filter             : Enabled       646 days
Intercompany Media Engine         : Disabled      perpetual

This platform has a Base license.

The flash permanent activation key is the SAME as the running permanent key.

Active Timebased Activation Key:
0xa821d549 0x35725fe4 0xc918b97b 0xce0b987b 0x47c7c285
Botnet Traffic Filter        : Enabled    646 days

0xyadayad2 0xyadayad2 0xyadayad2 0xyadayad2 0xyadayad2
Total UC Proxy Sessions      : 10         62 days
```

例 2：show activation-key detail のスタンドアロン ユニットの出力

次に、実行ライセンス（永続ライセンスと時間ベース ライセンスの組み合わせ）、および永続ライセンスとインストールされている各時間ベース ライセンス（アクティブおよび非アクティブ）を示す、スタンドアロン ユニットの **show activation-key detail** コマンドの出力例を示します。

```
ciscoasa# show activation-key detail

Serial Number:  88810093382
Running Permanent Activation Key: 0xce06dc6b 0x8a7b5ab7 0xa1e21dd4 0xd2c4b8b8 0xc4594f9c
Running Timebased Activation Key: 0xa821d549 0x35725fe4 0xc918b97b 0xce0b987b 0x47c7c285

Licensed features for this platform:
Maximum Physical Interfaces    : 8              perpetual
VLANs                          : 20             DMZ Unrestricted
Dual ISPs                      : Enabled        perpetual
VLAN Trunk Ports               : 8              perpetual
Inside Hosts                   : Unlimited      perpetual
Failover                       : Active/Standby perpetual
VPN-DES                        : Enabled        perpetual
VPN-3DES-AES                   : Enabled        perpetual
AnyConnect Premium Peers          : 2              perpetual
AnyConnect Essentials             : Disabled       perpetual
Other VPN Peers                   : 25             perpetual
Total VPN Peers                   : 25              perpetual
AnyConnect for Mobile             : Disabled       perpetual
AnyConnect for Cisco VPN Phone    : Disabled       perpetual
Advanced Endpoint Assessment      : Disabled       perpetual
UC Phone Proxy Sessions        : 2              perpetual
Total UC Proxy Sessions        : 2              perpetual
Botnet Traffic Filter          : Enabled        39 days
Intercompany Media Engine      : Disabled       perpetual

This platform has an ASA 5512-X Security Plus license.

Running Permanent Activation Key: 0xce06dc6b 0x8a7b5ab7 0xa1e21dd4 0xd2c4b8b8 0xc4594f9c

Licensed features for this platform:
```

```
Maximum Physical Interfaces    : 8              perpetual
VLANs                          : 20             DMZ Unrestricted
Dual ISPs                      : Enabled        perpetual
VLAN Trunk Ports               : 8              perpetual
Inside Hosts                   : Unlimited      perpetual
Failover                       : Active/Standby perpetual
VPN-DES                        : Enabled        perpetual
VPN-3DES-AES                   : Enabled        perpetual
AnyConnect Premium Peers          : 2              perpetual
AnyConnect Essentials             : Disabled       perpetual
Other VPN Peers                   : 25             perpetual
Total VPN Peers                   : 25              perpetual
AnyConnect for Mobile             : Disabled       perpetual
AnyConnect for Cisco VPN Phone    : Disabled       perpetual
Advanced Endpoint Assessment      : Disabled       perpetual
UC Phone Proxy Sessions        : 2              perpetual
Total UC Proxy Sessions        : 2              perpetual
Botnet Traffic Filter          : Enabled        39 days
Intercompany Media Engine      : Disabled       perpetual

The flash permanent activation key is the SAME as the running permanent key.

Active Timebased Activation Key:
0xa821d549 0x35725fe4 0xc918b97b 0xce0b987b 0x47c7c285
Botnet Traffic Filter           : Enabled    39 days

Inactive Timebased Activation Key:
0xyadayada3 0xyadayada3 0xyadayada3 0xyadayada3 0xyadayada3
AnyConnect Premium Peers                   : 25     7 days
```

例 3：show activation-key detail に対するフェールオーバー ペアのプライマリ ユニット出力

次に、プライマリ フェールオーバー ユニットの **show activation-key detail** コマンドの出力例を示します。

- プライマリ ユニット ライセンス（永続ライセンスと時間ベース ライセンスの組み合わせ）。
- プライマリおよびセカンダリ装置のライセンスの組み合わせである、「フェールオーバー クラスタ」ライセンス。これは、ASA で実際に実行されているライセンスです。プライマリおよびセカンダリ ライセンスの組み合わせを反映したこのライセンスの値は、太字になっています。
- プライマリ ユニットの永続ライセンス。
- プライマリ ユニットのインストール済みの時間ベース ライセンス（アクティブおよび非アクティブ）。

```
ciscoasa# show activation-key detail

Serial Number:  P3000000171
Running Permanent Activation Key: 0xce06dc6b 0x8a7b5ab7 0xa1e21dd4 0xd2c4b8b8 0xc4594f9c
Running Timebased Activation Key: 0xa821d549 0x35725fe4 0xc918b97b 0xce0b987b 0x47c7c285

Licensed features for this platform:
Maximum Physical Interfaces    : Unlimited      perpetual
Maximum VLANs                  : 150            perpetual
```

```
Inside Hosts                  : Unlimited      perpetual
Failover                      : Active/Active  perpetual
VPN-DES                       : Enabled        perpetual
VPN-3DES-AES                  : Enabled        perpetual
Security Contexts             : 12             perpetual
GTP/GPRS                      : Enabled        perpetual
AnyConnect Premium Peers          : 2             perpetual
AnyConnect Essentials             : Disabled      perpetual
Other VPN Peers                   : 750           perpetual
Total VPN Peers                   : 750           perpetual
Shared License                    : Disabled       perpetual
AnyConnect for Mobile             : Disabled      perpetual
AnyConnect for Cisco VPN Phone    : Disabled      perpetual
Advanced Endpoint Assessment      : Disabled      perpetual
UC Phone Proxy Sessions       : 2              perpetual
Total UC Proxy Sessions       : 2              perpetual
Botnet Traffic Filter         : Enabled        33 days
Intercompany Media Engine     : Disabled       perpetual

This platform has an ASA 5520 VPN Plus license.

Failover cluster licensed features for this platform:
Maximum Physical Interfaces   : Unlimited      perpetual
Maximum VLANs                 : 150            perpetual
Inside Hosts                  : Unlimited      perpetual
Failover                      : Active/Active  perpetual
VPN-DES                       : Enabled        perpetual
VPN-3DES-AES                  : Enabled        perpetual
Security Contexts             : 12             perpetual
GTP/GPRS                      : Enabled        perpetual
AnyConnect Premium Peers      : 4           perpetual
AnyConnect Essentials             : Disabled      perpetual
Other VPN Peers                   : 750           perpetual
Total VPN Peers                   : 750           perpetual
Shared License                    : Disabled      perpetual
AnyConnect for Mobile             : Disabled      perpetual
AnyConnect for Cisco VPN Phone    : Disabled      perpetual
Advanced Endpoint Assessment      : Disabled      perpetual
UC Phone Proxy Sessions       : 4              perpetual
Total UC Proxy Sessions       : 4              perpetual
Botnet Traffic Filter         : Enabled        33 days
Intercompany Media Engine     : Disabled       perpetual

This platform has an ASA 5520 VPN Plus license.

Running Permanent Activation Key: 0xce06dc6b 0x8a7b5ab7 0xa1e21dd4 0xd2c4b8b8 0xc4594f9c

Licensed features for this platform:
Maximum Physical Interfaces   : Unlimited      perpetual
Maximum VLANs                 : 150            perpetual
Inside Hosts                  : Unlimited      perpetual
Failover                      : Active/Active  perpetual
VPN-DES                       : Enabled        perpetual
VPN-3DES-AES                  : Disabled       perpetual
Security Contexts             : 2              perpetual
GTP/GPRS                      : Disabled       perpetual
AnyConnect Premium Peers          : 2             perpetual
AnyConnect Essentials             : Disabled      perpetual
Other VPN Peers                   : 750           perpetual
Total VPN Peers                   : 750           perpetual
Shared License                    : Disabled       perpetual
AnyConnect for Mobile             : Disabled      perpetual
AnyConnect for Cisco VPN Phone    : Disabled      perpetual
Advanced Endpoint Assessment      : Disabled      perpetual
```

```
UC Phone Proxy Sessions        : 2              perpetual
Total UC Proxy Sessions        : 2              perpetual
Botnet Traffic Filter          : Disabled       perpetual
Intercompany Media Engine      : Disabled       perpetual

The flash permanent activation key is the SAME as the running permanent key.

Active Timebased Activation Key:
0xa821d549 0x35725fe4 0xc918b97b 0xce0b987b 0x47c7c285
Botnet Traffic Filter           : Enabled    33 days

Inactive Timebased Activation Key:
0xyadayad3 0xyadayad3 0xyadayad3 0xyadayad3 0xyadayad3
Security Contexts               : 2          7 days
AnyConnect Premium Peers                   : 100        7 days

0xyadayad4 0xyadayad4 0xyadayad4 0xyadayad4 0xyadayad4
Total UC Proxy Sessions         : 100        14 days
```

例 4：show activation-key detail に対するフェールオーバー ペアのセカンダリ ユニット出力

次に、セカンダリ フェールオーバー ユニットの **show activation-key detail** コマンドの出力例を示します。

- セカンダリ ユニット ライセンス（永続ライセンスと時間ベース ライセンスの組み合わせ）。
- プライマリおよびセカンダリ装置のライセンスの組み合わせである、「フェールオーバー クラスタ」ライセンス。これは、ASA で実際に実行されているライセンスです。プライマリおよびセカンダリ ライセンスの組み合わせを反映したこのライセンスの値は、太字になっています。
- セカンダリ ユニットの永続ライセンス。
- セカンダリのインストール済みの時間ベース ライセンス（アクティブおよび非アクティブ）。このユニットには時間ベース ライセンスはないため、この出力例には何も表示されません。

```
ciscoasa# show activation-key detail

Serial Number:  P3000000011
Running Activation Key: 0xyadayad1 0xyadayad1 0xyadayad1 0xyadayad1 0xyadayad1

Licensed features for this platform:
Maximum Physical Interfaces    : Unlimited      perpetual
Maximum VLANs                  : 150            perpetual
Inside Hosts                   : Unlimited      perpetual
Failover                       : Active/Active  perpetual
VPN-DES                        : Enabled        perpetual
VPN-3DES-AES                   : Disabled       perpetual
Security Contexts              : 2              perpetual
GTP/GPRS                       : Disabled       perpetual
AnyConnect Premium Peers          : 2              perpetual
AnyConnect Essentials             : Disabled       perpetual
Other VPN Peers                   : 750            perpetual
Total VPN Peers                   : 750            perpetual
Shared License                    : Disabled        perpetual
```

```
AnyConnect for Mobile             : Disabled       perpetual
AnyConnect for Cisco VPN Phone    : Disabled       perpetual
Advanced Endpoint Assessment      : Disabled       perpetual
UC Phone Proxy Sessions        : 2              perpetual
Total UC Proxy Sessions        : 2              perpetual
Botnet Traffic Filter          : Disabled       perpetual
Intercompany Media Engine      : Disabled       perpetual

This platform has an ASA 5520 VPN Plus license.

Failover cluster licensed features for this platform:
Maximum Physical Interfaces    : Unlimited      perpetual
Maximum VLANs                  : 150            perpetual
Inside Hosts                   : Unlimited      perpetual
Failover                       : Active/Active  perpetual
VPN-DES                        : Enabled        perpetual
VPN-3DES-AES                   : Enabled        perpetual
Security Contexts              : 10             perpetual
GTP/GPRS                       : Enabled        perpetual
AnyConnect Premium Peers          : 4              perpetual
AnyConnect Essentials             : Disabled       perpetual
Other VPN Peers                   : 750            perpetual
Total VPN Peers                   : 750            perpetual
Shared License                    : Disabled        perpetual
AnyConnect for Mobile             : Disabled       perpetual
AnyConnect for Cisco VPN Phone    : Disabled       perpetual
Advanced Endpoint Assessment      : Disabled       perpetual
UC Phone Proxy Sessions        : 4              perpetual
Total UC Proxy Sessions        : 4              perpetual
Botnet Traffic Filter          : Enabled        33 days
Intercompany Media Engine      : Disabled       perpetual

This platform has an ASA 5520 VPN Plus license.

Running Permanent Activation Key: 0xyadayad1 0xyadayad1 0xyadayad1 0xyadayad1 0xyadayad1

Licensed features for this platform:
Maximum Physical Interfaces    : Unlimited      perpetual
Maximum VLANs                  : 150            perpetual
Inside Hosts                   : Unlimited      perpetual
Failover                       : Active/Active  perpetual
VPN-DES                        : Enabled        perpetual
VPN-3DES-AES                   : Disabled       perpetual
Security Contexts              : 2              perpetual
GTP/GPRS                       : Disabled       perpetual
AnyConnect Premium Peers          : 2              perpetual
AnyConnect Essentials             : Disabled       perpetual
Other VPN Peers                   : 750            perpetual
Total VPN Peers                   : 750            perpetual
Shared License                    : Disabled        perpetual
AnyConnect for Mobile             : Disabled       perpetual
AnyConnect for Cisco VPN Phone    : Disabled       perpetual
Advanced Endpoint Assessment      : Disabled       perpetual
UC Phone Proxy Sessions        : 2              perpetual
Total UC Proxy Sessions        : 2              perpetual
Botnet Traffic Filter          : Disabled       perpetual
Intercompany Media Engine      : Disabled       perpetual

The flash permanent activation key is the SAME as the running permanent key.
```

例 5：show activation-key に対する、フェールオーバー ペアでの ASA サービス モジュールのプライマリ ユニット出力

次に、プライマリ フェールオーバー ユニットの **show activation-key** コマンドの出力例を示します。

- プライマリ ユニット ライセンス（永続ライセンスと時間ベース ライセンスの組み合わせ）。
- プライマリおよびセカンダリ装置のライセンスの組み合わせである、「フェールオーバー クラスタ」ライセンス。これは、ASA で実際に実行されているライセンスです。プライマリおよびセカンダリ ライセンスの組み合わせを反映したこのライセンスの値は、太字になっています。
- プライマリ ユニットのインストール済みの時間ベース ライセンス（アクティブおよび非アクティブ）。

```
ciscoasa# show activation-key

erial Number:  SAL144705BF
Running Permanent Activation Key: 0x4d1ed752 0xc8cfeb37 0xf4c38198 0x93c04c28 0x4a1c049a
Running Timebased Activation Key: 0xbc07bbd7 0xb15591e0 0xed68c013 0xd79374ff 0x44f87880

Licensed features for this platform:
Maximum Interfaces                : 1024           perpetual
Inside Hosts                      : Unlimited      perpetual
Failover                          : Active/Active  perpetual
DES                               : Enabled        perpetual
3DES-AES                          : Enabled        perpetual
Security Contexts                 : 25             perpetual
GTP/GPRS                          : Enabled        perpetual
Botnet Traffic Filter             : Enabled        330 days

This platform has an WS-SVC-ASA-SM1 No Payload Encryption license.


Failover cluster licensed features for this platform:
Maximum Interfaces                : 1024           perpetual
Inside Hosts                      : Unlimited      perpetual
Failover                          : Active/Active  perpetual
DES                               : Enabled        perpetual
3DES-AES                          : Enabled        perpetual
Security Contexts                 : 50 perpetual
GTP/GPRS                          : Enabled        perpetual
Botnet Traffic Filter             : Enabled        330 days
This platform has an WS-SVC-ASA-SM1 No Payload Encryption license.

The flash permanent activation key is the SAME as the running permanent key.

Active Timebased Activation Key:
0xbc07bbd7 0xb15591e0 0xed68c013 0xd79374ff 0x44f87880
Botnet Traffic Filter           : Enabled    330 days
```

例 6：show activation-key に対する、フェールオーバー ペアでの ASA サービス モジュールのセカンダリ ユニット出力

次に、セカンダリ フェールオーバー ユニットの **show activation-key** コマンドの出力例を示します。

- セカンダリ ユニット ライセンス（永続ライセンスと時間ベース ライセンスの組み合わせ）。
- プライマリおよびセカンダリ装置のライセンスの組み合わせである、「フェールオーバー クラスタ」ライセンス。これは、ASA で実際に実行されているライセンスです。プライマリおよびセカンダリ ライセンスの組み合わせを反映したこのライセンスの値は、太字になっています。
- セカンダリのインストール済みの時間ベース ライセンス（アクティブおよび非アクティブ）。このユニットには時間ベース ライセンスはないため、この出力例には何も表示されません。

```
ciscoasa# show activation-key detail

Serial Number:  SAD143502E3
Running Permanent Activation Key: 0xf404c46a 0xb8e5bd84 0x28c1b900 0x92eca09c 0x4e2a0683

Licensed features for this platform:
Maximum Interfaces                : 1024           perpetual
Inside Hosts                      : Unlimited      perpetual
Failover                          : Active/Active  perpetual
DES                               : Enabled        perpetual
3DES-AES                          : Enabled        perpetual
Security Contexts                 : 25             perpetual
GTP/GPRS                          : Disabled       perpetual
Botnet Traffic Filter             : Disabled       perpetual

This platform has an WS-SVC-ASA-SM1 No Payload Encryption license.


Failover cluster licensed features for this platform:
Maximum Interfaces                : 1024           perpetual
Inside Hosts                      : Unlimited      perpetual
Failover                          : Active/Active  perpetual
DES                               : Enabled        perpetual
3DES-AES                          : Enabled        perpetual
Security Contexts                 : 50 perpetual
GTP/GPRS                          : Enabled perpetual
Botnet Traffic Filter             : Enabled 330 days

This platform has an WS-SVC-ASA-SM1 No Payload Encryption license.

The flash permanent activation key is the SAME as the running permanent key.
```

例 7：クラスタでの show activation-key の出力

```
ciscoasa# show activation-key
 Serial Number: JMX1504L2TD
 Running Permanent Activation Key: 0x4a3eea7b 0x54b9f61a 0x4143a90c 0xe5849088 0x4412d4a9


 Licensed features for this platform:
 Maximum Physical Interfaces : Unlimited perpetual
 Maximum VLANs : 100 perpetual
 Inside Hosts : Unlimited perpetual
 Failover : Active/Active perpetual
 Encryption-DES : Enabled perpetual
 Encryption-3DES-AES : Enabled perpetual
```

```
Security Contexts : 2 perpetual
GTP/GPRS : Disabled perpetual
AnyConnect Premium Peers : 2 perpetual
AnyConnect Essentials : Disabled perpetual
Other VPN Peers : 250 perpetual
Total VPN Peers : 250 perpetual
Shared License : Disabled perpetual
AnyConnect for Mobile : Disabled perpetual
AnyConnect for Cisco VPN Phone : Disabled perpetual
Advanced Endpoint Assessment : Disabled perpetual
UC Phone Proxy Sessions : 2 perpetual
Total UC Proxy Sessions : 2 perpetual
Botnet Traffic Filter : Disabled perpetual
Intercompany Media Engine : Disabled perpetual
Cluster : Enabled perpetual

This platform has an ASA 5585-X base license.

Failover cluster licensed features for this platform:
Maximum Physical Interfaces : Unlimited perpetual
Maximum VLANs : 100 perpetual
Inside Hosts : Unlimited perpetual
Failover : Active/Active perpetual
Encryption-DES : Enabled perpetual
Encryption-3DES-AES : Enabled perpetual
Security Contexts : 4 perpetual
GTP/GPRS : Disabled perpetual
AnyConnect Premium Peers : 4 perpetual
AnyConnect Essentials : Disabled perpetual
Other VPN Peers : 250 perpetual
Total VPN Peers : 250 perpetual
Shared License : Disabled perpetual
AnyConnect for Mobile : Disabled perpetual
AnyConnect for Cisco VPN Phone : Disabled perpetual
Advanced Endpoint Assessment : Disabled perpetual
UC Phone Proxy Sessions : 4 perpetual
Total UC Proxy Sessions : 4 perpetual
Botnet Traffic Filter : Disabled perpetual
Intercompany Media Engine : Disabled perpetual
Cluster : Enabled perpetual

This platform has an ASA 5585-X base license.

The flash permanent activation key is the SAME as the running permanent key.
```

共有ライセンスのモニタリング

共有ライセンスをモニタするには、次のいずれかのコマンドを入力します。

- **show shared license** [**detail** | **client** [*hostname*] | **backup**]

  共有ライセンス統計情報を表示します。オプション キーワードはライセンス サーバだけに使用できます。**detail** キーワードを使用すると、参加システムごとの統計情報が表示されます。表示内容を 1 台の参加システムに限定するには、**client** キーワードを使用します。**backup** キーワードを使用すると、バックアップ サーバに関する情報が表示されます。

  共有ライセンスの統計情報をクリアするには、**clear shared license** コマンドを入力します。

  次に、ライセンス参加ユニットでの **show shared license** コマンドの出力例を示します。

```
ciscoasa>  show shared license
Primary License Server : 10.3.32.20
  Version              : 1
  Status               : Inactive

Shared license utilization:
  SSLVPN:
    Total for network :     5000
    Available         :     5000
    Utilized          :        0
  This device:
    Platform limit    :      250
    Current usage     :        0
    High usage        :        0
  Messages Tx/Rx/Error:
    Registration    : 0 / 0 / 0
    Get             : 0 / 0 / 0
    Release         : 0 / 0 / 0
    Transfer        : 0 / 0 / 0
```

次に、ライセンス サーバ上での **show shared license detail** コマンドの出力例を示します。

```
ciscoasa>  show shared license detail
Backup License Server Info:

Device ID           : ABCD
Address             : 10.1.1.2
Registered          : NO
HA peer ID          : EFGH
Registered          : NO
  Messages Tx/Rx/Error:
    Hello           : 0 / 0 / 0
    Sync            : 0 / 0 / 0
    Update          : 0 / 0 / 0

Shared license utilization:
  SSLVPN:
    Total for network :      500
    Available         :      500
    Utilized          :        0
  This device:
    Platform limit    :      250
    Current usage     :        0
    High usage        :        0
  Messages Tx/Rx/Error:
    Registration    : 0 / 0 / 0
    Get             : 0 / 0 / 0
    Release         : 0 / 0 / 0
    Transfer        : 0 / 0 / 0


Client Info:

  Hostname          : 5540-A
  Device ID         : XXXXXXXXXXX
  SSLVPN:
    Current usage   : 0
    High            : 0
  Messages Tx/Rx/Error:
    Registration    : 1 / 1 / 0
    Get             : 0 / 0 / 0
    Release         : 0 / 0 / 0
    Transfer        : 0 / 0 / 0
```

. . .

- **show activation-key**

  ASA にインストールされているライセンスを表示します。**show version** コマンドでもライセンス情報が表示されます。

- **show vpn-sessiondb**

  VPN セッションのライセンス情報を表示します。

PAK ライセンスの履歴

機能名	プラットフォーム リリース	説明
接続数と VLAN 数の増加	7.0(5)	次の制限値が増加されました。 • ASA5510 Base ライセンス接続は 32000 から 5000 に、VLAN は 0 から 10 に増加。 • ASA5510 Security Plus ライセンス接続は 64000 から 130000 に、VLAN は 10 から 25 に増加。 • ASA5520 接続は 130000 から 280000 に、VLAN は 25 から 100 に増加。 • ASA5540 接続は 280000 から 400000 に、VLAN は 100 から 200 に増加。
SSL VPN ライセンス	7.1(1)	SSL VPN ライセンスが導入されました。
SSL VPN ライセンスの追加	7.2(1)	5000 ユーザの SSL VPN ライセンスが ASA 5550 以降に対して導入されました。
ASA 5510 上の基本ライセンスに対する増加したインターフェイス	7.2(2)	ASA 5510 上の基本ライセンスについて、最大インターフェイス数が 3 プラス管理インターフェイスから無制限のインターフェイスに増加しました。

機能名	プラットフォーム リリース	説明
VLAN 数の増加	7.2(2)	ASA 5505 上の Security Plus ライセンスに対する VLAN 最大数が、5（3 つのフル機能インターフェイス、1 つのフェールオーバー インターフェイス、1 つのバックアップ インターフェイスに制限されるインターフェイス）から 20 のフル機能インターフェイスに増加されました。また、トランク ポート数も 1 から 8 に増加されました。フル機能のインターフェイスの数が 20 になり、バックアップ ISP インターフェイスを停止するために backup interface コマンドを使用する必要がなくなりました。つまり、バックアップ ISP インターフェイス用にフル機能のインターフェイスを使用できるようになりました。backup interface コマンドは、これまでどおり Easy VPN 設定用に使用できます。 VLAN の制限値も変更されました。ASA 5510 の基本ライセンスでは 10 から 50 に、Security Plus ライセンスでは 25 から 100 に、ASA 5520 では 100 から 150 に、ASA 5550 では 200 から 250 に増えています。

機能名	プラットフォーム リリース	説明
ASA 5510 Security Plus ライセンスに対するギガビット イーサネット サポート	7.2(3)	ASA 5510 は、Security Plus ライセンスを使用する Ethernet 0/0 および 0/1 ポート用にギガビット イーサネット（1000 Mbps）をサポートしています。基本ライセンスでは、これらのポートは引き続きファスト イーサネット（100 Mbps）ポートとして使用されます。いずれのライセンスに対しても、Ethernet 0/2、0/3、および 0/4 はファスト イーサネット ポートのままです。 （注） インターフェイス名は Ethernet 0/0 および Ethernet 0/1 のままです。 **speed** コマンドを使用してインターフェイスの速度を変更します。また、**show interface** コマンドを使用して各インターフェイスの現在の設定速度を確認します。

機能名	プラットフォーム リリース	説明
Advanced Endpoint Assessment ライセンス	8.0(2)	Advanced Endpoint Assessment ライセンスが導入されました。Cisco AnyConnect またはクライアントレス SSL VPN 接続の条件としてリモート コンピュータでスキャン対象となる、アンチウイルス アプリケーションやアンチスパイウェア アプリケーション、ファイアウォール、オペレーティング システム、および関連アップデートの種類が、大幅に拡張されました。また、任意のレジストリ エントリ、ファイル名、およびプロセス名を指定してスキャン対象にすることもできます。スキャン結果を ASA に送信します。ASA は、ユーザ ログイン クレデンシャルとコンピュータ スキャン結果の両方を使用して、ダイナミック アクセス ポリシー（DAP）を割り当てます。 Advanced Endpoint Assessment ライセンスを使用すると、バージョン要件を満たすように非準拠コンピュータのアップデートを試行する機能を設定して、Host Scan を拡張できます。 シスコは、Host Scan でサポートされるアプリケーションとバージョンの一覧に、Cisco Secure Desktop とは異なるパッケージで、タイムリーなアップデートを提供できます。
ASA 5510 の VPN ロード バランシング	8.0(2)	VPN ロード バランシングが ASA 5510 Security Plus ライセンスでサポートされるようになりました。
AnyConnect for Mobile ライセンス	8.0(3)	AnyConnect for Mobile ライセンスが導入されました。これにより、Windows モバイル デバイスは AnyConnect クライアントを使用して、ASA に接続できます。
時間ベース ライセンス	8.0(4)/8.1(2)	時間ベース ライセンスがサポートされるようになりました。

機能名	プラットフォーム リリース	説明
ASA 5580 の VLAN 数の増加	8.1(2)	ASA 5580 上でサポートされる VLAN 数が 100 から 250 に増加されました。
Unified Communications Proxy セッション ライセンス	8.0(4)	UC Proxy セッション ライセンスが導入されました。電話プロキシ、Presence Federation Proxy、および Encrypted Voice Inspection アプリケーションでは、それらの接続に TLS プロキシセッションが使用されます。各 TLS プロキシ セッションは、UC ライセンスの制限に対してカウントされます。これらのアプリケーションは、すべて UC Proxy として包括的にライセンスされるので、混在させたり、組み合わせたりできます。 この機能は、バージョン 8.1 では使用できません。
ボットネット トラフィック フィルタ ライセンス	8.2(1)	ボットネット トラフィック フィルタ ライセンスが導入されました。ボットネット トラフィック フィルタでは、既知の不正なドメインや IP アドレスに対する接続を追跡して、マルウェア ネットワーク アクティビティから保護します。

機能名	プラットフォーム リリース	説明
AnyConnect Essentials ライセンス	8.2(1)	AnyConnect Essentials ライセンスが導入されました。このライセンスにより、AnyConnect VPN クライアントは ASA にアクセスできるようになります。このライセンスでは、ブラウザベースの SSL VPN アクセスまたは Cisco Secure Desktop はサポートされていません。これらの機能に対しては、AnyConnect Essentials ライセンスの代わりに AnyConnect Premium ライセンスがアクティブ化されます。 （注） AnyConnect Essentials ライセンスを所有する VPN ユーザは、Web ブラウザを使用してログインし、AnyConnect クライアントをダウンロードおよび起動（WebLaunch）することができます。 このライセンスと AnyConnect Premium ライセンスのいずれでイネーブル化されたかには関係なく、AnyConnect クライアント ソフトウェアには同じクライアント機能のセットが装備されています。 特定の ASA では、AnyConnect Premium ライセンス（全タイプ）または Advanced Endpoint Assessment ライセンスを、AnyConnect Essentials ライセンスと同時にアクティブにすることはできません。ただし、同じネットワーク内の異なる ASA で、AnyConnect Essentials ライセンスと AnyConnect Premium ライセンスを実行することは可能です。 デフォルトでは、ASA は AnyConnect Essentials ライセンスを使用しますが、**webvpn** を使用し、次に **no anyconnect-essentials** コマンド を使用すると、AnyConnect Essentials ライセンスを無効にして他のライセンスを使用できます。

機能名	プラットフォーム リリース	説明
SSL VPN ライセンスの AnyConnect Premium SSL VPN Edition ライセンスへの変更	8.2(1)	SSL VPN ライセンスの名前が AnyConnect Premium SSL VPN Edition ライセンスに変更されました。
SSL VPN の共有ライセンス	8.2(1)	SSL VPN の共有ライセンスが導入されました。複数の ASA で、SSL VPN セッションのプールを必要に応じて共有できます。
モビリティ プロキシ アプリケーションでの Unified Communications Proxy ライセンス不要化	8.2(2)	モビリティ プロキシに UC Proxy ライセンスが必要なくなりました。
ASA 5585-X（SSP-20）用 10 GE I/O ライセンス	8.2(3)	ASA 5585-X（SSP-20）の 10 GE I/O ライセンスを導入し、ファイバポートでの 10 ギガビット イーサネットの速度をイネーブルにしました。SSP-60 は、デフォルトで 10 ギガビット イーサネットの速度をサポートします。 （注） ASA 5585-X は 8.3(x) ではサポートされていません。
ASA 5585-X（SSP-10）用 10 GE I/O ライセンス	8.2(4)	ASA 5585-X（SSP-10）の 10 GE I/O ライセンスを導入し、ファイバポートでの 10 ギガビット イーサネットの速度をイネーブルにしました。SSP-40 は、デフォルトで 10 ギガビット イーサネットの速度をサポートします。 （注） ASA 5585-X は 8.3(x) ではサポートされていません。
同一でないフェールオーバー ライセンス	8.3(1)	フェールオーバー ライセンスが各ユニット上で同一である必要がなくなりました。両方のユニットで使用するライセンスは、プライマリ ユニットおよびセカンダリ ユニットからの結合されたライセンスです。 **show activation-key** および **show version** の各コマンドが変更されました。

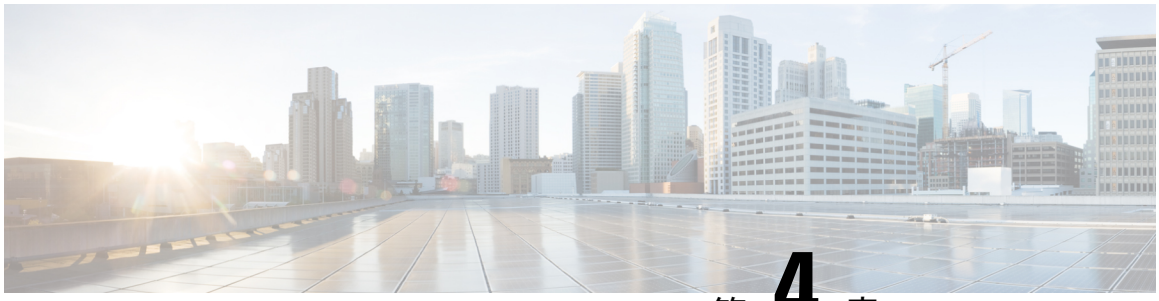
機能名	プラットフォーム リリース	説明
スタック可能な時間ベース ライセンス	8.3(1)	時間ベース ライセンスがスタッカブルになりました。多くの場合、時間ベース ライセンスは更新の必要があり、旧ライセンスから新しいライセンスへシームレスに移行する必要があります。時間ベース ライセンスだけで使用される機能では、新しいライセンスが適用される前に、ライセンスの有効期限が切れてしまわないことが特に重要です。ASA では時間ベース ライセンスをスタックできるので、ライセンスの有効期限が切れたり、新しいライセンスを早めにインストールしたために時間が無駄になったりする心配はありません。
Intercompany Media Engine ライセンス	8.3(1)	IME ライセンスが導入されました。
複数の時間ベース ライセンスの同時アクティブ化	8.3(1)	時間ベース ライセンスを複数インストールできるようになり、同時に機能ごとに 1 つのアクティブなライセンスを保持できるようになりました。 **show activation-key** および **show version** の各コマンドが変更されました。
時間ベース ライセンスのアクティブ化と非アクティブ化の個別化	8.3(1)	コマンドを使用して、時間ベース ライセンスをアクティブ化または非アクティブ化できるようになりました。 **activation-key** [**activate** | **deactivate**] コマンドが変更されました。
AnyConnect Premium SSL VPN Edition ライセンスの AnyConnect Premium SSL VPN ライセンスへの変更	8.3(1)	AnyConnect Premium SSL VPN Edition ライセンスの名前が AnyConnect Premium SSL VPN ライセンスに変更されました。

機能名	プラットフォーム リリース	説明
輸出用のペイロード暗号化なしイメージ	8.3(2)	ASA 5505 ～ 5550 にペイロード暗号化機能のないソフトウェアをインストールした場合、Unified Communications、強力な暗号化VPN、強力な暗号化管理プロトコルをディセーブルにします。 （注） この特殊なイメージは 8.3(x) でのみサポートされます。8.4(1) 以降で暗号化機能のないソフトウェアをサポートするには、ASA の特別なハードウェア バージョンを購入する必要があります。
ASA 5550、5580、および 5585-X でのコンテキストの増加	8.4(1)	ASA 5550 および ASA 5585-X（SSP-10）では、コンテキストの最大数が 50 から 100 に引き上げられました。ASA 5580 および 5585-X（SSP-20）以降では、コンテキストの最大数が 50 から 250 に引き上げられました。
ASA 5580 および 5585-X での VLAN 数の増加	8.4(1)	ASA 5580 および ASA 5585-X では、VLAN の最大数が 250 から 1024 に引き上げられました。
ASA 5580 および 5585-X での接続数の増加	8.4(1)	ファイアウォール接続の最大数が次のように引き上げられました。 • ASA 5580-20：1,000,000 から 2,000,000 へ。 • ASA 5580-40：2,000,000 から 4,000,000 へ。 • ASA 5585-X with SSP-10：750,000 から 1,000,000 へ。 • ASA 5585-X with SSP-20：1,000,000 から 2,000,000 へ。 • ASA 5585-X with SSP-40：2,000,000 から 4,000,000 へ。 • ASA 5585-X with SSP-60：2,000,000 から 10,000,000 へ。

機能名	プラットフォーム リリース	説明
AnyConnect Premium SSL VPN ライセンスの AnyConnect Premium ライセンスへの変更	8.4(1)	AnyConnect Premium SSL VPN ライセンスの名前が AnyConnect Premium ライセンスに変更されました。ライセンス情報の表示が「SSL VPN ピア」から「AnyConnect Premium ピア」に変更されました。
ASA 5580 での AnyConnect VPN セッション数の増加	8.4(1)	AnyConnect VPN セッションの最大数が 5,000 から 10,000 に引き上げられました。
ASA 5580 での AnyConnect 以外の VPN セッション数の増加	8.4(1)	AnyConnect 以外の VPN セッションの最大数が 5,000 から 10,000 に引き上げられました。
IKEv2 を使用した IPsec リモート アクセス	8.4(1)	AnyConnect Essentials ライセンスおよび AnyConnect Premium ライセンスに IKEv2 を使用した IPsec リモート アクセス VPN が追加されました。 （注） ASA での IKEv2 のサポートに関して、重複するセキュリティ アソシエーションがサポートされていないという制約が現在あります。 Other VPN ライセンス（以前の IPsec VPN）には IKEv2 サイトツーサイト セッションが追加されました。Other VPN ライセンスは基本ライセンスに含まれています。
輸出用のペイロード暗号化なしハードウェア	8.4(1)	ペイロード暗号化機能のないモデルでは（ASA 5585-X など）、特定の国に ASA を輸出できるよう、ASA ソフトウェアのユニファイド コミュニケーションと VPN 機能を無効にしています。

機能名	プラットフォーム リリース	説明
デュアル SSP（SSP-20 および SSP-40）	8.4(2)	SSP-40 および SSP-60 の場合、同じシャーシでレベルが同じ 2 つの SSP を使用できます。レベルが混在した SSP はサポートされていません（たとえば、SSP-40 と SSP-60 の組み合わせはサポートされていません）。各 SSP は個別のコンフィギュレーションおよび管理を持つ独立したデバイスとして動作します。必要に応じて 2 つの SSP をフェールオーバーペアとして使用できます。2 個の SSP をシャーシで使用する場合、VPN はサポートされません。しかし、VPN がディセーブルになっていないことに注意してください。
ASA 5512-X ～ ASA 5555-X での IPS モジュール ライセンス	8.6(1)	ASA 5512-X、ASA 5515-X、ASA 5525-X、ASA 5545-X、および ASA 5555-X での IPS SSP ソフトウェア モジュールには IPS モジュール ライセンスが必要です。
ASA 5580 および ASA 5585-X のクラスタリング ライセンス。	9.0(1)	クラスタリング ライセンスが ASA 5580 および ASA 5585-X に対して追加されました。
ASASM での VPN のサポート	9.0(1)	ASASM は、すべての VPN 機能をサポートするようになりました。
ASASM でのユニファイド コミュニケーションのサポート	9.0(1)	ASASM は、すべてのユニファイド コミュニケーション機能をサポートするようになりました。
SSP-10 および SSP-20 に対する ASA 5585-X デュアル SSP サポート（SSP-40 および SSP-60 に加えて）、デュアル SSP に対する VPN サポート	9.0(1)	ASA 5585-X は、すべての SSP モデルでデュアル SSP をサポートするようになりました（同一シャーシ内で同じレベルの SSP を 2 つ使用できます）。デュアル SSP を使用するときに VPN がサポートされるようになりました。

機能名	プラットフォーム リリース	説明
ASA 5500-X でのクラスタリングのサポート	9.1(4)	ASA 5512-X、ASA 5515-X、ASA 5525-X、ASA 5545-X および ASA 5555-X が 2 ユニット クラスタをサポートするようになりました。2 ユニットのクラスタリングは、基本ライセンスではデフォルトでイネーブルになります。ASA 5512-X では Security Plus ライセンスが必要です。
ASA 5585-X の 16 のクラスタ メンバのサポート	9.2(1)	ASA 5585-X が 16 ユニット クラスタをサポートするようになりました。
ASAv4 および ASAv30 の標準およびプレミアム モデル ライセンスの導入	9.2(1)	シンプルなライセンス方式で ASAv が導入されました（標準またはプレミアム レベルの ASAv4 および ASAv30 永続ライセンス）。アドオン ライセンスは使用できません。



第 4 章

ライセンス：スマート ソフトウェア ライセンス（ASAv、ASA on Firepower）

シスコ スマート ソフトウェア ライセンスによって、ライセンスを購入し、ライセンスのプールを一元管理できます。製品認証キー（PAK）ライセンスとは異なり、スマート ライセンスは特定のシリアル番号に関連付けられません。各ユニットのライセンス キーを管理しなくても、簡単に ASA を導入したり使用を終了したりできます。スマート ソフトウェア ライセンスを利用すれば、ライセンスの使用状況と要件をひと目で確認することもできます。

（注） スマート ソフトウェア ライセンスは、ASAv および ASA Firepower シャーシでのみサポートされます。他のモデルは、PAK ライセンスを使用します。「PAK ライセンスについて （57 ページ）」を参照してください。

スマート ソフトウェア ライセンスについて

ここでは、スマート ソフトウェア ライセンスの仕組みについて説明します。

Firepower 9300 シャーシの ASA のスマート ソフトウェア ライセンシング

Firepower 9300 シャーシ 上の ASA では、スマート ソフトウェア ライセンシングの設定は、Firepower 9300 シャーシ スーパバイザと ASA に分割されています。

- Firepower 9300 シャーシ：License Authority との通信に使用するパラメータなど、すべてのスマート ソフトウェア ライセンシング インフラストラクチャをシャーシで設定します。Firepower 9300 シャーシ 自体の動作にライセンスは必要ありません。
- ASA アプリケーション：ASA のすべてのライセンスの権限付与を設定します。

Smart Software Manager とアカウント

デバイスの 1 つ以上のライセンスを購入する場合は、Cisco Smart Software Manager で管理します。

https://software.cisco.com/#module/SmartLicensing

Smart Software Manager では、組織のマスター アカウントを作成できます。

（注） まだアカウントをお持ちでない場合は、リンクをクリックして新しいアカウントを設定してください。Smart Software Manager では、組織のマスター アカウントを作成できます。

デフォルトで、ライセンスはマスターアカウントの下のデフォルト仮想アカウントに割り当てられます。アカウント管理者であれば、任意で追加の仮想アカウントを作成できます。たとえば、地域、部門、または子会社のアカウントを作成できます。複数の仮想アカウントを使用すると、大量のライセンスおよびデバイスをより簡単に管理できます。

仮想アカウントごとに管理されるライセンスとデバイス

ライセンスとデバイスは仮想アカウントごとに管理されます。アカウントに割り当てられたライセンスを使用できるのは、その仮想アカウントのデバイスのみです。追加のライセンスが必要な場合は、別の仮想アカウントから未使用のライセンスを転用できます。仮想アカウント間でデバイスを転送することもできます。

Firepower 9300 シャーシ 上で動作する ASA の場合：シャーシのみがデバイスとして登録される一方で、シャーシ内の ASA アプリケーションはそれぞれ固有のライセンスを要求します。たとえば、3 つのセキュリティ モジュールを搭載した Firepower 9300 シャーシでは、全シャーシが 1 つのデバイスとして登録されますが、各モジュールは合計 3 つのライセンスを別個に使用します。

評価ライセンス

ASAv

ASAv は、評価モードをサポートしていません。Licensing Authority への登録の前に、ASAv は厳しいレート制限状態で動作します。

Firepower 9300 シャーシ

Firepower 9300 シャーシ は、次の 2 種類の評価ライセンスをサポートしています。

- シャーシ レベル評価モード：Firepower 9300 シャーシによる Licensing Authority への登録の前に、評価モードで 90 日間（合計使用期間）動作します。このモードでは、ASA は固有の権限付与を要求できません。デフォルトの権限のみが有効になります。この期間が終了すると、Firepower 9300 シャーシ はコンプライアンス違反の状態になります。
- 権限付与ベースの評価モード：Firepower 9300 シャーシ が Licensing Authority に登録をした後、ASA に割り当て可能な時間ベースの評価ライセンスを取得できます。ASA で、通常どおりに権限付与を要求します。時間ベースのライセンスの期限が切れると、時間ベースのライセンスを更新するか、または永続ライセンスを取得する必要があります。

（注） 高度暗号化（3DES/AES）の評価ライセンスを受け取ることはできません。License Authority に登録して永続ライセンスを取得する必要があります。

Smart Software Manager 通信

このセクションでは、デバイスの Smart Software Manager に対する通信方法について説明します。

デバイスの登録とトークン

各仮想アカウントに対し、登録トークンを作成できます。このトークンは、デフォルトで 30 日間有効です。各デバイスを展開するか、または既存のデバイスを登録する場合は、このトークン ID と権限レベルを入力します。既存のトークンの有効期限が切れている場合は、新しいトークンを作成できます。

（注） Firepower 9300 シャーシ：デバイス登録は、ASA 論理デバイス上ではなく、シャーシで設定されます。

展開後の起動時、または既存のデバイスでこれらのパラメータを手動で設定した後、デバイスは Cisco License Authority に登録されます。デバイスがトークンにより登録されると、デバイスとライセンス機関との間の通信に使用する ID 証明書がライセンス機関により発行されます。この証明書の有効期間は 1 年ですが、6 か月ごとに更新されます。

License Authority との定期通信

デバイスは 30 日ごとに License Authority と通信します。Smart Software Manager に変更を行う場合、デバイスの認証を更新して変更をすぐに反映させることができます。またはスケジュール設定されたデバイスの通信を待つこともできます。

必要に応じて、HTTP プロキシを設定できます。

ASAv

ASAv は直接または HTTP プロキシ経由で少なくとも 30 日ごとにインターネット アクセスを行う必要があります。ASAv には猶予期間がありません。Licensing Authority に連絡しない限り、正常に再認証できるまで、ASAv は厳しくレート制限されます。

Firepower 9300

Firepower 9300では、少なくとも 90 日おきに、直接接続または HTTP プロキシを介したインターネット アクセスが必要です。通常のライセンス通信が 30 日ごとに行われますが、猶予期間によって、デバイスは Call Home なしで最大 90 日間動作します。猶予期間後、Licensing Authority に連絡しない限り、特別なライセンスを必要とする機能の設定変更を行なえませんが、動作には影響ありません。

非適合状態

デバイスは、次の状況においてコンプライアンス違反になる可能性があります。

- 使用率超過：デバイスが使用不可のライセンスを使用している場合。
- ライセンスの有効期限切れ：時間ベースのライセンスの有効期限が切れている場合。
- 通信の欠落：デバイスが再許可を得るために Licensing Authority に到達できない場合。

アカウントのステータスがコンプライアンス違反状態なのか、違反状態に近づいているのかを確認するには、デバイスで現在使用中の権限付与とスマートアカウントのものを比較する必要があります。

コンプライアンス違反状態では、モデルによってはデバイスが制限されている可能性があります。

- ASAv：正常に再認証できるまで、ASAv は厳しくレート制限されます。
- Firepower 9300：特別なライセンスが必要な機能への設定変更はできなくなりますが、動作には影響ありません。たとえば、標準のライセンス制限を超える既存のコンテキストは実行を継続でき、その構成を変更することもできますが、新しいコンテキストを追加することはできません。

Smart Call Home インフラストラクチャ

デフォルトでは、Licensing Authority の URL を指定する Smart Call Home プロファイルがコンフィギュレーションに存在します。このプロファイルは削除できません。ライセンスプロファ

イルの唯一の設定可能なオプションが License Authority の宛先アドレス URL であることに注意してください。Cisco TAC に指示されない限り、License Authority の URL は変更しないでください。

（注） Firepower 9300 シャーシ の場合、ライセンスの Smart Call Home は ASA ではなく Firepower 9300 シャーシ スーパバイザで設定されます。

スマート ソフトウェア ライセンスの Smart Call Home をディセーブルにすることはできません。たとえば、**no service call-home** コマンドを使用して Smart Call Home を無効化しても、スマート ソフトウェア ライセンシングは無効化されません。

他の Smart Call Home の機能は、特に設定しない限り、有効になりません。

ライセンスに関する注意事項

次の表に、ライセンスに関する追加情報を示します。

AnyConnect Plus および Apex ライセンス

AnyConnect Plus および Apex ライセンスは、ライセンスが指定するユーザ プールを共有するすべての複数の ASA に適用できる同時使用ライセンスです。スマート ライセンスを使用するデバイスでは、実際のプラットフォームに AnyConnect ライセンスを物理的に適用する必要はありません。ただし、同じライセンスを購入して、ソフトウェア センターへのアクセスやテクニカル サポートを使用するために契約番号を Cisco.com ID に関連付ける必要があります。詳細については、以下を参照してください。

- 『Cisco AnyConnect Ordering Guide』
- AnyConnect Licensing Frequently Asked Questions (FAQ)

その他の VPN ライセンス

その他の VPN セッションには、次の VPN タイプが含まれています。

- IKEv1 を使用した IPsec リモート アクセス VPN
- IKEv1 を使用した IPsec サイトツーサイト VPN
- IKEv2 を使用した IPsec サイトツーサイト VPN

このライセンスは基本ライセンスに含まれています。

合計 VPN セッション、全タイプ

- VPN セッションの最大数の合計が、VPN AnyConnect とその他の VPN セッションの最大数よりも多くなっても、組み合わせたセッション数が VPN セッションの制限を超えるこ

とはできません。VPN の最大セッション数を超えた場合、ASA をオーバーロードして、適切なネットワークのサイズに設定してください。

- クライアントレス SSL VPN セッションを開始した後、ポータルから AnyConnect クライアントセッションを開始した場合は、合計 1 つのセッションが使用されています。これに対して、最初に AnyConnect クライアントを（スタンドアロン クライアントなどから）開始した後、クライアントレス SSL VPN ポータルにログインした場合は、2 つのセッションが使用されています。

暗号化ライセンス

高度暗号化：ASAv

ライセンス認証局に接続する前に、高度暗号化（3DES/AES）を管理接続に使用できるので、ASDM を起動してライセンス認証局に接続することができます。through-the-box トラフィックの場合、License Authority に接続して高度暗号化ライセンスを取得するまで、スループットは厳しく制限されます。

ASAv が後でコンプライアンス違反になった場合、ASAv はレート制限状態に戻ります。

高度暗号化：Firepower 9300 シャーシ

ASDM には 3DES が必要なため、CLI を使用して ASA 設定で高度暗号化ライセンスを手動で要求する必要があります。ASA がコンプライアンス違反になると、管理トラフィックやこのライセンスを必要とするスルートラフィックは許可されません。

DES：すべてのモデル

DES ライセンスはディセーブルにできません。3DES ライセンスをインストールしている場合、DES は引き続き使用できます。強力な暗号化だけを使用したい場合に DES の使用を防止するには、強力な暗号化だけを使用するようにすべての関連コマンドを設定する必要があります。

合計 UC プロキシ セッション

Encrypted Voice Inspection の各 TLS プロキシ セッションは、TLS ライセンスの制限に対してカウントされます。

TLS プロキシセッションを使用するその他のアプリケーション（ライセンスが不要な Mobility Advantage Proxy など）では、TLS 制限に対してカウントしません。

アプリケーションによっては、1 つの接続に複数のセッションを使用する場合があります。たとえば、プライマリとバックアップの Cisco Unified Communications Manager を電話に設定した場合は、TLS プロキシ接続は 2 つ使用されます。

TLS プロキシの制限は、**tls-proxy maximum-sessions** コマンドまたは ASDM で [Configuration] > [Firewall] > [Unified Communications] > [TLS Proxy] ペインを使用して個別に設定できます。モデルの制限を表示するには、**tls-proxy maximum-sessions ?** コマンドを入力します。デフォルトの TLS プロキシ制限よりも高い TLS プロキシライセンスを適用する場合、ASA では、そのラ

イセンスに一致するように TLS プロキシの制限が自動的に設定されます。ライセンスの制限よりも TLS プロキシ制限が優先されます。TLS プロキシ制限をライセンスよりも少なく設定すると、ライセンスですべてのセッションを使用できません。

（注） 「K8」で終わるライセンス製品番号（たとえばユーザ数が 250 未満のライセンス）では、TLS プロキシセッション数は 1000 までに制限されます。「K9」で終わるライセンス製品番号（たとえばユーザ数が 250 以上のライセンス）では、TLS プロキシの制限はコンフィギュレーションに依存し、モデルの制限が最大数になります。K8 と K9 は、エクスポートについてそのライセンスが制限されるかどうかを示します。K8 は制限されず、K9 は制限されます。

（たとえば **clear configure all** コマンドを使用して）コンフィギュレーションをクリアすると、TLS プロキシ制限がモデルのデフォルトに設定されます。このデフォルトがライセンスの制限よりも小さいと、**tls-proxy maximum-sessions** コマンドを使用したときに、再び制限を高めるようにエラー メッセージが表示されます（ASDM の [TLS Proxy] ペインを使用）。フェールオーバーを使用して、**write standby** コマンドを入力するか、または ASDM でプライマリ装置に対して [File] > [Save Running Configuration to Standby Unit] を使用して強制的にコンフィギュレーションの同期を行うと、セカンダリ装置で **clear configure all** コマンドが自動的に生成され、セカンダリ装置に警告メッセージが表示されることがあります。コンフィギュレーションの同期によりプライマリ装置の TLS プロキシ制限の設定が復元されるため、この警告は無視できます。

接続には、SRTP 暗号化セッションを使用する場合もあります。

- K8 ライセンスでは、SRTP セッション数は 250 までに制限されます。
- K9 ライセンスでは、制限はありません。

（注） メディアの暗号化/復号化を必要とするコールだけが、SRTP 制限に対してカウントされます。コールに対してパススルーが設定されている場合は、両方のレッグが SRTP であっても、SRTP 制限に対してカウントされません。

VLAN、最大

VLAN 制限の対象としてカウントするインターフェイスに、VLAN を割り当てます。 次に例を示します。

```
interface gigabitethernet 0/0.100
vlan 100
```

ボットネット トラフィック フィルタ ライセンス

ダイナミック データベースをダウンロードするには、強力な暗号化（3DES/AES）ライセンスが必要です。

フェールオーバーまたは ASA クラスタ ライセンス

ASAv のフェールオーバー ライセンス

スタンバイ ユニットにはプライマリ ユニットと同じモデル ライセンスが必要です。

Firepower 9300 シャーシ の ASA のフェールオーバー ライセンス

各 Firepower 9300 シャーシは、License Authority またはサテライト サーバに登録されている必要があります。セカンダリ ユニットに追加費用はかかりません。永続ライセンスを予約するには、シャーシごとに個別のライセンスを購入する必要があります。

各 ASA に同じ暗号化ライセンスが必要です。通常の Smart Software Manager（SSM）ユーザの場合、強力な暗号化ライセンスは、Firepower 9300 シャーシ で登録トークンを適用すると、対象となるお客様の場合には自動的に有効化されます。古い Cisco Smart Software Manager サテライトが導入されている場合は、以下を参照してください。

ASA ライセンス設定では、その他のライセンスは各フェールオーバー ユニットで一致している必要はなく、各ユニットで別個にライセンスを設定できます。各ユニットには、サーバからの各自のライセンスが必要です。両方のユニットから要求されるライセンスは単一のフェールオーバーライセンスにまとめられ、フェールオーバーのペアで共有されます。この集約ライセンスはスタンバイ ユニットにキャッシュされ、将来アクティブなユニットとなったときに使用されます。通常、プライマリユニットのみライセンスを設定すれば済みます。

各ライセンス タイプは次のように処理されます:

- Standard：デフォルトで各ユニットに Standard ライセンスが含まれています。したがって、フェールオーバーのペアでは、サーバから 2 つの標準ライセンスが要求されます。
- Context：各ユニットは自身の Context ライセンスを要求できます。ただし、デフォルトで Standard ライセンスには 10 のコンテキストが含まれ、これは両方のユニットにあります。各ユニットの Standard ライセンスの値と、両方のユニットにあるオプションの Context ライセンスの値はプラットフォームの上限まで加算されます。次に例を示します。
  - Standard ライセンスに 10 のコンテキストが含まれ、2 つのユニットでは 20 のコンテキストがあります。250 の Context ライセンスをアクティブ/スタンバイペアのプライマリユニットに設定した場合を考えます。この場合、集約されたフェールオーバーライセンスには 270 のコンテキストが含まれています。しかし、ユニットごとのプラットフォームの制限が 250 であるため、結合されたライセンスでは最大 250 のコンテキストが許容されます。この場合では、プライマリの Context ライセンスとして 230 コンテキストを設定する必要があります。
  - Standard ライセンスには 10 のコンテキストがあり、2 つユニットがあるため、合計で 20 のコンテキストがあります。アクティブ/アクティブペアのプライマリユニットに 10 Context ライセンスを設定し、セカンダリ ユニットにも 10 Context ライセンスを設定します。この場合、集約されたフェールオーバーライセンスには 40 のコンテキストが含まれています。たとえば、一方のユニットが 22 コンテキストを使用し、他方が 18 コンテキストを使用します（合計 40 の場合）。ユニットごとのプラットフォー

ムの制限が 250 であるため、結合されたライセンスでは最大 250 のコンテキストが許容されます。40 コンテキストは制限の範囲内です。

- キャリア：ユニット 1 つのみがこのライセンスを要求する必要があり、両方のユニットがこれを使用できます。
- 高度暗号化（3DES）（2.3.0 より前の Cisco Smart Software Manager サテライト導入の場合のみ）：各ユニットがサーバからの各自のライセンスを要求する必要があります。他のライセンス設定とは異なり、この設定はスタンバイ ユニットに複製されます。スマート ソフトウェア マネージャ サテライトが導入されている場合、ASDM や他の高度暗号機能を使用するには、クラスタ展開後にプライマリユニットで ASA CLI を使い高度暗号化ライセンスを有効にする必要があります。高度暗号化（3DES）ライセンスの評価ライセンスは一切ありません。

Firepower 9300 シャーシ 上の ASA の ASA クラスタ ライセンス

マスター ユニットでのみライセンスを要求できます。ライセンスはスレーブ ユニットでは集約されます。複数のユニットにライセンスがある場合は、これらが統合されて単一の実行 ASA クラスタ ライセンスとなります。マスター ユニットで完了したライセンス設定はスレーブ ユニットに複製されません。クラスタリングを無効にし、ライセンスを設定し、クラスタリングを再度有効にした場合限り、スレーブユニットに個別のライセンス権限付与を設定できます。

（注） ASDM や他の高度暗号機能を使用するには、クラスタ展開後にマスター ユニットで ASA CLI を使用して高度暗号化（3DES）ライセンスを有効にする必要があります。このライセンスは、スレーブユニットによって継承されます。このライセンスは、各ユニットで個別に設定する必要はありません。高度暗号化（3DES）ライセンスの評価ライセンスは一切ありません。

（注） マスター ユニットに障害が発生し、30 日（ライセンス猶予期間）以内に再参加しない場合、継承されたライセンスは消滅します。その場合、新しいマスターユニットに消滅したライセンスを手動で設定する必要があります。

スマート ソフトウェア ライセンスの前提条件

- ASAv：デバイスからのインターネットアクセス、または HTTP プロキシアクセスを確保します。
- ASAv：デバイスが License Authority の名前を解決できるように DNS サーバを設定します。
- ASAv：デバイスのクロックを設定します。
- Firepower 9300 シャーシ：ASA ライセンス資格を設定する前に、Firepower 9300 シャーシでスマート ソフトウェア ライセンス インフラストラクチャを設定します。

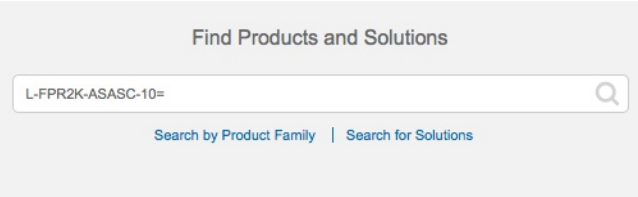
- Cisco Smart Software Manager でマスター アカウントを作成します。

  https://software.cisco.com/#module/SmartLicensing

  まだアカウントをお持ちでない場合は、リンクをクリックして新しいアカウントを設定してください。Smart Software Manager では、組織のマスター アカウントを作成できます。

- ライセンスは、シスコまたは販売代理店からデバイスを購入した際に、スマート ソフトウェア ライセンシング アカウントにリンクされています。ただし、主導でライセンスを追加する必要がある場合は、Cisco Commerce Workspace で [Find Products and Solutions] 検索フィールドを使用します。次のライセンス PID を検索します。

図 7:ライセンス検索



ASAv PID：

- ASAv5：L-ASAV5S-K9=
- ASAv10：L-ASAV10S-K9=
- ASAv30：L-ASAV30S-K9=
- ASAv50：L-ASAV50S-K9=

Firepower 4100 PID：

Firepower 9300 PID：

スマート ソフトウェア ライセンスのガイドライン

- スマート ソフトウェア ライセンスのみがサポートされます。ASAvの古いソフトウェアについては、PAK ライセンスが供与された既存の ASAv をアップグレードする場合、前にインストールしたアクティベーション キーは無視されますが、デバイスに保持されます。ASAv をダウングレードすると、アクティベーション キーが復活します。
- （FirePOWER 9300 ASA セキュリティ モジュール）ASDM および VPN などの他の強力な暗号化機能を使用するには、ASA の展開後、ASA CLI を使用するマスター ユニット上で Strong Encryption（3DES）ライセンスを有効にする必要があります。クラスタリングの場合、マスター ユニットのライセンスを設定します。このライセンスは、スレーブ ユニットによって継承されます。このライセンスは、各ユニットで個別に設定する必要はありません。

スマート ソフトウェア ライセンスのデフォルト

ASAv

- ASAv のデフォルト設定には、認証局の URL を指定する Smart Call Home プロファイルが含まれています。

```
call-home
  profile License
    destination address http
https://tools.cisco.com/its/service/oddce/services/DDCEService
```

- ASAv を導入するときに、機能層とスループット レベルを設定します。現時点では、標準レベルのみを使用できます。

```
license smart
  feature tier standard
  throughput level {100M | 1G | 2G}
```

- また、導入時に任意で HTTP プロキシを設定できます。

```
call-home
  http-proxy ip_address port port
```

Firepower 9300 シャーシ 上の ASA

デフォルト設定はありません。標準ライセンス階層、およびその他のオプション ライセンスは手動で有効化する必要があります。

ASAv：スマート ソフトウェア ライセンシングの設定

このセクションでは、ASAv にスマート ソフトウェア ライセンスを設定する方法を説明します。

手順

ASAv：スマート ソフトウェア ライセンシングの設定 （142 ページ）。

ASAv：スマート ソフトウェア ライセンシングの設定

ASAv を展開する場合は、デバイスを事前に設定し、License Authority に登録するために登録トークンを適用して、スマート ソフトウェア ライセンシングを有効にすることができます。HTTP プロキシ サーバ、ライセンス権限付与を変更する必要がある場合、または ASAv を登録する必要がある場合（Day0 コンフィギュレーションに ID トークンを含めなかった場合など）は、このタスクを実行します。

（注） ASAv を展開したときに、HTTP プロキシとライセンス権限付与が事前に設定されている可能性があります。また、ASAv を展開したときに Day0 コンフィギュレーションで登録トークンが含まれている可能性があります。その場合は、この手順を使用して再登録する必要はありません。

手順

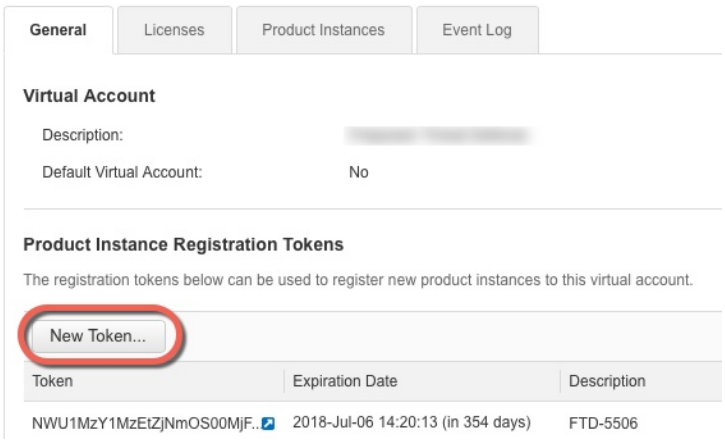
ステップ 1 Smart Software Manager（Cisco Smart Software Manager）で、このデバイスを追加するバーチャル アカウントの登録トークンを要求してコピーします。

a) [Inventory] をクリックします。

図 *8*：インベントリ

b) [General] タブで、[New Token] をクリックします。

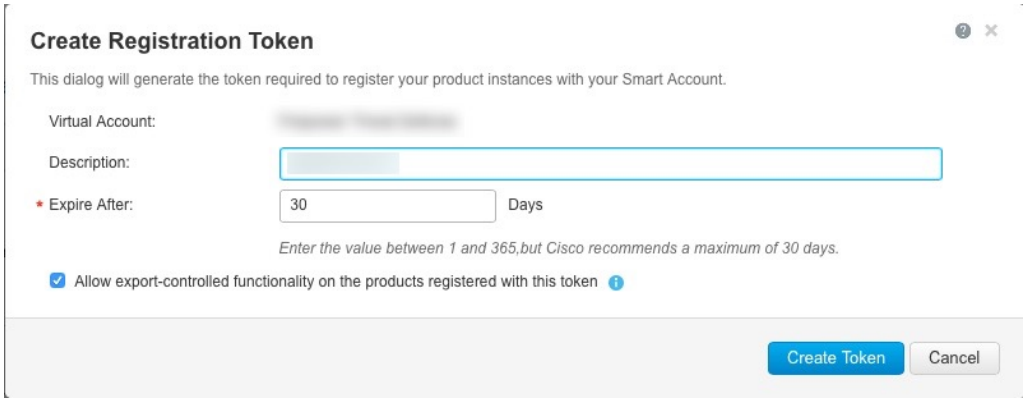
図 *9*：新しいトークン



c) [Create Registration Token] ダイアログボックスで、以下の設定値を入力してから [Create Token] をクリックします。

- **[説明（Description）]**
- Expire After：推奨値は 30 日です。
- Allow export-controlled functionaility on the products registered with this token：輸出コンプライアンス フラグを有効にします。

図 *10* : 登録トークンの作成



トークンはインベントリに追加されます。

d) トークンの右側にある矢印アイコンをクリックして [Token] ダイアログボックスを開き、トークン ID をクリップボードにコピーできるようにします。ASA の登録が必要なときに後の手順で使用するために、このトークンを準備しておきます。

図 *11* : トークンの表示

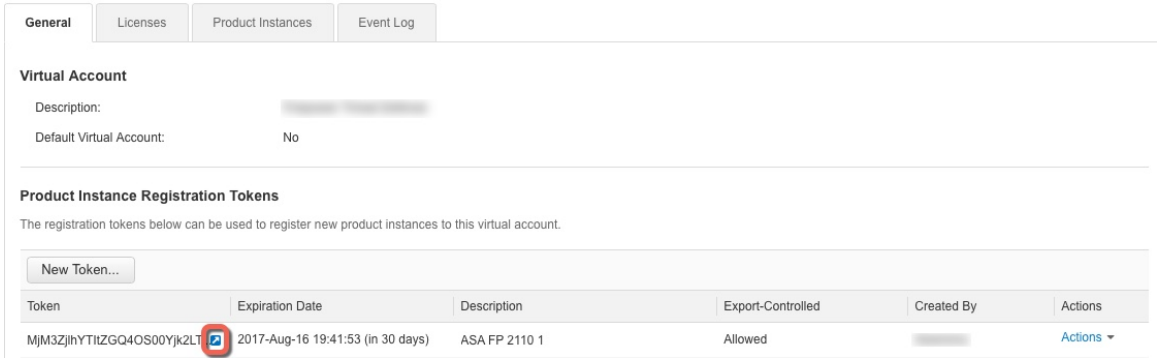
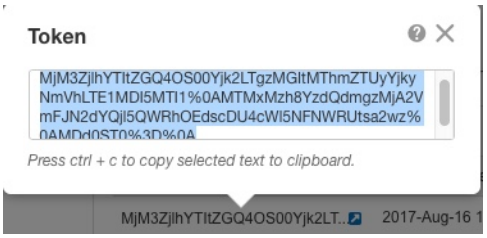


図 *12*：トークンのコピー



ステップ 2 （任意） ASAv で、HTTP プロキシ URL を指定します。

call-home

http-proxy *ip_address* **port** *port*

ネットワークでインターネット アクセスに HTTP プロキシを使用する場合、スマート ソフトウェア ライセンスのプロキシ アドレスを設定する必要があります。このプロキシは、一般に Smart Call Home にも使用されます。

例：

```
ciscoasa(config)# call-home
ciscoasa(cfg-call-home)# http-proxy 10.1.1.1 port 443
```

ステップ 3 ライセンス権限付与を設定します。

a) ライセンス スマート コンフィギュレーション モードを開始します。

license smart

例：

```
ciscoasa(config)# license smart
ciscoasa(config-smart-lic)#
```

b) 機能層を設定します。

feature tier standard

使用できるのは標準層だけです。

c) スループット レベルを設定します。

throughput level {100M | 1G | 2G}

例：

```
ciscoasa(config-smart-lic)# throughput level 2G
```

a) ライセンス スマート モードを終了して、変更を適用します。

exit

明示的にモードを終了する（**exit** または **end**）か、別のモードに移行するコマンドを入力することによってライセンス スマート コンフィギュレーション モードを終了するまで、変更が有効になりません。

例：

```
ciscoasa(config-smart-lic)# exit
ciscoasa(config)#
```

ステップ 4 ASAv の License Authority への登録.

License Authority に ASAv を登録すると、ASAv と License Authority の間の通信に使用する ID 証明書が発行されます。また、該当する仮想アカウントに ASAv が割り当てられます。通常、この手順は 1 回で済みます。ただし、通信の問題などが原因でアイデンティティ証明書の期限が切れた場合は、ASAv の再登録が必要になります。

a) ASAv の登録トークンを入力します。

license smart register idtoken *id_token* [**force**]

例：

force キーワードを使用すると、License Authority と同期されていない可能性がある登録済みの ASAv を登録できます。たとえば、Smart Software Manager から誤って ASAv を削除した場合に **force** を使用します。

ASAv は、License Authority への登録を試み、設定されたライセンス資格の認証を要求します。

例：

```
ciscoasa# license smart register idtoken YjE3Njc5MzYtMGQzMi00OTA4
LWJhODItNzBhMGQ5NGRlYjUxLTE0MTQ5NDAy%0AODQzNzl8NXk2bzV3SDE0ZkgwQk
dYRmZ1NTNCNGlvRnBHUFpjcm02WTB4TU4w%0Ac2NnMD0%3D%0A
```

（オプション）ASAv の登録解除

ASAv の登録を解除すると、アカウントから ASAv が削除され、ASAv のすべてのライセンス資格と証明書が削除されます。登録を解除することで、ライセンスを新しい ASAv に利用することもできます。あるいは、Smart Software Manager（SSM）から ASAv を削除できます。

手順

ASAv の登録解除

license smart deregister

ASAv がリロードされます。

（オプション）ASAv ID 証明書またはライセンス権限付与の更新

デフォルトでは、アイデンティティ証明書は 6 ヵ月ごと、ライセンス資格は 30 日ごとに自動的に更新されます。インターネット アクセスの期間が限られている場合や、Smart Software Manager でライセンスを変更した場合などは、これらの登録を手動で更新することもできます。

手順

ステップ 1 アイデンティティ証明書を更新します。

license smart renew id

ステップ 2 Renew the license entitlement:

license smart renew auth

Firepower 9300 シャーシ：スマート ソフトウェア ライセンシングの設定

この手順は、License Authority を使用するシャーシ、サテライト サーバのユーザに適用されます。方法を前提条件として設定するには、FXOS 設定ガイドを参照してください。。

（注） 高度暗号化（3DES/AES）ライセンスはデフォルトで有効になっていないため、ASA CLI を使用して高度暗号化ライセンスをリクエストするまで、ASA の設定に ASDM を使用することはできません。他の強力な暗号化機能も、このリクエストを行うまでは使用できません。

始める前に

ASA クラスタの場合は、設定作業のために標準出荷単位にアクセスする必要があります。Firepower Chassis Manager で、標準出荷単位を確認します。この手順に示すように、ASA CLI からも確認できます。

手順

ステップ 1 Firepower 9300 シャーシ CLI（コンソールまたは SSH）に接続し、次に ASA にセッション接続します。

connect module *slot* **console connect asa**

例：

```
Firepower> connect module 1 console
Firepower-module1> connect asa

asa>
```

次回 ASA コンソールに接続するときは、ASA に直接移動します。**connect asa** を再入力する必要はありません。

ASA クラスタの場合、ライセンス設定などの設定を行う場合にのみ、マスター ユニットにアクセスする必要があります。通常、マスターユニットがスロット 1 にあるため、このモジュールにまず接続する必要があります。

ステップ 2 ASA CLI で、グローバル コンフィギュレーション モードを入力します。デフォルトではイネーブル パスワードは空白ですが。

enable configure terminal

例：

```
asa> enable
Password:
asa# configure terminal
asa(config)#
```

ステップ 3 ASA クラスタの場合は、必要に応じて、このユニットが標準出荷単位であることを確認します。

show cluster info

例：

```
asa(config)# show cluster info
Cluster stbu: On
  This is "unit-1-1" in state SLAVE
    ID : 0
    Version : 9.5(2)
    Serial No.: P3000000025
    CCL IP : 127.2.1.1
    CCL MAC : 000b.fcf8.c192
    Last join : 17:08:59 UTC Sep 26 2015
    Last leave: N/A
Other members in the cluster:
  Unit "unit-1-2" in state SLAVE
    ID : 1
    Version : 9.5(2)
    Serial No.: P3000000001
```

```
    CCL IP : 127.2.1.2
    CCL MAC : 000b.fcf8.c162
    Last join : 19:13:11 UTC Sep 23 2015
    Last leave: N/A
  Unit "unit-1-3" in state MASTER
    ID : 2
    Version : 9.5(2)
    Serial No.: JAB0815R0JY
    CCL IP : 127.2.1.3
    CCL MAC : 000f.f775.541e
    Last join : 19:13:20 UTC Sep 23 2015
    Last leave: N/A
```

別のユニットが標準出荷単位の場合は、接続を終了し、正しいユニットに接続します。接続の終了については、以下を参照してください。

ステップ 4 ライセンス スマート コンフィギュレーション モードを開始します。

license smart

例：

```
ciscoasa(config)# license smart
ciscoasa(config-smart-lic)#
```

ステップ 5 機能層を設定します。

feature tier standard

使用できるのは標準層だけです。ティア ライセンスは、他の機能ライセンスを追加するための前提条件です。

ステップ 6 次の機能の 1 つ以上をリクエストします。

- モバイル SP （GTP/GPRS）

  feature mobile-sp

- セキュリティ コンテキスト

  feature context *<1-248>*

- 高度暗号化（3DES/AES）

  feature strong-encryption

例：

```
ciscoasa(config-smart-lic)# feature strong-encryption
ciscoasa(config-smart-lic)# feature context 50
```

ステップ 7 ASA コンソールを終了して Telnet アプリケーションに戻るには、プロンプトで「~」と入力します。スーパバイザ CLI に戻るには、「**quit**」と入力します。

モデルごとのライセンス

このセクションでは、ASAv および Firepower 9300 シャーシASA セキュリティ モジュールに使用可能なライセンス資格を示します。

ASAv

次の表に、ASAv シリーズのライセンス機能を示します。

ライセンス	**Standard ライセンス**	
ファイアウォール ライセンス		
Botnet Traffic Filter	イネーブル	
ファイアウォールの接続、同時	ASAv5：100,000 ASAv10：100,000 ASAv30：500,000	
GTP/GPRS	イネーブル	
合計 UC プロキシ セッション	ASAv5: 500 ASAv10：500 ASAv30：1000	
VPN ライセンス		
AnyConnect ピア	ディセーブル	オプションの *AnyConnect Plus* または *Apex* ライセンス、最大： *ASAv5: 50* *ASAv10*：*250* *ASAv30*：*750*
その他の VPN ピア	ASAv5：250 ASAv10：250 ASAv30：1000	
合計 VPN ピア。全タイプの合計	ASAv5：250 ASAv10：250 ASAv30：1000	

ライセンス	Standard ライセンス
一般ライセンス	
スループット レベル	ASAv5：1 Gbps ASAv10：1 Gbps ASAv30：2 Gbps
暗号化	Strong（3DES/AES）
フェールオーバー	アクティブ/スタンバイ
セキュリティ コンテキスト	サポートなし
クラスタ	サポートなし
VLAN、最大	ASAv5：50 ASAv10：50 ASAv30：200
RAM、vCPUs	ASAv5：2 GB、1 vCPU ASAv10：2 GB、1 vCPU ASAv30：8 GB、4 vCPU

Firepower 9300 ASA アプリケーション

次の表に、Firepower 9300 ASA アプリケーションのライセンス機能を示します。

ライセンス	Standard ライセンス	
ファイアウォール ライセンス		
Botnet Traffic Filter	サポートなし。	
ファイアウォールの接続、同時	Firepower 9300 SM-36：60,000,000、最大 70,000,000（3 モジュールを搭載したシャーシ） Firepower 9300 SM-24：55,000,000、最大 70,000,000（3 モジュールを搭載したシャーシ）	
GTP/GPRS	無効	オプション ライセンス：*Mobile SP*
合計 UC プロキシ セッション	15,000	
VPN は、Firepower Chassis Manager 1.1.2 以前にはサポートしていません。		

ライセンス	Standard ライセンス	
一般ライセンス		
暗号化	Base（DES）または Strong（3DES/AES）	
セキュリティ コンテキスト	10	オプション ライセンス：最大 *250*、*10* 単位
クラスタ	イネーブル	
VLAN、最大	1024	

Smart Software Licensing のモニタリング

デバッグ メッセージをイネーブルにするだけでなく、ライセンスの機能、ステータス、および証明書をモニタすることもできます。

現在のライセンスの表示

ライセンスを表示するには、次の コマンドを参照してください。

- **show license features**

  次に、基本ライセンスのみの ASAv の例を示します（現在のライセンス権限なし）。

```
Serial Number:  9AAHGX8514R

ASAv Platform License State: Unlicensed
No active entitlement: no feature tier configured

Licensed features for this platform:
Maximum Physical Interfaces       : 10             perpetual
Maximum VLANs                     : 50             perpetual
Inside Hosts                      : Unlimited      perpetual
Failover                          : Active/Standby perpetual
Encryption-DES                    : Enabled        perpetual
Encryption-3DES-AES               : Enabled        perpetual
Security Contexts                 : 0              perpetual
GTP/GPRS                          : Disabled       perpetual
AnyConnect Premium Peers          : 2              perpetual
AnyConnect Essentials             : Disabled       perpetual
Other VPN Peers                   : 250            perpetual
Total VPN Peers                   : 250            perpetual
Shared License                    : Disabled       perpetual
AnyConnect for Mobile             : Disabled       perpetual
AnyConnect for Cisco VPN Phone    : Disabled       perpetual
Advanced Endpoint Assessment      : Disabled       perpetual
UC Phone Proxy Sessions           : 2              perpetual
Total UC Proxy Sessions           : 2              perpetual
Botnet Traffic Filter             : Enabled        perpetual
Intercompany Media Engine         : Disabled       perpetual
Cluster                           : Disabled       perpetual
```

- **show license entitlement**

  使用中の各権限、ハンドル（整数 ID など）、数、タグ、強制モード（適合、非適合など）、バージョン、および権限が要求されたタイミングに関する詳細情報を表示します。

スマート ライセンス ステータスの表示

ライセンス ステータスを表示するには、次のコマンドを参照してください。

- **すべてのライセンスの表示**

  スマート ソフトウェア ライセンシング、スマート エージェントのバージョン、UDI 情報、スマート エージェントの状態、グローバル コンプライアンス ステータス、資格ステータス、使用許可証明書情報および予定のスマート エージェント タスクを表示します。

  次の例では、ASAv ライセンスを表示します。

```
ciscoasa# show license all

Cisco Smart Licensing Agent, Version 1.1.1

Smart Licensing Enabled: Yes

UDI:
PID:ASAv,SN:9AC5KH5H9FW

Compliance Status: In Compliance

Assigned License Pool: ASAv Internal Users

Grace period: Not in use

Entitlement:
   Tag: regid.2014-08.com.cisco.ASAv-STD-1G,1.0_4fd3bdbd-29ae-4cce-ad82-45ad3db1070c,
 Version: 1.0, Enforce Mode: Authorized
    Requested Time: Sep 15 13:08:23 2015 UTC,  Requested Count: 1
    Vendor String: (null)

Smart Licensing State: authorized (4)

Licensing Certificates:
    ID Cert Info:
        Start Date: Sep 15 12:59:29 2015 UTC. Expiry Date: Sep 14 12:59:29 2016 UTC

        Serial Number: 214929
        Version: 3
        Subject/SN: 16cab27f-a239-4d2d-a8db-d81dc48ec6bb
        Common Name: 55d246e3160a5dab39ec218f0b6b00f03422ef0d::1,2
    Signing Cert Info:
        Start Date: Jun 14 20:18:52 2013 UTC. Expiry Date: Apr 24 21:55:42 2033 UTC

        Serial Number: 3
        Version: 3

Upcoming Scheduled Jobs:
    Certificate Renewal: Mar 13 13:03:06 2016 UTC (172 days, 11 hours, 24 minutes,
8 seconds remaining)
   Certificate Expiration: Sep 14 13:00:03 2016 UTC (357 days, 11 hours, 21 minutes,
 5 seconds remaining)
```

```
    Authorization Renewal: Oct 22 18:58:18 2015 UTC (29 days, 17 hours, 19 minutes,
 20 seconds remaining)
   Authorization Expiration: Dec 21 18:55:28 2015 UTC (89 days, 17 hours, 16 minutes,
 30 seconds remaining)
    Daily Job: Sep 23 13:09:27 2015 UTC (11 hours, 30 minutes, 29 seconds remaining)

HA Info:    HA not available
    HA Sudi: Not Available
```

- **ライセンス登録の表示**：

  現在のスマート ライセンスの登録ステータスを表示します。

- **show license pool**

  このデバイスが割り当てられる権限付与プールを表示します。

アイデンティティ証明書情報の表示

ライセンス アイデンティティ証明書を表示するには、次のコマンドを参照してください。

- **show license cert**

  アイデンティティ証明書の内容、発行日、および有効期限を表示します。

スマート ソフトウェア ライセンスのデバッグ

クラスタリングのデバッグについては、次のコマンドを参照してください。

- **debug license agent** {**error** | **trace** | **debug** | **all**}

  スマート エージェントからのデバッグをオンにします。

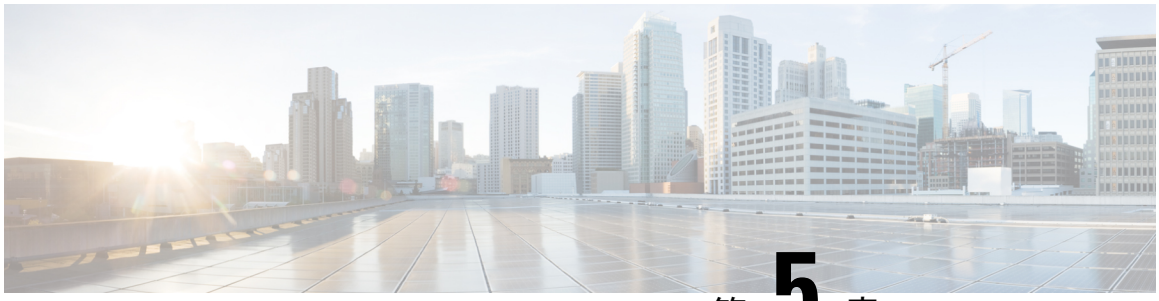
- **debug license** *level*

  Smart Software Licensing Manager のデバッグの各種レベルをオンにします。

スマート ソフトウェア ライセンスの履歴

機能名	プラットフォーム リリース	説明
FirePOWER 9300 の ASA のシスコ スマート ソフトウェア ライセンシング	9.4(1.150)	FirePOWER 9300 に ASA のシスコ スマート ソフトウェア ライセンシングが導入されました。 次のコマンドが導入されました。**feature strong-encryption**、**feature mobile-sp**、**feature context**

機能名	プラットフォーム リリース	説明
ASAv のシスコ スマート ソフトウェア ライセンシング	9.3(2)	Smart Software Licensing では、ライセンスのプールを購入して管理することができます。PAK ライセンスとは異なり、スマート ライセンスは特定のシリアル番号に関連付けられません。各ユニットのライセンス キーを管理しなくても、簡単に ASAv を導入したり導入を終了したりできます。スマート ソフトウェア ライセンスを利用すれば、ライセンスの使用状況と要件をひと目で確認することもできます。 **clear configure license**、**debug license agent**、**feature tier**、**http-proxy**、**license smart**、**license smart deregister**、**license smart register**、**license smart renew**、**show license**、**show running-config license**、**throughput level** 各コマンドが導入されました。



第 5 章

論理デバイス Firepower 9300

Firepower 9300は柔軟なセキュリティ プラットフォームが 1 つまたは複数の論理デバイスをインストールすることができます。この章では、基本的なインターフェイスの設定、および Firepower Chassis Manager を使用したスタンドアロンまたはハイ アベイラビリティ論理デバイスの追加方法について説明します。クラスタ化された論理デバイスを追加する場合は、Firepower 9300 シャーシ の ASA クラスタ （415 ページ）を参照してください。FXOS CLI を使用する場合は、FXOS CLI コンフィギュレーション ガイドを参照してください。高度な FXOS の手順とトラブルシューティングについては、FXOS コンフィギュレーション ガイドを参照してください。

Firepower インターフェイスについて

Firepower 9300 シャーシは、物理インターフェイスおよび EtherChannel（ポートチャネル）インターフェイスをサポートします。EtherChannel のインターフェイスには、同じタイプのメンバ インターフェイスを最大で 16 個含めることができます。

シャーシ管理インターフェイス

シャーシ管理インターフェイスは、SSH または Firepower Chassis Manager で、FXOS シャーシの管理に使用されます。このインターフェイスは、アプリケーション管理の論理デバイスに割り当てる管理タイプのインターフェイスから分離されています。

このインターフェイスのパラメータを設定するには、CLI から設定にする必要があります。このインターフェイスについての情報を FXOS CLI で表示するには、ローカル管理に接続し、管理ポートを表示します。

FirePOWER **connect local-mgmt**

firepower(local-mgmt) # **show mgmt-port**

物理ケーブルまたは SFP モジュールが取り外されている場合や **mgmt-port shut** コマンドが実行されている場合でも、シャーシ管理インターフェイスは稼働状態のままである点に注意してください。

インターフェイス タイプ

各インターフェイスは、次のいずれかのタイプになります。

- Data：通常のデータに使用します。データインターフェイスは論理デバイス間で共有できません。データインターフェイスを論理デバイス間で共有することはできません。また、論理デバイスからバックプレーンを介して他の論理デバイスに通信することはできません。データインターフェイスのトラフィックの場合、すべてのトラフィックは別の論理デバイスに到達するために、あるインターフェイスでシャーシを抜け出し、別のインターフェイスで戻る必要があります。
- Mgmt：アプリケーション インスタンスの管理に使用します。これらのインターフェイスは、外部ホストにアクセスするために 1 つまたは複数の論理デバイスで共有できます。論理デバイスが、このインターフェイスを介して、インターフェイスを共有する他の論理デバイスと通信することはできません。各論理デバイスには、管理インターフェイスを 1 つだけ割り当てることができます。
- Firepower-eventing：FTD デバイスのセカンダリ管理インターフェイスとして使用します。このインターフェイスを使用するには、FTD CLI で IP アドレスなどのパラメータを設定する必要があります。たとえば、イベント（Web イベントなど）から管理トラフィックを分類できます。Firepower Management Center 構成ガイドのシステム設定の章にある「管理インターフェイス」のセクションを参照してください。Firepower-eventing インターフェイスは、外部ホストにアクセスするために 1 つまたは複数の論理デバイスで共有できます。論理デバイスはこのインターフェイスを介してインターフェイスを共有する他の倫理デバイスと通信することはできません。
- Cluster：クラスタ化された論理デバイスのクラスタ制御リンクとして使用します。デフォルトでは、クラスタ制御リンクは 48 番のポートチャネル上に自動的に作成されます。このタイプは、EtherChannel インターフェイスのみでサポートされます。

シャーシとアプリケーションの独立したインターフェイスの状態

管理上、シャーシとアプリケーションの両方で、インターフェイスを有効および無効にできます。インターフェイスを動作させるには、両方のオペレーティング システムで、インターフェイスを有効にする必要があります。インターフェイスの状態は個別に制御されるので、シャーシとアプリケーションの間に不一致が生じることがあります。

論理デバイスについて

論理デバイスでは、1 つのアプリケーション インスタンス。

論理デバイスを追加するときに、アプリケーション インスタンスのタイプおよびバージョンの定義、インターフェイスの割り当て、アプリケーション構成にプッシュされるブートストラップ設定の構成も行います。

スタンドアロン論理デバイスとクラスタ化論理デバイス

次の論理デバイス タイプを追加できます。

- スタンドアロン：スタンドアロン論理デバイスは、スタンドアロン ユニットまたはハイアベイラビリティ ペアのユニットとして動作します。
- クラスタ：クラスタ化論理デバイスを使用すると複数の装置をグループ化することで、単一デバイスのすべての利便性（管理、ネットワークへの統合）を提供し、同時に複数デバイスによる高いスループットと冗長性を実現できます。Firepower 9300 などの複数のモジュール デバイスが、シャーシ内クラスタリングをサポートします。Firepower 9300 の場合、3 つすべてのモジュールが。

ハードウェアとソフトウェアの組み合わせの要件と前提条件

Firepower 9300では、複数のモデル、セキュリティモジュール、アプリケーションタイプ、および高可用性と拡張性の機能がサポートされています。許可された組み合わせについては、次の要件を参照してください。

Firepower 9300 の要件

Firepower 9300 には、3 つのセキュリティモジュール スロットと複数タイプのセキュリティモジュールが実装されています。次の要件を参照してください。

- セキュリティモジュール タイプ：Firepower 9300 のすべてのモジュールは同じタイプである必要があります。
- クラスタリング：クラスタ内またはシャーシ間であるかどうかにかかわらず、クラスタ内のすべてのセキュリティモジュールは同じタイプである必要があります。各シャーシに異なる数のセキュリティモジュールをインストールできますが、すべての空のスロットを含め、シャーシのすべてのモジュールをクラスタに含める必要があります。たとえば、シャーシ 1 に 2 つの SM-36 を、シャーシ 2 に 3 つの SM-36 をインストールできます。
- 高可用性：高可用性は Firepower 9300 の同じタイプのモジュール間でのみサポートされています。

- ASA および FTD のアプリケーションタイプ：シャーシ、ASA、または FTD には、1 つのアプリケーションタイプのみインストールできます。
- ASA または FTD のバージョン：個別のモジュールで異なるバージョンのアプリケーションインスタンス タイプを実行することもたとえば、モジュール 1 に FTD 6.3 を、モジュール 2 に FTD 6.4 を、モジュール 3 に FTD 6.5 をインストールできます。

論理デバイスに関する注意事項と制約事項

ガイドラインと制限事項については、以下のセクションを参照してください。

Firepower インターフェイスに関する注意事項と制約事項

デフォルトの MAC アドレス

デフォルトの MAC アドレスの割り当ては、インターフェイスのタイプによって異なります。

- 物理インターフェイス：物理インターフェイスは、Burned-in MAC Address を使用します。
- EtherChannel：EtherChannel の場合は、そのチャネル グループに含まれるすべてのインターフェイスが同じ MAC アドレスを共有します。この機能によって、EtherChannel はネットワーク アプリケーションとユーザに対してトランスペアレントになります。ネットワーク アプリケーションやユーザから見えるのは 1 つの論理接続のみであり、個々のリンクのことは認識しないためです。ポート チャネル インターフェイスは、プールからの一意の MAC アドレスを使用します。インターフェイスのメンバーシップは、MAC アドレスには影響しません。

一般的なガイドラインと制限事項

ファイアウォール モード

FTD のブートストラップ設定でファイアウォール モードをルーテッドまたはトランスペアレントに設定できます。 ASA の場合、展開後に、ファイアウォール モードをトランスペアレントに変更することができます。 ASA のトランスペアレント ファイアウォール モードへの変更（170 ページ）を参照してください。

ハイ アベイラビリティ

- アプリケーション設定内でハイアベイラビリティを設定します。
- 任意のデータ インターフェイスをフェールオーバー リンクおよびステート リンクとして使用できます。
- ハイ アベイラビリティ フェールオーバーを設定される 2 つのユニットは、次の条件を満たしている必要があります。

- 同じモデルであること。
- ハイ アベイラビリティ論理デバイスに同じインターフェイスが割り当てられていること。
- インターフェイスの数とタイプが同じであること。ハイアベイラビリティを有効にする前に、すべてのインターフェイスを FXOS で事前に同じ設定にすること。

- 詳細については、フェールオーバーのシステム要件（252ページ）を参照してください。

コンテキスト モード

- ASA ではマルチ コンテキスト モードはサポートされていません。
- 展開後に、ASA のマルチ コンテキスト モードを有効にします。
- の で TLS 暗号化アクセラレーション を有効にできます。

インターフェイスの設定

デフォルトでは、物理インターフェイスはディセーブルになっています。インターフェイスを有効にし、EtherChannels、、インターフェイス プロパティを編集して。

（注） FXOS でインターフェイスを削除した場合（たとえば、ネットワーク モジュールの削除、EtherChannel の削除、または EtherChannel へのインターフェイスの再割り当てなど）、必要な調整を行うことができるように、ASA 設定では元のコマンドが保持されます。設定からインターフェイスを削除すると、幅広い影響が出る可能性があります。ASA OS の古いインターフェイス設定は手動で削除できます。

物理インターフェイスの設定

インターフェイスを物理的に有効および無効にすること、およびインターフェイスの速度とデュプレックスを設定することができます。インターフェイスを使用するには、インターフェイスをFXOSで物理的に有効にし、アプリケーションで論理的に有効にする必要があります。

始める前に

- すでに EtherChannel のメンバーであるインターフェイスは個別に変更できません。EtherChannel に追加する前に、設定を行ってください。

手順

ステップ 1 インターフェイス モードに入ります。

scope eth-uplink

scope fabric a

ステップ 2 インターフェイスをイネーブルにします。

enter interface *interface_id*

enable

例：

```
Firepower /eth-uplink/fabric # enter interface Ethernet1/8
Firepower /eth-uplink/fabric/interface # enable
```

（注） すでにポートチャネルのメンバであるインターフェイスは個別に変更できません。ポート チャネルのメンバーであるインターフェイスで **enter interface** コマンドまたは **scope interface** コマンドを使用すると、オブジェクトが存在しないことを示すエラーを受け取ります。ポートチャネルに追加する前に、**enter interface** コマンドを使用してインターフェイスを編集する必要があります。

ステップ 3 （オプション）インターフェイス タイプを設定します。

set port-type {**data** | **mgmt** | **cluster**}

例：

```
Firepower /eth-uplink/fabric/interface # set port-type mgmt
```

data キーワードがデフォルトのタイプです。**cluster** キーワードは選択しないでください。デフォルトでは、クラスタ制御リンクはポートチャネル 48 に自動的に作成されます。

ステップ 4 インターフェイスでサポートされている場合、自動ネゴシエーションを有効化または無効化します。

set auto-negotiation {**on** | **off**}

例：

```
Firepower /eth-uplink/fabric/interface* # set auto-negotiation off
```

ステップ 5 インターフェイスの速度を設定します。

set admin-speed {**10mbps** | **100mbps** | **1gbps** | **10gbps** | **40gbps** | **100gbps**}

例：

```
Firepower /eth-uplink/fabric/interface* # set admin-speed 1gbps
```

ステップ 6 インターフェイスのデュプレックス モードを設定します。

set admin-duplex {**fullduplex** | **halfduplex**}

例：

```
Firepower /eth-uplink/fabric/interface* # set admin-duplex halfduplex
```

ステップ 7 デフォルトのフロー制御ポリシーを編集した場合は、インターフェイスにすでに適用されています。新しいポリシーを作成した場合は、そのポリシーをインターフェイスに適用します。

set flow-control-policy *name*

例：

```
Firepower /eth-uplink/fabric/interface* # set flow-control-policy flow1
```

ステップ 8 設定を保存します。

commit-buffer

例：

```
Firepower /eth-uplink/fabric/interface* # commit-buffer
Firepower /eth-uplink/fabric/interface #
```

EtherChannel（ポート チャネル）の追加

EtherChannel（別名ポート チャネル）には、同じタイプのメンバー インターフェイスを最大 16 個含めることができます。リンク集約制御プロトコル（LACP）では、2 つのネットワーク デバイス間でリンク集約制御プロトコル データ ユニット（LACPDU）を交換することによって、インターフェイスが集約されます。

各メンバー インターフェイスが LACP 更新を送受信するように、Firepower 9300 シャーシは Etherchannel をアクティブ LACP モードでしかサポートしません。アクティブ EtherChannel は、アクティブまたはパッシブ EtherChannel と接続を確立できます。LACP トラフィックを最小にする必要がある場合以外は、アクティブ モードを使用する必要があります。

LACP では、ユーザが介入しなくても、EtherChannel へのリンクの自動追加および削除が調整されます。また、コンフィギュレーションの誤りが処理され、メンバインターフェイスの両端が正しいチャネル グループに接続されていることがチェックされます。

手順

ステップ 1 インターフェイス モードを開始します。

scope eth-uplink

scope fabric a

ステップ 2 ポートチャネルを作成します。

create port-channel *ID*

enable

ステップ 3 メンバ インターフェイスを割り当てます。

create member-port *interface_id*

例：

```
Firepower /eth-uplink/fabric/port-channel* # create member-port Ethernet1/1
Firepower /eth-uplink/fabric/port-channel/member-port* # exit
Firepower /eth-uplink/fabric/port-channel* # create member-port Ethernet1/2
Firepower /eth-uplink/fabric/port-channel/member-port* # exit
Firepower /eth-uplink/fabric/port-channel* # create member-port Ethernet1/3
Firepower /eth-uplink/fabric/port-channel/member-port* # exit
Firepower /eth-uplink/fabric/port-channel* # create member-port Ethernet1/4
Firepower /eth-uplink/fabric/port-channel/member-port* # exit
```

ステップ 4 （任意） インターフェイス タイプを設定します。

set port-type {**data** | **mgmt** | **cluster**}

例：

```
Firepower /eth-uplink/fabric/port-channel # set port-type data
```

data キーワードがデフォルトのタイプです。デフォルトの代わりにこのポートチャネルをクラスタ制御リンクとして使用する場合以外は、**cluster** キーワードを選択しないでください。

ステップ 5 （任意） ポートチャネルのすべてのメンバーのインターフェイス速度を設定します。

set speed {**10mbps** | **100mbps** | **1gbps** | **10gbps** | **40gbps** | **100gbps**}

例：

```
Firepower /eth-uplink/fabric/port-channel* # set speed 1gbps
```

ステップ 6 （任意） ポートチャネルのすべてのメンバーのデュプレックスを設定します。

set duplex {**fullduplex** | **halfduplex**}

例：

```
Firepower /eth-uplink/fabric/port-channel* # set duplex fullduplex
```

ステップ 7 インターフェイスでサポートされている場合、自動ネゴシエーションを有効化または無効化します。

set auto-negotiation {**on** | **off**}

例：

```
Firepower /eth-uplink/fabric/interface* # set auto-negotiation off
```

ステップ 8 デフォルトのフロー制御ポリシーを編集した場合は、インターフェイスにすでに適用されています。新しいポリシーを作成した場合は、そのポリシーをインターフェイスに適用します。

set flow-control-policy *name*

例：

```
Firepower /eth-uplink/fabric/interface* # set flow-control-policy flow1
```

ステップ 9 設定をコミットします。

commit-buffer

論理デバイスの設定

Firepower 9300 シャーシに、スタンドアロン論理デバイスまたはハイ アベイラビリティ ペアを追加します。

クラスタ リングについては、#unique_207を参照してください。

スタンドアロン ASA の追加

スタンドアロンの論理デバイスは、単独またはハイ アベイラビリティ ペアで動作します。複数のセキュリティモジュールを搭載する Firepower 9300 では、クラスタまたはスタンドアロンデバイスのいずれかを展開できます。クラスタはすべてのモジュールを使用する必要があるため、たとえば、2モジュール クラスタと単一のスタンドアロンデバイスをうまく組み合わせることはできません。

Firepower 9300 シャーシからルーテッド ファイアウォール モード ASA を展開できます。ASA をトランスペアレント ファイアウォール モードに変更するには、この手順を完了し、ASA のトランスペアレント ファイアウォール モードへの変更 （170 ページ）を参照してください。

マルチ コンテキスト モードの場合、最初に論理デバイスを展開してから、ASA アプリケーションでマルチ コンテキスト モードを有効にする必要があります。

始める前に

- 論理デバイスに使用するアプリケーション イメージを Cisco.com からダウンロードして、そのイメージを Firepower 9300 シャーシ にダウンロードします。
- 論理デバイスで使用する管理インターフェイスを設定します。管理インターフェイスが必要です。この管理インターフェイスは、シャーシの管理のみに使用されるシャーシ管理ポートと同じではありません（FXOS では、MGMT、management0 のような名前で表示されます）。
- 次の情報を用意します。
  - このデバイスのインターフェイス ID
  - 管理インターフェイス IP アドレスとネットワーク マスク
  - ゲートウェイ IP アドレス

手順

ステップ 1 セキュリティ サービス モードを開始します。

scope ssa

例：

```
Firepower# scope ssa
Firepower /ssa #
```

ステップ 2 アプリケーション インスタンスのイメージ バージョンを設定します。

a) 使用可能なイメージを表示します。使用するバージョン番号をメモします。

show app

例：

```
Firepower /ssa # show app
    Name       Version         Author     Supported Deploy Types CSP Type    Is
Default App
    ---------- --------------- ---------- ---------------------- -----------
--------------
    asa        9.9.1           cisco      Native                 Application No
    asa        9.10.1          cisco      Native                 Application Yes
    ftd        6.2.3           cisco      Native                 Application Yes
```

b) セキュリティ モジュール/エンジン スロットに範囲を設定します。

scope slot *slot_id*

slot_id は、Firepower 9300 の場合は 1、2、または 3 です。

例：

```
Firepower /ssa # scope slot 1
Firepower /ssa/slot #
```

c) アプリケーション インスタンスを作成します。

enter app-instance asa

例：

```
Firepower /ssa/slot # enter app-instance asa
Firepower /ssa/slot/app-instance* #
```

d) ASA イメージバージョンを設定します。

set startup-version *version*

例：

```
Firepower /ssa/slot/app-instance* # set startup-version 9.10.1
```

e) スロット モードを終了します。

exit

例：

```
Firepower /ssa/slot/app-instance* # exit
Firepower /ssa/slot* #
```

f) 終了して ssa モードを開始します。

exit

例：

```
Firepower /ssa/slot* # exit
Firepower /ssa* #
```

例：

```
Firepower /ssa # scope slot 1
Firepower /ssa/slot # enter app-instance asa
Firepower /ssa/slot/app-instance* # set startup-version 9.10.1
Firepower /ssa/slot/app-instance* # exit
Firepower /ssa/slot* # exit
Firepower /ssa* #
```

ステップ 3 論理デバイスを作成します。

enter logical-device *device_name* **asa** *slot_id* **standalone**

例：

```
Firepower /ssa # enter logical-device ASA1 asa 1 standalone
Firepower /ssa/logical-device* #
```

ステップ 4 管理インターフェイスとデータインターフェイスを論理デバイスに割り当てます。各インターフェイスに対して、手順を繰り返します。

create external-port-link *name interface_id* **asa**

set description *description*

exit

- *name*：この名前は Firepower 9300 シャーシ スーパバイザによって使用されます。これは ASA の設定で使用するインターフェイス名ではありません。
- *description*：フレーズを引用符（"）で囲み、スペースを追加します。

管理インターフェイスは、シャーシ管理ポートとは異なります。ASA のデータ インターフェイスを後で有効にして設定します。これには、IP アドレスの設定も含まれます。

例：

```
Firepower /ssa/logical-device* # create external-port-link inside Ethernet1/1 asa
Firepower /ssa/logical-device/external-port-link* # set description "inside link"
Firepower /ssa/logical-device/external-port-link* # exit
Firepower /ssa/logical-device* # create external-port-link management Ethernet1/7 asa
Firepower /ssa/logical-device/external-port-link* # set description "management link"
Firepower /ssa/logical-device/external-port-link* # exit
Firepower /ssa/logical-device* # create external-port-link outside Ethernet1/2 asa
Firepower /ssa/logical-device/external-port-link* # set description "external link"
Firepower /ssa/logical-device/external-port-link* # exit
```

ステップ 5 管理ブートストラップ情報を設定します。

a) ブートストラップ オブジェクトを作成します。

create mgmt-bootstrap asa

例：

```
Firepower /ssa/logical-device* # create mgmt-bootstrap asa
Firepower /ssa/logical-device/mgmt-bootstrap* #
```

b) admin とを指定します。

create bootstrap-key-secret PASSWORD

set value

値の入力：*password*

値の確認：*password*

exit

例：

事前設定されているASA管理者ユーザはパスワードの回復時に役立ちます。FXOSアクセスができる場合、管理者ユーザ パスワードを忘れたときにリセットできます。

例：

```
Firepower /ssa/logical-device/mgmt-bootstrap* # create bootstrap-key-secret PASSWORD
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key-secret* # set value
Enter a value: floppylampshade
Confirm the value: floppylampshade
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key-secret* # exit
Firepower /ssa/logical-device/mgmt-bootstrap* #
```

c) IPv4 管理インターフェイスの設定を行います。

create ipv4 *slot_id* **default**

set ip *ip_address* **mask** *network_mask*

set gateway *gateway_address*

exit

例：

```
Firepower /ssa/logical-device/mgmt-bootstrap* # create ipv4 1 default
Firepower /ssa/logical-device/mgmt-bootstrap/ipv4* # set ip 10.10.10.34 mask
255.255.255.0
Firepower /ssa/logical-device/mgmt-bootstrap/ipv4* # set gateway 10.10.10.1
Firepower /ssa/logical-device/mgmt-bootstrap/ipv4* # exit
Firepower /ssa/logical-device/mgmt-bootstrap* #
```

d) IPv6 管理インターフェイスの設定を行います。

create ipv6 *slot_id* **default**

set ip *ip_address* **prefix-length** *prefix*

set gateway *gateway_address*

exit

例：

```
Firepower /ssa/logical-device/mgmt-bootstrap* # create ipv6 1 default
Firepower /ssa/logical-device/mgmt-bootstrap/ipv6* # set ip 2001:0DB8:BA98::3210
prefix-length 64
Firepower /ssa/logical-device/mgmt-bootstrap/ipv6* # set gateway 2001:0DB8:BA98::3211
Firepower /ssa/logical-device/mgmt-bootstrap/ipv6* # exit
Firepower /ssa/logical-device/mgmt-bootstrap* #
```

e) 管理ブートストラップ モードを終了します。

exit

例：

```
Firepower /ssa/logical-device/mgmt-bootstrap* # exit
Firepower /ssa/logical-device* #
```

ステップ 6 設定を保存します。

commit-buffer

シャーシは、指定したソフトウェアバージョンをダウンロードし、アプリケーションインスタンスにブートストラップ設定と管理インターフェイス設定をプッシュすることで、論理デバイスを導入します。**show app-instance** コマンドを使用して、導入のステータスを確認します。[Admin State] が [Enabled] で、[Oper State] が [Online] の場合、アプリケーション インスタンスは実行中であり、使用できる状態になっています。

例：

```
Firepower /ssa/logical-device* # commit-buffer
Firepower /ssa/logical-device # exit
Firepower /ssa # show app-instance
App Name   Identifier Slot ID    Admin State Oper State       Running Version Startup
Version Deploy Type Profile Name Cluster State   Cluster Role
---------- ---------- ---------- ----------- --------------- ---------------
--------------- ------------ ------------ ---------------- ------------
asa        asa1       2          Disabled    Not Installed                    9.12.1
       Native                    Not Applicable  None
ftd        ftd1       1          Enabled     Online          6.4.0.49         6.4.0.49
       Container   Default-Small Not Applicable  None
```

ステップ 7 セキュリティ ポリシーの設定を開始するには、ASA コンフィギュレーション ガイドを参照してください。

例

```
Firepower# scope ssa
Firepower /ssa # scope slot 1
Firepower /ssa/slot # enter app-instance asa
Firepower /ssa/slot/app-instance* # set startup-version 9.10.1
Firepower /ssa/slot/app-instance* # exit
Firepower /ssa/slot* # exit
Firepower /ssa* # create logical-device MyDevice1 asa 1 standalone
Firepower /ssa/logical-device* # create external-port-link inside Ethernet1/1 asa
Firepower /ssa/logical-device/external-port-link* # set description "inside link"
Firepower /ssa/logical-device/external-port-link* # exit
Firepower /ssa/logical-device* # create external-port-link management Ethernet1/7 asa
Firepower /ssa/logical-device/external-port-link* # set description "management link"
Firepower /ssa/logical-device/external-port-link* # exit
Firepower /ssa/logical-device* # create external-port-link outside Ethernet1/2 asa
Firepower /ssa/logical-device/external-port-link* # set description "external link"
Firepower /ssa/logical-device/external-port-link* # exit
Firepower /ssa/logical-device* # create mgmt-bootstrap asa
Firepower /ssa/logical-device/mgmt-bootstrap* # create bootstrap-key-secret PASSWORD
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key-secret* # set value
Enter a value: secretglassine
Confirm the value: secretglassine
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key-secret* # exit
Firepower /ssa/logical-device/mgmt-bootstrap* # create ipv4 1 default
Firepower /ssa/logical-device/mgmt-bootstrap/ipv4* # set gateway 10.0.0.1
Firepower /ssa/logical-device/mgmt-bootstrap/ipv4* # set ip 10.0.0.31 mask 255.255.255.0
Firepower /ssa/logical-device/mgmt-bootstrap/ipv4* # exit
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key* # commit-buffer
```

```
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key #
```

ハイ アベイラビリティ ペアの追加

ASA ハイ アベイラビリティ（フェールオーバーとも呼ばれます）は、FXOS ではなくアプリケーション内で設定されます。ただし、ハイアベイラビリティのシャーシを準備するには、次の手順を参照してください。

始める前に

- ハイ アベイラビリティ フェールオーバーを設定される 2 つのユニットは、次の条件を満たしている必要があります。
  - 同じモデルであること。
  - ハイアベイラビリティ論理デバイスに同じインターフェイスが割り当てられていること。
  - インターフェイスの数とタイプが同じであること。ハイアベイラビリティを有効にする前に、すべてのインターフェイスを FXOS で事前に同じ設定にすること。
- 高可用性システム要件については、フェールオーバーのシステム要件（252ページ）を参照してください。

手順

ステップ 1 各論理デバイスは個別のシャーシ上にある必要があります。Firepower 9300 のシャーシ内のハイ アベイラビリティは推奨されず、サポートされない可能性があります。

ステップ 2 各論理デバイスに同一のインターフェイスを割り当てます。

ステップ 3 フェールオーバー リンクとステート リンクに 1 つまたは 2 つのデータ インターフェイスを割り当てます。

これらのインターフェイスは、2つのシャーシ間でハイ アベイラビリティ トラフィックを交換します。統合されたフェールオーバー リンクとステート リンクには、10GB のデータ インターフェイスを使用することを推奨します。別のフェールオーバーおよび状態のリンクを使用できます使用可能なインターフェイスがあれば、状態のリンクには、ほとんどの帯域幅が必要です。フェールオーバー リンクまたはステート リンクに管理タイプのインターフェイスを使用することはできません。同じネットワーク セグメント上で他のデバイスをフェールオーバー インターフェイスとして使用せずに、シャーシ間でスイッチを使用することをお勧めします。

ステップ 4 論理デバイスでハイ アベイラビリテを有効にします。ハイ アベイラビリティのためのフェールオーバー（251 ページ）を参照してください。

ステップ 5 ハイアベイラビリティを有効にした後でインターフェイスを変更する必要がある場合は、最初にスタンバイ装置で変更を実行してから、アクティブ装置で変更を実行します。

（注） ASA の場合、FXOS でインターフェイスを削除すると（たとえば、ネットワーク モジュールの削除、EtherChannel の削除、または EtherChannel へのインターフェイスの再割り当てなど）、必要な調整を行うことができるように、ASA 設定では元のコマンドが保持されます。設定からインターフェイスを削除すると、幅広い影響が出る可能性があります。ASA OS の古いインターフェイス設定は手動で削除できます。

ASA のトランスペアレント ファイアウォール モードへの変更

Firepower 9300 シャーシのルーテッド ファイアウォール モード ASA のみを導入できます。ASA をトランスペアレント ファイアウォール モードに変更するには、初期導入を完了し、ASA CLI 内でファイアウォール モードを変更します。スタンドアロン ASA の場合、ファイアウォール モードを変更すると設定が消去されるため、Firepower 9300 シャーシ から設定を再展開して、ブートストラップ設定を回復する必要があります。ASA はトランスペアレント モードのままで、ブートストラップ設定が機能した状態になっています。クラスタ化 ASA の場合、設定は消去されないため、FXOS からブートストラップ設定を再導入する必要はありません。

手順

ステップ 1 アプリケーションのコンソールへの接続（172 ページ）に従って、ASA コンソールに接続します。クラスタの場合、プライマリ ユニットに接続します。フェールオーバー ペアの場合、アクティブ ユニットに接続します。

ステップ 2 コンフィギュレーション モードに入ります。

enable

configure terminal

デフォルトでは、イネーブル パスワードは空白です。

ステップ 3 ファイアウォール モードをトランスペアレントに設定します。

firewall transparent

ステップ 4 設定を保存します。

write memory

クラスタまたはフェールオーバー ペアの場合、この設定はセカンダリ ユニットに複製されます。

```
asa(config)# firewall transparent
asa(config)# write memory
Building configuration...
Cryptochecksum: 9f831dfb 60dffa8c 1d939884 74735b69

3791 bytes copied in 0.160 secs
[OK]
asa(config)#
```

```
Beginning configuration replication to Slave unit-1-2
 End Configuration Replication to slave.

asa(config)#
```

ステップ 5 Firepower Chassis Manager の [Logical Devices] ページで、[Edit] アイコンをクリックして ASA を編集します。

[Provisioning] ページが表示されます。

ステップ 6 デバイスのアイコンをクリックして、ブートストラップ設定を編集します。設定の値を変更し、[OK] をクリックします。

少なくとも 1 つのフィールド（[Password] フィールドなど）の値を変更する必要があります。

ブートストラップ設定の変更に関する警告が表示されます。[Yes] をクリックします。

ステップ 7 ASA に設定を再配置する**保存**をクリックします。

シャーシ/セキュリティ モジュールがリロードし、ASA が再度稼働するまで数分待ちます。ASA は、これでブートストラップ設定が機能するようになりますが、トランスペアレント モードのままです。

ASA 論理デバイスのインターフェイスの変更

ASA 論理デバイスでは、管理インターフェイスの割り当て、割り当て解除、または置き換えを行うことができます。ASDM は、新しいインターフェイスを自動的に検出します。

新しいインターフェイスを追加したり、未使用のインターフェイスを削除したりしても、ASA の設定に与える影響は最小限です。ただし、FXOS で割り当てられたインターフェイスを削除する場合（ネットワーク モジュールの削除、EtherChannel の削除、割り当てられたインターフェイスの EtherChannel への再割り当てなど）、そのインターフェイスがセキュリティポリシーで使用されると、削除は ASA の設定に影響を与えます。この場合、ASA 設定では元のコマンドが保持されるため、必要な調整を行うことができます。ASA OS の古いインターフェイス設定は手動で削除できます。

（注） 論理デバイスに影響を与えずに、割り当てられた EtherChannel のメンバーシップを編集できます。

始める前に

- 物理インターフェイスの設定 （159 ページ）および EtherChannel（ポート チャネル）の追加 （161 ページ）に従って、インターフェイスを設定し、EtherChannel を追加します。
- すでに割り当てられているインターフェイスを EtherChannel に追加するには（たとえば、デフォルトではすべてのインターフェイスがクラスタに割り当てられます）、まず論理デ

バイスからインターフェイスの割り当てを解除し、次にEtherChannelにインターフェイスを追加する必要があります。新しいEtherChannelの場合、デバイスにEtherChannelを割り当てることができます。

- クラスタ リングまたはフェールオーバーを追加するか、すべてのユニット上のインターフェイスの削除を確認します。最初にスレーブ/スタンバイ ユニットでインターフェイスを変更してから、マスター/アクティブ ユニットで変更することをお勧めします。新しいインターフェイスは管理上ダウンした状態で追加されるため、インターフェイスモニタリングに影響を及ぼしません。

手順

ステップ 1 セキュリティ サービス モードを開始します。

Firepower# **scope ssa**

ステップ 2 論理デバイスを編集します。

Firepower /ssa # **scope logical-device** *device_name*

ステップ 3 論理デバイスからインターフェイスの割り当てを解除します。

Firepower /ssa/logical-device # **delete external-port-link** *name*

show external-port-link コマンドを入力して、インターフェイス名を表示します。

管理インターフェイスの場合、新しい管理インターフェイスを追加する前に、現在のインターフェイスを削除し、**commit-buffer** コマンドを使用して変更をコミットします。

ステップ 4 論理デバイスに新しいインターフェイスを割り当てます。

Firepower /ssa/logical-device* # **create external-port-link** *name interface_id* **asa**

ステップ 5 設定をコミットします。

commit-buffer

トランザクションをシステムの設定にコミットします。

アプリケーションのコンソールへの接続

次の手順に従ってアプリケーションのコンソールに接続します。

手順

ステップ 1 、モジュール CLI に接続します。

connect module *slot_number* **console**

複数のセキュリティ モジュールをサポートしないデバイスのセキュリティ エンジンに接続するには、*slot_number* として **1** を使用します。

例：

```
Firepower# connect module 1 console
Telnet escape character is '~'.
Trying 127.5.1.1...
Connected to 127.5.1.1.
Escape character is '~'.

CISCO Serial Over LAN:
Close Network Connection to Exit

Firepower-module1>
```

ステップ 2 アプリケーションのコンソールに接続します。

connect asa

例：

```
Firepower-module1> connect asa
Connecting to asa(asa1) console... hit Ctrl + A + D  to return to bootCLI
[...]
asa>
```

ステップ 3 アプリケーション コンソールを終了して FXOS モジュール CLI に移動します。

- ASA：**Ctrl-a, d** と入力

ステップ 4 FXOS CLI のスーパバイザ レベルに戻ります。

a) ~ と入力

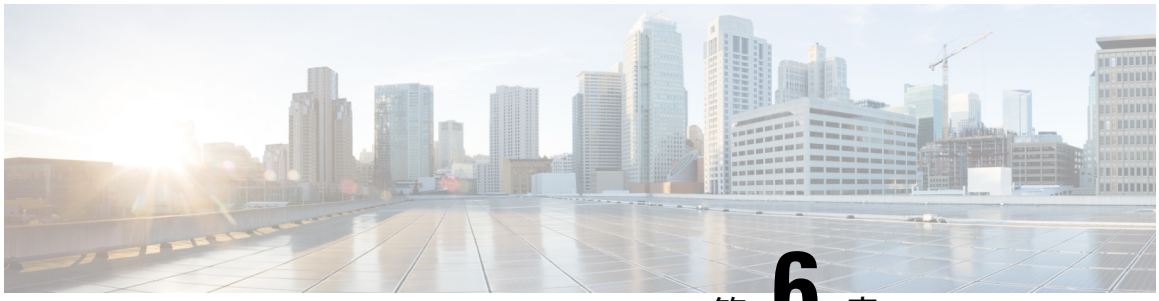
Telnet アプリケーションに切り替わります。

b) Telnet アプリケーションを終了するには、次を入力します。

telnet>**quit**

論理デバイスの履歴

機能	バージョン	詳細
Firepower 9300 用シャーシ内 ASA クラスタリング	9.4（1.150）	FirePOWER 9300 シャーシ内では、最大 3 つセキュリティ モジュールをクラスタ化できます。シャーシ内のすべてのモジュールは、クラスタに属している必要があります。 次のコマンドを導入しました。**cluster replication delay**、**debug service-module**、**management-only individual**、**show cluster chassis**



第 6 章

トランスペアレントファイアウォールモードまたはルーテッドファイアウォールモード

この章では、ファイアウォール モードをルーテッドまたはトランスペアレントに設定する方法と、ファイアウォールが各ファイアウォール モードでどのように機能するかについて説明します。

マルチコンテキスト モードでは、コンテキストごとに別個にファイアウォール モードを設定できます。

ファイアウォール モードについて

ASA は、でルーテッド ファイアウォール モードとトランスペアレント ファイアウォール モードの 2 つのファイアウォール モードをサポートします。

ルーテッド ファイアウォール モードについて

ルーテッド モードでは、ASAはネットワーク内のルータ ホップと見なされます。ルーティングを行う各インターフェイスは異なるサブネット上にあります。 コンテキスト間でレイヤ3インターフェイスを共有することもできます。

トランスペアレント ファイアウォール モードについて

従来、ファイアウォールはルーテッドホップであり、保護されたサブネットのいずれかに接続するホストのデフォルト ゲートウェイとして機能します。これに対し、トランスペアレント ファイアウォールは、「Bump In The Wire」または「ステルス ファイアウォール」のように動作するレイヤ2ファイアウォールであり、接続されたデバイスへのルータ ホップとしては認識されません。ただし、他のファイアウォールのように、インターフェイス間のアクセス制御は管理され、ファイアウォールによる通常のすべてのチェックが実施されます。

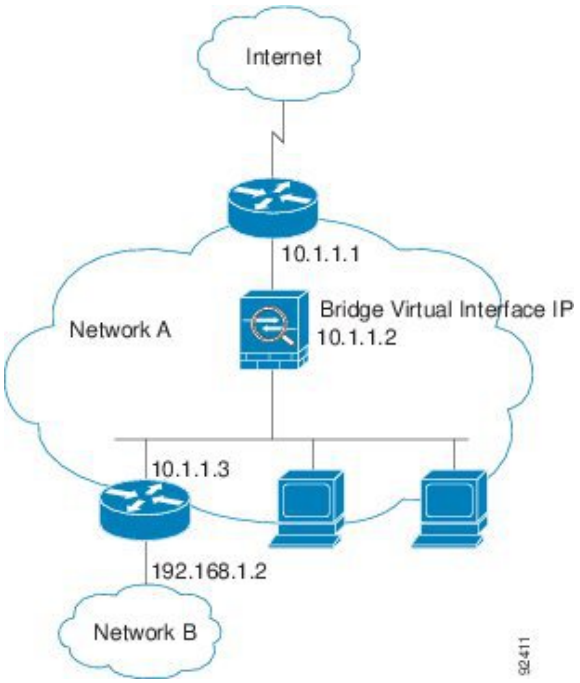
レイヤ 2 の接続は、ネットワークの内部と外部のインターフェイスをまとめた「ブリッジグループ」を使用して実現されます。また、ASA はブリッジング技術を使用してインターフェイス間のトラフィックを通すことができます。各ブリッジ グループには、ネットワーク上で IP アドレスが割り当てられるブリッジ仮想インターフェイス（BVI）が含まれます。複数のネットワークに複数のブリッジ グループを設定できます。トランスペアレント モードでは、これらのブリッジ グループは相互通信できません。

ネットワーク内でトランスペアレント ファイアウォールの使用

ASA は、自身のインターフェイス間を同じネットワークで接続します。トランスペアレント ファイアウォールはルーティングされたホップではないため、既存のネットワークに簡単に導入できます。

次の図に、外部デバイスが内部デバイスと同じサブネット上にある一般的なトランスペアレント ファイアウォール ネットワークを示します。内部ルータとホストは、外部ルータに直接接続されているように見えます。

図 *13:* トランスペアレント ファイアウォール ネットワーク



ブリッジグループについて

ブリッジ グループは、ASA がルーティングではなくブリッジするインターフェイスのグループです。 ブリッジグループはトランスペアレント ファイアウォール モードでのみサポートされています。他のファイアウォールインターフェイスのように、インターフェイス間のアクセス制御は管理され、ファイアウォールによる通常のすべてのチェックが実施されます。

ブリッジ仮想インターフェイス（BVI）

各ブリッジ グループには、ブリッジ仮想インターフェイス（BVI）が含まれます。ASA は、ブリッジ グループから発信されるパケットの送信元アドレスとしてこの BVI IP アドレスを使用します。BVI IP アドレスはブリッジ グループ メンバー インターフェイスと同じサブネット上になければなりません。BVI では、セカンダリ ネットワーク上のトラフィックはサポートされていません。BVI IP アドレスと同じネットワーク上のトラフィックだけがサポートされています。

インターフェイス ベースの各機能はブリッジ グループのメンバー インターフェイスだけを指定でき、これらについてのみ使用できます。

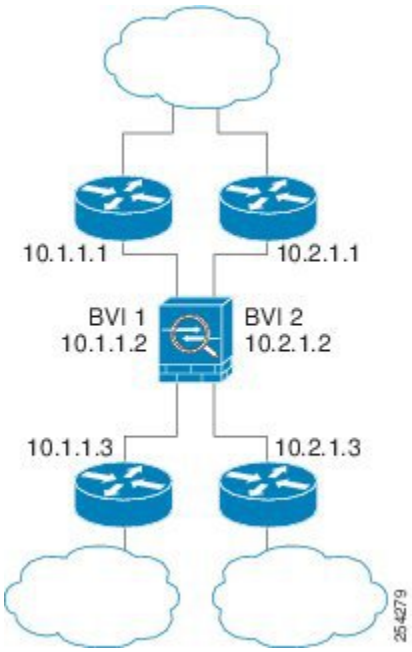
トランスペアレント ファイアウォール モードのブリッジ グループ

ブリッジグループのトラフィックは他のブリッジグループから隔離され、トラフィックはASA 内の他のブリッジグループにはルーティングされません。また、トラフィックは外部ルータから ASA 内の他のブリッジ グループにルーティングされる前に、ASA から出る必要があります。ブリッジング機能はブリッジ グループごとに分かれていますが、その他の多くの機能はすべてのブリッジ グループ間で共有されます。たとえば、syslog サーバまたは AAA サーバの設定は、すべてのブリッジ グループで共有されます。セキュリティ ポリシーを完全に分離するには、各コンテキスト内に 1 つのブリッジ グループにして、セキュリティ コンテキストを使用します。

1 つのブリッジグループにつき複数のインターフェイスを入れることができます。サポートされるブリッジ グループとインターフェイスの正確な数については、ファイアウォール モードのガイドライン （183 ページ）を参照してください。ブリッジグループごとに 2 つ以上のインターフェイスを使用する場合は、内部、外部への通信だけでなく、同一ネットワーク上の複数のセグメント間の通信を制御できます。たとえば、相互通信を希望しない内部セグメントが 3 つある場合、インターフェイスを別々のセグメントに置き、外部インターフェイスとのみ通信させることができます。または、インターフェイス間のアクセスルールをカスタマイズし、希望通りのアクセスを設定できます。

次の図に、2 つのブリッジ グループを持つ、ASA に接続されている 2 つのネットワークを示します。

図 *14 : 2* つのブリッジ グループを持つトランスペアレント ファイアウォール ネットワーク



管理 [インターフェイス（Interface）]

各ブリッジ仮想インターフェイス（BVI）IP アドレスのほかに、別の管理 スロット/ポート インターフェイスを追加できます。このインターフェイスはどのブリッジグループにも属さず、ASA への管理トラフィックのみを許可します。詳細については、管理インターフェイス（466 ページ）を参照してください。

レイヤ 3 トラフィックの許可

- ユニキャストの IPv4 および IPv6 トラフィックは、セキュリティの高いインターフェイスからセキュリティの低いインターフェイスに移動する場合、アクセス ルールなしで自動的にブリッジ グループを通過できます。
- セキュリティの低いインターフェイスからセキュリティの高いインターフェイスに移動するレイヤ 3 トラフィックの場合、セキュリティの低いインターフェイスでアクセル ルールが必要です。
- ARP は、アクセス ルールなしで両方向にブリッジグループを通過できます。ARP トラフィックは、ARP インスペクションによって制御できます。
- IPv6 ネイバー探索およびルータ送信要求パケットは、アクセス ルールを使用して通過させることができます。
- ブロードキャストおよびマルチキャスト トラフィックは、アクセス ルールを使用して通過させることができます。

許可される MAC アドレス

アクセス ポリシーで許可されている場合、以下の宛先 MAC アドレスをブリッジグループで使用できます（レイヤ 3 トラフィックの許可（178 ページ）を参照）。このリストにない MAC アドレスはドロップされます。

- FFFF.FFFF.FFFF の TRUE ブロードキャスト宛先 MAC アドレス
- 0100.5E00.0000 ～ 0100.5EFE.FFFF までの IPv4 マルチキャスト MAC アドレス
- 3333.0000.0000 ～ 3333.FFFF.FFFF までの IPv6 マルチキャスト MAC アドレス
- 0100.0CCC.CCCD の BPDU マルチキャスト アドレス
- 0900.0700.0000 ～ 0900.07FF.FFFF までの AppleTalk マルチキャスト MAC アドレス

ルーテッド モードで許可されないトラフィックの通過

ルーテッド モードでは、アクセス ルールで許可しても、いくつかのタイプのトラフィックは ASA を通過できません。ただし、ブリッジグループは、アクセス ルール（IP トラフィックの場合）または EtherType ルール（非 IP トラフィックの場合）を使用してほとんどすべてのトラフィックを許可できます。

- IP トラフィック：ルーテッド ファイアウォール モードでは、ブロードキャストとマルチキャスト トラフィックは、アクセス ルールで許可されている場合でもブロックされます。これには、サポートされていないダイナミック ルーティング プロトコルおよび DHCP（DHCP リレーを設定している場合を除く）が含まれます。ブリッジ グループ内では、このトラフィックをアクセス ルール（拡張 ACL を使用）で許可できます。
- 非 IP トラフィック：AppleTalk、IPX、BPDU や MPLS などは、EtherType ルールを使用することで、通過するように設定できます。

（注） ブリッジ グループは、CDP パケットおよび 0x600 以上の有効な EtherType を持たないパケットの通過を拒否します。サポートされる例外は、BPDU および IS-IS です。

BPDU の処理

スパニング ツリー プロトコルの使用によるループを回避するために、デフォルトで BPDU が渡されます。BPDU をブロックするには、これらを拒否する EtherType ルールを設定する必要があります。フェールオーバーを使用している場合、BPDU をブロックして、トポロジが変更されたときにスイッチ ポートがブロッキング ステートに移行することを回避できます。詳細については、「フェールオーバーのトランスペアレント ファイアウォール モード ブリッジ グループ要件 （268 ページ）」を参照してください。

MAC アドレスとルート ルックアップ

ブリッジ グループ内のトラフィックでは、パケットの発信インターフェイスは、ルート ルックアップではなく宛先 MAC アドレス ルックアップを実行することによって決定されます。

ただし、次の場合にはルート ルックアップが必要です。

- トラフィックの発信元が ASA：syslog サーバなどがあるリモート ネットワーク宛てのトラフィック用に、ASA にデフォルト/スタティック ルートを追加します。
- インスペクションが有効になっている Voice over IP（VoIP）および TFTP トラフィック、エンドポイントが 1 ホップ以上離れている：セカンダリ接続が成功するように、リモート エンドポイント宛てのトラフィック用に、ASA にスタティック ルートを追加します。ASA は、セカンダリ接続を許可するためにアクセス コントロール ポリシーに一時的な「ピンホール」を作成します。セカンダリ接続ではプライマリ接続とは異なる IP アドレスのセットが使用される可能性があるため、ASA は正しいインターフェイスにピンホールをインストールするために、ルート ルックアップを実行する必要があります。

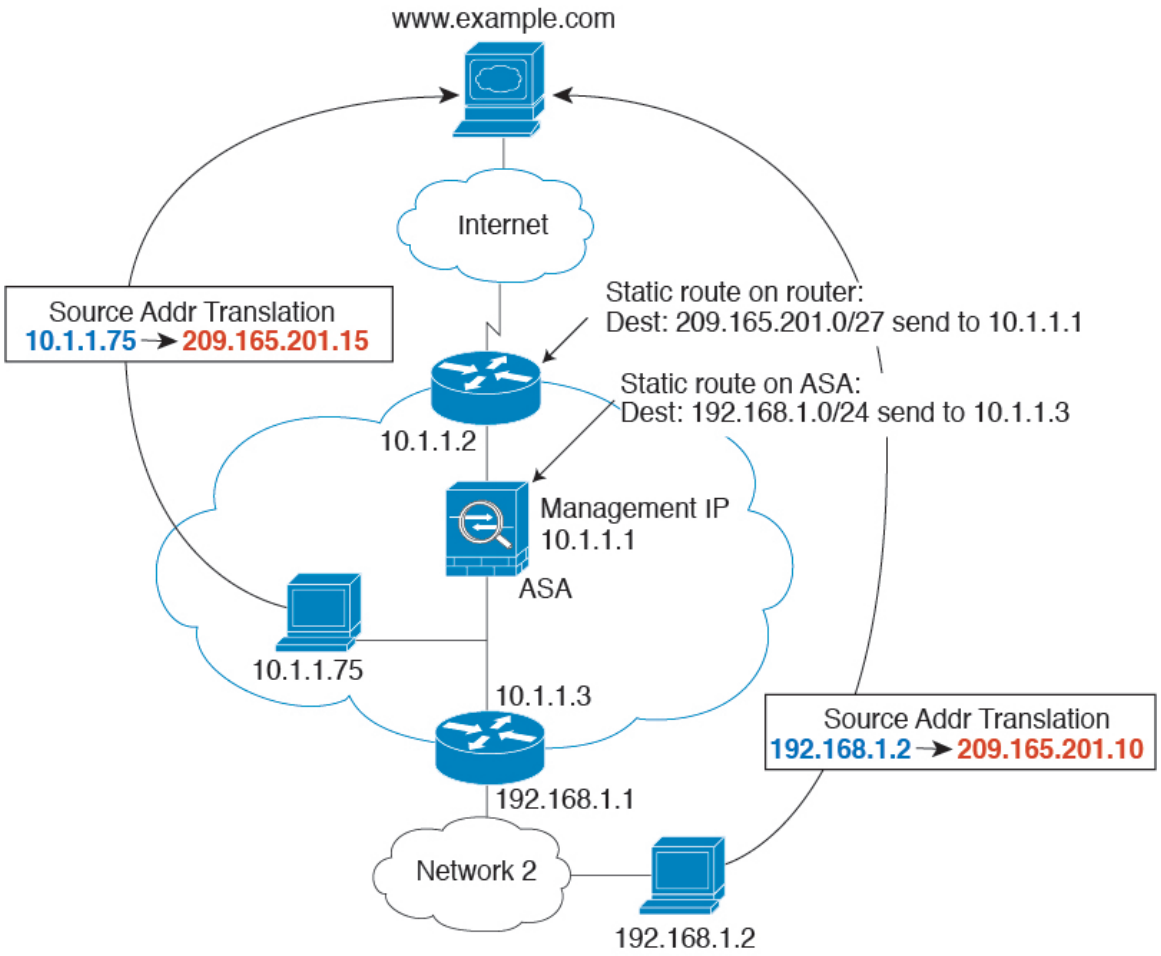
  影響を受けるアプリケーションは次のとおりです。

  - CTIQBE
  - GTP
  - H.323
  - MGCP
  - RTSP
  - SIP
  - Skinny（SCCP）
  - SQL*Net
  - SunRPC
  - TFTP

- ASA が NAT を実行する 1 ホップ以上離れたトラフィック：リモート ネットワーク宛てのトラフィック用に、ASA にスタティック ルートを設定します。また、ASA に送信されるマッピング アドレス宛てのトラフィック用に、上流に位置するルータにもスタティック ルートが必要です。

  このルーティング要件は、インスペクションと NAT が有効になっている VoIP と DNS の、1 ホップ以上離れている組み込み IP アドレスにも適用されます。ASA は、変換を実行できるように正しい出力インターフェイスを識別する必要があります。

図 *15 : NAT* の例：ブリッジ グループ内の *NAT*



トランスペアレント モードのブリッジ グループのサポートされていない機能

次の表に、トランスペアレント モードのブリッジ グループでサポートされない機能を示します。

表 *3 :* トランスペアレント モードでサポートされない機能

機能	説明
ダイナミック DNS	-

機能	説明
DHCP リレー	トランスペアレント ファイアウォールは DHCPv4 サーバとして機能することができますが、DHCP リレー コマンドはサポートしません。2つのアクセスルールを使用してDHCP トラフィックを通過させることができるので、DHCP リレーは必要ありません。1つは内部インターフェイスから外部インターフェイスへの DHCP 要求を許可し、もう 1 つはサーバからの応答を逆方向に許可します。
ダイナミック ルーティング プロトコル	ただし、ブリッジグループ メンバー インターフェイスの場合、ASAで発信されたトラフィックにスタティック ルートを追加できます。アクセス ルールを使用して、ダイナミック ルーティング プロトコルがASAを通過できるようにすることもできます。
マルチキャスト IP ルーティング	アクセス ルールで許可することによって、マルチキャスト トラフィックがASAを通過できるようにすることができます。
QoS	—
通過トラフィック用のVPNターミネーション	トランスペアレント ファイアウォールは、ブリッジグループ メンバー インターフェイスでのみ、管理接続用のサイト間VPNトンネルをサポートします。これは、ASAを通過するトラフィックに対して VPN 接続を終端しません。アクセス ルールを使用して VPN トラフィックにASA を通過させることはできますが、非管理接続は終端されません。クライアントレス SSL VPN もサポートされていません。
ユニファイド コミュニケーション	—

ルーテッド モード機能のためのトラフィックの通過

トランスペアレントファイアウォールで直接サポートされていない機能の場合は、アップストリーム ルータとダウンストリーム ルータが機能をサポートできるようにトラフィックの通過を許可することができます。たとえば、アクセスルールを使用することによって、（サポートされていない DHCP リレー機能の代わりに）DHCP トラフィックを許可したり、IP/TV で作成されるようなマルチキャスト トラフィックを許可したりできます。また、トランスペアレントファイアウォールを通過するルーティング プロトコル隣接関係を確立することもできます。つ

まり、OSPF、RIP、EIGRP、または BGP トラフィックをアクセス ルールに基づいて許可できます。同様に、HSRP や VRRP などのプロトコルは ASA を通過できます。

デフォルト設定

デフォルト モード

デフォルト モードはルーテッド モードです。

ブリッジグループのデフォルト

デフォルトでは、すべての ARP パケットはブリッジ グループ内で渡されます。

ファイアウォール モードのガイドライン

コンテキスト モードのガイドライン

コンテキストごとにファイアウォール モードを設定します。

ブリッジグループのガイドライン（トランスペアレントモード）

- 4 のインターフェイスをもつブリッジ グループを 250 まで作成できます。
- 直接接続された各ネットワークは同一のサブネット上にある必要があります。
- ASA では、セカンダリ ネットワーク上のトラフィックはサポートされていません。BVI IP アドレスと同じネットワーク上のトラフィックだけがサポートされています。
- IPv4 の場合は、管理トラフィックと、ASA を通過するトラフィックの両方の各ブリッジ グループに対し、BVI の IP アドレスが必要です。IPv6 アドレスは BVI でサポートされますが必須ではありません。
- IPv6 アドレスは手動でのみ設定できます。
- BVI IP アドレスは、接続されたネットワークと同じサブネット内にある必要があります。サブネットにホスト サブネット（255.255.255.255）を設定することはできません。
- 管理インターフェイスはブリッジ グループのメンバーとしてサポートされません。
- トランスペアレント モードでは、少なくとも 1 つのブリッジ グループを使用し、データ インターフェイスがブリッジ グループに属している必要があります。
- トランスペアレント モードでは、接続されたデバイス用のデフォルト ゲートウェイとして BVI IP アドレスを指定しないでください。デバイスは ASA の他方側のルータをデフォルト ゲートウェイとして指定する必要があります。
- トランスペアレント モードでは、管理トラフィックの戻りパスを指定するために必要な *default* ルートは、1 つのブリッジ グループ ネットワークからの管理トラフィックにだけ適

用されます。これは、デフォルトルートはブリッジグループのインターフェイスとブリッジ グループ ネットワークのルータ IP アドレスを指定しますが、ユーザは 1 つのデフォルト ルートしか定義できないためです。複数のブリッジ グループ ネットワークからの管理トラフィックが存在する場合は、管理トラフィックの発信元ネットワークを識別する標準のスタティック ルートを指定する必要があります。

- トランスペアレント モードでは、PPPoE は 管理 インターフェイスでサポートされません。
- Bidirectional Forwarding Detection（BFD）エコー パケットは、ブリッジ グループ メンバを使用するときに、ASA を介して許可されません。BFD を実行している ASA の両側に 2 つのネイバーがある場合、ASA は BFD エコー パケットをドロップします。両方が同じ送信元および宛先 IP アドレスを持ち、LAND 攻撃の一部であるように見えるからです。

その他のガイドラインと制限事項

- ファイアウォールモードを変更すると、多くのコマンドが両方のモードでサポートされていないため、ASA は実行コンフィギュレーションをクリアします。スタートアップ コンフィギュレーションは変更されません。保存しないでリロードすると、スタートアップ コンフィギュレーションがロードされて、モードは元の設定に戻ります。 コンフィギュレーション ファイルのバックアップについては、ファイアウォール モードの設定 （184 ページ）を参照してください。
- **firewall transparent** コマンドでモードを使用して変更するテキスト コンフィギュレーションを ASA にダウンロードする場合、コマンドをコンフィギュレーションの先頭に配置してください。このコマンドが読み込まれるとすぐに ASA がモードを変更し、その後ダウンロードされたコンフィギュレーションを引き続き読み込みます。コマンドがコンフィギュレーションの後ろの方にあると、ASA はそのコマンドよりも前の位置に記述されているすべての行をクリアします。テキスト ファイルのダウンロードの詳細については、ASA イメージ、ASDM、およびスタートアップ コンフィギュレーションの設定（1020 ページ）を参照してください。

ファイアウォール モードの設定

この項では、ファイアウォール モードを変更する方法を説明します。

（注） ファイアウォールモードを変更すると実行コンフィギュレーションがクリアされるので、他のコンフィギュレーションを行う前にファイアウォールモードを設定することをお勧めします。

始める前に

モードを変更すると、ASA は実行コンフィギュレーションをクリアします（詳細については、ファイアウォール モードのガイドライン （183 ページ）を参照してください）。

- 設定済みのコンフィギュレーションがある場合は、モードを変更する前にコンフィギュレーションをバックアップしてください。新しいコンフィギュレーション作成時の参照としてこのバックアップを使用できます。コンフィギュレーションまたはその他のファイルのバックアップおよび復元 （1023 ページ）を参照してください。
- モードを変更するには、コンソール ポートで CLI を使用します。ASDM コマンドラインインターフェイス ツールや SSH などの他のタイプのセッションを使用する場合、コンフィギュレーションがクリアされるときにそれが切断されるので、いずれの場合もコンソールポートを使用して ASA に再接続する必要があります。
- コンテキスト内でモードを設定します。

（注） 設定が削除された後にファイアウォール モードをトランスペアレントに設定し、ASDM への管理アクセスを設定するには、ASDM アクセスの設定 （32 ページ）を参照してください。

手順

ファイアウォール モードをトランスペアレントに設定します。

firewall transparent

例：

```
ciscoasa(config)# firewall transparent
```

モードをルーテッドに変更するには、**no firewall transparent** コマンドを入力します。

（注） ファイアウォール モードの変更では確認は求められず、ただちに変更が行われます。

ファイアウォール モードの例

このセクションには、ルーテッド ファイアウォール モードとトランスペアレント ファイアウォール モードで、ASA を介してどのようにトラフィックが転送されるかを説明する例が含まれます。

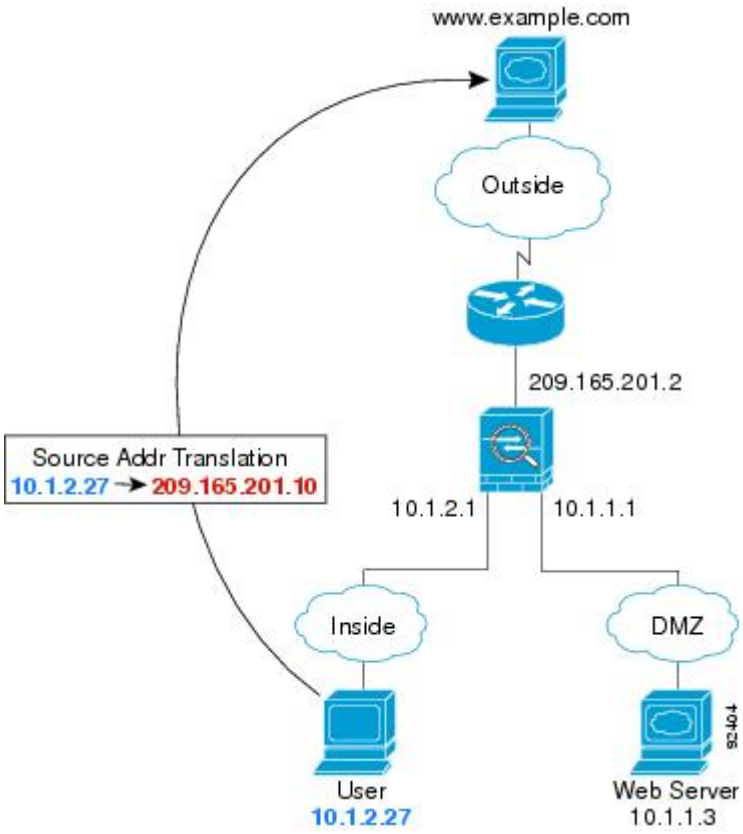
ルーテッド ファイアウォール モードで ASA を通過するデータ

次のセクションでは、複数のシナリオのルーテッド ファイアウォール モードで、データが ASA をどのように通過するかを示します。

内部ユーザが Web サーバにアクセスする

次の図は、内部ユーザが外部 Web サーバにアクセスしていることを示しています。

図 *16 :* 内部から外部へ



次の手順では、データが ASA をどのように通過するかを示します。

1. 内部ネットワークのユーザは、www.example.com から Web ページを要求します。
2. ASA はパケットを受信します。これは新しいセッションであるため、ASA はセキュリティ ポリシーの条件に従って、パケットが許可されているか確認します。

   マルチ コンテキスト モードの場合、ASA はパケットをまずコンテキストに分類します。
3. ASA は、実アドレス（10.1.2.27）をマップ アドレス 209.165.201.10 に変換します。このマップ アドレスは外部インターフェイスのサブネット上にあります。

   マップ アドレスは任意のサブネット上に設定できますが、外部インターフェイスのサブネット上に設定すると、ルーティングが簡素化されます。
4. 次に、ASAはセッションが確立されたことを記録し、外部インターフェイスからパケットを転送します。
5. www.example.com が要求に応答すると、パケットはASAを通過します。これはすでに確立されているセッションであるため、パケットは、新しい接続に関連する多くのルックアッ

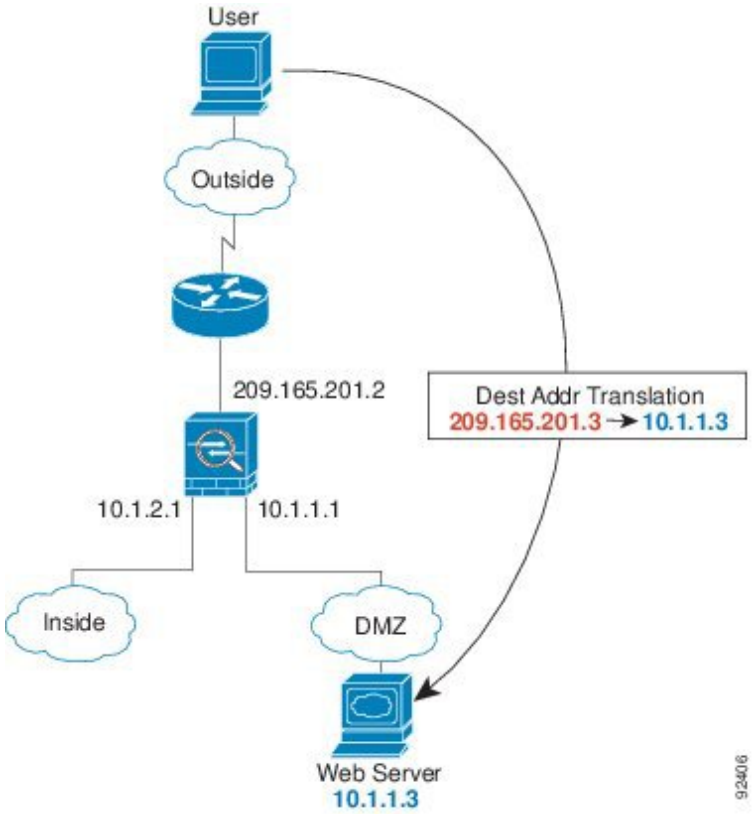
プをバイパスします。ASA は、グローバル宛先アドレスをローカルユーザアドレス 10.1.2.27 に変換せずに、NAT を実行します。

6. ASAは、パケットを内部ユーザに転送します。

外部ユーザが DMZ 上の Web サーバにアクセスする

次の図は、外部ユーザが DMZ の Web サーバにアクセスしていることを示しています。

図 *17*：外部から *DMZ* へ



次の手順では、データが ASA をどのように通過するかを示します。

1. 外部ネットワーク上のユーザがマップ アドレス 209.165.201.3 を使用して、DMZ 上の Web サーバに Web ページを要求します。これは、外部インターフェイスのサブネット上のアドレスです。
2. ASA はパケットを受信し、マッピング アドレスは実アドレス 10.1.1.3 に変換しません。
3. ASA は新しいセッションであるため、セキュリティ ポリシーの条件に従って、パケットが許可されていることを確認します。

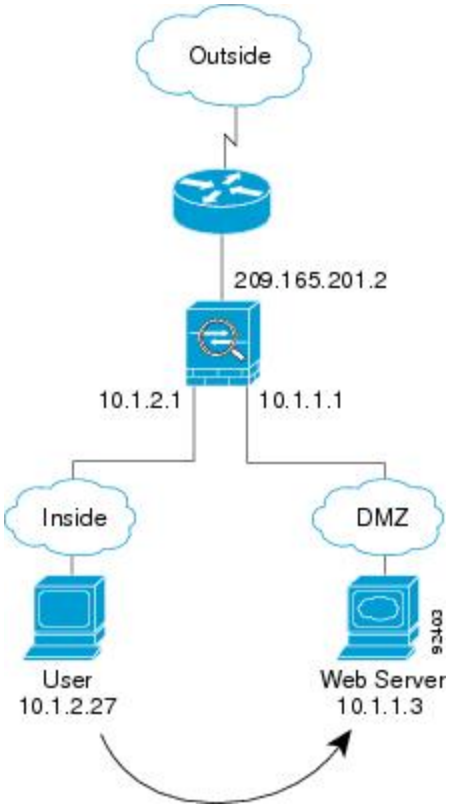
   マルチ コンテキスト モードの場合、ASA はパケットをまずコンテキストに分類します。
4. 次に、ASAはセッションエントリを高速パスに追加し、DMZインターフェイスからパケットを転送します。

5. DMZ Web サーバが要求に応答すると、パケットはASAを通過します。また、セッションがすでに確立されているため、パケットは、新しい接続に関連する多くのルックアップをバイパスします。ASA は、実アドレスを 209.165.201.3 に変換することで NAT を実行します。
6. ASAは、パケットを外部ユーザに転送します。

内部ユーザが DMZ 上の Web サーバにアクセスする

次の図は、内部ユーザが DMZ の Web サーバにアクセスしていることを示しています。

図 *18 :* 内部から *DMZ* へ



次の手順では、データが ASA をどのように通過するかを示します。

1. 内部ネットワーク上のユーザは、宛先アドレス 10.1.1.3 を使用して DMZ Web サーバから Web ページを要求します。
2. ASAはパケットを受信します。これは新しいセッションであるため、ASAはセキュリティポリシーの条件に従ってパケットが許可されているか確認します。

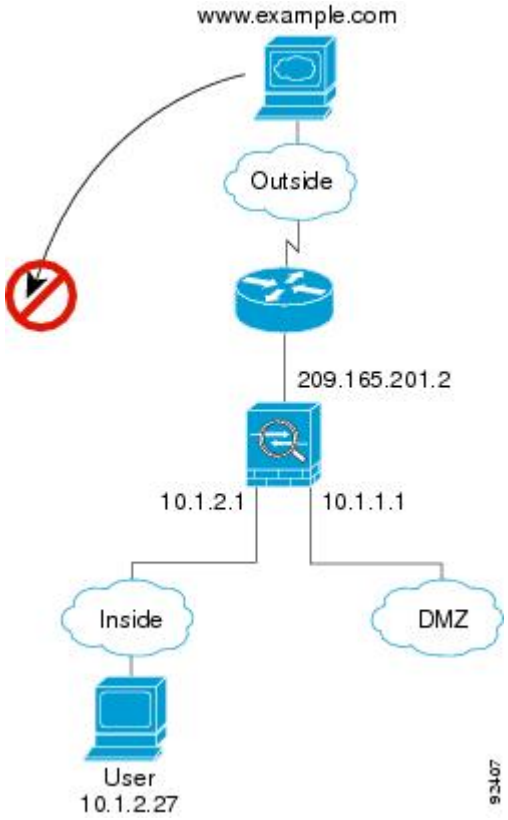
   マルチ コンテキスト モードの場合、ASA はパケットをまずコンテキストに分類します。
3. 次に、ASAはセッションが確立されたことを記録し、DMZ インターフェイスからパケットを転送します。

4. DMZ Web サーバが要求に応答すると、パケットは高速パスを通過します。これのため、パケットは、新しい接続に関連する多くのルックアップをバイパスします。
5. ASAは、パケットを内部ユーザに転送します。

外部ユーザが内部ホストにアクセスしようとする

次の図は、外部ユーザが内部ネットワークにアクセスしようとしていることを示しています。

図 *19 :* 外部から内部へ



次の手順では、データが ASA をどのように通過するかを示します。

1. 外部ネットワーク上のユーザが、内部ホストに到達しようとします（ホストにルーティング可能な IP アドレスがあると想定します）。

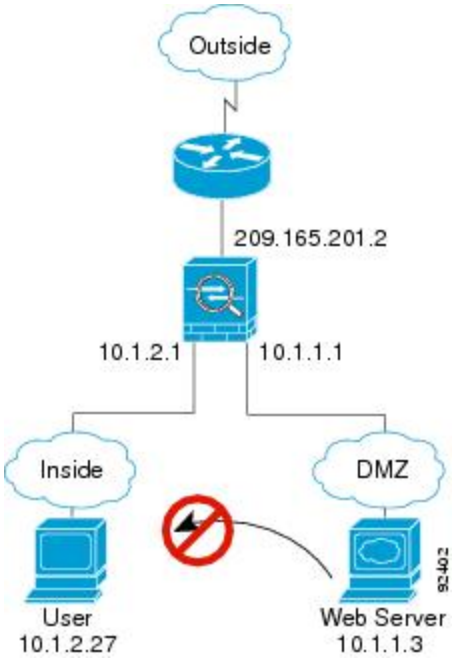
   内部ネットワークがプライベート アドレスを使用している場合、外部ユーザが NAT なしで内部ネットワークに到達することはできません。外部ユーザは既存の NAT セッションを使用して内部ユーザに到達しようとすることが考えられます。
2. ASA はパケットを受信します。これは新しいセッションであるため、ASA はセキュリティ ポリシーに従って、パケットが許可されているか確認します。
3. パケットが拒否され、ASAはパケットをドロップし、接続試行をログに記録します。

外部ユーザが内部ネットワークを攻撃しようとした場合、ASAは多数のテクノロジーを使用して、すでに確立されたセッションに対してパケットが有効かどうかを判別します。

DMZ ユーザによる内部ホストへのアクセスの試み

次の図は、DMZ 内のユーザが内部ネットワークにアクセスしようとしていることを示しています。

図 *20 : DMZ* から内部へ



次の手順では、データが ASA をどのように通過するかを示します。

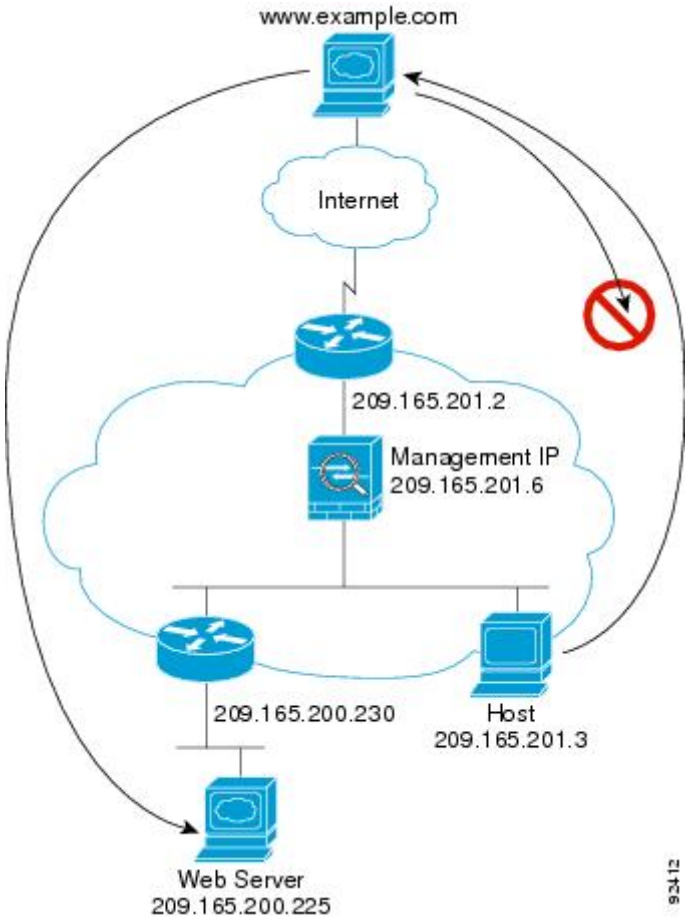
1. DMZネットワーク上のユーザが、内部ホストに到達しようとします。DMZはインターネット上のトラフィックをルーティングする必要がないので、プライベートアドレッシング方式はルーティングを回避しません。
2. ASAはパケットを受信します。これは新しいセッションであるため、ASAはセキュリティポリシーに従って、パケットが許可されているか確認します。

   パケットが拒否され、ASAはパケットをドロップし、接続試行をログに記録します。

トランスペアレント ファイアウォールを通過するデータの動き

次の図に、パブリック Web サーバを含む内部ネットワークを持つ一般的なトランスペアレント ファイアウォールの実装を示します。内部ユーザがインターネット リソースにアクセスできるよう、ASA にはアクセス ルールがあります。別のアクセス ルールによって、外部ユーザは内部ネットワーク上の Web サーバだけにアクセスできます。

図 *21* : 一般的なトランスペアレント ファイアウォールのデータ パス

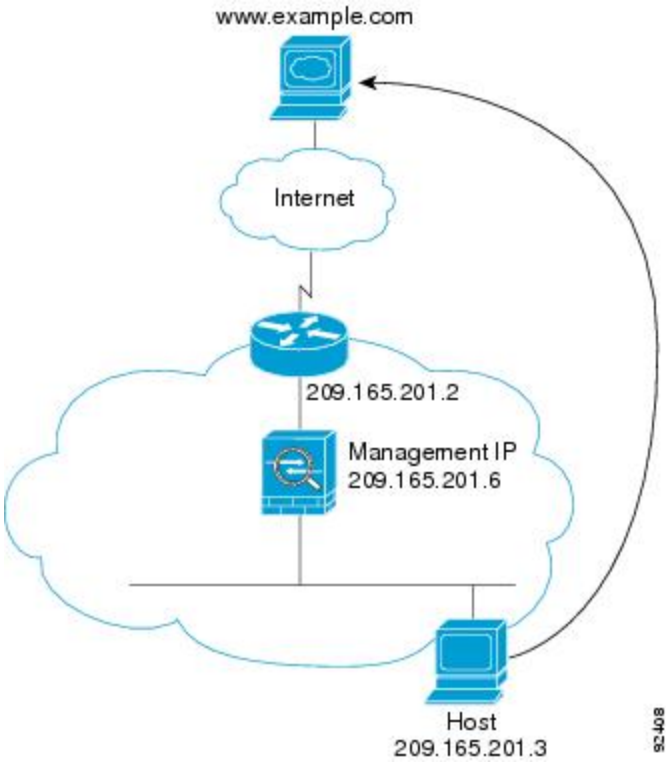


次のセクションでは、データが ASA をどのように通過するかを示します。

内部ユーザが Web サーバにアクセスする

次の図は、内部ユーザが外部 Web サーバにアクセスしていることを示しています。

図 *22 :* 内部から外部へ



次の手順では、データが ASA をどのように通過するかを示します。

1. 内部ネットワークのユーザは、www.example.com から Web ページを要求します。
2. ASAはパケットを受信し、必要な場合、送信元 MAC アドレスを MAC アドレス テーブルに追加します。これは新しいセッションであるため、セキュリティ ポリシーの条件に従って、パケットが許可されていることを確認します。

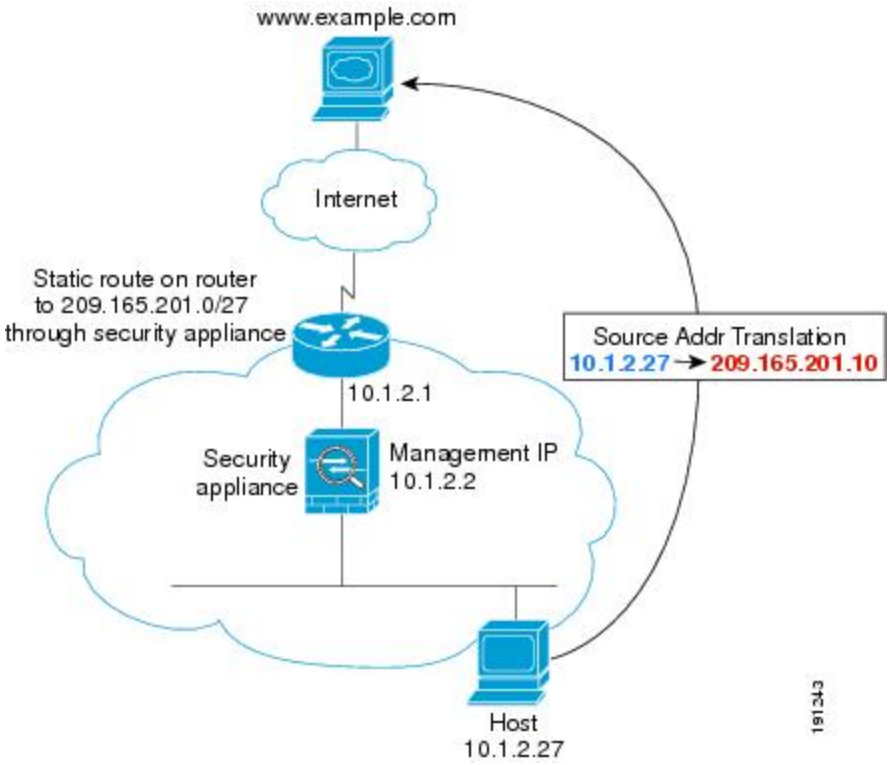
   マルチ コンテキスト モードの場合、ASA はパケットをまずコンテキストに分類します。
3. ASAは、セッションが確立されたことを記録します。
4. 宛先 MAC アドレスがテーブル内にある場合、ASAは外部インターフェイスからパケットを転送します。宛先 MAC アドレスは、アップストリーム ルータのアドレス 209.165.201.2 です。

   宛先 MAC アドレスが ASA のテーブルにない場合、ASA は MAC アドレスを検出するために ARP 要求または ping を送信します。最初のパケットはドロップされます。
5. Web サーバが要求に応答します。セッションがすでに確立されているため、パケットは、新しい接続に関連する多くのルックアップをバイパスします。
6. ASAは、パケットを内部ユーザに転送します。

NAT を使用して内部ユーザが Web サーバにアクセスする

次の図は、内部ユーザが外部 Web サーバにアクセスしていることを示しています。

図 *23 : NAT* を使用して内部から外部へ



次の手順では、データが ASA をどのように通過するかを示します。

1. 内部ネットワークのユーザは、www.example.com から Web ページを要求します。
2. ASAはパケットを受信し、必要な場合、送信元 MAC アドレスを MAC アドレス テーブルに追加します。これは新しいセッションであるため、セキュリティ ポリシーの条件に従って、パケットが許可されていることを確認します。

   マルチ コンテキスト モードの場合、ASAは、固有なインターフェイスに従ってパケットを分類します。
3. ASAは実際のアドレス（10.1.2.27）をマッピング アドレス 209.165.201.10 に変換します。

   マッピングアドレスは外部インターフェイスと同じネットワーク上にないため、アップストリーム ルータにASAをポイントするマッピング ネットワークへのスタティック ルートがあることを確認します。
4. 次に、ASAはセッションが確立されたことを記録し、外部インターフェイスからパケットを転送します。
5. 宛先 MAC アドレスがテーブル内にある場合、ASAは外部インターフェイスからパケットを転送します。宛先MACアドレスは、アップストリーム ルータのアドレス 10.1.2.1 です。

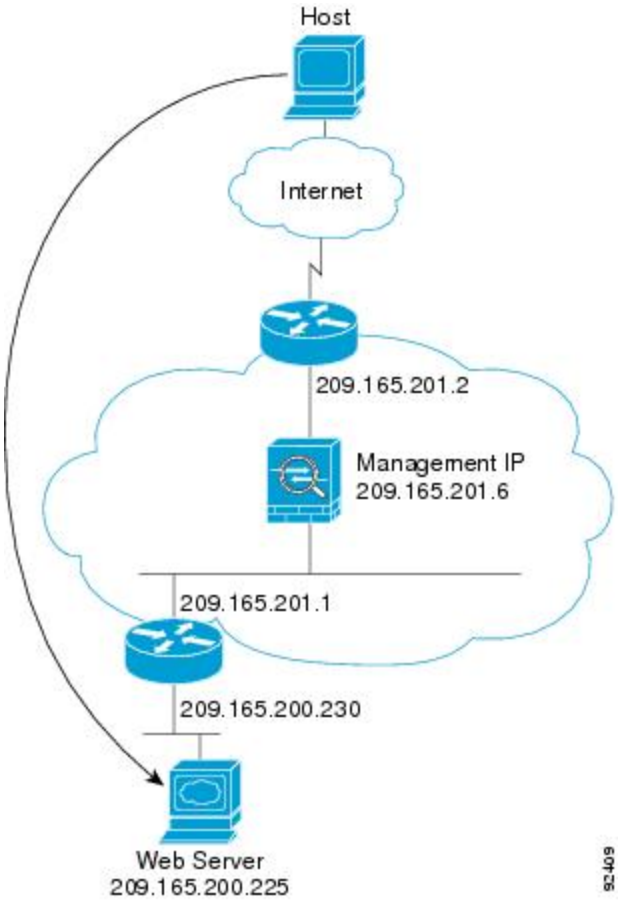
宛先 MAC アドレスが ASA のテーブルにない場合、ASA は MAC アドレスを検出するために ARP 要求と ping を送信します。最初のパケットはドロップされます。

6. Web サーバが要求に応答します。セッションがすでに確立されているため、パケットは、新しい接続に関連する多くのルックアップをバイパスします。
7. ASA は、マッピング アドレスを実際のアドレス 10.1.2.27 にせずに、NAT を実行します。

外部ユーザが内部ネットワーク上の Web サーバにアクセスする

次の図は、外部ユーザが内部の Web サーバにアクセスしていることを示しています。

図 *24* : 外部から内部へ



次の手順では、データが ASA をどのように通過するかを示します。

1. 外部ネットワーク上のユーザは、内部 Web サーバから Web ページを要求します。
2. ASAはパケットを受信し、必要な場合、送信元 MAC アドレスを MAC アドレス テーブルに追加します。これは新しいセッションであるため、セキュリティ ポリシーの条件に従って、パケットが許可されていることを確認します。

   マルチ コンテキスト モードの場合、ASA はパケットをまずコンテキストに分類します。

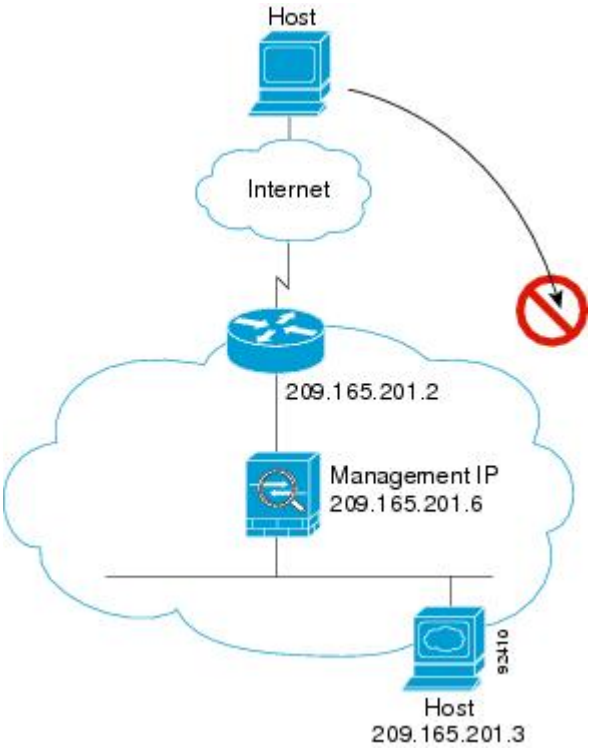
3. ASAは、セッションが確立されたことを記録します。
4. 宛先 MAC アドレスがテーブル内にある場合、ASAは内部インターフェイスからパケットを転送します。宛先 MAC アドレスは、ダウンストリーム ルータ 209.165.201.1 のアドレスです。

   宛先 MAC アドレスが ASA のテーブルにない場合、ASA は MAC アドレスを検出するために ARP 要求と ping を送信します。最初のパケットはドロップされます。
5. Web サーバが要求に応答します。セッションがすでに確立されているため、パケットは、新しい接続に関連する多くのルックアップをバイパスします。
6. ASAは、パケットを外部ユーザに転送します。

外部ユーザが内部ホストにアクセスしようとする

次の図は、外部ユーザが内部ネットワーク上のホストにアクセスしようとしていることを示しています。

図 *25 :* 外部から内部へ



次の手順では、データが ASA をどのように通過するかを示します。

1. 外部ネットワーク上のユーザが、内部ホストに到達しようとします。
2. ASAはパケットを受信し、必要な場合、送信元 MAC アドレスを MAC アドレス テーブルに追加します。これは新しいセッションであるため、セキュリティ ポリシーの条件に従って、パケットが許可されているか確認します。

マルチ コンテキスト モードの場合、ASA はパケットをまずコンテキストに分類します。

3. 外部ホストを許可するアクセス ルールは存在しないため、パケットは拒否され、ASA によってドロップされます。
4. 外部ユーザが内部ネットワークを攻撃しようとした場合、ASAは多数のテクノロジーを使用して、すでに確立されたセッションに対してパケットが有効かどうかを判別します。

ファイアウォール モードの履歴

表 *4:* ファイアウォール モードの各機能履歴

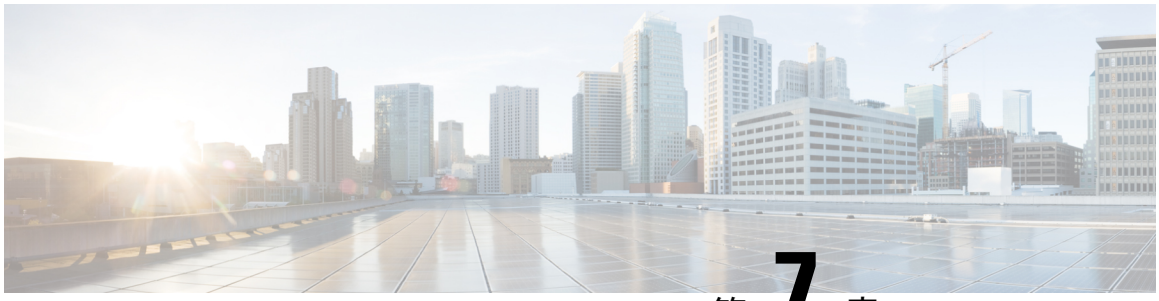
機能名	プラットフォーム リリース	機能情報
トランスペアレント ファイアウォール モード	7.0(1)	トランスペアレント ファイアウォールは、「Bump In The Wire」または「ステルス ファイアウォール」のように動作するレイヤ 2 ファイアウォールであり、接続されたデバイスへのルータ ホップとしては認識されません。 **firewall transparent**、および **show firewall** コマンドが導入されました。

機能名	プラットフォーム リリース	機能情報
トランスペアレント ファイアウォール ブリッジ グループ	8.4(1)	セキュリティ コンテキストのオーバーヘッドを避けたい場合、またはセキュリティ コンテキストを最大限に使用したい場合、インターフェイスをブリッジ グループにグループ化し、各ネットワークに 1 つずつ複数のブリッジ グループを設定できます。ブリッジ グループのトラフィックは他のブリッジ グループから隔離されます。シングル モードでは最大 8 個、マルチ モードではコンテキストあたり最大 8 個のブリッジ グループを設定でき、各ブリッジ グループには最大 4 個のインターフェイスを追加できます。 （注） ASA 5505 に複数のブリッジ グループを設定できますが、ASA 5505 のトランスペアレント モードのデータ インターフェイスは 2 つという制限は、実質的にブリッジ グループを 1 つだけ使用できることを意味します。 **interface bvi**、**bridge-group**、**show bridge-group** の各コマンドが導入されました。
マルチ コンテキスト モードのファイアウォール モードの混合がサポートされます。	8.5(1)/9.0(1)	セキュリティ コンテキスごとに個別のファイアウォール モードを設定できます。したがってその一部をトランスペアレント モードで実行し、その他をルーテッド モードで実行することができます。 **firewall transparent** コマンドが変更されました。

機能名	プラットフォーム リリース	機能情報
トランスペアレントモードのブリッジグループの最大数が 250 に増加	9.3(1)	ブリッジグループの最大数が 8 個から 250 個に増えました。シングル モードでは最大 250 個、マルチ モードではコンテキストあたり最大 8 個のブリッジグループを設定でき、各ブリッジ グループには最大 4 個のインターフェイスを追加できます。 **interface bvi** コマンド、**bridge-group** コマンドが変更されました。

第 II 部

ハイ アベイラビリティとスケーラビリティ



第 7 章

マルチ コンテキスト モード

この章では、Cisco ASA でマルチセキュリティ コンテキストの設定方法について説明します。

セキュリティ コンテキストについて

単一の ASA は、セキュリティ コンテキストと呼ばれる複数の仮想デバイスにパーティション化できます。各コンテキストは、独自のセキュリティ ポリシー、インターフェイス、および管理者を持つ独立したデバイスとして機能します。マルチ コンテキストは、複数のスタンドアロン デバイスを使用することに似ています。マルチ コンテキスト モードでサポートされない機能については、マルチ コンテキスト モードのガイドライン （214 ページ）を参照してください。

この項では、セキュリティ コンテキストの概要について説明します。

セキュリティ コンテキストの一般的な使用方法

マルチセキュリティ コンテキストを使用する状況には次のようなものがあります。

- サービス プロバイダーとして、多数のカスタマーにセキュリティ サービスを販売する。ASA 上でマルチ セキュリティ コンテキストを有効にすることによって、費用対効果の高

い、省スペース ソリューションを実装できます。このソリューションでは、カスタマーのトラフィックすべての分離とセキュリティが確保され、設定も容易です。

- 大企業または広大な大学の構内で、各部門の完全な独立を維持する必要がある。
- 企業で、部門ごとに個別のセキュリティ ポリシーの提供が求められている。
- 複数の ASA が必要なネットワークを使用する場合。

コンテキスト コンフィギュレーション ファイル

この項では、ASA がマルチ コンテキスト モードのコンフィギュレーションを実装する方法について説明します。

コンテキスト コンフィギュレーション

コンテキストごとに、ASA の中に 1 つのコンフィギュレーションがあり、この中ではセキュリティ ポリシーやインターフェイスに加えて、スタンドアロン デバイスで設定できるすべてのオプションが指定されています。コンテキスト コンフィギュレーションはフラッシュ メモリ内に保存することも、TFTP、FTP、または HTTP（S）サーバからダウンロードすることもできます。

システム設定

システム管理者は、各コンテキスト コンフィギュレーションの場所、割り当てられたインターフェイス、およびその他のコンテキスト操作パラメータをシステム コンフィギュレーションに設定することで、コンテキストを追加および管理します。このコンフィギュレーションは、シングル モードのコンフィギュレーション同様、スタートアップ コンフィギュレーションです。システム コンフィギュレーションは、ASA の基本設定を識別します。システム コンフィギュレーションには、ネットワーク インターフェイスやネットワーク設定は含まれません。その代わりに、ネットワーク リソースにアクセスする必要が生じたときに（サーバからコンテキストをダウンロードするなど）、システムは管理コンテキストとして指定されているコンテキストのいずれかを使用します。システム コンフィギュレーションに含まれているものに、フェールオーバー トラフィック専用の特殊なフェールオーバー インターフェイスがあります。

管理コンテキストの設定

管理コンテキストは、他のコンテキストとまったく同じです。ただ、ユーザが管理コンテキストにログインすると、システム管理者権限を持つので、システム コンテキストおよび他のすべてのコンテキストにアクセス可能になる点が異なります。管理コンテキストは制限されていないため、通常のコンテキストとして使用できます。ただし、管理コンテキストにログインすると、すべてのコンテキストへの管理者特権が付与されるため、場合によっては、管理コンテキストへのアクセスを適切なユーザに制限する必要があります。管理コンテキストは、リモートではなくフラッシュ メモリに置く必要があります。

システムがすでにマルチ コンテキスト モードになっている場合、またはシングル モードから変換された場合、管理コンテキストが admin.cfg と呼ばれるファイルとして内部フラッシュ メ

モリに自動的に作成されます。このコンテキストの名前は "admin" です。admin.cfg を管理コンテキストとして使用しない場合は、管理コンテキストを変更できます。

ASA がパケットを分類する方法

ASA に入ってくるパケットはいずれも分類する必要があります。その結果、ASA は、どのコンテキストにパケットを送信するかを決定できます。

（注） 宛先 MAC アドレスがマルチキャストまたはブロードキャスト MAC アドレスの場合、パケットが複製され、各コンテキストに送信されます。

有効な分類子基準

この項では、分類子で使用される基準について説明します。

（注） インターフェイス宛の管理トラフィックでは、インターフェイス IP アドレスが分類に使用されます。

ルーティング テーブルはパケット分類には使用されません。

固有のインターフェイス

入力インターフェイスに関連付けられているコンテキストが 1 つだけの場合、ASA はパケットをそのコンテキストに分類します。トランスペアレント ファイアウォール モードでは、各コンテキストに固有のインターフェイスが必要なため、この方法は、常にパケット分類の目的で使用されます。

固有の MAC アドレス

複数のコンテキストが同じインターフェイスを共有している場合は、各コンテキストでそのインターフェイスに割り当てられた一意の MAC アドレスが分類子で使用されます。固有の MAC アドレスがないと、アップストリーム ルータはコンテキストに直接ルーティングできません。MAC アドレスの自動生成を有効にできます。各インターフェイスを設定するときに、手動で MAC アドレスを設定することもできます。

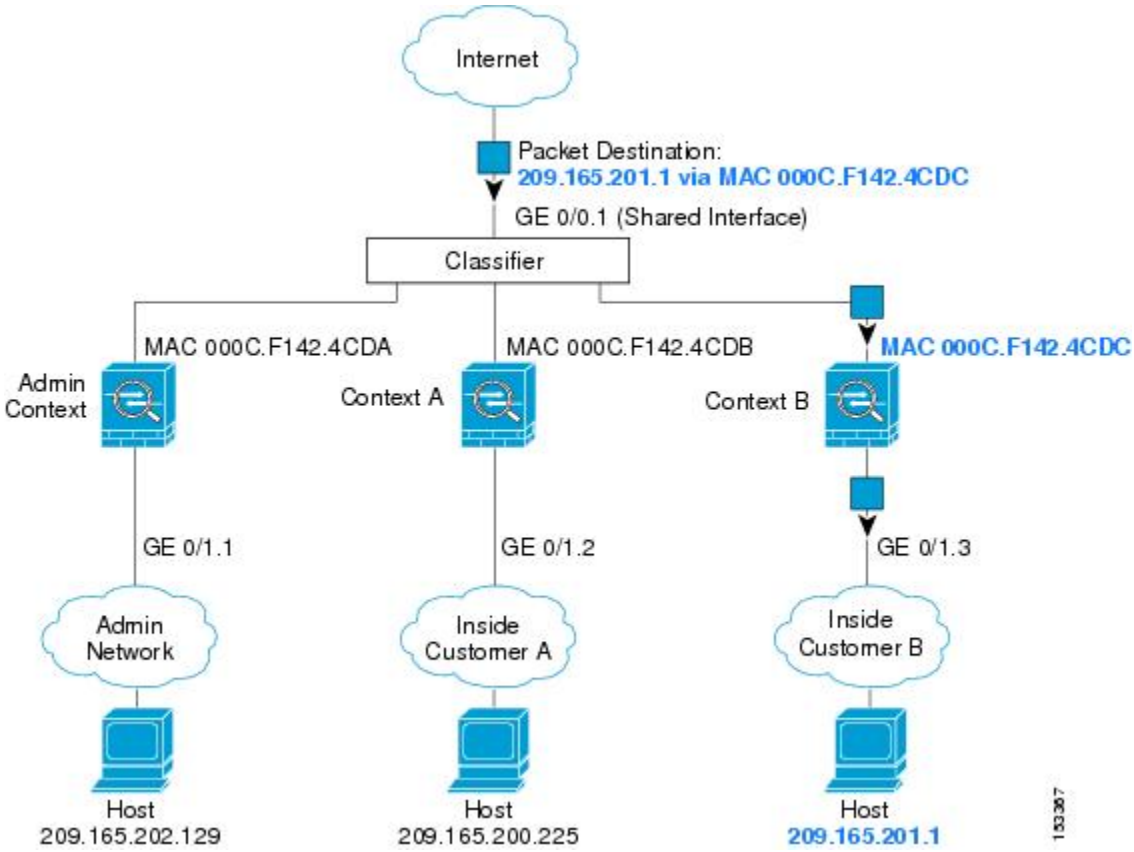
NAT の設定

固有の MAC アドレスの使用を有効にしなければ、ASA は、NAT コンフィギュレーション内のマッピングされたアドレスを使用してパケットを分類します。NAT コンフィギュレーションの完全性に関係なくトラフィック分類を行うことができるように、NAT ではなく MAC アドレスを使用することをお勧めします。

分類例

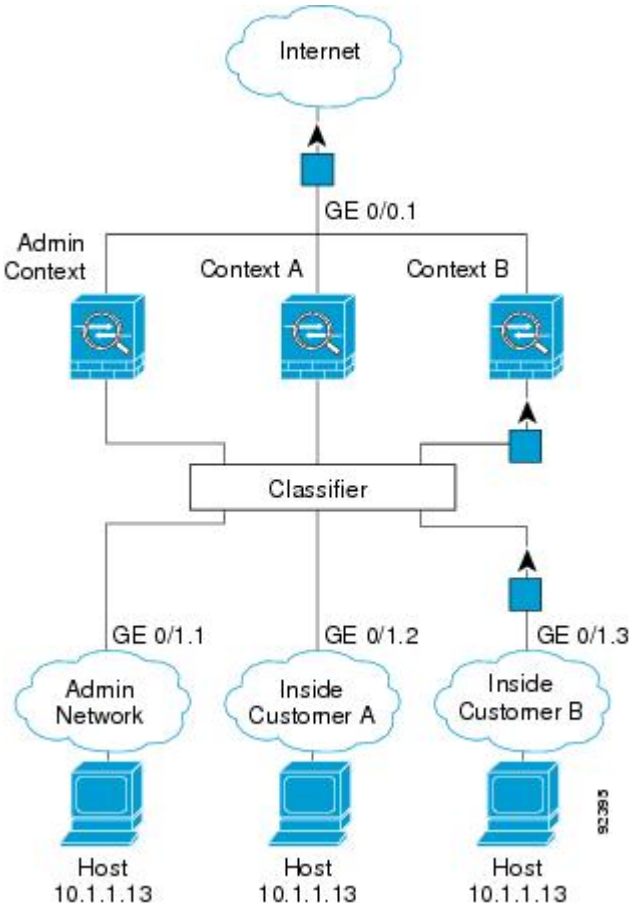
次の図に、外部インターフェイスを共有するマルチ コンテキストを示します。コンテキスト B にはルータがパケットを送信する MAC アドレスが含まれているため、分類子はパケットをコンテキスト B に割り当てます。

図 *26 : MAC* アドレスを使用した共有インターフェイスのパケット分類



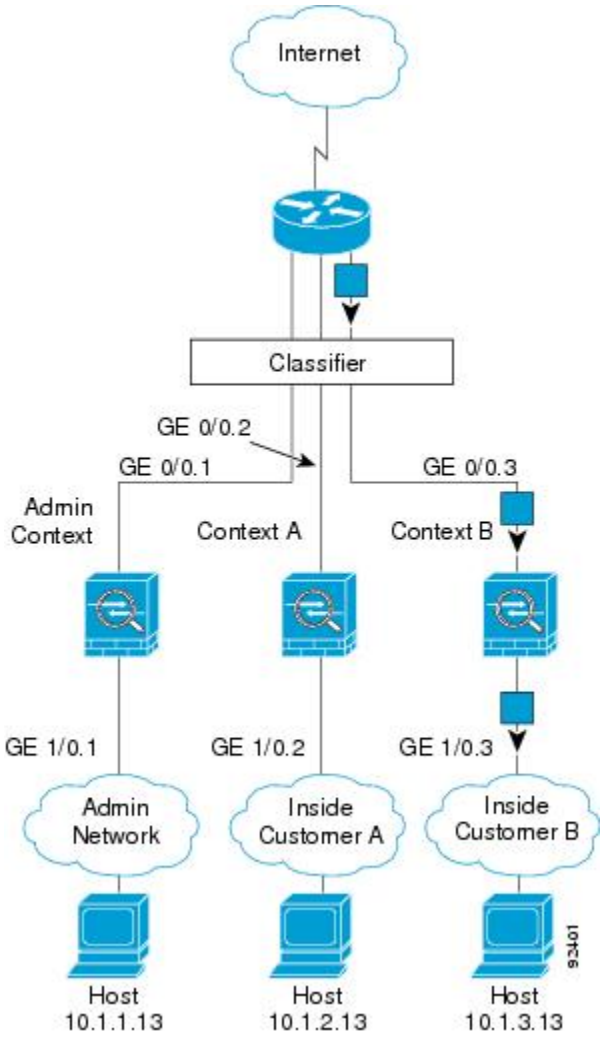
内部ネットワークからのものを含め、新たに着信するトラフィックすべてが分類される点に注意してください。次の図に、インターネットにアクセスするネットワーク内のコンテキストBのホストを示します。分類子は、パケットをコンテキストBに割り当てます。これは、入力インターフェイスがギガビット イーサネット 0/1.3 で、このイーサネットがコンテキスト B に割り当てられているためです。

図 *27:* 内部ネットワークからの着信トラフィック



トランスペアレントファイアウォールでは、固有のインターフェイスを使用する必要があります。次の図に、ネットワーク内のコンテキストBのホストに向けられたインターネットからのパケットを示します。分類子は、パケットをコンテキストBに割り当てます。これは、入力インターフェイスがギガビット イーサネット 1/0.3 で、このイーサネットがコンテキスト B に割り当てられているためです。

図 *28 :* トランスペアレント ファイアウォール コンテキスト



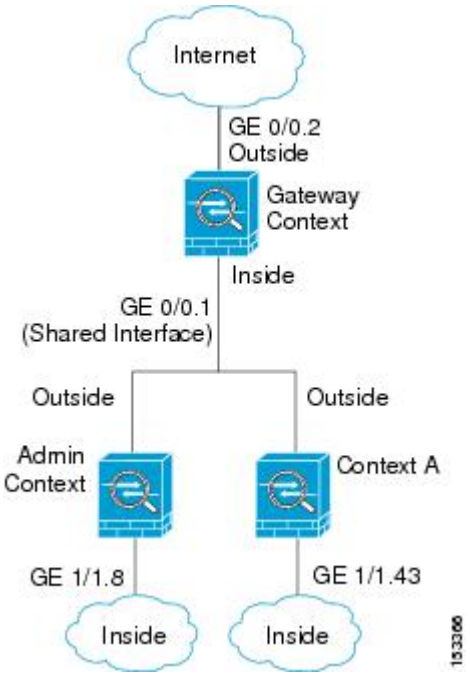
セキュリティ コンテキストのカスケード接続

コンテキストを別のコンテキストのすぐ前に置くことを、コンテキストをカスケード接続するといいます。一方のコンテキストの外部インターフェイスは、他方のコンテキストの内部インターフェイスと同じインターフェイスです。いくつかのコンテキストのコンフィギュレーションを単純化する場合、最上位のコンテキストの共有パラメータを設定することで、コンテキストをカスケード接続できます。

（注） コンテキストをカスケード接続するには、各コンテキスト インターフェイスに固有の MAC アドレスが必要です。MAC アドレスのない共有インターフェイスのパケットを分類するには限界があるため、固有の MAC アドレスを設定しないでコンテキストのカスケード接続を使用することはお勧めしません。

次の図に、ゲートウェイの背後に2つのコンテキストがあるゲートウェイ コンテキストを示します。

図 *29 :* コンテキストのカスケード接続



セキュリティ コンテキストへの管理アクセス

ASA では、マルチ コンテキスト モードでのシステム管理アクセスと、各コンテキスト管理者のアクセスを提供します。次の各項では、システム管理者またはコンテキスト管理者としてのログインについて説明します。

システム管理者のアクセス

2 つの方法で、システム管理者として ASA をアクセスできます。

- ASA コンソールにアクセスする。

  コンソールからシステム実行スペースにアクセスします。この場合、入力したコマンドは、システム コンフィギュレーションまたはシステムの実行（run-time コマンド）だけに影響します。

- Telnet、SSH、または ASDM を使用して管理コンテキストにアクセスする

システム管理者として、すべてのコンテキストにアクセスできます。

システム実行スペースでは AAA コマンドはサポートされていませんが、個別のログインのために、固有のイネーブル パスワードおよびユーザ名をローカル データベースに設定することができます。

コンテキスト管理者のアクセス

Telnet、SSH、または ASDM を使用して、コンテキストにアクセスできます。管理外コンテキストにログインすると、アクセスできるのはそのコンテキストのコンフィギュレーションだけになります。そのコンテキストに個別のログインを付与できます。

リソース管理の概要

デフォルトでは、すべてのセキュリティ コンテキストは ASA のリソースに無制限でアクセスできますが、コンテキストあたりの上限が定められている場合を除きます。唯一の例外は、VPNのリソース（デフォルトでディセーブルになっています）です。特定のコンテキストが使用しているリソースが多すぎることが原因で、他のコンテキストが接続を拒否されるといった現象が発生した場合は、コンテキストあたりのリソースの使用量を制限するようにリソース管理を設定できます。VPN のリソースについては、VPN トンネルを許可するようにリソース管理を設定する必要があります。

リソース クラス

ASAは、リソースクラスにコンテキストを割り当てることによって、リソースを管理します。各コンテキストでは、クラスによって設定されたリソース制限が使用されます。クラスの設定を使用するには、コンテキストを定義するときに、そのコンテキストをクラスに割り当てます。すべてのコンテキストは、別のクラスに割り当てられていなければ、デフォルトクラスに属します。したがって、コンテキストをデフォルト クラスに割り当てる必要は特にありません。コンテキストは1つのリソース クラスにだけ割り当てることができます。このルールの例外は、メンバ クラスで未定義の制限はデフォルト クラスから継承されることです。そのため実際には、コンテキストがデフォルト クラスおよび別のクラスのメンバになります。

リソース制限値

個々のリソースの制限値は、パーセンテージ（ハードシステム制限がある場合）または絶対値として設定できます。

ほとんどのリソースについては、ASAはクラスに割り当てられたコンテキストごとにリソースの一部を確保することはしません。代わりに、ASAはコンテキストごとに上限を設定します。リソースをオーバーサブスクライブする場合、または一部のリソースを無制限にする場合は、少数のコンテキストがこれらのリソースを「使い果たし」、他のコンテキストへのサービスに影響する可能性があります。例外は、VPN リソース タイプです。このリソースはオーバーサブスクライブできないため、各コンテキストに割り当てられたリソースは保証されます割り当てられた量を超える、VPNセッションの一時的なバーストに対応できるように、ASAは「burst」という VPN リソース タイプをサポートしています。このリソースは、残りの未割り当て VPN セッションに等しくなります。バーストセッションはオーバーサブスクライブでき、コンテキストが先着順で使用できます。

デフォルト クラス

すべてのコンテキストは、別のクラスに割り当てられていない場合はデフォルトクラスに属します。コンテキストをデフォルト クラスに積極的に割り当てる必要はありません。

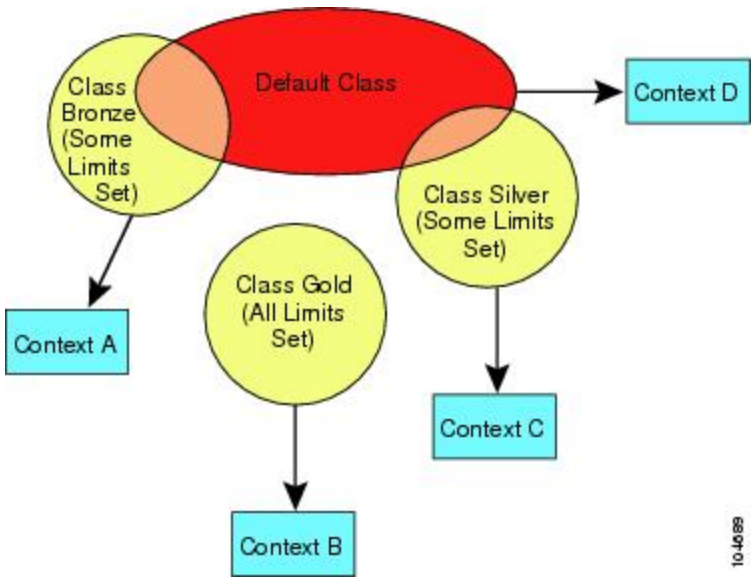
コンテキストがデフォルト クラス以外のクラスに属する場合、それらのクラス設定は常にデフォルト クラス設定を上書きします。ただし、他のクラスに定義されていない設定がある場合、メンバ コンテキストはそれらの制限にデフォルト クラスを使用します。たとえば、すべての同時接続に 2% の制限を設定したがその他の制限を設定せずにクラスを作成した場合、他のすべての制限はデフォルトクラスから継承されます。これとは逆に、すべてのリソースに対する制限値を設定してクラスを作成すると、そのクラスではデフォルトクラスの設定を何も使用しません。

ほとんどのリソースについては、デフォルトクラスではすべてのコンテキストがリソースに無制限でアクセスできます。ただし、次の制限を除きます。

- Telnet セッション：5 セッション。（コンテキストあたりの最大値）。
- SSH セッション：5 セッション。（コンテキストあたりの最大値）。
- IPsec セッション：5 セッション。（コンテキストあたりの最大値）。
- MAC アドレス：65,535 エントリ。（システムの最大値）。
- VPN サイトツーサイト トンネル：0 セッション（VPN セッションを許可するようにクラスを手動で設定する必要があります）。

次の図に、デフォルト クラスと他のクラスの関係を示します。コンテキスト A および C は、いくつかの制限が設定されたクラスに属しており、それ以外の制限はデフォルトクラスから継承します。コンテキスト B は、属している Gold クラスですべての制限が設定されているため、デフォルトクラスから制限値を継承しません。コンテキスト D はクラスに割り当てられなかったため、デフォルトでデフォルト クラスのメンバになります。

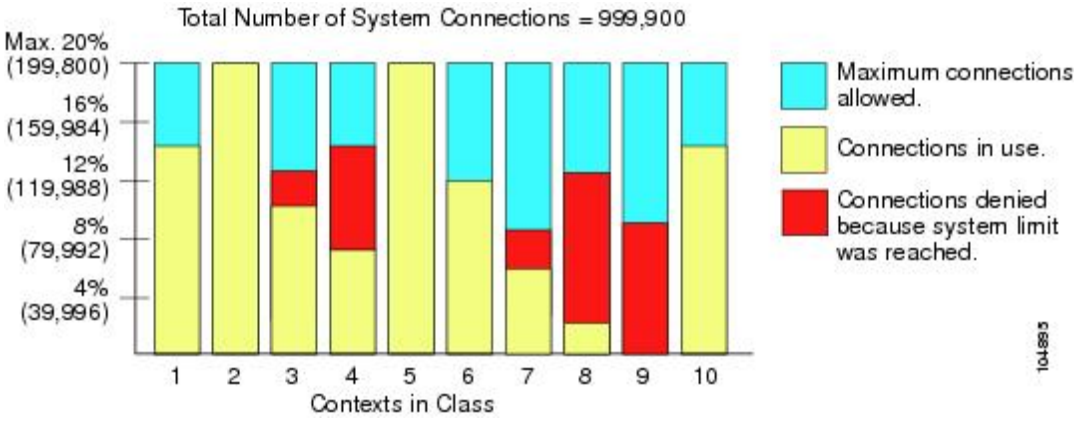
図 *30* : リソース クラス



オーバーサブスクライブ リソースの使用

ASA をオーバーサブスクライブするには、割り当て率の合計が 100% を超えるようにあるリソースをすべてのコンテキストに割り当てます（非バーストの VPN リソースを除く）。たとえば、接続がコンテキストあたり 20% までに制限されるように Bronze クラスを設定し、それから10個のコンテキストをそのクラスに割り当てれば、リソースの合計を200%にできます。コンテキストがシステム制限を超えて同時に使用する場合、各コンテキストは意図した 20% を下回ります。

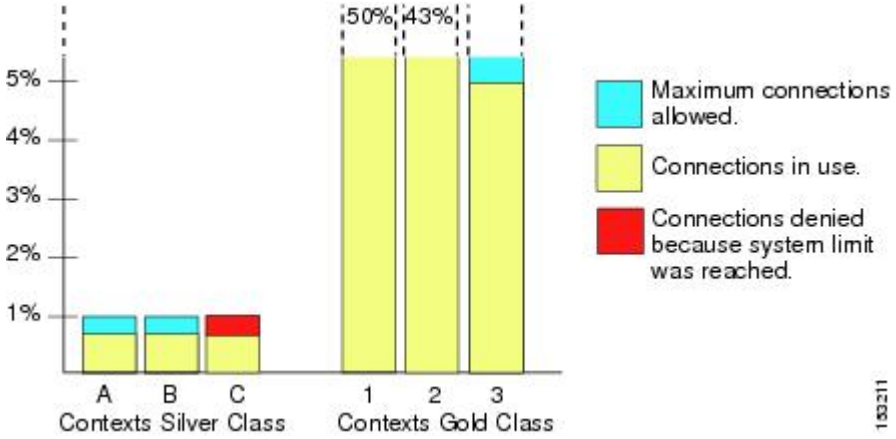
図 *31* : リソース オーバーサブスクリプション



無限リソースの使用

ASAは、パーセンテージや絶対値ではなく、クラス内の1つ以上のリソースに無制限アクセスを割り当てることができます。リソースが無制限の場合、コンテキストはシステムで使用可能な量までリソースを使用できます。たとえば、コンテキスト A、B、C が Silver クラスに属しており、クラスの各メンバの使用量が接続の 1% に制限されていて、合計 3% が割り当てられているが、3 つのコンテキストが現在使用しているのは合計 2% だけだとします。Gold クラスは、接続に無制限にアクセスできます。Gold クラスのコンテキストは、「未割り当て」接続のうち 97% を超える分も使用できます。つまり、現在コンテキスト A、B、C で使用されていない、接続の 1% も使用できます。その場合は、コンテキスト A、B、C の使用量が、これらの制限の合計である 3% に達することは不可能になります無制限アクセスの設定は、ASA のオーバーサブスクライブと同様ですが、システムをどの程度オーバーサブスクライブできるかを詳細には制御できません。

図 *32 :* 無限リソース



MAC アドレスについて

手動で MAC アドレスを割り当ててデフォルトをオーバーライドできます。マルチコンテキストモードでは、（コンテキストに割り当てられているすべてのインターフェイスの）一意の MAC アドレスと。

（注） 親インターフェイスと同じ組み込みの MAC アドレスを使用するので、ASA で定義されたサブインターフェイスに一意の MAC アドレスを割り当てることもできます。たとえば、サービスプロバイダーによっては、MAC アドレスに基づいてアクセス コントロールを実行する場合があります。また、IPv6 リンクローカル アドレスは MAC アドレスに基づいて生成されるため、サブインターフェイスに一意の MAC アドレスを割り当てることで、一意の IPv6 リンクローカル アドレスが可能になり、ASA で特定のインスタンスでのトラフィックの中断を避けることができます。

マルチコンテキスト モードでの MAC アドレス

MAC アドレスは、コンテキスト内でパケットを分類するために使用されます。あるインターフェイスを共有させる場合に、コンテキストごとにそのインターフェイスの固有 MAC アドレスを設定していなかった場合は、他の分類方法が試行されますが、その方法では十分にカバーされないことがあります。

コンテキスト間でのインターフェイス共有を許可するには、共有されるコンテキストインターフェイスそれぞれで仮想 MAC アドレスの自動生成を有効にしてください。 ASASM の場合のみ、自動生成はマルチ コンテキスト モードではデフォルトで有効になっています。

自動 MAC アドレス

マルチ コンテキスト モードでは、自動生成によって一意の MAC アドレスがコンテキストに割り当てられているすべてのインターフェイスに割り当てられます。

MAC アドレスを手動で割り当てた場合、自動生成がイネーブルになっていても、手動で割り当てた MAC アドレスが使用されます。後で手動 MAC アドレスを削除すると、自動生成されたアドレスが使用されます（有効になっている場合）。

生成した MAC アドレスがネットワーク内の別のプライベート MAC アドレスと競合することがまれにあります。この場合は、インターフェイスの MAC アドレスを手動で設定できます。

自動生成されたアドレス（プレフィックスを使用するとき）は A2 で始まるため、自動生成も使用する予定のときは手動 MAC アドレスを A2 で始めることはできません。

ASA は、次の形式を使用して MAC アドレスを生成します。

A2*xx.yyzz.zzzz*

xx.yy はユーザ定義プレフィックスまたはインターフェイス MAC アドレスの最後の 2 バイトに基づいて自動生成されるプレフィックスです。*zz.zzzz* は ASA によって生成される内部カウンタです。スタンバイ MAC アドレスの場合、内部カウンタが 1 増えることを除けばアドレスは同じです。

プレフィックスの使用方法を示す例の場合、プレフィックス 77 を設定すると、ASA は 77 を 16 進数値 004D（*yyxx*）に変換します。MAC アドレスで使用すると、プレフィックスは ASA ネイティブ形式に一致するように逆にされます（*xxyy*）。

A24**D.00***zz.zzzz*

プレフィックス 1009（03F1）の場合、MAC アドレスは次のようになります。

A2**F1.03***zz.zzzz*

（注） プレフィックスのない MAC アドレス形式は従来のバージョンです。従来の形式に関する詳細については、コマンド リファレンスの **mac-address auto** コマンドを参照してください。

VPN サポート

VPN のリソースについては、VPN トンネルを許可するようにリソース管理を設定する必要があります。

マルチ コンテキスト モードでサイト間 VPN を使用できます。

リモート アクセス VPN はサポートされていません。

マルチ コンテキスト モードのライセンス

モデル	ライセンス要件
ASA 5506-X	サポートしない

モデル	ライセンス要件
ASA 5508-X	Security Plus ライセンス：2 コンテキスト オプション ライセンス：*5* コンテキスト
ASA 5512-X	• 基本ライセンス：サポートされない。 • Security Plus ライセンス：2 コンテキスト オプション ライセンス：*5* コンテキスト
ASA 5515-X	基本ライセンス：2 コンテキスト オプション ライセンス：*5* コンテキスト
ASA 5516-X	Security Plus ライセンス：2 コンテキスト オプション ライセンス：*5* コンテキスト
ASA 5525-X	基本ライセンス：2 コンテキスト オプション ライセンス：*5*、*10*、または *20* コンテキスト
ASA 5545-X	基本ライセンス：2 コンテキスト オプション ライセンス：*5*、*10*、*20*、または *50* コンテキスト
ASA 5555-X	基本ライセンス：2 コンテキスト オプション ライセンス：*5*、*10*、*20*、*50*、または *100* コンテキスト。
ASA 5585-X（SSP-10）	基本ライセンス：2 コンテキスト オプション ライセンス：*5*、*10*、*20*、*50*、または *100* コンテキスト。
ASA 5585-X（SSP-20、-40、および -60）	基本ライセンス：2 コンテキスト オプション ライセンス:*5*、*10*、*20*、*50*、*100*、または *250* コンテキスト。
ASASM	基本ライセンス：2 コンテキスト オプション ライセンス:*5*、*10*、*20*、*50*、*100*、または *250* コンテキスト。
Firepower 9300	基本ライセンス：10 コンテキスト オプションのライセンス：*10* コンテキストずつの追加で、*250* コンテキストまで。
ASAv	サポートしない

マルチ コンテキスト モードの前提条件

マルチ コンテキスト モードに切り替えた後で、システム コンフィギュレーションにアクセスするためにシステムまたは管理コンテキストに接続します。管理以外のコンテキストからシステムを設定することはできません。デフォルトでは、マルチ コンテキスト モードをイネーブルにした後はデフォルトの管理 IP アドレスを使用して管理コンテキストに接続できます。

マルチ コンテキスト モードのガイドライン

フェールオーバー

アクティブ/アクティブ モード フェールオーバーは、マルチ コンテキスト モードでのみサポートされます。

IPv6

クロス コンテキスト IPv6 ルーティングはサポートされません。

サポートされない機能

マルチコンテキスト モードでは、次の機能をサポートしません。

- RIP
- OSPFv3 （OSPFv2 がサポートされます）。
- マルチキャスト ルーティング
- 脅威の検出
- ユニファイド コミュニケーション
- QoS
- リモート アクセス VPN （サイトツーサイト VPN がサポートされます）。

その他のガイドライン

- コンテキスト モード（シングルまたはマルチ）は、リブートされても持続されますが、コンフィギュレーション ファイルには保存されません。コンフィギュレーションを別のデバイスにコピーする必要がある場合は、新規デバイスのモードを match に設定します。
- フラッシュ メモリのルート ディレクトリにコンテキスト コンフィギュレーションを保存する場合、一部のモデルでは、メモリに空き容量があっても、そのディレクトリに保存する余地がなくなることがあります。この場合は、コンフィギュレーション ファイルのサブディレクトリを作成します。背景：一部のモデル（ASA 5585-X など）では内部フラッシュ メモリに FAT 16 ファイルシステムが使用されており、8.3 形式に準拠した短い名前を使用

していない、または大文字を使用している場合、長いファイル名を保存するためにファイルシステムのスロットが使い尽くされるため、512 以上のファイルやフォルダを保存できません（http://support.microsoft.com/kb/120138/en-us を参照）。

マルチ コンテキスト モードのデフォルト

- デフォルトで、ASA はシングル コンテキスト モードになります。
- 「デフォルト クラス （208 ページ）」を参照してください。

マルチ コンテキストの設定

手順

ステップ 1 マルチ コンテキスト モードの有効化またはディセーブル化 （215 ページ）。

ステップ 2 （任意）リソース管理用のクラスの設定 （217 ページ）。

（注） VPN のサポートのために、リソース クラスの VPN リソースを設定する必要があります。デフォルト クラスは VPN を許可しません。

ステップ 3 システム実行スペースでインターフェイスを設定します。

- ASA 5500-X：基本的なインターフェイス設定 （465 ページ）。
- Firepower 9300—論理デバイス Firepower 9300 （155 ページ）
- ASASM：ASASM クイックスタート ガイド。

ステップ 4 セキュリティ コンテキストの設定 （221 ページ）。

ステップ 5 （任意）コンテキスト インターフェイスへの MAC アドレスの自動割り当て （225 ページ）。

ステップ 6 コンテキストのインターフェイス コンフィギュレーションを完成させます。「ルーテッド モード インターフェイスとトランスペアレント モード インターフェイス （523 ページ）」を参照してください。

マルチ コンテキスト モードの有効化またはディセーブル化

シスコへの発注方法によっては、ASA がすでにマルチセキュリティ コンテキスト用に設定されている場合があります。シングル モードからマルチ モードに変換する必要がある場合は、この項の手順に従ってください。

マルチ コンテキスト モードの有効化

シングル モードからマルチ モードに変換すると、ASA は実行コンフィギュレーションを 2 つのファイルに変換します。これらはシステム コンフィギュレーションで構成される新規スタートアップ コンフィギュレーションと、（内部フラッシュ メモリのルート ディレクトリの）管理コンテキストで構成される admin.cfg です。元の実行コンフィギュレーションは、old_running.cfg として（内部フラッシュ メモリのルート ディレクトリに）保存されます。元のスタートアップ コンフィギュレーションは保存されません。ASA は、管理コンテキストのエントリをシステム コンフィギュレーションに「admin」という名前で自動的に追加します。

始める前に

スタートアップの設定をバックアップします。シングル モードからマルチ モードに変換すると、ASA は実行コンフィギュレーションを 2 つのファイルに変換します。元のスタートアップ コンフィギュレーションは保存されません。コンフィギュレーションまたはその他のファイルのバックアップおよび復元 （1023 ページ）を参照してください。

手順

マルチ コンテキスト モードに変更します。

mode multiple

例：

```
ciscoasa(config)# mode multiple
```

ASA をリブートするよう求められます。

シングルコンテキスト モードの復元

以前の実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーしてモードをシングル モードに変更するには、次の手順を実行します。

始める前に

この手順はシステム実行スペースで実行します。

手順

ステップ 1 元の実行コンフィギュレーションのバックアップ バージョンを現在のスタートアップ コンフィギュレーションにコピーします。

copy disk0:old_running.cfg startup-config

例：

```
ciscoasa(config)# copy disk0:old_running.cfg startup-config
```

ステップ 2 モードをシングル モードに設定します。

mode single

例：

```
ciscoasa(config)# mode single
```

ASA をリブートするよう求められます。

リソース管理用のクラスの設定

システム コンフィギュレーションでクラスを設定するには、次の手順を実行します。新しい値を指定してコマンドを再入力すると、特定のリソース制限値を変更できます。

始める前に

- この手順はシステム実行スペースで実行します。
- 以下の表に、リソース タイプおよび制限を記載します。**show resource types** コマンドも参照してください。

（注） 「システム制限」に「該当なし」と記述されている場合、そのリソースにはハード システム制限がないため、リソースのパーセンテージを設定できません。

表 *5:* リソース名および制限

リソース名	レートまたは同時	コンテキストあたりの最小数と最大数	システム制限	説明
asdm	同時接続数	最小 1 最大 20	32	SSH 管理セッション。 ASDM セッションでは、2 つの HTTPS 接続が使用されます。一方は常に存在するモニタ用で、もう一方は変更を行ったときにだけ存在する設定変更用です。たとえば、ASDM セッションのシステム制限が 32 の場合、HTTPS セッション数は 64 に制限されます。

リソース名	レートまたは同時	コンテキストあたりの最小数と最大数	システム制限	説明
conns	同時またはレート	該当なし	同時接続数：モデルごとの接続制限については、モデルごとにサポートされている機能のライセンス（86 ページ）を参照してください。 レート：該当なし	任意の 2 つのホスト間の TCP または UDP 接続（1 つのホストと他の複数のホストとの間の接続を含む）。 （注） syslog メッセージは、xlates または conns のいずれか制限が低い方に対して生成されます。たとえば、xlates の制限を 7、conns の制限を 9 に設定した場合、ASA は syslog メッセージ 321001（「Resource 'xlates' limit of 7 reached for context 'ctx1'」）のみ生成し、321002（「Resource 'conn rate' limit of 5 reached for context 'ctx1'」）は生成しません。
ホスト	同時接続数	該当なし	該当なし	ASA 経由で接続可能なホスト。
inspects	レート	該当なし	該当なし	アプリケーション インスペクション数/秒。
mac-addresses	同時接続数	該当なし	65,535	トランスペアレント ファイアウォール モードでは、MAC アドレス テーブルで許可される MAC アドレス数。
routes	同時接続数	該当なし	該当なし	ダイナミック ルート。

リソース名	レートまたは同時	コンテキストあたりの最小数と最大数	システム制限	説明
vpn burst other	同時接続数	該当なし	モデルに応じた Other VPN セッション数から、**vpn other** 用にすべてのコンテキストに割り当てられたセッション数の合計を差し引いた値。	**vpn other** でコンテキストに割り当てられた数を超えて許可されるサイトツーサイト VPN セッションの数。たとえばモデルが 5000 セッションをサポートしており、**vpn other** のすべてのコンテキスト全体で 4000 セッションを割り当てると、残りの 1000 セッションは **vpn burst other** に使用できます。**vpn other** ではセッション数がコンテキストに対して保証されますが、対照的に **vpn burst other** ではオーバーサブスクライブが可能です。すべてのコンテキストでバースト プールを先着順に使用できます。
vpn other	同時接続数	該当なし	モデルごとの使用可能な Other VPN セッション数については、モデルごとにサポートされている機能のライセンス （86 ページ）を参照してください。	サイトツーサイト VPN セッション。このリソースはオーバーサブスクライブできません。すべてのコンテキストへの割り当て合計がモデルの制限を超えてはなりません。このリソースに割り当てたセッションは、そのコンテキストに対して保証されます。
ikev1 in-negotiation	同時（パーセンテージのみ）	該当なし	このコンテキストに割り当てられている Other VPN セッションのパーセンテージ。セッションをコンテキストに割り当てるには、**vpn other** リソースを参照してください。	コンテキストでの Other VPN パーセンテージ制限として表される、着信 IKEv1 SA ネゴシエーション。
ssh	同時接続数	最小 1 最大 5	100	SSH セッション
syslogs	レート	該当なし	該当なし	Syslog メッセージ数/秒。
Telnet	同時接続数	最小 1 最大 5	100	Telnet セッション。
xlates	同時接続数	該当なし	該当なし	ネットワーク アドレス変換。

手順

ステップ 1 クラス名を指定して、クラス コンフィギュレーション モードを開始します。

class *name*

例：

```
ciscoasa(config)# class gold
```

name は、最大 20 文字の文字列です。デフォルト クラスの制限値を設定するには、名前として **default** と入力します。

ステップ 2 リソース タイプのリソース制限を設定します。

limit-resource [**rate**] *resource_name number*[**%**]

例：

```
ciscoasa(config-class)# limit-resource rate inspects 10
```

- リソース タイプのリストについては、上記の表を参照してください。**all** を指定すると、すべてのリソースが同じ値に設定されます。特定のリソースの値も指定した場合は、その制限は **all** に対して設定された制限よりも優先されます。
- **rate** 引数を入力して、特定のリソースの毎秒あたりのレートを設定します。
- ほとんどのリソースについては、**0** を *number* に対して設定すると、そのリソースは無制限となるか、システム制限を上限とする（システム制限がある場合）ことになります。VPN のリソースについては、**0** を指定すると制限なしと設定されます。
- システム制限がないリソースの場合は、パーセンテージ（**%**）を設定できません。絶対値のみを設定できます。

例

たとえば、conns のデフォルト クラス制限を無制限ではなく 10% に設定し、サイト ツーサイト VPN トンネル 5 本と VPN バースト用のトンネル 2 本を許可するには、次のコマンドを入力します。

```
ciscoasa(config)# class default
ciscoasa(config-class)# limit-resource conns 10%
ciscoasa(config-class)# limit-resource vpn other 5
ciscoasa(config-class)# limit-resource vpn burst other 2
```

他のリソースはすべて無制限のままです。

gold というクラスを追加するには、次のコマンドを入力します。

```
ciscoasa(config)# class gold
ciscoasa(config-class)# limit-resource mac-addresses 10000
ciscoasa(config-class)# limit-resource conns 15%
ciscoasa(config-class)# limit-resource rate conns 1000
ciscoasa(config-class)# limit-resource rate inspects 500
ciscoasa(config-class)# limit-resource hosts 9000
ciscoasa(config-class)# limit-resource asdm 5
ciscoasa(config-class)# limit-resource ssh 5
ciscoasa(config-class)# limit-resource rate syslogs 5000
ciscoasa(config-class)# limit-resource telnet 5
ciscoasa(config-class)# limit-resource xlates 36000
ciscoasa(config-class)# limit-resource routes 5000
ciscoasa(config-class)# limit-resource vpn other 10
ciscoasa(config-class)# limit-resource vpn burst other 5
```

セキュリティ コンテキストの設定

システム コンフィギュレーションのセキュリティ コンテキスト定義では、コンテキスト名、コンフィギュレーション ファイルの URL、コンテキストが使用できるインターフェイス、およびその他の設定値を指定します。

始める前に

- この手順はシステム実行スペースで実行します。
- インターフェイスを設定します。
  - ASA 5500-X：基本的なインターフェイス設定 （465 ページ）。
  - Firepower 9300—論理デバイス Firepower 9300 （155 ページ）
  - ASASM：ASASM クイックスタート ガイド。
- 管理コンテキストがない場合（コンフィギュレーションをクリアした場合など）は、最初に次のコマンドを入力して管理コンテキスト名を指定する必要があります。

  ```
  ciscoasa(config)# admin-context name
  ```

  このコンテキストはコンフィギュレーション内にまだ存在しませんが、続いて **context** *name* コマンドを入力して管理コンテキスト コンフィギュレーションに進むことができます。

手順

ステップ 1 コンテキストを追加または変更します。

context *name*

例：

```
ciscoasa(config)# context admin
```

name は最大 32 文字の文字列です。この名前では大文字と小文字が区別されるため、たとえば、「customerA」および「CustomerA」という 2 つのコンテキストを保持できます。文字、数字、またはハイフンを使用できますが、名前の先頭または末尾にハイフンは使用できません。

（注） 「System」および「Null」（大文字と小文字の両方）は予約されている名前であり、使用できません。

ステップ 2 （任意） このコンテキストの説明を追加します。

description *text*

例：

```
ciscoasa(config-ctx)# description Admin Context
```

ステップ 3 コンテキストで使用できるインターフェイスを指定します。

インターフェイスを割り当てるには：

allocate-interface *interface_id* [*mapped_name*] [**visible** | **invisible**]

1 つまたは複数のサブインターフェイスを割り当てるには：

allocate-interface *interface_id*.*subinterface* [-*interface_id*.*subinterface*] [*mapped_name*[-*mapped_name*]] [**visible** | **invisible**]

例：

```
ciscoasa(config-ctx)# allocate-interface gigabitethernet0/1.100 int1
ciscoasa(config-ctx)# allocate-interface gigabitethernet0/1.200 int2
ciscoasa(config-ctx)# allocate-interface gigabitethernet0/2.300-gigabitethernet0/2.305
int3-int8
```

（注） インターフェイス タイプとポート番号の間にスペースを含めないでください。

- これらのコマンドを複数回入力して複数の範囲を指定します。このコマンドの **no** 形式を使用して割り当てを削除すると、このインターフェイスを含むコンテキスト コマンドはいずれも実行コンフィギュレーションから削除されます。
- トランスペアレント ファイアウォール モードでは、限られた数のインターフェイスのみがトラフィックを通過させることができます。ただし、専用の管理インターフェイスである Management *slot*/*port*（物理、サブインターフェイス、冗長、または EtherChannel）を管理トラフィック用の追加インターフェイスとして使用できます。 独立した管理インターフェイスは、ASASM では使用できません。
- ルーテッドモードでは、必要に応じて同じインターフェイスを複数のコンテキストに割り当てることができます。トランスペアレントモードでは、インターフェイスを共有できません。
- *mapped_name* は、インターフェイス ID の代わりにコンテキスト内で使用できるインターフェイスの英数字のエイリアスです。マッピング名を指定しない場合、インターフェイス IDがコンテキスト内で使用されます。セキュリティ目的で、コンテキストがどのインターフェイスを使用しているかをコンテキスト管理者には知らせないようにすることができま

す。マッピング名はアルファベットで始まり、アルファベットまたは数字で終わる必要があります。その間の文字には、アルファベット、数字、または下線のみを使用できます。たとえば、次の名前を使用できます。**int0**、**inta**、**int_0**。

- サブインターフェイスの範囲を指定する場合は、マッピング名の一致範囲を指定できます。範囲については、次のガイドラインに従ってください。
  - マッピング名は、アルファベット部分と、それに続く数値部分で構成する必要があります。マッピング名のアルファベット部分は、範囲の両端で一致している必要があります。たとえば、次のような範囲を入力します。**int0-int10**。たとえば、gig0/1.1-gig0/1.5 **happy**1-**sad**5 と入力した場合、このコマンドは失敗します。
  - マッピング名の数値部分には、サブインターフェイスの範囲と同じ個数の数値を含める必要があります。たとえば、次のように、両方の範囲に 100 個のインターフェイスが含まれている場合：**gigabitethernet0/0.100-gigabitethernet0/0.199 int1-int100**。たとえば、gig0/0.**100**-gig0/0.**199** int**1**-int**15** と入力した場合、コマンドは失敗します。
- マッピング名を設定している場合に **show interface** コマンドで実際のインターフェイス ID を参照するには、**visible** を指定します。デフォルトの **invisible** キーワードでは、マッピング名だけが表示されます。

ステップ 4 システムがコンテキスト コンフィギュレーションをダウンロードする URL を識別します。

config-url *url*

例：

```
ciscoasa(config-ctx)# config-url ftp://user1:passw0rd@10.1.1.1/configlets/test.cfg
```

ステップ 5 （任意） コンテキストをリソース クラスに割り当てます。

member *class_name*

例：

```
ciscoasa(config-ctx)# member gold
```

クラスを指定しない場合、コンテキストはデフォルト クラスに属します。コンテキストは1つのリソース クラスにだけ割り当てることができます。

ステップ 6 （任意） このコンテキストに IPS 仮想センサーを割り当てます（IPS モジュールがインストールされている場合）。

allocate-ips *sensor_name* [*mapped_name*] [**default**]

例：

```
ciscoasa(config-ctx)# allocate-ips sensor1 highsec
```

仮想センサーの詳細については、IPS クイック スタート ガイドを参照してください。

- コンテキストのURLを追加すると、そのコンテキストをただちにロードし、コンフィギュレーションが使用可能であればコンテキストを実行できるようにします。
- **config-url** コマンドを入力する前に、allocate-interface コマンドを入力します。**config-url** コマンドを先に入力した場合、ASAはただちにコンテキスト コンフィギュレーションをロードします。そのコンテキストが（未設定）インターフェイスを参照するコマンドを含んでいる場合、それらのコマンドは失敗します。
- ファイル名にファイル拡張子は必要ありませんが、「.cfg」を使用することを推奨します。管理コンテキストからサーバにアクセス可能である必要があります。コンフィギュレーション ファイルが存在しない場合は、次の警告メッセージが表示されます。

```
WARNING: Could not fetch the URL url
INFO: Creating context with default config
```

- HTTP（S）以外の URL の場合、対象 URL にファイルを書き込むには、URL を指定した後、そのコンテキストに変更し、CLIに設定して、**write memory** コマンドを入力します。（HTTP（S）は読み取り専用です）。
- 管理コンテキスト ファイルは内部フラッシュ メモリに保存する必要があります。
- 使用可能なURLには次のタイプがあります。**disk***number*（フラッシュ メモリ用）、**ftp**、**http**、**https**、**tftp**。
- URL を変更するには、新しい URL で config-url コマンドを再入力します。

ステップ 7 （任意）アクティブ/アクティブ フェールオーバーのフェールオーバー グループにコンテキストを割り当てます。

join-failover-group {**1** | **2**}

例：

```
ciscoasa(config-ctx)# join-failover-group 2
```

デフォルトでは、コンテキストはグループ 1 にあります。管理コンテキストは常にグループ 1 に置く必要があります。

ステップ 8 （任意） このコンテキストに対してクラウド Web セキュリティをイネーブルにします。

scansafe [**license** *key*]

例：

```
ciscoasa(config-ctx)# scansafe
```

license を指定しない場合は、システム コンフィギュレーションで設定されているライセンスがこのコンテキストで使用されます。ASAは、要求がどの組織からのものかを示すために、認証キーをクラウド Web セキュリティ プロキシ サーバに送信します。認証キーは 16 バイトの 16 進数です。

ScanSafe の詳細については、『ファイアウォールの構成ガイド』を参照してください。

例

次の例では、管理コンテキストを「administrator」と設定し、「administrator」というコンテキストを内部フラッシュ メモリに作成してから、2 つのコンテキストを FTP サーバから追加します。

```
ciscoasa(config)# admin-context admin
ciscoasa(config)# context admin
ciscoasa(config-ctx)# allocate-interface gigabitethernet0/0.1
ciscoasa(config-ctx)# allocate-interface gigabitethernet0/1.1
ciscoasa(config-ctx)# config-url disk0:/admin.cfg

ciscoasa(config-ctx)# context test
ciscoasa(config-ctx)# allocate-interface gigabitethernet0/0.100 int1
ciscoasa(config-ctx)# allocate-interface gigabitethernet0/0.102 int2
ciscoasa(config-ctx)# allocate-interface gigabitethernet0/0.110-gigabitethernet0/0.115
int3-int8
ciscoasa(config-ctx)# config-url ftp://user1:passw0rd@10.1.1.1/configlets/test.cfg
ciscoasa(config-ctx)# member gold


ciscoasa(config-ctx)# context sample
ciscoasa(config-ctx)# allocate-interface gigabitethernet0/1.200 int1
ciscoasa(config-ctx)# allocate-interface gigabitethernet0/1.212 int2
ciscoasa(config-ctx)# allocate-interface gigabitethernet0/1.230-gigabitethernet0/1.235
int3-int8
ciscoasa(config-ctx)# config-url ftp://user1:passw0rd@10.1.1.1/configlets/sample.cfg
ciscoasa(config-ctx)# member silver
```

コンテキスト インターフェイスへの MAC アドレスの自動割り当て

この項では、MACアドレスの自動生成の設定方法について説明します。MACアドレスは、コンテキスト内でパケットを分類するために使用されます。

始める前に

- コンテキストでインターフェイスの **nameif** コマンドを設定すると、ただちに新規MACアドレスが生成されます。コンテキストインターフェイスを設定した後でこの機能をイネーブルにした場合は、イネーブルにした直後に、すべてのインターフェイスの MAC アドレスが生成されます。この機能をディセーブルにすると、各インターフェイスの MAC アドレスはデフォルトの MAC アドレスに戻ります。たとえば、GigabitEthernet 0/1 のサブインターフェイスは GigabitEthernet 0/1 の MAC アドレスを使用するようになります。
- 生成した MAC アドレスがネットワーク内の別のプライベート MAC アドレスと競合することがまれにあります。この場合は、コンテキスト内のインターフェイスの MAC アドレスを手動で設定できます。

手順

プライベート MAC アドレスを各コンテキスト インターフェイスに自動的に割り当てます。

mac-address auto [**prefix** *prefix*]

例：

```
ciscoasa(config)# mac-address auto prefix 19
```

プレフィックスを入力しない場合は、ASA によって、インターフェイス（ASA 5500-X）またはバックプレーン（ASASM）MAC アドレスの最後の 2 バイトに基づいてプレフィックスが自動生成されます。

手動でプレフィックスを入力する場合は、*prefix* に 0 ～ 65535 の 10 進数値を指定します。このプレフィックスは 4 桁の 16 進数値に変換され、MAC アドレスの一部として使用されます。

コンテキストとシステム実行スペースの切り替え

システム実行スペース（または管理コンテキスト）にログインした場合は、コンテキストを切り替えながら、各コンテキスト内でコンフィギュレーションやタスクのモニタリングを実行することができます。コンフィギュレーション モードで編集される実行コンフィギュレーション、つまり **copy** コマンドや **write** コマンドで使用される実行コンフィギュレーションは、ユーザのログイン先によって決まります。システム実行スペースにログインした場合、実行コンフィギュレーションはシステム コンフィギュレーションのみで構成され、コンテキストにログインした場合は、実行コンフィギュレーションはそのコンテキストのみで構成されます。たとえば、**show running-config** コマンドを入力しても、すべての実行コンフィギュレーション（システムおよびすべてのコンテキスト）を表示することはできません。現在のコンフィギュレーションだけが表示されます。

手順

ステップ 1 コンテキストに変更します。

changeto context *name*

プロンプトが ciscoasa/*name*# に変化します。

ステップ 2 システム実行スペースに変更します。

changeto system

プロンプトが ciscoasa# に変化します。

セキュリティ コンテキストの管理

この項では、セキュリティ コンテキストを管理する方法について説明します。

セキュリティ コンテキストの削除

現在の管理コンテキストは削除できません。ただし、**clear context** コマンドを使用してすべてのコンテキストを削除すれば、管理コンテキストも削除できます。

（注） フェールオーバーを使用すると、アクティブ装置でコンテキストを削除した時刻と、スタンバイ装置でコンテキストが削除された時刻との間で遅延が生じます。アクティブ装置とスタンバイ装置の間でインターフェイス数が一致していないことを示すエラーメッセージが表示される場合があります。このエラーは一時的に表示されるもので、無視できます。

始める前に

この手順はシステム実行スペースで実行します。

手順

ステップ 1 単一のコンテキストを削除します。

no context *name*

すべてのコンテキスト コマンドを削除することもできます。コンテキスト コンフィギュレーション ファイルがコンフィギュレーション URL の場所から削除されることはありません。

ステップ 2 すべてのコンテキスト（管理コンテキストを含む）を削除します。

clear context

コンテキスト コンフィギュレーション ファイルがコンフィギュレーション URL の場所から削除されることはありません。

管理コンテキストの変更

システム コンフィギュレーションには、ネットワーク インターフェイスやネットワーク設定は含まれません。その代わりに、ネットワーク リソースにアクセスする必要が生じたときに（サーバからコンテキストをダウンロードするなど）、システムは管理コンテキストとして指定されているコンテキストのいずれかを使用します。

管理コンテキストは、他のコンテキストとまったく同じです。ただ、ユーザが管理コンテキストにログインすると、システム管理者権限を持つので、システム コンテキストおよび他のすべてのコンテキストにアクセス可能になる点が異なります。管理コンテキストは制限されていないため、通常のコンテキストとして使用できます。ただし、管理コンテキストにログインすると、すべてのコンテキストへの管理者特権が付与されるため、場合によっては、管理コンテキストへのアクセスを適切なユーザに制限する必要があります。

始める前に

- コンフィギュレーション ファイルが内部フラッシュ メモリに保存されている限り、任意のコンテキストを管理コンテキストとして設定できます。
- この手順はシステム実行スペースで実行します。

手順

管理コンテキストを設定します。

admin-context *context_name*

例：

```
ciscoasa(config)# admin-context administrator
```

Telnet、SSH、HTTPS など、管理コンテキストに接続しているリモート管理セッションはすべて終了します。新しい管理コンテキストに再接続する必要があります。

いくつかのシステム コンフィギュレーション コマンド、たとえば **ntp server** では、管理コンテキストに所属するインターフェイス名が指定されます。管理コンテキストを変更した場合に、そのインターフェイス名が新しい管理コンテキストに存在しないときは、そのインターフェイスを参照するシステム コマンドはすべて、アップデートしてください。

セキュリティ コンテキスト URL の変更

この項では、コンテキスト URL を変更する方法について説明します。

始める前に

- セキュリティ コンテキスト URL は、新しい URL からコンフィギュレーションをリロードしないと変更できません。ASA は、新しいコンフィギュレーションを現在の実行コンフィギュレーションにマージします。
- 同じ URL を再入力した場合でも、保存されたコンフィギュレーションが実行コンフィギュレーションにマージされます。

- マージによって、新しいコンフィギュレーションから実行コンフィギュレーションに新しいコマンドが追加されます。
  - コンフィギュレーションが同じ場合、変更は発生しません。
  - コマンドが衝突する場合、またはコマンドがコンテキストの実行に影響を与える場合、マージの結果はコマンドによって異なります。エラーが発生することも、予期できない結果が生じることもあります。実行コンフィギュレーションが空白の場合（たとえば、サーバが使用不可でコンフィギュレーションがダウンロードされなかった場合）は、新しいコンフィギュレーションが使用されます。
- コンフィギュレーションをマージしない場合は、コンテキストを経由する通信を妨げる実行コンフィギュレーションをクリアしてから、新しい URL からコンフィギュレーションをリロードすることができます。
- この手順はシステム実行スペースで実行します。

手順

ステップ 1 （オプション、マージを実行しない場合）コンテキストに変更して、コンフィギュレーションをクリアします。

changeto context *name*

clear configure all

例：

```
ciscoasa(config)# changeto context ctx1
ciscoasa/ctx1(config)# clear configure all
```

マージを実行する場合は、ステップ 2 にスキップします。

ステップ 2 システム実行スペースに変更します。

changeto system

例：

```
ciscoasa/ctx1(config)# changeto system
ciscoasa(config)#
```

ステップ 3 変更するコンテキストのコンテキスト コンフィギュレーション モードを開始します。

context *name*

例：

```
ciscoasa(config)# context ctx1
```

ステップ 4 新しい URL を入力します。システムは、動作中になるように、ただちにコンテキストをロードします。

config-url *new_url*

例：

```
ciscoasa(config)# config-url ftp://user1:passw0rd@10.1.1.1/configlets/ctx1.cfg
```

セキュリティ コンテキストのリロード

セキュリティ コンテキストは、次の 2 つの方法でリロードできます。

- 実行コンフィギュレーションをクリアしてからスタートアップ コンフィギュレーションをインポートする。

  このアクションでは、セキュリティ コンテキストに関連付けられている接続や NAT テーブルなどの属性の大部分がクリアされます。

- セキュリティ コンテキストをシステム コンフィギュレーションから削除する。

  このアクションでは、トラブルシューティングに役立つ可能性のあるメモリ割り当てなど補足的な属性がクリアされます。しかし、コンテキストをシステムに戻して追加するには、URL とインターフェイスを再指定する必要があります。

コンフィギュレーションのクリアによるリロード

手順

ステップ 1 リロードするコンテキストに変更します。

changeto context *name*

例：

```
ciscoasa(config)# changeto context ctx1
ciscoasa/ctx1(comfig)#
```

ステップ 2 実行コンフィギュレーションをクリアします。

clear configure all

このコマンドを実行するとすべての接続がクリアされます。

ステップ 3 コンフィギュレーションをリロードします。

copy startup-config running-config

例：

```
ciscoasa/ctx1(config)# copy startup-config running-config
```

ASA は、システム コンフィギュレーションに指定された URL からコンフィギュレーションをコピーします。コンテキスト内で URL を変更することはできません。

コンテキストの削除および再追加によるリロード

コンテキストを削除し、その後再追加することによってコンテキストをリロードするには、次の手順を実行してください。

手順

ステップ 1 セキュリティ コンテキストの削除 （227 ページ）。

ステップ 2 セキュリティ コンテキストの設定 （221 ページ）

セキュリティ コンテキストのモニタリング

この項では、コンテキスト情報を表示およびモニタリングする方法について説明します。

コンテキスト情報の表示

システム実行スペースから、名前、割り当てられているインターフェイス、コンフィギュレーション ファイル URL を含むコンテキストのリストを表示できます。

手順

すべてのコンテキストの表示：

show context [*name* | **detail**| **count**]

特定のコンテキストの情報を表示する場合は、*name* にコンテキスト名を指定します。

detail オプションを指定すると、追加情報が表示されます。詳細については、次の出力例を参照してください。

count オプションを指定すると、コンテキストの合計数が表示されます。

例

次に、**show context** コマンドの出力例を示します。この出力例は、3 個のコンテキストを示しています。

```
ciscoasa# show context

Context Name      Interfaces                  URL
*admin            GigabitEthernet0/1.100      disk0:/admin.cfg
                  GigabitEthernet0/1.101
contexta          GigabitEthernet0/1.200      disk0:/contexta.cfg
                  GigabitEthernet0/1.201
contextb          GigabitEthernet0/1.300      disk0:/contextb.cfg
                  GigabitEthernet0/1.301
Total active Security Contexts: 3
```

次の表は、各フィールドの説明を示しています。

表 *6 : show context* のフィールド

フィールド	説明
Context Name	すべてのコンテキスト名が表示されます。アスタリスク（*）の付いているコンテキスト名は、管理コンテキストです。
インターフェイス	このコンテキストに割り当てられたインターフェイス。
URL	ASA がコンテキストのコンフィギュレーションをロードする URL。

次に、**show context detail** コマンドの出力例を示します。

```
ciscoasa# show context detail

Context "admin", has been created, but initial ACL rules not complete
  Config URL: disk0:/admin.cfg
  Real Interfaces: Management0/0
  Mapped Interfaces: Management0/0
  Flags: 0x00000013, ID: 1

Context "ctx", has been created, but initial ACL rules not complete
  Config URL: ctx.cfg
  Real Interfaces: GigabitEthernet0/0.10, GigabitEthernet0/1.20,
     GigabitEthernet0/2.30
  Mapped Interfaces: int1, int2, int3
  Flags: 0x00000011, ID: 2

Context "system", is a system resource
  Config URL: startup-config
  Real Interfaces:
  Mapped Interfaces: Control0/0, GigabitEthernet0/0,
     GigabitEthernet0/0.10, GigabitEthernet0/1, GigabitEthernet0/1.10,
     GigabitEthernet0/1.20, GigabitEthernet0/2, GigabitEthernet0/2.30,
```

```
    GigabitEthernet0/3, Management0/0, Management0/0.1
  Flags: 0x00000019, ID: 257

Context "null", is a system resource
  Config URL: ... null ...
  Real Interfaces:
  Mapped Interfaces:
  Flags: 0x00000009, ID: 258
```

detail の出力の詳細については、コマンド リファレンスを参照してください。

次に、**show context count** コマンドの出力例を示します。

```
ciscoasa# show context count
Total active contexts: 2
```

リソースの割り当ての表示

システム実行スペースから、すべてのクラスおよびクラス メンバーに渡るリソースごとの割り当て状況を表示できます。

手順

リソース割り当てを表示します。

show resource allocation [**detail**]

このコマンドは、リソース割り当てを表示しますが、実際に使用されているリソースは表示しません。実際のリソース使用状況の詳細については、リソースの使用状況の表示 （236ページ）を参照してください。

detail 引数を指定すると、追加情報が表示されます。詳細については、次の出力例を参照してください。

例

次の出力例には、各リソースの合計割り当て量が絶対値および使用可能なシステム リソースの割合として示されています。

```
ciscoasa# show resource allocation
Resource                    Total       % of Avail
 Conns [rate]               35000           N/A
 Inspects [rate]            35000           N/A
 Syslogs [rate]             10500           N/A
 Conns                     305000           30.50%
 Hosts                      78842           N/A
 SSH                           35           35.00%
 Routes                      5000           N/A
 Telnet                        35           35.00%
```

```
Xlates                       91749           N/A

Other VPN Sessions             20            2.66%
Other VPN Burst                20            2.66%
All                       unlimited
```

次の表は、各フィールドの説明を示しています。

表 *7: show resource allocation* のフィールド

フィールド	説明
Resource	制限を課すことのできるリソースの名前。
Total	すべてのコンテキストで割り当てられるリソースの総量。この数量は、同時発生インスタンスまたは 1 秒あたりのインスタンスの絶対量です。クラス定義でパーセンテージを指定した場合、ASAはこの表示のためにパーセンテージを絶対数に変換します。
% of Avail	リソースにハードウェア システム制限がある場合に、コンテキスト全体に渡って割り当てられている合計システム リソースの割合。リソースにシステム制限がない場合、このカラムには N/A と表示されます。

次に、**show resource allocation detail** コマンドの出力例を示します。

```
ciscoasa# show resource allocation detail
Resource Origin:
    A    Value was derived from the resource 'all'
    C    Value set in the definition of this class
    D    Value set in default class
Resource         Class          Mmbrs  Origin      Limit      Total    Total %
Conns [rate]     default          all      CA  unlimited
                 gold               1       C      34000      34000     N/A
                 silver             1      CA      17000      17000     N/A
                 bronze             0      CA       8500
                 All Contexts:      3                         51000     N/A

Inspects [rate]  default          all      CA  unlimited
                 gold               1      DA  unlimited
                 silver             1      CA      10000      10000     N/A
                 bronze             0      CA       5000
                 All Contexts:      3                         10000     N/A

Syslogs [rate]   default          all      CA  unlimited
                 gold               1       C       6000       6000     N/A
                 silver             1      CA       3000       3000     N/A
                 bronze             0      CA       1500
                 All Contexts:      3                          9000     N/A

Conns            default          all      CA  unlimited
                 gold               1       C     200000     200000     20.00%
                 silver             1      CA     100000     100000     10.00%
```

```
                bronze             0      CA      50000
                All Contexts:      3                        300000     30.00%

Hosts           default          all      CA  unlimited
                gold               1      DA  unlimited
                silver             1      CA      26214       26214      N/A
                bronze             0      CA      13107
                All Contexts:      3                        26214      N/A

SSH             default          all       C          5
                gold               1       D          5           5      5.00%
                silver             1      CA         10          10     10.00%
                bronze             0      CA          5
                All Contexts:      3                          20     20.00%

Telnet          default          all       C          5
                gold               1       D          5           5      5.00%
                silver             1      CA         10          10     10.00%
                bronze             0      CA          5
                All Contexts:      3                          20     20.00%

Routes          default          all       C  unlimited                 N/A
                gold               1       D  unlimited           5      N/A
                silver             1      CA         10          10      N/A
                bronze             0      CA          5                  N/A
                All Contexts:      3                          20      N/A

Xlates          default          all      CA  unlimited
                gold               1      DA  unlimited
                silver             1      CA      23040       23040     N/A
                bronze             0      CA      11520
                All Contexts:      3                        23040     N/A

mac-addresses   default          all       C      65535
                gold               1       D      65535       65535    100.00%
                silver             1      CA       6553        6553      9.99%
                bronze             0      CA       3276
                All Contexts:      3                        137623    209.99%
```

次の表は、各フィールドの説明を示しています。

表 *8 : show resource allocation detail* のフィールド

フィールド	説明
Resource	制限を課すことのできるリソースの名前。
Class	デフォルト クラスを含む、各クラスの名前。 すべてのコンテキスト フィールドには、すべてのクラス全体での合計値が表示されます。
Mmbrs	各クラスに割り当てられるコンテキストの数。

フィールド	説明
Origin	リソース制限の生成元。値は次のとおりです。 • A：この制限を個々のリソースとしてではなく、**all** オプションを使用して設定します。 • C：この制限はメンバー クラスから生成されます。 • D：この制限はメンバー クラスでは定義されたのではなく、デフォルト クラスから生成されました。デフォルト クラスに割り当てられたコンテキストの場合、値は「D」ではなく「C」になります。 ASA では、「C」または「D」を「A」に組み合わせることができます。
Limit	コンテキストごとのリソース制限（絶対数として）。クラス定義でパーセンテージを指定した場合、ASA はこの表示のためにパーセンテージを絶対数に変換します。
Total	クラス内のすべてのコンテキストにわたって割り当てられているリソースの合計数。この数量は、同時発生インスタンスまたは 1 秒あたりのインスタンスの絶対量です。リソースが無制限の場合、この表示は空白です。
% of Avail	クラス内のコンテキスト全体に渡って割り当てられている合計システム リソースの割合。リソースが無制限の場合、この表示は空白です。リソースにシステム制限がない場合、このカラムの表示は N/A になります。

リソースの使用状況の表示

システム実行スペースで、コンテキストごとのリソースの使用状況やシステム リソースの使用状況を表示できます。

手順

コンテキストごとのリソース使用状況を表示します。

show resource usage [**context** *context_name* | **top** *n* | **all** | **summary** | **system**] [**resource** {*resource_name* | **all**} | **detail**] [**counter** *counter_name* [*count_threshold*]]

- デフォルトでは、**all**（すべての）コンテキストの使用状況が表示されます。各コンテキストは個別にリスト表示されます。
- 指定したリソースの上位 **n** 人のユーザとなっているコンテキストを表示するには、*top n* キーワードを入力します。このオプションでは、**resource all** ではなく、リソース タイプを 1 つのみ指定する必要があります。
- **summary** オプションを指定すると、すべてのコンテキストの使用状況が組み合されて表示されます。
- **system** オプションでは、すべてのコンテキストの使用状況が組み合されて表示されますが、組み合されたコンテキスト制限ではなく、リソースに対するシステムの制限が表示されます。
- **resource** *resource_name* で使用可能なリソース名については、リソース管理用のクラスの設定 （217 ページ） を参照してください。**show resource type** コマンドも参照してください。すべてのタイプを表示するには **all**（デフォルト）を指定します。
- **detail** オプションを指定すると、管理できないリソースを含むすべてのリソースの使用状況が表示されます。たとえば、TCP 代行受信の数を表示できます。
- **counter** *counter_name* には、次のいずれかのキーワードを指定します。
  - **current**：リソースのアクティブな同時発生インスタンス数、またはリソースの現在のレートを表示します。
  - **denied**：Limit カラムに示されるリソース制限を超えたため拒否されたインスタンスの数を表示します。
  - **peak**：ピーク時のリソースの同時発生インスタンス数、またはピーク時のリソースのレートを表示します。これは、統計情報が **clear resource usage** コマンドまたはデバイスのリブートによって最後にクリアされた時点から計測されます。
  - **all**：（デフォルト）すべての統計情報を表示します。
- *count_threshold* は、表示するリソースの下限を設定します。デフォルトは 1 です。リソースの使用状況がここで設定する回数を下回っている場合、そのリソースは表示されません。カウンタ名に **all** を指定した場合、*count_threshold* は現在の使用状況に適用されます。
- すべてのリソースを表示するには、*count_threshold* を **0** に設定します。

例

次に、**show resource usage context** コマンドの出力例を示します。ここでは、admin コンテキストのリソース使用状況を表示する例を示しています。

```
ciscoasa# show resource usage context admin

Resource              Current         Peak      Limit    Denied  Context
Telnet                      1            1          5         0  admin
Conns                      44           55        N/A         0  admin
Hosts                      45           56        N/A         0  admin
```

次に、**show resource usage summary** コマンドの出力例を示します。ここでは、すべてのコンテキストとすべてのリソースのリソース使用状況を表示する例を示しています。ここでは、6 コンテキスト分の制限値が表示されています。

```
ciscoasa# show resource usage summary

Resource              Current         Peak      Limit     Denied Context
Syslogs [rate]           1743         2132      N/A            0 Summary
Conns                     584          763      280000(S)      0 Summary
Xlates                   8526         8966      N/A            0 Summary
Hosts                     254          254      N/A            0 Summary
Conns [rate]              270          535      N/A         1704 Summary
Inspects [rate]           270          535      N/A            0 Summary

Other VPN Sessions        0             10      10           740 Summary
Other VPN Burst           0             10      10           730 Summary

S = System: Combined context limits exceed the system limit; the system limit is shown.
```

次に、**show resource usage summary** コマンドの出力例を示します。このコマンドでは、25 コンテキストの制限が示されます。Telnet 接続および SSH 接続のコンテキストの限界がコンテキストごとに 5 であるため、合計の限界は 125 です。システムの限界が単に 100 であるため、システムの限界が表示されています。

```
ciscoasa# show resource usage summary

Resource              Current         Peak      Limit    Denied   Context
Telnet                      1            1        100[S]      0   Summary
SSH                         2            2        100[S]      0   Summary
Conns                      56           90        130000(S)   0   Summary
Hosts                      89          102        N/A         0   Summary
S = System: Combined context limits exceed the system limit; the system limit is shown.
```

次に、**show resource usage system** コマンドの出力例を示します。このコマンドは、すべてのコンテキストのリソース使用状況を表示しますが、組み合わせたコンテキストの限界ではなく、システムの限界を表示しています。現在使用中でないリソースを表示するには、**counter all 0** オプションを指定します。Denied の統計情報は、システム制限がある場合に、その制限によってリソースが拒否された回数を示します。

```
ciscoasa# show resource usage system counter all 0

Resource              Current         Peak      Limit          Denied    Context
Telnet                      0            0        100               0    System
SSH                         0            0        100               0    System
ASDM                        0            0         32               0    System
Routes                      0            0        N/A               0    System
IPSec                       0            0          5               0    System
```

```
Syslogs [rate]              1           18        N/A             0    System
Conns                       0            1     280000             0    System
Xlates                      0            0        N/A             0    System
Hosts                       0            2        N/A             0    System
Conns [rate]                1            1        N/A             0    System
Inspects [rate]             0            0        N/A             0    System

Other VPN Sessions          0           10        750           740    System
Other VPN Burst             0           10        750           730    System
```

コンテキストでの SYN 攻撃のモニタリング

ASA は TCP 代行受信を使用して SYN 攻撃を阻止します。TCP 代行受信では、SYN クッキーアルゴリズムを使用して TCP SYN フラッディング攻撃を防ぎます。SYN フラッディング攻撃は、通常はスプーフィングされた IP アドレスから送信されてくる一連の SYN パケットで構成されています。SYN パケットのフラッディングが定常的に生じると、SYN キューが一杯になる状況が続き、接続要求に対してサービスを提供できなくなります。接続の初期接続しきい値を超えると、ASA はサーバのプロキシとして動作し、クライアント SYN 要求に対する SYN-ACK 応答を生成します。ASA がクライアントから ACK を受信すると、クライアントを認証し、サーバへの接続を許可できます。

手順

ステップ 1 各コンテキストについて、攻撃の割合をモニタリングします。

show perfmon

ステップ 2 個々のコンテキストの TCP 代行受信で使用されるリソースの量をモニタします。

show resource usage detail

ステップ 3 システム全体の TCP 代行受信で使用されるリソースをモニタします。

show resource usage summary detail

例

次に、**show perfmon** コマンドの出力例を示します。このコマンドは、admin というコンテキストの TCP 代行受信レートを表示します。

```
ciscoasa/admin# show perfmon

Context:admin
PERFMON STATS:   Current      Average
Xlates               0/s          0/s
Connections          0/s          0/s
TCP Conns            0/s          0/s
UDP Conns            0/s          0/s
URL Access           0/s          0/s
```

```
URL Server Req       0/s          0/s
WebSns Req           0/s          0/s
TCP Fixup            0/s          0/s
HTTP Fixup           0/s          0/s
FTP Fixup            0/s          0/s
AAA Authen           0/s          0/s
AAA Author           0/s          0/s
AAA Account          0/s          0/s
TCP Intercept    322779/s     322779/s
```

次に、**show resource usage detail** コマンドの出力例を示します。このコマンドは、個々のコンテキストの TCP 代行受信で使用されるリソース量を表示します。（**太字**のサンプル テキストは、TCP 代行受信情報を示します）。

```
ciscoasa(config)# show resource usage detail
Resource              Current         Peak      Limit        Denied Context
memory                 843732       847288  unlimited             0 admin
chunk:channels             14           15  unlimited             0 admin
chunk:fixup                15           15  unlimited             0 admin
chunk:hole                  1            1  unlimited             0 admin
chunk:ip-users             10           10  unlimited             0 admin
chunk:list-elem            21           21  unlimited             0 admin
chunk:list-hdr              3            4  unlimited             0 admin
chunk:route                 2            2  unlimited             0 admin
chunk:static                1            1  unlimited             0 admin
tcp-intercepts         328787       803610  unlimited             0 admin
np-statics                  3            3  unlimited             0 admin
statics                     1            1  unlimited             0 admin
ace-rules                   1            1  unlimited             0 admin
console-access-rul          2            2  unlimited             0 admin
fixup-rules                14           15  unlimited             0 admin
memory                 959872       960000  unlimited             0 c1
chunk:channels             15           16  unlimited             0 c1
chunk:dbgtrace              1            1  unlimited             0 c1
chunk:fixup                15           15  unlimited             0 c1
chunk:global                1            1  unlimited             0 c1
chunk:hole                  2            2  unlimited             0 c1
chunk:ip-users             10           10  unlimited             0 c1
chunk:udp-ctrl-blk          1            1  unlimited             0 c1
chunk:list-elem            24           24  unlimited             0 c1
chunk:list-hdr              5            6  unlimited             0 c1
chunk:nat                   1            1  unlimited             0 c1
chunk:route                 2            2  unlimited             0 c1
chunk:static                1            1  unlimited             0 c1
tcp-intercept-rate      16056        16254  unlimited             0 c1
globals                     1            1  unlimited             0 c1
np-statics                  3            3  unlimited             0 c1
statics                     1            1  unlimited             0 c1
nats                        1            1  unlimited             0 c1
ace-rules                   2            2  unlimited             0 c1
console-access-rul          2            2  unlimited             0 c1
fixup-rules                14           15  unlimited             0 c1
memory              232695716    232020648  unlimited             0 system
chunk:channels             17           20  unlimited             0 system
chunk:dbgtrace              3            3  unlimited             0 system
chunk:fixup                15           15  unlimited             0 system
chunk:ip-users              4            4  unlimited             0 system
chunk:list-elem          1014         1014  unlimited             0 system
chunk:list-hdr              1            1  unlimited             0 system
chunk:route                 1            1  unlimited             0 system
block:16384               510          885  unlimited             0 system
```

```
block:2048                 32           34  unlimited             0 system
```

次の出力例は、システム全体の TCP 代行受信で使用されるリソースを示します（**太字**のサンプル テキストは、TCP 代行受信情報を示します）。

```
ciscoasa(config)# show resource usage summary detail
Resource              Current         Peak      Limit        Denied Context
memory              238421312    238434336  unlimited             0 Summary
chunk:channels              46           48  unlimited             0 Summary
chunk:dbgtrace               4            4  unlimited             0 Summary
chunk:fixup                 45           45  unlimited             0 Summary
chunk:global                 1            1  unlimited             0 Summary
chunk:hole                   3            3  unlimited             0 Summary
chunk:ip-users              24           24  unlimited             0 Summary
chunk:udp-ctrl-blk           1            1  unlimited             0 Summary
chunk:list-elem           1059         1059  unlimited             0 Summary
chunk:list-hdr              10           11  unlimited             0 Summary
chunk:nat                    1            1  unlimited             0 Summary
chunk:route                  5            5  unlimited             0 Summary
chunk:static                 2            2  unlimited             0 Summary
block:16384                510          885  unlimited             0 Summary
block:2048                  32           35  unlimited             0 Summary
tcp-intercept-rate      341306       811579  unlimited             0 Summary
globals                      1            1  unlimited             0 Summary
np-statics                   6            6  unlimited             0 Summary
statics                      2            2        N/A             0 Summary
nats                         1            1        N/A             0 Summary
ace-rules                    3            3        N/A             0 Summary
console-access-rul           4            4        N/A             0 Summary
fixup-rules                 43           44        N/A             0 Summary
```

割り当てられた MAC アドレスの表示

システム コンフィギュレーション内またはコンテキスト内の自動生成された MAC アドレスを表示できます。

システム設定での MAC アドレスの表示

この項では、システム コンフィギュレーション内の MAC アドレスを表示する方法について説明します。

始める前に

MAC アドレスをインターフェイスに手動で割り当てるものの、その際に自動生成がイネーブルになっていると、手動 MAC アドレスが使用中のアドレスとなりますが、コンフィギュレーションには自動生成されたアドレスが引き続き表示されます。後で手動 MAC アドレスを削除すると、表示されている自動生成アドレスが使用されます。

手順

システム実行スペースから割り当てられた MAC アドレスを表示します。

show running-config all context [*name*]

割り当てられた MAC アドレスを表示するには、**all** オプションが必要です。**mac-address auto** コマンドは、グローバル コンフィギュレーション モードに限りユーザ設定可能ですが、コンテキスト コンフィギュレーション モードでは、このコマンドは読み取り専用エントリとして、割り当てられた MAC アドレスとともに表示されます。コンテキスト内で **nameif** コマンドで設定される割り当て済みのインターフェイスだけに MAC アドレスが割り当てられます。

例

show running-config all context admin コマンドからの次の出力には、Management0/0 インターフェイスに割り当てられたプライマリおよびスタンバイ MAC アドレスが表示されます。

```
ciscoasa# show running-config all context admin

context admin
  allocate-interface Management0/0
  mac-address auto Management0/0 a24d.0000.1440 a24d.0000.1441
  config-url disk0:/admin.cfg
```

show running-config all context コマンドからの次の出力には、すべてのコンテキスト インターフェイスのすべての MAC アドレス（プライマリおよびスタンバイ）が表示されます。GigabitEthernet0/0 と GigabitEthernet0/1 の各メイン インターフェイスはコンテキスト内部に **nameif** コマンドで設定されないため、それらのインターフェイスの MAC アドレスは生成されていないことに注意してください。

```
ciscoasa# show running-config all context

admin-context admin
context admin
  allocate-interface Management0/0
  mac-address auto Management0/0 a2d2.0400.125a a2d2.0400.125b
  config-url disk0:/admin.cfg
!

context CTX1
  allocate-interface GigabitEthernet0/0
  allocate-interface GigabitEthernet0/0.1-GigabitEthernet0/0.5
  mac-address auto GigabitEthernet0/0.1 a2d2.0400.11bc a2d2.0400.11bd
  mac-address auto GigabitEthernet0/0.2 a2d2.0400.11c0 a2d2.0400.11c1
  mac-address auto GigabitEthernet0/0.3 a2d2.0400.11c4 a2d2.0400.11c5
  mac-address auto GigabitEthernet0/0.4 a2d2.0400.11c8 a2d2.0400.11c9
  mac-address auto GigabitEthernet0/0.5 a2d2.0400.11cc a2d2.0400.11cd
  allocate-interface GigabitEthernet0/1
  allocate-interface GigabitEthernet0/1.1-GigabitEthernet0/1.3
  mac-address auto GigabitEthernet0/1.1 a2d2.0400.120c a2d2.0400.120d
  mac-address auto GigabitEthernet0/1.2 a2d2.0400.1210 a2d2.0400.1211
  mac-address auto GigabitEthernet0/1.3 a2d2.0400.1214 a2d2.0400.1215
  config-url disk0:/CTX1.cfg
!

context CTX2
  allocate-interface GigabitEthernet0/0
```

```
  allocate-interface GigabitEthernet0/0.1-GigabitEthernet0/0.5
  mac-address auto GigabitEthernet0/0.1 a2d2.0400.11ba a2d2.0400.11bb
  mac-address auto GigabitEthernet0/0.2 a2d2.0400.11be a2d2.0400.11bf
  mac-address auto GigabitEthernet0/0.3 a2d2.0400.11c2 a2d2.0400.11c3
  mac-address auto GigabitEthernet0/0.4 a2d2.0400.11c6 a2d2.0400.11c7
  mac-address auto GigabitEthernet0/0.5 a2d2.0400.11ca a2d2.0400.11cb
  allocate-interface GigabitEthernet0/1
  allocate-interface GigabitEthernet0/1.1-GigabitEthernet0/1.3
  mac-address auto GigabitEthernet0/1.1 a2d2.0400.120a a2d2.0400.120b
  mac-address auto GigabitEthernet0/1.2 a2d2.0400.120e a2d2.0400.120f
  mac-address auto GigabitEthernet0/1.3 a2d2.0400.1212 a2d2.0400.1213
  config-url disk0:/CTX2.cfg
!
```

コンテキスト内の MAC アドレスの表示

この項では、コンテキスト内で MAC アドレスを表示する方法について説明します。

手順

コンテキスト内で各インターフェイスに使用されている MAC アドレスを表示します。

/context# show interface | include (Interface)|(MAC)

例

次に例を示します。

```
ciscoasa/context# show interface | include (Interface)|(MAC)

Interface GigabitEthernet1/1.1 "g1/1.1", is down, line protocol is down
        MAC address a201.0101.0600, MTU 1500
Interface GigabitEthernet1/1.2 "g1/1.2", is down, line protocol is down
        MAC address a201.0102.0600, MTU 1500
Interface GigabitEthernet1/1.3 "g1/1.3", is down, line protocol is down
        MAC address a201.0103.0600, MTU 1500
...
```

（注） **show interface** コマンドは、使用中の MAC アドレスを表示します。MAC アドレスを手動で割り当てた場合に、自動生成がイネーブルになっていたときは、システム コンフィギュレーション内の未使用の自動生成アドレスのみを表示できます。

マルチ コンテキスト モードの例

次に例を示します。

- 各コンテキストのMACアドレスを、カスタムプレフィックスを使用して自動的に設定します。
- connsのデフォルト クラス制限を、無制限ではなく10%に設定し、VPN otherセッション数を10、バーストを5に設定します。
- goldリソース クラスを作成します。
- 管理コンテキストを「administrator」と設定します。
- 「administrator」というコンテキストを、デフォルトのリソース クラスの一部になるように、内部フラッシュ メモリ上に作成します。
- goldリソース クラスの一部としてFTPサーバから2個のコンテキストを追加します。

```
ciscoasa(config)# mac-address auto prefix 19

ciscoasa(config)# class default
ciscoasa(config-class)# limit-resource conns 10%
ciscoasa(config-class)# limit-resource vpn other 10
ciscoasa(config-class)# limit-resource vpn burst other 5

ciscoasa(config)# class gold
ciscoasa(config-class)# limit-resource mac-addresses 10000
ciscoasa(config-class)# limit-resource conns 15%
ciscoasa(config-class)# limit-resource rate conns 1000
ciscoasa(config-class)# limit-resource rate inspects 500
ciscoasa(config-class)# limit-resource hosts 9000
ciscoasa(config-class)# limit-resource asdm 5
ciscoasa(config-class)# limit-resource ssh 5
ciscoasa(config-class)# limit-resource rate syslogs 5000
ciscoasa(config-class)# limit-resource telnet 5
ciscoasa(config-class)# limit-resource xlates 36000
ciscoasa(config-class)# limit-resource routes 700
ciscoasa(config-class)# limit-resource vpn other 100
ciscoasa(config-class)# limit-resource vpn burst other 50

ciscoasa(config)# admin-context administrator
ciscoasa(config)# context administrator
ciscoasa(config-ctx)# allocate-interface gigabitethernet0/0.1
ciscoasa(config-ctx)# allocate-interface gigabitethernet0/1.1
ciscoasa(config-ctx)# config-url disk0:/admin.cfg

ciscoasa(config-ctx)# context test
ciscoasa(config-ctx)# allocate-interface gigabitethernet0/0.100 int1
ciscoasa(config-ctx)# allocate-interface gigabitethernet0/0.102 int2
ciscoasa(config-ctx)# allocate-interface gigabitethernet0/0.110-gigabitethernet0/0.115
int3-int8
ciscoasa(config-ctx)# config-url ftp://user1:passw0rd@10.1.1.1/configlets/test.cfg
ciscoasa(config-ctx)# member gold

ciscoasa(config-ctx)# context sample
ciscoasa(config-ctx)# allocate-interface gigabitethernet0/1.200 int1
ciscoasa(config-ctx)# allocate-interface gigabitethernet0/1.212 int2
ciscoasa(config-ctx)# allocate-interface gigabitethernet0/1.230-gigabitethernet0/1.235
int3-int8
ciscoasa(config-ctx)# config-url ftp://user1:passw0rd@10.1.1.1/configlets/sample.cfg
ciscoasa(config-ctx)# member gold
```

マルチ コンテキスト モードの履歴

表 *9:* マルチ コンテキスト モードの履歴

機能名	プラットフォーム リリース	機能情報
マルチセキュリティ コンテキスト	7.0(1)	マルチ コンテキスト モードが導入されました。 **context**、**mode**、**class** の各コマンドが導入されました。
MAC アドレス自動割り当て	7.2(1)	コンテキスト インターフェイスへの MAC アドレス自動割り当てが導入されました。 **mac-address auto** コマンドが導入されました。
リソース管理	7.2(1)	リソース管理が導入されました。 **class**、**limit-resource**、**member** の各コマンドが導入されました。
IPS 仮想センサー	8.0(2)	IPS ソフトウェアのバージョン 6.0 以降を実行している AIP SSM では、複数の仮想センサーを実行できます。つまり、AIP SSM に複数のセキュリティ ポリシーを設定することができます。各コンテキストまたはシングル モード ASA を 1 つまたは複数の仮想センサーに割り当てたり、複数のセキュリティ コンテキストを同じ仮想センサーに割り当てることができます。 **allocate-ips** コマンドが導入されました。

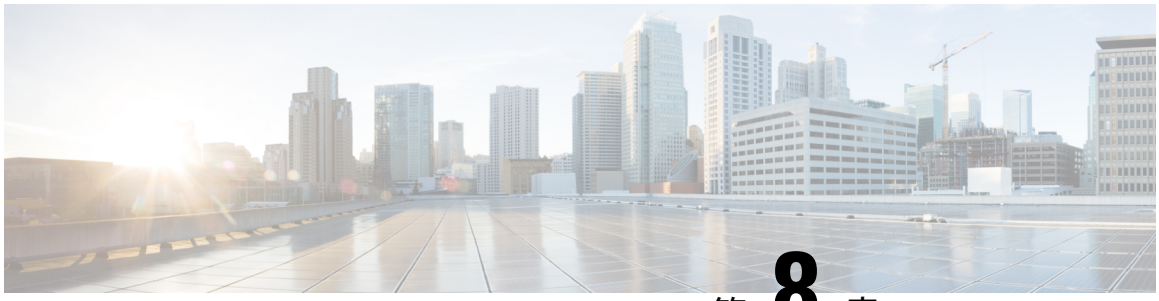
機能名	プラットフォーム リリース	機能情報
MAC アドレス自動割り当ての機能強化	8.0(5)/8.2(2)	MACアドレス形式が変更されました。プレフィックスが使用され、固定開始値（A2）が使用されます。また、フェールオーバーペアのプライマリ装置とセカンダリ装置の MAC アドレスそれぞれに異なるスキームが使用されます。MAC アドレスはリロード後も維持されるようになりました。コマンドパーサーは現在、自動生成がイネーブルになっているかどうかをチェックします。MAC アドレスを手動でも割り当てることができるようにする場合は、A2 を含む手動MACアドレスは開始できません。 **mac-address auto prefix** コマンドが変更されました。
ASA 5550 および 5580 の最大コンテキスト数の増加	8.4(1)	ASA 5550 の最大セキュリティ コンテキスト数が 50 から 100 に増加しました。ASA 5580 での最大数が 50 から 250 に増加しました。
MACアドレスの自動割り当てのデフォルトでの有効化	8.5(1)	MAC アドレスの自動割り当てが、デフォルトでイネーブルになりました。 **mac-address auto** コマンドが変更されました。

機能名	プラットフォーム リリース	機能情報
MAC アドレス プレフィックスの自動生成	8.6(1)	

機能名	プラットフォーム リリース	機能情報
		マルチ コンテキスト モードで、ASA が MAC アドレス自動生成のコンフィギュレーションを変換し、デフォルトのプレフィックスを使用できるようになりました。ASA は、インターフェイス（ASA 5500-X）またはバックプレーン（ASASM）の MAC アドレスの最後の 2 バイトに基づいてプレフィックスを自動生成します。この変換は、リロード時または MAC アドレス生成を再度イネーブルにすると、自動的に行われます。生成のプレフィックス方式は、セグメント上で一意の MAC アドレスがより適切に保証されるなど、多くの利点をもたらします。**show running-config mac-address** コマンドを入力して、自動生成されたプレフィックスを表示できます。プレフィックスを変更する場合、カスタムプレフィックスによって機能を再設定できます。MAC アドレス生成の従来の方法は使用できなくなります。 （注） フェールオーバーペアのヒットレス アップグレードを維持するため、ASA は、フェールオーバーが有効である場合、既存のコンフィギュレーションの MAC アドレス メソッドをリロード時に変換しません。ただし、フェールオーバーを使用するときは、生成メソッドをプレフィックスに手動で変更することを強く推奨します（特に ASASM の場合）。プレフィックス メソッドを使用しない場合、異なるスロット番号にインストールされた ASASM では、フェールオーバーが発生した場合に MAC アドレスの変更が行われ、トラフィックの中断が発生することがあります。アップグレード後に、

機能名	プラットフォーム リリース	機能情報
		MAC アドレス生成のプレフィックス方式を使用するには、デフォルトのプレフィックスを使用する MAC アドレス生成を再びイネーブルにします。 **mac-address auto** コマンドが変更されました。
ASASM 以外のすべてのモデル上での MACアドレスの自動割り当てはデフォルトでディセーブル	9.0(1)	自動 MAC アドレスの割り当ては ASASM を除いて、デフォルトでディセーブルになりました。 **mac-address auto** コマンドが変更されました。
セキュリティ コンテキストでのダイナミック ルーティング	9.0(1)	EIGRP と OSPFv2 ダイナミック ルーティング プロトコルが、マルチ コンテキスト モードでサポートされるようになりました。OSPFv3、RIP、およびマルチキャスト ルーティングはサポートされません。
ルーティング テーブル エントリのための新しいリソース タイプ	9.0(1)	新規リソース タイプ routes が作成されました。これは、各コンテキストでのルーティング テーブル エントリの最大数を設定するためです。 **limit-resource**、**show resource types**、**show resource usage**、**show resource allocation** の各コマンドが変更されました。
マルチ コンテキスト モードのサイトツーサイト VPN	9.0(1)	サイトツーサイト VPN トンネルが、マルチ コンテキスト モードでサポートされるようになりました。

機能名	プラットフォーム リリース	機能情報
サイトツーサイト VPN トンネルのための新しいリソース タイプ	9.0(1)	新しいリソース タイプ vpn other と vpn burst other が作成されました。これは、各コンテキストでのサイトツーサイト VPN トンネルの最大数を設定するためです。 **limit-resource**、**show resource types**、**show resource usage**、**show resource allocation** の各コマンドが変更されました。
IKEv1 SA ネゴシエーションの新しいリソース タイプ	9.1(2)	CPU と暗号化エンジンの過負荷を防ぐため、コンテキストごとに IKEv1 SA ネゴシエーションの最大パーセンテージを設定するための新しいリソース タイプ ikev1 in-negotiation が作成されました。特定の条件（大容量の証明書、CRL、チェックなど）によっては、このリソースを制限する必要がある場合があります。 **limit-resource**、**show resource types**、**show resource usage**、**show resource allocation** の各コマンドが変更されました。
IKEv2 のリモート アクセス VPN は、マルチ コンテキスト モードでサポートされています。	9.9(2)	リモート アクセス VPN は、IKEv2 のマルチ コンテキスト モードで構成できます。



第 8 章

ハイ アベイラビリティのためのフェールオーバー

この章では、Cisco ASA のハイ アベイラビリティを達成するために、アクティブ/スタンドバイまたはアクティブ/アクティブ フェールオーバーを設定する方法について説明します。

フェールオーバーについて

フェールオーバーの設定では、専用フェールオーバー リンク（および任意でステート リンク）を介して相互に接続された 2 つの同じ ASA が必要です。アクティブ装置およびインターフェイスのヘルスがモニタされて、所定のフェールオーバー条件に一致しているかどうかが判断されます。所定の条件に一致すると、フェールオーバーが行われます。

フェールオーバー モード

ASA は、アクティブ/アクティブ フェールオーバーとアクティブ/スタンバイ フェールオーバーの 2 つのフェールオーバー モードをサポートします。各フェールオーバー モードには、フェールオーバーを判定および実行する独自の方式があります。

- アクティブ/スタンバイ フェールオーバーでは、1 台の装置がアクティブ装置です。この装置がトラフィックを渡します。スタンバイ装置は、アクティブにトラフィックを渡しま

せん。フェールオーバーが発生すると、アクティブ装置がスタンバイ装置にフェールオーバーし、そのスタンバイ装置がアクティブになります。シングルまたはマルチ コンテキスト モードでは、ASA のアクティブ/スタンバイ フェールオーバーを使用できます。

- アクティブ/アクティブ フェールオーバー コンフィギュレーションでは、両方の ASA がネットワーク トラフィックを渡すことができます。アクティブ/アクティブ フェールオーバーは、マルチ コンテキスト モードの ASA でのみ使用できます。アクティブ/アクティブ フェールオーバーでは、ASA のセキュリティ コンテキストを 2 つのフェールオーバー グループ に分割します。フェールオーバー グループは、1 つまたは複数のセキュリティ コンテキストの論理グループにすぎません。一方のグループは、プライマリ ASA でアクティブになるよう割り当てられます。他方のグループは、セカンダリ ASA でアクティブになるよう割り当てられます。フェールオーバーが行われる場合は、フェールオーバー グループ レベルで行われます。

両方のフェールオーバー モードとも、ステートフルまたはステートレス フェールオーバーをサポートします。

フェールオーバー のシステム要件

この項では、フェールオーバー コンフィギュレーションにあるASAのハードウェア要件、ソフトウェア要件、およびライセンス要件について説明します。

ハードウェア要件

フェールオーバー コンフィギュレーションの 2 台の装置は、次の条件を満たしている必要があります。

- 同じモデルであること。
- インターフェイスの数とタイプが同じであること。

  Firepower 9300 シャーシ では、フェールオーバー を有効にする前に、すべてのインターフェイスがFXOS で同一に事前構成されている必要があります。フェールオーバーを有効にした後でインターフェイスを変更する場合は、スタンバイ ユニットのFXOS でインターフェイスを変更し、アクティブ ユニットで同じ変更を行います。 FXOS でインターフェイスを削除した場合（たとえば、ネットワーク モジュールの削除、EtherChannel の削除、またはEtherChannel へのインターフェイスの再割り当てなど）、必要な調整を行うことができるように、ASA 設定では元のコマンドが保持されます。設定からインターフェイスを削除すると、幅広い影響が出る可能性があります。ASA OS の古いインターフェイス設定は手動で削除できます。
- 同じモジュール（存在する場合）がインストールされていること。
- 同じ RAM がインストールされていること。

フェールオーバー コンフィギュレーションで装置に異なるサイズのフラッシュ メモリを使用している場合、小さい方のフラッシュ メモリを取り付けた装置に、ソフトウェア イメージ ファイルおよびコンフィギュレーション ファイルを格納できる十分な容量があることを確認してく

ださい。十分な容量がない場合、フラッシュ メモリの大きい装置からフラッシュ メモリの小さい装置にコンフィギュレーションの同期が行われると、失敗します。

ソフトウェア要件

フェールオーバー コンフィギュレーションの2台の装置は、次の条件を満たしている必要があります。

- コンテキスト モードが同じであること（シングルまたはマルチ）。
- 単一モードの場合：同じファイアウォールモードにあること（ルーテッドまたはトランスペアレント）。

  マルチコンテキスト モードでは、ファイアウォール モードはコンテキスト レベルで設定され、混合モードを使用できます。
- ソフトウェア バージョンが、メジャー（最初の番号）およびマイナー（2番目の番号）ともに同じであること。ただし、アップグレードプロセス中は、異なるバージョンのソフトウェアを一時的に使用できます。たとえば、ある装置をバージョン 8.3(1) からバージョン 8.3(2) にアップグレードし、フェールオーバーをアクティブ状態のままにできます。長期的に互換性を維持するために、両方の装置を同じバージョンにアップグレードすることをお勧めします。
- 同じ AnyConnect イメージを持っていること。中断のないアップグレードを実行するときにフェールオーバー ペアのイメージが一致しないと、アップグレード プロセスの最後のリブート手順でクライアントレス SSL VPN 接続が切断され、データベースには孤立したセッションが残り、IP プールではクライアントに割り当てられた IP アドレスが「使用中」として示されます。

ライセンス要件

フェールオーバー コンフィギュレーションの2台の装置は、ライセンスが同じである必要はありません。これらのライセンスは結合され、1つのフェールオーバー クラスタ ライセンスが構成されます。

フェールオーバー リンクとステートフル フェールオーバー リンク

フェールオーバー リンクとオプションのステートフル フェールオーバー リンクは、2 つの装置間の専用接続です。シスコでは、フェールオーバー リンクまたはステートフル フェールオーバー リンク内の2つのデバイス間で同じインターフェイスを使用することを推奨しています。たとえば、フェールオーバー リンクで、デバイス 1 で eth0 を使用していた場合は、デバイス 2 でも同じインターフェイス（eth0）を使用します。

⚠

注意 フェールオーバー リンクおよびステート リンク経由で送信される情報は、IPsec トンネルまたはフェールオーバー キーを使用して通信を保護しない限り、すべてクリア テキストで送信されます。VPN トンネルの終端に ASA を使用する場合、この情報には、トンネルの確立に使用されたすべてのユーザ名、パスワード、および事前共有キーが含まれています。この機密データをクリア テキストで転送することは、非常に大きなセキュリティ リスクになるおそれがあります。ASA を使用して VPN トンネルを終端する場合は、フェールオーバー通信を IPsec トンネルまたはフェールオーバー キーによってセキュリティ保護することをお勧めします。

フェールオーバー リンク

フェールオーバー ペアの 2 台の装置は、フェールオーバー リンク経由で常に通信して、各装置の動作ステータスを確認しています。

フェールオーバー リンク データ

次の情報がフェールオーバー リンク経由で伝達されています。

- 装置の状態（アクティブまたはスタンバイ）
- hello メッセージ（キープアライブ）
- ネットワーク リンクの状態
- MAC アドレス交換
- コンフィギュレーションの複製および同期

フェールオーバー リンクのインターフェイス

使用されていないデータ インターフェイス（物理、サブインターフェイス、冗長、または EtherChannel）はいずれもフェールオーバー リンクとして使用できます。ただし、現在名前が設定されているインターフェイスは指定できません。フェールオーバー リンク インターフェイスは、通常のネットワーク インターフェイスとしては設定されません。フェールオーバー通信のためにだけ存在します。このインターフェイスは、フェールオーバー リンク用にのみ使用できます（ステート リンク用としても使用できます）。ほとんどのモデルでは、以下で明示的に説明されていない限り、フェールオーバー用の管理インターフェイスを使用できません。

ASA は、ユーザ データとフェールオーバー リンク間でのインターフェイスの共有をサポートしていません。同じ親の別のサブインターフェイスをフェールオーバー リンクやデータのために使用することもできません。

フェールオーバー リンクについては、次のガイドラインを参照してください。

- 5506-X ～ 5555-X：管理インターフェイスをフェールオーバー リンクとして使用できません。データ インターフェイスを使用する必要があります。
- 5585-X：データ インターフェイスとしては使用できますが、管理 0/0 インターフェイスは使用しないでください。この用途で必要とされるパフォーマンスをサポートしていません。

- Firepower 4100/9300：統合されたフェールオーバー リンクとステート リンクには、10 GB のデータ インターフェイスを使用することを推奨します。フェールオーバー リンクに管理タイプのインターフェイスを使用することはできません。
- 他のすべてのモデル：1 GB インターフェイスは、フェールオーバーとステート リンクを組み合わせるには十分な大きさです。

フェールオーバー リンクとして使用される冗長インターフェイスについては、冗長性の増強による次の利点を参照してください:

- フェールオーバー ユニットが起動すると、メンバー インターフェイスを交互に実行し、アクティブ ユニットを検出します。
- メンバー インターフェイスの 1 つにあるピアからのキープアライブ メッセージの受信をフェールオーバー ユニットが停止した場合、別のメンバー インターフェイスに切り替えます。

フェールオーバー リンクとして使用される EtherChannel の場合は、順序が不正なパケットを防止するために、EtherChannel 内の 1 つのインターフェイスのみが使用されます。そのインターフェイスで障害が発生した場合は、EtherChannel 内の次のリンクが使用されます。フェールオーバー リンクとして使用中の EtherChannel の設定は変更できません。

フェールオーバー リンクの接続

フェールオーバー リンクを次の 2 つの方法のいずれかで接続します。

- ASAのフェールオーバーインターフェイスと同じネットワーク セグメント（ブロードキャスト ドメインまたは VLAN）に他の装置のないスイッチを使用する。
- イーサネット ケーブルを使用して装置を直接接続します。外部スイッチは必要ありません。

装置間でスイッチを使用しない場合、インターフェイスに障害が発生すると、リンクは両方のピアでダウンします。このような状況では、障害が発生してリンクがダウンする原因になったインターフェイスがどちらの装置のものかを簡単に特定できないため、トラブルシューティング作業が困難になる場合があります。

ASAは、銅線イーサネット ポートで Auto-MDI/MDIX をサポートしているため、クロスオーバー ケーブルまたはストレート ケーブルのいずれかを使用できます。ストレート ケーブルを使用した場合は、インターフェイスが自動的にケーブルを検出して、送信/受信ペアの 1 つを MDIX にスワップします。

ステートフル フェールオーバー リンク

ステートフル フェールオーバーを使用するには、接続ステート情報を渡すためのステートフル フェールオーバー リンク（ステート リンクとも呼ばれる）を設定する必要があります。

（注） ステートフル フェールオーバー リンクの帯域幅は、少なくともデータ インターフェイスの帯域幅と同等にすることを推奨します。

フェールオーバー リンクの共有

インターフェイスを節約するための最適な方法はフェールオーバー リンクの共有です。ただし、設定が大規模でトラフィックが膨大なネットワークを使用している場合は、ステート リンクとフェールオーバー リンク専用のインターフェイスを検討する必要があります。

専用のインターフェイス

ステート リンク専用のデータ インターフェイス（物理、冗長、またはEtherChannel）を使用できます。ステート リンクとして使用されるEtherChannelの場合は、順序が不正なパケットを防止するために、EtherChannel 内の 1 つのインターフェイスのみが使用されます。そのインターフェイスで障害が発生した場合は、EtherChannel 内の次のリンクが使用されます。

次の 2 つの方法のいずれかで、専用のステート リンクを接続します。

- ASA デバイスのフェールオーバー インターフェイスと同じネットワーク セグメント（ブロードキャスト ドメインまたは VLAN）に他の装置のないスイッチを使用する。
- イーサネット ケーブルを使用してアプライアンスを直接接続します。外部スイッチは必要ありません。

  装置間でスイッチを使用しない場合、インターフェイスに障害が発生すると、リンクは両方のピアでダウンします。このような状況では、障害が発生してリンクがダウンする原因になったインターフェイスがどちらの装置のものかを簡単に特定できないため、トラブルシューティング作業が困難になる場合があります。

  ASAは、銅線イーサネット ポートで Auto-MDI/MDIX をサポートしているため、クロスオーバー ケーブルまたはストレート ケーブルのいずれかを使用できます。ストレート ケーブルを使用した場合は、インターフェイスが自動的にケーブルを検出して、送信/受信ペアの 1 つを MDIX にスワップします。

長距離のフェールオーバーを使用する場合のステート リンクの遅延は、パフォーマンスを最善にするには 10 ミリ秒未満でなければならず、250 ミリ秒を超えないようにする必要があります。遅延が10ミリ秒を上回る場合、フェールオーバー メッセージの再送信によって、パフォーマンスが低下する可能性があります。

フェールオーバーの中断の回避とデータ リンク

すべてのインターフェイスで同時に障害が発生する可能性を減らすために、フェールオーバー リンクとデータ インターフェイスは異なるパスを通すことを推奨します。フェールオーバー リンクがダウンした場合、フェールオーバーが必要かどうかの決定に、ASA はデータ インターフェイスを使用できます。その後、フェールオーバー動作は、フェールオーバー リンクのヘルスが復元されるまで停止されます。

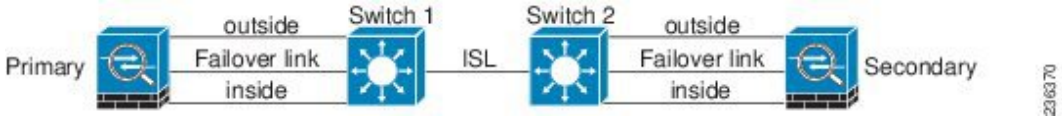
耐障害性のあるフェールオーバー ネットワークの設計については、次の接続シナリオを参照してください。

シナリオ 1：非推奨

単一のスイッチまたはスイッチ セットが 2 つの ASA 間のフェールオーバー インターフェイスとデータ インターフェイスの両方の接続に使用される場合、スイッチまたはスイッチ間リンクがダウンすると、両方の ASA がアクティブになります。したがって、次の図で示されている次の 2 つの接続方式は推奨しません。

図 *33 :* 単一のスイッチを使用した接続：非推奨

図 *34 : 2* つのスイッチを使用した接続：非推奨



シナリオ 2：推奨

フェールオーバー リンクには、データ インターフェイスと同じスイッチを使用しないことを推奨します。代わりに、次の図に示すように、別のスイッチを使用するか直接ケーブルを使用して、フェールオーバー リンクを接続します。

図 *35 :* 異なるスイッチを使用した接続

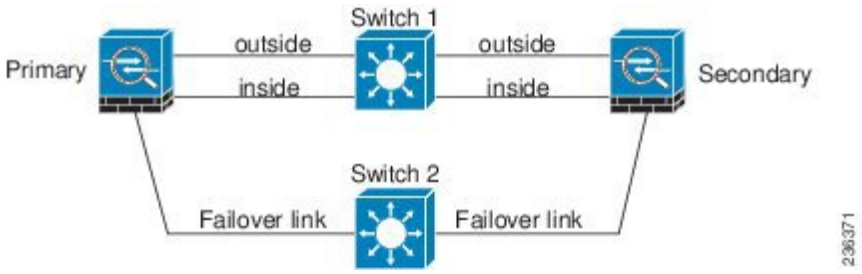
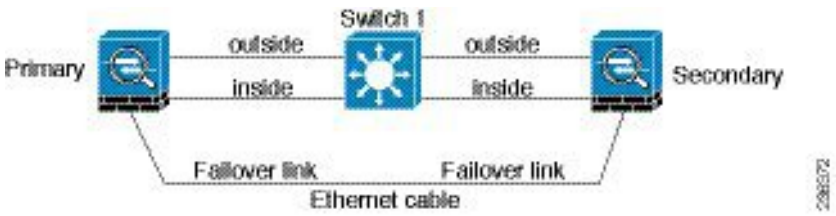


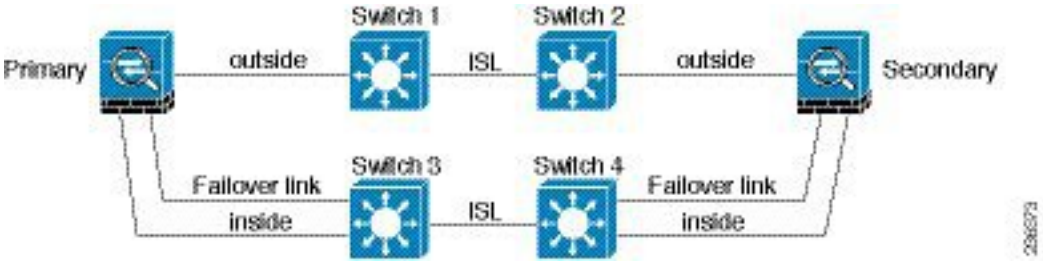
図 *36 :* ケーブルを使用した接続



シナリオ 3：推奨

ASA データ インターフェイスが複数セットのスイッチに接続されている場合、フェールオーバー リンクはいずれかのスイッチに接続できます。できれば、次の図に示すように、ネットワークのセキュアな側（内側）のスイッチに接続します。

図 *37*：セキュア スイッチを使用した接続



シナリオ 4：推奨

最も信頼性の高いフェールオーバー構成では、次の図に示すように、フェールオーバー リンクに冗長インターフェイスを使用します。

図 *38*：冗長インターフェイスを使用した接続

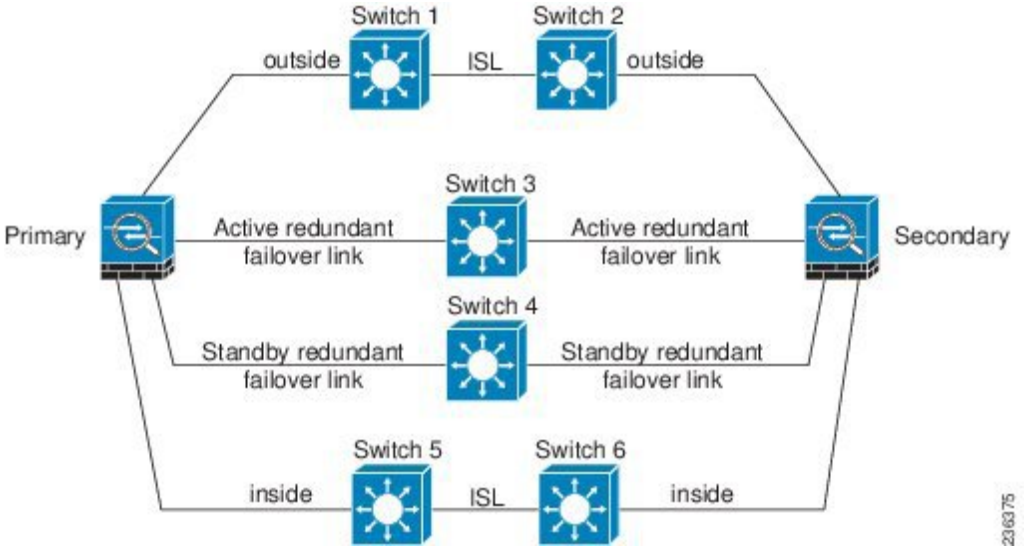
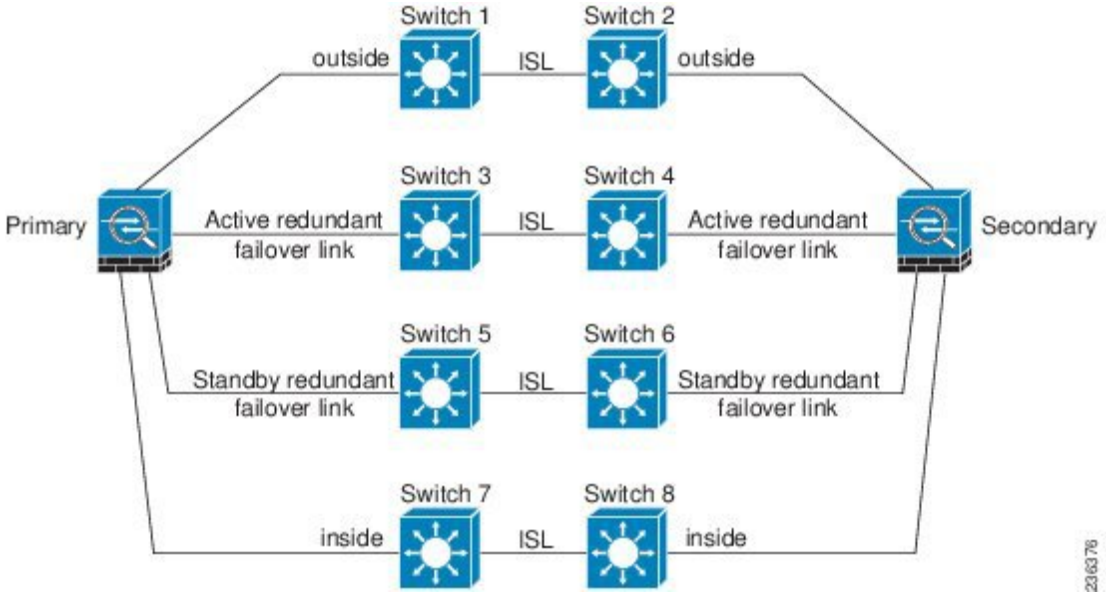


図 *39 : Inter-Switch Link*（*ISL*）を使用した接続



フェールオーバー の MAC アドレスと IP アドレス

インターフェイスを設定する場合、同じネットワーク上のアクティブ IP アドレスとスタンバイ IP アドレスを指定できます。一般的に、フェールオーバーが発生した場合、新しいアクティブ装置がアクティブな IP アドレスと MAC アドレスを引き継ぎます。ネットワーク デバイスは、MAC と IP アドレスの組み合わせについて変更を認識しないため、ネットワーク上のどのような場所でも ARP エントリが変更されたり、タイムアウトが生じたりすることはありません。

（注） スタンバイ アドレスを設定することが推奨されていますが、必須ではありません。スタンバイ IP アドレスがないと、アクティブ装置はスタンバイ インターフェイスの状態を確認するためのネットワーク テストを実行できません。リンク ステートのみ追跡できます。また、管理目的でそのインターフェイスのスタンバイ装置に接続することもできません。

ステート リンク用の IP アドレスおよび MAC アドレスは、フェールオーバー実行後も変更されません。

アクティブ/スタンバイ IP アドレスと MAC アドレス

アクティブ/スタンバイ フェールオーバー の場合、フェールオーバー イベント中の IP アドレスと MAC アドレスの使用については、次を参照してください。

1. アクティブ装置は常にプライマリ装置の IP アドレスと MAC アドレスを使用します。
2. アクティブ装置が故障すると、スタンバイ装置は故障した装置の IP アドレスと MAC アドレスを引き継ぎ、トラフィックを通過させます。

3. 故障した装置がオンラインに復帰すると、スタンバイ状態となり、スタンバイ IP アドレスと MAC アドレスを引き継ぎます。

ただし、セカンダリ装置がプライマリ装置を検出せずにブートした場合、セカンダリ装置がアクティブ装置になります。プライマリ装置の MAC アドレスを認識していないため、自分の MAC アドレスを使用します。プライマリ装置が使用可能になると、セカンダリ（アクティブ）装置は MAC アドレスをプライマリ装置の MAC アドレスに変更します。これによって、ネットワーク トラフィックが中断されることがあります。同様に、プライマリ装置を新しいハードウェアと交換すると、新しい MAC アドレスが使用されます。

仮想 MAC アドレスがこの中断を防ぎます。なぜなら、アクティブ MAC アドレスは起動時にセカンダリ装置によって認識され、プライマリ装置のハードウェアが新しくなっても変わらないからです。仮想 MAC アドレスを設定しなかった場合、トラフィック フローを復元するために、接続されたルータの ARP テーブルをクリアする必要がある場合があります。ASA は MAC アドレスを変更するときに、スタティック NAT アドレスに対して Gratuitous ARP を送信しません。そのため、接続されたルータはこれらのアドレスの MAC アドレスの変更を認識できません。

アクティブ/アクティブ IP アドレスと MAC アドレス

アクティブ/アクティブ フェールオーバーの場合、フェールオーバー イベント中の IP アドレスと MAC アドレスの使用については、次を参照してください。

1. プライマリ装置は、フェールオーバー グループ 1 および 2 のコンテキストのすべてのインターフェイスに対して、アクティブおよびスタンバイ MAC アドレスを自動生成します。必要に応じて、たとえば、MAC アドレスの競合がある場合は、MAC アドレスを手動で設定できます。
2. 各装置は、そのアクティブ フェールオーバー グループにアクティブな IP アドレスと MAC アドレスを使用し、そのスタンバイ フェールオーバー グループにスタンバイ アドレスを使用します。たとえば、フェールオーバー グループ 1 でプライマリ装置がアクティブである場合、フェールオーバー グループ 1 のコンテキストでアクティブなアドレスを使用します。フェールオーバー グループ 2 のコンテキストではスタンバイであるため、スタンバイ アドレスを使用します。
3. 装置が故障すると、他の装置は故障したフェールオーバー グループの アクティブな IP アドレスと MAC アドレスを引き継ぎ、トラフィックを通過させます。
4. 故障した装置がオンラインに戻り、preempt オプションが有効になっている場合、フェールオーバー グループを再開します。

仮想 MAC アドレス

ASA には、仮想 MAC アドレスを設定する複数の方法があります。1 つの方法のみ使用することをお勧めします。複数の方法を使用して MAC アドレスを設定した場合は、どの MAC アドレスが使用されるかは多くの可変要素によって決まるため、予測できないことがあります。手動方法にはインターフェイス モードの **mac-address** コマンド、**failover mac address** コマンドが

含まれ、アクティブ / アクティブ フェールオーバーでは、フェールオーバー グループ モードの **mac address** コマンドが、以下で説明する自動生成方法に加えて含まれます。

マルチ コンテキスト モードでは、共有インターフェイスに仮想アクティブおよびスタンバイ MAC アドレスを自動的に生成するように ASA を設定することができ、これらの割り当てはセカンダリ ユニットに同期されます（**mac-address auto** コマンドを参照してください）。共有以外のインターフェイスでは、アクティブ/スタンバイ モードの MAC アドレスを手動で設定することができます（アクティブ/アクティブ モードはすべてのインターフェイスに MAC アドレスを自動生成します）。

アクティブ/アクティブ フェールオーバーでは、仮想 MAC アドレスはデフォルト値またはインターフェイスごとに設定できる値のいずれかとともに常に使用されます。

ASAサービスモジュールのシャーシ内およびシャーシ間モジュール配置

プライマリとセカンダリの ASASM は、同じスイッチ内または 2 台の異なるスイッチに搭載できます。

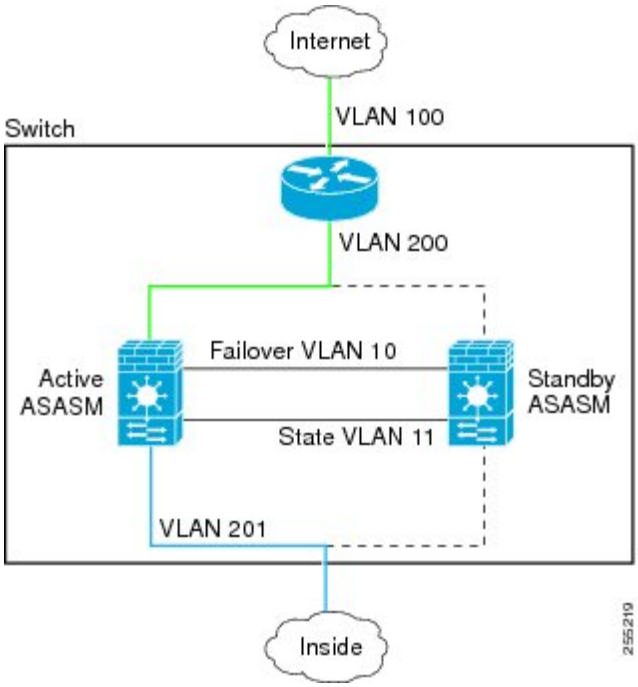
シャーシ内フェールオーバー

セカンダリ ASASM をプライマリ ASASM と同じスイッチに搭載した場合は、モジュール レベルの障害から保護する必要があります。

両方の ASASM に同じ VLAN が割り当てられますが、ネットワーキングに参加するのはアクティブ モジュールだけです。スタンバイ モジュールは、トラフィックを転送しません。

次の図は、一般的なスイッチ内の構成を示します。

図 *40 :* スイッチ内フェールオーバー



シャーシ間フェールオーバー

スイッチレベルの障害から保護するため、セカンダリ ASASM を別のスイッチに搭載できます。ASASM は直接スイッチとフェールオーバーを調整するのではなく、スイッチと協調してフェールオーバー操作を行います。スイッチのフェールオーバー設定については、スイッチのマニュアルを参照してください。

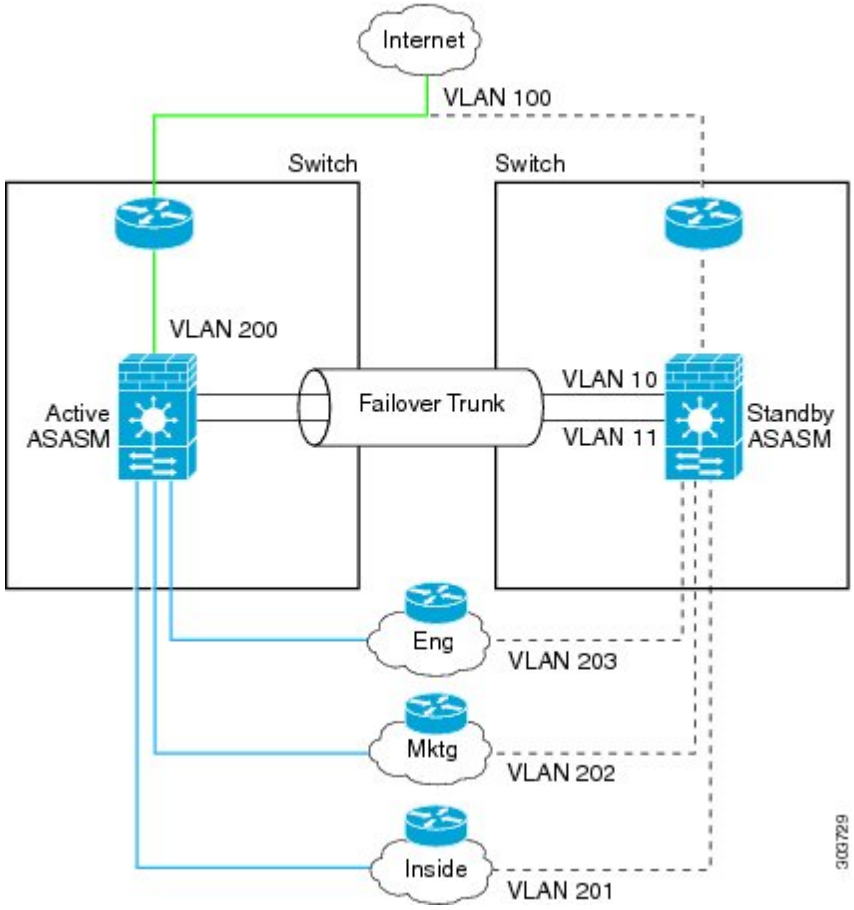
ASASM 間のフェールオーバー通信の信頼性を高めるために、2 台のスイッチ間に EtherChannel トランク ポートを設定して、フェールオーバーおよびステート VLAN を伝送することをお勧めします。

他の VLAN については、両方のスイッチがすべてのファイアウォール VLAN にアクセスでき、モニタ対象 VLAN が両方のスイッチ間で正常に hello パケットを渡すことができるようにします。

次の図は、スイッチと ASASM の一般的な冗長構成を示します。2 台のスイッチ間のトランクは、フェールオーバー ASASM VLAN（VLAN 10 と 11）を転送します。

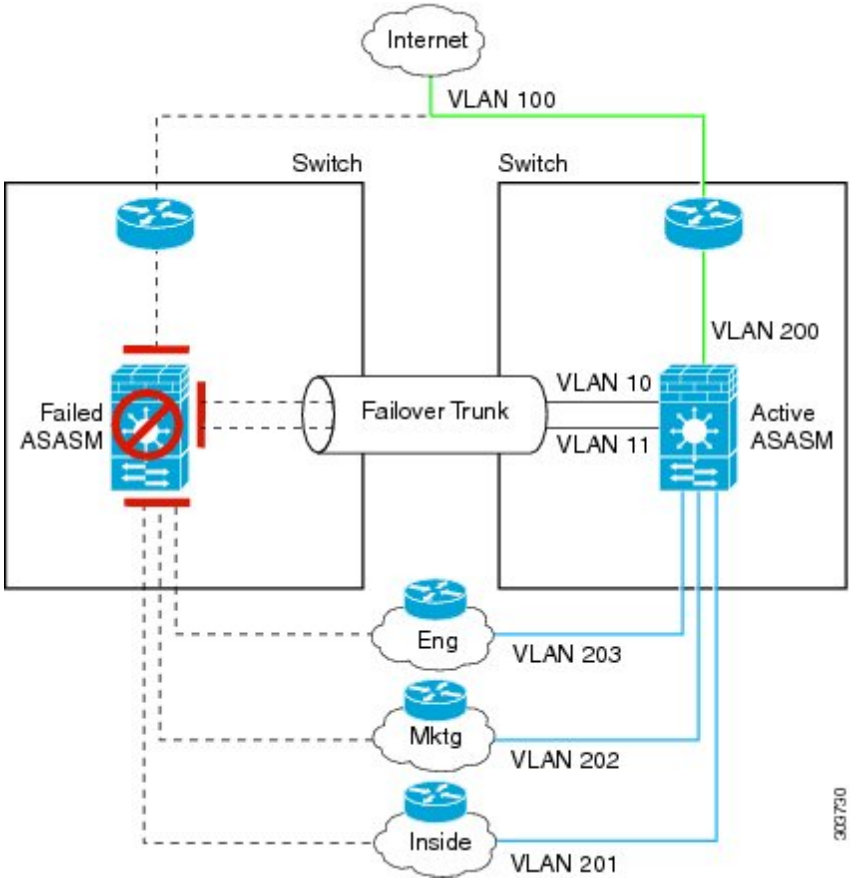
（注） ASASM のフェールオーバーはスイッチのフェールオーバーに依存しない独立した機能ですが、スイッチのフェールオーバーが発生した場合には、ASASM もそれに対応します。

図 *41* : 通常の動作



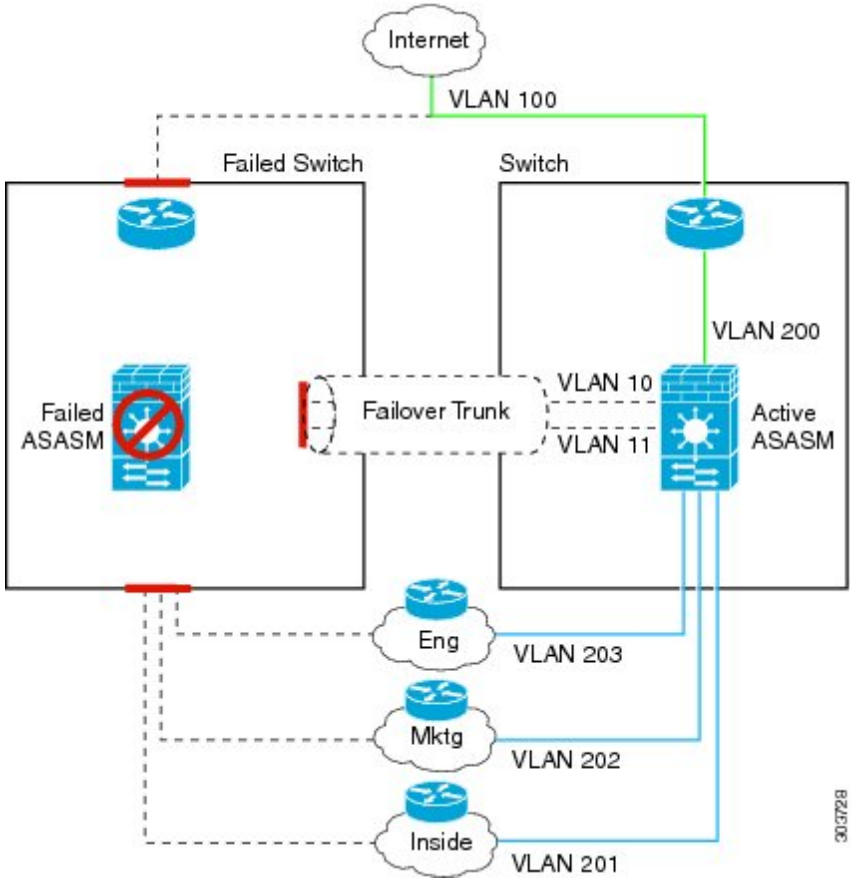
プライマリ ASASM に障害が発生すると、セカンダリ ASASM がアクティブになってファイアウォール VLAN を通過します。

図 *42 : ASASM* の障害



スイッチ全体に障害が発生し、ASASMにも障害が発生した場合（電源切断など）には、スイッチと ASASM の両方でセカンダリ ユニットへのフェールオーバーが実行されます。

図 *43 :* スイッチの障害



ステートレス フェールオーバーとステートフル フェールオーバー

ASA は、アクティブ/スタンバイ モードとアクティブ/アクティブ モードの両方に対して、ステートレスとステートフルの 2 種類のフェールオーバーをサポートします。

（注） クライアントレス SSL VPN の一部のコンフィギュレーション要素（ブックマークやカスタマイゼーションなど）はVPNフェールオーバーサブシステムを使用していますが、これはステートフル フェールオーバーの一部です。フェールオーバー ペアのメンバ間でこれらの要素を同期するには、ステートフルフェールオーバーを使用する必要があります。ステートレスフェールオーバーは、クライアントレス SSL VPN には推奨されません。

ステートレス フェールオーバー

フェールオーバーが行われると、アクティブ接続はすべてドロップされます。新しいアクティブ装置が引き継ぐ場合、クライアントは接続を再確立する必要があります。

（注） クライアントレス SSL VPN の一部のコンフィギュレーション要素（ブックマークやカスタマイゼーションなど）はVPNフェールオーバーサブシステムを使用していますが、これはステートフル フェールオーバーの一部です。フェールオーバー ペアのメンバ間でこれらの要素を同期するには、ステートフル フェールオーバーを使用する必要があります。ステートレス（標準）フェールオーバーは、クライアントレス SSL VPN には推奨できません。

Stateful Failover

ステートフル フェールオーバーが有効の場合、アクティブ装置は接続ごとのステート情報をスタンバイ装置に継続的に渡します。アクティブ/アクティブ フェールオーバーの場合は、アクティブとスタンバイのフェールオーバー グループ間でこれが行われます。フェールオーバーの発生後も、新しいアクティブ装置で同じ接続情報が利用できます。サポートされているエンドユーザのアプリケーションでは、同じ通信セッションを保持するために再接続する必要はありません。

サポートされる機能

ステートフル フェールオーバーでは、次のステート情報がスタンバイ ASAに渡されます。

- NAT 変換テーブル
- TCP 接続と UDP 接続、および状態。他のタイプの IP プロトコルおよび ICMP は、新しいパケットが到着したときに新しいアクティブユニットで確立されるため、アクティブ装置によって解析されません。
- HTTP 接続テーブル（HTTP 複製を有効にしない場合）。
- HTTP 接続状態（HTTP 複製が有効化されている場合）：デフォルトでは、ステートフル フェールオーバーが有効化されているときには、ASA はHTTPセッション情報を複製しません。HTTP レプリケーションを有効にすることをお勧めします。
- ARP テーブル
- レイヤ 2 ブリッジ テーブル（ブリッジ グループ用）
- ISAKMP および IPSec SA テーブル
- GTP PDP 接続データベース
- SIP シグナリング セッションとピンホール。
- ICMP 接続状態：ICMP 接続の複製は、個々のインターフェイスが非対称ルーティング グループに割り当てられている場合にだけイネーブルになります。
- スタティックおよびダイナミック ルーティングテーブル：ステートフル フェールオーバーはダイナミック ルーティング プロトコル（OSPF や EIGRP など）に参加するため、アクティブ装置上のダイナミック ルーティング プロトコルによる学習ルートが、スタンバイ装置のルーティング情報ベース（RIB）テーブルに維持されます。フェールオーバーイベントで、アクティブなセカンダリ ユニットには最初にプライマリ ユニットをミラーリン

グするルールがあるため、パケットは通常は最小限の中断でトラフィックに移動します。フェールオーバーの直後に、新しくアクティブになった装置で再コンバージェンス タイマーが開始されます。次に、RIBテーブルのエポック番号が増加します。再コンバージェンス中に、OSPFおよびEIGRPルートは新しいエポック番号で更新されます。タイマーが期限切れになると、失効したルートエントリ（エポック番号によって決定される）はテーブルから削除されます。これで、RIBには新しくアクティブになった装置での最新のルーティング プロトコル転送情報が含まれています。

（注） ルートは、アクティブ装置上のリンクアップまたはリンクダウンイベントの場合のみ同期されます。スタンバイ装置上でリンクがアップまたはダウンすると、アクティブ装置から送信されたダイナミック ルートが失われることがあります。これは正常な予期された動作です。

- DHCP サーバ：DHCP アドレス リースは複製されません。ただし、インターフェイスで設定されたDHCPサーバは、DHCPクライアントにアドレスを付与する前にアドレスが使用されていないことを確認するためにpingを送信するため、サービスに影響はありません。ステート情報は、DHCP リレーまたは DDNS とは関連性がありません。
- Cisco IP SoftPhone セッション：コール セッション ステート情報がスタンバイ装置に複製されるため、Cisco IP SoftPhone セッションの実行中にフェールオーバーが起こっても、コールは実行されたままです。コールが終了すると、IP SoftPhone クライアントは Cisco Call Manager との接続を失います。これは、CTIQBE ハングアップ メッセージのセッション情報がスタンバイ装置に存在しないために発生します。IP SoftPhoneクライアントでは、一定の時間内にCallManagerからの応答が受信されない場合、CallManagerに到達できないものと判断されて登録が解除されます。
- RA VPN：リモート アクセス VPN エンドユーザは、フェールオーバー後に VPN セッションを再認証または再接続する必要はありません。ただし、VPN 接続上で動作するアプリケーションは、フェールオーバープロセス中にパケットを失って、パケット損失から回復できない可能性があります。

サポートされない機能

ステートフル フェールオーバーでは、次のステート情報はスタンバイ ASAに渡されません。

- ユーザ認証（uauth）テーブル
- TCP ステート バイパス接続
- マルチキャスト ルーティング。
- ASA FirePOWER モジュールなどのモジュールのステート情報。
- 選択された次のクライアントレス SSL VPN 機能：
  - スマート トンネル

- ポート転送
- プラグイン
- Java アプレット
- IPv6 クライアントレスまたは Anyconnect セッション
- Citrix 認証（Citrix ユーザはフェールオーバー後に再認証が必要です）

フェールオーバーのトランスペアレント ファイアウォール モード ブリッジ グループ要件

ブリッジグループを使用する際に、フェールオーバーの特殊な考慮事項があります。

トランスペアレント モードアプライアンス、ASAv のブリッジグループ必須要件

アクティブ装置がスタンバイ装置にフェールオーバーするときに、スパニングツリープロトコル（STP）を実行している接続済みスイッチ ポートは、トポロジ変更を検出すると 30 ～ 50 秒間ブロッキング ステートに移行できます。ポートがブロッキング ステートである間のトラフィックの損失を回避するために、スイッチ ポート モードに応じて次の回避策のいずれかを設定できます。

- アクセス モード：スイッチで STP PortFast 機能をイネーブルにします。

```
interface interface_id
  spanning-tree portfast
```

PortFast 機能を設定すると、リンクアップと同時にポートが STP フォワーディング モードに遷移します。ポートは引き続き STP に参加しています。したがって、ポートがループの一部になる場合、最終的には STP ブロッキング モードに遷移します。

- トランク モード：EtherType アクセス ルールを使用して、ブリッジグループのメンバー インターフェイス上の ASA の BPDU をブロックします。

```
access-list id ethertype deny bpdu
access-group id in interface name1
access-group id in interface name2
```

BPDU をブロックすると、スイッチの STP はディセーブルになります。ネットワーク レイアウトで ASA を含むループを設定しないでください。

上記のオプションのどちらも使用できない場合は、フェールオーバー機能または STP の安定性に影響する、推奨度の低い次の回避策のいずれかを使用できます。

- インターフェイス モニタリングをディセーブルにします。

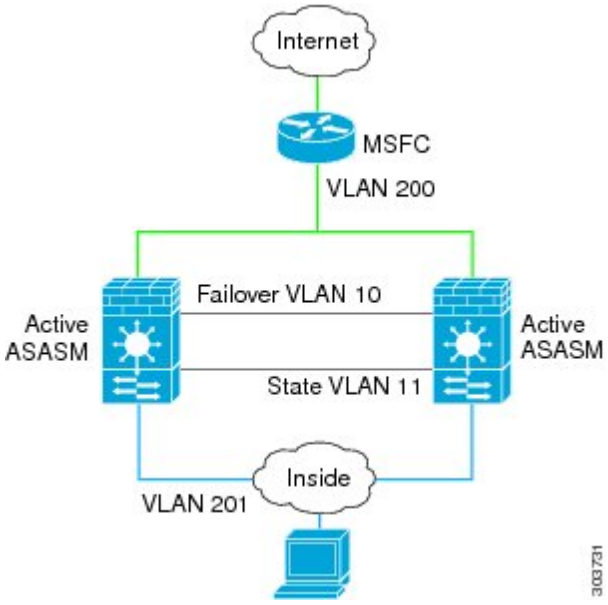
- ASA がフェールオーバーする前に、インターフェイスのホールド時間を STP が収束可能になる大きい値に増やします。
- STP がインターフェイスのホールド時間よりも速く収束するように、STP タイマーを減らします。

トランスペアレント モードASA サービス モジュールのブリッジグループ必須要件

ブリッジグループでのフェールオーバーの使用時にループを回避するには、BPDUの通過を許可し（デフォルト）、BPDU転送をサポートするスイッチ ソフトウェアを使用する必要があります。

両方のモジュールが互いの存在を検出する場合や、不正なフェールオーバー リンクなどによって、両方のモジュールが同時にアクティブになるときに、ループが発生することがあります。両方の ASASM が 2 つの同じ VLAN 間でパケットをブリッジングするので、ブリッジグループ メンバー間のパケットが両方の ASASM によって無限に複製され、ループが発生します。BPDU がタイミングよく交換された場合は、スパニングツリープロトコルによって、これらのループが遮断されます。ループを遮断するには、VLAN 200 と VLAN 201 間で送信される BPDU をブリッジングする必要があります。

図 *44 :* ブリッジグループ ループ



フェールオーバーのヘルス モニタ

ASAは、各装置について全体的なヘルスおよびインターフェイス ヘルスをモニタします。この項では、各装置の状態を判断するために、ASAがテストを実行する方法について説明します。

ユニットのヘルス モニタリング

ASAは、helloメッセージでフェールオーバー リンクをモニタして相手装置のヘルスを判断します。フェールオーバー リンクで3回連続してhelloメッセージを受信しなかったときは、フェールオーバー リンクを含む各データ インターフェイスでLANTESTメッセージを送信し、ピアが応答するかどうかを確認します。ASAが行うアクションは、相手装置からの応答によって決まります。次の可能なアクションを参照してください。

- ASAがフェールオーバー リンクで応答を受信した場合、フェールオーバーは行われません。
- ASAがフェールオーバー リンクで応答を受信せず、データ インターフェイスで応答を受信した場合、装置のフェールオーバーは行われません。フェールオーバー リンクが故障とマークされます。フェールオーバー リンクがダウンしている間、装置はスタンバイ装置にフェールオーバーできないため、できるだけ早くフェールオーバー リンクを復元する必要があります。
- ASAがどのインターフェイスでも応答を受信しなかった場合、スタンバイ装置がアクティブ モードに切り替わり、相手装置を故障に分類します。

インターフェイス モニタリング

最大1025のインターフェイスを監視できます（マルチコンテキスト モードでは、すべてのコンテキスト間で分割）。重要なインターフェイスをモニタする必要があります。たとえば、マルチコンテキスト モードでは、共有インターフェイスを監視するように1つのコンテキストを設定する場合があります（インターフェイスが共有されているため、すべてのコンテキストがそのモニタリングによる利点を得ることができます）。

ユニットは、モニタ対象のインターフェイス上で15秒間helloメッセージを受信しなかった場合に（デフォルト）、インターフェイス テストを実行します。（この時間を変更するには、**failover polltime interface** コマンド、アクティブ/アクティブ フェールオーバーの場合は **polltime interface** コマンドを参照してください）1つのインターフェイスに対するインターフェイス テストのいずれかが失敗したものの、他のユニット上のこの同じインターフェイスが正常にトラフィックを渡し続けている場合は、そのインターフェイスに障害があるものと見なされ、ASAはテストの実行を停止します。

障害が発生したインターフェイスの数に対して定義したしきい値が満たされ（**failover interface-policy** コマンド、またはアクティブ/アクティブ フェールオーバーの場合は **interface-policy** コマンドを参照）、さらに、アクティブ ユニットでスタンバイ装置よりも多くの障害が発生した場合は、フェールオーバーが発生します。両方のユニット上のインターフェイスに障害が発生した場合は、両方のインターフェイスが「未知」状態になり、フェールオーバー インターフェイス ポリシーで定義されているフェールオーバー限界値に向けてのカウントは行われません。

インターフェイスは、何らかのトラフィックを受信すると、再度動作状態になります。故障したASAは、インターフェイス障害しきい値が満たされなくなった場合、スタンバイ モードに戻ります。

ASA FirePOWER モジュールがある場合、ASA はバックプレーン インターフェイスを介してモジュールの健全性もモニタします。モジュールの障害は装置の障害と見なされ、フェールオーバーがトリガーされます。この設定は設定可能です。

インターフェイスに IPv4 および IPv6 アドレスが設定されている場合、ASAは IPv4 を使用してヘルス モニタリングを実行します。インターフェイスに IPv6 アドレスだけが設定されている場合、ASAは ARP ではなく IPv6 ネイバー探索を使用してヘルス モニタリング テストを実行します。ブロードキャスト ping テストの場合、ASAは IPv6 全ノードアドレス（FE02::1）を使用します。

（注） 障害が発生した装置が回復せず、実際には障害は発生していないと考えられる場合は、**failover reset** コマンドを使用して状態をリセットできます。ただし、フェールオーバー条件が継続している場合、装置は再び障害状態になります。

インターフェイス テスト

ASAでは、次のインターフェイス テストが使用されます。各テストの時間はデフォルトで約 1.5 秒、またはフェールオーバー インターフェイスの保留時間の 1/16 です（**failover polltime interface** command を参照するか、またはアクティブ/アクティブ フェールオーバーの場合は **interface-policy** コマンドを参照）。

1. リンクアップ/ダウンテスト：インターフェイス ステータスのテストです。リンクアップ/ダウンテストでインターフェイスがダウンしていることが示された場合、ASAは障害が発生し、テストが停止したと見なします。ステータスがアップの場合、ASAはネットワークアクティビティを実行します。

2. ネットワーク動作のテスト：ネットワークの受信動作のテストです。テストの開始時に、各装置はインターフェイスの受信パケットカウントをリセットします。テスト中にユニットが適切なパケットを受信すると、すぐにインターフェイスは正常に動作していると見なされます。両方の装置がトラフィックを受信した場合、テストは停止します。どちらか一方のユニットだけがトラフィックを受信している場合は、トラフィックを受信していないユニットのインターフェイスで障害が発生していると見なされ、テストは停止します。どちらのユニットもトラフィックを受信していない場合は、ASA は ARP テストを開始します。

3. ARP テスト：ARP が正しく応答するかどうかをテストします。各ユニットは、ARP テーブル内の最新のエントリの IP アドレスに対して単一の ARP 要求を送信します。ユニットがテスト中に ARP 応答またはその他のネットワーク トラフィックを受信する場合、インターフェイスは動作していると見なされます。ユニットが ARP 応答を受信しない場合、ASAは、ARP テーブル内の「次の」エントリの IP アドレスに対して単一の ARP 要求を送信します。ユニットがテスト中に ARP 応答またはその他のネットワーク トラフィックを受信する場合、インターフェイスは動作していると見なされます。両方のユニットがトラフィックを受信した場合、テストは停止します。どちらか一方のユニットだけがトラフィックを受信している場合は、トラフィックを受信していないユニットのインターフェイスで障害が発生していると見なされ、テストは停止します。どちらのユニットもトラフィックを受信していない場合は、ASA はブートストラップ ping テストを開始します。

4. ブロードキャストPingテスト：ping応答が正しいかどうかをテストします。各ユニットがブロードキャストpingを送信し、受信したすべてのパケットをカウントします。パケットはテスト中にパケットを受信すると、インターフェイスは正常に動作していると見なされます。両方のユニットがトラフィックを受信した場合、テストは停止します。どちらか一方のユニットだけがトラフィックを受信している場合は、トラフィックを受信していないユニットのインターフェイスで障害が発生していると見なされ、テストは停止します。どちらのユニットもトラフィックを受信しない場合、ARPテストを使用してテストが再開されます。両方の装置が ARP およびブロードキャスト ping テストからトラフィックを受信し続けない場合、これらのテストは永久に実行し続けます。

Interface Status

モニタ対象のインターフェイスには、次のステータスがあります。

- Unknown：初期ステータスです。このステータスは、ステータスを特定できないことを意味する場合もあります。
- Normal：インターフェイスはトラフィックを受信しています。
- Testing：ポーリング 5 回の間、インターフェイスで hello メッセージが検出されていません。
- Link Down：インターフェイスまたは VLAN は管理のためにダウンしています。
- No Link：インターフェイスの物理リンクがダウンしています。
- Failed：インターフェイスではトラフィックを受信していませんが、ピア インターフェイスではトラフィックを検出しています。

フェールオーバー 時間

次の表に、最小、デフォルト、最大フェールオーバー時間を示します。

（注） CLI または ASDM を使用して手動でフェールオーバーした場合、もしくは ASA をリロードした場合、フェールオーバーはすぐに開始され、次に示すタイマーの影響は受けません。

表 *10 : ASA*

フェールオーバー条件	最小ハードウェア	デフォルト	最大
アクティブ装置で電源断が生じる、または通常の動作が停止する。	800 ミリ秒	15 秒	45 秒
アクティブ ユニット メインボード インターフェイスリンクがダウンする。	500 ミリ秒	5 秒	15 秒

フェールオーバー条件	最小ハードウェア	デフォルト	最大
アクティブ装置の 4GE モジュール インターフェイス リンクがダウンする。	2 秒	5 秒	15 秒
アクティブ ユニット Firepower モジュールは失敗する。	2 秒	2 秒	2 秒
アクティブ装置のインターフェイスは実行されているが、接続の問題によりインターフェイス テストを行っている。	5 秒	25 秒	75 秒

設定の同期

フェールオーバーには、さまざまなタイプのコンフィギュレーション同期があります。

コンフィギュレーションの複製の実行

コンフィギュレーションの複製は、フェールオーバーペアの一方または両方のデバイスのブート時に実行されます。

アクティブ/スタンバイ フェールオーバーでは、コンフィギュレーションは常に、アクティブ装置からスタンバイ装置に同期化されます。

アクティブ/アクティブ フェールオーバーでは、起動ユニットのプライマリまたはセカンダリ指定に関係なく、2番目に起動したユニットは、最初に起動したユニットから実行コンフィギュレーションを取得します。両方のユニットの起動後、システム実行スペースに入力されたコマンドは、フェールオーバー グループ 1 がアクティブ状態であるユニットから複製されます。

スタンバイ/セカンドユニットが初期スタートアップを完了すると、実行コンフィギュレーションを削除し（アクティブ ユニットとの通信に必要な **failover** コマンドを除く）、アクティブ ユニットはコンフィギュレーション全体をスタンバイ/セカンド ユニットに送信します。複製が開始されると、アクティブ ユニットの ASA コンソールに「Beginning configuration replication: Sending to mate,」というメッセージが表示され、完了すると ASA に「End Configuration Replication to mate.」というメッセージが表示されます。コンフィギュレーションのサイズによって、複製には数秒から数分かかります。

コンフィギュレーションを受信する装置の場合、コンフィギュレーションは実行メモリにだけ存在します。コンフィギュレーションの変更の保存 （50 ページ）に従ってコンフィギュレーションをフラッシュ メモリに保存する必要があります。たとえば、アクティブ/アクティブ フェールオーバーでは、フェールオーバー グループ 1 がアクティブ状態であるユニット上のシステム実行スペースに **write memory all** コマンドを入力します。コマンドはピア装置に複製され、コンフィギュレーションがフラッシュ メモリに書き込まれます。

（注） 複製中、コンフィギュレーションを送信しているユニット上に入力されたコマンドは、ピアユニットに正常に複製されず、コンフィギュレーションを受信するユニット上に入力されたコマンドは、受信したコンフィギュレーションによって上書きできます。コンフィギュレーションの複製処理中には、フェールオーバーペアのどちらの装置にもコマンドを入力しないでください。

（注） **crypto ca server** コマンドおよび関連するサブコマンドはフェールオーバーをサポートしません。**no crypto ca server** コマンドを使用して削除する必要があります。

ファイル複製

コンフィギュレーションの同期は次のファイルと構成コンポーネントを複製しません。したがって、これらのファイルが一致するように手動でコピーする必要があります。

- AnyConnect イメージ
- CSD イメージ
- AnyConnect プロファイル

  ASA では、フラッシュ ファイル システムに保存されたファイルではなく、cache:/stc/profiles に保存された AnyConnect クライアント ファイルのキャッシュ済みファイルが使用されます。AnyConnect クライアント プロファイルをスタンバイ装置に複製するには、次のいずれかを実行します。

  - アクティブ装置で **write standby** コマンドを入力します。
  - アクティブ装置でプロファイルを再適用します。
  - スタンバイ装置をリロードします。

- ローカル認証局（CA）
- ASA イメージ
- ASDM イメージ

コマンド複製

起動した後、アクティブ装置で入力したコマンドはただちにスタンバイ装置に複製されます。コマンドを複製する場合、アクティブ コンフィギュレーションをフラッシュ メモリに保存する必要はありません。

アクティブ/アクティブ フェールオーバーでは、システム実行スペースに入力したコマンドは、フェールオーバー グループ 1 がアクティブ状態である装置から複製されます。

コマンドの複製を行うのに適切な装置上でコマンドを入力しなかった場合は、コンフィギュレーションは同期されません。この変更内容は、次回に初期コンフィギュレーション同期が行われると失われることがあります。

スタンバイ ASA に複製されるコマンドは、次のとおりです。

- すべてのコンフィギュレーション コマンド（**mode**、**firewall**、および **failover lan unit** を除く）
- **copy running-config startup-config**
- **delete**
- **mkdir**
- **rename**
- **rmdir**
- **write memory**

スタンバイ ASA に複製されないコマンドは、次のとおりです。

- すべての形式の **copy** コマンド（**copy running-config startup-config** を除く）
- すべての形式の **write** コマンド（**write memory** を除く）
- **debug**
- **failover lan unit**
- **firewall**
- **show**
- **terminal pager** および **pager**

アクティブ/スタンバイ フェールオーバーについて

アクティブ/スタンバイ フェールオーバーでは、障害が発生した装置の機能を、スタンバイ ASAに引き継ぐことができます。アクティブ装置に障害が発生した場合、スタンバイ装置がアクティブ装置になります。

（注） マルチ コンテキスト モードでは、ASA は装置全体（すべてのコンテキストを含む）のフェールオーバーを行いますが、各コンテキストを個別にフェールオーバーすることはできません。

プライマリ/セカンダリ ロールとアクティブ/スタンバイ ステータス

フェールオーバーペアの2つのユニットの主な相違点は、どちらのユニットがアクティブでどちらのユニットがスタンバイであるか、つまりどちらの IP アドレスを使用するか、およびどちらのユニットがアクティブにトラフィックを渡すかということに関連します。

しかし、プライマリである装置（コンフィギュレーションで指定）とセカンダリである装置との間で、いくつかの相違点があります。

- 両方の装置が同時にスタートアップした場合（さらに動作ヘルスが等しい場合）、プライマリ装置が常にアクティブ装置になります。
- プライマリ ユニットの MAC アドレスは常に、アクティブ IP アドレスと結び付けられています。このルールの例外は、セカンダリ ユニットがアクティブであり、フェールオーバー リンク経由でプライマリ ユニットの MAC アドレスを取得できない場合に発生します。この場合、セカンダリ装置の MAC アドレスが使用されます。

起動時のアクティブ装置の判別

アクティブ装置は、次の条件で判別されます。

- 装置がブートされ、ピアがすでにアクティブとして動作中であることを検出すると、その装置はスタンバイ装置になります。
- 装置がブートされてピアを検出できないと、その装置はアクティブ装置になります。
- 両方の装置が同時にブートされた場合は、プライマリ装置がアクティブ装置になり、セカンダリ装置がスタンバイ装置になります。

フェールオーバー イベント

アクティブ/スタンバイ フェールオーバーでは、フェールオーバーはユニットごとに行われます。マルチコンテキストモードで動作中のシステムでも、個々のコンテキストまたはコンテキストのグループをフェールオーバーすることはできません。

次の表に、各障害イベントに対するフェールオーバーアクションを示します。この表には、各フェールオーバー イベントに対して、フェールオーバー ポリシー（フェールオーバーまたはフェールオーバーなし）、アクティブ装置が行うアクション、スタンバイ装置が行うアクション、およびフェールオーバー条件とアクションに関する特別な注意事項を示します。

表 *11* : フェールオーバー イベント

障害の状況	ポリシー	アクティブグループのアクション	スタンバイグループのアクション	注記
アクティブ装置が故障（電源またはハードウェア）	フェールオーバー	n/a	アクティブになる アクティブに故障とマークする	モニタ対象インターフェイスまたはフェールオーバー リンクで hello メッセージは受信されません。
以前にアクティブであった装置の復旧	フェールオーバーなし	スタンバイになる	動作なし	なし。

障害の状況	ポリシー	アクティブグループのアクション	スタンバイグループのアクション	注記
スタンバイ装置が故障（電源またはハードウェア）	フェールオーバーなし	スタンバイに故障とマークする	n/a	スタンバイ装置が故障とマークされている場合、インターフェイス障害しきい値を超えても、アクティブ装置はフェールオーバーを行いません。
動作中にフェールオーバーリンクに障害が発生した	フェールオーバーなし	フェールオーバーリンクに故障とマークする	フェールオーバーリンクに故障とマークする	フェールオーバーリンクがダウンしている間、装置はスタンバイ装置にフェールオーバーできないため、できるだけ早くフェールオーバーリンクを復元する必要があります。
スタートアップ時にフェールオーバーリンクに障害が発生した	フェールオーバーなし	フェールオーバーリンクに故障とマークする	アクティブになる	スタートアップ時にフェールオーバーリンクがダウンしていると、両方の装置がアクティブになります。
ステートリンクの障害	フェールオーバーなし	動作なし	動作なし	ステート情報が古くなり、フェールオーバーが発生するとセッションが終了します。
アクティブ装置におけるしきい値を超えたインターフェイス障害	フェールオーバー	アクティブに故障とマークする	アクティブになる	なし。
スタンバイ装置におけるしきい値を超えたインターフェイス障害	フェールオーバーなし	動作なし	スタンバイに故障とマークする	スタンバイ装置が故障とマークされている場合、インターフェイス障害しきい値を超えても、アクティブ装置はフェールオーバーを行いません。

アクティブ/アクティブ フェールオーバーの概要

この項では、アクティブ/アクティブ フェールオーバーについて説明します。

アクティブ/アクティブ フェールオーバーの概要

アクティブ/アクティブ フェールオーバー コンフィギュレーションでは、両方の ASA がネットワーク トラフィックを渡すことができます。アクティブ/アクティブ フェールオーバーは、マルチ コンテキスト モードの ASA でのみ使用できます。アクティブ/アクティブ フェールオーバーでは、ASA のセキュリティ コンテキストを 2 つまでのフェールオーバー グループに分割します。

フェールオーバー グループは、1 つまたは複数のセキュリティ コンテキストの論理グループにすぎません。フェールオーバー グループをプライマリ ASA でアクティブに割り当て、フェールオーバー グループ 2 をセカンデリ ASA でアクティブに割り当てることができます。フェールオーバーが行われる場合は、フェールオーバー グループ レベルで行われます。たとえば、インターフェイス障害パターンに応じて、フェールオーバー グループ 1 をセカンデリ ASA にフェールオーバーし、続いてフェールオーバー グループ 2 をプライマリ ASA にフェールオーバーすることができます。このイベントは、プライマリ ASA でフェールオーバー グループ 1 のインターフェイスがダウンしたがセカンデリではアップしており、セカンデリ ASA でフェールオーバー グループ 2 のインターフェイスがダウンしたがプライマリ ASA ではアップしている場合に発生する可能性があります。

管理コンテキストは、常にフェールオーバー グループ 1 のメンバです。未割り当てセキュリティ コンテキストもまた、デフォルトでフェールオーバー グループ 1 のメンバです。アクティブ/アクティブ フェールオーバーが必要であるが複数コンテキストは必要ない場合、最もシンプルな設定は他のコンテキストを 1 つ追加し、それをフェールオーバー グループ 2 に割り当てることです。

（注） アクティブ/アクティブ フェールオーバーを構成する場合は、両方の装置の合計トラフィックが各装置の容量以内になるようにしてください。

（注） 必要に応じて両方のフェールオーバー グループを 1 つの ASA に割り当てることもできますが、この場合、アクティブな ASA を 2 つ持つというメリットはありません。

フェールオーバー グループのプライマリ/セカンデリ ロールとアクティブ/スタンバイ ステータス

アクティブ/スタンバイ フェールオーバーと同様、アクティブ/アクティブ フェールオーバー ペアの 1 つの装置がプライマリ ユニットに指定され、もう 1 つの装置がセカンダリ ユニットに指定されます。アクティブ/スタンバイ フェールオーバーの場合とは異なり、両方の装置が同時に起動された場合、この指定ではどちらの装置がアクティブになるか指示しません。代わりに、プライマリまたはセカンダリの指定時に、次の 2 つの点を判定します。

- ペアが同時に起動したときに、プライマリ装置が実行コンフィギュレーションを提供します。
- コンフィギュレーションの各フェールオーバー グループは、プライマリまたはセカンダリ装置プリファレンスが設定されます。プリエンプションで使用すると、このプレファレンスはフェールオーバー グループが起動後に正しいユニットで実行されるようにします。プリエンプションがない場合、両方のグループは最初に起動したユニットで動作します。

起動時のフェールオーバー グループのアクティブ装置の決定

フェールオーバー グループがアクティブになる装置は、次のように決定されます。

- ピア装置が使用できないときに装置がブートされると、両方のフェールオーバー グループがピア装置でアクティブになります。
- ピア装置がアクティブ（両方のフェールオーバー グループがアクティブ状態）の場合に装置がブートされると、フェールオーバー グループは、アクティブ装置でアクティブ状態のままになります。これは、次のいずれかの状態になるまで、フェールオーバー グループのプライマリ プリファレンスまたはセカンダリ プリファレンスには関係ありません。
  - フェールオーバーが発生した。
  - 手動でフェールオーバーを強制実行した。
  - フェールオーバー グループにプリエンプションを設定した。この設定により、優先する装置が使用可能になると、フェールオーバー グループはその装置上で自動的にアクティブになります。

フェールオーバー イベント

アクティブ/アクティブ フェールオーバー コンフィギュレーションでは、フェールオーバーは、システムごとに行うのではなく、フェールオーバー グループごとに行われます。たとえば、プライマリ装置で両方のフェールオーバー グループをアクティブと指定し、フェールオーバー グループ 1 が故障すると、フェールオーバー グループ 2 はプライマリ装置でアクティブのままですが、フェールオーバー グループ 1 はセカンダリ装置でアクティブになります。

フェールオーバー グループには複数のコンテキストを含めることができ、また各コンテキストには複数のインターフェイスを含めることができるので、1 つのコンテキストのインターフェイスがすべて故障しても、そのコンテキストに関連するフェールオーバー グループが故障と判断されない可能性があります。

次の表に、各障害イベントに対するフェールオーバーアクションを示します。各障害イベントに対して、ポリシー（フェールオーバーまたはフェールオーバーなし）、アクティブ フェールオーバー グループのアクション、およびスタンバイ フェールオーバー グループのアクションを示します。

表 *12 :* フェールオーバー イベント

障害の状況	ポリシー	アクティブグループのアクション	スタンバイグループのアクション	注記
装置で電源断またはソフトウェア障害が発生した	フェールオーバー	スタンバイになり、故障とマークする	アクティブになる アクティブに故障とマークする	フェールオーバーペアの装置が故障すると、その装置のアクティブ フェールオーバー グループはすべて故障とマークされ、ピア装置のフェールオーバー グループがアクティブになります。
アクティブ フェールオーバー グループにおけるしきい値を超えたインターフェイス障害	フェールオーバー	アクティブ グループに故障とマークする	アクティブになる	なし。
スタンバイ フェールオーバー グループにおけるしきい値を超えたインターフェイス障害	フェールオーバーなし	動作なし	スタンバイ グループに故障とマークする	スタンバイ フェールオーバー グループが故障とマークされている場合、インターフェイス フェールオーバー障害しきい値を超えても、アクティブ フェールオーバー グループはフェールオーバーを行いません。
以前にアクティブであったフェールオーバー グループの復旧	フェールオーバーなし	動作なし	動作なし	フェールオーバー グループのプリエンプションが設定されている場合を除き、フェールオーバー グループは現在の装置でアクティブのままです。
スタートアップ時にフェールオーバー リンクに障害が発生した	フェールオーバーなし	アクティブになる	アクティブになる	スタートアップ時にフェールオーバー リンクがダウンしていると、両方の装置の両方のフェールオーバー グループがアクティブになります。

障害の状況	ポリシー	アクティブグループのアクション	スタンバイグループのアクション	注記
ステートリンクの障害	フェールオーバーなし	動作なし	動作なし	ステート情報が古くなり、フェールオーバーが発生するとセッションが終了します。
動作中にフェールオーバーリンクに障害が発生した	フェールオーバーなし	n/a	n/a	各装置で、フェールオーバーリンクが故障とマークされます。フェールオーバーリンクがダウンしている間、装置はスタンバイ装置にフェールオーバーできないため、できるだけ早くフェールオーバーリンクを復元する必要があります。

フェールオーバーのライセンス

フェールオーバーユニットは、各ユニット上で同一のライセンスを必要としません。両方のユニット上にライセンスがある場合、これらのライセンスは単一の実行フェールオーバークラスタ ライセンスに結合されます。このルールには、いくつかの例外があります。フェールオーバーの正確なライセンス要件については、次の表を参照してください。

モデル	ライセンス要件
ASA 5506-X および ASA 5506W-X	• アクティブ/スタンバイ：Security Plus ライセンス。 • アクティブ/アクティブ：サポートなし。 （注） 各ユニットに同じ暗号化ライセンスが必要です。

モデル	ライセンス要件
ASA 5512-X ～ ASA 5555-X	• ASA 5512：Security Plus ライセンス。 • その他のモデル：基本ライセンス。 （注） • 各ユニットに同じ暗号化ライセンスが必要です。 • マルチ コンテキスト モードでは、各ユニットに同じ AnyConnect Apex ライセンスが必要です。 • 各ユニットに同じ IPS モジュール ライセンスが必要です。両方の装置の IPS 側で IPS シグニチャ サブスクリプションも必要です。次のガイドラインを参照してください。 • IPS シグニチャ サブスクリプションを購入するには、IPS がプリインストールされた ASA が必要です（ASA5525-IPS-K9 のように、製品番号に「IPS」が含まれている必要があります）。IPS 以外の製品番号の ASA に IPS シグニチャ サブスクリプションを購入することはできません。 • 両方の装置に IPS シグニチャ サブスクリプションが必要です。このサブスクリプションは ASA ライセンスではないため、フェールオーバー間で共有されません。 • IPS シグニチャ サブスクリプションには、装置ごとに個別の IPS モジュール ライセンスが必要です。他の ASA のライセンスと同様に、IPS モジュール ライセンスも技術的にはフェールオーバー クラスタ ライセンスで共有されます。しかし、IPS シグニチャ サブスクリプションの要件によって、装置ごとに個別の IPS モジュール ライセンスを購入する必要があります。
ASAv	ASAv のフェールオーバー ライセンス （138 ページ）を参照してください。

モデル	ライセンス要件
Firepower 9300	Firepower 9300 シャーシ の ASA のフェールオーバー ライセンス （138 ページ）を参照してください。
他のすべてのモデル	基本ライセンスまたは標準ライセンス。 （注） • 各ユニットに同じ暗号化ライセンスが必要です。 • マルチ コンテキスト モードでは、各ユニットに同じ AnyConnect Apex ライセンスが必要です。

（注） 有効な永続キーが必要です。まれに、PAK 認証キーを削除できることもあります。キーがすべて 0 の場合は、フェールオーバーを有効化するには有効な認証キーを再インストールする必要があります。

フェールオーバーのガイドライン

コンテキスト モード

- アクティブ/アクティブ モードは、マルチ コンテキスト モードでのみサポートされます。
- マルチ コンテキスト モードでは、特に注記がない限り、手順はすべてシステム実行スペースで実行します。
- ステートフル フェールオーバーは、マルチ コンテキスト モードの AnyConnect 接続ではサポートされません。

サポート モデル

- ASA 5506W-X：内部 GigabitEthernet 1/9 インターフェイスのインターフェイス モニタリングを無効にする必要があります。これらのインターフェイスは、デフォルトのインターフェイス モニタリング チェックを実行するために通信することができないため、予期されたインターフェイス通信の障害により、スイッチがアクティブからスタンバイに切り替えられ、元に戻ります。
- Firepower 9300：シャーシ間フェールオーバーを使用して最良の冗長性を確保することを推奨します。
- Microsoft Azure や Amazon Web Services などのパブリック クラウド ネットワーク上の ASAv では、レイヤ 2 接続が必要なため、フェールオーバーはサポートされません。

- ASA FirePOWER モジュールはフェールオーバーを直接サポートしていません。ASA がフェールオーバーすると、既存の ASA FirePOWER フローは新しい ASA に転送されます。新しい ASA の ASA FirePOWER モジュールが、その転送の時点からトラフィックの検査を開始します。古いインスペクションのステートは転送されません。

  フェールオーバーの動作の整合性を保つために、ハイアベイラビリティな ASA ペアの ASA FirePOWER モジュールで一貫したポリシーを保持する必要があります。

  （注） ASA FirePOWER モジュールを設定する前に、フェールオーバーペアを作成します。モジュールが両方のデバイスにすでに設定されている場合は、フェールオーバーペアを作成する前にスタンバイデバイスのインターフェイスの設定をクリアします。スタンバイ デバイスの CLI から、 **clear configure interface** コマンドを入力します。

ハイ アベイラビリティのための ASAv フェールオーバー

ASAv を使用してフェールオーバー ペアを作成する場合は、データ インターフェイスを各 ASAv に同じ順序で追加する必要があります。完全に同じインターフェイスが異なる順序で各 ASAv に追加されると、ASAv コンソールにエラーが表示される可能性があります。また、フェールオーバー機能にも影響が出ることがあります。

その他のガイドライン

- アクティブ装置がスタンバイ装置にフェールオーバーするときに、スパニングツリープロトコル（STP）を実行している接続済みスイッチ ポートは、トポロジ変更を検出すると 30 ～ 50 秒間ブロッキング ステートに移行できます。ポートがブロッキング ステートである間のトラフィック損失を防ぐには、スイッチで STP PortFast 機能を有効にします。

  interface *interface_id* **spanning-tree portfast**

  この回避策は、ルーテッド モードおよびブリッジ グループ インターフェイスの両方に接続されているスイッチに適用されます。PortFast 機能を設定すると、リンクアップと同時にポートが STP フォワーディング モードに遷移します。ポートは引き続き STP に参加しています。したがって、ポートがループの一部になる場合、最終的には STP ブロッキング モードに遷移します。

- ローカル CA サーバが設定されている場合、フェールオーバーを有効にできません。CA コンフィギュレーションを削除するには、**no crypto ca server** コマンドを使用します。

- ASA フェールオーバーペアに接続されたスイッチ上でポートセキュリティを設定すると、フェールオーバーイベントが発生したときに通信の問題が起きることがあります。この問題は、あるセキュア ポートで設定または学習されたセキュア MAC アドレスが別のセキュア ポートに移動し、スイッチのポート セキュリティ機能によって違反フラグが付けられた場合に発生します。

- すべてのコンテキストにわたり、1台の装置の最大1025のインターフェイスをモニタできます。
- アクティブ/スタンバイ フェールオーバーと VPN IPsec トンネルの場合、SNMP を使用して VPN トンネル上でアクティブ ユニットとスタンバイ ユニットの両方をモニタすることはできません。スタンバイ ユニットにはアクティブ VPN トンネルがないため、NMS に向けられたトラフィックはドロップされます。代わりに暗号化付き SNMPv3 を使用すれば、IPsec トンネルが不要になります。
- アクティブ/アクティブ フェールオーバーでは、同じコンテキスト内の2つのインターフェイスを同じ ASR グループ内で設定することはできません。
- アクティブ/アクティブ フェールオーバーでは、最大 2 つのフェールオーバー グループを定義できます。
- アクティブ/アクティブ フェールオーバーでフェールオーバー グループを削除する場合は、フェールオーバー グループ 1 を最後に削除する必要があります。フェールオーバー グループ1には常に管理コンテキストが含まれます。フェールオーバー グループに割り当てられていないコンテキストはすべて、デフォルトでフェールオーバー グループ1になります。コンテキストが明示的に割り当てられているフェールオーバー グループは削除できません。

フェールオーバーのデフォルト

デフォルトでは、フェールオーバー ポリシーは次の事項が含まれます。

- ステートフル フェールオーバーでの HTTP 複製は行われません。
- 単一のインターフェイス障害でフェールオーバーが行われます。
- インターフェイスのポーリング時間は 5 秒です。
- インターフェイスのホールド時間は 25 秒です。
- 装置のポーリング時間は 1 秒です。
- 装置のホールド時間は 15 秒です。
- 仮想MACアドレスはマルチコンテキストモードで無効化されていますが、ASASMでは、デフォルトで有効になっています。
- すべての物理インターフェイスをモニタリングします。ASASM では、すべての VLAN インターフェイスをモニタリングします。

アクティブ/スタンバイ フェールオーバーの設定

アクティブ/スタンバイ フェールオーバーを設定するには、プライマリ装置とセカンデリ装置の両方で基本的なフェールオーバー設定を構成します。その他すべての設定をプライマリ装置でのみ行った後、セカンデリ装置に設定を同期させます。

アクティブ/スタンバイ フェールオーバーのプライマリ装置の設定

この項の手順に従って、アクティブ/スタンバイ フェールオーバー構成のプライマリを設定します。この手順では、プライマリ装置でフェールオーバーをイネーブルにするために必要な最小のコンフィギュレーションが用意されています。

始める前に

- フェールオーバー リンクとステート リンクを除くすべてのインターフェイスのスタンバイ IP アドレスを設定することを推奨します。
- フェールオーバー リンクおよびステート リンクに **nameif** を設定しないでください。
- マルチ コンテキスト モードでは、システム実行スペースで次の手順を実行します。コンテキストからシステム実行スペースに切り替えるには、**changeto system** コマンドを入力します。

手順

ステップ 1 この装置をプライマリ装置に指定します。

failover lan unit primary

ステップ 2 フェールオーバー リンクとして使用するインターフェイスを指定します。

failover lan interface *if_name interface_id*

例：

```
ciscoasa(config)# failover lan interface folink gigabitethernet0/3
```

このインターフェイスは、他の目的には使用できません（オプションのステート リンクは除く）。

if_name 引数は、インターフェイスに名前を割り当てます。

interface_id 引数には、データ物理インターフェイス、サブインターフェイス、冗長インターフェイス、またはEtherChannelインターフェイスIDを指定できます。ASASMでは、*interface_id* は VLAN ID です。Firepower 9300 では、任意のデータタイプ インターフェイスを使用できます。

ステップ 3 アクティブ IP アドレスとスタンバイ IP アドレスをフェールオーバー リンクに割り当てます。

failover interface ip *failover_if_name* {*ip_address mask* | *ipv6_address* / *prefix*} **standby** *ip_address*

例：

```
ciscoasa(config)# failover interface ip folink 172.27.48.1 255.255.255.0 standby
172.27.48.2
```

または：

```
ciscoasa(config)# failover interface ip folink 2001:a0a:b00::a0a:b70/64 standby
2001:a0a:b00::a0a:b71
```

このアドレスは未使用のサブネット上になければなりません。169.254.0.0/16 と fd00:0:0:*::/64 は内部的に使用されるサブネットであり、フェールオーバー リンクやステート リンクに使用することはできません。

スタンバイ IP アドレスは、アクティブ IP アドレスと同じサブネットである必要があります。

ステップ 4 フェールオーバー リンクをイネーブルにします。

interface *failover_interface_id*

no shutdown

例：

```
ciscoasa(config)# interface gigabitethernet 0/3
ciscoasa(config-if)# no shutdown
```

ステップ 5 （オプション）ステート リンクとして使用するインターフェイスを指定します。

failover link *if_name interface_id*

例：

```
ciscoasa(config)# failover link folink gigabitethernet0/3
```

フェールオーバー リンクをステート リンクと共有することができます。

if_name 引数は、インターフェイスに名前を割り当てます。

interface_id 引数には、物理インターフェイス、サブインターフェイス、冗長インターフェイス、または EtherChannel インターフェイス ID を指定できます。ASASM では、*interface_id* は VLAN ID です。

ステップ 6 別のステート リンクを指定した場合、ステート リンクにアクティブ IP アドレスとスタンバイ IP アドレスを割り当てます。

failover interface ip *state_if_name* {*ip_address mask* | *ipv6_address*/*prefix*} **standby** *ip_address*

例：

```
ciscoasa(config)# failover interface ip statelink 172.27.49.1 255.255.255.0 standby
```

```
172.27.49.2
```

または：

```
ciscoasa(config)# failover interface ip statelink 2001:a0a:b00:a::a0a:b70/64 standby
2001:a0a:b00:a::a0a:b71
```

このアドレスは、フェールオーバー リンクとは異なる未使用のサブネット上になければなりません。169.254.0.0/16 と fd00:0:0:*::/64 は内部的に使用されるサブネットであり、フェールオーバー リンクやステート リンクに使用することはできません。

スタンバイ IP アドレスは、アクティブ IP アドレスと同じサブネットである必要があります。

ステート リンクを共有する場合は、この手順をとばしてください。

ステップ 7 別のステート リンクを指定した場合、ステート リンクをイネーブルにします。

interface *state_interface_id*

no shutdown

例：

```
ciscoasa(config)# interface gigabitethernet 0/4
ciscoasa(config-if)# no shutdown
```

ステート リンクを共有する場合は、この手順をとばしてください。

ステップ 8 （オプション）フェールオーバー リンクおよびステート リンクの通信を暗号化するには、次のいずれかを実行します。

- （優先）すべてのフェールオーバー通信を暗号化するには、装置間のフェールオーバー リンクおよびステート リンクの IPsec LAN-to-LAN トンネルを確立します。

  failover ipsec pre-shared-key [**0** | **8**] *key*

  例：

  ```
  ciscoasa(config)# failover ipsec pre-shared-key a3rynsun
  ```

  key は最大 128 文字です。両方の装置に同じキーを指定します。キーは IKEv2 によってトンネルを確立するために使用されます。

  マスターパスフレーズ（マスター パスフレーズの設定 （590 ページ）を参照）を使用している場合、キーはコンフィギュレーション内で暗号化されています。コンフィギュレーションからコピーする場合は（たとえば **more system:running-config** の出力からのコピー）、キーワード **8** を使用してキーが暗号化されていることを指定します。デフォルトでは、暗号化されていないパスワードを指定する **0** が使用されます。

  show running-config の出力では、**failover ipsec pre-shared-key** は ***** のように表示されます。このマスクされたキーはコピーできません。

フェールオーバー リンクおよびステート リンクの暗号化を設定しない場合、フェールオーバー通信はクリア テキストになります。この通信にはコマンド複製中に送信されるコンフィギュレーション内のすべてのパスワードやキーも含まれます。

IPsec 暗号化とレガシーの **failover key** 暗号化の両方を使用することはできません。両方の方法を設定した場合は、IPsec が使用されます。ただし、マスター パスフレーズを使用する場合、IPsec 暗号化を設定する前に **no failover key** コマンドを使用してフェールオーバー キーを削除する必要があります。

フェールオーバー LAN-to-LAN トンネルは、IPsec（その他の VPN）ライセンスには適用されません。

- （オプション）フェールオーバー リンクおよびステート リンクのフェールオーバー通信を暗号化します。

  failover key [**0** | **8**] {**hex** *key* | *shared_secret*}

  例：

  ```
  ciscoasa(config)# failover key johncr1cht0n
  ```

  1 ～ 63 文字の *shared_secret* または 32 文字の **16 進数**キーを使用します。*shared_secret* には、数字、文字、または句読点の任意の組み合わせを使用できます。共有秘密または 16 進数キーは暗号キーを生成するために使用されます。両方の装置に同じキーを指定します。

  マスターパスフレーズ（マスターパスフレーズの設定 （590ページ）を参照）を使用している場合、共有秘密または 16 進数キーはコンフィギュレーション内で暗号化されています。コンフィギュレーションからコピーする場合は（たとえば **more system:running-config** の出力からのコピー）、キーワード **8** を使用して共有秘密または 16 進数キーが暗号化されていることを指定します。デフォルトでは、暗号化されていないパスワードを指定する **0** が使用されます。

  failover key の共有秘密は、**show running-config** の出力に ***** と表示されます。このマスクされたキーはコピーできません。

  フェールオーバー リンクおよびステート リンクの暗号化を設定しない場合、フェールオーバー通信はクリア テキストになります。この通信にはコマンド複製中に送信されるコンフィギュレーション内のすべてのパスワードやキーも含まれます。

ステップ 9 フェールオーバーをイネーブルにします。

failover

ステップ 10 システム コンフィギュレーションをフラッシュ メモリに保存します。

write memory

例

次に、プライマリ装置用のフェールオーバー パラメータの設定例を示します。

```
failover lan unit primary
failover lan interface folink gigabitethernet0/3
failover interface ip folink 172.27.48.1 255.255.255.0 standby 172.27.48.2

interface gigabitethernet 0/3
  no shutdown
failover link folink gigabitethernet0/3
failover ipsec pre-shared-key a3rynsun
failover
```

アクティブ/スタンバイ フェールオーバーのセカンダリ装置の設定

セカンデリ装置に必要なコンフィギュレーションは、フェールオーバー リンクのコンフィギュレーションだけです。セカンダリ装置には、プライマリ装置と初期に通信するために、これらのコマンドが必要です。プライマリ装置がセカンダリ装置にコンフィギュレーションを送信した後、2 つのコンフィギュレーション間で唯一、不変の相違点は **failover lan unit** コマンドです。このコマンドで各装置がプライマリかセカンダリかを識別します。

始める前に

- フェールオーバー リンクおよびステート リンクに **nameif** を設定しないでください。
- マルチ コンテキスト モードでは、システム実行スペースで次の手順を実行します。コンテキストからシステム実行スペースに切り替えるには、**changeto system** コマンドを入力します。

手順

ステップ 1 **failover lan unit primary** コマンドを除いて、プライマリ装置とまったく同じコマンドを再入力します。任意で **failover lan unit secondary** コマンドに置き換えることもできますが、**secondary** はデフォルト設定のため、必須ではありません。アクティブ/スタンバイ フェールオーバーのプライマリ装置の設定 （286 ページ）を参照してください。

次に例を示します。

```
ciscoasa(config)# failover lan interface folink gigabitethernet0/3
INFO: Non-failover interface config is cleared on GigabitEthernet0/3 and its sub-interfaces
ciscoasa(config)# failover interface ip folink 172.27.48.1 255.255.255.0 standby
172.27.48.2
ciscoasa(config)# interface gigabitethernet 0/3
ciscoasa(config-ifc)# no shutdown
ciscoasa(config-ifc)# failover link folink gigabitethernet0/3
ciscoasa(config)# failover ipsec pre-shared-key a3rynsun
```

```
ciscoasa(config)# failover
```

ステップ 2 フェールオーバー コンフィギュレーションが同期された後で、コンフィギュレーションをフラッシュ メモリに保存します。

```
ciscoasa(config)# write memory
```

アクティブ/アクティブ フェールオーバーの設定

ここでは、アクティブ/アクティブ フェールオーバーの設定方法について説明します。

アクティブ/アクティブ フェールオーバーのプライマリ装置の設定

この項の手順に従って、アクティブ/アクティブ フェールオーバー コンフィギュレーションでプライマリ装置を設定します。この手順では、プライマリ装置でフェールオーバーをイネーブルにするために必要な最小のコンフィギュレーションが用意されています。

始める前に

- マルチ コンテキスト モードの有効化またはディセーブル化（215 ページ）に従って、マルチ コンテキスト モードをイネーブルにします。
- ルーテッド モード インターフェイスとトランスペアレント モード インターフェイス（523 ページ）に従って、フェールオーバー リンクとステート リンクを除くすべてのインターフェイスのスタンバイ IP アドレスを設定することを推奨します。
- フェールオーバー リンクおよびステート リンクに **nameif** を設定しないでください。
- この手順はシステム実行スペースで実行します。コンテキストからシステム実行スペースに切り替えるには、**changeto system** コマンドを入力します。

手順

ステップ 1 この装置をプライマリ装置に指定します。

failover lan unit primary

ステップ 2 フェールオーバー リンクとして使用するインターフェイスを指定します。

failover lan interface *if_name interface_id*

例：

```
ciscoasa(config)# failover lan interface folink gigabitethernet0/3
```

このインターフェイスは、他の目的には使用できません（オプションのステート リンクは除く）。

if_name 引数は、インターフェイスに名前を割り当てます。

interface_id 引数には、物理インターフェイス、サブインターフェイス、冗長インターフェイス、または EtherChannel インターフェイス ID を指定できます。Firepower 9300 では、任意のデータタイプ インターフェイスを使用できます。

ステップ 3 アクティブ IP アドレスとスタンバイ IP アドレスをフェールオーバー リンクに割り当てます。

standby failover interface ip *if_name* {*ip_address mask* | *ipv6_address*/*prefix* } **standby** *ip_address*

例：

```
ciscoasa(config)# failover interface ip folink 172.27.48.1 255.255.255.0 standby
172.27.48.2
```

または：

```
ciscoasa(config)# failover interface ip folink 2001:a0a:b00::a0a:b70/64 standby
2001:a0a:b00::a0a:b71
```

このアドレスは未使用のサブネット上になければなりません。169.254.0.0/16 と fd00:0:0:*::/64 は内部的に使用されるサブネットであり、フェールオーバー リンクやステート リンクに使用することはできません。

スタンバイ IP アドレスは、アクティブ IP アドレスと同じサブネットである必要があります。

ステップ 4 フェールオーバー リンクをイネーブルにします。

interface *failover_interface_id*

no shutdown

例：

```
ciscoasa(config)# interface gigabitethernet 0/3
ciscoasa(config-if)# no shutdown
```

ステップ 5 （オプション）ステート リンクとして使用するインターフェイスを指定します。

failover link *if_name interface_id*

例：

```
ciscoasa(config)# failover link statelink gigabitethernet0/4
```

フェールオーバー リンクまたはデータ インターフェイスとは異なるインターフェイスを指定することをお勧めします。

if_name 引数は、インターフェイスに名前を割り当てます。

interface_id 引数には、物理インターフェイス、サブインターフェイス、冗長インターフェイス、または EtherChannel インターフェイス ID を指定できます。ASASM では、*interface_id* に VLAN ID を指定します。

ステップ 6 別のステート リンクを指定した場合、ステート リンクにアクティブ IP アドレスとスタンバイ IP アドレスを割り当てます。

このアドレスは、フェールオーバー リンクとは異なる未使用のサブネット上になければなりません。169.254.0.0/16 と fd00:0:0:*::/64 は内部的に使用されるサブネットであり、フェールオーバー リンクやステート リンクに使用することはできません。

スタンバイ IP アドレスは、アクティブ IP アドレスと同じサブネットである必要があります。

ステート リンクを共有する場合は、この手順をとばしてください。

failover interface ip state *if_name* {*ip_address mask* | *ipv6_address*/*prefix*} **standby** *ip_address*

例：

```
ciscoasa(config)# failover interface ip statelink 172.27.49.1 255.255.255.0 standby
172.27.49.2
```

または：

```
ciscoasa(config)# failover interface ip statelink 2001:a0a:b00:a::a0a:b70/64 standby
2001:a0a:b00:a::a0a:b71
```

ステップ 7 別のステート リンクを指定した場合、ステート リンクをイネーブルにします。

interface *state_interface_id*

no shutdown

例：

```
ciscoasa(config)# interface gigabitethernet 0/4
ciscoasa(config-if)# no shutdown
```

ステート リンクを共有する場合は、この手順をとばしてください。

ステップ 8 （オプション）フェールオーバー リンクおよびステート リンクの通信を暗号化するには、次のいずれかを実行します。

- （優先）すべてのフェールオーバー通信を暗号化するには、装置間のフェールオーバー リンクおよびステート リンクの IPsec LAN-to-LAN トンネルを確立します。

  failover ipsec pre-shared-key [**0** | **8**] *key*

  ```
  ciscoasa(config)# failover ipsec pre-shared-key a3rynsun
  ```

  key は最大 128 文字です。両方の装置に同じキーを指定します。キーは IKEv2 によってトンネルを確立するために使用されます。

マスターパスフレーズ（マスターパスフレーズの設定（590ページ）を参照）を使用している場合、キーはコンフィギュレーション内で暗号化されています。コンフィギュレーションからコピーする場合は（たとえば**more system:running-config**の出力からのコピー）、キーワード**8**を使用してキーが暗号化されていることを指定します。デフォルトでは、暗号化されていないパスワードを指定する **0** が使用されます。

show running-config の出力では、**failover ipsec pre-shared-key** は ***** のように表示されます。このマスクされたキーはコピーできません。

フェールオーバー リンクおよびステート リンクの暗号化を設定しない場合、フェールオーバー通信はクリア テキストになります。この通信にはコマンド複製中に送信されるコンフィギュレーション内のすべてのパスワードやキーも含まれます。

IPsec 暗号化とレガシーの **failover key** 暗号化の両方を使用することはできません。両方の方法を設定した場合は、IPsec が使用されます。ただし、マスター パスフレーズを使用する場合、IPsec 暗号化を設定する前に **no failover key** コマンドを使用してフェールオーバー キーを削除する必要があります。

フェールオーバー LAN-to-LAN トンネルは、IPsec（その他の VPN）ライセンスには適用されません。

- （オプション）フェールオーバー リンクおよびステート リンクのフェールオーバー通信を暗号化します。

  failover key [**0** | **8**] {**hex** *key* | *shared_secret*}

  ```
  ciscoasa(config)# failover key johncr1cht0n
  ```

  1 ～ 63 文字の *shared_secret* または 32 文字の **16 進数**キーを使用します。

  shared_secret には、数字、文字、または句読点の任意の組み合わせを使用できます。共有秘密または16進数キーは暗号キーを生成するために使用されます。両方の装置に同じキーを指定します。

  マスターパスフレーズ（マスターパスフレーズの設定（590ページ）を参照）を使用している場合、共有秘密または 16 進数キーはコンフィギュレーション内で暗号化されています。コンフィギュレーションからコピーする場合は（たとえば**more system:running-config**の出力からのコピー）、キーワード **8** を使用して共有秘密または 16 進数キーが暗号化されていることを指定します。デフォルトでは、暗号化されていないパスワードを指定する **0** が使用されます。

  failover key の共有秘密は、**show running-config** の出力に ***** と表示されます。このマスクされたキーはコピーできません。

  フェールオーバー リンクおよびステート リンクの暗号化を設定しない場合、フェールオーバー通信はクリア テキストになります。この通信にはコマンド複製中に送信されるコンフィギュレーション内のすべてのパスワードやキーも含まれます。

ステップ 9　フェールオーバー グループ 1 を作成します。

failover group 1

primary

preempt [*delay*]

例：

```
ciscoasa(config-fover-group)# failover group 1
ciscoasa(config-fover-group)# primary
ciscoasa(config-fover-group)# preempt 1200
```

通常、プライマリ装置にグループ 1 を割り当て、セカンデリ装置にグループ 2 を割り当てます。グループの primary または secondary の設定にかかわらず、両方のフェールオーバー グループが最初にブートしたユニットでアクティブになります（それらが同時に起動したように見える場合でも、一方のユニットが最初にアクティブになります）。**preempt** コマンドは、指定された装置が使用可能になったときに、フェールオーバー グループがその装置で自動的にアクティブになるようにします。

オプションの *delay* 値に秒数を入力して、その時間フェールオーバー グループが現在の装置でアクティブ状態に維持され、その後に指定された装置で自動的にアクティブになるようにできます。有効な値は 1 ～ 1200 です。

ステートフル フェールオーバーがイネーブルの場合、プリエンプションは、フェールオーバー グループが現在アクティブになっている装置から接続が複製されるまで遅延されます。

手動でフェールオーバーすると、**preempt** コマンドは無視されます。

ステップ 10 フェールオーバー グループ 2 を作成して、セカンデリ装置に割り当てます。

failover group 2

secondary

preempt [*delay*]

例：

```
ciscoasa(config-fover-group)# failover group 2
ciscoasa(config-fover-group)# secondary
ciscoasa(config-fover-group)# preempt 1200
```

ステップ 11 特定のコンテキストのコンテキスト コンフィギュレーション モードに入り、そのコンテキストをフェールオーバー グループに割り当てます。

context *name*

join-failover-group{**1** |**2**}

例：

```
ciscoasa(config)# context Eng
ciscoasa(config-ctx)# join-failover-group 2
```

コンテキストごとにこのコマンドを繰り返します。

未割り当てのコンテキストはすべて、自動的にフェールオーバー グループ 1 に割り当てられます。管理コンテキストは常にフェールオーバー グループ 1 のメンバーです。グループ 2 に割り当てることはできません。

ステップ 12 フェールオーバーをイネーブルにします。

failover

ステップ 13 システム コンフィギュレーションをフラッシュ メモリに保存します。

write memory

例

次に、プライマリ装置用のフェールオーバー パラメータの設定例を示します。

```
failover lan unit primary
failover lan interface folink gigabitethernet0/3
failover interface ip folink 172.27.48.1 255.255.255.0 standby 172.27.48.2

interface gigabitethernet 0/3
  no shutdown
failover link statelink gigabitethernet0/4
failover interface ip statelink 172.27.49.1 255.255.255.0 standby 172.27.49.2

interface gigabitethernet 0/4
  no shutdown
failover group 1
  primary
  preempt
failover group 2
  secondary
  preempt
context admin
  join-failover-group 1
failover ipsec pre-shared-key a3rynsun
failover
```

アクティブ/アクティブ フェールオーバーのセカンデリ装置の設定

セカンデリ装置に必要なコンフィギュレーションは、フェールオーバー リンクのコンフィギュレーションだけです。セカンダリ装置には、プライマリ装置と初期に通信するために、これらのコマンドが必要です。プライマリ装置がセカンダリ装置にコンフィギュレーションを送信した後、2 つのコンフィギュレーション間で唯一、不変の相違点は **failover lan unit** コマンドです。このコマンドで各装置がプライマリかセカンダリかを識別します。

始める前に

- マルチ コンテキスト モードの有効化またはディセーブル化（215 ページ）に従って、マルチ コンテキスト モードをイネーブルにします。

- フェールオーバー リンクおよびステート リンクに **nameif** を設定しないでください。
- この手順はシステム実行スペースで実行します。コンテキストからシステム実行スペースに切り替えるには、**changeto system** コマンドを入力します。

手順

ステップ 1 **failover lan unit primary** コマンドを除いて、プライマリ装置とまったく同じコマンドを再入力します。任意で **failover lan unit secondary** コマンドに置き換えることもできますが、**secondary** はデフォルト設定のため、必須ではありません。また、プライマリ装置から複製されるので、**failover group** コマンドおよび **join-failover-group** コマンドを入力する必要もありません。アクティブ/アクティブ フェールオーバーのプライマリ装置の設定（291 ページ）を参照してください。

次に例を示します。

```
ciscoasa(config)# failover lan interface folink gigabitethernet0/3
INFO: Non-failover interface config is cleared on GigabitEthernet0/3 and its sub-interfaces
ciscoasa(config)# failover interface ip folink 172.27.48.1 255.255.255.0 standby
172.27.48.2
ciscoasa(config)# interface gigabitethernet 0/3
no shutdown
ciscoasa(config)# failover link statelink gigabitethernet0/4
INFO: Non-failover interface config is cleared on GigabitEthernet0/4 and its sub-interfaces
ciscoasa(config)# failover interface ip statelink 172.27.49.1 255.255.255.0 standby
172.27.49.2
ciscoasa(config)# interface gigabitethernet 0/4
no shutdown
ciscoasa(config)# failover ipsec pre-shared-key a3rynsun
ciscoasa(config)# failover
```

ステップ 2 フェールオーバー コンフィギュレーションがプライマリ装置と同期された後で、コンフィギュレーションをフラッシュ メモリに保存します。

ciscoasa(config)# **write memory**

ステップ 3 必要に応じて、フェールオーバー グループ 2 がセカンデリ装置でアクティブになるように設定します。

failover active group 2

オプションのフェールオーバー パラメータの設定

必要に応じてフェールオーバー設定をカスタマイズできます。

フェールオーバー基準とその他の設定の構成

この項で変更可能な多くのパラメータのデフォルト設定については、フェールオーバーのデフォルト（285ページ）を参照してください。アクティブ/アクティブモードでは、ほとんどの条件をフェールオーバー グループごとに設定します。

始める前に

- マルチ コンテキスト モードのシステム実行スペースで次の設定を行います。

手順

ステップ 1 装置のポーリング時間およびホールド時間を変更します。

failover polltime [**unit**] [**msec**] *poll_time* [**holdtime** [**msec**] *time*]

例：

```
ciscoasa(config)# failover polltime unit msec 200 holdtime msec 800
```

polltime の範囲は 1 ～ 15 秒または 200 ～ 999 ミリ秒です。**holdtime** の範囲は 1 ～ 45 秒または 800 ～ 999 ミリ秒です。ユニットのポーリング時間の 3 倍未満のホールド時間の値を入力することはできません。ポーリング間隔を短くすると、ASA で障害を検出し、フェールオーバーをトリガーする速度が速くなります。ただし短時間での検出は、ネットワークが一時的に輻輳した場合に不要な切り替えが行われる原因となります。

1 回のポーリング期間中に、装置がフェールオーバー通信インターフェイスで hello パケットを検出しなかった場合、残りのインターフェイスで追加テストが実行されます。それでも保持時間内にピア装置から応答がない場合、その装置は故障していると見なされ、故障した装置がアクティブ装置の場合は、スタンバイ装置がアクティブ装置を引き継ぎます。

アクティブ/アクティブモードでは、システムに対してこのレートを設定します。フェールオーバー グループごとにこのレートを設定することはできません。

ステップ 2 セッションの複製レートを、1 秒間の接続数で設定します。

failover replication rate *conns*

例：

```
ciscoasa(config)# failover replication rate 20000
```

最小および最大レートはモデルによって異なります。デフォルトは最大レートです。アクティブ/アクティブ モードでは、システムに対してこのレートを設定します。フェールオーバー グループごとにこのレートを設定することはできません。

ステップ 3 スタンバイ装置またはコンテキストのコンフィギュレーションを直接変更できないようにします。

failover standby config-lock

デフォルトでは、スタンバイ ユニットまたはスタンバイ コンテキストに対するコンフィギュレーションは、警告メッセージ付きで許可されます。

ステップ 4 （アクティブ/アクティブ モードのみ）カスタマイズするフェールオーバー グループを指定します。

failover group {**1** | **2**}

例：

```
ciscoasa(config)# failover group 1
ciscoasa(config-fover-group)#
```

ステップ 5 HTTP ステート複製をイネーブルにします。

- アクティブ/スタンバイ モードの場合

  failover replication http

- アクティブ/アクティブ モードの場合

  replication http

HTTP 接続がステート情報複製に含まれるようにするには、HTTP 複製をイネーブルにする必要があります。HTTP ステート複製を有効にすることをお勧めします。

（注） フェールオーバーを使用しているときに、スタンバイ装置からHTTPフローを削除すると遅延が生じます。このため **show conn count** 出力には、アクティブ装置とスタンバイ装置で異なる数が表示されることがあります。数秒待ってコマンドを再発行すると、両方の装置で同じカウントが表示されます。

ステップ 6 インターフェイスに障害が発生したときのフェールオーバーのしきい値を設定します。

- アクティブ/スタンバイ モードの場合

  failover interface-policy *num* [%]

  例：

  ```
  ciscoasa (config)# failover interface-policy 20%
  ```

- アクティブ/アクティブ モードの場合

  interface-policy *num* [%]

  例：

  ```
  ciscoasa(config-fover-group)# interface-policy 20%
  ```

デフォルトでは、1 つのインターフェイス障害でフェールオーバーが行われます。

インターフェイスの具体的な数を指定するときは、*num* 引数に 1 ～ 1025 を設定できます。

インターフェイスの割合を指定するときは、*num* 引数に 1 ～ 100 を設定できます。

ステップ 7 インターフェイスのポーリング時間とホールド時間を変更します。

- アクティブ/スタンバイ モードの場合

  failover polltime interface [**msec**] *polltime* [**holdtime** *time*]

  例：

  ```
  ciscoasa(config)# failover polltime interface msec 500 holdtime 5
  ```

- アクティブ/アクティブ モードの場合

  polltime interface [**msec**] *polltime* [**holdtime***time*]

  例：

  ```
  ciscoasa(config-fover-group)# polltime interface msec 500 holdtime 5
  ```

- *polltime*：helloパケットをピアに送信するまで待機する時間を設定します。polltimeに有効な値は 1 ～ 15 秒で、オプションの **msec** キーワードを使用する場合は 500 ～ 999 ミリ秒です。デフォルトは 5 秒です。
- **holdtime***time*：ピア ユニットからの最後に受信した hello メッセージとインターフェイス テストの開始との間の時間（計算として）を設定して、インターフェイスの健全性を判断します。また、各インターフェイス テストの期間を holdtime/16 として設定します。有効な値は 5 ～ 75 秒です。デフォルトは、polltime の5倍です。polltime の 5 倍よりも短い holdtime 値は入力できません。

  インターフェイステストを開始するまでの時間（y）を計算するには、次のようにします。

  1. x = (*holdtime*/*polltime*)/2、最も近い整数に丸められます。（.4 以下は切り下げ、.5 以上は切り上げ。）
  2. y = x**polltime*

  たとえば、デフォルトの holdtime は 25 で、polltime が 5 の場合は y は 15 秒です。

ステップ 8 インターフェイスの仮想 MAC アドレスを設定します。

- アクティブ/スタンバイ モードの場合

  failover mac address *phy_if active_mac standby_mac*

  例：

  ```
  ciscoasa(config)# failover mac address gigabitethernet0/2 00a0.c969.87c8 00a0.c918.95d8
  ```

- アクティブ/アクティブ モードの場合

  mac address *phy_if active_mac standby_mac*

例：

```
ciscoasa(config-fover-group)# mac address gigabitethernet0/2 00a0.c969.87c8
00a0.c918.95d8
```

phy_if 引数は、インターフェイスの物理名（gigabitethernet0/1 など）です。

active_mac および *standby_mac* 引数は、H.H.H 形式（H は 16 ビットの 16 進数）の MAC アドレスです。たとえば、MAC アドレスが 00-0C-F1-42-4C-DE の場合、000C.F142.4CDE と入力します。

active_mac アドレスはインターフェイスのアクティブ *IP* アドレスに関連付けられ、standby_mac はインターフェイスのスタンバイ IP アドレスに関連付けられます。

他のコマンドまたは方法を使用して MAC アドレスを設定することもできますが、1 つの方法だけを使用することを推奨します。複数の方法を使用して MAC アドレスを設定した場合は、どの MAC アドレスが使用されるかは多くの可変要素によって決まるため、予測できないことがあります。

show interface コマンドを使用して、インターフェイスが使用している MAC アドレスを表示します。

ステップ 9 （アクティブ/アクティブ モードのみ）他のフェールオーバー グループについてこの手順を繰り返します。

インターフェイス モニタリングの設定

デフォルトでは、すべての物理インターフェイス、または ASASM の場合、すべての VLAN インターフェイス、および ASA にインストールされるすべてのハードウェアまたはソフトウェアモジュール（ASA FirePOWER モジュールなど）でモニタリングが有効になっています。

重要度の低いネットワークに接続されているインターフェイスがフェールオーバー ポリシーに影響を与えないように除外できます。

装置ごとに最大 1025 のインターフェイスをモニタできます（マルチ コンテキスト モードのすべてのコンテキストにわたって）。

始める前に

マルチ コンテキスト モードで、各コンテキスト内のインターフェイスを設定します。

手順

インターフェイスのヘルス モニタリングをイネーブルまたはディゼーブルにします。

[**no**] **monitor-interface** {*if_name* | **service-module**}

例：

```
ciscoasa(config)# monitor-interface inside
ciscoasa(config)# no monitor-interface eng1
```

ASA FirePOWERモジュールなどの特定のハードウェア/ソフトウェア モジュールの障害によってフェールオーバーをトリガーすることが望ましくない場合は、**no monitor-interface service-module** コマンドを使用してモジュールのモニタリングを無効化できます。なお、ASA 5585-X では、サービス モジュールのモニタリングを無効にする場合、個別にモニタされるモジュール上の各インターフェイスのモニタリングを無効にすることもできます。

非対称にルーティングされたパケットのサポートの設定（アクティブ/アクティブ モード）

アクティブ/アクティブ フェールオーバーでの実行中に、ピア装置を経由して開始された接続に対する返送パケットを、装置が受信する場合があります。そのパケットを受信する ASA にはそのパケットの接続情報がないために、パケットはドロップされます。このドロップが多く発生するのは、アクティブ/アクティブ フェールオーバー ペアの 2 台の ASA が異なるサービス プロバイダーに接続されており、アウトバウンド接続に NAT アドレスが使用されていない場合です。

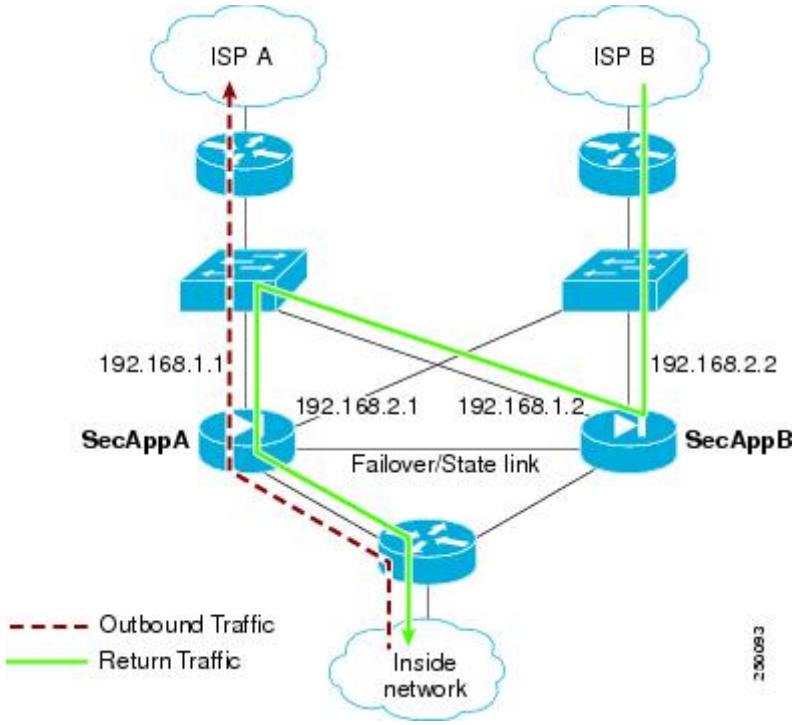
返送パケットのドロップは、非対称にルーティングされたパケットを許可することによって防ぐことができます。そのためには、それぞれの ASA の同様のインターフェイスを同じ ASR グループに割り当てます。たとえば、両方の ASA が、内部インターフェイスでは同じ内部ネットワークに接続している一方、外部インターフェイスでは別の ISP に接続しているとします。プライマリ装置で、アクティブ コンテキストの外部インターフェイスを ASR グループ 1 に割り当て、セカンダリ装置でも、アクティブ コンテキストの外部インターフェイスを同じ ASR グループ 1 に割り当てます。プライマリ装置の外部インターフェイスがセッション情報を持たないパケットを受信すると、同じグループ（この場合 ASR グループ 1）内のスタンバイ コンテキストの他のインターフェイスのセッション情報をチェックします。一致する情報が見つからない場合、パケットはドロップされます。一致する情報が見つかると、次の動作のうちいずれかが開始します。

- 着信トラフィックがピア装置に発信されると、レイヤ 2 ヘッダーの一部またはすべてが書き直され、パケットは他の装置にリダイレクトされます。このリダイレクトは、セッションがアクティブである限り続行されます。
- 着信トラフィックが同じ装置の別のインターフェイスに発信されると、レイヤ 2 ヘッダーの一部またはすべてが書き直され、パケットはストリームに再注入されます。

（注） この機能は、非対称ルーティングを提供しません。非対称にルーティングされたパケットを正しいインターフェイスに戻します。

次の図に、非対称にルーティングされたパケットの例を示します。

図 *45 : ASR* の例



1. アウトバウンドセッションが、アクティブな SecAppA コンテキストを持つ ASA を通過します。このパケットは、インターフェイス外の ISP-A（192.168.1.1）から送信されます。
2. 非対称ルーティングがアップストリームのどこかで設定されているため、リターン トラフィックは、アクティブな SecAppB コンテキストを持つ ASA のインターフェイス外部の ISP-B（192.168.2.2）経由で戻ります。
3. 通常、リターン トラフィックは、そのインターフェイス 192.168.2.2 上にリターン トラフィックに関するセッション情報がないので、ドロップされます。しかし、このインターフェイスは、ASR グループ 1 の一部として設定されています。装置は、同じ ASR グループ ID で設定された他のインターフェイス上のセッションを探します。
4. このセッション情報は、SecAppB を持つ装置上のスタンバイ状態のインターフェイス outsideISP-A（192.168.1.2）にあります。ステートフル フェールオーバーは、SecAppA から SecAppB にセッション情報を複製します。
5. ドロップされる代わりに、レイヤ 2 ヘッダーはインターフェイス 192.168.1.1 の情報で書き直され、トラフィックはインターフェイス 192.168.1.2 からリダイレクトされます。そこから、発信元の装置のインターフェイスを経由して戻ります（SecAppA の 192.168.1.1）。この転送は、必要に応じて、セッションが終了するまで続行されます。

始める前に

- ステートフル フェールオーバー：アクティブ フェールオーバー グループにあるインターフェイスのセッションのステート情報を、スタンバイ フェールオーバー グループに渡します。
- replication http：HTTP セッションのステート情報は、スタンバイ フェールオーバー グループに渡されないため、スタンバイ インターフェイスに存在しません。ASA が非対称にルーティングされた HTTP パケットを再ルーティングできるように、HTTP ステート情報を複製する必要があります。
- プライマリ装置およびセカンダリ装置の各アクティブ コンテキスト内でこの手順を実行します。
- コンテキスト内に ASR グループとトラフィック ゾーンの両方を設定することはできません。コンテキスト内にゾーンを設定した場合、どのコンテキストインターフェイスも ASR グループに含めることはできません。

手順

ステップ 1 プライマリ装置で、非対称にルーティングされたパケットを許可するインターフェイスを指定します。

interface *phy_if*

例：

```
primary/admin(config)# interface gigabitethernet 0/0
```

ステップ 2 インターフェイスの ASR グループ番号を設定します。

asr-group *num*

例：

```
primary/admin(config-ifc)# asr-group 1
```

num 範囲に有効な値は、1 ～ 32 です。

ステップ 3 セカンダリ装置で、非対称にルーティングされたパケットを許可するインターフェイスを指定します。

interface *phy_if*

例：

```
secondary/ctx1(config)# interface gigabitethernet 0/1
```

ステップ 4 インターフェイスの ASR グループ番号をプライマリ装置のインターフェイスに一致するように設定します。

asr-group *num*

例：

```
secondary/ctx1(config-ifc)# asr-group 1
```

例

2 つの装置に次のコンフィギュレーションがあります（コンフィギュレーションは関連するコマンドだけを示します）。図の「SecAppA」というラベルの付いたデバイスは、フェールオーバー ペアのプライマリ装置です。

プライマリ装置のシステム コンフィギュレーション

```
interface GigabitEthernet0/1
  description LAN/STATE Failover Interface
interface GigabitEthernet0/2
  no shutdown
interface GigabitEthernet0/3
  no shutdown
interface GigabitEthernet0/4
  no shutdown
interface GigabitEthernet0/5
  no shutdown
failover
failover lan unit primary
failover lan interface folink GigabitEthernet0/1
failover link folink
failover interface ip folink 10.0.4.1 255.255.255.0 standby 10.0.4.11
failover group 1
  primary
failover group 2
  secondary
admin-context SecAppA
context admin
  allocate-interface GigabitEthernet0/2
  allocate-interface GigabitEthernet0/3
  config-url flash:/admin.cfg
  join-failover-group 1
context SecAppB
  allocate-interface GigabitEthernet0/4
  allocate-interface GigabitEthernet0/5
  config-url flash:/ctx1.cfg
  join-failover-group 2
```

SecAppA コンテキスト コンフィギュレーション

```
interface GigabitEthernet0/2
  nameif outsideISP-A
  security-level 0
  ip address 192.168.1.1 255.255.255.0 standby 192.168.1.2
  asr-group 1
interface GigabitEthernet0/3
  nameif inside
  security-level 100
```

```
  ip address 10.1.0.1 255.255.255.0 standby 10.1.0.11
monitor-interface outside
```

SecAppB コンテキスト コンフィギュレーション

```
interface GigabitEthernet0/4
  nameif outsideISP-B
  security-level 0
  ip address 192.168.2.2 255.255.255.0 standby 192.168.2.1
  asr-group 1
interface GigabitEthernet0/5
  nameif inside
  security-level 100
  ip address 10.2.20.1 255.255.255.0 standby 10.2.20.11
```

フェールオーバー の管理

この項では、フェールオーバーの設定を変更する方法、ある装置から別の装置にフェールオーバーを強制実行する方法など、フェールオーバーをイネーブルにした後にフェールオーバー装置を管理する方法について説明します。

フェールオーバーの強制実行

スタンバイ装置を強制的にアクティブにするには、次の手順を実行します。

始める前に

マルチ コンテキスト モードでは、システム実行スペースでこの手順を実行します。

手順

ステップ 1 スタンバイ装置で入力した場合、フェールオーバーが強制実行されます。スタンバイ装置はアクティブ装置になります。

group *group_id* を指定する場合は、指定するアクティブ/アクティブ フェールオーバー グループのスタンバイ装置でこのコマンドを入力すると、フェールオーバーが強制実行されます。スタンバイ装置はそのフェールオーバー グループのアクティブ装置になります。

- アクティブ/スタンバイ モードのスタンバイ装置の場合

  failover active

- アクティブ/アクティブ モードのスタンバイ装置の場合

  failover active [**group** *group_id*]

  例：

```
standby# failover active group 1
```

ステップ 2 アクティブ装置で入力した場合、フェールオーバーが強制実行されます。アクティブ装置はスタンバイ装置になります。

group *group_id* を指定する場合は、指定するフェールオーバー グループのアクティブ装置でこのコマンドを入力すると、フェールオーバーが強制実行されます。アクティブ装置はそのフェールオーバー グループのスタンバイ装置になります。

- アクティブ/スタンバイ モードのアクティブ装置の場合

  no failover active

- アクティブ/アクティブ モードのアクティブ装置の場合

  no failover active [**group** *group_id*]

  例：

```
active# no failover active group 1
```

フェールオーバーのディセーブル化

1 つまたは両方の装置でフェールオーバーをディセーブルにすると、リロードするまで各装置のアクティブおよびスタンバイ状態が維持されます。アクティブ/アクティブ フェールオーバー ペアの場合、どの装置を優先するように設定されていようと、フェールオーバー グループはアクティブであるすべての装置でアクティブ状態のまま維持されます。

フェールオーバーをディセーブルにする際、次の特性を参照してください。

- スタンバイ装置/コンテキストはスタンバイ モードのまま維持されるので、両方の装置はトラフィックの転送を開始しません（これは疑似スタンバイ状態と呼ばれます）。
- スタンバイ装置/コンテキストは、アクティブ装置/コンテキストに接続されていない場合でもそのスタンバイ IP アドレスを引き続き使用します。
- スタンバイ装置/コンテキストによる、フェールオーバー上における接続に対するリッスンは継続されます。フェールオーバーをアクティブ装置/コンテキストで再度イネーブルにすると、そのコンフィギュレーションの残りが再同期化された後に、スタンバイ装置/コンテキストが通常のスタンバイ状態に戻ります。
- スタンバイ装置で手動でフェールオーバーをイネーブルにしてアクティブ化しないでください。代わりに、フェールオーバーの強制実行（306 ページ）を参照してください。スタンバイ装置でフェールオーバーをイネーブルにすると、MAC アドレスの競合が発生し、IPv6 トラフィックが中断される可能性があります。

- 完全にフェールオーバーをディセーブルにするには、no failover コンフィギュレーションをスタートアップ コンフィギュレーションに保存してからリロードします。

始める前に

マルチ コンテキスト モードでは、システム実行スペースでこの手順を実行します。

手順

ステップ 1 フェールオーバーをディセーブルにします。

no failover

ステップ 2 完全にフェールオーバーをディセーブルにするには、コンフィギュレーションを保存してをリロードします。

write memory

reload

障害が発生した装置の復元

障害が発生した装置を障害のない状態に復元するには、次の手順を実行します。

始める前に

マルチ コンテキスト モードでは、システム実行スペースでこの手順を実行します。

手順

ステップ 1 障害が発生したユニットを障害が発生していない状態に復元します。

- アクティブ/スタンバイ モードの場合

  failover reset

- アクティブ/アクティブ モードの場合

  failover reset [**group** *group_id*]

  例：

```
ciscoasa(config)# failover reset group 1
```

障害が発生した装置を障害のない状態に復元しても、その装置が自動的にアクティブになるわけではありません。復元された装置は、（強制または自然な形での）フェールオーバーによってアクティブになるまではスタンバイ状態のままです。例外は、フェールオーバー グループ

（アクティブ/アクティブ モードのみ）にフェールオーバー プリエンプションが設定されている場合です。以前アクティブであったフェールオーバー グループにプリエンプションが設定されており、障害が発生した装置が優先装置の場合、そのフェールオーバー グループはアクティブになります。

group *group_id* を指定した場合、このコマンドは障害が発生したアクティブ/アクティブ フェールオーバー グループを障害のない状態に復元します。

ステップ 2 （アクティブ/アクティブ モードのみ）フェールオーバーをフェールオーバー グループ レベルで復元するには次を行います。

a) システムで、[Monitoring] > [Failover] > [Failover Group #] を開きます。#は、制御するフェールオーバー グループの番号です。

b) [Reset Failover] をクリックします。

コンフィギュレーションの再同期

アクティブ装置に write standby コマンドを入力すると、スタンバイ装置で実行コンフィギュレーションが削除され（アクティブ装置との通信に使用するフェールオーバー コマンドを除く）、アクティブ装置のコンフィギュレーション全体がスタンバイ装置に送信されます。

マルチ コンテキスト モードの場合、システム実行スペースに **write standby** コマンドを入力すると、すべてのコンテキストが複製されます。あるコンテキスト内で **write standby** コマンドを入力すると、コマンドはそのコンテキスト コンフィギュレーションだけを複製します。

複製されたコマンドは、実行コンフィギュレーションに保存されます。

フェールオーバー機能のテスト

フェールオーバー機能をテストするには、次の手順を実行します。

手順

ステップ 1 FTPなどを使用して、異なるインターフェイス上のホスト間でファイルを送信し、アクティブ装置が予期したとおりにトラフィックを渡しているかどうかをテストします。

ステップ 2 アクティブ装置で次のコマンドを入力し、フェールオーバーを強制実行します。

アクティブ/スタンバイ モード

ciscoasa(config)# **no failover active**

アクティブ/アクティブ モード

ciscoasa(config)# **no failover active group** *group_id*

ステップ 3 FTP を使用して、2 つの同じホスト間で別のファイルを送信します。

ステップ 4 テストが成功しなかった場合は、**show failover** コマンドを入力してフェールオーバー ステータスを確認します。

ステップ 5 テストが終了したら、新しくアクティブになった装置で次のコマンドを入力すると、装置をアクティブ ステータスに復元できます。

アクティブ/スタンバイ モード

ciscoasa(config)# **no failover active**

アクティブ/アクティブ モード

ciscoasa(config)# **failover active group** *group_id*

（注） ASA インターフェイスの 1 つがダウンしたとき、フェールオーバーの観点からは、これも装置の問題と見なされます。インターフェイスの 1 つがダウンしていることを ASA が検出した場合は、インターフェイスのホールド時間を待たずに、フェールオーバーがただちに行われます。インターフェイスのホールド時間が有効であるのは、ASA が自身のステータスを OK と見なしているときだけです（ピアから hello パケットを受信していなくても）。インターフェイスのホールド時間をシミュレートするには、ピアが他のピアから hello パケットを受信するのを停止させるために、スイッチ上で VLAN をシャットダウンします。

リモート コマンドの実行

リモート コマンドを実行すると、コマンドラインに入力されたコマンドを特定のフェールオーバー ピアに送信できます。

コマンドの送信

コンフィギュレーション コマンドはアクティブ装置またはコンテキストからスタンバイ装置またはコンテキストに複製されるため、いずれの装置にログインしているかにかかわらず、**failover exec** コマンドを使用して正しい装置にコンフィギュレーション コマンドを入力できます。たとえば、スタンバイ装置にログインしている場合、**failover exec active** コマンドを使用して、コンフィギュレーションの変更をアクティブ装置に送信できます。その後、これらの変更はスタンバイ装置に複製されます。スタンバイ装置やコンテキストへの設定コマンドの送信には、**failover exec** コマンドを使用しないでください。これらの設定の変更はアクティブ装置に複製されないため、2 つの設定が同期されなくなります。

configuration、exec、および **show** コマンドの出力は、現在のターミナル セッションで表示されるため、 **failover exec** コマンドを使用し、ピア装置で **show** コマンドを発行して、その結果を現在のターミナルに表示することができます。

ピア装置でコマンドを実行するには、ローカル装置でコマンドを実行できるだけの十分な権限を持っている必要があります。

手順

ステップ 1 マルチ コンテキスト モードの場合は、**changeto context***name* コマンドを使用して、設定したいコンテキストに変更します。**failover exec** コマンドを使用して、フェールオーバー ピアでコンテキストを変更することはできません。

ステップ 2 次のコマンドを使用して、所定のフェールオーバー装置にコマンドを送信します。

ciscoasa(config)# **failover exec** {**active** | **mate** | **standby**}

active または **standby** キーワードを使用すると、その装置が現在の装置であっても、コマンドは指定された装置で実行されます。**mate** キーワードを使用すると、コマンドはフェールオーバー ピアで実行されます。

コマンドモードを変更するコマンドによって、現在のセッションのプロンプトが変更されることはありません。コマンドが実行されるコマンド モードを表示するには、 **show failover exec** コマンドを使用する必要があります。詳細については、コマンドモードの変更を参照してください。

コマンド モードの変更

failover exec コマンドは、お使いのターミナル セッションのコマンド モードとは異なるコマンド モード状態を維持します。デフォルトでは、**failover exec** コマンド モードは、指定されたデバイスのグローバル コンフィギュレーション モードで開始されます。このコマンド モードを変更するには、 **failover exec** コマンドを使用して適切なコマンド（**interface** コマンドなど）を送信します。**failover exec** を使用してモードを変更しても、セッション プロンプトは変更されません。

たとえば、フェールオーバーペアのアクティブ装置のグローバル コンフィギュレーション モードにログインし、**failover exec active** コマンドを使用してインターフェイス コンフィギュレーション モードを変更した場合、ターミナル プロンプトはグローバル コンフィギュレーション モードのままですが、**failover exec** を使用して入力されるコマンドは、インターフェイス コンフィギュレーション モードで入力されます。

次の例は、ターミナル セッション モードと **failover exec** コマンド モードの違いを示しています。この例で、管理者はアクティブ装置の **failover exec** モードを、インターフェイス GigabitEthernet0/1 用のインターフェイス コンフィギュレーション モードに変更します。その後、**failover exec active** を使用して入力されたすべてのコマンドがインターフェイス GigabitEthernet0/1 用のインターフェイス コンフィギュレーション モードに送信されます。次に、管理者は failover exec active を使用して、そのインターフェイスに IP アドレスを割り当てます。プロンプトはグローバル コンフィギュレーション モードを示していますが、**failover exec active** モードはインターフェイス コンフィギュレーション モードです。

```
ciscoasa(config)# failover exec active interface GigabitEthernet0/1
ciscoasa(config)# failover exec active ip address 192.168.1.1 255.255.255.0 standby
192.168.1.2
ciscoasa(config)# router rip
```

```
ciscoasa(config-router)#
```

デバイスとの現在のセッションのコマンド モードを変更しても、**failover exec** コマンドで使用されるコマンド モードには影響しません。たとえば、アクティブ装置のインターフェイス コンフィギュレーション モードで、**failover exec** コマンド モードを変更していない場合、次のコマンドはグローバル コンフィギュレーション モードで実行されます。その結果、デバイスとのセッションはインターフェイス コンフィギュレーション モードのままで、**failover exec active** を使用して入力されたコマンドは、指定されたルーティング プロセスを実行するためルータ コンフィギュレーション モードに送信されます。

```
ciscoasa(config-if)# failover exec active router ospf 100
ciscoasa(config-if)#
```

show failover exec コマンドを使用すると、指定したデバイスにコマンド モードが表示されます。**failover exec** コマンドを使用して送信されたコマンドは、このモードで実行されます。**show failover exec** コマンドでは、**failover exec** コマンドと同じキーワード、つまり **active**、**mate**、または **standby** が使用されます。各デバイスの **failover exec** モードは個別に追跡されます。

次に、スタンバイ装置に入力された **show failover exec** コマンドの出力例を示します。

```
ciscoasa(config)# failover exec active interface GigabitEthernet0/1
ciscoasa(config)# sh failover exec active
Active unit Failover EXEC is at interface sub-command mode

ciscoasa(config)# sh failover exec standby
Standby unit Failover EXEC is at config mode

ciscoasa(config)# sh failover exec mate
Active unit Failover EXEC is at interface sub-command mode
```

セキュリティに関する注意事項

failover exec コマンドは、フェールオーバー リンクを使用してコマンドをピア装置に送信し、実行されたコマンドの出力をピア装置から受信します。盗聴や中間者攻撃を防ぐためには、フェールオーバー リンクの暗号化をイネーブルにする必要があります。

リモート コマンドの実行に関する制限事項

リモート コマンドの使用には、次の制限事項があります。

- ゼロダウンタイム アップグレード手順を使用して 1 台の装置だけをアップグレードする場合は、機能するコマンドとして **failover exec** コマンドをサポートしているソフトウェアが両方の装置で動作している必要があります。
- コマンドの完成およびコンテキスト ヘルプは、*cmd_string* 引数のコマンドでは使用できません。
- マルチ コンテキスト モードでは、ピア装置のピア コンテキストだけにコマンドを送信できます。異なるコンテキストにコマンドを送信するには、まずログインしている装置でそのコンテキストに変更する必要があります。

- 次のコマンドを **failover exec** コマンドと一緒に使用することはできません。
  - **changeto**
  - **debug (undebug)**
- スタンバイ装置が故障状態の場合、故障の原因がサービス カードの不具合であれば、**failover exec** コマンドからのコマンドは受信できます。それ以外の場合、リモート コマンドの実行は失敗します。
- **failover exec** コマンドを使用して、フェールオーバー ピアで特権 EXEC モードをグローバル コンフィギュレーション モードに切り替えることはできません。たとえば、現在の装置が特権 EXEC モードのときに **failover exec mate configure terminal** を入力すると、**show failover exec mate** の出力に、failover exec セッションがグローバル コンフィギュレーション モードであることが示されます。ただし、ピア装置で **failover exec** を使用してコンフィギュレーション コマンドを入力した場合、現在の装置でグローバル コンフィギュレーション モードを開始しない限り、その処理は失敗します。
- **failover exec mate failover exec mate** コマンドのような、再帰的な failover exec コマンドは入力できません。
- ユーザの入力または確認が必要なコマンドでは、**noconfirm** オプションを使用する必要があります。たとえば、mate をリロードするには、次を入力します。

  failover exec mate reload noconfirm

モニタリング フェールオーバー

このセクションでは、フェールオーバー ステータスをモニタできます。

フェールオーバー メッセージ

フェールオーバーが発生すると、両方の ASA がシステム メッセージを送信します。

フェールオーバーの syslog メッセージ

ASA は、深刻な状況を表すプライオリティ レベル 2 のフェールオーバーについて、複数の syslog メッセージを発行します。これらのメッセージを表示するには、『syslog メッセージ ガイド』を参照してください。フェールオーバーに関連付けられているメッセージ ID の範囲は次のとおりです：101xxx、102xxx、103xxx、104xxx、105xxx、210xxx、311xxx、709xxx、727xxx。たとえば、105032 および 105043 はフェールオーバー リンクとの問題を示しています。

（注） フェールオーバーの最中に、ASAは論理的にシャットダウンした後、インターフェイスを起動し、syslog メッセージ 411001 および 411002 を生成します。これは通常のアクティビティです。

フェールオーバー デバッグ メッセージ

デバッグ メッセージを表示するには、**debug fover** コマンドを入力します。詳細については、コマンド リファレンスを参照してください。

（注） CPUプロセスではデバッグ出力に高プライオリティが割り当てられているため、デバッグ出力を行うとシステム パフォーマンスに大きく影響することがあります。このため、特定の問題のトラブルシューティングを行う場合や、Cisco TAC とのトラブルシューティング セッションの間に限り **debug fover** コマンドを使用してください。

SNMP のフェールオーバー トラップ

フェールオーバーに対する SNMP syslog トラップを受信するには、SNMP トラップを SNMP 管理ステーションに送信するように SNMP エージェントを設定し、syslog ホストを定義し、お使いの SNMP 管理ステーションに Cisco syslog MIB をコンパイルします。

フェールオーバー ステータスのモニタリング

フェールオーバー ステータスをモニタするには、次のいずれかのコマンドを入力します。

- **show failover**

  装置のフェールオーバー状態についての情報を表示します。

- **show failover group**

  装置のフェールオーバー状態に関する情報を表示します。表示される情報は、**show failover** コマンドの場合と似ていますが、指定されたグループに対象が限定されます。

- **show monitor-interface**

  モニタ対象インターフェイスの情報を表示します。

- **show running-config failover**

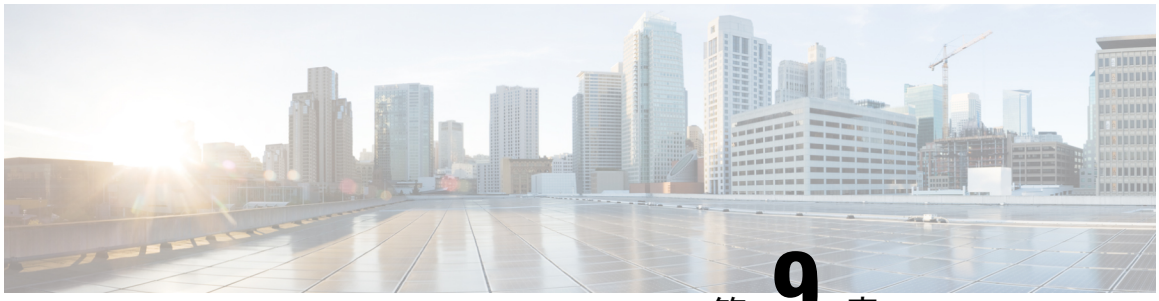
  実行コンフィギュレーション内のフェールオーバー コマンドを表示します。

フェールオーバーの履歴

機能名	リリース	機能情報
アクティブ/スタンバイ フェールオーバー	7.0(1)	この機能が導入されました。
アクティブ/アクティブ フェールオーバー	7.0(1)	この機能が導入されました。
フェールオーバー キーの 16 進数値サポート	7.0(4)	フェールオーバー リンクの暗号化用に16進数値が指定できるようになりました。 **failover key hex** コマンドが変更されました。
フェールオーバー キーのマスター パスフレーズのサポート	8.3(1)	フェールオーバー キーが、実行コンフィギュレーションとスタートアップ コンフィギュレーションの共有キーを暗号化するマスターパスフレーズをサポートするようになりました。一方のASAから他方に共有秘密をコピーする場合、たとえば、**more system:running-config** コマンドを使用して、正常に暗号化共有キーをコピーして貼り付けることができます。 （注） **failover key** の共有秘密は、**show running-config** の出力に ***** と表示されます。このマスクされたキーはコピーできません。 **failover key** [**0** | **8**] コマンドが変更されました。
フェールオーバーにIPv6のサポートが追加されました。	8.2(2)	次のコマンドが変更されました。**failover interface ip**、**show failover**、**ipv6 address**、**show monitor-interface**

機能名	リリース	機能情報
「同時」ブートアップ中のフェールオーバー グループのユニットの設定の変更。	9.0(1)	以前のバージョンのソフトウェアでは「同時」ブートアップが許可されていたため、フェールオーバー グループを優先ユニットでアクティブにする **preempt** コマンドは必要ありませんでした。しかし、この機能は、両方のフェールオーバー グループが最初に起動するユニットでアクティブになるように変更されました。
フェールオーバー リンクおよびステート リンクの通信を暗号化する IPsec LAN-to-LAN トンネルのサポート	9.1(2)	フェールオーバー キーに独自の暗号化を使用する代わりに（**failover key** コマンド）、フェールオーバー リンクおよびステート リンクの暗号化に IPsec LAN-to-LAN トンネルが使用できるようになりました。 （注） フェールオーバー LAN-to-LAN トンネルは、IPsec（その他の VPN）ライセンスには適用されません。 **failover ipsec pre-shared-key**、**show vpn-sessiondb** の各コマンドが導入または変更されました。
ハードウェア モジュールのヘルス モニタリングの無効化	9.3(1)	ASA はデフォルトで、インストール済みハードウェア モジュール（ASA FirePOWER モジュールなど）のヘルス モニタリングを行います。特定のハードウェア モジュールの障害によってフェールオーバーをトリガーすることが望ましくない場合は、モジュールのモニタリングをディセーブルにできます。 **monitor-interface service-module** コマンドが変更されました。

機能名	リリース	機能情報
フェールオーバーペアのスタンバイ装置またはスタンバイ コンテキストのコンフィギュレーション変更のロック	9.3(2)	通常のコンフィギュレーションの同期を除いてスタンバイ装置上で変更ができないように、スタンバイ装置（アクティブ/スタンバイ フェールオーバー）またはスタンバイ コンテキスト（アクティブ/アクティブ フェールオーバー）のコンフィギュレーション変更をロックできるようになりました。 **failover standby config-lock** コマンドが導入されました。



第 9 章

ASA クラスタ

クラスタリングを利用すると、複数の ASA をグループ化して 1 つの論理デバイスとすることができます。クラスタは、単一デバイスのすべての利便性（管理、ネットワークへの統合）を備える一方で、複数デバイスによって高いスループットおよび冗長性を達成します。

（注） 一部の機能は、クラスタリングを使用する場合、サポートされません。「クラスタリングでサポートされない機能 （330 ページ）」を参照してください。

ASA クラスタリングの概要

ここでは、クラスタリング アーキテクチャとその動作について説明します。

ASA クラスタをネットワークに適合させる方法

クラスタは、1 つのユニットとして機能する複数の ASA から構成されます。ASA をクラスタとして機能させるには、次のインフラストラクチャが必要です。

- クラスタ内通信用の、隔離された高速バックプレーン ネットワーク。クラスタ制御リンクと呼ばれます。
- 各 ASA への管理アクセス（コンフィギュレーションおよびモニタリングのため）。

クラスタをネットワーク内に配置するときは、クラスタが送受信するデータのロードバランシングを、アップストリームおよびダウンストリームのルータが次のいずれかの方法でできることが必要です。

- スパンド EtherChannel（推奨）：クラスタ内の複数のメンバのインターフェイスをグループ化して 1 つの EtherChannel とします。この EtherChannel がユニット間のロードバランシングを実行します。
- ポリシーベース ルーティング（ルーテッド ファイアウォール モードのみ）：アップストリームとダウンストリームのルータが、ルートマップと ACL を使用してユニット間のロード バランシングを実行します。
- 等コスト マルチパス ルーティング（ルーテッド ファイアウォール モードのみ）：アップストリームとダウンストリームのルータが、等コストのスタティックまたはダイナミックルートを使用してユニット間のロード バランシングを実行します。

パフォーマンス スケーリング係数

複数のユニットを結合して 1 つのクラスタとしたときに、期待できるパフォーマンスの概算値は次のようになります。

- 合計スループットの 70 %
- 最大接続数の 60 %
- 接続数/秒の 50 %

たとえば、スループットについては、ASA 5585-X と SSP-40 が処理できる実際のファイアウォール トラフィックは、単独動作時は約 10 Gbps となります。8 ユニットのクラスタでは、合計スループットの最大値は約 80 Gbps（8 ユニット x 10 Gbps）の 70 %、つまり 56 Gbps となります。

クラスタ メンバー

クラスタ メンバーは連携して動作し、セキュリティ ポリシーおよびトラフィック フローの共有を達成します。ここでは、各メンバーのロールの特長について説明します。

ブートストラップ コンフィギュレーション

各デバイスで、最小限のブートストラップ コンフィギュレーション（クラスタ名、クラスタ制御リンク インターフェイスなどのクラスタ設定）を設定します。クラスタリングを最初にイネーブルにしたユニットが一般的にはマスターユニットとなります。以降のユニットに対してクラスタリングをイネーブルにすると、そのユニットはスレーブとしてクラスタに参加します。

マスターおよびスレーブ ユニットの役割

クラスタ内のメンバの 1 つがマスター ユニットです。マスター ユニットは、ブートストラップ コンフィギュレーション内のプライオリティ設定によって決まります。プライオリティは1 ～ 100 の範囲内で設定され、1 が最高のプライオリティです。他のすべてのメンバはスレーブ ユニットです。一般的には、クラスタを作成した後で最初に追加したユニットがマスター ユニットとなります。これは単に、その時点でクラスタに存在する唯一のユニットであるからです。

すべてのコンフィギュレーション作業（ブートストラップ コンフィギュレーションを除く）は、マスターユニット上のみで実行する必要があります。コンフィギュレーションは、スレーブ ユニットに複製されます。物理的資産（たとえばインターフェイス）の場合は、マスターユニットのコンフィギュレーションがすべてのスレーブユニット上でミラーリングされます。たとえば、GigabitEthernet 0/1 を内部インターフェイスとして、GigabitEthernet 0/0 を外部インターフェイスとして設定した場合は、これらのインターフェイスはスレーブユニット上でも、内部および外部のインターフェイスとして使用されます。

機能によっては、クラスタ内でスケーリングしないものがあり、そのような機能についてはマスター ユニットがすべてのトラフィックを処理します。

マスター ユニット選定

クラスタのメンバは、クラスタ制御リンクを介して通信してマスターユニットを選定します。方法は次のとおりです。

1. ユニットに対してクラスタリングをイネーブルにしたとき（または、クラスタリングがイネーブル済みの状態でそのユニットを初めて起動したとき）に、そのユニットは選定要求を 3 秒間隔でブロードキャストします。
2. プライオリティの高い他のユニットがこの選定要求に応答します。プライオリティは 1 ～ 100 の範囲内で設定され、1 が最高のプライオリティです。
3. 45 秒経過しても、プライオリティの高い他のユニットからの応答を受信していない場合は、そのユニットがマスターになります。

（注） 最高のプライオリティを持つユニットが複数ある場合は、クラスタ ユニット名、次にシリアル番号を使用してマスターが決定されます。

4. 後からクラスタに参加したユニットのプライオリティの方が高い場合でも、そのユニットが自動的にマスター ユニットになることはありません。既存のマスター ユニットは常にマスターのままです。ただし、マスターユニットが応答を停止すると、その時点で新しいマスター ユニットが選定されます。

（注） 特定のユニットを手動で強制的にマスターにすることができます。中央集中型機能については、マスターユニット変更を強制するとすべての接続がドロップされるので、新しいマスターユニット上で接続を再確立する必要があります。

クラスタ インターフェイス

データインターフェイスは、スパンドEtherChannelとして設定することも、個別インターフェイスとして設定することもできます。1つのクラスタ内のすべてのデータインターフェイスのタイプが同一であることが必要です。詳細については、「クラスタインターフェイスについて（347ページ）」を参照してください。

クラスタ制御リンク

各ユニットの、少なくとも1つのハードウェアインターフェイスをクラスタ制御リンク専用とする必要があります。詳細については、「クラスタ制御リンクについて（348ページ）」を参照してください。

ASA クラスタ内のハイ アベイラビリティ

ASAクラスタリングは、ユニットとインターフェイスの正常性を監視し、ユニット間で接続状態を複製することにより、ハイ アベイラビリティを提供します。

ユニットのヘルス モニタリング

マスター ユニットは、各スレーブ ユニットをモニタするために、クラスタ制御リンクを介してキープアライブ メッセージを定期的に送信します（間隔は設定可能です）。各スレーブ ユニットは、同じメカニズムを使用してマスター ユニットをモニタします。ユニットの健全性チェックが失敗すると、ユニットはクラスタから削除されます。

インターフェイス モニタリング

各ユニットは、使用中のすべての指名されたハードウェア インターフェイスのリンク ステータスをモニタし、ステータス変更をマスター ユニットに報告します。

- スパンドEtherChannel：クラスタ Link Aggregation Control Protocol（cLACP）を使用します。各ユニットは、リンク ステータスおよびcLACPプロトコル メッセージをモニタして、ポートがまだEtherChannelでアクティブであるかどうかを判断します。ステータスがマスター ユニットに報告されます。
- 個別インターフェイス（ルーテッドモードのみ）：各ユニットが自身のインターフェイスを自己モニタし、インターフェイスのステータスをマスター ユニットに報告します。

ヘルス モニタリングをイネーブルにすると、すべての物理インターフェイス（主要な EtherChannel インターフェイスおよび冗長インターフェイスのタイプを含む）がデフォルトでモニタされるため、オプションでインターフェイスごとのモニタリングをディセーブルにすることができます。指名されたインターフェイスのみモニタできます。たとえば、指名された EtherChannel に障害が発生したと判断される必要がある場合、つまり、EtherChannel のすべてのメンバー ポートはクラスタ削除をトリガーすることに失敗する必要があります（最小ポート バンドリング設定に応じて）。

ユニットのモニタ対象のインターフェイスが失敗した場合、そのユニットはクラスタから削除されます。ASA がメンバーをクラスタから削除するまでの時間は、インターフェイスのタイプと、そのユニットが確立済みメンバーであるか、またはクラスタに参加しようとしているかによって異なります。EtherChannel の場合（スパニングかどうかを問わない）は、確立済みメンバーのインターフェイスがダウン状態のときに、ASA はそのメンバーを 9 秒後に削除します。ASA は、ユニットがクラスタに参加する最初の 90 秒間はインターフェイスを監視ししません。この間にインターフェイスのステータスが変化しても、ASA はクラスタから削除されません。非 EtherChannel の場合は、メンバー状態に関係なく、ユニットは 500 ミリ秒後に削除されます。

障害後のステータス

クラスタ内のユニットで障害が発生したときに、そのユニットでホスティングされている接続は他のユニットにシームレスに移管されます。トラフィック フローのステート情報は、クラスタ制御リンクを介して共有されます。

マスターユニットで障害が発生した場合は、そのクラスタの他のメンバーのうち、プライオリティが最高（番号が最小）のものがマスター ユニットになります。

障害イベントに応じて、ASA は自動的にクラスタへの再参加を試みます。

（注） ASA が非アクティブになり、クラスタへの自動再参加に失敗すると、すべてのデータ インターフェイスがシャットダウンされます。管理専用インターフェイスのみがトラフィックを送受信できます。 管理インターフェイスは、そのユニットがクラスタ IP プールから受け取った IP アドレスを使用して引き続き稼働状態となります。ただし、リロードする場合、クラスタでユニットがまだ非アクティブになっていると、管理インターフェイスはディセーブルになります。それ以降のコンフィギュレーション作業には、コンソール ポートを使用する必要があります。

クラスタへの再参加

クラスタ メンバがクラスタから削除された後、クラスタに再参加できる方法は、削除された理由によって異なります。

- クラスタ制御リンクの障害：クラスタ制御リンクの問題を解決した後、コンソールポートで **cluster group** *name* と入力してから **enable** と入力して、クラスタリングを再びイネーブルにすることによって、手動でクラスタに再参加する必要があります。

- データ インターフェイスの障害：ASA は自動的に最初は 5 分後、次に 10 分後、最終的に 20 分後に再参加を試みます。20 分後に参加できない場合、ASA はクラスタリングをディセーブルにします。データ インターフェイスの問題を解決した後、コンソール ポートで **cluster group** *name* と入力してから **enable** と入力して、クラスタリングを手動でイネーブルにする必要があります。
- ASA 5585-X 上の ASA FirePOWER モジュールの障害：ASA は自動的に 5 分後に再参加を試行します。
- ASA FirePOWE ソフトウェア モジュールの障害：モジュールの問題を解決した後、コンソール ポートで **cluster group** *name* と入力してから **enable** と入力して、手動でクラスタリングをイネーブルにする必要があります。
- ユニットの障害：ユニットがヘルスチェック失敗のためクラスタから削除された場合、クラスタへの再参加は失敗の原因によって異なります。たとえば、一時的な電源障害の場合は、クラスタ制御リンクが稼働していて、クラスタリングが **enable** コマンドでまだイネーブルになっているなら、ユニットは再起動するとクラスタに再参加することを意味します。ASA は 5 秒ごとにクラスタへの再参加を試みます。
- 内部エラー：内部の障害には、アプリケーション同期のタイムアウト、矛盾したアプリケーション ステータスなどがあります。 問題を解決したら、コンソール ポートで **cluster group** *name* と入力してから **enable** と入力することでクラスタリングを再び有効にして、クラスタに手動で再参加する必要があります。

マスター ユニットのブートストラップの設定 （370 ページ）を参照してください。

データ パス接続状態の複製

どの接続にも、1 つのオーナーおよび少なくとも 1 つのバックアップ オーナーがクラスタ内にあります。バックアップ オーナーは、障害が発生しても接続を引き継ぎません。代わりに、TCP/UDP のステート情報を保存します。これは、障害発生時に接続が新しいオーナーにシームレスに移管されるようにするためです。バックアップ オーナーは通常ディレクタでもあります。

トラフィックの中には、TCP または UDP レイヤよりも上のステート情報を必要とするものがあります。この種類のトラフィックに対するクラスタリングのサポートの可否については、次の表を参照してください。

表 *13*：クラスタ全体で複製される機能

Traffic	状態のサポート	注意
Up time	Yes	システム アップ タイムをトラッキングします。
ARP Table	Yes	トランスペアレント モードのみ。

Traffic	状態のサポート	注意
MAC アドレス テーブル	Yes	トランスペアレント モードのみ。
ユーザ アイデンティティ	Yes	AAA ルール（uauth）とアイデンティティ ファイアウォールが含まれます。
IPv6 ネイバー データベース	Yes	—
ダイナミック ルーティング	Yes	—
SNMP エンジン ID	なし	—
集中型 VPN（サイト間）	なし	VPN セッションは、マスター ユニットで障害が発生すると切断されます。

設定の複製

クラスタ内のすべてのユニットは、単一のコンフィギュレーションを共有します。コンフィギュレーション変更を加えることができるのはマスターユニット上だけであり、変更は自動的にクラスタ内の他のすべてのユニットに同期されます。

ASA クラスタ管理

ASA クラスタリングを使用することの利点の 1 つは、管理のしやすさです。ここでは、クラスタを管理する方法について説明します。

管理ネットワーク

すべてのユニットを単一の管理ネットワークに接続することを推奨します。このネットワークは、クラスタ制御リンクとは別のものです。

管理インターフェイス

管理インターフェイスについては、専用管理インターフェイスの 1 つを使用することを推奨します。管理インターフェイスは、個別インターフェイスとして設定することも（ルーテッド モードとトランスペアレント モードの両方）、スパンド EtherChannel インターフェイスとして設定することもできます。

管理用には、個別インターフェイスを使用することを推奨します（スパンド EtherChannel をデータインターフェイスに使用している場合でも）。個別インターフェイスならば、必要に応じて各ユニットに直接接続できますが、スパンド EtherChannel インターフェイスでは、現在のマスター ユニットへのリモート接続しかできません。

（注） スパンドEtherChannelインターフェイス モードを使用しているときに、管理インターフェイスを個別インターフェイスとして設定する場合は、管理インターフェイスに対してダイナミック ルーティングをイネーブルにすることはできません。スタティック ルートを使用する必要があります。

個別インターフェイスの場合は、メイン クラスタ IP アドレスはそのクラスタの固定アドレスであり、常に現在のマスターユニットに属します。インターフェイスごとに、管理者はアドレス範囲も設定します。これで、各ユニット（現在のマスターも含まれます）がその範囲内のローカル アドレスを使用できるようになります。このメイン クラスタ IP アドレスによって、管理アクセスのアドレスが一本化されます。マスター ユニットが変更されると、メイン クラスタ IP アドレスは新しいマスター ユニットに移動するので、クラスタの管理をシームレスに続行できます。ローカル IP アドレスは、ルーティングに使用され、トラブルシューティングにも役立ちます。

たとえば、クラスタを管理するにはメイン クラスタ IP アドレスに接続します。このアドレスは常に、現在のマスター ユニットに関連付けられています。個々のメンバを管理するには、ローカル IP アドレスに接続します。

TFTP や syslog などの発信管理トラフィックの場合、マスター ユニットを含む各ユニットは、ローカル IP アドレスを使用してサーバに接続します。

スパンド EtherChannel インターフェイスの場合は、IP アドレスは 1 つだけ設定でき、その IP アドレスは常にマスターユニットに関連付けられます。EtherChannelインターフェイスを使用してスレーブ ユニットに直接接続することはできません。管理インターフェイスは個別インターフェイスとして設定することを推奨します。各ユニットに接続できるようにするためです。デバイス ローカル EtherChannel を管理に使用できます。

マスター ユニット管理とスレーブ ユニット管理

すべての管理とモニタリングはマスター ユニットで実行できます。マスター ユニットから、すべてのユニットの実行時統計情報やリソース使用状況などのモニタリング情報を調べることができます。また、クラスタ内のすべてのユニットに対してコマンドを発行することや、コンソール メッセージをスレーブ ユニットからマスター ユニットに複製することもできます。

必要に応じて、スレーブ ユニットを直接モニタできます。マスター ユニットからでもできますが、ファイル管理をスレーブユニット上で実行できます（コンフィギュレーションのバックアップや、イメージの更新など）。次の機能は、マスター ユニットからは使用できません。

- ユニットごとのクラスタ固有統計情報のモニタリング。
- ユニットごとの Syslog モニタリング（コンソール レプリケーションが有効な場合にコンソールに送信される syslog を除く）。
- SNMP
- NetFlow

RSA キー複製

マスター ユニット上で RSA キーを作成すると、そのキーはすべてのスレーブ ユニットに複製されます。メイン クラスタ IP アドレスへの SSH セッションがある場合に、マスター ユニットで障害が発生すると接続が切断されます。新しいマスター ユニットは、SSH 接続に対して同じキーを使用するので、新しいマスターユニットに再接続するときに、キャッシュ済みの SSH ホスト キーを更新する必要はありません。

ASDM 接続証明書 IP アドレス不一致

デフォルトでは、自己署名証明書は、ローカル IP アドレスに基づいて ASDM 接続に使用されます。ASDM を使用してメイン クラスタ IP アドレスに接続する場合は、IP アドレス不一致に関する警告メッセージが表示されます。これは、証明書で使用されているのがローカル IP アドレスであり、メイン クラスタ IP アドレスではないからです。このメッセージは無視して、ASDM 接続を確立できます。ただし、この種の警告を回避するには、新しい証明書を登録し、この中でメイン クラスタ IP アドレスと、IP アドレス プールからのすべてのローカル IP アドレスを指定します。この証明書を各クラスタ メンバに使用します。

サイト間クラスタリング

サイト間インストールの場合、推奨されるガイドラインに従っていれば、ASA クラスタリングを活用できます。

各クラスタ シャーシを個別のサイト ID に属するように設定できます。

サイト ID は、サイト固有の MAC アドレスと連動します。クラスタから送信されたパケットは、サイト固有の MAC アドレスを使用するのに対し、クラスタで受信したパケットは、グローバル MAC アドレスを使用します。この機能により、MAC フラッピングの原因となる 2 つの異なるポートで両方のサイトから同じグローバル MAC アドレスをスイッチが学習するのを防止します。代わりに、スイッチはサイトの MAC アドレスのみを学習します。サイト固有の MAC アドレスは、スパンド EtherChannel のみを使用したルーテッド モードでサポートされます。

サイト間クラスタリングの詳細については、以下の項を参照してください。

- Data Center Interconnect のサイジング：ASA クラスタリングの要件と前提条件 （340 ページ）
- サイト間のガイドライン：ASA クラスタリングのガイドライン （342 ページ）
- サイト間での例：サイト間クラスタリングの例 （407 ページ）

ASA クラスタが接続を管理する方法

接続をクラスタの複数のメンバにロードバランスできます。接続のロールにより、通常動作時とハイ アベイラビリティ状況時の接続の処理方法が決まります。

接続のロール

接続ごとに定義された次のロールを参照してください。

- オーナー：通常、最初に接続を受信するユニット。オーナーは、TCP 状態を保持し、パケットを処理します。1 つの接続に対してオーナーは 1 つだけです。元のオーナーに障害が発生すると、新しいユニットが接続からパケットを受信したときにディレクタがこれらのユニットの新しいオーナーを選択します。

- バックアップ オーナー：オーナーから受信した TCP/UDP ステート情報を格納するユニット。これにより、障害が発生した場合に新しいオーナーにシームレスに接続を転送できます。バックアップ オーナーは、障害発生時に接続を引き継ぎません。オーナーが使用不可能になった場合は、その接続からパケットを受け取る最初のユニット（ロードバランシングに基づく）がバックアップ オーナーに問い合わせて、関連するステート情報を取得し、これでそのユニットが新しいオーナーになることができます。

  ディレクタ（下記参照）がオーナーと同じユニットでない限り、ディレクタはバックアップ オーナーでもあります。オーナーがディレクタとして自分自身を選択すると、別のバックアップ オーナーが選択されます。

- ディレクタ：フォワーダからのオーナールックアップ要求を処理するユニット。オーナーが新しい接続を受信すると、オーナーは、送信元/宛先 IP アドレスおよび ポートのハッシュに基づいてディレクタを選択し、新しい接続を登録するためにメッセージをそのディレクタに送信します。パケットがオーナー以外のユニットに到着した場合は、そのユニットはどのユニットがオーナーかをディレクタに問い合わせます。これで、パケットを転送できるようになります。1 つの接続に対してディレクタは 1 つだけです。ディレクタが失敗すると、オーナーは新しいディレクタを選択します。

  ディレクタがオーナーと同じユニットでない限り、ディレクタはバックアップ オーナーでもあります（上記参照）。オーナーがディレクタとして自分自身を選択すると、別のバックアップ オーナーが選択されます。

- フォワーダ：パケットをオーナーに転送するユニット。フォワーダが接続のパケットを受信したときに、その接続のオーナーが自分ではない場合は、フォワーダはディレクタにオーナーを問い合わせてから、そのオーナーへのフローを確立します。これは、この接続に関してフォワーダが受信するその他のパケット用です。ディレクタは、フォワーダにもなることができます。フォワーダが SYN-ACK パケットを受信した場合、フォワーダはパケットの SYN クッキーからオーナーを直接取得できるので、ディレクタに問い合わせる必要がないことに注意してください（TCP シーケンスのランダム化をディセーブ ルにした場合は、SYN Cookie は使用されないので、ディレクタへの問い合わせが必要です）。存続期間が短いフロー（たとえばDNSやICMP）の場合は、フォワーダは問い合わせの代わりにパケットを即座にディレクタに送信し、ディレクタがそのパケットをオーナーに送信します。1 つの接続に対して、複数のフォワーダが存在できます。最も効率的なスループットを実現できるのは、フォワーダが1つもなく、接続のすべてのパケットをオーナーが受信するという、優れたロードバランシング方法が使用されている場合です。

接続でポート アドレス変換（PAT）を使用すると、PAT のタイプ（per-session または multi-session）が、クラスタのどのメンバが新しい接続のオーナーになるかに影響します。

- Per-session PAT：オーナーは、接続の最初のパケットを受信するユニットです。

  デフォルトでは、TCP および DNS UDP トラフィックは per-session PAT を使用します。

- Multi-session PAT：オーナーは常にマスター ユニットです。multi-session PAT 接続がスレーブ ユニットで最初に受信される場合、スレーブ ユニットはその接続をマスター ユニットに転送します。

  デフォルトでは、UDP（DNS UDP を除く）および ICMP トラフィックは multi-session PAT を使用するので、これらの接続は常にマスター ユニットによって所有されています。

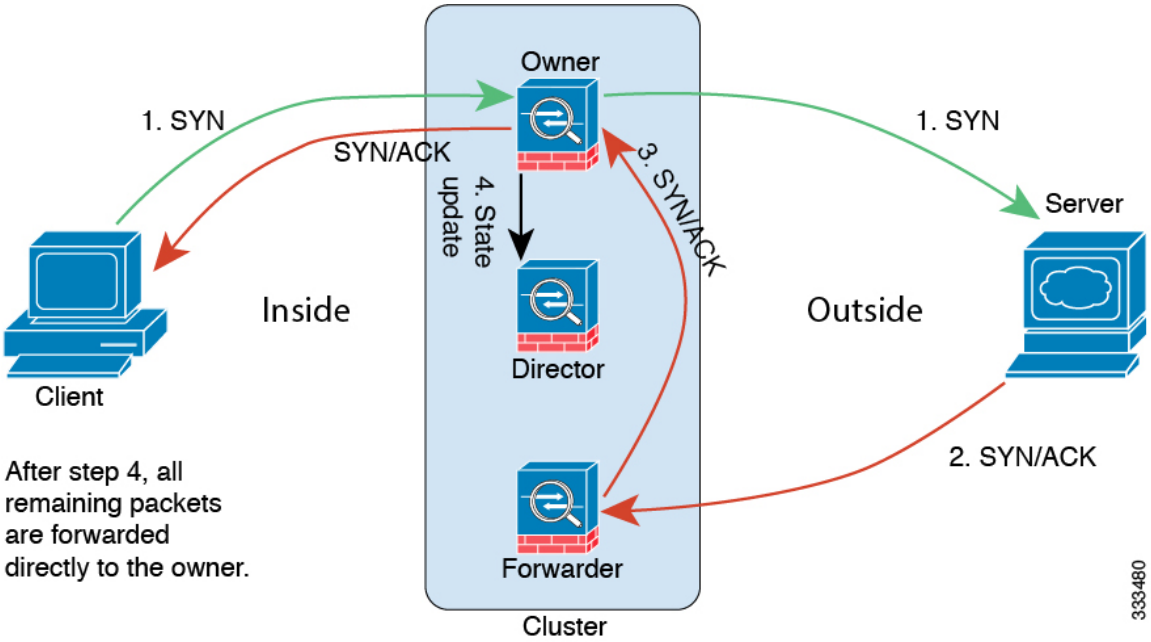
TCP および UDP の per-session PAT デフォルトを変更できるので、これらのプロトコルの接続は、その設定に応じて per-session または multi-session で処理されます。ICMP の場合は、デフォルトの multi-session PAT から変更することはできません。per-session PAT の詳細については、『ファイアウォールの構成ガイド』を参照してください。

新しい接続の所有権

新しい接続がロードバランシング経由でクラスタのメンバに送信される場合は、そのユニットがその接続の両方向のオーナーとなります。接続のパケットが別のユニットに到着した場合は、そのパケットはクラスタ制御リンクを介してオーナーユニットに転送されます。最適なパフォーマンスを得るには、適切な外部ロードバランシングが必要です。1 つのフローの両方向が同じユニットに到着するとともに、フローがユニット間に均等に分散されるようにするためです。逆方向のフローが別のユニットに到着した場合は、元のユニットにリダイレクトされます。

サンプル データ フロー

次の例は、新しい接続の確立を示します。



1. SYN パケットがクライアントから発信され、ASA の 1 つ（ロード バランシング方法に基づく）に配信されます。これがオーナーとなります。オーナーはフローを作成し、オーナー情報をエンコードして SYN Cookie を生成し、パケットをサーバに転送します。
2. SYN-ACK パケットがサーバから発信され、別の ASA（ロード バランシング方法に基づく）に配信されます。この ASA はフォワーダです。
3. フォワーダはこの接続を所有してはいないので、オーナー情報を SYN Cookie からデコードし、オーナーへの転送フローを作成し、SYN-ACK をオーナーに転送します。
4. オーナーはディレクタに状態アップデートを送信し、SYN-ACK をクライアントに転送します。
5. ディレクタは状態アップデートをオーナーから受信し、オーナーへのフローを作成し、オーナーと同様に TCP ステート情報を記録します。ディレクタは、この接続のバックアップ オーナーとしての役割を持ちます。
6. これ以降、フォワーダに配信されたパケットはすべて、オーナーに転送されます。
7. パケットがその他のユニットに配信された場合は、そのユニットはディレクタに問い合わせてオーナーを特定し、フローを確立します。
8. フローの状態が変化した場合は、状態アップデートがオーナーからディレクタに送信されます。

新しい TCP 接続のクラスタ全体での再分散

アップストリームまたはダウンストリーム ルータによるロード バランシングの結果として、フロー分散に偏りが生じた場合は、新しい TCP フローを過負荷のユニットから他のユニットにリダイレクトするように設定できます。既存のフローは他のユニットには移動されません。

ASA の各機能とクラスタリング

ASA の一部の機能は ASA クラスタリングではサポートされず、一部はマスター ユニットだけでサポートされます。その他の機能については適切な使用に関する警告がある場合があります。

クラスタリングでサポートされない機能

これらの機能は、クラスタリングがイネーブルのときは設定できず、コマンドは拒否されます。

- TLS プロキシを使用するユニファイド コミュニケーション機能
- リモート アクセス VPN（SSL VPN および IPSec VPN）
- 次のアプリケーション インスペクション：
  - CTIQBE
  - GTP

- H323、H225、および RAS
- IPsec パススルー
- MGCP
- MMP
- RTSP
- SCCP（Skinny）
- WAAS
- WCCP

- Botnet Traffic Filter
- Auto Update Server
- DHCP クライアント、サーバ、およびプロキシDHCP リレーがサポートされている。
- VPN ロード バランシング
- フェールオーバー
- ASA CX モジュール
- デッド接続検出（DCD）

クラスタリングの中央集中型機能

次の機能は、マスターユニット上だけでサポートされます。クラスタの場合もスケーリングされません。たとえば、8ユニットから成るクラスタがあるとします（5516-X）。その他の VPN ライセンスでは、1 つの ASA 5516-X に対して最大 300 のサイト間 IPsec トンネルが許可されますが、8 ユニットのクラスタ全体では、300 トンネルのみ使用できます。この機能は拡張されません。

（注） 中央集中型機能のトラフィックは、クラスタ制御リンク経由でメンバ ユニットからマスター ユニットに転送されます。

再分散機能を使用する場合は、中央集中型機能のトラフィックが中央集中型機能として分類される前に再分散が行われて、マスター以外のユニットに転送されることがあります。この場合は、トラフィックがマスター ユニットに送り返されます。

中央集中型機能については、マスターユニットで障害が発生するとすべての接続がドロップされるので、新しいマスター ユニット上で接続を再確立する必要があります。

- サイト間 VPN
- 次のアプリケーション インスペクション：
  - DCERPC

- ESMTP
- IM
- NetBIOS
- PPTP
- RADIUS
- RSH
- SNMP
- SQLNET
- SUNRPC
- TFTP
- XDMCP

- ダイナミック ルーティング（スパンド EtherChannel モードのみ）
- マルチキャスト ルーティング（個別インターフェイス モードのみ）
- スタティック ルート モニタリング
- IGMP マルチキャスト コントロール プレーン プロトコル処理（データ プレーン フォワーディングはクラスタ全体に分散されます）
- PIM マルチキャスト コントロール プレーン プロトコル処理（データ プレーン転送はクラスタ全体に分散されます）
- ネットワーク アクセスの認証および許可。アカウンティングは非集中型です。
- フィルタリング サービス

個々のユニットに適用される機能

これらの機能は、クラスタ全体またはマスター ユニットではなく、各 ASA ユニットに適用されます。

- QoS：QoS ポリシーは、コンフィギュレーション複製の一部としてクラスタ全体で同期されます。ただし、ポリシーは、各ユニットに対して個別に適用されます。たとえば、出力に対してポリシングを設定する場合は、適合レートおよび適合バースト値は、特定の ASA から出て行くトラフィックに適用されます。3 ユニットから成るクラスタがあり、トラフィックが均等に分散している場合は、適合レートは実際にクラスタのレートの 3 倍になります。
- 脅威検出：脅威検出は、各ユニットに対して個別に機能します。たとえば、上位統計情報は、ユニット別です。たとえば、ポート スキャン検出が機能しないのは、スキャン トラフィックが全ユニット間で分散されるので、1 つのユニットがすべてのトラフィックを読み取ることはないからです。

- リソース管理：マルチ コンテキスト モードでのリソース管理は、ローカル使用状況に基づいて各ユニットに個別に適用されます。
- ASA Firepowerモジュール：ASA Firepowerモジュール間でのコンフィギュレーションの同期や状態の共有は行われません。Firepower Management Center を使用して、クラスタ内の ASA Firepower モジュールで一貫したポリシーを保持する必要があります。クラスタ内のデバイスに異なる ASA インターフェイスベースのゾーン定義を使用しないでください。
- ASA IPS モジュール：IPS モジュール間でのコンフィギュレーションの同期や状態の共有は行われません。IPS シグニチャによっては、IPS が複数の接続にわたって状態を保持することが必要になります。たとえば、ポート スキャン シグニチャが使用されるのは、同じ人物が同じサーバへの多数の接続を、それぞれ異なるポートを使用して開いていることをIPSモジュールが検出した場合です。クラスタリングでは、これらの接続は複数のASAデバイス間で分散されます。これらのデバイスそれぞれに専用のIPSモジュールがあります。これらの IPS モジュールはステート情報を共有しないので、結果としてのポート スキャンをクラスタが検出できない場合があります。

ネットワーク アクセス用の AAA とクラスタリング

ネットワーク アクセス用の AAA は、認証、許可、アカウンティングの 3 つのコンポーネントで構成されます。認証および許可は、クラスタリング マスター上で中央集中型機能として実装されており、データ構造がクラスタ スレーブに複製されます。マスターが選定されたときは、確立済みの認証済みユーザおよびユーザに関連付けられた許可を引き続き中断なく運用するのに必要なすべての情報を、新しいマスターが保有します。ユーザ認証のアイドルおよび絶対タイムアウトは、マスター ユニット変更が発生したときも維持されます。

アカウンティングは、クラスタ内の分散型機能として実装されています。アカウンティングはフロー単位で実行されるので、フローを所有するクラスタ ユニットがアカウンティング開始と停止のメッセージを AAA サーバに送信します（フローに対するアカウンティングが設定されているとき）。

FTP とクラスタリング

- FTPデータ チャネルとコントロール チャネルのフローがそれぞれ別のクラスタ メンバによって所有されている場合は、データ チャネルのオーナーは定期的にアイドル タイムアウト アップデートをコントロール チャネルのオーナーに送信し、アイドル タイムアウト値を更新します。ただし、コントロール フローのオーナーがリロードされて、コントロール フローが再ホスティングされた場合は、親子フロー関係は維持されなくなります。したがって、コントロール フローのアイドル タイムアウトは更新されません。
- FTP アクセスに AAA を使用している場合、制御チャネルのフローはマスター ユニットに集中化されます。

アイデンティティ ファイアウォールとクラスタリング

マスター ユニットのみが AD から user-group を取得し、AD エージェントから user-ip マッピングを取得します。マスターユニットからユーザ情報がスレーブに渡されるので、スレーブは、セキュリティ ポリシーに基づいてユーザ ID の一致の決定を行うことができます。

マルチキャスト ルーティングとクラスタリング

マルチキャスト ルーティングは、インターフェイス モードによって動作が異なります。

スパンド EtherChannel モードでのマルチキャスト ルーティング

スパンド EtherChannel モードでは、ファースト パス転送が確立されるまでの間、マスター ユニットがすべてのマルチキャスト ルーティング パケットとデータ パケットを処理します。接続が確立された後は、各スレーブがマルチキャスト データ パケットを転送できます。

個別インターフェイス モードでのマルチキャスト ルーティング

個別インターフェイスモードでは、マルチキャストに関してユニットが個別に動作することはありません。データおよびルーティングのパケットはすべてマスターユニットで処理されて転送されるので、パケット レプリケーションが回避されます。

NAT とクラスタリング

NAT は、クラスタの全体的なスループットに影響を与えることがあります。着信および発信の NAT パケットが、クラスタ内のそれぞれ別の ASA に送信されることがあります。これは、ロードバランシング アルゴリズムは IP アドレスとポートに依存していますが、NAT が使用される場合、着信と発信でパケットの IP アドレスやポートが異なるためです。NAT オーナーではない ASA に到着したパケットは、クラスタ制御リンクを介してオーナーに転送されるので、大量のトラフィックがクラスタ制御リンク上で発生します。NAT オーナーはセキュリティおよびポリシーチェックの結果に応じてパケットの接続を作成するため、受信側ユニットは転送フローをオーナーに作成しません。

それでもクラスタリングで NAT を使用する場合は、次のガイドラインを考慮してください。

- プロキシ ARP なし：個別インターフェイスの場合は、マッピング アドレスについてプロキシ ARP 応答が送信されることはありません。これは、クラスタに存在しなくなった可能性のある ASA と隣接ルータとがピア関係を維持することを防ぐためです。アップストリーム ルータは、メイン クラスタ IP アドレスを指すマッピング アドレスについてはスタティック ルートまたは PBR とオブジェクト トラッキングを使用する必要があります。これは、スパンド EtherChannel の問題ではありません。クラスタ インターフェイスには関連付けられた IP アドレスが 1 つしかないためです。
- 個別インターフェイスのインターフェイス PAT なし：インターフェイス PAT は、個別インターフェイスではサポートされていません。
- ダイナミック PAT 用 NAT プール アドレス分散：マスター ユニットは、アドレスをクラスタ全体に均等に分配します。メンバーが接続を受信したときに、そのメンバーのアドレスが 1 つも残っていない場合は、接続はドロップされます（他のメンバーにはまだ使用可

能なアドレスがある場合でも）。最低でも、クラスタ内のユニットと同数の NAT アドレスが含まれていることを確認してください。各ユニットが確実に 1 つのアドレスを受け取るようにするためです。アドレス割り当てを表示するには、**show nat pool cluster** コマンドを使用します。

- ラウンドロビンなし：PAT プールのラウンドロビンは、クラスタリングではサポートされません。
- マスターユニットによって管理されるダイナミック NAT xlate：マスターユニットが xlate テーブルを維持し、スレーブ ユニットに複製します。ダイナミック NAT を必要とする接続をスレーブ ユニットが受信したときに、その xlate がテーブル内にない場合は、スレーブはマスター ユニットに xlate を要求します。スレーブ ユニットが接続を所有します。
- Per-session PAT 機能：クラスタリングに限りませんが、Per-session PAT 機能によって PAT のスケーラビリティが向上します。クラスタリングの場合は、各スレーブユニットが独自の PAT 接続を持てるようになります。対照的に、Multi-Session PAT 接続はマスターユニットに転送する必要があり、マスターユニットがオーナーとなります。デフォルトでは、すべての TCP トラフィックおよび UDP DNS トラフィックは per-session PAT xlate を使用します。これに対し、ICMP および他のすべての UDP トラフィックは multi-session を使用します。TCP および UDP に対しこれらのデフォルトを変更するように per-session NAT ルールを設定できますが、ICMP に per-session PAT を設定することはできません。H.323、SIP、または Skinny などの multi-session PAT のメリットを活用できるトラフィックでは、関連付けられている TCP ポートに対し per-session PAT を無効にできます（それらの H.323 および SIP の UDP ポートはデフォルトですでに multi-session になっています）。per-session PAT の詳細については、『ファイアウォールの構成ガイド』を参照してください。
- 次のインスペクション用のスタティック PAT はありません。
  - FTP
  - PPTP
  - RSH
  - SQLNET
  - TFTP
  - XDMCP
  - SIP

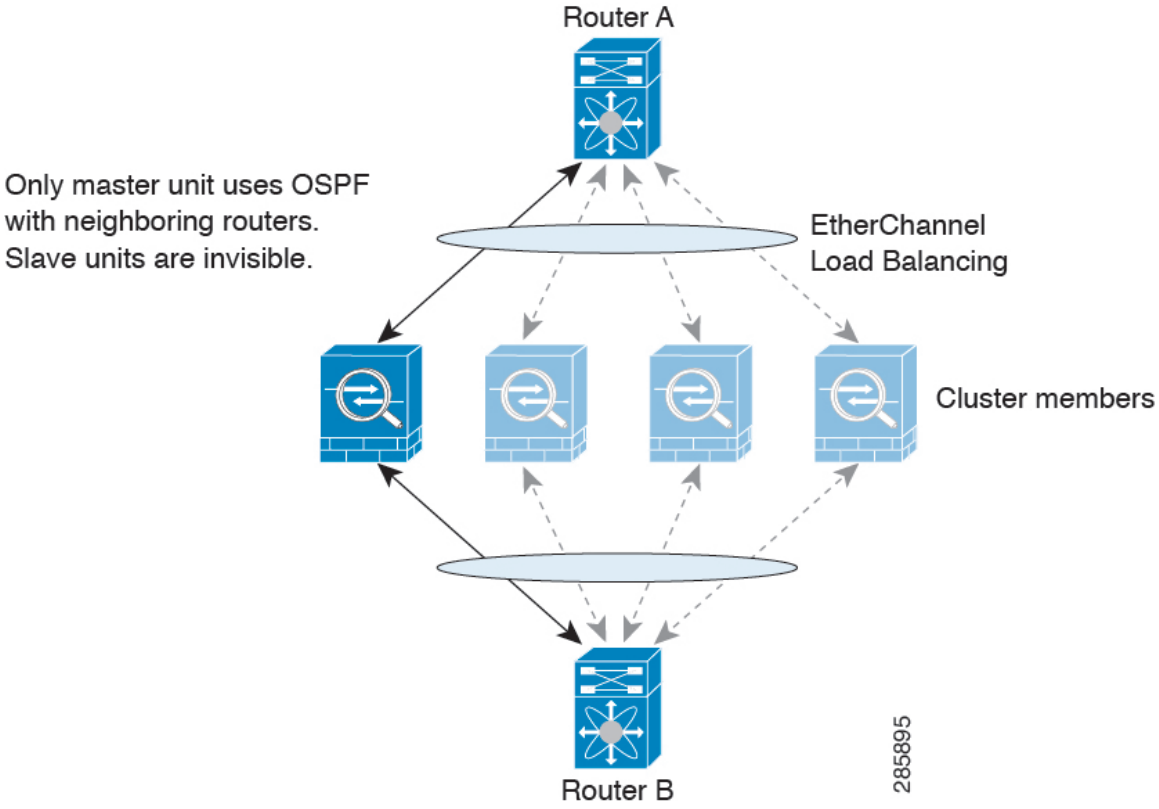
ダイナミック ルーティングおよびクラスタリング

ここでは、クラスタリングでダイナミック ルーティングを使用する方法について説明します。

スパンド EtherChannel モードでのダイナミック ルーティング

スパンド EtherChannel モード：ルーティング プロセスはマスター ユニット上だけで実行されます。ルートはマスターユニットを介して学習され、スレーブに複製されます。ルーティングパケットがスレーブに到着した場合は、マスター ユニットにリダイレクトされます。

図 *46 :* スパンド *EtherChannel* モードでのダイナミック ルーティング



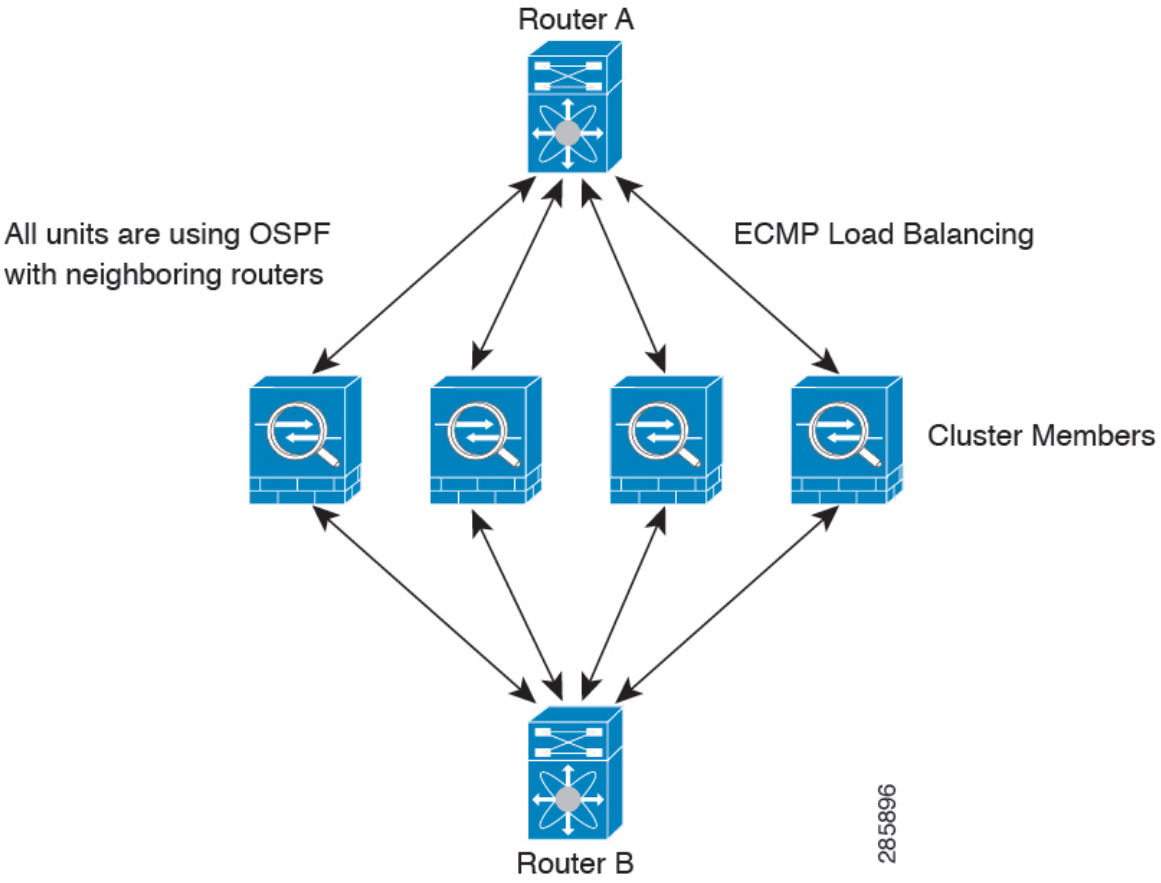
スレーブ メンバがマスター ユニットからルートを学習した後は、各ユニットが個別に転送に関する判断を行います。

OSPF LSA データベースは、マスター ユニットからスレーブ ユニットに同期されません。マスターユニットのスイッチオーバーが発生した場合は、隣接ルータが再起動を検出します。スイッチオーバーは透過的ではありません。OSPF プロセスが IP アドレスの 1 つをルータ ID として選択します必須ではありませんが、スタティック ルータ ID を割り当てることができます。これで、同じルータ ID がクラスタ全体で使用されるようになります。割り込みを解決するには、OSPF ノンストップ フォワーディング機能を参照してください。

個別インターフェイス モードでのダイナミック ルーティング

個別インターフェイス モードでは、各ユニットがスタンドアロン ルータとしてルーティング プロトコルを実行します。ルートの学習は、各ユニットが個別に行います。

図 *47* : 個別インターフェイス モードでのダイナミック ルーティング



上の図では、ルータ A はルータ B への等コスト パスが 4 本あることを学習します。パスはそれぞれ 1 つの ASA を通過します。ECMP を使用して、4 パス間でトラフィックのロード バランシングを行います。各 ASA は、外部ルータと通信するときに、それぞれ異なるルータ ID を選択します。

管理者は、各ユニットが別のルータ ID を使用できるように、ルータ ID のクラスタ プールを設定する必要があります。

EIGRP は、個別のインターフェイス モードのクラスタ ピアとのネイバー関係を形成しません。

（注） 冗長性の目的で、クラスタに同じルータへの複数の隣接関係がある場合、非対称ルーティングは許容できないトラフィック損失の原因となる可能性があります。非対称ルーティングを避けるためには、同じトラフィック ゾーンにこれらすべての ASA インターフェイスをまとめます。トラフィック ゾーンの設定 （573 ページ）を参照してください。

SIP インスペクションとクラスタリング

制御フローは、任意のユニットで作成できます（ロードバランシングのため）。その子データフローは同じユニットに存在する必要があります。

TLS プロキシ設定はサポートされていません。

SNMP とクラスタリング

SNMP エージェントは、個々の ASA を、そのローカル IP アドレスによってポーリングします。クラスタの統合データをポーリングすることはできません。

SNMP ポーリングには、メイン クラスタ IP アドレスではなく、常にローカル アドレスを使用してください。SNMP エージェントがメイン クラスタ IP アドレスをポーリングする場合は、新しいマスターが選定されたときに、新しいマスター ユニットのポーリングに失敗します。

syslog および NetFlow とクラスタリング

- Syslog：クラスタの各ユニットは自身の syslog メッセージを生成します。各ユニットの syslog メッセージ ヘッダー フィールドで使用されるデバイス ID を同一にするか、別にするかを設定できます。たとえば、ホスト名コンフィギュレーションはクラスタ内のすべてのユニットに複製されて共有されます。ホスト名をデバイス ID として使用するようにロギングを設定した場合は、どのユニットで生成された syslog メッセージも 1 つのユニットからのように見えます。クラスタ ブートストラップ コンフィギュレーションで割り当てられたローカル ユニット名をデバイス ID として使用するようにロギングを設定した場合は、syslog メッセージはそれぞれ別のユニットからのように見えます。
- NetFlow：クラスタの各ユニットは自身の NetFlow ストリームを生成します。NetFlow コレクタは、各 ASA を独立した NetFlow エクスポータとしてのみ扱うことができます。

Cisco TrustSec とクラスタリング

マスター ユニットだけがセキュリティ グループ タグ（SGT）情報を学習します。マスター ユニットからこの SGT がスレーブに渡されるので、スレーブは、セキュリティ ポリシーに基づいて SGT の一致決定を下せます。

VPN とクラスタリング

サイトツーサイト VPN は、中央集中型機能です。マスターユニットだけが VPN 接続をサポートします。分散型サイト間 VPN クラスタリングがサポートされています。詳細については、この pdf のハイ アベイラビリティ オプションを検索してください。

（注） リモート アクセス VPN は、クラスタリングではサポートされません。

VPN 機能を使用できるのはマスター ユニットだけであり、クラスタのハイ アベイラビリティ能力は活用されません。マスター ユニットで障害が発生した場合は、すべての既存の VPN 接

続が失われ、VPNユーザにとってはサービスの中断となります。新しいマスターが選定されたときに、VPN 接続を再確立する必要があります。

VPN トンネルをスパンドEtherChannelアドレスに接続すると、接続が自動的にマスターユニットに転送されます。PBR または ECMP を使用するときの個別インターフェイスへの接続については、ローカル アドレスではなく、常にメイン クラスタ IP アドレスに接続する必要があります。

VPN 関連のキーと証明書は、すべてのユニットに複製されます。

ASA クラスタリングのライセンス

クラスタ ユニットは、各ユニット上で同じライセンスを必要としません。一般的には、マスター ユニット用のライセンスのみを購入します。スレーブ ユニットはマスターのライセンスを継承します。複数のユニットにライセンスがある場合は、これらが統合されて単一の実行 ASA クラスタ ライセンスとなります。

このルールには、例外があります。クラスタリングの正確なライセンス要件については、次の表を参照してください。

モデル	ライセンス要件
ASA 5585-X	クラスタ ライセンス、最大 16 ユニットをサポートします。 （注） 各ユニットに、同じ暗号化ライセンスが必要です。各ユニットに同じ 10 GE I/O/Security Plus ライセンスが必要です（ASA 5585-X と SSP-10 および SSP-20）。
ASA 5512-X	Security Plus ライセンス、2 ユニットをサポートします。 （注） 各ユニットに同じ暗号化ライセンスが必要です。
ASA 5515-X、ASA 5525-X、ASA 5545-X、ASA 5555-X	基本ライセンス、2 ユニットをサポートします。 （注） 各ユニットに同じ暗号化ライセンスが必要です。
Firepower 9300 シャーシ	Firepower 9300 シャーシ 上の ASA の ASA クラスタ ライセンス （139 ページ）を参照してください。
他のすべてのモデル	サポートしない

ASA クラスタリングの要件と前提条件

モデルの要件

- ASA 5512-X、5515-X、5525-X、5545-X、および 5555-X：最大 2 ユニット
- ASA 5585 X：最大 16 ユニット

  ASA 5585-X と SSP-10 および SSP-20（2 個の 10 ギガビット イーサネット インターフェイスを持つ）については、一方のインターフェイスをクラスタ制御リンクに使用し、他方をデータに使用することを推奨します（データについてはサブインターフェイスを使用できます）。この設定は、クラスタ制御リンクの冗長性には対応しませんが、クラスタ制御リンクのサイズをデータ インターフェイスのサイズと一致させるという要件は満たされます。

- ASA FirePOWER モジュール：ASA FirePOWER モジュールはクラスタリングを直接サポートしていませんが、クラスタ内でこれらのモジュールを使用できます。クラスタ内の ASA FirePOWER モジュールで一貫したポリシーを保持する必要があります。

（注） ASA FirePOWER モジュールを設定する前に、クラスタを作成します。モジュールがスレーブ デバイスにすでに設定されている場合、クラスタにこれらを追加する前に、デバイスのインターフェイスの設定をクリアします。CLI から **clear configure interface** コマンドを入力します。

ASA のハードウェアおよびソフトウェア要件

クラスタ内のすべてのユニット：

- 同じ DRAM を使用する同じモデルである必要があります。フラッシュ メモリの容量は同一である必要はありません。
- イメージアップグレード時を除き、同じソフトウェアを実行する必要があります。ヒットレス アップグレードがサポートされます。
- セキュリティ コンテキスト モードが一致している必要があります（シングルまたはマルチ）。
- （シングル コンテキスト モード）ファイアウォール モードが一致している必要があります（ルーテッドまたはトランスペアレント）。
- コンフィギュレーション複製前の初期クラスタ制御リンク通信のために、新しいクラスタ メンバは、マスター ユニットと同じ SSL 暗号化設定（**ssl encryption** コマンド）を使用する必要があります。

- 同じクラスタライセンス、暗号化ライセンス、そして ASA 5585-X の場合は 10 GE I/O ライセンスが必要です。

スイッチ要件

- ASA でクラスタリングを設定する前に、スイッチのコンフィギュレーションを完了する必要があります。
- サポートされているスイッチのリストについては、『Cisco ASA Compatibility』[英語] を参照してください。

ASA の要件

- ユニットを管理ネットワークに追加する前に、一意の IP アドレスを各ユニットに提供します。
  - ASA への接続および管理 IP アドレスの設定に関する詳細については、「使用する前に」の章を参照してください。
  - マスター装置（通常は最初にクラスタに追加された装置）で使用される IP アドレスを除き、これらの管理 IP アドレスは一時的に使用されるだけです。
  - スレーブがクラスタに参加すると、管理インターフェイス設定はマスター装置からの複製に置き換えられます。
- クラスタ制御リンクでジャンボフレームを使用する場合は（推奨）、クラスタリングをイネーブルにする前に、ジャンボ フレームの予約をイネーブルにする必要があります。

サイト間クラスタリング用の Data Center Interconnect のサイジング

次の計算と同等の帯域幅をクラスタ制御リンク トラフィック用に Data Center Interconnect（DCI）に確保する必要があります。

$$\frac{\#\text{ of cluster members per site}}{2} \times \text{cluster control link size per member}$$

メンバの数が各サイトで異なる場合、計算には大きい方の値を使用します。DCI の最小帯域幅は、1 つのメンバに対するクラスタ制御リンクのサイズ未満にすることはできません。

次に例を示します。

- 4 サイトの 2 メンバの場合。
  - 合計 4 クラスタ メンバ
  - 各サイト 2 メンバ
  - メンバあたり 5 Gbps クラスタ制御リンク

  予約する DCI 帯域幅 = 5 Gbps（2/2 x 5 Gbps）。

- 3 サイトの 6 メンバの場合、サイズは増加します。
  - 合計 6 クラスタ メンバ
  - サイト 1 は 3 メンバ、サイト 2 は 2 メンバ、サイト 3 は 1 メンバ
  - メンバあたり 10 Gbps クラスタ制御リンク

  予約する DCI 帯域幅 = 15 Gbps（3/2 x 10 Gbps）。
- 2 サイトの 2 メンバの場合。
  - 合計 2 クラスタ メンバ
  - 各サイト 1 メンバ
  - メンバあたり 10 Gbps クラスタ制御リンク

  予約する DCI 帯域幅 = 10 Gbps（1/2 x 10 Gbps = 5 Gbps、ただし最小帯域幅がクラスタ制御リンク（10 Gbps）のサイズ未満になってはなりません）。

その他の要件

ターミナル サーバを使用して、すべてのクラスタ メンバ ユニットのコンソール ポートにアクセスすることをお勧めします。初期設定および継続的な管理（ユニットがダウンしたときなど）では、ターミナル サーバがリモート管理に役立ちます。

ASA クラスタリングのガイドライン

コンテキスト モード

モードは、各メンバー ユニット上で一致している必要があります。

ファイアウォール モード

シングル モードの場合、ファイアウォール モードがすべてのユニットで一致している必要があります。

フェールオーバー

フェールオーバーは、クラスタリングではサポートされません。

IPv6

クラスタ制御リンクは、IPv4 のみを使用してサポートされます。

スイッチ

- ASR 9006 では、非デフォルト MTU を設定する場合は、ASR インターフェイス MTU をクラスタ デバイス MTU より 14 バイト大きく設定します。そうしないと、**mtu-ignore** オプ

ションを使用しない限り、OSPF 隣接関係（アジャセンシー）ピアリングの試行が失敗する可能性があります。クラスタ デバイス MTU は、ASR *IPv4* MTU と一致する必要があります。

- クラスタ制御リンク インターフェイスのスイッチでは、クラスタ ユニットに接続されるスイッチ ポートに対してスパニングツリー PortFast をイネーブルにすることもできます。このようにすると、新規ユニットの参加プロセスを高速化できます。
- スイッチ上のスパンド EtherChannel のバンドリングが遅いときは、スイッチの個別インターフェイスに対して LACP 高速レートをイネーブルにできます。Nexus シリーズなど一部のスイッチでは、インサービス ソフトウェア アップグレード（ISSU）を実行する際に LACP 高速レートがサポートされないことに注意してください。そのため、クラスタリングで ISSU を使用することは推奨されません。
- スイッチでは、EtherChannel ロードバランシング アルゴリズム **source-dest-ip** または **source-dest-ip-port**（Cisco Nexus OS および Cisco IOS の **port-channel load-balance** コマンドを参照）を使用することをお勧めします。クラスタのデバイスにトラフィックを不均一に配分する場合があるので、ロード バランス アルゴリズムでは **vlan** キーワードを使用しないでください。クラスタデバイスのデフォルトのロードバランシング アルゴリズムは変更しないでください。
- スイッチの EtherChannel ロードバランシング アルゴリズムを変更すると、スイッチの EtherChannel インターフェイスは一時的にトラフィックの転送を停止し、スパニングツリー プロトコルが再始動します。トラフィックが再び流れ出すまでに、少し時間がかかります。
- 一部のスイッチは、LACP でのダイナミック ポート プライオリティをサポートしていません（アクティブおよびスタンバイ リンク）。ダイナミック ポート プライオリティを無効にすることで、スパンド EtherChannel との互換性を高めることができます。
- クラスタ制御リンク パスのスイッチでは、L4 チェックサムを検証しないようにする必要があります。クラスタ制御リンク経由でリダイレクトされたトラフィックには、正しい L4 チェックサムが設定されていません。L4 チェックサムを検証するスイッチにより、トラフィックがドロップされる可能性があります。
- ポートチャネル バンドルのダウンタイムは、設定されているキープアライブ インターバルを超えてはなりません。
- Supervisor 2T EtherChannel では、デフォルトのハッシュ配信アルゴリズムは適応型です。VSS 設計での非対称トラフィックを避けるには、クラスタ デバイスに接続されているポートチャネルでのハッシュ アルゴリズムを固定に変更します。

  router(config)# **port-channel** *id* **hash-distribution fixed**

  アルゴリズムをグローバルに変更しないでください。VSS ピア リンクに対しては適応型アルゴリズムを使用できます。

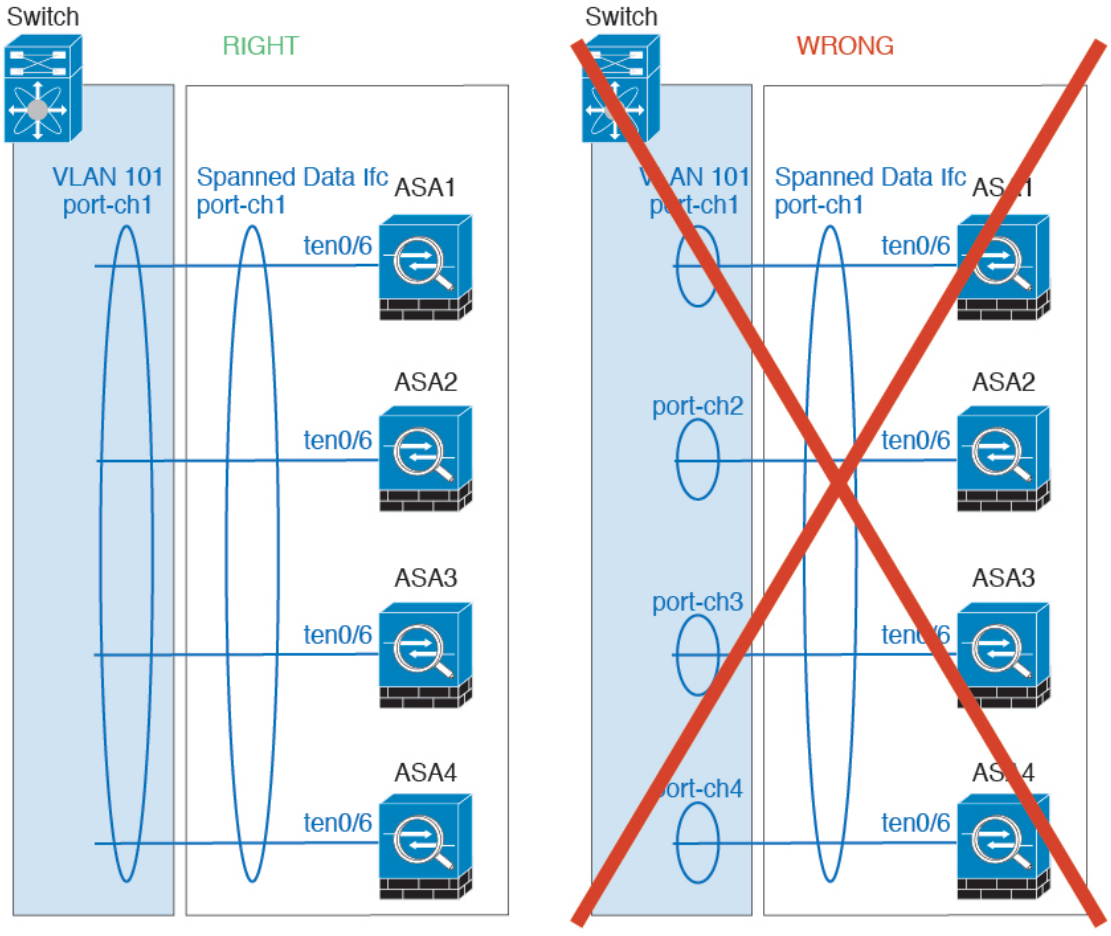
- Cisco Nexus スイッチのクラスタに接続されたすべての EtherChannel インターフェイスで、LACP グレースフル コンバージェンス機能をディセーブルにする必要があります。

EtherChannel

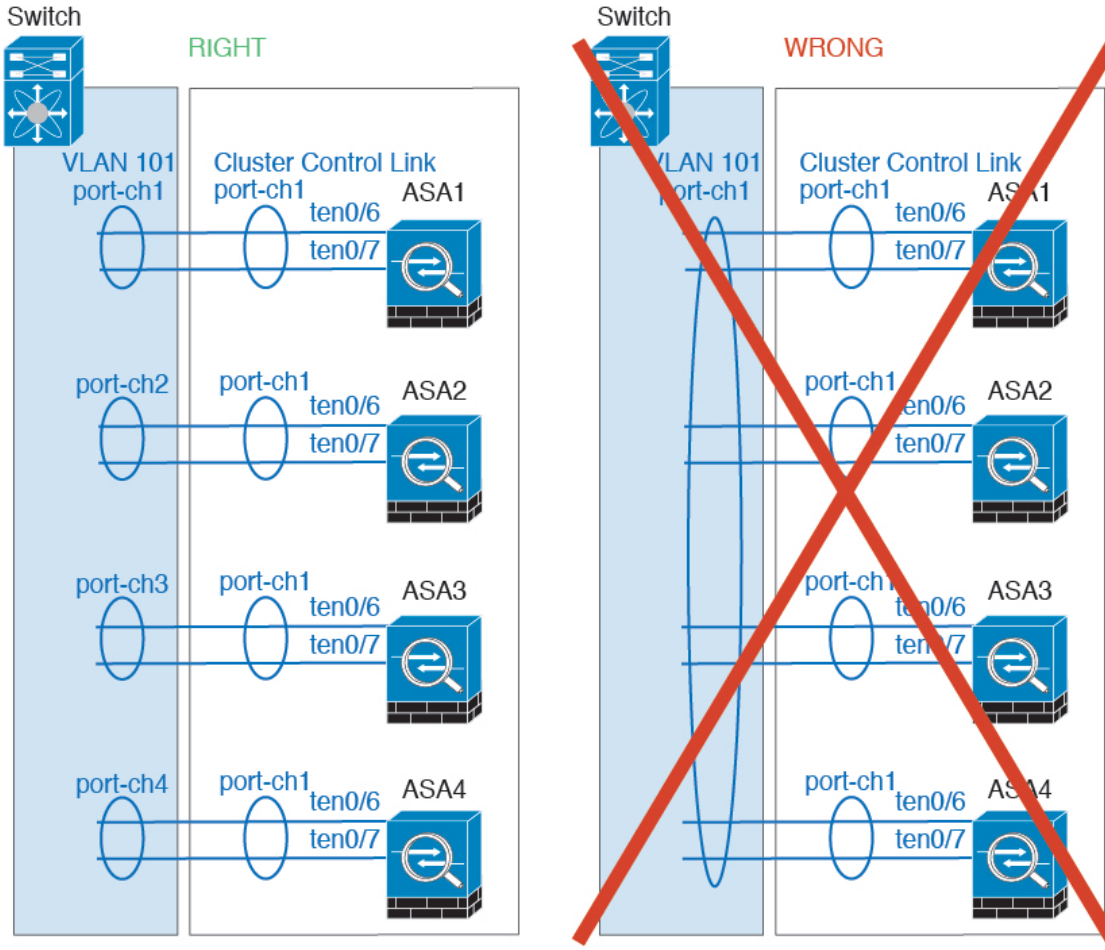
- 15.1(1)S2 より前の Catalyst 3750-X Cisco IOS ソフトウェア バージョンでは、クラスタ ユニットはスイッチ スタックに EtherChannel を接続することをサポートしていませんでした。デフォルトのスイッチ設定では、クラスタ ユニット EtherChannel がクロス スタックに接続されている場合、マスター スイッチの電源がオフになると、残りのスイッチに接続されている EtherChannel は起動しません。互換性を高めるため、**stack-mac persistent timer** コマンドを設定して、十分なリロード時間を確保できる大きな値、たとえば 8 分、0（無制限）などを設定します。または、15.1(1)S2 など、より安定したスイッチ ソフトウェア バージョンにアップグレードできます。

- スパンド EtherChannel とデバイス ローカル EtherChannel のコンフィギュレーション：スパンド EtherChannel と デバイス ローカル EtherChannel に対してスイッチを適切に設定します。

  - スパンド EtherChannel：クラスタ ユニット スパンド EtherChannel（クラスタのすべてのメンバに広がる）の場合は、複数のインターフェイスが結合されてスイッチ上の単一の EtherChannel となります。各インターフェイスがスイッチ上の同じチャネル グループ内にあることを確認してください。



- デバイス ローカル EtherChannel：クラスタ ユニット デバイス ローカル EtherChannel（クラスタ制御リンク用に設定された EtherChannel もこれに含まれます）は、それぞれ独立した EtherChannel としてスイッチ上で設定してください。スイッチ上で複数のクラスタ ユニット EtherChannel を結合して 1 つの EtherChannel としないでください。



サイト間のガイドライン

サイト間クラスタリングについては、次のガイドラインを参照してください。

- 次のインターフェイスおよびファイアウォール モードで Inter-Site クラスタリングをサポートします。

インターフェイス モード	ファイアウォール モード	
	ルーテッド	Transparent
個別インターフェイス	○	該当なし
スパンド EtherChannel	なし	○

- 個別インターフェイス モードでは、マルチキャスト ランデブー ポイント（RP）に向けてECMP を使用する場合、ネクスト ホップとしてメイン クラスタ IP アドレスを使用する RP IP アドレスのスタティック ルートを使用することをお勧めします。このスタティック ルートは、スレーブ ユニットにユニキャスト PIM 登録パケットが送信されるのを防ぎます。スレーブ ユニットが PIM 登録パケットを受け取った場合、パケットはドロップされ、マルチキャスト ストリームは登録できません。

- クラスタ制御リンクの遅延が、ラウンドトリップ時間（RTT）20 ms 未満である必要があります。

- クラスタ制御リンクは、順序の異常やパケットのドロップがない信頼性の高いものである必要があります。たとえば、専用リンクを使用する必要があります。

- 接続の再分散を設定しないでください。異なるサイトのクラスタ メンバには接続を再分散できません。

- クラスタの実装では、着信接続用の複数のサイトでメンバが区別されません。したがって、特定の接続に対する接続のロールが複数のサイトにまたがる場合があります。これは想定されている動作です。

- トランスペアレント モードの場合、内部ルータと外部ルータのペア間にクラスタを配置すると（AKA ノースサウス挿入）、両方の内部ルータが同じ MAC アドレスを共有し、両方の外部ルータが同じ MAC アドレスを共有する必要があります。サイト 1 のクラスタ メンバがサイト 2 のメンバに接続を転送するとき、宛先 MAC アドレスは維持されます。MAC アドレスがサイト 1 のルータと同じである場合にのみ、パケットはサイト 2 のルータに到達します。

- トランスペアレント モードの場合、内部ネットワーク間のファイル用に各サイトのデータ ネットワークとゲートウェイ ルータ間にクラスタを配置すると（AKA イーストウェスト挿入）、各ゲートウェイ ルータは、HSRP などの First Hop Redundancy Protocol（FHRP）を使用して、各サイトで同じ仮想 IP および MAC アドレスの宛先を提供します。データ VLAN は、オーバーレイ トランスポート仮想化（OTV）または同様のものを使用してサイト全体にわたって拡張されます。ローカル ゲートウェイ ルータ宛てのトラフィックが DCI 経由で他のサイトに送信されないようにするには、フィルタを作成する必要があります。ゲートウェイ ルータが 1 つのサイトで到達不能になった場合、トラフィックが正常に他のサイトのゲートウェイに到達できるようにフィルタを削除する必要があります。

その他のガイドライン

- 大々的なトポロジ変更が発生する場合（EtherChannel インターフェイスの追加または削除、ASA 上でのインターフェイスまたはスイッチの有効化または無効化、VSS または vPC を形成するための追加スイッチの追加など）、ヘルス チェック機能や無効なインターフェイスのインターフェイス モニタリングを無効にする必要があります。トポロジの変更が完了して、コンフィギュレーション変更がすべてのユニットに同期されたら、インターフェイスのヘルス チェック機能を再度有効にできます。

- ユニットを既存のクラスタに追加したときや、ユニットをリロードしたときは、一時的に、限定的なパケット/接続ドロップが発生します。これは予定どおりの動作です。場合

によっては、ドロップされたパケットが原因で接続がハングすることがあります。たとえば、FTP 接続の FIN/ACK パケットがドロップされると、FTP クライアントがハングします。この場合は、FTP 接続を再確立する必要があります。

- スパンド EtherChannel に接続された Windows 2003 Server を使用している場合、syslog サーバ ポートがダウンし、サーバが ICMP エラー メッセージを調整しないと、多数の ICMP メッセージが ASA クラスタに送信されます。このようなメッセージにより、ASA クラスタの一部のユニットで CPU 使用率が高くなり、パフォーマンスに影響する可能性があります。ICMP エラー メッセージを調節することを推奨します。
- 個別インターフェイス モードの VXLAN はサポートされていません。スパンド EtherChannel モードでのみ VXLAN をサポートしています。

ASA クラスタリングのデフォルト

- スパンド EtherChannel を使用するときは、cLACP システム ID は自動生成され、システム プライオリティはデフォルトで 1 です。
- クラスタのヘルス チェック機能は、デフォルトでイネーブルになり、ホールド時間は 3 秒です。デフォルトでは、すべてのインターフェイスでインターネット ヘルス モニタリングがイネーブルになっています。
- 接続再分散は、デフォルトでは無効になっています。接続再分散を有効にした場合の、デフォルトの負荷情報交換間隔は 5 秒です。

ASA クラスタリングの設定

クラスタリングを設定するには、次のタスクを実行します。

（注） クラスタリングを有効または無効にするには、コンソール接続（CLI の場合）または ASDM 接続を使用します。

ユニットのケーブル接続およびインターフェイスの設定

クラスタリングを設定する前に、クラスタ制御リンク ネットワーク、管理ネットワーク、およびデータ ネットワークをケーブルで接続します。次に、インターフェイスを設定します。

クラスタ インターフェイスについて

データ インターフェイスは、スパンド EtherChannel として設定することも、個別インターフェイスとして設定することもできます。1 つのクラスタ内のすべてのデータ インターフェイスのタイプが同一であることが必要です。また、各ユニットの、少なくとも 1 つのハードウェア インターフェイスをクラスタ制御リンク専用とする必要があります。

クラスタ制御リンクについて

各ユニットの、少なくとも1つのハードウェアインターフェイスをクラスタ制御リンク専用とする必要があります。

クラスタ制御リンク トラフィックの概要

クラスタ制御リンク トラフィックには、制御とデータの両方のトラフィックが含まれます。

制御トラフィックには次のものが含まれます。

- マスター選定。
- コンフィギュレーションの複製
- ヘルス モニタリング。

データ トラフィックには次のものが含まれます。

- ステート複製。
- 接続所有権クエリおよびデータ パケット転送。

クラスタ制御リンク インターフェイスとネットワーク

次の例外を除き、クラスタ制御リンクには任意のデータ インターフェイスを使用できます。

- VLAN サブインターフェイスをクラスタ制御リンクとして使用することはできません。
- 管理 *x/x* インターフェイスをクラスタ制御リンクとして使用することはできません（単独か EtherChannel かにかかわらず）。
- ASA FirePOWER モジュールを搭載した ASA 5585-X では、クラスタ制御リンクに ASA FirePOWER モジュール上のインターフェイスではなく、ASA インターフェイスを使用することを推奨しています。モジュール インターフェイスは、ソフトウェア アップグレード中に発生するリロードを含め、モジュールのリロード中に最大 30 秒間トラフィックをドロップできます。ただし、必要に応じて、モジュールインターフェイスとASAインターフェイスを同じクラスタ制御リンク EtherChannel で使用できます。モジュール インターフェイスがドロップした場合、EtherChannel の残りのインターフェイスはまだ稼働しています。ASA 5585-X ネットワーク モジュールは別のオペレーティング システムを実行しないため、この問題の影響を受けません。

  モジュール上のデータインターフェイスはリロードの低下によっても影響を受けることに注意してください。シスコでは、EtherChannel内で常にASAインターフェイスをモジュール インターフェイスと冗長的に使用することを推奨しています。

  ASA 5585-X と SSP-10 および SSP-20（2 個の 10 ギガビット イーサネット インターフェイスを持つ）については、一方のインターフェイスをクラスタ制御リンクに使用し、他方をデータに使用することを推奨します（データについてはサブインターフェイスを使用できます）。この設定は、クラスタ制御リンクの冗長性には対応しませんが、クラスタ制御リンクのサイズをデータ インターフェイスのサイズと一致させるという要件は満たされます。

EtherChannel インターフェイスまたは冗長インターフェイスを使用できます。

各クラスタ制御リンクは、同じサブネット上の IP アドレスを持ちます。このサブネットは、他のすべてのトラフィックからは隔離し、ASA クラスタ制御リンク インターフェイスだけが含まれるようにしてください。

2 メンバー クラスタの場合、ASA と ASA の間をクラスタ制御リンクで直接接続しないでください。インターフェイスを直接接続した場合、一方のユニットで障害が発生すると、クラスタ制御リンクが機能せず、他の正常なユニットも動作しなくなります。スイッチを介してクラスタ制御リンクを接続した場合は、正常なユニットについてはクラスタ制御リンクは動作を維持します。

クラスタ制御リンクのサイズ

可能であれば、各シャーシの予想されるスループットに合わせてクラスタ制御リンクをサイジングする必要があります。そうすれば、クラスタ制御リンクが最悪のシナリオを処理できます。 たとえば、ASA 5585-X と SSP-60 を使用する場合は、クラスタのユニットあたり最大 14 Gbps を通過させることができるので、クラスタ制御リンクに割り当てるインターフェイスも、最低 14 Gbps の通過が可能となるようにしてください。この場合は、たとえば 10 ギガビット イーサネット インターフェイス 2 つを EtherChannel としてクラスタ制御リンクに使用し、残りのインターフェイスを必要に応じてデータ リンクに使用します。

クラスタ制御リンク トラフィックの内容は主に、状態アップデートや転送されたパケットです。クラスタ制御リンクでのトラフィックの量は常に変化します。転送されるトラフィックの量は、ロードバランシングの有効性、または中央集中型機能のための十分なトラフィックがあるかどうかによって決まります。次に例を示します。

- NAT では接続のロード バランシングが低下するので、すべてのリターン トラフィックを正しいユニットに再分散する必要があります。
- ネットワーク アクセスに対する AAA は一元的な機能であるため、すべてのトラフィックがマスター ユニットに転送されます。
- メンバーシップが変更されると、クラスタは大量の接続の再分散を必要とするため、一時的にクラスタ制御リンクの帯域幅を大量に使用します。

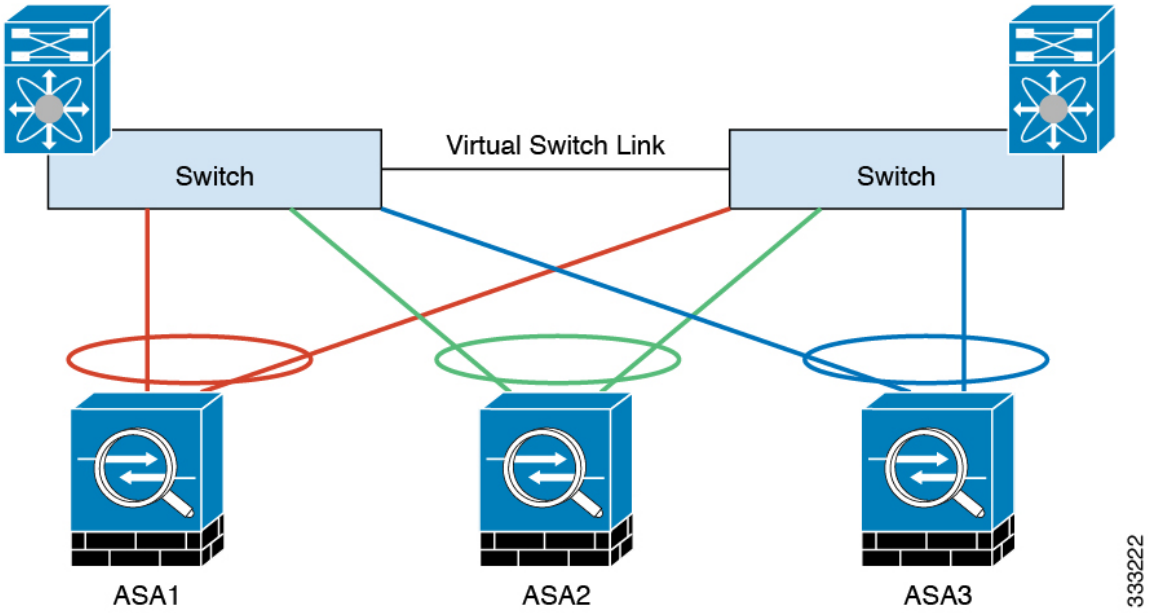
クラスタ制御リンクの帯域幅を大きくすると、メンバーシップが変更されたときの収束が高速になり、スループットのボトルネックを回避できます。

（注） クラスタに大量の非対称（再分散された）トラフィックがある場合は、クラスタ制御リンクのサイズを大きくする必要があります。

クラスタ制御リンク冗長性

クラスタ制御リンクには EtherChannel を使用することを推奨します。冗長性を実現しながら、EtherChannel 内の複数のリンクにトラフィックを渡すことができます。

次の図は、仮想スイッチングシステム（VSS）または仮想ポートチャネル（vPC）環境でクラスタ制御リンクとして EtherChannel を使用する方法を示します。EtherChannel のすべてのリンクがアクティブです。スイッチが VSS または vPC の一部である場合は、同じ EtherChannel 内の ASA インターフェイスをそれぞれ、VSS または vPC 内の異なるスイッチに接続できます。スイッチ インターフェイスは同じ EtherChannel ポートチャネル インターフェイスのメンバです。複数の個別のスイッチが単一のスイッチのように動作するからです。この EtherChannel は、スパンド EtherChannel ではなく、デバイス ローカルであることに注意してください。



クラスタ制御リンクの信頼性

クラスタ制御リンクの機能を保証するには、ユニット間のラウンドトリップ時間（RTT）が 20 ms 未満になるようにします。この最大遅延により、異なる地理的サイトにインストールされたクラスタ メンバとの互換性が向上します。遅延を調べるには、ユニット間のクラスタ制御リンクで ping を実行します。

クラスタ制御リンクは、順序の異常やパケットのドロップがない信頼性の高いものである必要があります。たとえば、サイト間の導入の場合、専用リンクを使用する必要があります。

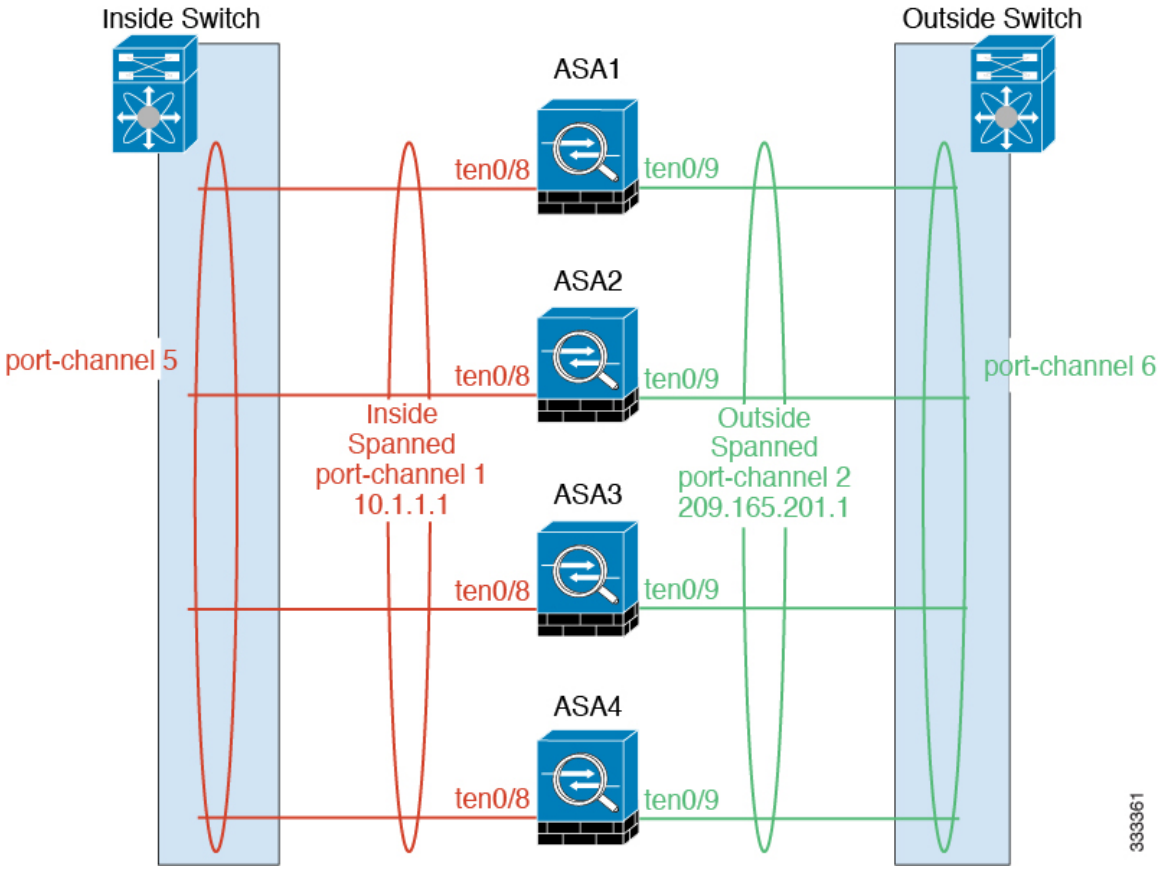
クラスタ制御リンクの障害

ユニットのクラスタ制御リンク回線プロトコルがダウンした場合、クラスタリングはディセーブルになります。データ インターフェイスはシャット ダウンされます。クラスタ制御リンクの修復後、クラスタリングを再度イネーブルにして手動でクラスタに再参加する必要があります。

（注） ASA が非アクティブになると、すべてのデータ インターフェイスがシャットダウンされます。管理専用インターフェイスのみがトラフィックを送受信できます。管理インターフェイスは、そのユニットがクラスタ IP プールから受け取った IP アドレスを使用して引き続き稼働状態となります。ただし、リロードする場合、クラスタでユニットがまだ非アクティブになっていると、管理インターフェイスはアクセスできません（マスター ユニットと同じメイン IP アドレスを使用するため）。それ以降のコンフィギュレーション作業には、コンソール ポートを使用する必要があります。

スパンド EtherChannel（推奨）

シャーシあたり 1 つ以上のインターフェイスをグループ化して、クラスタのすべてのシャーシに広がる EtherChannel とすることができます。EtherChannel によって、チャネル内の使用可能なすべてのアクティブ インターフェイスのトラフィックが集約されます。スパンド EtherChannel は、ルーテッドとトランスペアレントのどちらのファイアウォール モードでも設定できます。ルーテッド モードでは、EtherChannel は単一の IP アドレスを持つルーテッド インターフェイスとして設定されます。トランスペアレント モードでは、IP アドレスはブリッジグループ メンバーではなく BVI に割り当てられます。EtherChannel は初めから、ロードバランシング機能を基本的動作の一部として備えています。



スパンド *EtherChannel* の利点

EtherChannel 方式のロードバランシングは、次のような利点から、他の方式よりも推奨されます。

- 障害検出までの時間が短い。
- コンバージェンス時間が短い。個別インターフェイスはルーティング プロトコルに基づきトラフィックをロード バランシングしますが、ルーティング プロトコルはリンク障害時にコンバージェンスが遅くなることがよくあります。
- コンフィギュレーションが容易である。

最大スループットのガイドライン

最大スループットを実現するには、次のことを推奨します。

- 使用するロード バランシング ハッシュ アルゴリズムは「対称」であるようにします。つまり、どちらの方向からのパケットも同じハッシュを持たせて、スパンド EtherChannel 内の同じ ASA に送信します。送信元と宛先の IP アドレス（デフォルト）または送信元と宛先のポートをハッシュ アルゴリズムとして使用することを推奨します。
- ASA をスイッチに接続するときは、同じタイプのライン カードを使用します。すべてのパケットに同じハッシュ アルゴリズムが適用されるようにするためです。

ロード バランシング

EtherChannel リンクは、送信元または宛先 IP アドレス、TCP ポートおよび UDP ポート番号に基づいて、専用のハッシュ アルゴリズムを使用して選択されます。

（注） ASA では、デフォルトのロードバランシング アルゴリズムを変更しないでください。スイッチでは、アルゴリズム **source-dest-ip** または **source-dest-ip-port**（Cisco Nexus OS または Cisco IOS の **port-channel load-balance** コマンドを参照）を使用することをお勧めします。クラスタ内の ASA へのトラフィックが均等に分散されなくなることがあるため、ロードバランシング アルゴリズムでは、**vlan** キーワードを使用しないでください。

EtherChannel 内のリンク数はロード バランシングに影響を及ぼします。

対称ロード バランシングは常に可能とは限りません。NAT を設定する場合は、フォワード パケットとリターン パケットとで IP アドレスやポートが異なります。リターン トラフィックはハッシュに基づいて別のユニットに送信されるため、クラスタはほとんどのリターン トラフィックを正しいユニットにリダイレクトする必要があります。

EtherChannel の冗長性

EtherChannel には、冗長性機能が組み込まれています。これは、すべてのリンクの回線プロトコル ステータスをモニタします。リンクの 1 つで障害が発生すると、トラフィックは残りのリ

ンク間で再分散されます。EtherChannel のすべてのリンクが特定のユニット上で停止したが、他方のユニットがまだアクティブである場合は、そのユニットはクラスタから削除されます。

VSS または *vPC* への接続

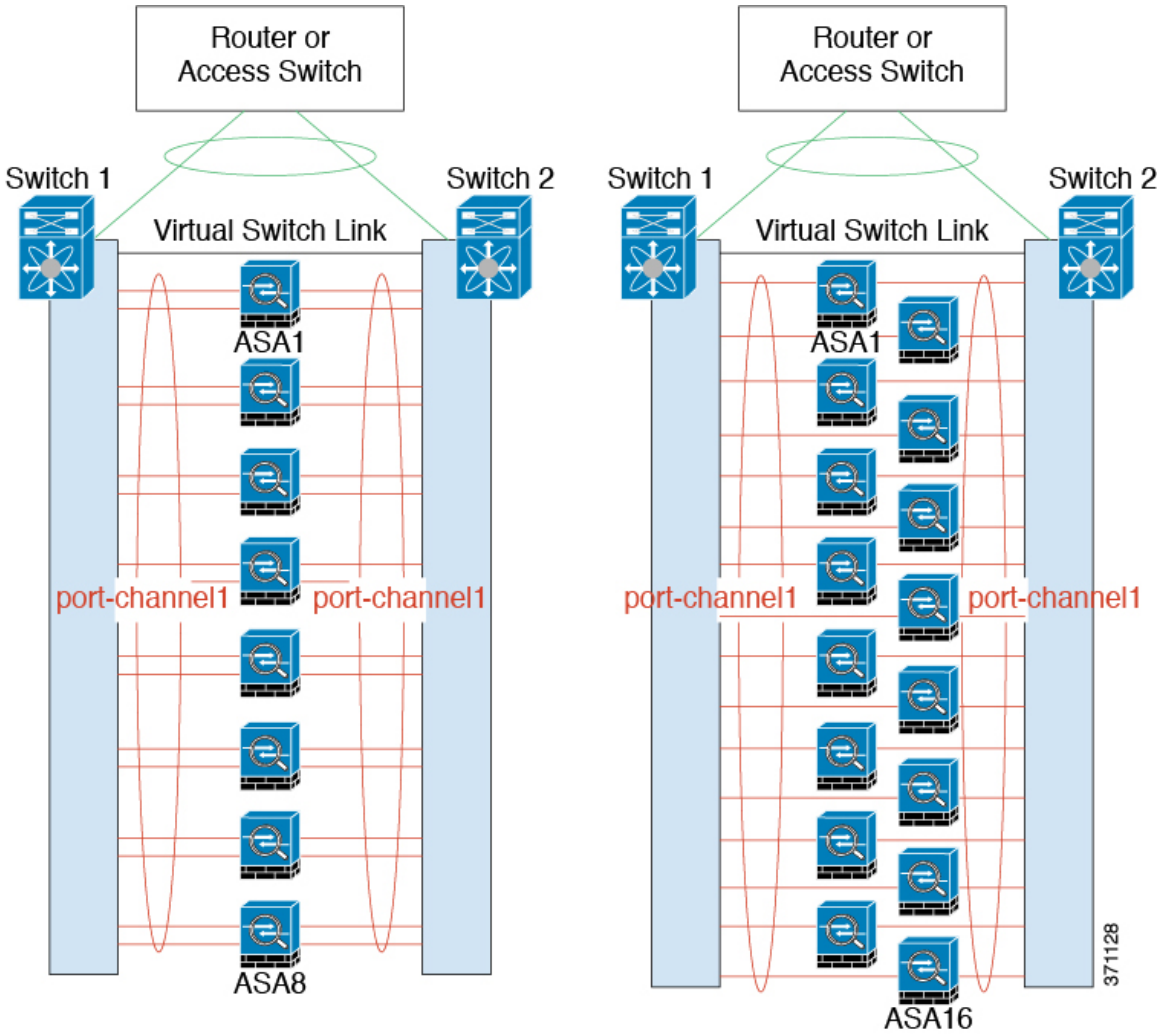
1 つの ASA につき複数のインターフェイスを、スパンド EtherChannel に入れることができます。1 つの ASA につき複数のインターフェイスが特に役立つのは、VSS または vPC の両方のスイッチに接続するときです。

スイッチによっては、スパンド EtherChannel に最大 32 個のアクティブ リンクを設定できます。この機能では、vPC 内の両方のスイッチが、それぞれ 16 個のアクティブ リンクの EtherChannel をサポートする必要があります（例：Cisco Nexus 7000 と F2 シリーズ 10 ギガビット イーサネット モジュール）。

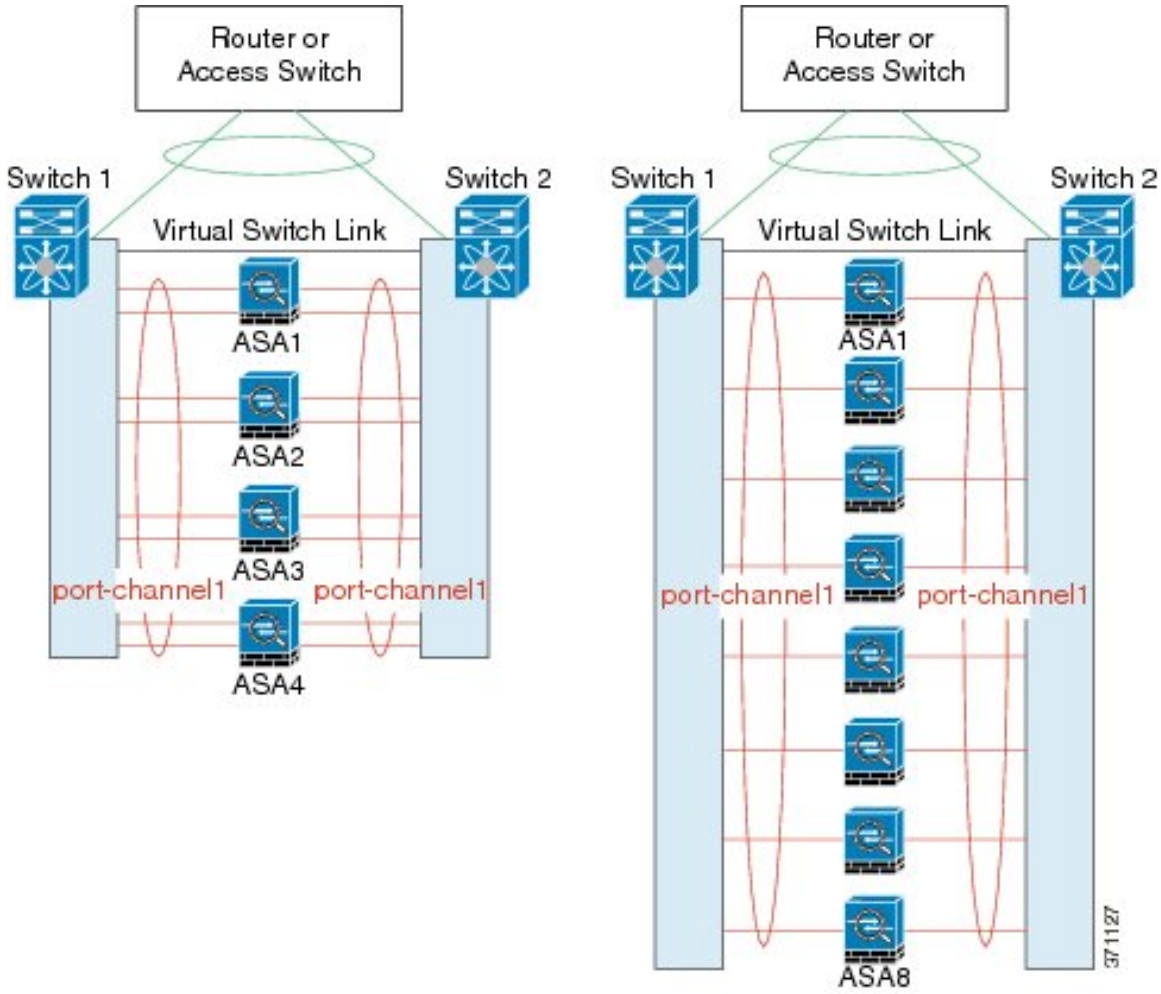
EtherChannel で 8 個のアクティブ リンクをサポートするスイッチの場合、VSS/vPC で 2 台のスイッチに接続すると、スパンド EtherChannel に最大 16 個のアクティブ リンクを設定できます。

スパンド EtherChannel で 8 個より多くのアクティブ リンクを使用する場合は、スタンバイ リンクも使用できません。9 ～ 32 個のアクティブ リンクをサポートするには、スタンバイ リンクの使用を可能にする cLACP ダイナミック ポート プライオリティをディセーブルにする必要があります。それでも、必要であれば、たとえば 1 台のスイッチに接続するときに、8 個のアクティブ リンクと 8 個のスタンバイ リンクを使用できます。

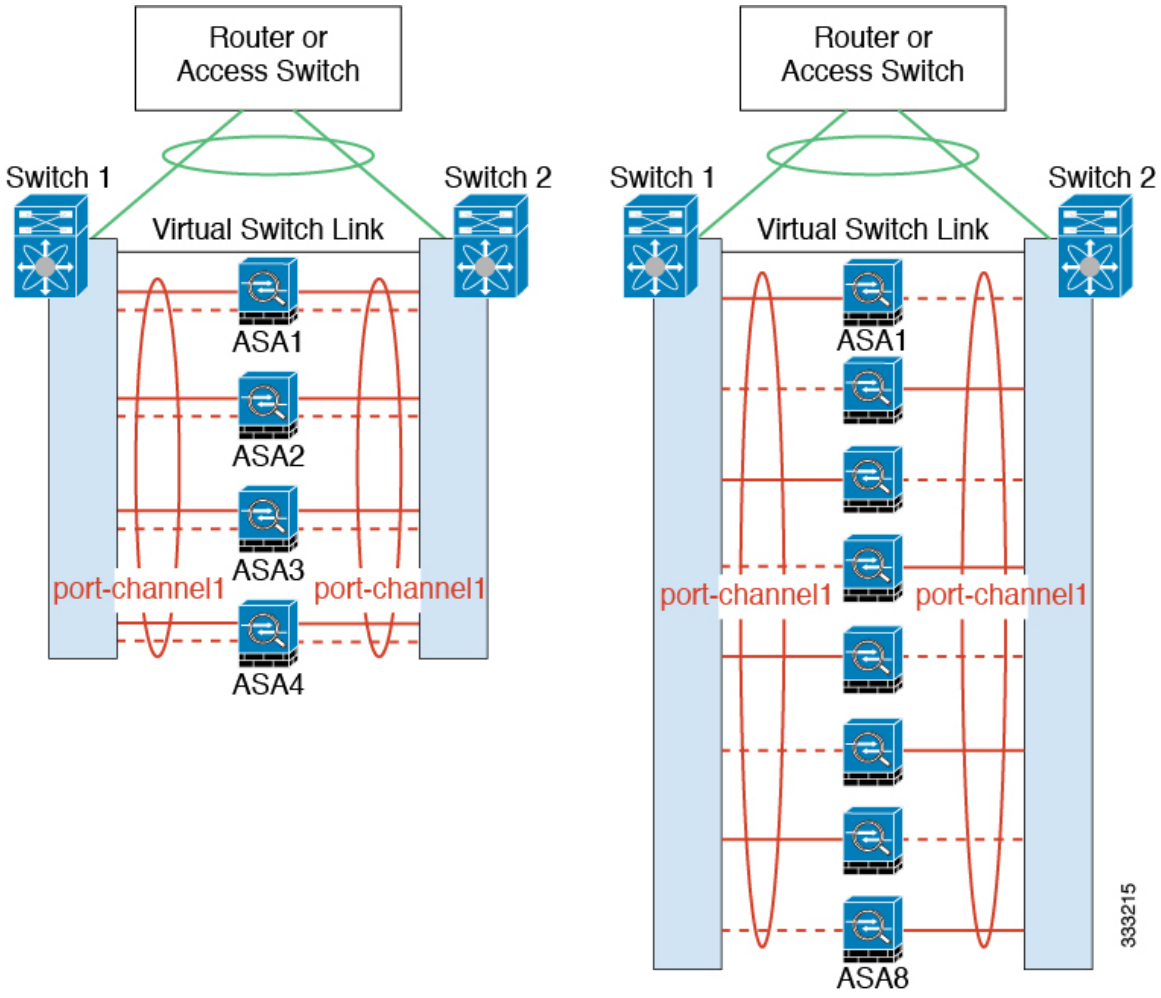
次の図では、8 ASA クラスタおよび 16 ASA クラスタでの 32 アクティブ リンクのスパンド EtherChannel を示します。



次の図では、4 ASA クラスタおよび 8 ASA クラスタでの 16 アクティブ リンクのスパンド EtherChannel を示します。



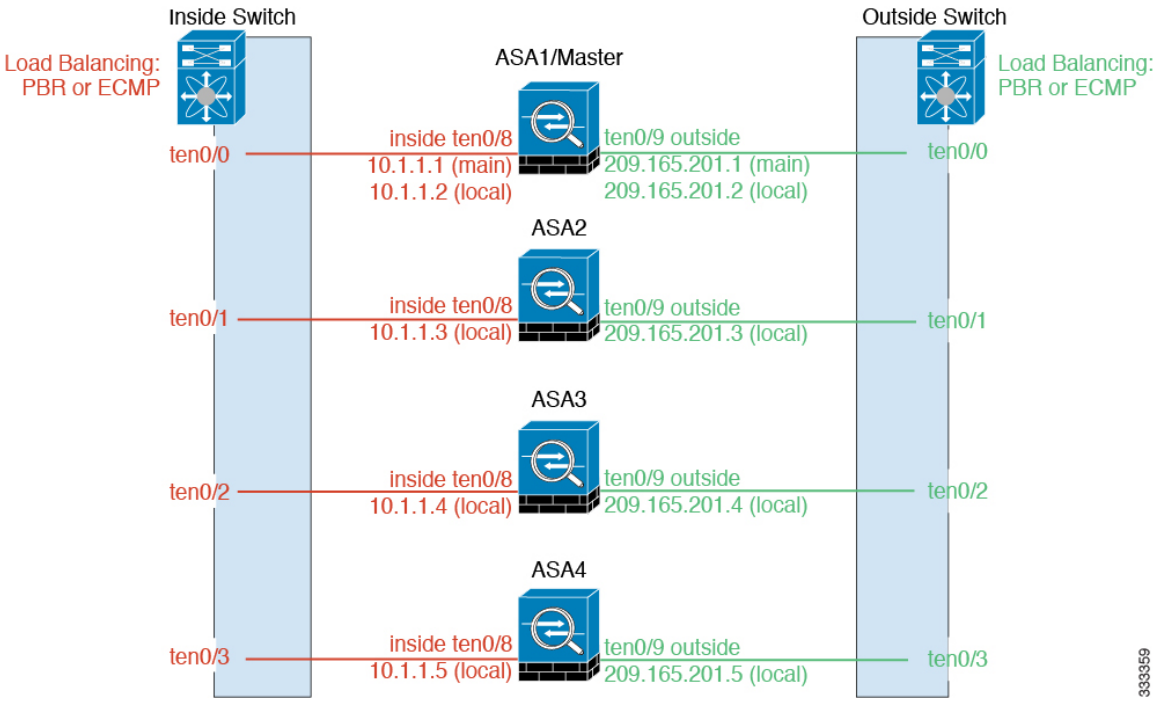
次の図では、4 ASA クラスタおよび 8 ASA クラスタでの従来の 8 アクティブ リンク/8 スタンバイ リンクのスパンド EtherChannel を示します。アクティブ リンクは実線で、非アクティブ リンクは点線で示しています。cLACP ロードバランシングは、EtherChannel のリンクのうち最良の 8 本を自動的に選択してアクティブにできます。つまり、cLACP は、リンク レベルでのロード バランシング実現に役立ちます。



個別インターフェイス（ルーテッド ファイアウォール モードのみ）

個別インターフェイスは通常のルーテッドインターフェイスであり、それぞれが専用のローカル *IP* アドレスを持ちます。インターフェイス コンフィギュレーションはマスター ユニット上だけで行う必要があるため、このインターフェイス コンフィギュレーションの中で IP アドレス プールを設定して、このプールのアドレスをクラスタ メンバ（マスター用を含む）のインターフェイスに使用させることができます。メイン クラスタ *IP* アドレスは、そのクラスタのための固定アドレスであり、常に現在のマスター ユニットに属します。メイン クラスタ IP アドレスは、マスター ユニットのスレーブ IP アドレスです。ローカル IP アドレスが常にルーティングのマスター アドレスになります。このメイン クラスタ IP アドレスによって、管理アクセスのアドレスが一本化されます。マスター ユニットが変更されると、メイン クラスタ IP アドレスは新しいマスターユニットに移動するので、クラスタの管理をシームレスに続行できます。ただし、ロードバランシングを別途する必要があります（この場合はアップストリーム スイッチ上で）。

（注） 個別インターフェイスはルーティング プロトコルに基づきトラフィックをロード バランシングしますが、ルーティング プロトコルはリンク障害時にコンバージェンスが遅くなることがよくあるので、個別インターフェイスの代わりにスパンド EtherChannel を推奨します。



ポリシーベース ルーティング（ルーテッド ファイアウォール モードのみ）

個別インターフェイスを使用するときは、各 ASA インターフェイスが専用の IP アドレスと MAC アドレスを維持します。ロード バランシング方法の 1 つが、ポリシーベース ルーティング（PBR）です。

この方法が推奨されるのは、すでに PBR を使用しており、既存のインフラストラクチャを活用したい場合です。また、この方法を使用すると、スパンド EtherChannel の場合と比べて、追加の調整オプションを利用できる場合もあります。

PBR は、ルート マップおよび ACL に基づいて、ルーティングの決定を行います。管理者は、手動でトラフィックをクラスタ内のすべての ASA 間で分ける必要があります。PBR は静的であるため、常に最適なロードバランシング結果を実現できないこともあります。最高のパフォーマンスを達成するには、PBR ポリシーを設定するときに、同じ接続のフォワードとリターンのパケットが同じ物理的 ASA に送信されるように指定することを推奨します。たとえば、Cisco ルータがある場合は、冗長性を実現するには Cisco IOS PBR をオブジェクト トラッキングとともに使用します。Cisco IOS オブジェクト トラッキングは、ICMP ping を使用して各 ASA をモニタします。これで、PBR は、特定の ASA の到達可能性に基づいてルート マップをイネーブルまたはディセーブルにできます。詳細については、次の URL を参照してください。

http://www.cisco.com/c/en/us/solutions/data-center-virtualization/intelligent-traffic-director/index.html

http://www.cisco.com/en/US/products/ps6599/products_white_paper09186a00800a4409.shtml

（注） このロードバランシング方法を使用する場合は、デバイス ローカル EtherChannel を個別インターフェイスとして使用できます。

等コスト マルチパス ルーティング（ルーテッド ファイアウォール モードのみ）

個別インターフェイスを使用するときは、各 ASA インターフェイスが専用の IP アドレスと MAC アドレスを維持します。ロードバランシング方法の 1 つが、等コストマルチパス（ECMP）ルーティングです。

この方法が推奨されるのは、すでに ECMP を使用しており、既存のインフラストラクチャを活用したい場合です。また、この方法を使用すると、スパンド EtherChannel の場合と比べて、追加の調整オプションを利用できる場合もあります。

ECMP ルーティングでは、ルーティング メトリックが同値で最高である複数の「最適パス」を介してパケットを転送できます。EtherChannel のように、送信元および宛先の IP アドレスや送信元および宛先のポートのハッシュを使用してネクストホップの 1 つにパケットを送信できます。ECMP ルーティングにスタティック ルートを使用する場合は、ASA の障害発生時に問題が起きることがあります。ルートは引き続き使用されるため、障害が発生した ASA へのトラフィックが失われるからです。スタティック ルートを使用する場合は必ず、オブジェクト トラッキングなどのスタティック ルート モニタリング機能を使用してください。ダイナミック ルーティング プロトコルを使用してルートの追加と削除を行うことを推奨します。この場合は、ダイナミック ルーティングに参加するように各 ASA を設定する必要があります。

（注） このロードバランシング方法を使用する場合は、デバイス ローカル EtherChannel を個別インターフェイスとして使用できます。

Nexus Intelligent Traffic Director（ルーテッド ファイアウォール モードのみ）

個別インターフェイスを使用するときは、各 ASA インターフェイスが専用の IP アドレスと MAC アドレスを維持します。Intelligent Traffic Director（ITD）とは、Nexus 5000、6000、7000 および 9000 スイッチ シリーズの高速ハードウェア ロードバランシング ソリューションです。従来の PBR の機能を完全に網羅していることに加え、簡略化された構成ワークフローを提供し、粒度の細かい負荷分散を実現するための複数の追加機能を備えています。

ITD は、IP スティッキ性、双方向フロー対称性のためのコンシステント ハッシュ法、仮想 IP アドレッシング、ヘルス モニタリング、高度な障害処理ポリシー（N+M 冗長性）、加重ロードバランシング、およびアプリケーション IP SLA プローブ（DNS を含む）をサポートします。ロードバランシングの動的な性質により、PBR に比べて、すべてのクラスタ メンバーでより均一なトラフィック分散を実現します。双方向フロー対称性を実現するために、接続のフォワードおよびリターン パケットが同じ物理 ASA に送信されるように ITD を設定することを推奨します。詳細については、次の URL を参照してください。

http://www.cisco.com/c/en/us/solutions/data-center-virtualization/intelligent-traffic-director/index.html

クラスタユニットのケーブル接続とアップストリームおよびダウンストリーム機器の設定

クラスタリングを設定する前に、クラスタ制御リンク ネットワーク、管理ネットワーク、およびデータ ネットワークをケーブルで接続します。

手順

クラスタ制御リンク ネットワーク、管理ネットワーク、およびデータ ネットワークをケーブルで接続します。

（注） クラスタに参加するようにユニットを設定する前に、少なくとも、アクティブなクラスタ制御リンク ネットワークが必要です。

アップストリームとダウンストリームの機器も設定する必要があります。たとえば、EtherChannel を使用する場合は、EtherChannel のアップストリーム/ダウンストリーム機器を設定する必要があります。

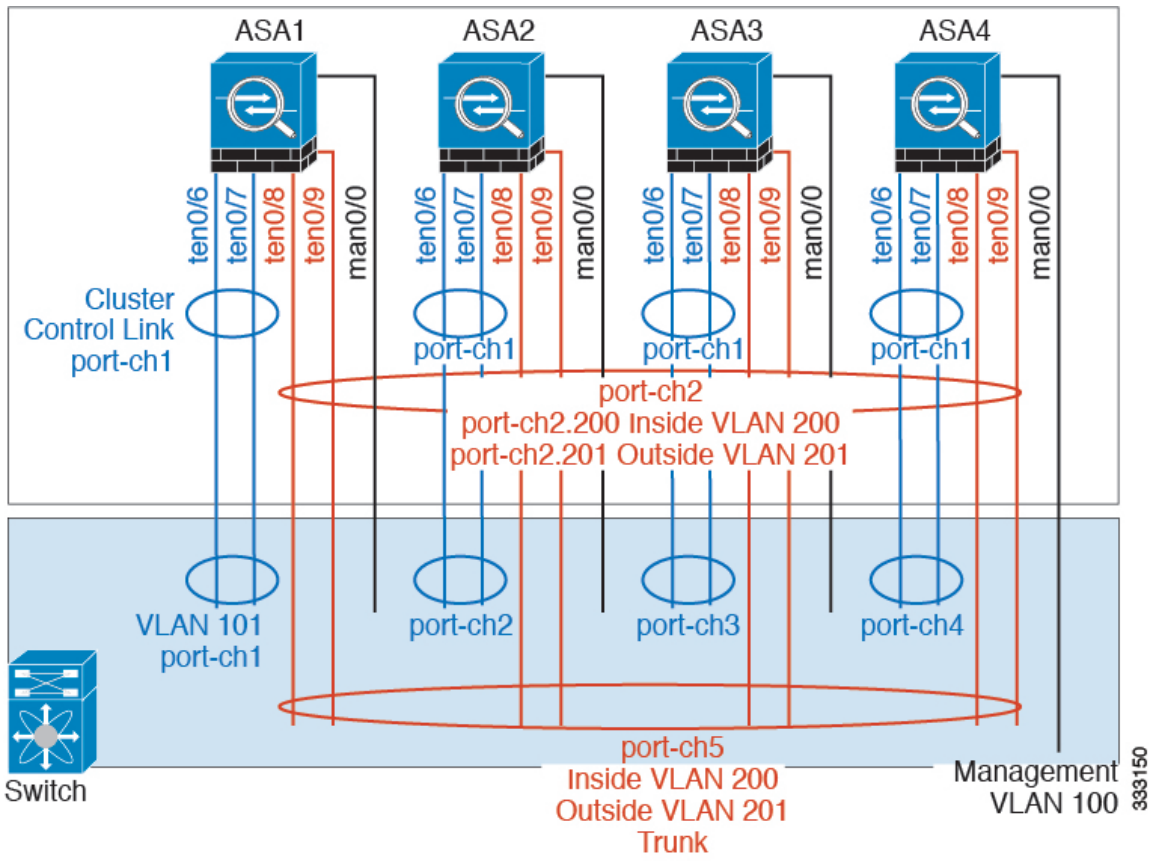
例

（注） この例では、ロードバランシングに EtherChannel を使用します。PBR または ECMP を使用する場合は、スイッチ コンフィギュレーションが異なります。

たとえば、4 台の ASA 5585-X のそれぞれにおいて、次のものを使用します。

- デバイス ローカル EtherChannel の 10 ギガビット イーサネット インターフェイス 2 個（クラスタ制御リンク用）。
- スパンド EtherChannel の 10 ギガビット イーサネット インターフェイス 2 個（内部および外部ネットワーク用）。各インターフェイスは、EtherChannel の VLAN サブインターフェイスです。サブインターフェイスを使用すると、内部と外部の両方のインターフェイスが EtherChannel の利点を活用できます。
- 管理インターフェイス 1 個。

内部と外部の両方のネットワーク用に 1 台のスイッチがあります。



目的	4 台の各 ASA の接続インターフェイス	スイッチ ポートへ
クラスタ制御リンク	TenGigabitEthernet 0/6 および TenGigabitEthernet 0/7	合計 8 ポート TenGigabitEthernet 0/6 と TenGigabitEthernet 0/7 のペアごとに、4 個の EtherChannel（ASA ごとに 1 個の EC）を設定します。 これらの EtherChannel すべてが、同一の独立クラスタ制御 VLAN 上（たとえば VLAN 101）に存在する必要があります。

目的	4 台の各 ASA の接続インターフェイス	スイッチ ポートへ
内部および外部インターフェイス	TenGigabitEthernet 0/8 および TenGigabitEthernet 0/9	合計 8 ポート 単一の EtherChannel を設定します（すべての ASA にまたがる）。 スイッチでは、この VLAN およびネットワークをここで設定できます。たとえば、VLAN 200（内部用）および VLAN 201（外部用）が含まれるトランクを設定します。
管理インターフェイス	Management 0/0	合計 4 ポート すべてのインターフェイスを、同一の独立管理 VLAN（たとえば VLAN 100）上に置きます。

各ユニットでのクラスタ インターフェイス モードの設定

クラスタリング用に設定できるインターフェイスのタイプは、スパンド EtherChannel と個別インターフェイスのいずれか一方のみです。1 つのクラスタ内でインターフェイス タイプを混在させることはできません。

始める前に

- モードの設定は、クラスタに追加する各 ASA で個別に行う必要があります。
- 管理専用インターフェイスはいつでも、個別インターフェイス（推奨）として設定できます（スパンド EtherChannel モードのときでも）。管理インターフェイスは、個別インターフェイスとすることができます（トランスペアレント ファイアウォール モードのときでも）。
- スパンド EtherChannel モードでは、管理インターフェイスを個別インターフェイスとして設定すると、管理インターフェイスに対してダイナミック ルーティングをイネーブルにできません。スタティック ルートを使用する必要があります。
- マルチ コンテキスト モードでは、すべてのコンテキストに対して 1 つのインターフェイス タイプを選択する必要があります。たとえば、トランスペアレント モードとルーテッド モードのコンテキストが混在している場合は、すべてのコンテキストにスパンド EtherChannel モードを使用する必要があります。これが、トランスペアレント モードで許可される唯一のインターフェイス タイプであるからです。

手順

ステップ 1 互換性のないコンフィギュレーションを表示し、強制的にインターフェイス モードにして後でコンフィギュレーションを修正できるようにします。このコマンドではモードは変更されません。

cluster interface-mode {**individual** | **spanned**} **check-details**

例：

```
ciscoasa(config)# cluster interface-mode spanned check-details
```

ステップ 2 クラスタリング用にインターフェイス モードを設定します。

cluster interface-mode {**individual** | **spanned**} **force**

例：

```
ciscoasa(config)# cluster interface-mode spanned force
```

デフォルト設定はありません。明示的にモードを選択する必要があります。モードを設定していない場合は、クラスタリングをイネーブルにできません。

force オプションを指定すると、互換性のないコンフィギュレーションの検査は行わずにモードが変更されます。コンフィギュレーションの問題がある場合は、モードを変更した後に手動で解決する必要があります。インターフェイス コンフィギュレーションの修正ができるのはモードの設定後に限られるので、**force** オプションを使用することを推奨します。このようにすれば、最低でも、既存のコンフィギュレーションの状態から開始できます。さらにガイダンスが必要な場合は、モードを設定した後で **check-details** オプションを再実行します。

force オプションを指定しないと、互換性のないコンフィギュレーションがある場合は、コンフィギュレーションをクリアしてリロードするように求められるので、コンソール ポートに接続して管理アクセスを再設定する必要があります。コンフィギュレーションに互換性の問題がない場合は（まれなケース）、モードが変更され、コンフィギュレーションは維持されます。コンフィギュレーションをクリアしたくない場合は、**n** を入力してコマンドを終了します。

インターフェイス モードを解除するには、**no cluster interface-mode** コマンドを入力します。

マスター ユニットでのインターフェイスの設定

クラスタリングを有効にする前に、現在 IP アドレスが設定されているインターフェイスをクラスタ対応に変更する必要があります。他のインターフェイスについては、クラスタリングをイネーブルにする前またはした後で設定できます。完全なコンフィギュレーションが新しいクラスタ メンバと同期するように、すべてのインターフェイスを事前に設定することを推奨します。

ここでは、クラスタリング互換となるようにインターフェイスを設定する方法について説明します。データ インターフェイスは、スパンド EtherChannel として設定することも、個別イン

ターフェイスとして設定することもできます。各方式は別のロードバランシング メカニズムを使用します。同じコンフィギュレーションで両方のタイプを設定することはできません。ただし、管理インターフェイスは例外で、スパンド EtherChannel モードであっても個別インターフェイスにできます。

個別のインターフェイスの設定（管理インターフェイスに推奨）

個別インターフェイスは通常のルーテッド インターフェイスであり、それぞれが専用の IP アドレスを IP アドレス プールから取得します。メイン クラスタ IP アドレスは、そのクラスタのための固定アドレスであり、常に現在のプライマリ ユニットに属します。

スパンドEtherChannelモードでは、管理インターフェイスを個別インターフェイスとして設定することを推奨します。個別管理インターフェイスならば、必要に応じて各ユニットに直接接続できますが、スパンドEtherChannelインターフェイスでは、現在のプライマリ ユニットへの接続しかできません。

始める前に

- 管理専用インターフェイスの場合を除き、個別インターフェイス モードであることが必要です。
- マルチ コンテキスト モードの場合は、この手順を各コンテキストで実行します。まだコンテキスト コンフィギュレーション モードに入っていない場合は、**changeto context** *name* コマンドを入力します。
- 個別インターフェイスの場合は、ネイバー デバイスでのロード バランシングを設定する必要があります。管理インターフェイスには、外部のロードバランシングは必要ありません。
- （オプション）インターフェイスをデバイス ローカルEtherChannelインターフェイスとして設定する、冗長インターフェイスを設定する、およびサブインターフェイスを設定する作業を必要に応じて行います。
  - EtherChannel の場合、この EtherChannel はユニットに対してローカルであり、スパンド EtherChannel ではありません。
  - 管理専用インターフェイスを冗長インターフェイスにすることはできません。

手順

ステップ 1 ローカル IP アドレス（IPv4 と IPv6 の一方または両方）のプールを設定します。このアドレスの 1 つが、このインターフェイス用に各クラスタ ユニットに割り当てられます。

（IPv4）

ip local pool *poolname first-address — last-address* [**mask** *mask*]

（IPv6）

ipv6 local pool *poolname ipv6-address*/*prefix-length number_of_addresses*

例：

```
ciscoasa(config)# ip local pool ins 192.168.1.2-192.168.1.9
ciscoasa(config-if)# ipv6 local pool insipv6 2001:DB8::1002/32 8
```

最低でも、クラスタ内のユニット数と同じ数のアドレスが含まれるようにしてください。クラスタを拡張する予定の場合は、アドレスを増やします。現在のプライマリ ユニットに属するメイン クラスタ IP アドレスは、このプールの一部ではありません。必ず、同じネットワークの IP アドレスの 1 つをメイン クラスタ IP アドレス用に確保してください。

各ユニットに割り当てられるローカルアドレスを、事前に正確に特定することはできません。各ユニットで使用されているアドレスを表示するには、**show ip[v6] local pool** *poolname* コマンドを入力します。各クラスタ メンバには、クラスタに参加したときにメンバ ID が割り当てられます。この ID によって、プールから使用されるローカル IP が決定します。

ステップ 2 インターフェイス コンフィギュレーション モードを開始します。

interface *interface_id*

例：

```
ciscoasa(config)# interface tengigabitethernet 0/8
```

ステップ 3 （管理インターフェイスのみ）インターフェイスを管理専用モードに設定してトラフィックが通過しないようにします。

management-only

デフォルトでは、管理タイプのインターフェイスは管理専用として設定されます。トランスペアレント モードでは、このコマンドは管理タイプのインターフェイスに対して常にイネーブルになります。

この設定は、クラスタ インターフェイス モードがスパンドの場合に必要です。

ステップ 4 インターフェイスの名前を指定します。

nameif *name*

例：

```
ciscoasa(config-if)# nameif inside
```

name は最大 48 文字のテキスト文字列です。大文字と小文字は区別されません。名前を変更するには、このコマンドで新しい値を再入力します。

ステップ 5 メイン クラスタの IP アドレスを設定し、クラスタ プールを指定します。

（IPv4）

ip address *ip_address* [*mask*] **cluster-pool** *poolname*

（IPv6）

ipv6 address *ipv6-address*/*prefix-length* **cluster-pool** *poolname*

例：

```
ciscoasa(config-if)# ip address 192.168.1.1 255.255.255.0 cluster-pool ins
ciscoasa(config-if)# ipv6 address 2001:DB8::1002/32 cluster-pool insipv6
```

この IP アドレスは、クラスタ プール アドレスと同じネットワーク上に存在している必要がありますが、プールに含まれていてはなりません。IPv4 アドレスと IPv6 アドレスの一方または両方を設定できます。

DHCP、PPPoE、および IPv6 自動設定はサポートされません。IP アドレスを手動で設定する必要があります。

ステップ 6 セキュリティ レベルを設定します。*number* には、0（最低）～ 100（最高）の整数を指定します。

security-level *number*

例：

```
ciscoasa(config-if)# security-level 100
```

ステップ 7 インターフェイスをイネーブルにします。

no shutdown

例

次の例では、管理 0/0 および管理 0/1 インターフェイスをデバイス ローカル EtherChannel として設定してから、この EtherChannel を個別インターフェイスとして設定します。

```
ip local pool mgmt 10.1.1.2-10.1.1.9
ipv6 local pool mgmtipv6 2001:DB8:45:1002/64 8
interface management 0/0

channel-group 1 mode active
no shutdown

interface management 0/1

channel-group 1 mode active
no shutdown

interface port-channel 1

nameif management
ip address 10.1.1.1 255.255.255.0 cluster-pool mgmt
ipv6 address 2001:DB8:45:1001/64 cluster-pool mgmtipv6
security-level 100
management-only
```

スパンド EtherChannel の設定

スパンド EtherChannel は、クラスタ内のすべての ASA に広がるものであり、EtherChannel の動作の一部としてロード バランシングを行うことができます。

始める前に

- スパンド EtherChannel インターフェイス モードにする必要があります。
- マルチ コンテキスト モードの場合は、この手順をシステム実行スペースで開始します。まだシステム コンフィギュレーション モードに入っていない場合は、**changeto system** コマンドを入力します。
- トランスペアレント モードの場合は、ブリッジ グループを設定します。ブリッジ仮想インターフェイス（BVI）の設定 （531 ページ）を参照してください。
- EtherChannel には最大および最小のリンク数を指定しないでください。EtherChannel の最大および最小のリンク数の指定（**lacp max-bundle** コマンドと **port-channel min-bundle** コマンド）は、ASA とスイッチのどちらにおいても行わないことを推奨します。これらを使用する必要がある場合は、次の点に注意してください。
  - ASA 上で設定されるリンクの最大数は、クラスタ全体のアクティブ ポートの合計数です。スイッチ上で設定された最大リンク数の値が、ASA での値を超えていないことを確認してください。
  - ASA 上で設定される最小リンク数は、ポートチャネル インターフェイスを起動するための最小アクティブ ポート数（ユニットあたり）です。スイッチ上では、最小リンク数はクラスタ全体の最小リンク数であるため、この値は ASA での値とは一致しません。
- デフォルトのロードバランシング アルゴリズムを変更しないでください（**port-channel load-balance** コマンドを参照）。スイッチでは、アルゴリズム **source-dest-ip** または **source-dest-ip-port**（Cisco Nexus OS および Cisco IOS の **port-channel load-balance** コマンドを参照）を使用することをお勧めします。クラスタ内の ASA へのトラフィックが均等に分散されなくなることがあるため、ロードバランシング アルゴリズムでは、**vlan** キーワードを使用しないでください。
- **lacp port-priority** コマンドと **lacp system-priority** コマンドは、スパンド EtherChannel には使用されません。
- スパンド EtherChannel を使用している場合、クラスタリングが完全にイネーブルになるまで、ポートチャネルインターフェイスは起動しません。この要件により、クラスタのアクティブではないユニットにトラフィックが転送されるのが防がれます。

手順

ステップ 1 チャネル グループに追加するインターフェイスを指定します。

interface *physical_interface*

例：

```
ciscoasa(config)# interface gigabitethernet 0/0
```

physical_interface ID には、タイプ、スロット、およびポート番号（type slot/port）が含まれます。チャネル グループのこの最初のインターフェイスによって、グループ内の他のすべてのインターフェイスのタイプと速度が決まります。

ステップ 2 EtherChannel にこのインターフェイスを割り当てます。

channel-group *channel_id* **mode active** [**vss-id** {**1** | **2**}]

例：

```
ciscoasa(config-if)# channel-group 1 mode active
```

channel_id は 1 ～ 48 です。このチャネル ID のポートチャネル インターフェイスがコンフィギュレーションにまだ存在しない場合は、自動的に追加されます。

interface port-channel *channel_id*

active モードだけがスパンド EtherChannel に対してサポートされます。

VSS または vPC の 2 台のスイッチに ASA を接続する場合は、このインターフェイスをどのスイッチに接続するかを指定するために **vss-id** キーワードを設定します（1 または 2）。また、ステップ 6 で **port-channel span-cluster vss-load-balance** コマンドをポートチャネル インターフェイスに対して使用する必要があります。

ステップ 3 インターフェイスをイネーブルにします。

no shutdown

ステップ 4 （オプション）EtherChannel にさらにインターフェイスを追加するには、上記のプロセスを繰り返します。

例：

```
ciscoasa(config)# interface gigabitethernet 0/1
ciscoasa(config-if)# channel-group 1 mode active
ciscoasa(config-if)# no shutdown
```

ユニットごとに複数のインターフェイスが EtherChannel に含まれていると、VSS または vPC のスイッチに接続する場合に役立ちます。デフォルトでは、クラスタの全メンバで最大 16 個のアクティブ インターフェイスのうち、スパンド EtherChannel が使用できるのは 8 個だけであることに注意してください。残りの 8 インターフェイスはリンク障害時のためのスタンバイです。8 個より多くのアクティブ インターフェイスを使用するには（ただしスタンバイ インターフェイスではなく）、**clacp static-port-priority** コマンドを使用してダイナミック ポート プライオリティをディセーブルにします。ダイナミック ポート プライオリティをディセーブルにすると、クラスタ全体で最大 32 個のアクティブ リンクを使用できます。たとえば、16 台の ASA から成るクラスタの場合は、各 ASA で最大 2 個のインターフェイスを使用でき、スパンド EtherChannel の合計は 32 インターフェイスとなります。

ステップ 5 ポートチャネル インターフェイスを指定します。

interface port-channel *channel_id*

例：

```
ciscoasa(config)# interface port-channel 1
```

このインターフェイスは、チャネル グループにインターフェイスを追加したときに自動的に作成されたものです。

ステップ 6 この EtherChannel をスパンド EtherChannel として設定します。

port-channel span-cluster [**vss-load-balance**]

例：

```
ciscoasa(config-if)# port-channel span-cluster
```

ASA を VSS または vPC の 2 台のスイッチに接続する場合は、**vss-load-balance** キーワードを使用して VSS ロードバランシングをイネーブルにする必要があります。この機能を使用すると、ASA と VSS（または vPC）ペアとの間の物理リンク接続の負荷が確実に分散されます。ロードバランシングをイネーブルにする前に、各メンバーインターフェイスに対して **channel-group** コマンドの **vss-id** キーワードを設定する必要があります（ステップ 2 を参照）。

ステップ 7 （オプション）ポートチャネル インターフェイスのイーサネット プロパティを設定します。この設定は、個別インターフェイスに対して設定されたプロパティよりも優先されます。

これらのパラメータはチャネル グループのすべてのインターフェイスで一致している必要があるため、この方法はこれらのパラメータを設定するショートカットになります。

ステップ 8 （オプション）この EtherChannel 上に VLAN サブインターフェイスを作成する予定の場合は、この時点で作成します。

例：

```
ciscoasa(config)# interface port-channel 1.10
ciscoasa(config-if)# vlan 10
```

この手順の残りの部分は、サブインターフェイスに適用されます。

ステップ 9 （マルチ コンテキスト モード）コンテキストにインターフェイスを割り当てます。その後で、次のとおりに入力します。

changeto context *name*
interface port-channel *channel_id*

例：

```
ciscoasa(config)# context admin
ciscoasa(config)# allocate-interface port-channel1
ciscoasa(config)# changeto context admin
```

```
ciscoasa(config-if)# interface port-channel 1
```

マルチ コンテキスト モードの場合は、インターフェイス コンフィギュレーションの残りの部分は各コンテキスト内で行われます。

ステップ 10 インターフェイスの名前を指定します。

nameif *name*

例：

```
ciscoasa(config-if)# nameif inside
```

name は最大 48 文字のテキスト文字列です。大文字と小文字は区別されません。名前を変更するには、このコマンドで新しい値を再入力します。

ステップ 11 ファイアウォール モードに応じて、次のいずれかを実行します。

- ルーテッド モード：IPv4 アドレスと IPv6 アドレスの一方または両方を設定します。

  （IPv4）

  ip address *ip_address* [*mask*]

  （IPv6）

  ipv6 address *ipv6-prefix*/*prefix-length*

  例：

  ```
  ciscoasa(config-if)# ip address 10.1.1.1 255.255.255.0
  ciscoasa(config-if)# ipv6 address 2001:DB8::1001/32
  ```

  DHCP、PPPoE、および IPv6 自動設定はサポートされません。

- トランスペアレント モード：インターフェイスをブリッジ グループに割り当てます。

  bridge-group *number*

  例：

  ```
  ciscoasa(config-if)# bridge-group 1
  ```

  number は、1 ～ 100 の整数です。ブリッジ グループには最大 4 個のインターフェイスを割り当てることができます。同一インターフェイスを複数のブリッジグループに割り当てることはできません。BVI のコンフィギュレーションには IP アドレスが含まれていることに注意してください。

ステップ 12 セキュリティ レベルを設定します。

security-level *number*

例：

```
ciscoasa(config-if)# security-level 50
```

number には、0（最下位）～ 100（最上位）の整数を指定します。

ステップ 13 潜在的なネットワークの接続問題を回避するために、スパンドEtherChannelのグローバルMACアドレスを設定します。

mac-address *mac_address*

例：

```
ciscoasa(config-if)# mac-address 000C.F142.4CDE
```

MAC アドレスが手動設定されている場合、その MAC アドレスは現在のマスター ユニットに留まります。MAC アドレスを設定していない場合に、マスター ユニットが変更された場合、新しいマスターユニットはインターフェイスに新しいMACアドレスを使用します。これにより、一時的なネットワークの停止が発生する可能性があります。

マルチコンテキストモードでは、コンテキスト間でインターフェイスを共有する場合は、MAC アドレスの自動生成を有効にして、手動で MAC アドレスを設定しなくてすむようにします。非共有インターフェイスの場合は、このコマンドを使用して MAC アドレスを手動で設定する必要があることに注意してください。

mac_address は、H.H.H 形式で指定します。H は 16 ビットの 16 進数です。たとえば、MAC アドレス 00-0C-F1-42-4C-DE は、000C.F142.4CDE と入力します。

自動生成された MAC アドレスも使用する場合、手動で割り当てる MAC アドレスの最初の 2 バイトには A2 を使用できません。

ブートストラップ コンフィギュレーションの作成

クラスタ内の各ユニットがクラスタに参加するには、ブートストラップ コンフィギュレーションが必要です。

マスター ユニットのブートストラップの設定

クラスタ内の各ユニットがクラスタに参加するには、ブートストラップ コンフィギュレーションが必要です。 一般的には、クラスタに参加するように最初に設定したユニットがマスター ユニットとなります。クラスタリングをイネーブルにした後で、選定期間が経過すると、クラスタのマスター ユニットが選定されます。最初はクラスタ内のユニットが 1 つだけであるため、そのユニットがマスター ユニットになります。それ以降クラスタに追加されるユニットは、スレーブ ユニットとなります。

始める前に

- コンフィギュレーションをバックアップします。後でクラスタから脱退する必要が生じたときに備えて、コンフィギュレーションを復元できるようにしておくためです。

- マルチ コンテキスト モードの場合、システム実行スペースで次の手順を実行します。コンテキストからシステム実行スペースに切り替えるには、**changeto system** コマンドを入力します。
- クラスタ制御リンクで使用するためのジャンボ フレームの予約をイネーブルにすることを推奨します。
- クラスタリングをイネーブルまたはディセーブルにするには、コンソール ポートを使用する必要があります。Telnet または SSH を使用することはできません。
- クラスタ制御リンクを除いて、コンフィギュレーション内のインターフェイスはすべて、クラスタ IP プールを指定して設定されているか、スパンド EtherChannel として設定されている必要があります。この設定は、クラスタリングをイネーブルにする前に、インターフェイス モードに応じて行います。既存のインターフェイス コンフィギュレーションがある場合は、そのインターフェイス コンフィギュレーションをクリアすることも（**clear configure interface**）、インターフェイスをクラスタ インターフェイスに変換することもできます。これは、クラスタリングをイネーブルにする前に行います。
- 稼働中のクラスタにユニットを追加すると、一時的に、限定的なパケット/接続ドロップが発生することがあります。これは予定どおりの動作です。
- クラスタ制御リンクのサイズをあらかじめ決定しておきます。クラスタ制御リンクのサイズ （349 ページ）を参照してください。

手順

ステップ 1 クラスタに参加する前に、クラスタ制御リンク インターフェイスをイネーブルにします。

後でクラスタリングをイネーブルにするときに、このインターフェイスをクラスタ制御リンクとして識別します。

十分な数のインターフェイスがある場合は、複数のクラスタ制御リンク インターフェイスを結合して 1 つの EtherChannel とすることを推奨します。この EtherChannel は ASA に対してローカルであり、スパンド EtherChannel ではありません。

クラスタ制御リンク インターフェイス コンフィギュレーションは、マスター ユニットからスレーブ ユニットには複製されませんが、同じコンフィギュレーションを各ユニットで使用する必要があります。このコンフィギュレーションは複製されないため、クラスタ制御リンク インターフェイスの設定は各ユニットで個別に行う必要があります。

- VLAN サブインターフェイスをクラスタ制御リンクとして使用することはできません。
- 管理 *x/x* インターフェイスをクラスタ制御リンクとして使用することはできません（単独か EtherChannel かにかかわらず）。
- ASA FirePOWER モジュールを搭載した ASA 5585-X では、クラスタ制御リンクに ASA FirePOWER モジュール上のインターフェイスではなく、ASA インターフェイスを使用することを推奨しています。モジュール インターフェイスは、ソフトウェア アップグレード中に発生するリロードを含め、モジュールのリロード中に最大 30 秒間トラフィックを

ドロップできます。ただし、必要に応じて、モジュールインターフェイスとASAインターフェイスを同じクラスタ制御リンク EtherChannel で使用できます。モジュール インターフェイスがドロップした場合、EtherChannel の残りのインターフェイスはまだ稼働しています。ASA 5585-X ネットワーク モジュールは別のオペレーティング システムを実行しないため、この問題の影響を受けません。

a) インターフェイス コンフィギュレーション モードを開始します。

interface *interface_id*

例：

```
ciscoasa(config)# interface tengigabitethernet 0/6
```

b) （任意、EtherChannel の場合）EtherChannel にこの物理インターフェイスを割り当てます。

channel-group *channel_id* **mode on**

例：

```
ciscoasa(config-if)# channel-group 1 mode on
```

channel_id は 1 ～ 48 です。このチャネル ID のポートチャネル インターフェイスがコンフィギュレーションにまだ存在しない場合は、自動的に追加されます。

interface port-channel *channel_id*

クラスタ制御リンクでの不要なトラフィックを削減できるように、クラスタ制御リンクのメンバー インターフェイスに対しては On モードを使用することを推奨します。クラスタ制御リンクは LACP トラフィックのオーバーヘッドを必要としません。これは隔離された、安定したネットワークであるからです。**注**：データ EtherChannel を Active モードに設定することをお勧めします。

c) インターフェイスをイネーブルにします。

no shutdown

必要があるのはインターフェイスのイネーブル化だけです。インターフェイスの名前などのパラメータを設定しないでください。

d) （EtherChannel の場合）EtherChannel に追加するインターフェイスごとに繰り返します。

例：

```
ciscoasa(config)# interface tengigabitethernet 0/7
ciscoasa(config-if)# channel-group 1 mode on
ciscoasa(config-if)# no shutdown
```

ステップ 2 （オプション）クラスタ制御リンク インターフェイスの最大伝送ユニットを指定します。

mtu cluster *bytes*

例：

```
ciscoasa(config)# mtu cluster 9000
```

MTU を 1400 ～ 9198 バイトの間で設定します。デフォルトの MTU は 1500 バイトです。

MTU を 1600 バイト以上に設定することを推奨します。このようにするには、この手順を続ける前にジャンボ フレームの予約をイネーブルにする必要があります。ジャンボ フレームの予約には、ASA のリロードが必要です。

このコマンドはグローバル コンフィギュレーション コマンドですが、ユニット間で複製されないブートストラップ コンフィギュレーションの一部でもあります。

ステップ 3 クラスタに名前を付け、クラスタ コンフィギュレーション モードにします。

cluster group *name*

例：

```
ciscoasa(config)# cluster group pod1
```

名前は 1 ～ 38 文字の ASCII 文字列であることが必要です。クラスタ グループはユニットあたり 1 つしか設定できません。クラスタのすべてのメンバが同じ名前を使用する必要があります。

ステップ 4 クラスタのこのメンバの名前を指定します。

local-unit *unit_name*

1 ～ 38 文字の一意の ASCII 文字列を使用します。各ユニットに固有の名前が必要です。クラスタ内の他のユニットと同じ名前を付けることはできません。

例：

```
ciscoasa(cfg-cluster)# local-unit unit1
```

ステップ 5 クラスタ制御リンク インターフェイス（EtherChannel を推奨）を指定します。

cluster-interface *interface_id* **ip** *ip_address mask*

例：

```
ciscoasa(cfg-cluster)# cluster-interface port-channel2 ip 192.168.1.1 255.255.255.0
INFO: Non-cluster interface config is cleared on Port-Channel2
```

サブインターフェイスと管理インターフェイスは許可されません。

IP アドレスには IPv4 アドレスを指定します。IPv6 は、このインターフェイスではサポートされません。このインターフェイスには、**nameif** を設定することはできません。

ユニットごとに、同じネットワークにある別の IP アドレスを指定します。

ステップ 6 マスター ユニットの選択に対するこのユニットのプライオリティを設定します。

priority *priority_number*

例：

```
ciscoasa(cfg-cluster)# priority 1
```

プライオリティは 1 ～ 100 であり、1 が最高のプライオリティです。

ステップ 7 （オプション）クラスタ制御リンクの制御トラフィックの認証キーを設定します。

key *shared_secret*

例：

```
ciscoasa(cfg-cluster)# key chuntheunavoidable
```

共有秘密は、1 ～ 63 文字の ASCII 文字列です。共有秘密は、キーを生成するために使用されます。このコマンドは、データパス トラフィック（接続状態アップデートや転送されるパケットなど）には影響しません。データパス トラフィックは、常にクリア テキストとして送信されます。

ステップ 8 （オプション）LACP のダイナミック ポート プライオリティをディセーブルにします。

clacp static-port-priority

一部のスイッチはダイナミック ポート プライオリティをサポートしていないため、このコマンドはスイッチの互換性を高めます。さらに、このコマンドは、9 ～ 32 のアクティブ スパンド EtherChannel メンバーのサポートをイネーブルにします。このコマンドを使用しないと、サポートされるのは 8 個のアクティブ メンバと 8 個のスタンバイ メンバのみです。このコマンドをイネーブルにした場合、スタンバイ メンバは使用できません。すべてのメンバがアクティブです。

ステップ 9 （オプション）cLACP システム ID およびシステムのプライオリティを手動で指定します。

clacp system-mac {*mac_address* | **auto**} [**system-priority** *number*]

例：

```
ciscoasa(cfg-cluster)# clacp system-mac 000a.0000.aaaa
```

スパンド EtherChannel を使用するときは、ASA は cLACP を使用してネイバー スイッチとの間で EtherChannel のネゴシエーションを行います。cLACP ネゴシエーションの際に、同じクラスタ内の ASA は互いに連携するため、スイッチには 1 つの（仮想）デバイスであるかのように見えます。cLACP ネゴシエーションのパラメータの 1 つであるシステム ID は、MAC アドレスの形式をとります。クラスタ内のすべての ASA が同じシステム ID を使用します。これはマスター ユニットによって自動生成され（デフォルト）、すべてのセカンダリ ユニットに複製されます。あるいは、このコマンドに *H.H.H* の形式で手動で指定することもできます。H は 16 ビットの 16 進数です。（たとえば、MAC アドレス 00-0A-00-00-AA-AA は、000A.0000.AAAA と入力します）。トラブルシューティングの目的で、たとえば、識別が容易な MAC アドレスを使用できるように、手動で MAC アドレスを設定することがあります。一般的には、自動生成された MAC アドレスを使用します。

システム プライオリティ（1 ～ 65535）は、どのユニットがバンドルの決定を行うかを決めるために使用されます。デフォルトでは、ASA はプライオリティ 1（最高のプライオリティ）を使用します。このプライオリティは、スイッチのプライオリティよりも高いことが必要です。

このコマンドは、ブートストラップ コンフィギュレーションの一部ではなく、マスターユニットからスレーブユニットに複製されます。ただし、クラスタリングをイネーブルにした後は、この値は変更できません。

ステップ 10 クラスタリングをイネーブルにします。

enable [**noconfirm**]

例：

```
ciscoasa(cfg-cluster)# enable
INFO: Clustering is not compatible with following commands:
policy-map global_policy
 class inspection_default
 inspect skinny
policy-map global_policy
 class inspection_default
  inspect sip
 Would you like to remove these commands? [Y]es/[N]o:Y

INFO: Removing incompatible commands from running configuration...
Cryptochecksum (changed): f16b7fc2 a742727e e40bc0b0 cd169999
INFO: Done
```

enable コマンドが入力されると、ASA は実行コンフィギュレーションをスキャンして、クラスタリングに対応していない機能の非互換コマンドの有無を調べます。デフォルト コンフィギュレーションにあるコマンドも、これに該当することがあります。互換性のないコマンドを削除するように求められます。応答として **No** を入力した場合は、クラスタリングはイネーブルになりません。確認を省略し、互換性のないコマンドを自動的に削除するには、**noconfirm** キーワードを使用します。

最初にイネーブルにしたユニットについては、マスターユニット選定が発生します。最初のユニットは、その時点でクラスタの唯一のメンバーであるため、そのユニットがマスターユニットになります。この期間中にコンフィギュレーション変更を実行しないでください。

クラスタリングをディセーブルにするには、**no enable** コマンドを入力します。

（注） クラスタリングをディセーブルにした場合は、すべてのデータ インターフェイスがシャットダウンされ、管理専用インターフェイスだけがアクティブになります。

例

次の例では、管理インターフェイスを設定し、クラスタ制御リンク用のデバイス ローカル EtherChannel を設定し、その後で、「unit1」という名前の ASA のクラスタリングをイネーブルにします。これは最初にクラスタに追加されるユニットであるため、マスター ユニットになります。

```
ip local pool mgmt 10.1.1.2-10.1.1.9
ipv6 local pool mgmtipv6 2001:DB8::1002/32 8
interface management 0/0
   nameif management
   ip address 10.1.1.1 255.255.255.0 cluster-pool mgmt
   ipv6 address 2001:DB8::1001/32 cluster-pool mgmtipv6
   security-level 100
   management-only
   no shutdown

interface tengigabitethernet 0/6
   channel-group 1 mode on
   no shutdown

interface tengigabitethernet 0/7
   channel-group 1 mode on
   no shutdown

cluster group pod1
   local-unit unit1
   cluster-interface port-channel1 ip 192.168.1.1 255.255.255.0
   priority 1
   key chuntheunavoidable
   enable noconfirm
```

スレーブ ユニットのブートストラップの設定

スレーブ ユニットを設定するには、次の手順に従います。

始める前に

- クラスタリングをイネーブルまたはディセーブルにするには、コンソール ポートを使用する必要があります。Telnet または SSH を使用することはできません。
- コンフィギュレーションをバックアップします。後でクラスタから脱退する必要が生じたときに備えて、コンフィギュレーションを復元できるようにしておくためです。
- マルチ コンテキスト モードでは、システム実行スペースで次の手順を実行します。コンテキストからシステム実行スペースに切り替えるには、**changeto system** コマンドを入力します。
- クラスタ制御リンクで使用するためのジャンボ フレームの予約をイネーブルにすることを推奨します。
- コンフィギュレーション内に、クラスタリング用として設定されていないインターフェイスがある場合は（たとえば、デフォルト コンフィギュレーションの管理 0/0 インターフェイス）、スレーブユニットとしてクラスタに参加させることができます（現在の選定でマスターになる可能性はありません）。
- 稼働中のクラスタにユニットを追加すると、一時的に、限定的なパケット/接続ドロップが発生することがあります。これは予定どおりの動作です。

手順

ステップ 1 マスターユニットに設定したものと同じクラスタ制御リンク インターフェイスを設定します。

例：

```
ciscoasa(config)# interface tengigabitethernet 0/6
ciscoasa(config-if)# channel-group 1 mode on
ciscoasa(config-if)# no shutdown
ciscoasa(config)# interface tengigabitethernet 0/7
ciscoasa(config-if)# channel-group 1 mode on
ciscoasa(config-if)# no shutdown
```

ステップ 2 マスター ユニットに設定したものと同じ MTU を指定します。

例：

```
ciscoasa(config)# mtu cluster 9000
```

ステップ 3 マスター ユニットに設定したものと同じクラスタ名を指定します。

例：

```
ciscoasa(config)# cluster group pod1
```

ステップ 4 クラスタのこのメンバに一意の文字列で名前を指定します。

local-unit *unit_name*

例：

```
ciscoasa(cfg-cluster)# local-unit unit2
```

1 ～ 38 文字の ASCII 文字列を指定します。

各ユニットに固有の名前が必要です。クラスタ内の他のユニットと同じ名前を付けることはできません。

ステップ 5 マスター ユニットに設定したものと同じクラスタ制御リンク インターフェイスを指定しますが、ユニットごとに同じネットワーク上の異なる IP アドレスを指定します。

cluster-interface *interface_id* **ip** *ip_address mask*

例：

```
ciscoasa(cfg-cluster)# cluster-interface port-channel2 ip 192.168.1.2 255.255.255.0
INFO: Non-cluster interface config is cleared on Port-Channel2
```

IP アドレスには IPv4 アドレスを指定します。IPv6 は、このインターフェイスではサポートされません。このインターフェイスには、**nameif** を設定することはできません。

各ユニットに固有の名前が必要です。クラスタ内の他のユニットと同じ名前を付けることはできません。

ステップ 6 マスターユニットの選択に対するこのユニットのプライオリティを設定します。通常は、マスター ユニットより高い値にします。

priority *priority_number*

例：

```
ciscoasa(cfg-cluster)# priority 2
```

プライオリティを 1 ～ 100 に設定します。1 が最高のプライオリティです。

ステップ 7 マスター ユニットに設定したものと同じ認証キーを設定します。

例：

```
ciscoasa(cfg-cluster)# key chuntheunavoidable
```

ステップ 8 クラスタリングをイネーブルにします。

enable as-slave

enable as-slave コマンドを使用することによって、コンフィギュレーションに関するすべての非互換性（主として、クラスタリングに対してまだ設定されていないインターフェイスの存在）を回避できます。このコマンドを実行すると、クラスタに参加させるスレーブが現在の選定においてマスターとなる可能性をなくすことができます。スレーブのコンフィギュレーションは、マスター ユニットから同期されたコンフィギュレーションによって上書きされます。

クラスタリングをディセーブルにするには、**no enable** コマンドを入力します。

（注） クラスタリングをディセーブルにした場合は、すべてのデータ インターフェイスがシャットダウンされ、管理インターフェイスだけがアクティブになります。

例

次の例には、スレーブ ユニット unit2 のコンフィギュレーションが含まれています。

```
interface tengigabitethernet 0/6

channel-group 1 mode on
no shutdown

interface tengigabitethernet 0/7

channel-group 1 mode on
no shutdown

cluster group pod1
```

```
local-unit unit2
cluster-interface port-channel1 ip 192.168.1.2 255.255.255.0
priority 2
key chuntheunavoidable
enable as-slave
```

クラスタリング動作のカスタマイズ

クラスタリング ヘルス モニタリング、TCP 接続複製の遅延、フローのモビリティ、他の最適化をカスタマイズできます。

マスター ユニットで次の手順を実行します。

ASA クラスタの基本パラメータの設定

マスター ユニット上のクラスタ設定をカスタマイズできます。

始める前に

- マルチ コンテキスト モードでは、マスター ユニット上のシステム実行スペースで次の手順を実行します。コンテキストからシステム実行スペースに切り替えるには、**changeto system** コマンドを入力します。

手順

ステップ 1 クラスタの設定モードを開始します。

cluster group *name*

ステップ 2 （任意）スレーブユニットからマスターユニットへのコンソール複製をイネーブルにします。

console-replicate

この機能はデフォルトで無効に設定されています。ASA は、特定の重大イベントが発生したときに、メッセージを直接コンソールに出力します。コンソール複製をイネーブルにすると、スレーブ ユニットからマスター ユニットにコンソール メッセージが送信されるので、モニタが必要になるのはクラスタのコンソール ポート 1 つだけとなります。

のヘルス モニタリングの設定

この手順では、ユニットとインターフェイスのヘルス モニタリングを設定します。

たとえば、管理インターフェイスなど、必須以外のインターフェイスのヘルス モニタリングをディセーブルにすることができます。任意のポート チャネル ID、冗長 ID、単一の物理インターフェイス ID、をモニタできます。ヘルス モニタリングは VLAN サブインターフェイス、

または VNI や BVI などの仮想インターフェイスでは実行されません。クラスタ制御リンクのモニタリングは設定できません。このリンクは常にモニタされています。

手順

ステップ 1 クラスタの設定モードを開始します。

cluster group *name*

例：

```
ciscoasa(config)# cluster group test
ciscoasa(cfg-cluster)#
```

ステップ 2 クラスタ ユニットのヘルス チェック機能をカスタマイズします。

health-check [**holdtime** *timeout*] [**vss-enabled**]

ユニットのヘルスを確認するため、ASA のクラスタ ユニットはクラスタ制御リンクで他のユニットにキープアライブ メッセージを送信します。ユニットが保留時間内にピア ユニットからキープアライブ メッセージを受信しない場合は、そのピア ユニットは応答不能またはデッド状態と見なされます。

- **holdtime** *timeout*：ユニットのキープアライブト ステータス メッセージの時間間隔を指定します。指定できる範囲は .8 ～ 45 秒で、デフォルトは 3 秒です。
- **vss-enabled**：クラスタ制御リンクのすべての EtherChannel インターフェイスでキープアライブ メッセージをフラッディングして、少なくとも 1 台のスイッチがそれを受信できるようにします。EtherChannel としてクラスタ制御リンクを設定し（推奨）、VSS または vPC ペアに接続している場合、**vss-enabled** オプションをイネーブルにする必要がある場合があります。一部のスイッチでは、VSS/vPC の 1 つのユニットがシャット ダウンまたは起動すると、そのスイッチに接続された EtherChannel メンバー インターフェイスが ASA に対してアップ状態であるように見えますが、これらのインターフェイスはスイッチ側のトラフィックを通していません。ASA holdtime timeout を低い値（0.8 秒など）に設定した場合、ASA が誤ってクラスタから削除される可能性があり、ASA はキープアライブ メッセージをこれらのいずれかの EtherChannel インターフェイスに送信します。

何らかのトポロジ変更（たとえばデータ インターフェイスの追加/削除、ASA、またはスイッチ上のインターフェイスの有効化/無効化、VSS または vPC を形成するスイッチの追加）を行うときには、ヘルス チェック機能を無効にし、無効化したインターフェイスのモニタリングも無効にしてください（**no health-check monitor-interface**）。トポロジの変更が完了して、コンフィギュレーション変更がすべてのユニットに同期されたら、ヘルス チェック機能を再度イネーブルにできます。

例：

```
ciscoasa(cfg-cluster)# health-check holdtime 5
```

ステップ 3 インターフェイスでインターフェイス ヘルス チェックを無効化します。

no health-check monitor-interface *interface_id*

インターフェイスのヘルスチェックはリンク障害をモニタします。特定の論理インターフェイスのすべての物理ポートが、特定のユニット上では障害が発生したが、別のユニット上の同じ論理インターフェイスでアクティブポートがある場合、そのユニットはクラスタから削除されます。ASA がメンバをクラスタから削除するまでの時間は、インターフェイスのタイプと、そのユニットが確立済みメンバであるか、またはクラスタに参加しようとしているかによって異なります。デフォルトでは、ヘルスチェックはすべてのインターフェイスでイネーブルになっています。このコマンドの **no** 形式を使用してディセーブル（無効）にすることができます。たとえば、管理インターフェイスなど、必須以外のインターフェイスのヘルスモニタリングをディセーブルにすることができます。

- *interface_id*：ポートチャネル ID と冗長 ID、または単一の物理インターフェイス ID のモニタリングを無効にします。ヘルス モニタリングは VLAN サブインターフェイス、または VNI や BVI などの仮想インターフェイスでは実行されません。クラスタ制御リンクのモニタリングは設定できません。このリンクは常にモニタされています。

何らかのトポロジ変更（たとえばデータ インターフェイスの追加/削除、ASA、またはスイッチ上のインターフェイスの有効化/無効化、VSS または vPC を形成するスイッチの追加）を行うときには、ヘルス チェック機能（**no health-check**）を無効にし、無効化したインターフェイスのモニタリングも無効にしてください。トポロジの変更が完了して、コンフィギュレーション変更がすべてのユニットに同期されたら、ヘルス チェック機能を再度イネーブルにできます。

例：

```
ciscoasa(cfg-cluster)# no health-check monitor-interface management0/0
```

例

次の例では、ヘルスチェック保留時間を .3 秒に設定し、VSS を有効にし、管理に使用されるイーサネット 1/2 インターフェイスのモニタリングを無効にし。

```
ciscoasa(config)# cluster group test
ciscoasa(cfg-cluster)# health-check holdtime .3 vss-enabled
ciscoasa(cfg-cluster)# no health-check monitor-interface ethernet1/2
```

接続の再分散

接続の再分散を設定できます。詳細については、新しい TCP 接続のクラスタ全体での再分散（330 ページ）を参照してください。

手順

ステップ 1 クラスタの設定モードを開始します。

cluster group *name*

ステップ 2 （オプション）TCP トラフィックの接続の再分散を有効化します。

conn-rebalance [**frequency** *seconds*]

例：

```
ciscoasa(cfg-cluster)# conn-rebalance frequency 60
```

このコマンドは、デフォルトでディセーブルになっています。有効化されている場合は、ASA は負荷情報を定期的に交換し、新しい接続の負荷を高負荷のデバイスから低負荷のデバイスに移動します。負荷情報を交換する間隔を、1 ～ 360 秒の範囲内で指定します。デフォルトは 5 秒です。

サイト間トポロジに対しては接続の再分散を設定しないでください。異なるサイトのクラスタ メンバには接続を再分散できません。

クラスタ メンバの管理

クラスタを導入した後は、コンフィギュレーションを変更し、クラスタ メンバを管理できます。

非アクティブなメンバーになる

クラスタの非アクティブなメンバーになるには、クラスタリング コンフィギュレーションは変更せずに、そのユニット上でクラスタリングをディセーブルにします。

（注） ASAが（手動で、またはヘルスチェック エラーにより）非アクティブになると、すべてのデータインターフェイスがシャットダウンされます。管理専用インターフェイスのみがトラフィックを送受信できます。トラフィック フローを再開させるには、クラスタリングを再びイネーブルにします。または、そのユニットをクラスタから完全に削除します。管理インターフェイスは、そのユニットがクラスタ IP プールから受け取った IP アドレスを使用して引き続き稼働状態となります。ただし、リロードしてもユニットがクラスタ内でまだアクティブではない場合（クラスタリングが無効な状態で設定を保存した場合など）、管理インターフェイスは無効になります。それ以降のコンフィギュレーション作業には、コンソール ポートを使用する必要があります。

始める前に

- コンソール ポートを使用する必要があります。クラスタリングのイネーブルまたはディセーブルを、リモート CLI 接続から行うことはできません。
- マルチ コンテキスト モードの場合は、この手順をシステム実行スペースで実行します。まだシステム コンフィギュレーション モードに入っていない場合は、**changeto system** コマンドを入力します。

手順

ステップ 1 クラスタの設定モードを開始します。

cluster group *name*

例：

```
ciscoasa(config)# cluster group pod1
```

ステップ 2 クラスタリングをディセーブルにします。

no enable

このユニットがマスターユニットであった場合は、新しいマスターの選定が実行され、別のメンバがマスター ユニットになります。

クラスタ コンフィギュレーションは維持されるので、後でクラスタリングを再度イネーブルにできます。

メンバーの非アクティブ化

ログインしているユニット以外のメンバを非アクティブにするには、次のステップを実行します。

（注） ASA が非アクティブになると、すべてのデータ インターフェイスがシャットダウンされます。管理専用インターフェイスのみがトラフィックを送受信できます。トラフィック フローを再開するには、クラスタリングを再度有効にします。管理インターフェイスは、そのユニットがクラスタ IP プールから受け取った IP アドレスを使用して引き続き稼働状態となります。ただし、リロードしてもユニットがクラスタ内でまだアクティブではない場合（クラスタリングが無効な状態で設定を保存した場合など）、管理インターフェイスは無効になります。それ以降のコンフィギュレーション作業には、コンソール ポートを使用する必要があります。

始める前に

マルチ コンテキスト モードの場合は、この手順をシステム実行スペースで実行します。まだシステム コンフィギュレーション モードに入っていない場合は、**changeto system** コマンドを入力します。

手順

ユニットをクラスタから削除します。

cluster remove unit *unit_name*

ブートストラップ コンフィギュレーションは変更されず、マスター ユニットから最後に同期されたコンフィギュレーションもそのままになるので、コンフィギュレーションを失わずに後でそのユニットを再度追加できます。マスター ユニットを削除するためにスレーブ ユニットでこのコマンドを入力した場合は、新しいマスター ユニットが選定されます。

メンバ名を一覧表示するには、**cluster remove unit ?** と入力するか、**show cluster info** コマンドを入力します。

例：

```
ciscoasa(config)# cluster remove unit ?

Current active units in the cluster:
asa2

ciscoasa(config)# cluster remove unit asa2
WARNING: Clustering will be disabled on unit asa2. To bring it back
to the cluster please logon to that unit and re-enable clustering
```

クラスタへの再参加

ユニットがクラスタから削除された場合（たとえば、障害が発生したインターフェイスの場合、またはメンバーを手動で非アクティブにした場合）は、クラスタに手動で再参加する必要があります。

始める前に

- クラスタリングを再イネーブルにするには、コンソール ポートを使用する必要があります。他のインターフェイスはシャットダウンされます。
- マルチ コンテキスト モードの場合は、この手順をシステム実行スペースで実行します。まだシステム コンフィギュレーション モードに入っていない場合は、**changeto system** コマンドを入力します。
- クラスタへの再参加を試行する前に、障害が解決されていることを確認します。

手順

ステップ 1 コンソールで、クラスタ コンフィギュレーション モードを開始します。

cluster group *name*

例：

```
ciscoasa(config)# cluster group pod1
```

ステップ 2 クラスタリングをイネーブルにします。

enable

クラスタからの脱退

クラスタから完全に脱退するには、クラスタ ブートストラップ コンフィギュレーション全体を削除する必要があります。各メンバの現在のコンフィギュレーションは（プライマリ ユニットから同期されて）同じであるため、クラスタから脱退すると、クラスタリング前のコンフィギュレーションをバックアップから復元するか、IP アドレスの競合を避けるためコンフィギュレーションを消去して初めからやり直すことも必要になります。

始める前に

コンソール ポートを使用する必要があります。クラスタのコンフィギュレーションを削除すると、管理インターフェイスとクラスタ制御リンクを含むすべてのインターフェイスがシャットダウンされます。さらに、クラスタリングのイネーブルまたはディセーブルを、リモート CLI 接続から行うことはできません。

手順

ステップ 1 セカンダリ ユニットの場合、クラスタリングを次のようにディセーブルにします。

cluster group *cluster_name* **no enable**

例：

```
ciscoasa(config)# cluster group cluster1
ciscoasa(cfg-cluster)# no enable
```

クラスタリングがセカンダリ ユニット上でイネーブルになっている間は、コンフィギュレーション変更を行うことはできません。

ステップ 2 クラスタ コンフィギュレーションをクリアします。

clear configure cluster

ASAは、管理インターフェイスとクラスタ制御リンクを含むすべてのインターフェイスをシャットダウンします。

ステップ 3 クラスタ インターフェイス モードをディセーブルにします。

no cluster interface-mode

モードはコンフィギュレーションには保存されないため、手動でリセットする必要があります。

ステップ 4 バックアップ コンフィギュレーションがある場合、実行コンフィギュレーションにバックアップ コンフィギュレーションをコピーします。

copy *backup_cfg* **running-config**

例：

```
ciscoasa(config)# copy backup_cluster.cfg running-config

Source filename [backup_cluster.cfg]?

Destination filename [running-config]?
ciscoasa(config)#
```

ステップ 5 コンフィギュレーションをスタートアップに保存します。

write memory

ステップ 6 バックアップ コンフィギュレーションがない場合は、管理アクセスを再設定します。たとえば、インターフェイス IP アドレスを変更し、正しいホスト名を復元します。

マスター ユニットの変更

⚠

注意 マスターユニットを変更する最良の方法は、マスターユニットでクラスタリングを無効にし、新しいマスターの選択を待ってから、クラスタリングを再度有効にする方法です。マスターにするユニットを厳密に指定する必要がある場合は、この項の手順を使用します。ただし、中央集中型機能の場合は、この手順を使用してマスターユニット変更を強制するとすべての接続がドロップされるので、新しいマスター ユニット上で接続を再確立する必要があります。

マスター ユニットを変更するには、次の手順を実行します。

始める前に

マルチ コンテキスト モードの場合は、この手順をシステム実行スペースで実行します。まだシステム コンフィギュレーション モードに入っていない場合は、**changeto system** コマンドを入力します。

手順

新しいユニットをマスター ユニットとして設定します。

cluster master unit *unit_name*

例：

```
ciscoasa(config)# cluster master unit asa2
```

メイン クラスタ IP アドレスへの再接続が必要になります。

メンバ名を一覧表示するには、**cluster master unit ?**（現在のユニットを除くすべての名前が表示される）と入力するか、**show cluster info** コマンドを入力します。

クラスタ全体でのコマンドの実行

コマンドをクラスタ内のすべてのメンバに、または特定のメンバに送信するには、次の手順を実行します。**show** コマンドをすべてのメンバに送信すると、すべての出力が収集されて現在のユニットのコンソールに表示されます。その他のコマンド、たとえば **capture** や **copy** も、クラスタ全体での実行を活用できます。

手順

コマンドをすべてのメンバに送信します。ユニット名を指定した場合は、特定のメンバに送信されます。

cluster exec [**unit** *unit_name*] *command*

例：

```
ciscoasa# cluster exec show xlate
```

メンバー名を一覧表示するには、**cluster exec unit ?**（現在のユニットを除くすべての名前が表示される）と入力するか、**show cluster info** コマンドを入力します。

例

同じキャプチャ ファイルをクラスタ内のすべてのユニットから同時に TFTP サーバにコピーするには、マスター ユニットで次のコマンドを入力します。

```
ciscoasa# cluster exec copy /pcap capture: tftp://10.1.1.56/capture1.pcap
```

複数の PCAP ファイル（各ユニットから 1 つずつ）が TFTP サーバにコピーされます。宛先のキャプチャ ファイル名には自動的にユニット名が付加され、capture1_asa1.pcap、capture1_asa2.pcap などとなります。この例では、asa1 および asa2 がクラスタ ユニット名です。

次の例では、**cluster exec show port-channel summary** コマンドの出力に、クラスタの各メンバーの EtherChannel 情報が表示されています。

```
ciscoasa# cluster exec show port-channel summary
master(LOCAL):*************************************************************
 Number of channel-groups in use: 2
Group  Port-channel  Protocol  Span-cluster  Ports
------+-------------+-----------+-----------------------------------------------
1         Po1             LACP       Yes  Gi0/0(P)
2         Po2             LACP       Yes  Gi0/1(P)
 slave:********************************************************************
 Number of channel-groups in use: 2
Group  Port-channel  Protocol  Span-cluster   Ports
------+-------------+-----------+-----------------------------------------------
1         Po1             LACP       Yes   Gi0/0(P)
2         Po2             LACP       Yes   Gi0/1(P)
```

ASA クラスタのモニタリング

クラスタの状態と接続をモニタおよびトラブルシューティングできます。

クラスタ ステータスのモニタリング

クラスタの状態のモニタリングについては、次のコマンドを参照してください。

- **show cluster info** [**health**]

  キーワードを指定しないで **show cluster info** コマンドを実行すると、クラスタ内のすべてのメンバのステータスが表示されます。

  show cluster info health コマンドは、インターフェイス、ユニットおよびクラスタ全体の現在の状態を表示します。

  show cluster info コマンドについては次の出力を参照してください。

```
ciscoasa# show cluster info
Cluster stbu: On
  This is "C" in state SLAVE
      ID        : 0

            Version   : 9.4(1)
      Serial No.: P3000000025
      CCL IP    : 10.0.0.3
      CCL MAC   : 000b.fcf8.c192
      Last join : 17:08:59 UTC Sep 26 2011
      Last leave: N/A
Other members in the cluster:
  Unit "D" in state SLAVE
```

```
    ID        : 1

          Version   : 9.4(1)
    Serial No.: P3000000001
    CCL IP    : 10.0.0.4
    CCL MAC   : 000b.fcf8.c162
    Last join : 19:13:11 UTC Sep 23 2011
    Last leave: N/A
Unit "A" in state MASTER
    ID        : 2

          Version   : 9.4(1)
    Serial No.: JAB0815R0JY
    CCL IP    : 10.0.0.1
    CCL MAC   : 000f.f775.541e
    Last join : 19:13:20 UTC Sep 23 2011
    Last leave: N/A
Unit "B" in state SLAVE
    ID        : 3

          Version   : 9.4(1)
    Serial No.: P3000000191
    CCL IP    : 10.0.0.2
    CCL MAC   : 000b.fcf8.c61e
    Last join : 19:13:50 UTC Sep 23 2011
    Last leave: 19:13:36 UTC Sep 23 2011
```

- **show cluster info transport{asp |cp}**

  次のトランスポート関連の統計情報を表示します。

  - **asp**：データ プレーンのトランスポート統計情報。
  - **cp**：コントロール プレーンのトランスポート統計情報。

- **show cluster history**

  クラスタの履歴を表示します。

クラスタ全体のパケットのキャプチャ

クラスタでのパケットのキャプチャについては、次のコマンドを参照してください。

cluster exec capture

クラスタ全体のトラブルシューティングをサポートするには、**cluster exec capture** コマンドを使用してマスターユニット上でのクラスタ固有トラフィックのキャプチャをイネーブルにします。これで、クラスタ内のすべてのスレーブ ユニットでも自動的にイネーブルになります。

クラスタ リソースのモニタリング

クラスタ リソースのモニタリングについては、次のコマンドを参照してください。

show cluster {**cpu** | **memory** | **resource**} [*options*]

クラスタ全体の集約データを表示します。使用可能な *options* はデータのタイプによって異なります。

クラスタ トラフィックのモニタリング

クラスタ トラフィックのモニタリングについては、次のコマンドを参照してください。

- **show conn [detail]、cluster exec show conn**

  show conn コマンドは、フローがディレクタ、バックアップ、またはフォワーダのどのフローであるかを示します。**cluster exec show conn** コマンドを任意のユニットで使用すると、すべての接続が表示されます。このコマンドの表示からは、1つのフローのトラフィックがクラスタ内のさまざまな ASA にどのように到達するかがわかります。クラスタのスループットは、ロード バランシングの効率とコンフィギュレーションによって異なります。このコマンドを利用すると、ある接続のトラフィックがクラスタ内をどのように流れるかが簡単にわかります。また、ロードバランサがフローのパフォーマンスにどのように影響を与えるかを理解するのに役立ちます。

  次に、**show conn detail** コマンドの出力例を示します。

```
ciscoasa/ASA2/slave# show conn detail
12 in use, 13 most used
Cluster stub connections: 0 in use, 46 most used
Flags: A - awaiting inside ACK to SYN, a - awaiting outside ACK to SYN,
       B - initial SYN from outside, b - TCP state-bypass or nailed,
       C - CTIQBE media, c - cluster centralized,
       D - DNS, d - dump, E - outside back connection, e - semi-distributed,
       F - outside FIN, f - inside FIN,
       G - group, g - MGCP, H - H.323, h - H.225.0, I - inbound data,
       i - incomplete, J - GTP, j - GTP data, K - GTP t3-response
       k - Skinny media,
       M - SMTP data, m - SIP media, n - GUP
       O - outbound data, o - offloaded,
       P - inside back connection,
       Q - Diameter, q - SQL*Net data,
       R - outside acknowledged FIN,
       R - UDP SUNRPC, r - inside acknowledged FIN, S - awaiting inside SYN,
       s - awaiting outside SYN, T - SIP, t - SIP transient, U - up,
       V - VPN orphan, W - WAAS,
       w - secondary domain backup,
       X - inspected by service module,
       x - per session, Y - director stub flow, y - backup stub flow,
       Z - Scansafe redirection, z - forwarding stub flow
ESP outside: 10.1.227.1/53744 NP Identity Ifc: 10.1.226.1/30604, , flags c, idle 0s,
 uptime
1m21s, timeout 30s, bytes 7544, cluster sent/rcvd bytes 0/0, owners (0,255) Traffic
 received
at interface outside Locally received: 7544 (93 byte/s) Traffic received at interface
 NP
Identity Ifc Locally received: 0 (0 byte/s) UDP outside: 10.1.227.1/500 NP Identity
 Ifc:
10.1.226.1/500, flags -c, idle 1m22s, uptime 1m22s, timeout 2m0s, bytes 1580, cluster
sent/rcvd bytes 0/0, cluster sent/rcvd total bytes 0/0, owners (0,255) Traffic
received at
interface outside Locally received: 864 (10 byte/s) Traffic received at interface
NP Identity
```

```
Ifc Locally received: 716 (8 byte/s)
```

接続フローのトラブルシューティングを行うには、最初にすべてのユニットの接続を一覧表示します。それには、任意のユニットで **cluster exec show conn** コマンドを入力します。ディレクタ（Y）、バックアップ（y）、およびフォワーダ（z）のフラグを持つフローを探します。次の例には、3 つのすべての ASA での 172.18.124.187:22 から 192.168.103.131:44727 への SSH 接続が表示されています。ASA1 には z フラグがあり、この接続のフォワーダであることを表しています。ASA3 には Y フラグがあり、この接続のディレクタであることを表しています。ASA2 には特別なフラグはなく、これがオーナーであることを表しています。アウトバウンド方向では、この接続のパケットは ASA2 の内部インターフェイスに入り、外部インターフェイスから出ていきます。インバウンド方向では、この接続のパケットは ASA1 および ASA3 の外部インターフェイスに入り、クラスタ制御リンクを介して ASA2 に転送され、次に ASA2 の内部インターフェイスから出ていきます。

```
ciscoasa/ASA1/master# cluster exec show conn
ASA1(LOCAL):**********************************************************
18 in use, 22 most used
Cluster stub connections: 0 in use, 5 most used
TCP outside  172.18.124.187:22 inside  192.168.103.131:44727, idle 0:00:00, bytes
37240828, flags z


ASA2:**********************************************************************
12 in use, 13 most used
Cluster stub connections: 0 in use, 46 most used
TCP outside  172.18.124.187:22 inside  192.168.103.131:44727, idle 0:00:00, bytes
37240828, flags UIO


ASA3:**********************************************************************
10 in use, 12 most used
Cluster stub connections: 2 in use, 29 most used
TCP outside  172.18.124.187:22 inside  192.168.103.131:44727, idle 0:00:03, bytes
0, flags  Y
```

- **show cluster info** [**conn-distribution** | **packet-distribution** | **loadbalance**]

  show cluster info conn-distribution コマンドと **show cluster info packet-distribution** コマンドは、すべてのクラスタユニットへのトラフィック分散を表示します。これらのコマンドは、外部ロードバランサを評価し、調整するのに役立ちます。

  show cluster info loadbalance コマンドは、接続再分散の統計情報を表示します。

- **show cluster** {**access-list** | **conn** | **traffic** | **user-identity** | **xlate**} [*options*]

  クラスタ全体の集約データを表示します。使用可能な *options* はデータのタイプによって異なります。

  show cluster access-list コマンドについては次の出力を参照してください。

```
ciscoasa# show cluster access-list
hitcnt display order: cluster-wide aggregated result, unit-A, unit-B,  unit-C, unit-D
access-list cached ACL log flows: total 0, denied 0 (deny-flow-max 4096) alert-interval
 300
access-list 101; 122 elements; name hash: 0xe7d586b5
```

```
access-list 101 line 1 extended permit tcp 192.168.143.0 255.255.255.0 any eq www
(hitcnt=0, 0, 0, 0, 0) 0x207a2b7d
access-list 101 line 2 extended permit tcp any 192.168.143.0 255.255.255.0 (hitcnt=0,
 0, 0, 0, 0) 0xfe4f4947
access-list  101 line 3 extended permit tcp host 192.168.1.183 host 192.168.43.238
(hitcnt=1, 0, 0, 0, 1) 0x7b521307
access-list 101 line 4 extended permit tcp host 192.168.1.116 host 192.168.43.238
(hitcnt=0, 0, 0, 0, 0) 0x5795c069
access-list 101 line 5 extended permit tcp host 192.168.1.177 host 192.168.43.238
(hitcnt=1, 0, 0, 1, 0) 0x51bde7ee
access list 101 line 6 extended permit tcp host 192.168.1.177 host 192.168.43.13
(hitcnt=0, 0, 0, 0, 0) 0x1e68697c
access-list 101 line 7 extended permit tcp host 192.168.1.177 host 192.168.43.132
(hitcnt=2, 0, 0, 1, 1) 0xc1ce5c49
access-list 101 line 8 extended permit tcp host 192.168.1.177 host 192.168.43.192
(hitcnt=3, 0, 1, 1, 1) 0xb6f59512
access-list 101 line 9 extended permit tcp host 192.168.1.177 host 192.168.43.44
(hitcnt=0, 0, 0, 0, 0) 0xdc104200
access-list 101 line 10 extended permit tcp host 192.168.1.112 host 192.168.43.44
(hitcnt=429, 109, 107, 109, 104)
0xce4f281d
access-list 101 line 11 extended permit tcp host 192.168.1.170 host 192.168.43.238
(hitcnt=3, 1, 0, 0, 2) 0x4143a818
access-list 101 line 12 extended permit tcp host 192.168.1.170 host 192.168.43.169
(hitcnt=2, 0, 1, 0, 1) 0xb18dfea4
access-list 101 line 13 extended permit tcp host 192.168.1.170 host 192.168.43.229
(hitcnt=1, 1, 0, 0, 0) 0x21557d71
access-list 101 line 14 extended permit tcp host 192.168.1.170 host 192.168.43.106
(hitcnt=0, 0, 0, 0, 0) 0x7316e016
access-list 101 line 15 extended permit tcp host 192.168.1.170 host 192.168.43.196
(hitcnt=0, 0, 0, 0, 0) 0x013fd5b8
access-list 101 line 16 extended permit tcp host 192.168.1.170 host 192.168.43.75
(hitcnt=0, 0, 0, 0, 0) 0x2c7dba0d
```

使用中の接続の、すべてのユニットでの 合計数を表示するには、次のとおりに入力します。

```
ciscoasa# show cluster conn count
Usage Summary In Cluster:*********************************************
  200 in use (cluster-wide aggregated)
     cl2(LOCAL):**************************************************************
  100 in use, 100 most used

  cl1:*********************************************************************
  100 in use, 100 most used
```

- **show asp cluster counter**

  このコマンドは、データパスのトラブルシューティングに役立ちます。

クラスタのルーティングのモニタリング

クラスタのルーティングについては、次のコマンドを参照してください。

- **show route cluster**
- **debug route cluster**

クラスタのルーティング情報を表示します。

クラスタリングのロギングの設定

クラスタリングのロギングの設定については、次のコマンドを参照してください。

logging device-id

クラスタ内の各ユニットは、syslog メッセージを個別に生成します。**logging device-id** コマンドを使用すると、同一または異なるデバイス ID 付きで syslog メッセージを生成することができ、クラスタ内の同一または異なるユニットからのメッセージのように見せることができます。

クラスタのインターフェイスのモニタリング

クラスタのインターフェイスのモニタリングについては、次のコマンドを参照してください。

- **show cluster interface-mode**

  クラスタ インターフェイスのモードを表示します。

- **show port-channel**

  ポートチャネルがスパンドかどうかに関する情報が含まれます。

- **show lacp cluster {system-mac | system-id}**

  cLACP システム ID およびプライオリティを表示します。

- **debug lacp cluster [all | ccp | misc | protocol]**

  cLACP のデバッグ メッセージを表示します。

クラスタリングのデバッグ

クラスタリングのデバッグについては、次のコマンドを参照してください。

- **debug cluster [ccp | datapath | fsm | general | hc | license | rpc | transport]**

  クラスタリングのデバッグ メッセージを表示します。

- **show cluster info trace**

  show cluster info trace コマンドは、トラブルシューティングのためのデバッグ情報を表示します。

  show cluster info trace コマンドについては次の出力を参照してください。

```
ciscoasa# show cluster info trace
 Feb 02 14:19:47.456 [DBUG]Receive CCP message: CCP_MSG_LOAD_BALANCE
 Feb 02 14:19:47.456 [DBUG]Receive CCP message: CCP_MSG_LOAD_BALANCE
 Feb 02 14:19:47.456 [DBUG]Send CCP message to all: CCP_MSG_KEEPALIVE from 80-1 at
MASTER
```

ASA クラスタリングの例

以下の例には、一般的な導入での ASA のクラスタ関連のすべてのコンフィギュレーションが含まれます。

ASA およびスイッチのコンフィギュレーションの例

次のコンフィギュレーション例は、ASA とスイッチ間の次のインターフェイスを接続します。

ASA インターフェイス	スイッチ インターフェイス
GigabitEthernet 0/2	GigabitEthernet 1/0/15
GigabitEthernet 0/3	GigabitEthernet 1/0/16
GigabitEthernet 0/4	GigabitEthernet 1/0/17
GigabitEthernet 0/5	GigabitEthernet 1/0/18

ASA の設定

各ユニットのインターフェイス モード

```
cluster interface-mode spanned force
```

ASA1 マスター ブートストラップ コンフィギュレーション

```
interface GigabitEthernet0/0
 channel-group 1 mode on
 no shutdown
!
interface GigabitEthernet0/1
 channel-group 1 mode on
 no shutdown
!
interface Port-channel1
 description Clustering Interface
!
cluster group Moya
 local-unit A
 cluster-interface Port-channel1 ip 10.0.0.1 255.255.255.0
 priority 10
 key emphyri0
 enable noconfirm
```

ASA2 スレーブ ブートストラップ コンフィギュレーション

```
interface GigabitEthernet0/0
 channel-group 1 mode on
```

```
 no shutdown
!
interface GigabitEthernet0/1
 channel-group 1 mode on
 no shutdown
!
interface Port-channel1
 description Clustering Interface
!
cluster group Moya
 local-unit B
 cluster-interface Port-channel1 ip 10.0.0.2 255.255.255.0
 priority 11
 key emphyri0
 enable as-slave
```

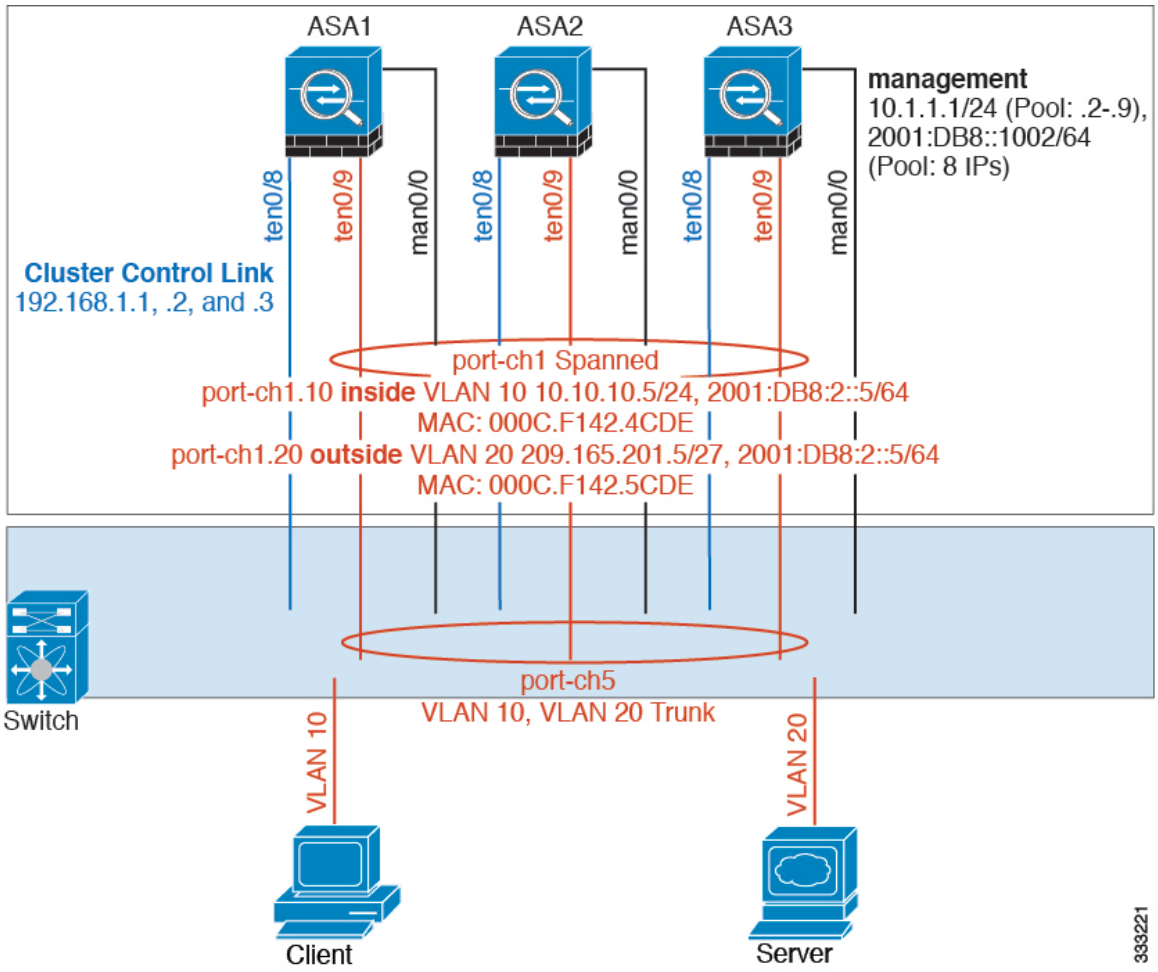
マスター インターフェイス コンフィギュレーション

```
ip local pool mgmt-pool 10.53.195.231-10.53.195.232

interface GigabitEthernet0/2
 channel-group 10 mode active
 no shutdown
!
interface GigabitEthernet0/3
 channel-group 10 mode active
 no shutdown
!
interface GigabitEthernet0/4
 channel-group 11 mode active
 no shutdown
!
interface GigabitEthernet0/5
 channel-group 11 mode active
 no shutdown
!
interface Management0/0
 management-only
 nameif management
 ip address 10.53.195.230 cluster-pool mgmt-pool
 security-level 100
 no shutdown
!
interface Port-channel10
 port-channel span-cluster
 mac-address aaaa.bbbb.cccc
 nameif inside
 security-level 100
 ip address 209.165.200.225 255.255.255.224
!
interface Port-channel11
 port-channel span-cluster
 mac-address aaaa.dddd.cccc
 nameif outside
 security-level 0
 ip address 209.165.201.1 255.255.255.224
```

Cisco IOS スイッチのコンフィギュレーション

```
interface GigabitEthernet1/0/15
 switchport access vlan 201
 switchport mode access
 spanning-tree portfast
 channel-group 10 mode active
!
interface GigabitEthernet1/0/16
 switchport access vlan 201
 switchport mode access
 spanning-tree portfast
 channel-group 10 mode active
!
interface GigabitEthernet1/0/17
 switchport access vlan 401
 switchport mode access
 spanning-tree portfast
 channel-group 11 mode active
!
interface GigabitEthernet1/0/18
 switchport access vlan 401
 switchport mode access
 spanning-tree portfast
 channel-group 11 mode active

interface Port-channel10
 switchport access vlan 201
 switchport mode access

interface Port-channel11
 switchport access vlan 401
 switchport mode access
```

スティック上のファイアウォール



異なるセキュリティ ドメインからのデータ トラフィックには、異なる VLAN が関連付けられます。たとえば内部ネットワーク用には VLAN 10、外部ネットワークには VLAN 20 とします。各 ASA は単一の物理ポートがあり、外部スイッチまたはルータに接続されます。トランキングがイネーブルになっているので、物理リンク上のすべてのパケットが 802.1q カプセル化されます。ASA は、VLAN 10 と VLAN 20 の間のファイアウォールです。

スパンド EtherChannel を使用するときは、スイッチ側ですべてのデータ リンクがグループ化されて 1 つの EtherChannel となります。ASA の 1 つが使用不可能になった場合は、スイッチは残りのユニット間でトラフィックを再分散します。

各ユニットのインターフェイス モード

```
cluster interface-mode spanned force
```

ASA1 マスター ブートストラップ コンフィギュレーション

```
interface tengigabitethernet 0/8

no shutdown
description CCL

cluster group cluster1

local-unit asa1
cluster-interface tengigabitethernet0/8 ip 192.168.1.1 255.255.255.0
priority 1
key chuntheunavoidable
enable noconfirm
```

ASA2 スレーブ ブートストラップ コンフィギュレーション

```
interface tengigabitethernet 0/8

no shutdown
description CCL

cluster group cluster1

local-unit asa2
cluster-interface tengigabitethernet0/8 ip 192.168.1.2 255.255.255.0
priority 2
key chuntheunavoidable
enable as-slave
```

ASA3 スレーブ ブートストラップ コンフィギュレーション

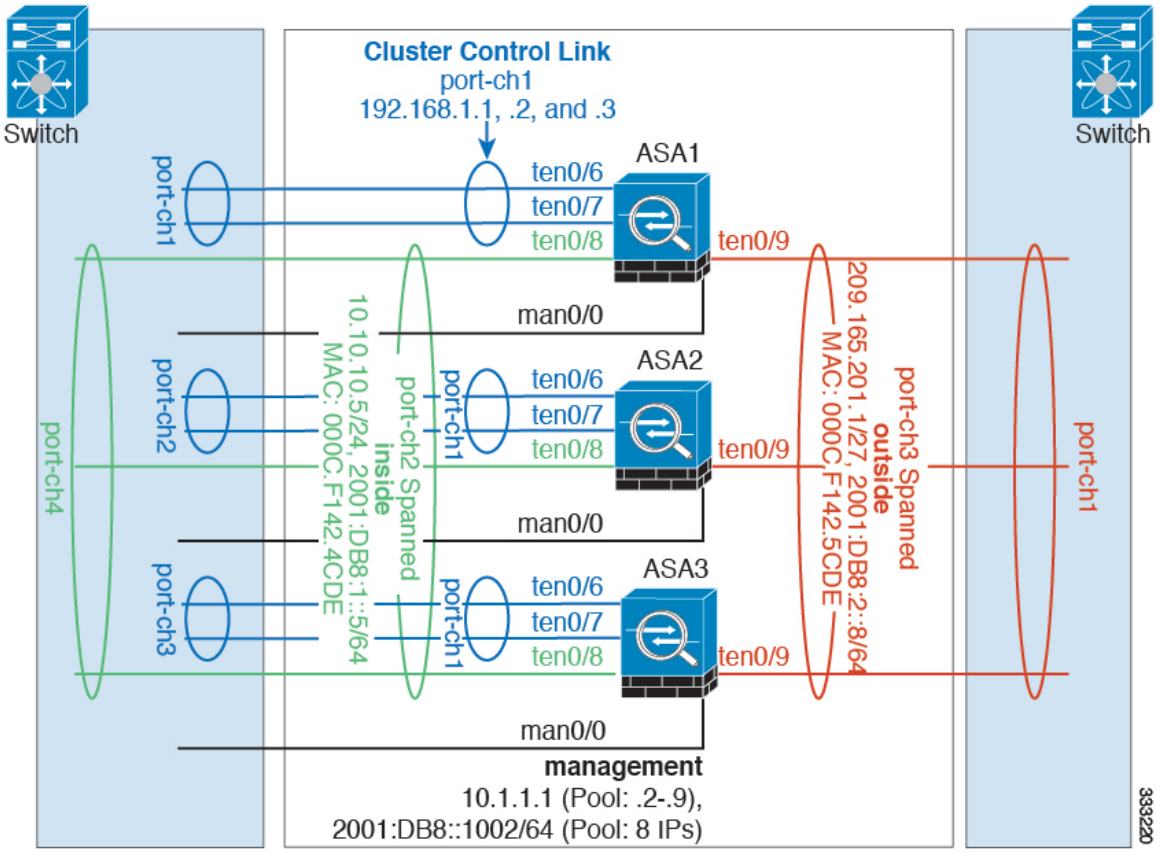
```
interface tengigabitethernet 0/8

no shutdown
description CCL

cluster group cluster1

local-unit asa3
cluster-interface tengigabitethernet0/8 ip 192.168.1.3 255.255.255.0
priority 3
key chuntheunavoidable
enable as-slave
```

マスター インターフェイス コンフィギュレーション

```
ip local pool mgmt 10.1.1.2-10.1.1.9
ipv6 local pool mgmtipv6 2001:DB8::1002/64 8
interface management 0/0

nameif management
ip address 10.1.1.1 255.255.255.0 cluster-pool mgmt
ipv6 address 2001:DB8::1001/32 cluster-pool mgmtipv6
security-level 100
management-only
```

```
no shutdown

interface tengigabitethernet 0/9

channel-group 2 mode active
no shutdown
interface port-channel 2
port-channel span-cluster
interface port-channel 2.10
vlan 10
nameif inside
ip address 10.10.10.5 255.255.255.0
ipv6 address 2001:DB8:1::5/64
mac-address 000C.F142.4CDE
interface port-channel 2.20
vlan 20
nameif outside
ip address 209.165.201.1 255.255.255.224
ipv6 address 2001:DB8:2::8/64
mac-address 000C.F142.5CDE
```

トラフィックの分離



内部ネットワークと外部ネットワークの間で、トラフィックを物理的に分離できます。

上の図に示すように、左側に一方のスパンドEtherChannelがあり、内部スイッチに接続されています。他方は右側にあり、外部スイッチに接続されています。必要であれば、各EtherChannel上にVLANサブインターフェイスを作成することもできます。

各ユニットのインターフェイス モード

```
cluster interface-mode spanned force
```

ASA1 マスター ブートストラップ コンフィギュレーション

```
interface tengigabitethernet 0/6

channel-group 1 mode on
no shutdown

interface tengigabitethernet 0/7

channel-group 1 mode on
no shutdown
interface port-channel 1
description CCL

cluster group cluster1

local-unit asa1
cluster-interface port-channel1 ip 192.168.1.1 255.255.255.0
priority 1
key chuntheunavoidable
enable noconfirm
```

ASA2 スレーブ ブートストラップ コンフィギュレーション

```
interface tengigabitethernet 0/6

channel-group 1 mode on
no shutdown

interface tengigabitethernet 0/7

channel-group 1 mode on
no shutdown
interface port-channel 1
description CCL

cluster group cluster1

local-unit asa2
cluster-interface port-channel1 ip 192.168.1.2 255.255.255.0
priority 2
key chuntheunavoidable
enable as-slave
```

ASA3 スレーブ ブートストラップ コンフィギュレーション

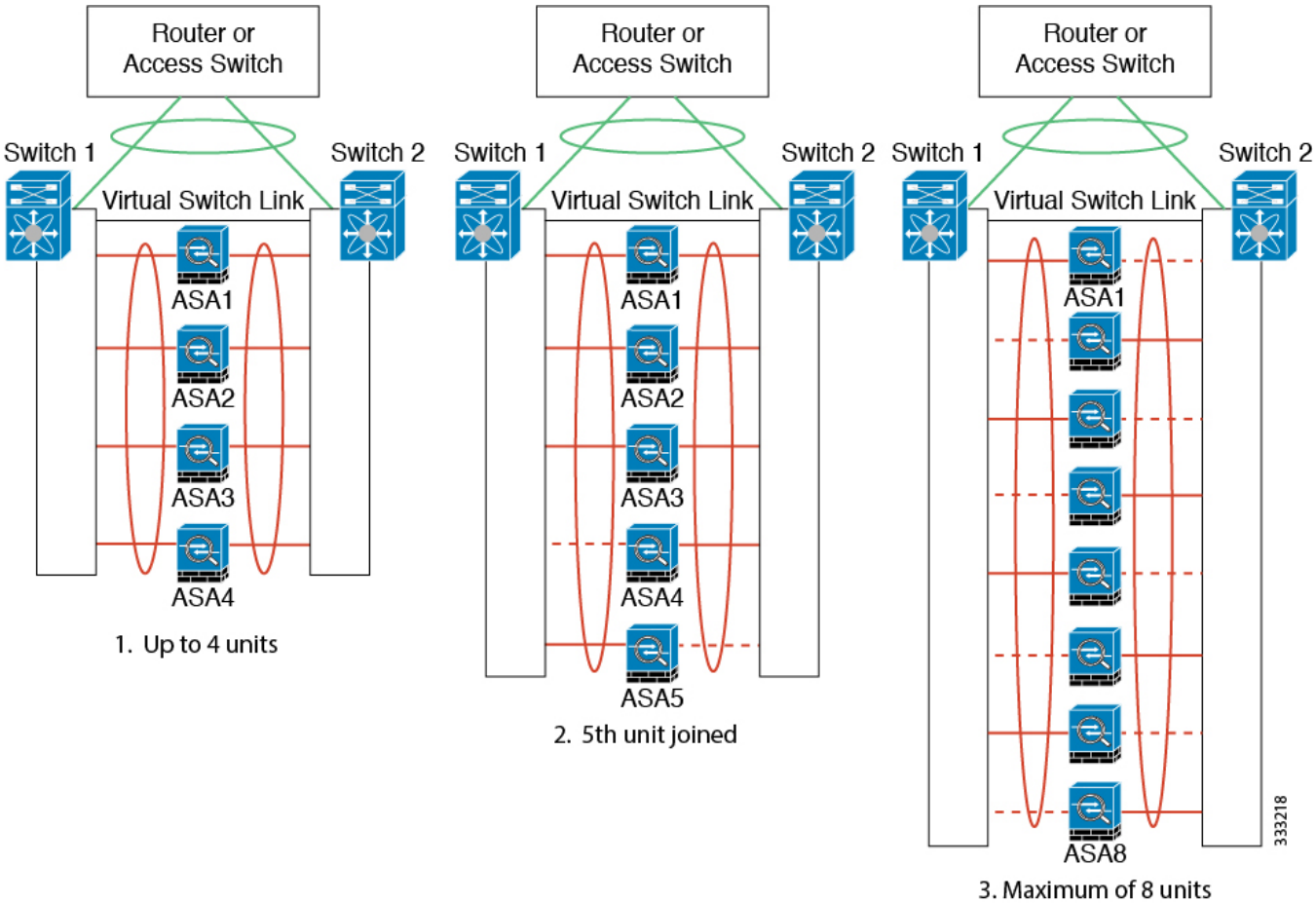
```
interface tengigabitethernet 0/6

channel-group 1 mode on
no shutdown

interface tengigabitethernet 0/7

channel-group 1 mode on
no shutdown
interface port-channel 1
description CCL

cluster group cluster1

local-unit asa3
cluster-interface port-channel1 ip 192.168.1.3 255.255.255.0
priority 3
key chuntheunavoidable
enable as-slave
```

マスター インターフェイス コンフィギュレーション

```
ip local pool mgmt 10.1.1.2-10.1.1.9
ipv6 local pool mgmtipv6 2001:DB8::1002/64 8
interface management 0/0

nameif management
ip address 10.1.1.1 255.255.255.0 cluster-pool mgmt
ipv6 address 2001:DB8::1001/32 cluster-pool mgmtipv6
security-level 100
management-only
no shutdown

interface tengigabitethernet 0/8

channel-group 2 mode active
no shutdown
interface port-channel 2
port-channel span-cluster
nameif inside
ip address 10.10.10.5 255.255.255.0
ipv6 address 2001:DB8:1::5/64
mac-address 000C.F142.4CDE

interface tengigabitethernet 0/9

channel-group 3 mode active
no shutdown
interface port-channel 3
port-channel span-cluster
nameif outside
ip address 209.165.201.1 255.255.255.224
ipv6 address 2001:DB8:2::8/64
mac-address 000C.F142.5CDE
```

スパンド EtherChannel とバックアップ リンク（従来の 8 アクティブ/8 スタンバイ）

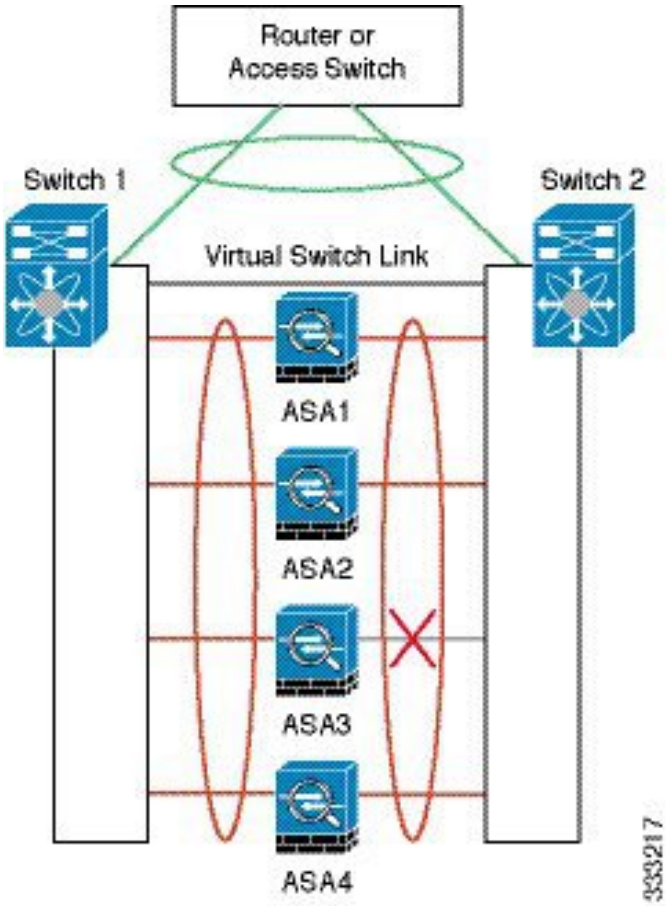
従来の EtherChannel のアクティブ ポートの最大数は、スイッチ側からの 8 に制限されます。8 台の ASA から成るクラスタがあり、EtherChannel にユニットあたり 2 ポートを割り当てた場合は、合計 16 ポートのうち 8 ポートをスタンバイ モードにする必要があります。ASA は、どのリンクをアクティブまたはスタンバイにするかを、LACP を使用してネゴシエートします。VSS または vPC を使用してマルチスイッチ EtherChannel をイネーブルにした場合は、スイッチ間の冗長性を実現できます。ASA では、すべての物理ポートが最初にスロット番号順、次にポート番号順に並べられます。次の図では、番号の小さいポートが「マスター」ポートとなり（たとえば GigabitEthernet 0/0）、他方が「スレーブ」ポートとなります（たとえば GigabitEthernet 0/1）。ハードウェア接続の対称性を保証する必要があります。つまり、すべてのマスター リンクは 1 台のスイッチが終端となり、すべてのスレーブ リンクは別のスイッチが終端となっている必要があります（VSS/vPC が使用されている場合）。次の図は、クラスタに参加するユニットが増えてリンクの総数が増加したときに、どのようになるかを示しています。



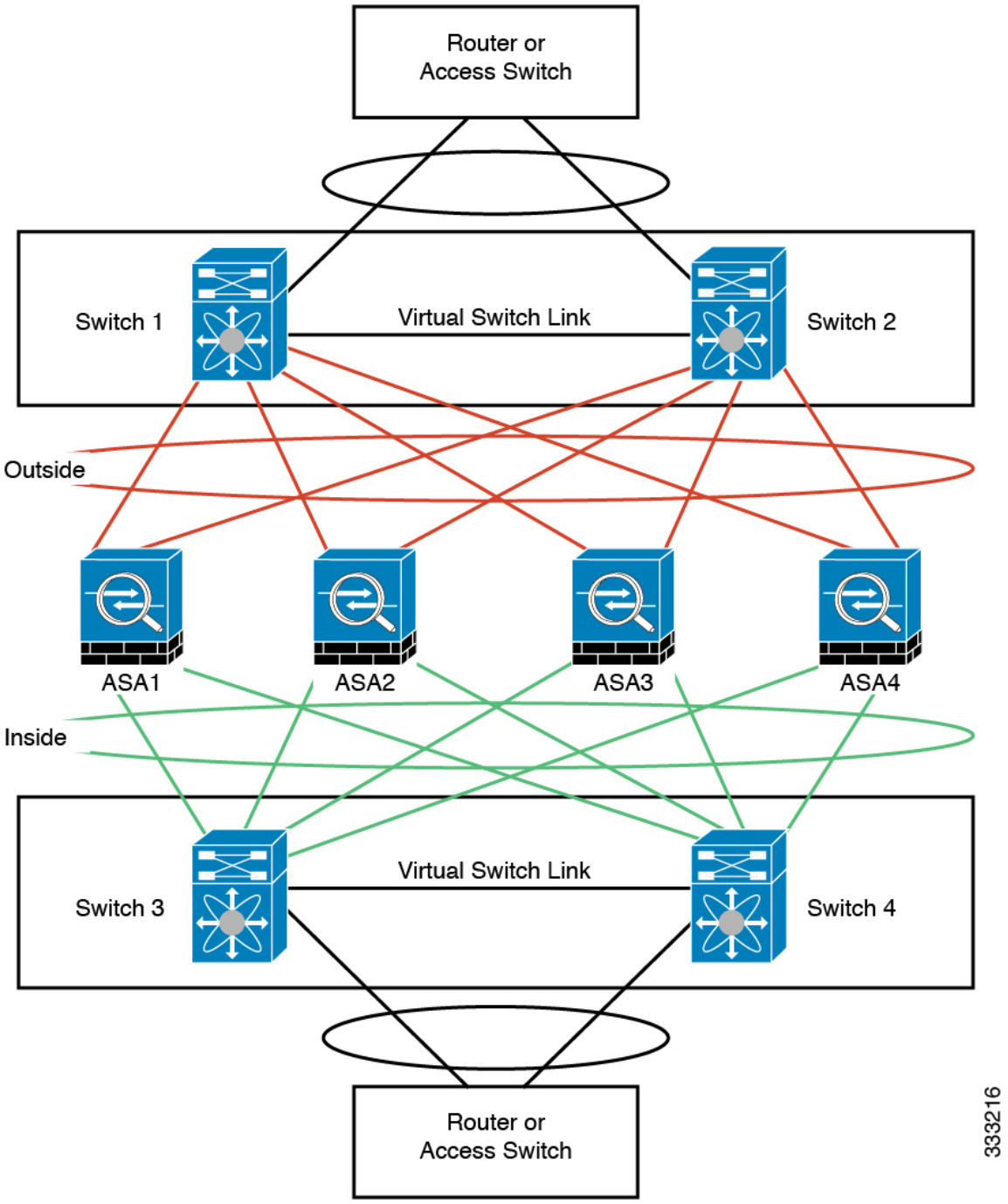
原則として、初めにチャネル内のアクティブ ポート数を最大化し、そのうえで、アクティブなマスター ポートとアクティブなスレーブ ポートの数のバランスを保ちます。5 番目のユニット

がクラスタに参加したときは、トラフィックがすべてのユニットに均等には分散されないことに注意してください。

リンクまたはデバイスの障害が発生したときも、同じ原則で処理されます。その結果、ロードバランシングが理想的な状態にはならないこともあります。次の図は、4 ユニットのクラスタを示しています。このユニットの 1 つで、単一リンク障害が発生しています。



ネットワーク内に複数の EtherChannel を設定することも考えられます。次の図では、EtherChannel が内部に 1 つ、外部に 1 つあります。ASA は、一方の EtherChannel でマスターとスレーブの両方のリンクが障害状態になった場合にクラスタから削除されます。これは、その ASA がすでに内部ネットワークへの接続を失っているにもかかわらず、外部ネットワークからトラフィックを受信するのを防ぐためです。



各ユニットのインターフェイス モード

```
cluster interface-mode spanned force
```

ASA1 マスター ブートストラップ コンフィギュレーション

```
interface tengigabitethernet 0/6

channel-group 1 mode on
no shutdown

interface tengigabitethernet 0/7

channel-group 1 mode on
no shutdown

interface tengigabitethernet 0/8

channel-group 1 mode on
no shutdown

interface tengigabitethernet 0/9

channel-group 1 mode on
no shutdown
interface port-channel 1
description CCL

cluster group cluster1

local-unit asa1
cluster-interface port-channel1 ip 192.168.1.1 255.255.255.0
priority 1
key chuntheunavoidable
enable noconfirm
```

ASA2 スレーブ ブートストラップ コンフィギュレーション

```
interface tengigabitethernet 0/6

channel-group 1 mode on
no shutdown

interface tengigabitethernet 0/7

channel-group 1 mode on
no shutdown

interface tengigabitethernet 0/8

channel-group 1 mode on
no shutdown

interface tengigabitethernet 0/9

channel-group 1 mode on
no shutdown
interface port-channel 1
description CCL

cluster group cluster1

local-unit asa2
cluster-interface port-channel1 ip 192.168.1.2 255.255.255.0
priority 2
```

```
key chuntheunavoidable
enable as-slave
```

ASA3 スレーブ ブートストラップ コンフィギュレーション

```
interface tengigabitethernet 0/6

channel-group 1 mode on
no shutdown

interface tengigabitethernet 0/7

channel-group 1 mode on
no shutdown

interface tengigabitethernet 0/8

channel-group 1 mode on
no shutdown

interface tengigabitethernet 0/9

channel-group 1 mode on
no shutdown
interface port-channel 1
description CCL

cluster group cluster1

local-unit asa3
cluster-interface port-channel1 ip 192.168.1.3 255.255.255.0
priority 3
key chuntheunavoidable
enable as-slave
```

ASA4 スレーブ ブートストラップ コンフィギュレーション

```
interface tengigabitethernet 0/6

channel-group 1 mode on
no shutdown

interface tengigabitethernet 0/7

channel-group 1 mode on
no shutdown

interface tengigabitethernet 0/8

channel-group 1 mode on
no shutdown

interface tengigabitethernet 0/9

channel-group 1 mode on
no shutdown
interface port-channel 1
description CCL
```

```
cluster group cluster1

local-unit asa4
cluster-interface port-channel1 ip 192.168.1.4 255.255.255.0
priority 4
key chuntheunavoidable
enable as-slave
```

マスター インターフェイス コンフィギュレーション

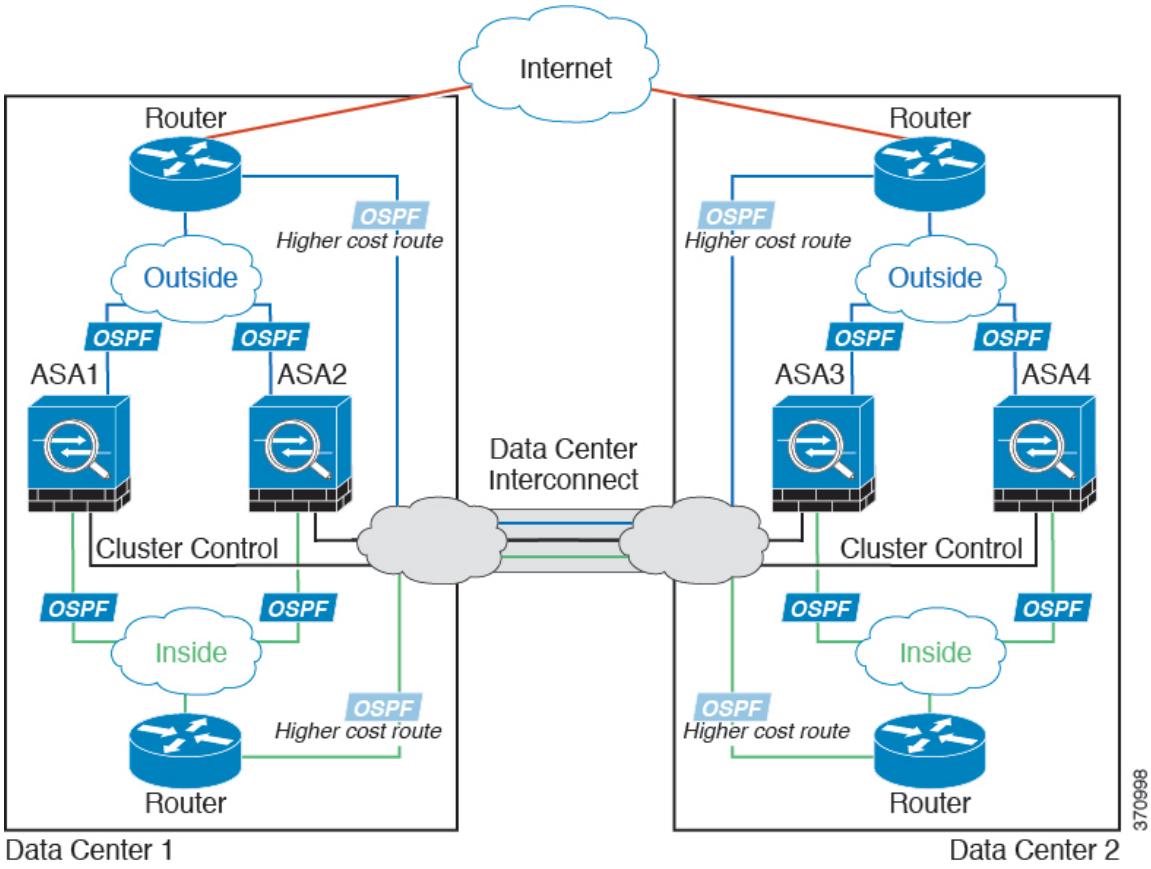
```
ip local pool mgmt 10.1.1.2-10.1.1.9
interface management 0/0

channel-group 2 mode active
no shutdown

interface management 0/1

channel-group 2 mode active
no shutdown
interface port-channel 2
nameif management
ip address 10.1.1.1 255.255.255.0 cluster-pool mgmt
security-level 100
management-only

interface tengigabitethernet 1/6

channel-group 3 mode active vss-id 1
no shutdown

interface tengigabitethernet 1/7

channel-group 3 mode active vss-id 2
no shutdown
interface port-channel 3
port-channel span-cluster vss-load-balance
nameif inside
ip address 10.10.10.5 255.255.255.0
mac-address 000C.F142.4CDE

interface tengigabitethernet 1/8

channel-group 4 mode active vss-id 1
no shutdown

interface tengigabitethernet 1/9

channel-group 4 mode active vss-id 2
no shutdown
interface port-channel 4
port-channel span-cluster vss-load-balance
nameif outside
ip address 209.165.201.1 255.255.255.224
mac-address 000C.F142.5CDE
```

サイト間クラスタリングの例

次の例ではサポートされるクラスタの導入を示します。

個別インターフェイス ルーテッド モード ノースサウス サイト間の例

次の例では、内部ルータと外部ルータの間に配置された（ノースサウス挿入）2 つのデータセンターのそれぞれに 2 つの ASA クラスタ メンバがある場合を示します。クラスタ メンバは、DCI 経由のクラスタ制御リンクによって接続されています。各データセンターの内部ルータと外部ルータは、OSPF と PBR または ECMP を使用してクラスタ メンバ間でトラフィックをロード バランスします。DCI に高コスト ルートを割り当てることにより、特定のサイトのすべての ASA クラスタ メンバがダウンしない限り、トラフィックは各データセンター内に維持されます。1 つのサイトのすべてのクラスタ メンバに障害が発生した場合、トラフィックは各ルータから DCI 経由で他のサイトの ASA クラスタ メンバに送られます。



スパンド EtherChannel トランスペアレント モード ノースサウス サイト間の例

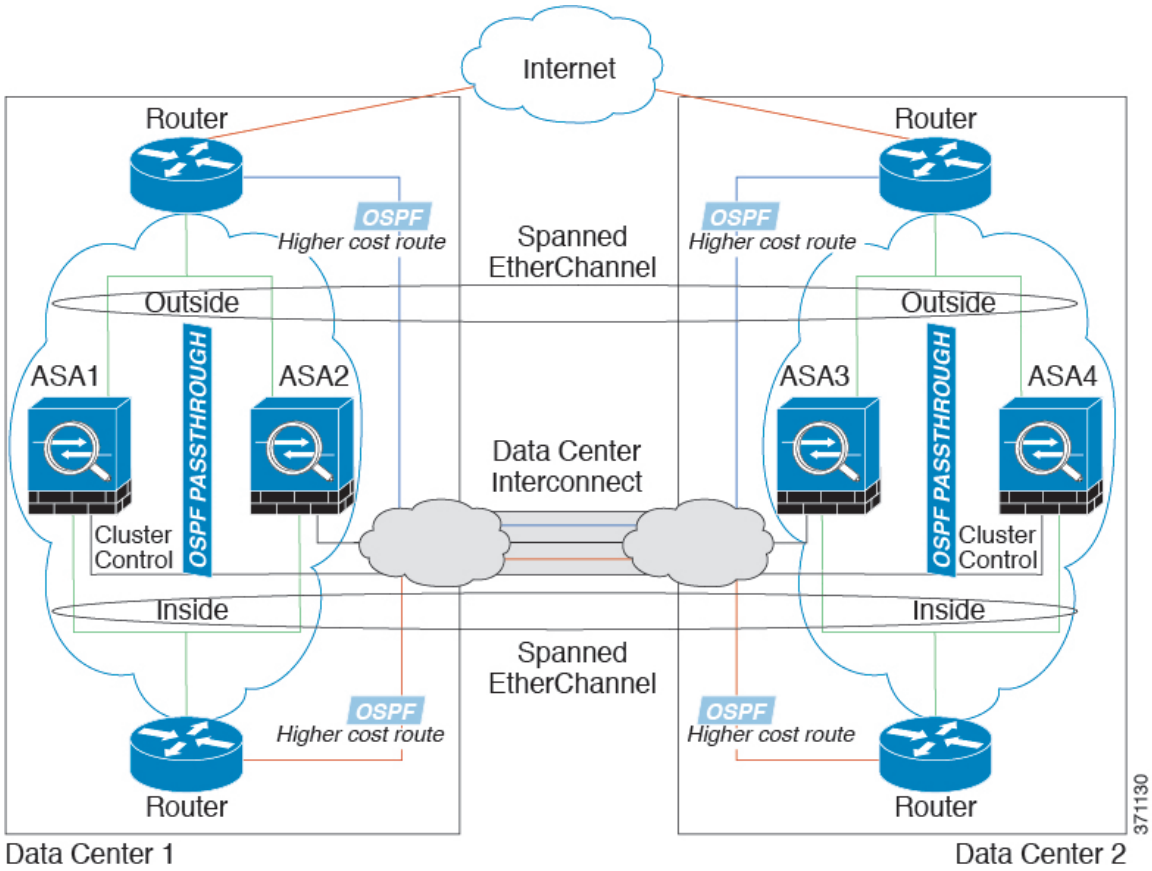
次の例では、内部ルータと外部ルータの間に配置された（ノースサウス挿入）2 つのデータセンターのそれぞれに 2 つのクラスタ メンバがある場合を示します。クラスタ メンバは、DCI 経由のクラスタ制御リンクによって接続されています。各サイトのクラスタ メンバは、内部および外部のスパンド EtherChannels を使用してローカル スイッチに接続します。各 EtherChannel は、クラスタ内のすべてのシャーシにスパンされます。

各データセンターの内部ルータと外部ルータは OSPF を使用し、トランスペアレント ASA を通過します。MAC とは異なり、ルータの IP はすべてのルータで一意です。DCI に高コスト ルートを割り当てることにより、特定のサイトですべてのクラスタ メンバがダウンしない限

り、トラフィックは各データセンター内に維持されます。クラスタが非対称型の接続を維持するため、ASA を通過する低コストのルートは、各サイトで同じブリッジ グループを横断する必要があります。1つのサイトのすべてのクラスタ メンバに障害が発生した場合、トラフィックは各ルータから DCI 経由で他のサイトのクラスタ メンバに送られます。

各サイトのスイッチの実装には、次のものを含めることができます。

- サイト間 VSS/vPC：このシナリオでは、データセンター 1 に 1 台のスイッチをインストールし、データセンター 2 に別のスイッチをインストールします。1つのオプションとして、各データセンターのクラスタ ユニットはローカル スイッチだけに接続し、VSS/vPC トラフィックはDCIを経由します。この場合、接続のほとんどの部分は各データセンターに対してローカルに維持されます。オプションとして、DCIが余分なトラフィック量を処理できる場合、各ユニットをDCI経由で両方のスイッチに接続できます。この場合、トラフィックは複数のデータセンターに分散されるため、DCIを非常に堅牢にするためには不可欠です。
- 各サイトのローカル VSS/vPC：スイッチの冗長性を高めるには、各サイトに 2 つの異なる VSS/vPC ペアをインストールできます。この場合、クラスタ ユニットは、両方のローカル スイッチだけに接続されたデータセンター 1 のシャーシおよびこれらのローカル スイッチに接続されたデータセンター 2 のシャーシとはスパンド EtherChannel を使用しますが、スパンド EtherChannel は基本的に「分離」しています。各ローカル VSS/vPC は、スパンド EtherChannel をサイトローカルの EtherChannel として認識します。

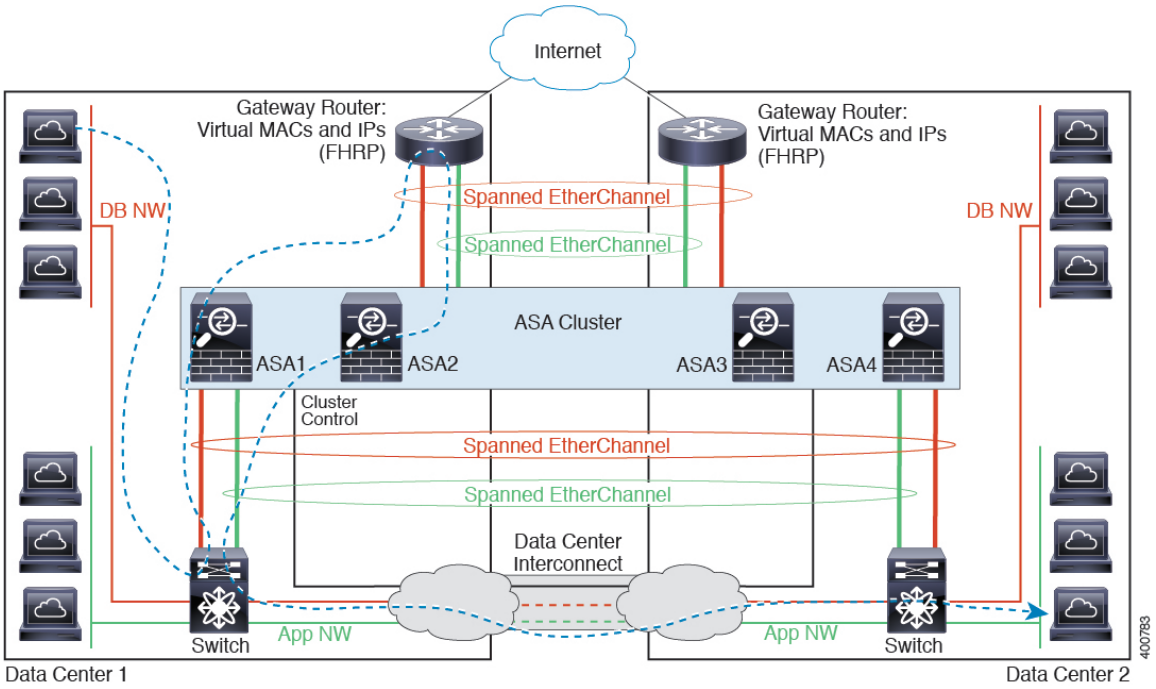


スパンド EtherChannel トランスペアレント モード イーストウェスト サイト間の例

次の例では、各サイトのゲートウェイ ルータと 2 つの内部ネットワーク（アプリケーション ネットワークと DB ネットワーク）間に配置された（イーストウェスト挿入）2 つのデータセンターのそれぞれに 2 つのクラスタ メンバがある場合を示します。クラスタ メンバは、DCI 経由のクラスタ制御リンクによって接続されています。各サイトのクラスタ メンバは、内部および外部のアプリケーション ネットワークと DB ネットワークの両方にスパンド EtherChannels を使用してローカル スイッチに接続します。各 EtherChannel は、クラスタ内のすべてのシャーシにスパンされます。

各サイトのゲートウェイ ルータは、HSRP などの FHRP を使用して、各サイトで同じ宛先の仮想 MAC アドレス と IP アドレスを提供します。MAC アドレスの予期せぬフラッピングを避けるため、**mac-address-table static** *outside_interface mac_address* コマンドを使用して、ゲートウェイルータの実際の MAC アドレスを ASA MAC アドレステーブルに静的に追加することをお勧めします。これらのエントリがないと、サイト 1 のゲートウェイがサイト 2 のゲートウェイと通信する場合に、そのトラフィックが ASA を通過して、内部インターフェイスからサイト 2 に到達しようとして、問題が発生する可能性があります。データ VLAN は、オーバーレイ トランスポート仮想化（OTV）（または同様のもの）を使用してサイト間に拡張されます。トラフィックがゲートウェイ ルータ宛てである場合にトラフィックが DCI を通過して他のサイトに送信されないようにするには、フィルタを追加する必要があります。1 つのサイトのゲート

ウェイ ルータが到達不能になった場合、トラフィックが他のサイトのゲートウェイに送信されるようにフィルタを削除する必要があります。



vPC/VSS オプションについては、スパンド EtherChannel トランスペアレント モード ノースサウス サイト間の例 （408 ページ）を参照してください。

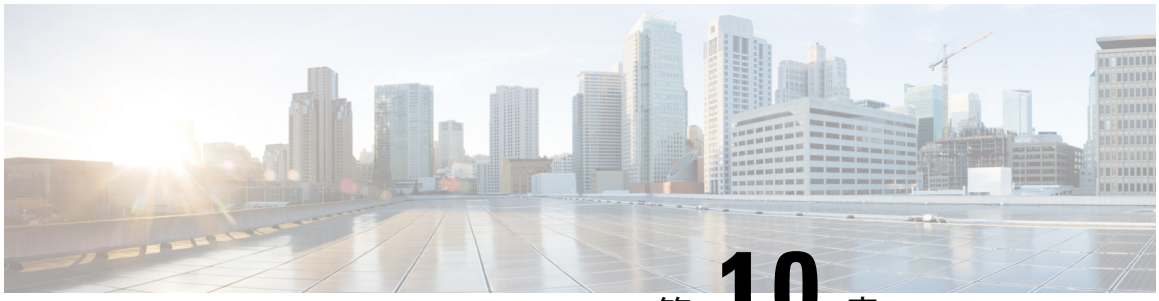
ASA クラスタリングの履歴

機能名	バージョン	機能情報
インターフェイスごとの ASA クラスタのヘルスモニタリングの有効化またはディセーブル化	9.4(1)	ヘルス モニタリングは、インターフェイスごとにイネーブルまたはディセーブルにすることができます。デフォルトでは、ポートチャネル、冗長、および単一のすべての物理インターフェイスでヘルス モニタリングがイネーブルになっています。ヘルス モニタリングは VLAN サブインターフェイス、または VNI や BVI などの仮想インターフェイスでは実行されません。クラスタ制御リンクのモニタリングは設定できません。このリンクは常にモニタされています。たとえば、管理インターフェイスなど、必須以外のインターフェイスのヘルス モニタリングをディセーブルにすることができます。 次のコマンドを導入しました。 **health-check monitor-interface**。

機能名	バージョン	機能情報
DHCP リレーの ASA クラスタリングのサポート	9.4(1)	ASA クラスタで DHCP リレーを設定できます。クライアントの DHCP 要求は、クライアントの MAC アドレスのハッシュを使用してクラスタ メンバにロードバランスされます。DHCP クライアントおよびサーバ機能はサポートされていません。 変更されたコマンドはありません。
ASA クラスタリングでの SIP インスペクションのサポート	9.4(1)	ASA クラスタで SIP インスペクションを設定できます。制御フローは、任意のユニットで作成できますが（ロード バランシングのため）、その子データ フローは同じユニットに存在する必要があります。TLS プロキシ設定はサポートされていません。 **show ssh sessions detail** コマンドが導入されました。
内部ネットワーク間に ASA クラスタ ファイアウォールを備えたトランスペアレントモードのサイト間導入	9.3(2)	各サイトの内部ネットワークとゲートウェイ ルータ間にトランスペアレント モードのクラスタを導入し（AKA イーストウェスト挿入）、サイト間に内部 VLAN を拡張できます。オーバーレイ トランスポート仮想化（OTV）の使用を推奨しますが、ゲートウェイ ルータの重複する MAC アドレスおよび IP アドレスがサイト間で漏えいしないようにする任意の方法を使用できます。HSRP などの First Hop Redundancy Protocol（FHRP）を使用して、同じ仮想 MAC アドレスおよび IP アドレスをゲートウェイ ルータに提供します。
ASA クラスタリングに対する BGP のサポート	9.3(1)	ASA クラスタリングに対する BGP のサポートが追加されました。 次のコマンドを導入しました。**bgp router-id clusterpool**。
トランスペアレント モードでの異なる地理的位置にあるクラスタ メンバのサポート（サイト間）	9.2(1)	トランスペアレント ファイアウォール モードでスパンド EtherChannel モードを使用すると、クラスタ メンバを異なる地理的な場所に配置できるようになりました。ルーテッド ファイアウォール モードのスパンド EtherChannel での Inter-Site クラスタリングはサポートされません。 変更されたコマンドはありません。
クラスタリングに対するスタティック LACP ポートプライオリティのサポート	9.2(1)	一部のスイッチは、LACP でのダイナミック ポート プライオリティをサポートしていません（アクティブおよびスタンバイ リンク）。ダイナミック ポート プライオリティをディセーブルにすることで、スパンド EtherChannel との互換性を高めることができるようになりました。次の注意事項にも従う必要があります。 • クラスタ制御リンク パスのネットワーク エレメントでは、L4 チェックサムを検証しないようにする必要があります。クラスタ制御リンク経由でリダイレクトされたトラフィックには、正しい L4 チェックサムが設定されていません。L4 チェックサムを検証するスイッチにより、トラフィックがドロップされる可能性があります。 • ポートチャネル バンドルのダウンタイムは、設定されているキープアライブ インターバルを超えてはなりません。 **clacp static-port-priority** コマンドが導入されました。

機能名	バージョン	機能情報
スパンド EtherChannel での 32 個のアクティブ リンクのサポート	9.2(1)	ASA EtherChannels は最大 16 個のアクティブ リンクをサポートするようになりました。スパンド EtherChannel ではその機能が拡張されて、vPC の 2 台のスイッチで使用し、ダイナミック ポート プライオリティをディセーブルにした場合、クラスタ全体で最大 32 個のアクティブ リンクをサポートします。スイッチは、16 個のアクティブ リンクの EtherChannel をサポートする必要があります（例：Cisco Nexus 7000 と F2 シリーズ 10 ギガビット イーサネット モジュール）。 8 個のアクティブ リンクをサポートする VSS または vPC のスイッチの場合は、スパンド EtherChannel に 16 個のアクティブ リンクを設定できます（各スイッチに接続された 8 個）。従来は、VSS/vPC で使用する場合であっても、スパンド EtherChannel は 8 個のアクティブ リンクと 8 個のスタンバイ リンクしかサポートしませんでした。 （注） スパンド EtherChannel で 8 個より多くのアクティブ リンクを使用する場合は、スタンバイ リンクも使用できません。9 ～ 32 個のアクティブ リンクをサポートするには、スタンバイ リンクの使用を可能にする cLACP ダイナミック ポート プライオリティをディセーブルにする必要があります。 **clacp static-port-priority** コマンドが導入されました。
ASA 5585-X の 16 のクラスタ メンバのサポート	9.2(1)	ASA 5585-X が 16 ユニット クラスタをサポートするようになりました。 変更されたコマンドはありません。
ASA 5500-X でのクラスタリングのサポート	9.1(4)	ASA 5512-X、ASA 5515-X、ASA 5525-X、ASA 5545-X および ASA 5555-X が 2 ユニット クラスタをサポートするようになりました。2 ユニットのクラスタリングは、基本ライセンスではデフォルトでイネーブルになります。ASA 5512-X では Security Plus ライセンスが必要です。 変更されたコマンドはありません。
ヘルス チェック モニタリングの VSS および vPC によるサポートの強化	9.1(4)	クラスタ制御リンクが EtherChannel として設定されていて（推奨）、VSS または vPC ペアに接続されている場合、ヘルス チェック モニタリングによって安定性を高めることができます。一部のスイッチ（Cisco Nexus 5000 など）では、VSS/vPC の 1 つのユニットがシャットダウンまたは起動すると、そのスイッチに接続されている EtherChannel メンバー インターフェイスが ASA に対してアップと認識される場合がありますが、スイッチ側にはトラフィックが渡されていません。ASA holdtime timeout を低い値（0.8 秒など）に設定した場合、ASA が誤ってクラスタから削除される可能性があり、ASA はキープアライブ メッセージをこれらのいずれかの EtherChannel インターフェイスに送信します。VSS/vPC ヘルス チェック機能をイネーブルにすると、ASA はクラスタ制御リンクのすべての EtherChannel インターフェイスでキープアライブ メッセージをフラッディングして、少なくとも 1 台のスイッチがそれを受信できることを確認します。 次のコマンドを変更しました。 **health-check**[**vss-enabled**]。

機能名	バージョン	機能情報
異なる地理的位置にあるクラスタ メンバのサポート（サイト間）。個別インターフェイス モードのみ	9.1(4)	個別インターフェイス モードを使用すると、クラスタ メンバを異なる地理的な場所に配置できるようになりました。 変更されたコマンドはありません。
ASA 5580 および 5585-X の ASA クラスタリング	9.0(1)	ASA クラスタリングを利用すると、最大で 8 の ASA をグループ化して、1 つの論理デバイスにすることができます。クラスタは、単一デバイスのすべての利便性（管理、ネットワークへの統合）を備える一方で、複数デバイスによって高いスループットおよび冗長性を達成します。ASA クラスタリングは、ASA 5580 および ASA 5585-X でサポートされます。1 つのクラスタ内のすべてのユニットが同一モデル、同一ハードウェア仕様であることが必要です。クラスタリングがイネーブルのときにサポートされない機能のリストについては、コンフィギュレーション ガイドを参照してください。 次のコマンドを導入または変更しました。**channel-group**、**clacp system-mac**、**clear cluster info**、**clear configure cluster**、**cluster exec**、**cluster group**、**cluster interface-mode**、**cluster-interface**、**conn-rebalance**、**console-replicate**、**cluster master unit**、**cluster remove unit**、**debug cluster**、**debug lacp cluster**、**enable**（クラスタ グループ）、**health-check**、**ip address**、**ipv6 address**、**key**（クラスタ グループ）、**local-unit**、**mac-address**（インターフェイス）、**mac-address pool**, **mtu cluster, port-channel span-cluster, priority**（クラスタ グループ）、**prompt cluster-unit**, **show asp cluster counter**、**show asp table cluster chash-table**、**show cluster**、**show cluster info**、**show cluster user-identity**、**show lacp cluster**、および **show running-config cluster**。



第 10 章

Firepower 9300 シャーシ の ASA クラスタ

クラスタリングを利用すると、複数のFirepower 9300 シャーシ ASA をグループ化して、1 つの論理デバイスにすることができます。Firepower 9300 シャーシ シリーズには、Firepower 9300。クラスタは、単一デバイスのすべての利便性（管理、ネットワークへの統合）を備える一方で、複数デバイスによって高いスループットおよび冗長性を達成します。

（注） FirePOWER 9300 は複数のシャーシにまたがる（シャーシ間）クラスタをサポートしません。シャーシ内クラスタリングのみをサポートします。

（注） 一部の機能は、クラスタリングを使用する場合、サポートされません。「クラスタリングでサポートされない機能 （420 ページ）」を参照してください。

Firepower 9300 シャーシでのクラスタリングについて

クラスタは、単一の論理ユニットとして機能する複数のデバイスから構成されます。Firepower 9300 シャーシ にクラスタを展開すると、以下の処理が実行されます。

- ユニット間通信用のクラスタ制御リンク（デフォルトのポート チャネル 48）を作成します。シャーシ内クラスタリングでは、このリンクは、クラスタ通信に Firepower 9300 バックプレーンを使用します。
- アプリケーション内のクラスタ ブートストラップ コンフィギュレーションを作成します。

  クラスタを展開すると、クラスタ名、クラスタ制御リンク インターフェイス、およびその他のクラスタ設定を含む各ユニットに対して、最小限のブートストラップ構成が Firepower 9300 シャーシ スーパーバイザからプッシュされます。 クラスタリング環境をカスタマイズする場合、ブートストラップ コンフィギュレーションの一部は、アプリケーション内でユーザが設定できます。
- スパンドインターフェイスとして、クラスタにデータ インターフェイスを割り当てます。

  シャーシ内クラスタリングでは、スパンドインターフェイスは、シャーシ間クラスタリングのように EtherChannel に制限されません。Firepower 9300 スーパーバイザは共有インターフェイスの複数のモジュールにトラフィックをロードバランシングするために内部で EtherChannel テクノロジーを使用するため、スパンドモードではあらゆるタイプのデータ インターフェイスが機能します。

  （注） 管理インターフェイス以外の個々のインターフェイスはサポートされていません。
- 管理インターフェイスをクラスタ内のすべてのユニットに指定します。

ここでは、クラスタリングの概念と実装について詳しく説明します。クラスタリングの参考資料 （454 ページ）も参照してください。

ブートストラップ コンフィギュレーション

クラスタを展開すると、クラスタ名、クラスタ制御リンク インターフェイス、およびその他のクラスタ設定を含む各ユニットに対して、最小限のブートストラップ構成が Firepower 9300 シャーシ スーパーバイザからプッシュされます。 クラスタリング環境をカスタマイズする場合、ブートストラップ コンフィギュレーションの一部はユーザが設定できます。

クラスタ メンバー

クラスタ メンバーは連携して動作し、セキュリティ ポリシーおよびトラフィック フローの共有を達成します。

クラスタ内のメンバの 1 つが**マスター** ユニットです。マスター ユニットは自動的に決定されます。他のすべてのメンバは**スレーブ** ユニットです。

すべてのコンフィギュレーション作業はマスターユニット上でのみ実行する必要があります。コンフィギュレーションはその後、スレーブ ユニットに複製されます。

機能によっては、クラスタ内でスケーリングしないものがあり、そのような機能についてはマスター ユニットがすべてのトラフィックを処理します。クラスタリングの中央集中型機能 （420 ページ） を参照してください。。

マスターおよびスレーブ ユニットの役割

クラスタ内のメンバの 1 つがマスター ユニットです。マスター ユニットは自動的に決定されます。他のすべてのメンバはスレーブ ユニットです。

すべてのコンフィギュレーション作業はマスターユニット上でのみ実行する必要があります。コンフィギュレーションはその後、スレーブ ユニットに複製されます。

機能によっては、クラスタ内でスケーリングしないものがあり、そのような機能についてはマスター ユニットがすべてのトラフィックを処理します。クラスタリングの中央集中型機能 （420 ページ） を参照してください。。

クラスタ制御リンク

クラスタ制御リンクはユニット間通信用の EtherChannel（ポート チャネル 48）です。シャーシ内クラスタリングでは、このリンクは、クラスタ通信に Firepower 9300 バックプレーンを使用します。

クラスタ制御リンク トラフィックには、制御とデータの両方のトラフィックが含まれます。

制御トラフィックには次のものが含まれます。

- マスター選定。
- コンフィギュレーションの複製
- ヘルス モニタリング。

データ トラフィックには次のものが含まれます。

- ステート複製。
- 接続所有権クエリおよびデータ パケット転送。

クラスタ制御リンク ネットワーク

Firepower 9300 シャーシは、シャーシ ID およびスロット ID（127.2.*chassis_id*.*slot_id*）に基づいて、各ユニットのクラスタ制御リンク インターフェイス IP アドレスを自動生成します。 FXOS とアプリケーション内のどちらでも、この IP アドレスを手動で設定することはできません。クラスタ制御リンク ネットワークには、ユニット間のルータを含めることはできません。レイヤ 2 スイッチングのみが許可されます。

クラスタ インターフェイス

シャーシ内クラスタリングでは、物理インターフェイス、EtherChannel （ポートチャネルとも呼ばれる）の両方を割り当てることができます。クラスタに割り当てられたインターフェイスはクラスタ内のすべてのメンバーのトラフィックのロード バランシングを行うスパンド インターフェイスです。

管理インターフェイス以外の個々のインターフェイスはサポートされていません。

VSS または vPC への接続

インターフェイスに冗長性を確保するため、EtherChannel を VSS または vPC に接続することを推奨します。

設定の複製

クラスタ内のすべてのユニットは、単一のコンフィギュレーションを共有します。コンフィギュレーション変更を加えることができるのはマスターユニット上だけであり、変更は自動的にクラスタ内の他のすべてのユニットに同期されます。

ASA クラスタの管理

ASA クラスタリングを使用することの利点の 1 つは、管理のしやすさです。ここでは、クラスタを管理する方法について説明します。

管理インターフェイス

管理タイプのインターフェイスをクラスタに割り当てる必要があります。このインターフェイスはスパンド インターフェイスではなく、特別な個別インターフェイスです。管理インターフェイスによって各単位に直接接続できます。

メイン クラスタ IP アドレスは、そのクラスタのための固定アドレスであり、常に現在のマスターユニットに属します。アドレス範囲も設定して、現在のマスターを含む各ユニットがその範囲内のローカル アドレスを使用できるようにします。このメイン クラスタ IP アドレスによって、管理アクセスのアドレスが一本化されます。マスターユニットが変更されると、メイン クラスタ IP アドレスは新しいマスター ユニットに移動するので、クラスタの管理をシームレスに続行できます。

たとえば、クラスタを管理するにはメイン クラスタ IP アドレスに接続します。このアドレスは常に、現在のマスター ユニットに関連付けられています。個々のメンバを管理するには、ローカル IP アドレスに接続します。

TFTP や syslog などの発信管理トラフィックの場合、マスター ユニットを含む各ユニットは、ローカル IP アドレスを使用してサーバに接続します。

マスター ユニット管理とスレーブ ユニット管理

すべての管理とモニタリングはマスター ユニットで実行できます。マスター ユニットから、すべてのユニットの実行時統計情報やリソース使用状況などのモニタリング情報を調べることができます。また、クラスタ内のすべてのユニットに対してコマンドを発行することや、コンソール メッセージをスレーブ ユニットからマスター ユニットに複製することもできます。

必要に応じて、スレーブ ユニットを直接モニタできます。マスター ユニットからでもできますが、ファイル管理をスレーブユニット上で実行できます（コンフィギュレーションのバックアップや、イメージの更新など）。次の機能は、マスター ユニットからは使用できません。

- ユニットごとのクラスタ固有統計情報のモニタリング。
- ユニットごとの Syslog モニタリング（コンソール レプリケーションが有効な場合にコンソールに送信される syslog を除く）。
- SNMP
- NetFlow

RSA キー複製

マスター ユニット上で RSA キーを作成すると、そのキーはすべてのスレーブ ユニットに複製されます。メイン クラスタ IP アドレスへの SSH セッションがある場合に、マスターユニットで障害が発生すると接続が切断されます。新しいマスター ユニットは、SSH 接続に対して同じキーを使用するので、新しいマスターユニットに再接続するときに、キャッシュ済みの SSH ホスト キーを更新する必要はありません。

ASDM 接続証明書 IP アドレス不一致

デフォルトでは、自己署名証明書は、ローカル IP アドレスに基づいて ASDM 接続に使用されます。ASDM を使用してメイン クラスタ IP アドレスに接続する場合は、IP アドレス不一致に関する警告メッセージが表示されます。これは、証明書で使用されているのがローカル IP アドレスであり、メイン クラスタ IP アドレスではないからです。このメッセージは無視して、ASDM 接続を確立できます。ただし、この種の警告を回避するには、新しい証明書を登録し、この中でメイン クラスタ IP アドレスと、IP アドレス プールからのすべてのローカル IP アドレスを指定します。この証明書を各クラスタ メンバに使用します。

ASA の各機能とクラスタリング

ASA の一部の機能は ASA クラスタリングではサポートされず、一部はマスター ユニットだけでサポートされます。その他の機能については適切な使用に関する警告がある場合があります。

クラスタリングでサポートされない機能

これらの機能は、クラスタリングがイネーブルのときは設定できず、コマンドは拒否されます。

- TLS プロキシを使用するユニファイド コミュニケーション機能
- 次のアプリケーション インスペクション：
  - CTIQBE
  - GTP
  - H323、H225、および RAS
  - IPsec パススルー
  - MGCP
  - MMP
  - RTSP
  - SCCP（Skinny）
  - WAAS
  - WCCP
- Botnet Traffic Filter
- Auto Update Server
- DHCP クライアント、サーバ、およびプロキシDHCP リレーがサポートされている。
- フェールオーバー
- デッド接続検出（DCD）

クラスタリングの中央集中型機能

次の機能は、マスターユニット上だけでサポートされます。クラスタの場合もスケーリングされません。

（注） 中央集中型機能のトラフィックは、クラスタ制御リンク経由でメンバ ユニットからマスター ユニットに転送されます。

再分散機能を使用する場合は、中央集中型機能のトラフィックが中央集中型機能として分類される前に再分散が行われて、マスター以外のユニットに転送されることがあります。この場合は、トラフィックがマスター ユニットに送り返されます。

中央集中型機能については、マスターユニットで障害が発生するとすべての接続がドロップされるので、新しいマスター ユニット上で接続を再確立する必要があります。

- 次のアプリケーション インスペクション：
  - DCERPC
  - NetBIOS
  - PPTP
  - RADIUS
  - RSH
  - SUNRPC
  - TFTP
  - XDMCP
- ダイナミック ルーティング
- スタティック ルート モニタリング
- IGMP マルチキャスト コントロール プレーン プロトコル処理（データ プレーン フォワーディングはクラスタ全体に分散されます）
- PIM マルチキャスト コントロール プレーン プロトコル処理（データ プレーン転送はクラスタ全体に分散されます）
- ネットワーク アクセスの認証および許可。アカウンティングは非集中型です。
- フィルタリング サービス

個々のユニットに適用される機能

これらの機能は、クラスタ全体またはマスター ユニットではなく、各 ASA ユニットに適用されます。

- QoS：QoS ポリシーは、コンフィギュレーション複製の一部としてクラスタ全体で同期されます。ただし、ポリシーは、各ユニットに対して個別に適用されます。たとえば、出力に対してポリシングを設定する場合は、適合レートおよび適合バースト値は、特定の ASA から出て行くトラフィックに適用されます。3 ユニットから成るクラスタがあり、トラ

フィックが均等に分散している場合は、適合レートは実際にクラスタのレートの 3 倍になります。

- 脅威検出：脅威検出は、各ユニットに対して個別に機能します。たとえば、上位統計情報は、ユニット別です。たとえば、ポート スキャン検出が機能しないのは、スキャン トラフィックが全ユニット間で分散されるので、1 つのユニットがすべてのトラフィックを読み取ることはないからです。
- リソース管理：マルチ コンテキスト モードでのリソース管理は、ローカル使用状況に基づいて各ユニットに個別に適用されます。

ネットワーク アクセス用の AAA とクラスタリング

ネットワーク アクセス用の AAA は、認証、許可、アカウンティングの 3 つのコンポーネントで構成されます。認証および許可は、クラスタリング マスター上で中央集中型機能として実装されており、データ構造がクラスタ スレーブに複製されます。マスターが選定されたときは、確立済みの認証済みユーザおよびユーザに関連付けられた許可を引き続き中断なく運用するのに必要なすべての情報を、新しいマスターが保有します。ユーザ認証のアイドルおよび絶対タイムアウトは、マスター ユニット変更が発生したときも維持されます。

アカウンティングは、クラスタ内の分散型機能として実装されています。アカウンティングはフロー単位で実行されるので、フローを所有するクラスタ ユニットがアカウンティング開始と停止のメッセージを AAA サーバに送信します（フローに対するアカウンティングが設定されているとき）。

FTP とクラスタリング

- FTP データ チャネルとコントロール チャネルのフローがそれぞれ別のクラスタ メンバよって所有されている場合は、データ チャネルのオーナーは定期的にアイドル タイムアウト アップデートをコントロール チャネルのオーナーに送信し、アイドル タイムアウト値を更新します。ただし、コントロール フローのオーナーがリロードされて、コントロール フローが再ホスティングされた場合は、親子フロー関係は維持されなくなります。したがって、コントロール フローのアイドル タイムアウトは更新されません。
- FTP アクセスに AAA を使用している場合、制御チャネルのフローはマスター ユニットに集中化されます。

アイデンティティ ファイアウォールとクラスタリング

マスター ユニットのみが AD から user-group を取得し、AD エージェントから user-ip マッピングを取得します。マスターユニットからユーザ情報がスレーブに渡されるので、スレーブは、セキュリティ ポリシーに基づいてユーザ ID の一致の決定を行うことができます。

マルチキャスト ルーティングとクラスタリング

ファーストパス転送が確立されるまでの間、マスターユニットがすべてのマルチキャストルーティング パケットとデータ パケットを処理します。接続が確立された後は、各スレーブがマルチキャスト データ パケットを転送できます。

NAT とクラスタリング

NAT は、クラスタの全体的なスループットに影響を与えることがあります。着信および発信の NAT パケットが、クラスタ内のそれぞれ別の ASA に送信されることがあります。これは、ロードバランシング アルゴリズムは IP アドレスとポートに依存していますが、NAT が使用される場合、着信と発信でパケットの IP アドレスやポートが異なるためです。NAT オーナーではない ASA に到着したパケットは、クラスタ制御リンクを介してオーナーに転送されるので、大量のトラフィックがクラスタ制御リンク上で発生します。NAT オーナーはセキュリティおよびポリシーチェックの結果に応じてパケットの接続を作成するため、受信側ユニットは転送フローをオーナーに作成しません。

それでもクラスタリングで NAT を使用する場合は、次のガイドラインを考慮してください。

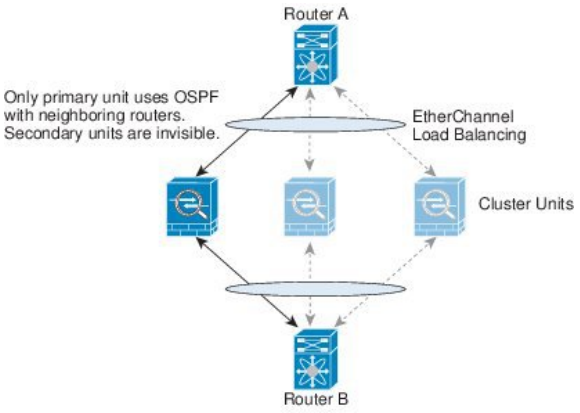
- ダイナミック PAT 用 NAT プール アドレス分散：マスター ユニットは、アドレスをクラスタ全体に均等に分配します。メンバーが接続を受信したときに、そのメンバーのアドレスが 1 つも残っていない場合は、接続はドロップされます（他のメンバーにはまだ使用可能なアドレスがある場合でも）。最低でも、クラスタ内のユニットと同数の NAT アドレスが含まれていることを確認してください。各ユニットが確実に 1 つのアドレスを受け取るようにするためです。アドレス割り当てを表示するには、**show nat pool cluster** コマンドを使用します。
- ラウンドロビンなし：PAT プールのラウンドロビンは、クラスタリングではサポートされません。
- マスター ユニットによって管理されるダイナミック NAT xlate：マスター ユニットが xlate テーブルを維持し、スレーブ ユニットに複製します。ダイナミック NAT を必要とする接続をスレーブ ユニットが受信したときに、その xlate がテーブル内にない場合は、スレーブはマスター ユニットに xlate を要求します。スレーブ ユニットが接続を所有します。
- Per-session PAT 機能：クラスタリングに限りませんが、Per-session PAT 機能によって PAT のスケーラビリティが向上します。クラスタリングの場合は、各スレーブユニットが独自の PAT 接続を持てるようになります。対照的に、Multi-Session PAT 接続はマスターユニットに転送する必要があり、マスターユニットがオーナーとなります。デフォルトでは、すべての TCP トラフィックおよび UDP DNS トラフィックは per-session PAT xlate を使用します。これに対し、ICMP および他のすべての UDP トラフィックは multi-session を使用します。TCP および UDP に対しこれらのデフォルトを変更するように per-session NAT ルールを設定できますが、ICMP に per-session PAT を設定することはできません。H.323、SIP、または Skinny などの multi-session PAT のメリットを活用できるトラフィックでは、関連付けられている TCP ポートに対し per-session PAT を無効にできます（それらの H.323 および SIP の UDP ポートはデフォルトですでに multi-session になっています）。per-session PAT の詳細については、『ファイアウォールの構成ガイド』を参照してください。

- 次のインスペクション用のスタティック PAT はありません。
  - FTP
  - PPTP
  - RSH
  - SQLNET
  - TFTP
  - XDMCP
  - SIP

ダイナミック ルーティングおよびクラスタリング

ルーティング プロセスはマスター ユニット上だけで実行されます。ルートはマスター ユニットを介して学習され、セカンダリに複製されます。ルーティング パケットがスレーブに到着した場合は、マスター ユニットにリダイレクトされます。

図 *48 :* ダイナミック ルーティング



スレーブ メンバがマスター ユニットからルートを学習した後は、各ユニットが個別に転送に関する判断を行います。

OSPF LSA データベースは、マスター ユニットからスレーブ ユニットに同期されません。マスターユニットのスイッチオーバーが発生した場合は、隣接ルータが再起動を検出します。スイッチオーバーは透過的ではありません。OSPF プロセスが IP アドレスの 1 つをルータ ID として選択します必須ではありませんが、スタティック ルータ ID を割り当てることができます。これで、同じルータ ID がクラスタ全体で使用されるようになります。割り込みを解決するには、OSPF ノンストップ フォワーディング機能を参照してください。

SIP インスペクションとクラスタリング

制御フローは、任意のユニットで作成できます（ロードバランシングのため）。その子データフローは同じユニットに存在する必要があります。

TLS プロキシ設定はサポートされていません。

SNMP とクラスタリング

SNMP エージェントは、個々の ASA を、そのローカル IP アドレスによってポーリングします。クラスタの統合データをポーリングすることはできません。

SNMP ポーリングには、メイン クラスタ IP アドレスではなく、常にローカル アドレスを使用してください。SNMP エージェントがメイン クラスタ IP アドレスをポーリングする場合は、新しいマスターが選定されたときに、新しいマスター ユニットのポーリングに失敗します。

syslog および NetFlow とクラスタリング

- Syslog：クラスタの各ユニットは自身の syslog メッセージを生成します。各ユニットの syslog メッセージ ヘッダー フィールドで使用されるデバイス ID を同一にするか、別にするかを設定できます。たとえば、ホスト名コンフィギュレーションはクラスタ内のすべてのユニットに複製されて共有されます。ホスト名をデバイス ID として使用するようにロギングを設定した場合は、どのユニットで生成された syslog メッセージも 1 つのユニットからのように見えます。クラスタ ブートストラップ コンフィギュレーションで割り当てられたローカル ユニット名をデバイス ID として使用するようにロギングを設定した場合は、syslog メッセージはそれぞれ別のユニットからのように見えます。
- NetFlow：クラスタの各ユニットは自身の NetFlow ストリームを生成します。NetFlow コレクタは、各 ASA を独立した NetFlow エクスポータとしてのみ扱うことができます。

Cisco TrustSec とクラスタリング

マスター ユニットだけがセキュリティ グループ タグ（SGT）情報を学習します。マスター ユニットからこの SGT がスレーブに渡されるので、スレーブは、セキュリティ ポリシーに基づいて SGT の一致決定を下せます。

Firepower9300シャーシでのクラスタリングの要件と前提条件

モデルあたりの最大クラスタリング ユニット

- Firepower 9300：16 モジュール。たとえば、16 のシャーシで 1 つのモジュールを使用したり、8 つのシャーシで 2 つのモジュールを使用して、最大 16 のモジュールを組み合わせることができます。

スイッチ要件

- Firepower 9300 シャーシのクラスタリングを設定する前に、スイッチの設定を完了し、シャーシからスイッチまですべての EtherChannel を良好に接続してください。
- サポートされているスイッチのリストについては、「Cisco FXOS Compatibility」を参照してください。

上のクラスタリングのライセンス Firepower 9300 シャーシ

マスター ユニットでのみライセンスを要求できます。ライセンスはスレーブ ユニットでは集約されます。複数のユニットにライセンスがある場合は、これらが統合されて単一の実行ASA クラスタ ライセンスとなります。マスター ユニットで完了したライセンス設定はスレーブ ユニットに複製されません。クラスタリングを無効にし、ライセンスを設定し、クラスタリングを再度有効にした場合限り、スレーブユニットに個別のライセンス権限付与を設定できます。

（注） ASDM や他の高度暗号機能を使用するには、クラスタ展開後にマスター ユニットで ASA CLI を使用して高度暗号化（3DES）ライセンスを有効にする必要があります。このライセンスは、スレーブ ユニットによって継承されます。このライセンスは、各ユニットで個別に設定する必要はありません。高度暗号化（3DES）ライセンスの評価ライセンスは一切ありません。

（注） マスター ユニットに障害が発生し、30 日（ライセンス猶予期間）以内に再参加しない場合、継承されたライセンスは消滅します。その場合、新しいマスターユニットに消滅したライセンスを手動で設定する必要があります。

クラスタリング ガイドラインと制限事項

- 大々的なトポロジ変更が発生する場合（EtherChannelインターフェイスの追加または削除、Firepower 9300 シャーシ 上でのインターフェイスまたはスイッチの有効化または無効化、VSS または vPC を形成するための追加スイッチの追加など）、ヘルス チェック機能や無効なインターフェイスのインターフェイスモニタリングを無効にする必要があります。トポロジの変更が完了して、コンフィギュレーション変更がすべてのユニットに同期されたら、ヘルス チェック機能を再度イネーブルにできます。
- ユニットを既存のクラスタに追加したときや、ユニットをリロードしたときは、一時的に、限定的なパケット/接続ドロップが発生します。これは予定どおりの動作です。場合によっては、ドロップされたパケットが原因で接続がハングすることがあります。たとえば、FTP 接続の FIN/ACK パケットがドロップされると、FTP クライアントがハングします。この場合は、FTP 接続を再確立する必要があります。
- スパンド EtherChannel インターフェイスに接続された Windows 2003 Server を使用している場合、syslog サーバポートがダウンしたときにサーバが ICMP エラーメッセージを抑制しないと、多数の ICMP メッセージがクラスタに送信されることになります。このようなメッセージにより、クラスタの一部のユニットで CPU 使用率が高くなり、パフォーマンスに影響する可能性があります。ICMP エラー メッセージを調節することを推奨します。
- 冗長性を持たせるため、VSS または vPC に EtherChannel を接続することを推奨します。
- シャーシ内では、スタンドアロン モードで一部のシャーシ セキュリティ モジュールをクラスタ化し、他のセキュリティ モジュールを実行することはできません。クラスタ内にすべてのセキュリティ モジュールを含める必要があります。

デフォルト

- クラスタのヘルス チェック機能は、デフォルトでイネーブルになり、ホールド時間は3秒です。デフォルトでは、すべてのインターフェイスでインターネット ヘルス モニタリングがイネーブルになっています。
- 接続再分散は、デフォルトでは無効になっています。接続再分散を有効にした場合の、デフォルトの負荷情報交換間隔は 5 秒です。

クラスタリングの設定 Firepower 9300 シャーシ

クラスタは、Firepower 9300 シャーシ スーパバイザから簡単に展開できます。すべての初期設定が各ユニットに自動的に生成されます。このセクションでは、デフォルトのブートストラップ設定と ASA で実行できるオプションのカスタマイズについて説明します。また、ASA 内からクラスタ メンバーを管理する方法についても説明します。クラスタ メンバーシップは Firepower 9300 シャーシ からも管理できます。詳細については、Firepower 9300 シャーシ のマニュアルを参照してください。

手順

ステップ 1 FXOS：ASA クラスタの追加 （428 ページ）
ステップ 2 ASA：ファイアウォール モードとコンテキスト モードの変更 （435 ページ）
ステップ 3 ASA：データ インターフェイスの設定 （436 ページ）
ステップ 4 ASA：クラスタ設定のカスタマイズ （439 ページ）
ステップ 5 ASA：クラスタ メンバの管理 （445 ページ）

FXOS：ASA クラスタの追加

単独の Firepower 9300 シャーシをシャーシ内クラスタとして追加することも、することもできます。

ASA クラスタの作成

クラスタは、Firepower 9300 シャーシ スーパバイザから簡単に展開できます。すべての初期設定が各ユニットに自動的に生成されます。

モジュールがインストールされていない場合でも、Firepower 9300 シャーシの 3 つすべてのモジュール スロットでクラスタリングを有効にする必要があります。3つすべてのモジュールを設定していないと、クラスタは機能しません。

マルチ コンテキスト モードの場合、最初に論理デバイスを展開してから、ASA アプリケーションでマルチ コンテキスト モードを有効にする必要があります。

ASA をトランスペアレント ファイアウォール モードに変更するには、初期導入を完了し、ASA CLI 内でファイアウォール モードを変更します。

クラスタを導入すると、Firepower 9300 シャーシ スーパバイザが次のブートストラップ コンフィギュレーションで各 ASA アプライアンスを設定します。ブートストラップ コンフィギュレーションの一部（**太字**のテキストで示されている部分）は、後から必要に応じて ASA から変更できます。

```
interface Port-channel48
   description Clustering Interface
cluster group <service_type_name>
   key <secret>
   local-unit unit-<chassis#-module#>

   cluster-interface port-channel48 ip 127.2.<chassis#>.<module#> 255.255.255.0
   priority <auto>
   health-check holdtime 3
   health-check data-interface auto-rejoin 3 5 2
   health-check cluster-interface auto-rejoin unlimited 5 1
   enable

ip local pool cluster_ipv4_pool <ip_address>-<ip_address> mask <mask>

interface <management_ifc>
```

```
   management-only individual
   nameif management
   security-level 0
   ip address <ip_address> <mask> cluster-pool cluster_ipv4_pool
   no shutdown

http server enable
http 0.0.0.0 0.0.0.0 management
route management <management_host_ip> <mask> <gateway_ip> 1
```

（注） **local-unit** 名は、クラスタリングを無効化した場合にのみ変更できます。

始める前に

- 論理デバイスに使用するアプリケーションイメージを Cisco.com からダウンロードして、そのイメージを Firepower 9300 シャーシ にアップロードします。
- 次の情報を用意します。
  - 管理インターフェイス ID、IP アドレス、およびネットワーク マスク
  - ゲートウェイ IP アドレス

手順

ステップ 1 インターフェイスを設定します。

a) クラスタを展開する前に、1 つ以上のデータ タイプのインターフェイスまたは EtherChannel（ポートチャネルとも呼ばれる）を追加します。

デフォルトでは、すべてのインターフェイスがクラスタに割り当てられます。導入後にもクラスタにデータ インターフェイスを追加できます。

b) 管理タイプのインターフェイスまたは EtherChannel を追加します。

管理インターフェイスが必要です。この管理インターフェイスは、シャーシの管理のみに使用されるシャーシ管理インターフェイスと同じではありません（FXOS では、シャーシ管理インターフェイスは MGMT、management0 のような名前で表示されます）。

ステップ 2 セキュリティ サービス モードを開始します。

scope ssa

例：

```
Firepower# scope ssa
Firepower /ssa #
```

ステップ 3 デフォルトのイメージバージョンを設定します。

a) 使用可能なイメージを表示します。使用するバージョン番号をメモします。

show app

例：

```
Firepower /ssa # show app
    Name       Version         Author     Supported Deploy Types CSP Type    Is
Default App
    ---------- --------------- ---------- ---------------------- -----------
--------------
    asa        9.9.1           cisco      Native                 Application No
    asa        9.10.1          cisco      Native                 Application Yes
    ftd        6.2.3           cisco      Native                 Application Yes
```

b) 範囲をイメージバージョンに設定します。

scope app asa *application_version*

例：

```
Firepower /ssa # scope asa ftd 9.10.1
Firepower /ssa/app #
```

c) このバージョンをデフォルトとして設定します。

set-default

例：

```
Firepower /ssa/app # set-default
Firepower /ssa/app* #
```

d) 終了して ssa モードを開始します。

exit

例：

```
Firepower /ssa/app* # exit
Firepower /ssa* #
```

例：

```
Firepower /ssa # scope app asa 9.12.1
Firepower /ssa/app # set-default
Firepower /ssa/app* # exit
Firepower /ssa* #
```

ステップ 4 クラスタを作成します。

enter logical-device *device_name* **asa** *slots* **clustered**

- *device_name*：Firepower 9300 シャーシスーパバイザがクラスタリングを設定してインターフェイスを割り当てるために使用します。この名前は、セキュリティモジュール設定で使

用されるクラスタ名ではありません。まだハードウェアをインストールしていなくても、3 つのセキュリティ モジュールすべてを指定する必要があります。

- スロット: シャーシ モジュールをクラスタに割り当てます。Firepower 4100 の場合は、**1** を指定します。Firepower 9300 の場合は、**1、2、3** を指定します。モジュールがインストールされていない場合でも、Firepower 9300 シャーシの 3 つすべてのモジュール スロットでクラスタリングを有効にする必要があります。3 つすべてのモジュールを設定していないと、クラスタは機能しません。

例：

```
Firepower /ssa # enter logical-device ASA1 asa 1,2,3 clustered
Firepower /ssa/logical-device* #
```

ステップ 5 クラスタ ブートストラップ パラメータを設定します。

これらの設定は、初期導入専用、またはディザスタ リカバリ用です。通常の運用では、後でアプリケーション CCLI 設定のほとんどの値を変更できます。

a) クラスタ ブートストラップ オブジェクトを作成します。

enter cluster-bootstrap

例：

```
Firepower /ssa/logical-device* # enter cluster-bootstrap
Firepower /ssa/logical-device/cluster-bootstrap* #
```

b) クラスタ制御リンクの制御トラフィックの認証キーを設定します。

set key

例：

```
Firepower /ssa/logical-device/cluster-bootstrap* # set key
Key: diamonddogs
```

共有秘密を入力するように求められます。

共有秘密は、1 ～ 63 文字の ASCII 文字列です。共有秘密は、キーを生成するために使用されます。このオプションは、データパストラフィック（接続状態アップデートや転送されるパケットなど）には影響しません。データパス トラフィックは、常にクリア テキストとして送信されます。

c) クラスタ インターフェイス モードを設定します。

set mode spanned-etherchannel

スパンド EtherChannel モードは、サポートされている唯一のモードです。

例：

```
Firepower /ssa/logical-device/cluster-bootstrap* # set mode spanned-etherchannel
```

```
Firepower /ssa/logical-device/cluster-bootstrap* #
```

d) セキュリティ モジュール設定のクラスタ グループ名を設定します。

set service-type *cluster_name*

名前は 1 ～ 38 文字の ASCII 文字列であることが必要です。

例：

```
Firepower /ssa/logical-device/cluster-bootstrap* # set service-type cluster1
Firepower /ssa/logical-device/cluster-bootstrap* #
```

e) 管理 IP アドレス情報を設定します。

この情報は、セキュリティ モジュール設定で管理インターフェイスを設定するために使用されます。

1. ローカル IP アドレスのプールを設定します。このアドレスの 1 つが、このインターフェイス用に各クラスタユニットに割り当てられます。

   set ipv4 pool *start_ip end_ip*

   set ipv6 pool *start_ip end_ip*

   最低でも、クラスタ内のユニット数と同じ数のアドレスが含まれるようにしてください。Firepower 9300 の場合、すべてのモジュール スロットが埋まっていないとしても、シャーシごとに 3 つのアドレスを含める必要があることに注意してください。クラスタを拡張する予定の場合は、アドレスを増やします。現在のマスターユニットに属する仮想 IP アドレス（メイン クラスタ IP アドレスと呼ばれる）は、このプールの一部ではありません。必ず、同じネットワークの IP アドレスの 1 つをメイン クラスタ IP アドレス用に確保してください。IPv4 アドレスと IPv6 アドレス（どちらか一方も可）を使用できます。

2. 管理インターフェイスのメインクラスタ IP アドレスを設定します。

   set virtual ipv4 *ip_address* **mask** *mask*

   set virtual ipv6 *ip_address* **prefix-length** *prefix*

   この IP アドレスは、クラスタ プール アドレスと同じネットワーク上に存在している必要がありますが、プールに含まれていてはなりません。

3. ネットワーク ゲートウェイ アドレスを入力します。

   set ipv4 gateway *ip_address*

   set ipv6 gateway *ip_address*

例：

```
Firepower /ssa/logical-device/cluster-bootstrap* # set ipv4 gateway 10.1.1.254
Firepower /ssa/logical-device/cluster-bootstrap* # set ipv4 pool 10.1.1.11 10.1.1.27
Firepower /ssa/logical-device/cluster-bootstrap* # set ipv6 gateway 2001:DB8::AA
Firepower /ssa/logical-device/cluster-bootstrap* # set ipv6 pool 2001:DB8::11
2001:DB8::27
```

```
Firepower /ssa/logical-device/cluster-bootstrap* # set virtual ipv4 10.1.1.1 mask
255.255.255.0
Firepower /ssa/logical-device/cluster-bootstrap* # set virtual ipv6 2001:DB8::1
prefix-length 64
```

f) クラスタ ブートストラップ モードを終了します。

exit

例：

```
Firepower /ssa/logical-device* # enter cluster-bootstrap
Firepower /ssa/logical-device/cluster-bootstrap* # set chassis-id 1
Firepower /ssa/logical-device/cluster-bootstrap* # set key
  Key: f@arscape
Firepower /ssa/logical-device/cluster-bootstrap* # set mode spanned-etherchannel
Firepower /ssa/logical-device/cluster-bootstrap* # set service-type cluster1
Firepower /ssa/logical-device/cluster-bootstrap* # exit
Firepower /ssa/logical-device/* #
```

ステップ 6 管理ブートストラップパラメータを設定します。

これらの設定は、初期導入専用、またはディザスタ リカバリ用です。通常の運用では、後でアプリケーション CCLI 設定のほとんどの値を変更できます。

a) 管理ブートストラップ オブジェクトを作成します。

enter mgmt-bootstrap asa

例：

```
Firepower /ssa/logical-device* # enter mgmt-bootstrap asa
Firepower /ssa/logical-device/mgmt-bootstrap* #
```

b) admin とを指定します。

create bootstrap-key-secret PASSWORD

set value

値の入力：*password*

値の確認：*password*

exit

例：

事前設定されているASA管理者ユーザはパスワードの回復時に役立ちます。FXOSアクセスができる場合、管理者ユーザ パスワードを忘れたときにリセットできます。

例：

```
Firepower /ssa/logical-device/mgmt-bootstrap* # create bootstrap-key-secret PASSWORD
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key-secret* # set value
Enter a value: floppylampshade
Confirm the value: floppylampshade
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key-secret* # exit
```

```
Firepower /ssa/logical-device/mgmt-bootstrap* #
```

c) 管理ブートストラップ モードを終了します。

exit

例：

```
Firepower /ssa/logical-device/mgmt-bootstrap* # exit
Firepower /ssa/logical-device* #
```

ステップ 7 設定を保存します。

commit-buffer

シャーシは、指定したソフトウェアバージョンをダウンロードし、アプリケーションインスタンスにブートストラップ設定と管理インターフェイス設定をプッシュすることで、論理デバイスを導入します。**show app-instance** コマンドを使用して、導入のステータスを確認します。[Admin State] が [Enabled] で、[Oper State] が [Online] の場合、アプリケーション インスタンスは実行中であり、使用できる状態になっています。

例：

```
Firepower /ssa/logical-device* # commit-buffer
Firepower /ssa/logical-device # exit
Firepower /ssa # show app-instance
App Name   Identifier Slot ID    Admin State Oper State       Running Version Startup
Version Deploy Type Profile Name Cluster State   Cluster Role
---------- ---------- ---------- ----------- ---------------- ---------------
--------------- ----------- ------------ --------------- ------------
ftd        cluster1   1          Enabled     Online           6.4.0.49        6.4.0.49
       Native                   In Cluster      Slave
ftd        cluster1   2          Enabled     Online           6.4.0.49        6.4.0.49
       Native                   In Cluster      Master
ftd        cluster1   3          Disabled    Not Available                    6.4.0.49
       Native                   Not Applicable  None
```

ステップ 8 マスター ユニット ASA に接続して、クラスタリング設定をカスタマイズします。

例

シャーシ 1：

```
scope eth-uplink
  scope fabric a
    enter port-channel 1
      set port-type data
      enable
      enter member-port Ethernet1/1
        exit
      enter member-port Ethernet1/2
        exit
      exit
```

```
    enter port-channel 2
      set port-type data
      enable
      enter member-port Ethernet1/3
        exit
      enter member-port Ethernet1/4
        exit
      exit
    enter port-channel 3
      set port-type data
      enable
      enter member-port Ethernet1/5
        exit
      enter member-port Ethernet1/6
        exit
      exit
    enter port-channel 4
      set port-type mgmt
      enable
      enter member-port Ethernet2/1
        exit
      enter member-port Ethernet2/2
        exit
      exit

    exit
  exit
commit-buffer

scope ssa
  enter logical-device ASA1 asa "1,2,3" clustered
    enter cluster-bootstrap
      set chassis-id 1
      set ipv4 gateway 10.1.1.254
      set ipv4 pool 10.1.1.11 10.1.1.27
      set ipv6 gateway 2001:DB8::AA
      set ipv6 pool 2001:DB8::11 2001:DB8::27
      set key
      Key: f@arscape
      set mode spanned-etherchannel
      set service-type cluster1
      set virtual ipv4 10.1.1.1 mask 255.255.255.0
      set virtual ipv6 2001:DB8::1 prefix-length 64
      exit
    exit
  scope app asa 9.5.2.1
    set-default
    exit
  commit-buffer
```

ASA：ファイアウォール モードとコンテキスト モードの変更

デフォルトでは、FXOS シャーシはルーテッドまたはトランスペアレント ファイアウォール モード、およびシングル コンテキスト モードでクラスタを展開します。

- ファイアウォール モードの変更：展開後にモードを変更するには、マスター ユニットでモードを変更します。モードは一致するようにすべてのスレーブ ユニットで自動的に変更されます。を参照してください。ファイアウォール モードの設定（184 ページ）マルチ コンテキスト モードでは、コンテキストごとにファイアウォール モードを設定します。

- マルチ コンテキスト モードに変更：展開後にマルチ コンテキスト モードに変更するには、マスター ユニットのモードを変更します。これにより、すべてのスレーブ ユニットのモードは一致するように自動的に変更されます。マルチ コンテキスト モードの有効化（216 ページ）を参照してください。

ASA：データ インターフェイスの設定

この手順では、FXOS にクラスタを展開したときにクラスタに割り当てられた各データ インターフェイスの基本的なパラメータを設定します。シャーシ間クラスタリングの場合、データ インターフェイスは常にスパンド EtherChannel インターフェイスです。

（注） 管理インターフェイスは、クラスタを展開したときに事前設定されました。ASA で管理インターフェイス パラメータを変更することもできますが、この手順はデータ インターフェイスに焦点を当てています。管理インターフェイスは、スパンドインターフェイスとは対照的に、個別のインターフェイスです。詳細については、「管理インターフェイス（418ページ）」を参照してください。

始める前に

- マルチ コンテキスト モードの場合は、この手順をシステム実行スペースで開始します。まだシステム コンフィギュレーション モードに入っていない場合は、**changeto system** コマンドを入力します。
- トランスペアレント モードの場合は、ブリッジ グループを設定します。
- シャーシ間クラスタリングにスパンドEtherChannelを使用している場合、クラスタリングが完全に有効になるまで、ポートチャネルインターフェイスは起動しません。この要件により、クラスタのアクティブではないユニットにトラフィックが転送されるのが防がれます。

手順

ステップ 1 インターフェイス ID を指定します

interface *id*

このクラスタに割り当てられているインターフェイスのFXOSシャーシを参照してください。インターフェイス ID には、次のものがあります。

- **port-channel** *integer*
- **ethernet** *slot/port*

例：

```
ciscoasa(config)# interface port-channel 1
```

ステップ 2 インターフェイスをイネーブルにします。

no shutdown

ステップ 3 （オプション）このインターフェイス上に VLAN サブインターフェイスを作成する予定の場合は、この時点で作成します。

例：

```
ciscoasa(config)# interface port-channel 1.10
ciscoasa(config-if)# vlan 10
```

この手順の残りの部分は、サブインターフェイスに適用されます。

ステップ 4 （マルチ コンテキスト モード）インターフェイスをコンテキストに割り当ててから、コンテキストに変更し、インターフェイス モードを開始します。

例：

```
ciscoasa(config)# context admin
ciscoasa(config)# allocate-interface port-channel1
ciscoasa(config)# changeto context admin
ciscoasa(config-if)# interface port-channel 1
```

マルチ コンテキスト モードの場合は、インターフェイス コンフィギュレーションの残りの部分は各コンテキスト内で行われます。

ステップ 5 インターフェイスの名前を指定します。

nameif *name*

例：

```
ciscoasa(config-if)# nameif inside
```

name は最大 48 文字のテキスト文字列です。大文字と小文字は区別されません。名前を変更するには、このコマンドで新しい値を再入力します。

ステップ 6 ファイアウォール モードに応じて、次のいずれかを実行します。

- ルーテッド モード：IPv4 アドレスと IPv6 アドレスの一方または両方を設定します。

  （IPv4）

  ip address *ip_address* [*mask*]

  （IPv6）

  ipv6 address *ipv6-prefix*/*prefix-length*

  例：

```
ciscoasa(config-if)# ip address 10.1.1.1 255.255.255.0
ciscoasa(config-if)# ipv6 address 2001:DB8::1001/32
```

DHCP、PPPoE、および IPv6 自動設定はサポートされません。

- トランスペアレント モード：インターフェイスをブリッジ グループに割り当てます。

  bridge-group *number*

  例：

  ```
  ciscoasa(config-if)# bridge-group 1
  ```

  number は、1 ～ 100 の整数です。ブリッジ グループには最大 4 個のインターフェイスを割り当てることができます。同一インターフェイスを複数のブリッジ グループに割り当てることはできません。BVI のコンフィギュレーションには IP アドレスが含まれていることに注意してください。

ステップ 7 セキュリティ レベルを設定します。

security-level *number*

例：

```
ciscoasa(config-if)# security-level 50
```

number には、0（最下位）～ 100（最上位）の整数を指定します。

ステップ 8 （シャーシ間クラスタリング）潜在的なネットワークの接続問題を回避するために、スパンド EtherChannel のグローバル MAC アドレスを設定します。

mac-address *mac_address*

- *mac_address*：MAC アドレスは、H.H.H 形式で指定します。H は 16 ビットの 16 進数です。たとえば、MAC アドレス 00-0C-F1-42-4C-DE は、000C.F142.4CDE と入力します。自動生成された MAC アドレスも使用する場合、手動で割り当てる MAC アドレスの最初の 2 バイトには A2 を使用できません。

MAC アドレスが手動設定されている場合、その MAC アドレスは現在のマスター ユニットに留まります。MAC アドレスを設定していない場合に、マスター ユニットが変更された場合、新しいマスターユニットはインターフェイスに新しい MAC アドレスを使用します。これにより、一時的なネットワークの停止が発生する可能性があります。

マルチコンテキストモードでは、コンテキスト間でインターフェイスを共有する場合は、MAC アドレスの自動生成を有効にして、手動で MAC アドレスを設定しなくてすむようにします。非共有インターフェイスの場合は、このコマンドを使用して MAC アドレスを手動で設定する必要があることに注意してください。

例：

```
ciscoasa(config-if)# mac-address 000C.F142.4CDE
```

ASA：クラスタ設定のカスタマイズ

クラスタを展開した後にブートストラップ設定を変更する場合や、クラスタリング ヘルス モニタリング、TCP 接続複製の遅延、フロー モビリティ、およびその他の最適化など、追加のオプションを設定する場合は、マスター ユニットで行うことができます。

ASA クラスタの基本パラメータの設定

マスター ユニット上のクラスタ設定をカスタマイズできます。

始める前に

- マルチ コンテキスト モードでは、マスター ユニット上のシステム実行スペースで次の手順を実行します。コンテキストからシステム実行スペースに切り替えるには、**changeto system** コマンドを入力します。
- local-unit name およびその他の複数のオプションは、FXOS シャーシでのみ設定することができます。また、それらのオプションは、クラスタリングを無効にしている場合にASAでのみ変更できます。そのため、次の手順には含まれていません。

手順

ステップ 1 このユニットがマスター ユニットであることを確認します。

show cluster info

例：

```
asa(config)# show cluster info
Cluster cluster1: On
    Interface mode: spanned
    This is "unit-1-2" in state MASTER
        ID        : 2
        Version   : 9.5(2)
        Serial No.: FCH183770GD
        CCL IP    : 127.2.1.2
        CCL MAC   : 0015.c500.019f
        Last join : 01:18:34 UTC Nov 4 2015
        Last leave: N/A
Other members in the cluster:
    Unit "unit-1-3" in state SLAVE
        ID        : 4
        Version   : 9.5(2)
        Serial No.: FCH19057ML0
        CCL IP    : 127.2.1.3
        CCL MAC   : 0015.c500.018f
```

```
        Last join : 20:29:57 UTC Nov 4 2015
        Last leave: 20:24:55 UTC Nov 4 2015
Unit "unit-1-1" in state SLAVE
        ID        : 1
        Version   : 9.5(2)
        Serial No.: FCH19057ML0
        CCL IP    : 127.2.1.1
        CCL MAC   : 0015.c500.017f
        Last join : 20:20:53 UTC Nov 4 2015
        Last leave: 20:18:15 UTC Nov 4 2015
```

別のユニットがマスター ユニットの場合は、接続を終了し、正しいユニットに接続します。ASA コンソールへのアクセス方法の詳細については、Cisco ASA for Firepower 4100 クイック スタート ガイド [英語] または Cisco ASA for Firepower 9300 クイック スタート ガイド [英語] を参照してください。

ステップ 2 クラスタ制御リンク インターフェイスの最大伝送ユニットを指定します。

mtu cluster *bytes*

例：

```
ciscoasa(config)# mtu cluster 9000
```

MTU の最大値を 9000 バイトに設定し、最小値を 1400 バイトに設定することをお勧めします。

ステップ 3 クラスタの設定モードを開始します。

cluster group *name*

ステップ 4 （任意） スレーブ ユニットからマスター ユニットへのコンソール複製をイネーブルにします。

console-replicate

この機能はデフォルトで無効に設定されています。ASA は、特定の重大イベントが発生したときに、メッセージを直接コンソールに出力します。コンソール複製をイネーブルにすると、スレーブ ユニットからマスター ユニットにコンソール メッセージが送信されるので、モニタが必要になるのはクラスタのコンソール ポート 1 つだけとなります。

ステップ 5 （任意） LACP のダイナミック ポートの優先順位を無効にします。

clacp static-port-priority

一部のスイッチはダイナミック ポート プライオリティをサポートしていないため、このコマンドはスイッチの互換性を高めます。さらに、このコマンドは、9 ～ 32 のアクティブ スパンド EtherChannel メンバーのサポートをイネーブルにします。このコマンドを使用しないと、サポートされるのは 8 個のアクティブ メンバと 8 個のスタンバイ メンバのみです。このコマンドをイネーブルにした場合、スタンバイ メンバは使用できません。すべてのメンバがアクティブです。

のヘルス モニタリングの設定

この手順では、ユニットとインターフェイスのヘルス モニタリングを設定します。

たとえば、管理インターフェイスなど、必須以外のインターフェイスのヘルスモニタリングをディセーブルにすることができます。ポートチャネル ID、または単一の物理インターフェイス ID をモニタできます。ヘルス モニタリングは VLAN サブインターフェイス、または VNI やBVI などの仮想インターフェイスでは実行されません。クラスタ制御リンクのモニタリングは設定できません。このリンクは常にモニタされています。

手順

ステップ 1 クラスタの設定モードを開始します。

cluster group *name*

ステップ 2 クラスタ ユニットのヘルス チェック機能を次のようにカスタマイズします。

health-check [**holdtime** *timeout*]

holdime は、ユニットのキープアライブ ステータス メッセージの間隔を指定します。指定できる範囲は .8 ～ 45 秒で、デフォルトは 3 秒です。

ユニットのヘルスを確認するため、ASA のクラスタ ユニットはクラスタ制御リンクで他のユニットにキープアライブ メッセージを送信します。ユニットが保留時間内にピア ユニットからキープアライブ メッセージを受信しない場合は、そのピア ユニットは応答不能またはデッド状態と見なされます。

何らかのトポロジ変更（たとえばデータ インターフェイスの追加/削除、ASA、Firepower 9300 シャーシ、またはスイッチ上のインターフェイスの有効化/無効化、VSS または vPC を形成するスイッチの追加）を行うときには、ヘルス チェック機能を無効にし、無効化したインターフェイスのモニタリングも無効にしてください（**no health-check monitor-interface**）。トポロジの変更が完了して、コンフィギュレーション変更がすべてのユニットに同期されたら、ヘルス チェック機能を再度イネーブルにできます。

例：

```
ciscoasa(cfg-cluster)# health-check holdtime 5
```

ステップ 3 インターフェイスでインターフェイス ヘルス チェックを次のように無効化します。

no health-check monitor-interface [*interface_id*]

インターフェイスのヘルスチェックはリンク障害をモニタします。特定の論理インターフェイスのすべての物理ポートが、特定のユニット上では障害が発生したが、別のユニット上の同じ論理インターフェイスでアクティブ ポートがある場合、そのユニットはクラスタから削除されます。ASA がメンバをクラスタから削除するまでの時間は、インターフェイスのタイプと、そのユニットが確立済みメンバであるか、またはクラスタに参加しようとしているかによって異なります。

デフォルトでは、ヘルスチェックはすべてのインターフェイスでイネーブルになっています。このコマンドの **no** 形式を使用してディセーブルにすることができます。たとえば、管理インターフェイスなど、必須以外のインターフェイスのヘルスモニタリングをディセーブルにすることができます。ヘルス モニタリングは VLAN サブインターフェイス、または VNI や BVI などの仮想インターフェイスでは実行されません。クラスタ制御リンクのモニタリングは設定できません。このリンクは常にモニタされています。

何らかのトポロジ変更（たとえばデータ インターフェイスの追加/削除、ASA、Firepower 9300 シャーシ、またはスイッチ上のインターフェイスの有効化/無効化、VSS または vPC を形成するスイッチの追加）を行うときには、ヘルスチェック機能（**no health-check**）を無効にし、無効化したインターフェイスのモニタリングも無効にしてください。トポロジの変更が完了して、コンフィギュレーション変更がすべてのユニットに同期されたら、ヘルスチェック機能を再度イネーブルにできます。

例：

```
ciscoasa(cfg-cluster)# no health-check monitor-interface port-channel1
```

ステップ 4 シャーシのヘルス チェック間隔を設定します。

app-agent heartbeat [**interval** *ms*] [**retry-count** *number*]

- **interval** *ms*：ハートビートの時間間隔を 300 ～ 6000 ms の範囲の 100 の倍数単位で設定します。デフォルトは 1000 ms です。
- **retry-count** *number*：再試行の回数を 1 ～ 30 の範囲の値に設定します。デフォルトの試行回数は 3 回です。

ASA はホストの Firepower シャーシとのバックプレーンを介して通信できるかどうかをチェックします。

例：

```
ciscoasa(cfg-cluster)# app-agent heartbeat interval 300
```

接続の再分散

接続の再分散を設定できます。

手順

ステップ 1 クラスタの設定モードを開始します。

cluster group *name*

ステップ 2 （オプション）TCP トラフィックの接続の再分散を有効化します。

conn-rebalance [**frequency** *seconds*]

例：

```
ciscoasa(cfg-cluster)# conn-rebalance frequency 60
```

このコマンドは、デフォルトでディセーブルになっています。有効化されている場合は、ASA は負荷情報を定期的に交換し、新しい接続の負荷を高負荷のデバイスから低負荷のデバイスに移動します。負荷情報を交換する間隔を、1 ～ 360 秒の範囲内で指定します。デフォルトは 5 秒です。

FXOS：クラスタ メンバの削除

ここでは、メンバを一時的に、またはクラスタから永続的に削除する方法について説明します。

一時的な削除

たとえば、ハードウェアまたはネットワークの障害が原因で、クラスタ メンバはクラスタから自動的に削除されます。この削除は、条件が修正されるまでの一時的なものであるため、クラスタに再参加できます。また、手動でクラスタリングを無効にすることもできます。

デバイスが現在クラスタ内にあるかどうかを確認するには、**show cluster info** コマンドを使用してアプリケーション内のクラスタ ステータスを確認します。

```
ciscoasa# show cluster info
Clustering is not enabled
```

- アプリケーションでのクラスタリングの無効化：アプリケーションCLIを使用してクラスタリングを無効にすることができます。**cluster remove unit** *name* コマンドを入力して、ログインしているユニット以外のすべてのユニットを削除します。ブートストラップ コンフィギュレーションは変更されず、マスターユニットから最後に同期されたコンフィギュレーションもそのままであるので、コンフィギュレーションを失わずに後でそのユニットを再度追加できます。マスター ユニットを削除するためにスレーブ ユニットでこのコマンドを入力した場合は、新しいマスター ユニットが選定されます。

  デバイスが非アクティブになると、すべてのデータ インターフェイスがシャットダウンされます。管理専用インターフェイスのみがトラフィックを送受信できます。トラフィック フローを再開するには、クラスタリングを再度有効にします。管理インターフェイスは、そのユニットがブートストラップ設定から受け取った IP アドレスを使用して引き続き稼働状態となります。ただし、リロードしてもユニットがクラスタ内でまだアクティブではない場合（クラスタリングが無効な状態で設定を保存した場合など）、管理インターフェイスは無効になります。

  クラスタリングを再度有効にするには、ASA で **cluster group** *name* を入力してから **enable** を入力します。

- アプリケーション インスタンスの無効化：FXOS CLI で、次の例を参照してください。

```
Firepower-chassis# scope ssa
Firepower-chassis /ssa # scope slot 1
Firepower-chassis /ssa/slot # scope app-instance asa asa1
Firepower-chassis /ssa/slot/app-instance # disable
Firepower-chassis /ssa/slot/app-instance* # commit-buffer
Firepower-chassis /ssa/slot/app-instance #
```

再度有効にするには、次の手順を実行します。

```
Firepower-chassis /ssa/slot/app-instance # enable
Firepower-chassis /ssa/slot/app-instance* # commit-buffer
Firepower-chassis /ssa/slot/app-instance #
```

- セキュリティ モジュール/エンジン のシャットダウン：FXOS CLI で、次の例を参照してください。

```
Firepower-chassis# scope service-profile server 1/1
Firepower-chassis /org/service-profile # power down soft-shut-down
Firepower-chassis /org/service-profile* # commit-buffer
Firepower-chassis /org/service-profile #
```

電源を投入するには、次の手順を実行します。

```
Firepower-chassis /org/service-profile # power up
Firepower-chassis /org/service-profile* # commit-buffer
Firepower-chassis /org/service-profile #
```

- シャーシのシャットダウン：FXOS CLI で、次の例を参照してください。

```
Firepower-chassis# scope chassis 1
Firepower-chassis /chassis # shutdown no-prompt
```

完全な削除

次の方法を使用して、クラスタ メンバを完全に削除できます。

- 論理デバイスの削除：FXOS CLI で、次の例を参照してください。

```
Firepower-chassis# scope ssa
Firepower-chassis /ssa # delete logical-device cluster1
Firepower-chassis /ssa* # commit-buffer
Firepower-chassis /ssa #
```

- サービスからのシャーシまたはセキュリティ モジュールの削除：サービスからデバイスを削除する場合は、交換用ハードウェアをクラスタの新しいメンバーとして追加できます。

ASA：クラスタ メンバの管理

クラスタを導入した後は、コンフィギュレーションを変更し、クラスタ メンバを管理できます。

非アクティブなメンバーになる

クラスタの非アクティブなメンバーになるには、クラスタリング コンフィギュレーションは変更せずに、そのユニット上でクラスタリングをディセーブルにします。

（注） ASAが（手動で、またはヘルスチェック エラーにより）非アクティブになると、すべてのデータ インターフェイスがシャットダウンされます。管理専用インターフェイスのみがトラフィックを送受信できます。トラフィック フローを再開させるには、クラスタリングを再びイネーブルにします。または、そのユニットをクラスタから完全に削除します。管理インターフェイスは、そのユニットがクラスタ IP プールから受け取った IP アドレスを使用して引き続き稼働状態となります。ただし、リロードしてもユニットがクラスタ内でまだアクティブではない場合（クラスタリングが無効な状態で設定を保存した場合など）、管理インターフェイスは無効になります。それ以降のコンフィギュレーション作業には、コンソール ポートを使用する必要があります。

始める前に

- コンソール ポートを使用する必要があります。クラスタリングのイネーブルまたはディセーブルを、リモート CLI 接続から行うことはできません。
- マルチ コンテキスト モードの場合は、この手順をシステム実行スペースで実行します。まだシステム コンフィギュレーション モードに入っていない場合は、**changeto system** コマンドを入力します。

手順

ステップ 1 クラスタの設定モードを開始します。

cluster group *name*

例：

```
ciscoasa(config)# cluster group pod1
```

ステップ 2 クラスタリングをディセーブルにします。

no enable

このユニットがマスターユニットであった場合は、新しいマスターの選定が実行され、別のメンバがマスター ユニットになります。

クラスタ コンフィギュレーションは維持されるので、後でクラスタリングを再度イネーブルにできます。

メンバーの非アクティブ化

ログインしているユニット以外のメンバを非アクティブにするには、次のステップを実行します。

（注） ASAが非アクティブになると、すべてのデータインターフェイスがシャットダウンされます。管理専用インターフェイスのみがトラフィックを送受信できます。トラフィック フローを再開するには、クラスタリングを再度有効にします。管理インターフェイスは、そのユニットがクラスタ IP プールから受け取った IP アドレスを使用して引き続き稼働状態となります。ただし、リロードしてもユニットがクラスタ内でまだアクティブではない場合（クラスタリングが無効な状態で設定を保存した場合など）、管理インターフェイスは無効になります。それ以降のコンフィギュレーション作業には、コンソール ポートを使用する必要があります。

始める前に

マルチ コンテキスト モードの場合は、この手順をシステム実行スペースで実行します。まだシステム コンフィギュレーション モードに入っていない場合は、**changeto system** コマンドを入力します。

手順

ユニットをクラスタから削除します。

cluster remove unit *unit_name*

ブートストラップ コンフィギュレーションは変更されず、マスター ユニットから最後に同期されたコンフィギュレーションもそのままになるので、コンフィギュレーションを失わずに後でそのユニットを再度追加できます。マスター ユニットを削除するためにスレーブ ユニットでこのコマンドを入力した場合は、新しいマスター ユニットが選定されます。

メンバ名を一覧表示するには、**cluster remove unit ?** と入力するか、**show cluster info** コマンドを入力します。

例：

```
ciscoasa(config)# cluster remove unit ?

Current active units in the cluster:
asa2
```

```
ciscoasa(config)# cluster remove unit asa2
WARNING: Clustering will be disabled on unit asa2. To bring it back
to the cluster please logon to that unit and re-enable clustering
```

クラスタへの再参加

ユニットがクラスタから削除された場合（たとえば、障害が発生したインターフェイスの場合、またはメンバーを手動で非アクティブにした場合）は、クラスタに手動で再参加する必要があります。

始める前に

- クラスタリングを再イネーブルにするには、コンソール ポートを使用する必要があります。他のインターフェイスはシャットダウンされます。
- マルチ コンテキスト モードの場合は、この手順をシステム実行スペースで実行します。まだシステム コンフィギュレーション モードに入っていない場合は、**changeto system** コマンドを入力します。
- クラスタへの再参加を試行する前に、障害が解決されていることを確認します。

手順

ステップ 1 コンソールで、クラスタ コンフィギュレーション モードを開始します。

cluster group *name*

例：

```
ciscoasa(config)# cluster group pod1
```

ステップ 2 クラスタリングをイネーブルにします。

enable

マスター ユニットの変更

⚠

注意 マスターユニットを変更する最良の方法は、マスターユニットでクラスタリングを無効にし、新しいマスターの選択を待ってから、クラスタリングを再度有効にする方法です。マスターにするユニットを厳密に指定する必要がある場合は、この項の手順を使用します。ただし、中央集中型機能の場合は、この手順を使用してマスターユニット変更を強制するとすべての接続がドロップされるので、新しいマスター ユニット上で接続を再確立する必要があります。

マスター ユニットを変更するには、次の手順を実行します。

始める前に

マルチ コンテキスト モードの場合は、この手順をシステム実行スペースで実行します。まだシステム コンフィギュレーション モードに入っていない場合は、**changeto system** コマンドを入力します。

手順

新しいユニットをマスター ユニットとして設定します。

cluster master unit *unit_name*

例：

```
ciscoasa(config)# cluster master unit asa2
```

メイン クラスタ IP アドレスへの再接続が必要になります。

メンバ名を一覧表示するには、**cluster master unit ?**（現在のユニットを除くすべての名前が表示される）と入力するか、**show cluster info** コマンドを入力します。

クラスタ全体でのコマンドの実行

コマンドをクラスタ内のすべてのメンバに、または特定のメンバに送信するには、次の手順を実行します。**show** コマンドをすべてのメンバーに送信すると、すべての出力が収集されて現在のユニットのコンソールに表示されます。（または、マスター ユニットで show コマンドを入力するとクラスタ全体の統計情報を表示できます。）**capture** や **copy** などのその他のコマンドも、クラスタ全体での実行を活用できます。

手順

コマンドをすべてのメンバに送信します。ユニット名を指定した場合は、特定のメンバに送信されます。

cluster exec [unit *unit_name*] コマンド

例：

```
ciscoasa# cluster exec show xlate
```

メンバー名を表示するには、**cluster exec unit ?** コマンドを入力するか（現在のユニットを除くすべての名前を表示する場合）、**show cluster info** コマンドを入力します。

例

同じキャプチャ ファイルをクラスタ内のすべてのユニットから同時に TFTP サーバにコピーするには、マスター ユニットで次のコマンドを入力します。

```
ciscoasa# cluster exec copy /pcap capture: tftp://10.1.1.56/capture1.pcap
```

複数の PCAP ファイル（各ユニットから 1 つずつ）が TFTP サーバにコピーされます。宛先のキャプチャ ファイル名には自動的にユニット名が付加され、capture1_asa1.pcap、capture1_asa2.pcap などとなります。この例では、asa1 および asa2 がクラスタ ユニット名です。

次の **cluster exec show memory** コマンドの出力例では、クラスタの各メンバーのメモリ情報が表示されています。

```
ciscoasa# cluster exec show memory
unit-1-1(LOCAL):*******************************************************
Free memory:      108724634538 bytes (92%)
Used memory:        9410087158 bytes ( 8%)
-------------     ------------------
Total memory:     118111600640 bytes (100%)


unit-1-3:*******************************************************************
Free memory:      108749922170 bytes (92%)
Used memory:        9371097334 bytes ( 8%)
-------------     ------------------
Total memory:     118111600640 bytes (100%)


unit-1-2:*******************************************************************
Free memory:      108426753537 bytes (92%)
Used memory:        9697869087 bytes ( 8%)
-------------     ------------------
Total memory:     118111600640 bytes (100%)
```

ASA：での ASA クラスタのモニタリング Firepower 9300 シャーシ

クラスタの状態と接続をモニタおよびトラブルシューティングできます。

クラスタ ステータスのモニタリング

クラスタの状態のモニタリングについては、次のコマンドを参照してください。

- **show cluster info [health], show cluster chassis info**

  キーワードを指定しないで **show cluster info** コマンドを実行すると、クラスタ内のすべてのメンバーのステータスが表示されます。

  show cluster info health コマンドは、インターフェイス、ユニットおよびクラスタ全体の現在の状態を表示します。

  show cluster info コマンドの次の出力を参照してください。

```
asa(config)# show cluster info
Cluster cluster1: On
    Interface mode: spanned
    This is "unit-1-2" in state MASTER
        ID        : 2
        Version   : 9.5(2)
        Serial No.: FCH183770GD
        CCL IP    : 127.2.1.2
        CCL MAC   : 0015.c500.019f
        Last join : 01:18:34 UTC Nov 4 2015
        Last leave: N/A
Other members in the cluster:
    Unit "unit-1-3" in state SLAVE
        ID        : 4
        Version   : 9.5(2)
        Serial No.: FCH19057ML0
        CCL IP    : 127.2.1.3
        CCL MAC   : 0015.c500.018f
        Last join : 20:29:57 UTC Nov 4 2015
        Last leave: 20:24:55 UTC Nov 4 2015
    Unit "unit-1-1" in state SLAVE
        ID        : 1
        Version   : 9.5(2)
        Serial No.: FCH19057ML0
        CCL IP    : 127.2.1.1
        CCL MAC   : 0015.c500.017f
        Last join : 20:20:53 UTC Nov 4 2015
        Last leave: 20:18:15 UTC Nov 4 2015
```

- **show cluster info transport{asp |cp}**

  次のトランスポート関連の統計情報を表示します。

- **asp**：データ プレーンのトランスポート統計情報。
- **cp**：コントロール プレーンのトランスポート統計情報。

- **show cluster history**

  クラスタの履歴を表示します。

クラスタ全体のパケットのキャプチャ

クラスタでのパケットのキャプチャについては、次のコマンドを参照してください。

cluster exec capture

クラスタ全体のトラブルシューティングをサポートするには、**cluster exec capture** コマンドを使用してマスターユニット上でのクラスタ固有トラフィックのキャプチャをイネーブルにします。これで、クラスタ内のすべてのスレーブ ユニットでも自動的にイネーブルになります。

クラスタ リソースのモニタリング

クラスタ リソースのモニタリングについては、次のコマンドを参照してください。

show cluster {cpu | memory | resource} [*options*]、**show cluster chassis [cpu | memory | resource usage]**

クラスタ全体の集約データを表示します。使用可能なオプションはデータのタイプによって異なります。

クラスタ トラフィックのモニタリング

クラスタ トラフィックのモニタリングについては、次のコマンドを参照してください。

- **show conn [detail | count], cluster exec show conn**

  show conn コマンドは、フローがディレクタ、バックアップ、またはフォワーダ フローのいずれであるかを示します。**cluster exec show conn** コマンドを任意のユニットで使用すると、すべての接続が表示されます。このコマンドの表示からは、1つのフローのトラフィックがクラスタ内のさまざまな ASA にどのように到達するかがわかります。クラスタのスループットは、ロード バランシングの効率とコンフィギュレーションによって異なります。このコマンドを利用すると、ある接続のトラフィックがクラスタ内をどのように流れるかが簡単にわかります。また、ロードバランサがフローのパフォーマンスにどのように影響を与えるかを理解するのに役立ちます。

  次に、**show conn detail** コマンドの出力例を示します。

```
ciscoasa/ASA2/slave# show conn detail
15 in use, 21 most used
Cluster:
        fwd connections: 0 in use, 0 most used
        dir connections: 0 in use, 0 most used
```

```
        centralized connections: 0 in use, 44 most used
Flags: A - awaiting inside ACK to SYN, a - awaiting outside ACK to SYN,
       B - initial SYN from outside, b - TCP state-bypass or nailed,
       C - CTIQBE media, c - cluster centralized,
       D - DNS, d - dump, E - outside back connection, e - semi-distributed,
       F - outside FIN, f - inside FIN,
       G - group, g - MGCP, H - H.323, h - H.225.0, I - inbound data,
       i - incomplete, J - GTP, j - GTP data, K - GTP t3-response
       k - Skinny media, L - LISP triggered flow owner mobility
       M - SMTP data, m - SIP media, n - GUP
       N - inspected by Snort
       O - outbound data, o - offloaded,
       P - inside back connection,
       Q - Diameter, q - SQL*Net data,
       R - outside acknowledged FIN,
       R - UDP SUNRPC, r - inside acknowledged FIN, S - awaiting inside SYN,
       s - awaiting outside SYN, T - SIP, t - SIP transient, U - up,
       V - VPN orphan, W - WAAS,
       w - secondary domain backup,
       X - inspected by service module,
       x - per session, Y - director stub flow, y - backup stub flow,
       Z - Scansafe redirection, z - forwarding stub flow

Cluster units to ID mappings:
  ID 0: unit-2-1
  ID 1: unit-1-1
  ID 2: unit-1-2
  ID 3: unit-2-2
  ID 4: unit-2-3
  ID 255: The default cluster member ID which indicates no ownership or affiliation

          with an existing cluster member
```

- **show cluster info [conn-distribution | packet-distribution | loadbalance]**

  show cluster info conn-distribution および **show cluster info packet-distribution** コマンドは、すべてのクラスタユニット間のトラフィックの分布を表示します。これらのコマンドは、外部ロード バランサを評価し、調整するのに役立ちます。

  show cluster info loadbalance コマンドは、接続再分散の統計情報を表示します。

- **show cluster {access-list | conn [count] | traffic | user-identity | xlate}** [*options*]、**show cluster chassis {access-list | conn | traffic | user-identity | xlate count}**

  クラスタ全体の集約データを表示します。使用可能なオプションはデータのタイプによって異なります。

  show cluster access-list コマンドの次の出力を参照してください。

```
ciscoasa# show cluster access-list
hitcnt display order: cluster-wide aggregated result, unit-A, unit-B,  unit-C, unit-D
access-list cached ACL log flows: total 0, denied 0 (deny-flow-max 4096) alert-interval
 300
access-list 101; 122 elements; name hash: 0xe7d586b5
access-list 101 line 1 extended permit tcp 192.168.143.0 255.255.255.0 any eq www
(hitcnt=0, 0, 0, 0, 0) 0x207a2b7d
access-list 101 line 2 extended permit tcp any 192.168.143.0 255.255.255.0 (hitcnt=0,
 0, 0, 0, 0) 0xfe4f4947
access-list  101 line 3 extended permit tcp host 192.168.1.183 host 192.168.43.238
(hitcnt=1, 0, 0, 0, 1) 0x7b521307
access-list 101 line 4 extended permit tcp host 192.168.1.116 host 192.168.43.238
```

```
(hitcnt=0, 0, 0, 0, 0) 0x5795c069
access-list 101 line 5 extended permit tcp host 192.168.1.177 host 192.168.43.238
(hitcnt=1, 0, 0, 1, 0) 0x51bde7ee
access list 101 line 6 extended permit tcp host 192.168.1.177 host 192.168.43.13
(hitcnt=0, 0, 0, 0, 0) 0x1e68697c
access-list 101 line 7 extended permit tcp host 192.168.1.177 host 192.168.43.132
(hitcnt=2, 0, 0, 1, 1) 0xc1ce5c49
access-list 101 line 8 extended permit tcp host 192.168.1.177 host 192.168.43.192
(hitcnt=3, 0, 1, 1, 1) 0xb6f59512
access-list 101 line 9 extended permit tcp host 192.168.1.177 host 192.168.43.44
(hitcnt=0, 0, 0, 0, 0) 0xdc104200
access-list 101 line 10 extended permit tcp host 192.168.1.112 host 192.168.43.44
(hitcnt=429, 109, 107, 109, 104)
0xce4f281d
access-list 101 line 11 extended permit tcp host 192.168.1.170 host 192.168.43.238
(hitcnt=3, 1, 0, 0, 2) 0x4143a818
access-list 101 line 12 extended permit tcp host 192.168.1.170 host 192.168.43.169
(hitcnt=2, 0, 1, 0, 1) 0xb18dfea4
access-list 101 line 13 extended permit tcp host 192.168.1.170 host 192.168.43.229
(hitcnt=1, 1, 0, 0, 0) 0x21557d71
access-list 101 line 14 extended permit tcp host 192.168.1.170 host 192.168.43.106
(hitcnt=0, 0, 0, 0, 0) 0x7316e016
access-list 101 line 15 extended permit tcp host 192.168.1.170 host 192.168.43.196
(hitcnt=0, 0, 0, 0, 0) 0x013fd5b8
access-list 101 line 16 extended permit tcp host 192.168.1.170 host 192.168.43.75
(hitcnt=0, 0, 0, 0, 0) 0x2c7dba0d
```

使用中の接続の、すべてのユニットでの 合計数を表示するには、次のとおりに入力します。

```
ciscoasa# show cluster conn count
Usage Summary In Cluster:*********************************************
124 in use, fwd connection 0 in use, dir connection 0 in use, centralized connection
0 in use (Cluster-wide aggregated)

unit-1-1(LOCAL):*****************************************************
40 in use, 48 most used, fwd connection 0 in use, 0 most used, dir connection 0 in
use,
0 most used, centralized connection 0 in use, 46 most used

unit-2-2:************************************************************
18 in use, 40 most used, fwd connection 0 in use, 0 most used, dir connection 0 in
use,
0 most used, centralized connection 0 in use, 45 most used
```

- **show asp cluster counter**

  このコマンドは、データパスのトラブルシューティングに役立ちます。

クラスタのルーティングのモニタリング

クラスタのルーティングについては、次のコマンドを参照してください。

- **show route cluster**
- **debug route cluster**

  クラスタのルーティング情報を表示します。

クラスタリングのロギングの設定

クラスタリングのロギングの設定については、次のコマンドを参照してください。

logging device-id

クラスタ内の各ユニットは、syslogメッセージを個別に生成します。**logging device-id** コマンドを使用すると、同一または異なるデバイスID付きでsyslogメッセージを生成することができ、クラスタ内の同一または異なるユニットからのメッセージのように見せることができます。

クラスタリングのデバッグ

クラスタリングのデバッグについては、次のコマンドを参照してください。

- **debug cluster [ccp | datapath | fsm | general | hc | license | rpc | service-module | transport]**

  クラスタリングのデバッグ メッセージを表示します。

- **debug service-module**

  スーパバイザとアプリケーション間のヘルス チェックの問題を含め、ブレード レベルの問題に関するデバッグ メッセージを表示します。

- **show cluster info trace**

  show cluster info trace コマンドは、トラブルシューティングのためのデバッグ情報を表示します。

  show cluster info trace コマンドについては次の出力を参照してください。

```
ciscoasa# show cluster info trace
 Feb 02 14:19:47.456 [DBUG]Receive CCP message: CCP_MSG_LOAD_BALANCE
 Feb 02 14:19:47.456 [DBUG]Receive CCP message: CCP_MSG_LOAD_BALANCE
 Feb 02 14:19:47.456 [DBUG]Send CCP message to all: CCP_MSG_KEEPALIVE from 80-1 at
MASTER
```

クラスタリングの参考資料

このセクションには、クラスタリングの動作に関する詳細情報が含まれます。

パフォーマンス スケーリング係数

複数のユニットをクラスタに結合した場合、期待できる合計クラスタ パフォーマンスの概算値は次のようになります。

- TCP または CPS の合計スループットの 80 %
- UDP の合計スループットの 90 %
- トラフィックの混在に応じて、イーサネットMIX（EMIX）の合計スループットの60 %。

たとえば、TCP スループットについては、3 つのモジュールを備えた Firepower 9300 は、単独で動作している場合、約 135 Gbps の実際のファイアウォール トラフィックを処理できます。2 シャーシの場合、最大スループットの合計は 270 Gbps（2 シャーシ X 135 Gbps）の約 80 %、つまり 216 Gbps です。

マスター ユニット選定

クラスタのメンバは、クラスタ制御リンクを介して通信してマスターユニットを選定します。方法は次のとおりです。

1. クラスタを展開すると、各ユニットは選定要求を 3 秒ごとにブロードキャストします。
2. プライオリティの高い他のユニットがこの選定要求に応答します。プライオリティはクラスタの展開時に設定され、設定の変更はできません。
3. 45 秒経過しても、プライオリティの高い他のユニットからの応答を受信していない場合は、そのユニットがマスターになります。
4. 後からクラスタに参加したユニットのプライオリティの方が高い場合でも、そのユニットが自動的にマスター ユニットになることはありません。既存のマスター ユニットは常にマスターのままです。ただし、マスターユニットが応答を停止すると、その時点で新しいマスター ユニットが選定されます。

（注） 特定のユニットを手動で強制的にマスターにすることができます。中央集中型機能については、マスターユニット変更を強制するとすべての接続がドロップされるので、新しいマスターユニット上で接続を再確立する必要があります。

クラスタ内のハイ アベイラビリティ

クラスタリングは、シャーシ、ユニットとインターフェイスの正常性を監視し、ユニット間で接続状態を複製することにより、ハイ アベイラビリティを提供します。

シャーシアプリケーションのモニタリング

シャーシアプリケーションのヘルス モニタリングは常に有効になっています。Firepower 9300 シャーシスーパーバイザはASAアプリケーションを定期的に確認します（毎秒）。ASAが作動中で、Firepower 9300 シャーシスーパーバイザと 3 秒間通信できなければASAは syslog メッセージを生成して、クラスタを離れます。

Firepower 9300 シャーシスーパーバイザが 45 秒後にアプリケーションと通信できなければ、ASAをリロードします。ASAがスーパーバイザと通信できなければ、自身をクラスタから削除します。

ユニットのヘルス モニタリング

マスター ユニットは、各スレーブ ユニットをモニタするために、クラスタ制御リンクを介してキープアライブ メッセージを定期的に送信します（間隔は設定可能です）。各スレーブ ユニットは、同じメカニズムを使用してマスター ユニットをモニタします。ユニットの健全性チェックが失敗すると、ユニットはクラスタから削除されます。

インターフェイス モニタリング

各ユニットは、使用中のすべてのハードウェア インターフェイスのリンク ステータスをモニタし、ステータス変更をマスター ユニットに報告します。ヘルス モニタリングを有効にすると、デフォルトではすべての物理インターフェイスがモニタされます（EtherChannel インターフェイスのメインEtherChannelを含む）。アップ状態の指名されたインターフェイスのみモニタできます。たとえば、名前付き EtherChannel がクラスタから削除される前に、EtherChannel のすべてのメンバー ポートがエラーとなる必要があります（最小ポート バンドル設定に基づく）。ヘルスチェックは、インターフェイスごとに、モニタリングをオプションで無効にすることができます。

あるモニタ対象のインターフェイスが、特定のユニット上では障害が発生したが、別のユニットではアクティブの場合は、そのユニットはクラスタから削除されます。ASAがメンバーをクラスタから削除するまでの時間は、そのユニットが確立済みメンバーであるか、またはクラスタに参加しようとしているかによって異なります。ASAは、ユニットがクラスタに参加する最初の 90 秒間はインターフェイスを監視ししません。この間にインターフェイスのステータスが変化しても、ASAはクラスタから削除されません。設定済みのメンバーの場合は、500 ミリ秒後にユニットが削除されます

障害後のステータス

クラスタ内のユニットで障害が発生したときに、そのユニットでホスティングされている接続は他のユニットにシームレスに移管されます。トラフィック フローのステート情報は、クラスタ制御リンクを介して共有されます。

マスターユニットで障害が発生した場合は、そのクラスタの他のメンバーのうち、プライオリティが最高（番号が最小）のものがマスター ユニットになります。

障害イベントに応じて、ASA は自動的にクラスタへの再参加を試みます。

（注） ASAが非アクティブになり、クラスタへの自動再参加に失敗すると、すべてのデータインターフェイスがシャットダウンされます。管理専用インターフェイスのみがトラフィックを送受信できます。 管理インターフェイスは、そのユニットがクラスタ IP プールから受け取った IP アドレスを使用して引き続き稼働状態となります。ただし、リロードする場合、クラスタでユニットがまだ非アクティブになっていると、管理インターフェイスはディセーブルになります。それ以降のコンフィギュレーション作業には、コンソール ポートを使用する必要があります。

クラスタへの再参加

クラスタ メンバがクラスタから削除された後、クラスタに再参加できる方法は、削除された理由によって異なります。

- クラスタ制御リンクの障害：クラスタ制御リンクの問題を解決した後、ASA コンソール ポートで **cluster group** *name* と入力してから **enable** と入力して、クラスタリングを再びイネーブルにすることによって、手動でクラスタに再参加する必要があります。
- データ インターフェイスの障害：ASA は自動的に最初は 5 分後、次に 10 分後、最終的に 20 分後に再参加を試みます。20 分後に参加できない場合、ASA はクラスタリングをディセーブルにします。データ インターフェイスの問題を解決した後、ASA コンソール ポートで **cluster group** *name* と入力してから **enable** と入力して、クラスタリングを手動でイネーブルにする必要があります。
- ユニットの障害：ユニットがヘルスチェック失敗のためクラスタから削除された場合、クラスタへの再参加は失敗の原因によって異なります。たとえば、一時的な電源障害の場合は、クラスタ制御リンクが稼働している限り、ユニットは再起動するとクラスタに再参加します。ユニットは 5 秒ごとにクラスタへの再参加を試みます。
- シャーシ アプリケーション通信の障害：ASA がシャーシ アプリケーションの状態が回復したことを検出すると、ASA は自動的にクラスタの再参加を試みます。
- 内部エラー：内部の障害には、アプリケーション同期のタイムアウト、矛盾したアプリケーション ステータスなどがあります。 問題を解決したら、コンソール ポートで **cluster group** *name* 入力してから **enable**と入力することでクラスタリングを再び有効にして、クラスタに手動で再参加する必要があります。

データ パス接続状態の複製

どの接続にも、1 つのオーナーおよび少なくとも 1 つのバックアップ オーナーがクラスタ内にあります。バックアップ オーナーは、障害が発生しても接続を引き継ぎません。代わりに、TCP/UDP のステート情報を保存します。これは、障害発生時に接続が新しいオーナーにシームレスに移管されるようにするためです。バックアップ オーナーは通常ディレクタでもあります。

トラフィックの中には、TCP または UDP レイヤよりも上のステート情報を必要とするものがあります。この種類のトラフィックに対するクラスタリングのサポートの可否については、次の表を参照してください。

表 *14*：クラスタ全体で複製される機能

Traffic	状態のサポート	注意
Up time	Yes	システム アップ タイムをトラッキングします。
ARP Table	Yes	トランスペアレント モードのみ。

Traffic	状態のサポート	注意
MAC アドレス テーブル	Yes	トランスペアレント モードのみ。
ユーザ アイデンティティ	Yes	AAA ルール（uauth）とアイデンティティ ファイアウォールが含まれます。
IPv6 ネイバー データベース	Yes	—
ダイナミック ルーティング	Yes	—
SNMP エンジン ID	なし	—
集中型 VPN（サイト間）	なし	VPN セッションは、マスター ユニットで障害が発生すると切断されます。

クラスタが接続を管理する方法

接続をクラスタの複数のメンバにロードバランスできます。接続のロールにより、通常動作時とハイ アベイラビリティ状況時の接続の処理方法が決まります。

接続のロール

接続ごとに定義された次のロールを参照してください。

- オーナー：通常、最初に接続を受信するユニット。オーナーは、TCP 状態を保持し、パケットを処理します。1 つの接続に対してオーナーは 1 つだけです。元のオーナーに障害が発生すると、新しいユニットが接続からパケットを受信したときにディレクタがこれらのユニットの新しいオーナーを選択します。
- バックアップ オーナー：オーナーから受信した TCP/UDP ステート情報を格納するユニット。これにより、障害が発生した場合に新しいオーナーにシームレスに接続を転送できます。バックアップ オーナーは、障害発生時に接続を引き継ぎません。オーナーが使用不可能になった場合は、その接続からパケットを受け取る最初のユニット（ロードバランシングに基づく）がバックアップ オーナーに問い合わせて、関連するステート情報を取得し、これでそのユニットが新しいオーナーになることができます。

  ディレクタ（下記参照）がオーナーと同じユニットでない限り、ディレクタはバックアップ オーナーでもあります。オーナーがディレクタとして自分自身を選択すると、別のバックアップ オーナーが選択されます。
- ディレクタ：フォワーダからのオーナールックアップ要求を処理するユニット。オーナーが新しい接続を受信すると、オーナーは、送信元/宛先 IP アドレスおよび ポートのハッシュに基づいてディレクタを選択し、新しい接続を登録するためにメッセージをそのディレクタに送信します。パケットがオーナー以外のユニットに到着した場合は、そのユニッ

トはどのユニットがオーナーかをディレクタに問い合わせます。これで、パケットを転送できるようになります。1 つの接続に対してディレクタは 1 つだけです。ディレクタが失敗すると、オーナーは新しいディレクタを選択します。

ディレクタがオーナーと同じユニットでない限り、ディレクタはバックアップ オーナーでもあります（上記参照）。オーナーがディレクタとして自分自身を選択すると、別のバックアップ オーナーが選択されます。

- フォワーダ：パケットをオーナーに転送するユニット。フォワーダが接続のパケットを受信したときに、その接続のオーナーが自分ではない場合は、フォワーダはディレクタにオーナーを問い合わせてから、そのオーナーへのフローを確立します。これは、この接続に関してフォワーダが受信するその他のパケット用です。ディレクタは、フォワーダにもなることができます。フォワーダが SYN-ACK パケットを受信した場合、フォワーダはパケットの SYN クッキーからオーナーを直接取得できるので、ディレクタに問い合わせる必要がないことに注意してください（TCP シーケンスのランダム化をディセーブ ルにした場合は、SYN Cookie は使用されないので、ディレクタへの問い合わせが必要です）。存続期間が短いフロー（たとえばDNSやICMP）の場合は、フォワーダは問い合わせの代わりにパケットを即座にディレクタに送信し、ディレクタがそのパケットをオーナーに送信します。1 つの接続に対して、複数のフォワーダが存在できます。最も効率的なスループットを実現できるのは、フォワーダが 1 つもなく、接続のすべてのパケットをオーナーが受信するという、優れたロードバランシング方法が使用されている場合です。

接続でポート アドレス変換（PAT）を使用すると、PAT のタイプ（per-session または multi-session）が、クラスタのどのメンバが新しい接続のオーナーになるかに影響します。

- Per-session PAT：オーナーは、接続の最初のパケットを受信するユニットです。

  デフォルトでは、TCP および DNS UDP トラフィックは per-session PAT を使用します。

- Multi-session PAT：オーナーは常にマスター ユニットです。multi-session PAT 接続がスレーブ ユニットで最初に受信される場合、スレーブ ユニットはその接続をマスター ユニットに転送します。

  デフォルトでは、UDP（DNS UDP を除く）および ICMP トラフィックは multi-session PAT を使用するので、これらの接続は常にマスター ユニットによって所有されています。

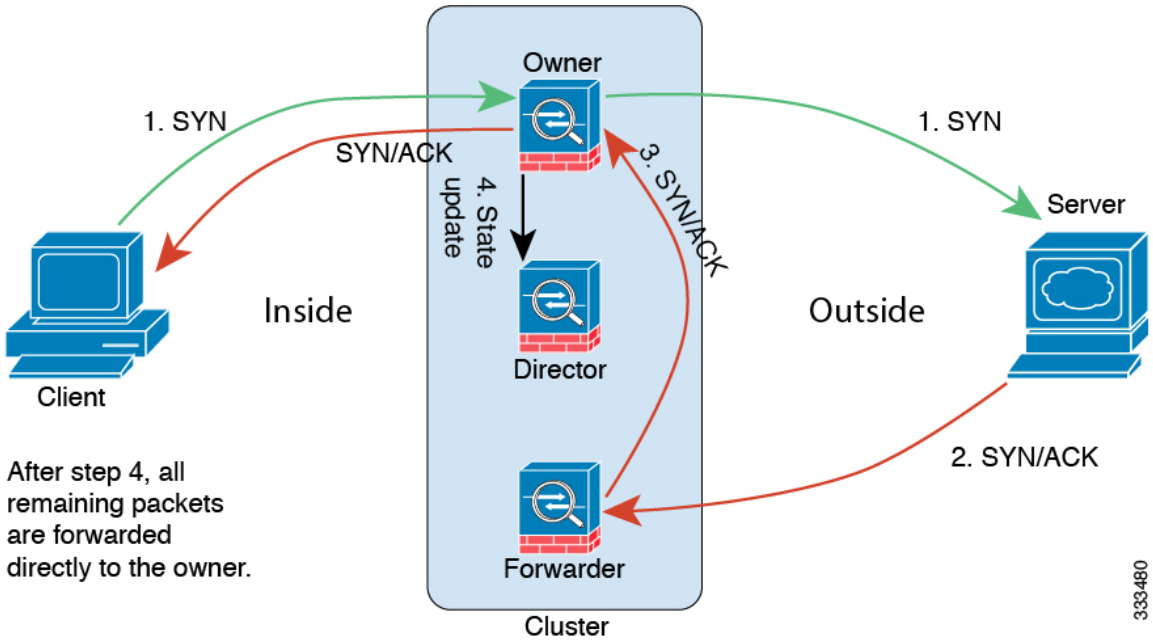
TCP および UDP の per-session PAT デフォルトを変更できるので、これらのプロトコルの接続は、その設定に応じて per-session または multi-session で処理されます。ICMP の場合は、デフォルトの multi-session PAT から変更することはできません。per-session PAT の詳細については、『ファイアウォールの構成ガイド』を参照してください。

新しい接続の所有権

新しい接続がロードバランシング経由でクラスタのメンバに送信される場合は、そのユニットがその接続の両方向のオーナーとなります。接続のパケットが別のユニットに到着した場合は、そのパケットはクラスタ制御リンクを介してオーナーユニットに転送されます。逆方向のフローが別のユニットに到着した場合は、元のユニットにリダイレクトされます。

サンプル データ フロー

次の例は、新しい接続の確立を示します。



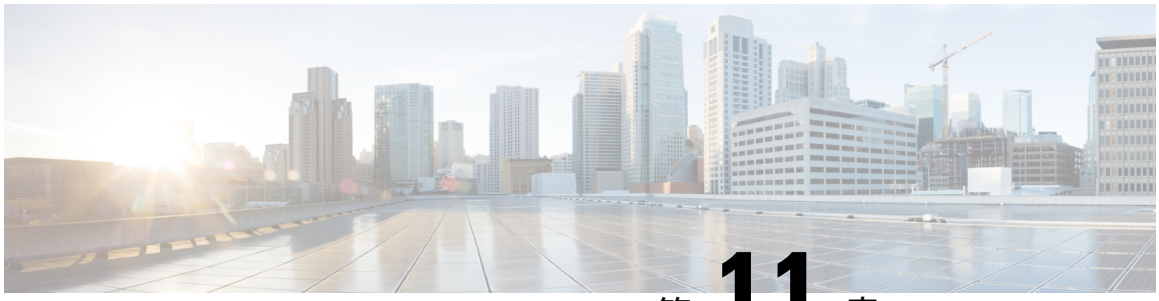
1. SYN パケットがクライアントから発信され、ASA の 1 つ（ロード バランシング方法に基づく）に配信されます。これがオーナーとなります。オーナーはフローを作成し、オーナー情報をエンコードして SYN Cookie を生成し、パケットをサーバに転送します。
2. SYN-ACK パケットがサーバから発信され、別の ASA（ロード バランシング方法に基づく）に配信されます。この ASA はフォワーダです。
3. フォワーダはこの接続を所有してはいないので、オーナー情報を SYN Cookie からデコードし、オーナーへの転送フローを作成し、SYN-ACK をオーナーに転送します。
4. オーナーはディレクタに状態アップデートを送信し、SYN-ACK をクライアントに転送します。
5. ディレクタは状態アップデートをオーナーから受信し、オーナーへのフローを作成し、オーナーと同様に TCP ステート情報を記録します。ディレクタは、この接続のバックアップ オーナーとしての役割を持ちます。
6. これ以降、フォワーダに配信されたパケットはすべて、オーナーに転送されます。
7. パケットがその他のユニットに配信された場合は、そのユニットはディレクタに問い合わせてオーナーを特定し、フローを確立します。
8. フローの状態が変化した場合は、状態アップデートがオーナーからディレクタに送信されます。

Firepower 9300 シャーシ 上の ASA クラスタリングの履歴

機能名	バージョン	機能情報
Firepower 9300 用シャーシ内 ASA クラスタリング	9.4(1.150)	FirePOWER 9300 シャーシ内では、最大 3 つセキュリティ モジュールをクラスタ化できます。シャーシ内のすべてのモジュールは、クラスタに属している必要があります。 次のコマンドを導入しました。**cluster replication delay**、**debug service-module**、**management-only individual**、**show cluster chassis**

第 III 部

インターフェイス



第 11 章

基本的なインターフェイス設定

この章では、イーサネット設定、ジャンボ フレーム設定などの基本インターフェイス設定について説明します。

（注） マルチコンテキストモードでは、この項のすべてのタスクをシステム実行スペースで実行してください。コンテキストからシステム実行スペースに切り替えるには、**changeto system** コマンドを入力します。。

（注） ASA サービス モジュール インターフェイスについては、『ASA Services Module quick start guide』を参照してください。

Firepower 9300 シャーシ では、FXOS オペレーティング システムで基本的なインターフェイス設定を行います。詳細については、お使いのシャーシの設定または導入ガイドを参照してください。

基本的なインターフェイス設定について

この項では、インターフェイスの機能と特殊なインターフェイスについて説明します。

Auto-MDI/MDIX 機能

RJ-45 インターフェイスでは、デフォルトの自動ネゴシエーション設定に Auto-MDI/MDIX 機能も含まれています。Auto-MDI/MDIX は、オートネゴシエーション フェーズでストレートケーブルを検出すると、内部クロスオーバーを実行することでクロス ケーブルによる接続を不要にします。インターフェイスの Auto-MDI/MDIX をイネーブルにするには、速度とデュプレックスのいずれかをオートネゴシエーションに設定する必要があります。速度とデュプレックスの両方に明示的に固定値を指定すると、両方の設定でオートネゴシエーションがディセーブルにされ、Auto-MDI/MDIX もディセーブルになります。ギガビット イーサネットの速度と二重通信をそれぞれ 1000 と全二重に設定すると、インターフェイスでは常にオートネゴシエーションが実行されるため、Auto-MDI/MDIX は常にイネーブルになり、ディセーブルにできません。

管理インターフェイス

管理インターフェイスは、使用しているモデルに応じて、管理トラフィック専用の個別インターフェイスとなります。

管理インターフェイスの概要

次のインターフェイスに接続して ASA を管理できます。

- 任意の通過トラフィック インターフェイス
- 専用の管理スロット/ポート インターフェイス（使用しているモデルで使用できる場合）

管理アクセス （957 ページ）の説明に従って、管理アクセスへのインターフェイスを設定する必要がある場合があります。

管理スロット/ポート インターフェイス

次の表に、モデルごとの管理インターフェイスを示します。

表 *15*：モデルごとの管理インターフェイス

モデル	管理 0/0	管理 0/1	管理 1/0	管理 1/1	通過トラフィックに対して設定可能	サブインターフェイスを使用可能
Firepower 9300	該当なし インターフェイス ID は ASA 論理デバイスに割り当てた物理 mgmt タイプ インターフェイスに基づいています。	—	—	—	—	○

モデル	管理 0/0	管理 0/1	管理 1/0	管理 1/1	通過トラフィックに対して設定可能	サブインターフェイスを使用可能
ASA 5506-X	—	—	—	○	—	—
ASA 5508-X	—	—	—	○	—	—
ASA 5512-X	○	—	—	—	—	—
ASA 5515-X	○	—	—	—	—	—
ASA 5516-X	—	—	—	○	—	—
ASA 5525-X	○	—	—	—	—	—
ASA 5545-X	○	—	—	—	—	—
ASA 5555-X	○	—	—	—	—	—
ASA 5585-X	○	○	○ SSP をスロット 1 に設置した場合は、Management 1/0 および 1/1 ではスロット 1 の SSP への管理アクセスのみが提供されます。	○	○	○
ISA 3000	—	—	—	○	—	—
ASASM	—	—	—	—	—	—
ASAv	○	—	—	—	—	—

（注） モジュールをインストールした場合は、モジュール管理インターフェイスでは、モジュールの管理アクセスのみが提供されます。ソフトウェア モジュールを搭載したモデルでは、ソフトウェア モジュールによって ASA と同じ物理管理インターフェイスが使用されます。

管理専用トラフィックに対する任意のインターフェイスの使用

任意のインターフェイスを、管理トラフィック用として設定することによって管理専用インターフェイスとして使用できます。これには、EtherChannel インターフェイスも含まれます（**management-only** コマンドを参照）。

トランスペアレント モードの管理インターフェイス

トランスペアレント ファイアウォール モードでは、許可される最大通過トラフィック インターフェイスに加えて、管理インターフェイス（物理インターフェイス、サブインターフェイス（使用しているモデルでサポートされている場合）、管理インターフェイスからなるEtherChannelインターフェイス（複数の管理インターフェイスがある場合）のいずれか）を個別の管理インターフェイスとして使用できます。他のインターフェイス タイプは管理インターフェイスとして使用できません。Firepower 9300 シャーシ では、管理インターフェイス ID は ASA 論理デバイスに割り当てた mgmt-type インターフェイスに基づいています。

マルチ コンテキスト モードでは、どのインターフェイスも（これには管理インターフェイスも含まれます）、コンテキスト間で共有させることはできません。コンテキスト単位で管理を行うには、管理インターフェイスのサブインターフェイスを作成し、管理サブインターフェイスを各コンテキストに割り当てます。ASA 5555-X 以前では、管理インターフェイスのサブインターフェイスは許可されないので、コンテキスト単位で管理を行うには、データ インターフェイスに接続する必要があります。

管理インターフェイスは、通常のブリッジ グループの一部ではありません。動作上の目的から、設定できないブリッジ グループの一部です。

（注） トランスペアレント ファイアウォール モードでは、管理インターフェイスによってデータ インターフェイスと同じ方法でMACアドレステーブルがアップデートされます。したがって、いずれかのスイッチ ポートをルーテッド ポートとして設定しない限り、管理インターフェイスおよびデータ インターフェイスを同じスイッチに接続しないでください（デフォルトでは、Catalyst スイッチがすべての VLAN スイッチ ポートの MAC アドレスを共有します）。そうしないと、物理的に接続されたスイッチから管理インターフェイスにトラフィックが到着すると、ASA によって、データ インターフェイスではなく、管理インターフェイスを使用してスイッチにアクセスするようにMACアドレステーブルがアップデートされます。この処理が原因で、一時的にトラフィックが中断します。セキュリティ上の理由から、少なくとも 30 秒間は、スイッチからデータ インターフェイスへのパケットのために MAC アドレス テーブルが ASA によって再アップデートされることはありません。

冗長管理インターフェイスの非サポート

冗長インターフェイスは、Management *slot*/*port* インターフェイスをメンバとしてサポートしません。ただし、管理インターフェイス以外の複数インターフェイスからなる冗長インターフェイスを、管理専用として設定できます。

ASA モデルの管理インターフェイスの特性

ASA 5585-X を除く ASA 5500-X モデルの管理インターフェイスには、次の特性があります。

- 通過トラフィックはサポートされません。
- サブインターフェイスはサポートされません
- プライオリティ キューはサポートされません

- マルチキャスト MAC はサポートされません
- ソフトウェア モジュールは、管理インターフェイスを共有します。ASA とモジュールに対して、別の MAC アドレスと IP アドレスがサポートされます。モジュールのオペレーティング システムでモジュールの IP アドレスのコンフィギュレーションを実行する必要があります。ただし、物理特性（インターフェイスの有効化など）は、ASA 上で設定されます。

基本インターフェイスの設定のライセンス

モデル	ライセンス要件
ASA 5585-X	SSP-10 および SSP-20 のインターフェイス速度： • 基本ライセンス：ファイバ インターフェイスの場合 1 ギガビット イーサネット • 10 GE I/O ライセンス（Security Plus）：ファイバ インターフェイスの場合 10 ギガビット イーサネット •（SSP-40 および SSP-60 は 10 ギガビット イーサネットをデフォルトでサポートします）。

基本インターフェイスの設定のガイドライン

トランスペアレント ファイアウォール モード

マルチコンテキストのトランスペアレントモードでは、各コンテキストが別個のインターフェイスを使用する必要があります。コンテキスト間でインターフェイスを共有することはできません。

フェールオーバー

データインターフェイスと、フェールオーバーまたはステートのインターフェイスを共有することはできません。

その他のガイドライン

一部の管理関連のサービスは、管理対象外のインターフェイスが有効になり、ASAが「システム レディ」状態になるまで使用できません。ASA が「System Ready」状態になると、次の syslog メッセージを生成します。

```
%ASA-6-199002: Startup completed.  Beginning operation.
```

基本インターフェイスのデフォルト設定

この項では、工場出荷時のデフォルトコンフィギュレーションが設定されていない場合のインターフェイスのデフォルト設定を示します。

インターフェイスのデフォルトの状態

インターフェイスのデフォルトの状態は、そのタイプおよびコンテキストモードによって異なります。

マルチ コンテキスト モードでは、システム実行スペース内でのインターフェイスの状態にかかわらず、すべての割り当て済みのインターフェイスがデフォルトでイネーブルになっています。ただし、トラフィックがインターフェイスを通過するためには、そのインターフェイスもシステム実行スペース内でイネーブルになっている必要があります。インターフェイスをシステム実行スペースでシャットダウンすると、そのインターフェイスは、それを共有しているすべてのコンテキストでダウンします。

シングルモードまたはシステム実行スペースでは、インターフェイスのデフォルトの状態は次のとおりです。

- 物理インターフェイス：ディセーブル。
- 冗長インターフェイス：イネーブル。ただし、トラフィックが冗長インターフェイスを通過するためには、メンバ物理インターフェイスもイネーブルになっている必要があります。
- VLAN サブインターフェイス：イネーブル。ただし、トラフィックがサブインターフェイスを通過するためには、物理インターフェイスもイネーブルになっている必要があります。
- VXLAN VNI インターフェイス：イネーブル。
- EtherChannel ポートチャネルインターフェイス（ASA モデル）：イネーブル。ただし、トラフィックが EtherChannel を通過するためには、チャネル グループ物理インターフェイスもイネーブルになっている必要があります。
- EtherChannel ポートチャネル インターフェイス（Firepower モデル）：ディセーブル。

（注） Firepower 9300 の場合、管理上、シャーシおよび ASA の両方で、インターフェイスを有効および無効にできます。インターフェイスを動作させるには、両方のオペレーティング システムで、インターフェイスを有効にする必要があります。インターフェイスの状態は個別に制御されるので、シャーシと ASA の間の不一致が生じることがあります。

デフォルトの速度および二重通信

- デフォルトでは、銅線（RJ-45）インターフェイスの速度とデュプレックスは、オートネゴシエーションに設定されます。
- 5585-X のファイバ インターフェイスでは、自動リンク ネゴシエーションの速度が設定されます。

デフォルトのコネクタ タイプ

2 つのコネクタ タイプ（copper RJ-45 と fiber SFP）を持つモデルもあります。RJ-45 がデフォルトです。ASA にファイバ SFP コネクタを使用するように設定できます。

デフォルトの MAC アドレス

デフォルトでは、物理インターフェイスはバーンドイン MAC アドレスを使用し、物理インターフェイスのすべてのサブインターフェイスは同じバーンドイン MAC アドレスを使用します。

物理インターフェイスのイネーブル化およびイーサネット パラメータの設定

ここでは、次の方法について説明します。

- 物理インターフェイスをイネーブルにする。
- 特定の速度と二重通信（使用できる場合）を設定する。
- フロー制御のポーズ フレームをイネーブルにする。

始める前に

マルチ コンテキスト モードでは、システム実行スペースで次の手順を実行します。コンテキストからシステム実行スペースに切り替えるには、**changeto system** コマンドを入力します。

手順

ステップ 1 設定するインターフェイスを指定します。

interface *physical_interface*

例：

```
ciscoasa(config)# interface gigabitethernet 0/0
```

physical_interface ID には、タイプ、スロット、およびポート番号（type[slot/]port）が含まれます。

物理インターフェイスのタイプには、次のものがあります。

- **gigabitethernet**
- **tengigabitethernet**
- **management**

タイプに続けてスロット/ポートを入力します。たとえば、**gigabitethernet0/1** というようになります。タイプとスロット/ポートの間のスペースは任意です。

ステップ 2 （任意）使用しているモデルで利用できる場合には、メディア タイプを SFP に設定します。

media-type sfp

デフォルトの RJ-45 に戻すには、**media-type rj45** コマンドを入力します。

ステップ 3 （任意）速度を設定します。

speed{**auto** |**10** |**100** |**1000** |**nonegotiate**}

例：

```
ciscoasa(config-if)# speed 100
```

RJ-45 インターフェイスのデフォルト設定は **auto** です。

SFP インターフェイスのデフォルト設定は **no speed nonegotiate** です。この設定では、速度が最大速度に設定され、フロー制御パラメータとリモート障害情報のリンク ネゴシエーションがイネーブルになります。**nonegotiate** キーワードは、SFP インターフェイスで使用できる唯一のキーワードです。**speed nonegotiate** コマンドは、リンク ネゴシエーションをディセーブルにします。

ステップ 4 （任意）RJ-45 インターフェイスのデュプレックスを設定します。

duplex {**auto** | **full** | **half**}

例：

```
ciscoasa(config-if)# duplex full
```

auto 設定がデフォルトです。EtherChannel インターフェイスのデュプレックスの設定は **Full** または **Auto** である必要があります。

ステップ 5 （任意）GigabitEthernet インターフェイスと TenGigabitEthernet インターフェイスのフロー制御のポーズ（XOFF）フレームをイネーブルにします。

flowcontrol send on [*low_water high_water pause_time*] [**noconfirm**]

例：

```
ciscoasa(config-if)# flowcontrol send on 95 200 10000
```

トラフィック バーストが発生している場合、バーストがNICのFIFOバッファまたは受信リングバッファのバッファリング容量を超えると、パケットがドロップされる可能性があります。フロー制御用のポーズ フレームをイネーブルにすると、このような問題の発生を抑制できます。ポーズ（XOFF）およびXONフレームは、FIFOバッファ使用量に基づいて、NICハードウェアによって自動的に生成されます。バッファ使用量が高ウォーター マークを超えると、ポーズ フレームが送信されます。デフォルトの *high_water* 値は128 KB（10ギガビット イーサネット）および24 KB（1ギガビット イーサネット）です。0 ～ 511（10ギガビット イーサネット）または0 ～ 47 KB（1ギガビット イーサネット）に設定できます。ポーズの送信後、バッファ使用量が低ウォーターマークよりも下回ると、XONフレームを送信できます。デフォルトでは、*low_water* 値は64 KB（10ギガビット イーサネット）および16 KB（1ギガビット イーサネット）です。0 ～ 511（10ギガビット イーサネット）または0 ～ 47 KB（1ギガビット イーサネット）に設定できます。リンク パートナーは、XONを受信した後、またはXOFFの期限が切れた後、トラフィックを再開できます。XOFFの期限は、ポーズフレーム内のタイマー値によって制御されます。デフォルトの *pause_time* 値は26624です。この値は0 ～ 65535に設定できます。バッファの使用量が継続的に高基準値を超えている場合は、ポーズリフレッシュのしきい値に指定された間隔でポーズ フレームが繰り返し送信されます。

このコマンドを使用すると、次の警告が表示されます。

```
Changing flow-control parameters will reset the interface. Packets may be lost during
the reset.
Proceed with flow-control changes?
```

プロンプトを表示しないでパラメータを変更するには、**noconfirm** キーワードを使用します。

（注） 802.3xに定義されているフロー制御フレームのみがサポートされています。プライオリティベースのフロー制御はサポートされていません。

ステップ6 インターフェイスをイネーブルにします。

no shutdown

例：

```
ciscoasa(config-if)# no shutdown
```

インターフェイスをディセーブルにするには、**shutdown** コマンドを入力します。**shutdown** コマンドを入力すると、すべてのサブインターフェイスもシャットダウンします。インターフェイスをシステム実行スペースでシャットダウンすると、そのインターフェイスは、そのインターフェイスを共有しているすべてのコンテキストでシャットダウンします。

ジャンボ フレーム サポートの有効化

ジャンボ フレームとは、標準的な最大値 1518 バイト（レイヤ 2 ヘッダーおよび VLAN ヘッダーを含む）より大きく、9216 バイトまでのイーサネット パケットのことです。イーサネットフレームを処理するためのメモリ容量を増やすことにより、すべてのインターフェイスに対してジャンボ フレームのサポートをイネーブルにできます。ジャンボ フレームに割り当てるメモリを増やすと、他の機能（ACL など）の最大使用量が制限される場合があります。ASA MTU はレイヤ 2（14 バイト）および VLAN ヘッダー（4 バイト）を含まずにペイロードサイズを設定するので、モデルによっては MTU 最大値が 9198 になることに注意してください。

始める前に

- マルチ コンテキスト モードでは、システム実行スペースでこのオプションを設定します。
- この設定を変更した場合は、ASA のリロードが必要です。
- ジャンボフレームを送信する必要のある各インターフェイスの MTU を、デフォルト値の 1500 より大きい値に設定してください。たとえば、**mtu** コマンドを使用して値を 9198 に設定します。マルチ コンテキスト モードでは、各コンテキスト内で MTU を設定します。
- Be sure to adjust the TCP MSS, either to disable it for non-IPsec traffic (use the **sysopt connection tcpmss 0** command), or to increase it in accord with the MTU.

手順

ジャンボ フレーム サポートをイネーブルにします。

jumbo-frame reservation

例

次に、ジャンボ フレームの予約をイネーブルにし、コンフィギュレーションを保存して ASA をリロードする例を示します。

```
ciscoasa(config)# jumbo-frame reservation
WARNING: this command will take effect after the running-config is saved
and the system has been rebooted. Command accepted.

ciscoasa(config)# write memory
Building configuration...
Cryptochecksum: 718e3706 4edb11ea 69af58d0 0a6b7cb5

70291 bytes copied in 3.710 secs (23430 bytes/sec)
[OK]
ciscoasa(config)# reload
Proceed with reload? [confirm] Y
```

モニタリング インターフェイス

次のコマンドを参照してください。

- **show interface**

  インターフェイス統計情報を表示します。

- **show interface ip brief**

  インターフェイスの IP アドレスとステータスを表示します。

基本インターフェイスの例

次の設定例を参照してください。

物理インターフェイス パラメータの例

次に、シングル モードで物理インターフェイスのパラメータを設定する例を示します。

```
interface gigabitethernet 0/1
speed 1000
duplex full
no shutdown
```

マルチ コンテキスト モードの例

次に、システム コンフィギュレーション用にマルチ コンテキスト モードでインターフェイス パラメータを設定し、GigabitEthernet 0/1.1 サブインターフェイスをコンテキスト A に割り当てる例を示します。

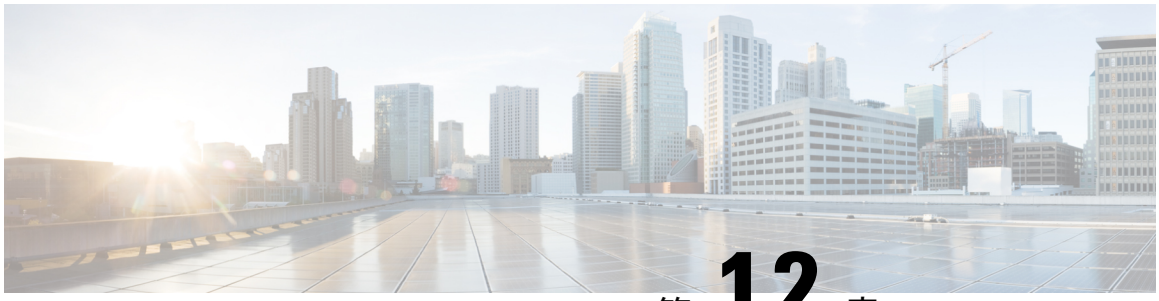
```
interface gigabitethernet 0/1
speed 1000
duplex full
no shutdown
interface gigabitethernet 0/1.1
vlan 101
context contextA
allocate-interface gigabitethernet 0/1.1
```

基本インターフェイスの設定の履歴

表 *16*：インターフェイスの履歴

機能名	リリース	機能情報
ASA 5510 上の基本ライセンスに対する増加したインターフェイス	7.2(2)	ASA 5510 上の基本ライセンスについて、最大インターフェイス数が 3 プラス管理インターフェイスから無制限のインターフェイスに増加しました。
ASA 5510 Security Plus ライセンスに対するギガビット イーサネット サポート	7.2(3)	ASA 5510 は、GE（ギガビット イーサネット）を Security Plus ライセンスのあるポート 0 および 1 でサポートするようになりました。ライセンスを Base から Security Plus にアップグレードした場合、外部 Ethernet 0/0 および Ethernet 0/1 ポートの容量は、元の FE（ファストイーサネット）の 100 Mbps から GE の 1000 Mbps に増加します。インターフェイス名は Ethernet 0/0 および Ethernet 0/1 のままです。**speed** コマンドを使用してインターフェイスの速度を変更します。また、**show interface** コマンドを使用して各インターフェイスの現在の設定速度を確認します。

機能名	リリース	機能情報
ASA 5580 に対するジャンボ パケット サポート	8.1(1)	Cisco ASA 5580 はジャンボ フレームをサポートしています。ジャンボフレームとは、標準的な最大値 1518 バイト（レイヤ 2 ヘッダーおよび FCS を含む）より大きく、9216 バイトまでのイーサネット パケットのことです。イーサネットフレームを処理するためのメモリ容量を増やすことにより、すべてのインターフェイスに対してジャンボフレームのサポートをイネーブルにできます。ジャンボフレームに割り当てるメモリを増やすと、他の機能（ACL など）の最大使用量が制限される場合があります。 この機能は、ASA 5585-X でもサポートされます。 **jumbo-frame reservation** コマンドが導入されました。
ASA 5580 10 ギガビット イーサネット インターフェイスでのフロー制御のポーズ フレームのサポート	8.2(2)	フロー制御のポーズ（XOFF）フレームをイネーブルにできるようになりました。 この機能は、ASA 5585-X でもサポートされます。 **flowcontrol** コマンドが導入されました。
ギガビットイーサネットインターフェイスでのフロー制御のポーズフレームのサポート	8.2(5)/8.4(2)	すべてのモデルでギガビットインターフェイスのフロー制御のポーズ（XOFF）フレームをイネーブルにできるようになりました。 **flowcontrol** コマンドが変更されました。



第 12 章

EtherChannelインターフェイスと冗長インターフェイス

この章では、EtherChannel インターフェイスと冗長インターフェイスを設定する方法について説明します。

（注） マルチコンテキストモードでは、この項のすべてのタスクをシステム実行スペースで実行してください。コンテキストからシステム実行スペースに切り替えるには、**changeto system** コマンドを入力します。。

特殊な必須要件を保有する ASA クラスタ インターフェイスについては、ASA クラスタ （319 ページ） を参照してください。

（注） Firepower 9300 シャーシ、EtherChannel インターフェイスは FXOS オペレーティングシステムで設定されます。冗長インターフェイスはサポートされません。詳細については、お使いのシャーシの設定または導入ガイドを参照してください。

EtherChannel インターフェイスと冗長インターフェイスについて

この項では、EtherChannel インターフェイスと冗長インターフェイスについて説明します。

冗長インターフェイスについて

論理冗長インターフェイスは、物理インターフェイスのペア（アクティブ インターフェイスとスタンバイ インターフェイス）で構成されます。アクティブ インターフェイスで障害が発生すると、スタンバイ インターフェイスがアクティブになって、トラフィックを通過させ始めます。冗長インターフェイスを設定してASAの信頼性を高めることができます。この機能は、デバイスレベルのフェールオーバーとは別個のものですが、必要な場合はデバイスレベルのフェールオーバーとともに冗長インターフェイスも設定できます。

最大 8 個の冗長インターフェイス ペアを設定できます。

冗長インターフェイスの MAC アドレス

冗長インターフェイスでは、追加した最初の物理インターフェイスの MAC アドレスを使用します。コンフィギュレーションでメンバー インターフェイスの順序を変更すると、MAC アドレスは、リストの最初になったインターフェイスの MAC アドレスと一致するように変更されます。または、冗長インターフェイスに手動で MAC アドレスを割り当てることができます。これはメンバー インターフェイスの MAC アドレスに関係なく使用されます。アクティブ インターフェイスがスタンバイ インターフェイスにフェールオーバーすると、トラフィックが中断しないように同じ MAC アドレスが維持されます。

関連トピック

MTUおよび TCP MSS の設定 （560 ページ）
マルチ コンテキストの設定 （215 ページ）

EtherChannel について

802.3ad EtherChannel は、単一のネットワークの帯域幅を増やすことができるように、個別のイーサネット リンク（チャネル グループ）のバンドルで構成される論理インターフェイスです（ポートチャネル インターフェイスと呼びます）。ポートチャネル インターフェイスは、インターフェイス関連の機能を設定するときに、物理インターフェイスと同じように使用します。

モデルでサポートされているインターフェイスの数に応じて、最大 48 個の Etherchannel を設定できます。

チャネル グループのインターフェイス

各チャネル グループには、最大 16 個のアクティブ インターフェイスを設定できます。8 個のアクティブインターフェイスだけをサポートするスイッチの場合、1つのチャネル グループに最大 16 個のインターフェイスを割り当てることができます。インターフェイスは 8 個のみアクティブにできるため、残りのインターフェイスは、インターフェイスの障害が発生した場合のスタンバイ リンクとして動作できます。16個のアクティブインターフェイスの場合、スイッチがこの機能をサポートしている必要があります（たとえば、Cisco Nexus 7000 と F2 シリーズ 10 ギガビット イーサネット モジュール）。

チャネル グループのすべてのインターフェイスは、同じタイプと速度である必要があります。チャネル グループに追加された最初のインターフェイスによって、正しいタイプと速度が決まります。

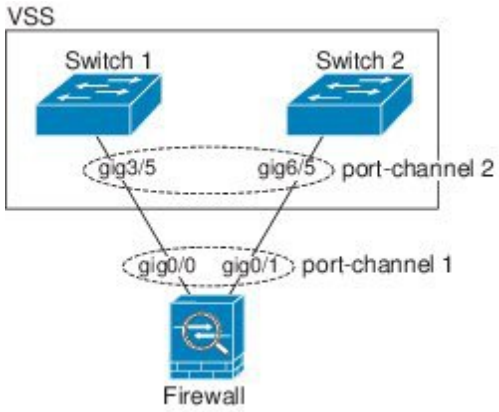
EtherChannel によって、チャネル内の使用可能なすべてのアクティブ インターフェイスのトラフィックが集約されます。インターフェイスは、送信元または宛先 MAC アドレス、IP アドレス、TCP および UDP ポート番号、および VLAN 番号に基づいて、独自のハッシュ アルゴリズムを使用して選択されます。

別のデバイスの EtherChannel への接続

ASA EtherChannel の接続先のデバイスも 802.3ad EtherChannel をサポートしている必要があります。たとえば、Catalyst 6500 スイッチまたは Cisco Nexus 7000 に接続できます。

スイッチが仮想スイッチング システム（VSS）または 仮想ポート チャネル（vPC）の一部である場合、同じ EtherChannel 内の ASA インターフェイスを VSS/vPC 内の個別のスイッチに接続できます。スイッチ インターフェイスは同じ EtherChannel ポートチャネル インターフェイスのメンバです。複数の個別のスイッチが単一のスイッチのように動作するからです。

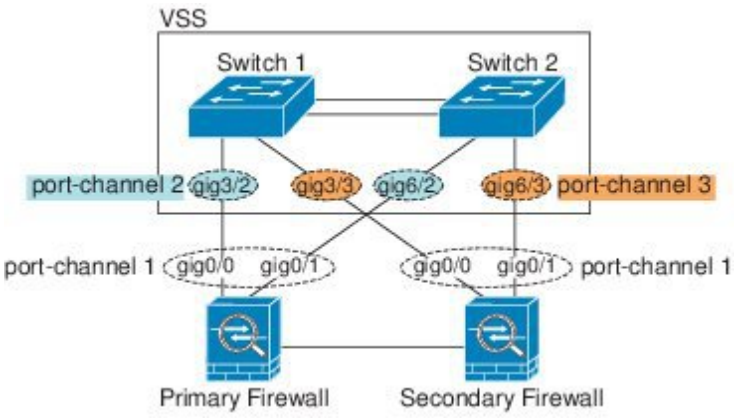
図 *49 : VSS/vPC* への接続



ASA をアクティブ/スタンバイ フェールオーバー配置で使用する場合、ASA ごとに 1 つ、VSS/vPC 内のスイッチで個別の EtherChannel を作成する必要があります。各 ASA で、1 つの EtherChannel が両方のスイッチに接続します。すべてのスイッチインターフェイスを両方の ASA に接続する単一の EtherChannel にグループ化できる場合でも（この場合、個別の ASA シ

ステム ID のため、EtherChannel は確立されません）、単一の EtherChannel は望ましくありません。これは、トラフィックをスタンバイ ASA に送信しないようにするためです。

図 *50 : アクティブ/スタンバイ フェールオーバーと VSS/vPC*



リンク集約制御プロトコル

リンク集約制御プロトコル（LACP）では、2 つのネットワーク デバイス間でリンク集約制御プロトコル データ ユニット（LACPDU）を交換することによって、インターフェイスが集約されます。

EtherChannel 内の各物理インターフェイスを次のように設定できます。

- アクティブ：LACP アップデートを送信および受信します。アクティブ EtherChannel は、アクティブまたはパッシブ EtherChannel と接続を確立できます。LACP トラフィックを最小にする必要がある場合以外は、アクティブ モードを使用する必要があります。
- パッシブ：LACP アップデートを受信します。パッシブ EtherChannel は、アクティブ EtherChannel のみと接続を確立できます。Firepower ハードウェア モデルではサポートされていません。
- オン：EtherChannel は常にオンであり、LACP は使用されません。「オン」の EtherChannel は、別の「オン」の EtherChannel のみと接続を確立できます。Firepower ハードウェア モデルではサポートされていません。

LACP では、ユーザが介入しなくても、EtherChannel へのリンクの自動追加および削除が調整されます。また、コンフィギュレーションの誤りが処理され、メンバインターフェイスの両端が正しいチャネル グループに接続されていることがチェックされます。「オン」モードではインターフェイスがダウンしたときにチャネル グループ内のスタンバイ インターフェイスを使用できず、接続とコンフィギュレーションはチェックされません。

ロード バランシング

ASA は、パケットの送信元および宛先 IP アドレスをハッシュすることによって、パケットを EtherChannel 内のインターフェイスに分散します（この基準は設定可能です）。生成されたハッシュ値をアクティブなリンクの数で割り、そのモジュロ演算で求められた余りの値によってフ

ローの割り当て先のインターフェイスが決まります。*hash_value* **mod** *active_links* の結果が 0 となるパケットはすべて、EtherChannel 内の最初のインターフェイスに送信されます。以降は同様に、結果が 1 となるものは 2 番目のインターフェイスに、結果が 2 となるものは 3 番目のインターフェイスに送信されます。たとえば、15 個のアクティブ リンクがある場合、モジュロ演算では 0 ～ 14 の値が得られます。6 個のアクティブ リンクの場合、値は 0 ～ 5 となり、以降も同様になります。

クラスタリングのスパンド EtherChannel では、ロードバランシングは ASA ごとに行われます。たとえば、8 台の ASA にわたるスパンド EtherChannel 内に 32 個のアクティブインターフェイスがあり、EtherChannel 内の 1 台の ASA あたり 4 個のインターフェイスがある場合、ロードバランシングは 1 台の ASA の 4 個のインターフェイス間でのみ行われます。

アクティブ インターフェイスがダウンし、スタンバイ インターフェイスに置き換えられない場合、トラフィックは残りのリンク間で再バランスされます。失敗はレイヤ 2 のスパニングツリーとレイヤ 3 のルーティング テーブルの両方からマスクされるため、他のネットワーク デバイスへのスイッチオーバーはトランスペアレントです。

関連トピック

EtherChannelのカスタマイズ （492 ページ）

EtherChannel MAC アドレス

1 つのチャネル グループに含まれるすべてのインターフェイスは、同じ MAC アドレスを共有します。この機能によって、EtherChannel はネットワーク アプリケーションとユーザに対してトランスペアレントになります。ネットワーク アプリケーションやユーザから見えるのは 1 つの論理接続のみであり、個々のリンクのことは認識しないからです。

ポート チャネル インターフェイスは、最も小さいチャネル グループ インターフェイスの MAC アドレスをポート チャネル MAC アドレスとして使用します。または、ポート チャネル インターフェイスの MAC アドレスを手動で設定することもできます。マルチコンテキスト モードでは、EtherChannel ポート インターフェイスを含め、一意の MAC アドレスを共有インターフェイスに自動的に割り当てることができます。グループ チャネル インターフェイスのメンバーシップを変更する場合は、固有の MAC アドレスを,手動で設定するか、または共有インターフェイスのマルチ コンテキスト モードでは自動的に設定することを推奨します。ポート チャネル MAC アドレスを提供していたインターフェイスを削除すると、そのポート チャネルの MAC アドレスは次に番号が小さいインターフェイスに変わるため、トラフィックが分断されます。

EtherChannel インターフェイスと冗長インターフェイスのガイドライン

フェールオーバー

- 冗長インターフェイスまたは EtherChannel インターフェイスを フェールオーバー リンクとして使用する場合、フェールオーバー ペアの両方のユニットでその事前設定を行う必要

があります。プライマリユニットで設定し、セカンダリ装置に複製されることは想定できません。これは、複製には フェールオーバー リンク自体が必要であるためです。

- 冗長インターフェイスまたはEtherChannelインターフェイスをステートリンクに対して使用する場合、特別なコンフィギュレーションは必要ありません。コンフィギュレーションは通常どおりプライマリ装置から複製されます。Firepower 9300 シャーシでは、Etherchannelを含むすべてのインターフェイスを両方のユニットで事前に設定する必要があります。
- **monitor-interface** コマンドを使用して、フェールオーバーの冗長インターフェイスまたはEtherChannelインターフェイスを監視できます。 この場合、論理冗長インターフェイス名を必ず参照してください。When an active member interface fails over to a standby interface, this activity does not cause the redundant or EtherChannel interface to appear to be failed when being monitored for device-level フェールオーバー. すべての物理インターフェイスで障害が発生した場合にのみ、冗長インターフェイスまたはEtherChannelインターフェイスで障害が発生しているように見えます（EtherChannel インターフェイスでは、障害の発生が許容されるメンバ インターフェイスの数を設定できます）。
- If you use an EtherChannel interface for a フェールオーバー or state link, then to prevent out-of-order packets, only one interface in the EtherChannel is used. そのインターフェイスで障害が発生した場合は、EtherChannel内の次のリンクが使用されます。フェールオーバー リンクとして使用中のEtherChannelの設定は変更できません。設定を変更するには、フェールオーバーを一時的に無効にする必要があります。これにより、フェールオーバーがその期間に発生することはありません。

サポート モデル

- 、Firepower 4100/9300、ASAv、または ASASM の場合、ASA に EtherChannel を追加することはできません。Firepower 4100/9300 は Etherchannel をサポートしていますが、シャーシ上の FXOS で Etherchannel のすべてのハードウェア設定を実行する必要があります。
- Firepower 9300 シャーシおよび ASASM では、冗長インターフェイスはサポートされていません。

クラスタ

- 冗長インターフェイスまたはEtherChannelインターフェイスをクラスタ制御リンクとして使用するときは、クラスタのすべての装置でそのリンクを事前に設定する必要があります。プライマリ装置で設定し、その設定がメンバー装置に複製されると期待することはできません。これは、クラスタ制御リンク自体が複製に必要であるためです。
- スパンドEtherChannelまたは個別クラスタインターフェイスを設定するには、クラスタリングの章を参照してください。

冗長インターフェイスの一般的なガイドライン

- 最大 8 個の冗長インターフェイス ペアを設定できます。

- すべてのASA コンフィギュレーションは、メンバ物理インターフェイスではなく論理冗長インターフェイスを参照します。
- EtherChannel の一部として冗長インターフェイスを使用することはできません。また、冗長インターフェイスの一部として EtherChannel を使用することはできません。冗長インターフェイスと EtherChannel インターフェイスでは同じ物理インターフェイスを使用できません。ただし、同じ物理インターフェイスを使用するのでなければ、両方のタイプを ASA 上で設定することができます。
- アクティブ インターフェイスをシャットダウンすると、スタンバイ インターフェイスがアクティブになります。
- 冗長インターフェイスは、管理 *slot*/*port*インターフェイスをメンバーとしてサポートしません。ただし、管理インターフェイス以外の複数インターフェイスからなる冗長インターフェイスを、管理専用として設定できます。

EtherChannel の一般的なガイドライン

- モデルで使用可能なインターフェイスの数に応じて、最大48 個の Etherchannel を設定できます。
- 各チャネル グループには、最大 16 個のアクティブ インターフェイスを設定できます。8 個のアクティブインターフェイスだけをサポートするスイッチの場合、1 つのチャネル グループに最大 16 個のインターフェイスを割り当てることができます。インターフェイスは 8 個のみアクティブにできるため、残りのインターフェイスは、インターフェイスの障害が発生した場合のスタンバイ リンクとして動作できます。16 個のアクティブインターフェイスの場合、スイッチがこの機能をサポートしている必要があります（たとえば、Cisco Nexus 7000 と F2 シリーズ 10 ギガビット イーサネット モジュール）。
- チャネル グループのすべてのインターフェイスは、同じタイプと速度である必要があります。チャネル グループに追加された最初のインターフェイスによって、正しいタイプと速度が決まります。
- ASA の EtherChannel の接続先デバイスも 802.3ad EtherChannel をサポートしている必要があります。
- ASA は、VLAN タグ付きの LACPDU をサポートしていません。Cisco IOS **vlan dot1Q tag native** コマンドを使用して、隣接スイッチのネイティブ VLAN タギングをイネーブルにすると ASA はタグ付きの LACPDU をドロップします。隣接スイッチのネイティブ VLAN タギングは、必ずディセーブルにしてください。マルチ コンテキスト モードでは、これらのメッセージはパケット キャプチャに含まれていないため、問題を効率的に診断できません。
- 15.1(1)S2 以前の Cisco IOS ソフトウェアバージョンを実行する ASA では、スイッチスタックへの EtherChannel の接続がサポートされていませんでした。デフォルトのスイッチ設定では、ASA EtherChannel がクロススタックに接続されている場合、マスタースイッチの電源がオフになると、残りのスイッチに接続されている EtherChannel は起動しません。互換性を高めるため、**stack-mac persistent timer** コマンドを設定して、十分なリロード時間を

確保できる大きな値、たとえば 8 分、0 （無制限）などを設定します。または、15.1(1)S2 など、より安定したスイッチ ソフトウェア バージョンにアップグレードできます。

- すべての ASA コンフィギュレーションは、メンバ物理インターフェイスではなく論理 EtherChannel インターフェイスを参照します。
- EtherChannel の一部として冗長インターフェイスを使用することはできません。また、冗長インターフェイスの一部として EtherChannel を使用することはできません。冗長インターフェイスと EtherChannel インターフェイスでは同じ物理インターフェイスを使用できません。ただし、同じ物理インターフェイスを使用するのでなければ、両方のタイプを ASA 上で設定することができます。

EtherChannel インターフェイスと冗長インターフェイのデフォルト設定

この項では、工場出荷時のデフォルト コンフィギュレーションが設定されていない場合のインターフェイスのデフォルト設定を示します。

インターフェイスのデフォルトの状態

インターフェイスのデフォルトの状態は、そのタイプおよびコンテキスト モードによって異なります。

マルチ コンテキスト モードでは、システム実行スペース内でのインターフェイスの状態にかかわらず、すべての割り当て済みのインターフェイスがデフォルトでイネーブルになっています。ただし、トラフィックがインターフェイスを通過するためには、そのインターフェイスもシステム実行スペース内でイネーブルになっている必要があります。インターフェイスをシステム実行スペースでシャットダウンすると、そのインターフェイスは、それを共有しているすべてのコンテキストでダウンします。

シングル モードまたはシステム実行スペースでは、インターフェイスのデフォルトの状態は次のとおりです。

- 物理インターフェイス：ディセーブル。
- 冗長インターフェイス：イネーブル。ただし、トラフィックが冗長インターフェイスを通過するためには、メンバ物理インターフェイスもイネーブルになっている必要があります。
- EtherChannel ポートチャネル インターフェイス：イネーブル。ただし、トラフィックが EtherChannel を通過するためには、チャネル グループ物理インターフェイスもイネーブルになっている必要があります。

冗長インターフェイスの設定

論理冗長インターフェイスは、物理インターフェイスのペア（アクティブインターフェイスとスタンバイ インターフェイス）で構成されます。アクティブ インターフェイスで障害が発生すると、スタンバイインターフェイスがアクティブになって、トラフィックを通過させ始めます。冗長インターフェイスを設定して ASA の信頼性を高めることができます。この機能は、デバイスレベルのフェールオーバーとは別個のものですが、必要な場合はフェールオーバーとともに冗長インターフェイスも設定できます。

この項では、冗長インターフェイスを設定する方法について説明します。

冗長インターフェイスの設定

この項では、冗長インターフェイスを作成する方法について説明します。デフォルトでは、冗長インターフェイスはイネーブルになっています。

始める前に

- 最大 8 個の冗長インターフェイス ペアを設定できます。
- 冗長インターフェイス遅延値は設定可能ですが、デフォルトでは、ASA はそのメンバー インターフェイスの物理タイプに基づくデフォルトの遅延値を継承します。
- 両方のメンバインターフェイスが同じ物理タイプである必要があります。たとえば、両方ともギガビット イーサネットにする必要があります。
- 名前が設定されている場合は、物理インターフェイスを冗長インターフェイスに追加できません。最初に、**no nameif** コマンドを使用して名前を削除する必要があります。
- マルチ コンテキスト モードでは、システム実行スペースで次の手順を実行します。コンテキストからシステム実行スペースに切り替えるには、**changeto system** コマンドを入力します。。

⚠

注意 コンフィギュレーション内で物理インターフェイスをすでに使用している場合、名前を削除すると、このインターフェイスを参照しているすべてのコンフィギュレーションが消去されます。

手順

ステップ 1 論理冗長インターフェイスを追加します。

interface redundant *number*

例：

```
ciscoasa(config)# interface redundant 1
```

number 引数は、1 ～ 8 の整数です。

冗長インターフェイスの名前などの論理パラメータを設定する前に、少なくとも 1 つのメンバー インターフェイスを冗長インターフェイスに追加する必要があります。

ステップ 2 最初のメンバー インターフェイスを冗長インターフェイスに追加します。

member-interface *physical_interface*

例：

```
ciscoasa(config-if)# member-interface gigabitethernet 0/0
```

冗長インターフェイスは、Management *slot*/*port* インターフェイスをメンバとしてサポートしません。

インターフェイスを追加すると、インターフェイスのコンフィギュレーション（IP アドレスなど）はすべて削除されます。

ステップ 3 2 番目のメンバー インターフェイスを冗長インターフェイスに追加します。

member-interface *physical_interface*

例：

```
ciscoasa(config-if)# member-interface gigabitethernet 0/1
```

2 つ目のインターフェイスの物理タイプは、必ず最初のインターフェイスと同じにしてください。

メンバー インターフェイスを削除するには、**no member-interface** *physical_interface* コマンドを入力します。冗長インターフェイスから両方のメンバインターフェイスは削除できません。冗長インターフェイスには、少なくとも 1 つのメンバ インターフェイスが必要です。

例

次の例では、2 つの冗長インターフェイスを作成します。

```
ciscoasa(config)# interface redundant 1
ciscoasa(config-if)# member-interface gigabitethernet 0/0
ciscoasa(config-if)# member-interface gigabitethernet 0/1
ciscoasa(config-if)# interface redundant 2
ciscoasa(config-if)# member-interface gigabitethernet 0/2
ciscoasa(config-if)# member-interface gigabitethernet 0/3
```

アクティブ インターフェイスの変更

デフォルトでは、コンフィギュレーションで最初にリストされているインターフェイスが（使用可能であれば）、アクティブ インターフェイスになります。

手順

ステップ 1 どのインターフェイスがアクティブかを表示するには、で次のコマンドを入力します。

show interface redundant *number* **detail** | **grep Member**

例：

```
ciscoasa# show interface redundant1 detail | grep Member
      Members GigabitEthernet0/3(Active), GigabitEthernet0/2
```

ステップ 2 アクティブ インターフェイスを変更します。

redundant-interface redundant *number* **active-member** *physical_interface*

redundant*number* 引数には、冗長インターフェイス ID（**redundant1** など）を指定します。

physical_interface には、アクティブにするメンバ インターフェイスの ID を指定します。

EtherChannel の設定

ここでは、EtherChannel ポートチャネル インターフェイスの作成、インターフェイスの EtherChannel への割り当て、EtherChannel のカスタマイズ方法について説明します。

EtherChannel へのインターフェイスの追加

ここでは、EtherChannel ポートチャネル インターフェイスを作成し、インターフェイスを EtherChannel に割り当てる方法について説明します。デフォルトでは、ポートチャネル インターフェイスはイネーブルになっています。

始める前に

- 使用しているモデルに設定されているインターフェイスの数に応じて、最大 48 個の EtherChannel を設定できます。
- 各チャネル グループには、最大 16 個のアクティブ インターフェイスをサポートしています。8 個のアクティブ インターフェイスだけをサポートするスイッチの場合、1 つのチャネル グループに最大16個のインターフェイスを割り当てることができます。インターフェイスは8個のみアクティブにできるため、残りのインターフェイスは、インターフェイスの障害が発生した場合のスタンバイ リンクとして動作できます。

- クラスタリング用にスパンド EtherChannel を設定するには、この手順の代わりにクラスタリングの章を参照してください。
- チャネル グループのすべてのインターフェイスは、同じタイプ、速度、および二重通信である必要があります。半二重はサポートされません。RJ-45 または SFP コネクタを使用するように設定できるインターフェイスの場合、同一の EtherChannel に RJ-45 インターフェイスと SFP インターフェイスの両方を含めることができることに注意してください。
- 名前が設定されている場合は、物理インターフェイスをチャネル グループに追加できません。最初に、**no nameif** コマンドを使用して、名前を削除する必要があります。
- マルチ コンテキスト モードでは、システム実行スペースで次の手順を実行します。コンテキストからシステム実行スペースに切り替えるには、**changeto system** コマンドを入力します。

注意 コンフィギュレーション内で物理インターフェイスをすでに使用している場合、名前を削除すると、このインターフェイスを参照しているすべてのコンフィギュレーションが消去されます。

手順

ステップ 1 チャネル グループに追加するインターフェイスを指定します。

interface *physical_interface*

例：

```
ciscoasa(config)# interface gigabitethernet 0/0
```

physical_interface ID には、タイプ、スロット、およびポート番号（type[slot/]port）が含まれます。チャネル グループのこの最初のインターフェイスによって、グループ内の他のすべてのインターフェイスのタイプと速度が決まります。

トランスペアレント モードで、複数の管理インターフェイスがあるチャネル グループを作成する場合は、この EtherChannel を管理専用インターフェイスとして使用できます。

ステップ 2 この物理インターフェイスを EtherChannel に割り当てます。

channel-group *channel_id* **mode** {**active** | **passive** | **on**}

例：

```
ciscoasa(config-if)# channel-group 1 mode active
```

channel_id は 1 ～ 48 の間の整数です。このチャネル ID のポートチャネル インターフェイスがコンフィギュレーションにまだ存在しない場合、ポートチャネルインターフェイスが作成されます。

interface port-channel *channel_id*

active モードを使用することを推奨します。

ステップ 3 （オプション）チャネルグループの物理インターフェイスのプライオリティを設定します。

lacp port-priority *number*

例：

```
ciscoasa(config-if)# lacp port-priority 12345
```

プライオリティの *number* は、1 ～ 65535 の整数です。デフォルトは 32768 です。数字が大きいほど、プライオリティは低くなります。使用可能な数よりも多くのインターフェイスを割り当てた場合、ASA ではこの設定を使用して、アクティブ インターフェイスとスタンバイ インターフェイスを決定します。ポートプライオリティ設定がすべてのインターフェイスで同じ場合、プライオリティはインターフェイス ID（スロット/ポート）で決まります。最も小さいインターフェイス ID が、最も高いプライオリティになります。たとえば、GigabitEthernet 0/0 のプライオリティは GigabitEthernet 0/1 よりも高くなります。

あるインターフェイスについて、インターフェイス ID は大きいが、そのインターフェイスがアクティブになるように優先順位を付ける場合は、より小さい値を持つようにこのコマンドを設定します。たとえば、GigabitEthernet 1/3 を GigabitEthernet 0/7 よりも前にアクティブにするには、**lacp port-priority** の値を、1/3 インターフェイスでは 12345 とし、0/7 インターフェイスではデフォルトの 32768 とします。

EtherChannel の反対の端にあるデバイスのポート プライオリティが衝突している場合、システム プライオリティを使用して使用するポート プライオリティが決定されます。**lacp system-priority** コマンドを参照してください。

ステップ 4 （オプション）ポートチャネル インターフェイスのイーサネット プロパティを設定します。この設定は、個別インターフェイスに対して設定されたプロパティよりも優先されます。

interface port-channel *channel_id*

イーサネットのコマンドについては、物理インターフェイスのイネーブル化およびイーサネット パラメータの設定 （471 ページ）を参照してください。これらのパラメータはチャネル グループのすべてのインターフェイスで一致している必要があるため、この方法はこれらのパラメータを設定するショートカットになります。

ステップ 5 チャネル グループに追加するインターフェイスごとに、ステップ 1 ～ 3 を繰り返します。

チャネル グループの各インターフェイスのタイプと速度が同一であることが必要です。半二重はサポートされません。一致しないインターフェイスを追加すると、一時停止状態になります。

関連トピック

リンク集約制御プロトコル （482 ページ）
EtherChannelのカスタマイズ （492 ページ）

EtherChannelのカスタマイズ

この項では、EtherChannel のインターフェイスの最大数、EtherChannel をアクティブにするための動作インターフェイスの最小数、ロード バランシング アルゴリズム、およびその他のオプション パラメータを設定する方法について説明します。

手順

ステップ 1 ポートチャネル インターフェイスを指定します。

interface port-channel *channel_id*

例：

```
ciscoasa(config)# interface port-channel 1
```

このインターフェイスは、チャネル グループにインターフェイスを追加したときに自動的に作成されたものです。まだインターフェイスを追加していない場合は、このコマンドを実行するとポートチャネル インターフェイスが作成されます。

少なくとも 1 つのメンバー インターフェイスをポートチャネル インターフェイスに追加してからでなければ、インターフェイスの論理パラメータ（名前など）は設定できません。

ステップ 2 チャネル グループで許可されるアクティブ インターフェイスの最大数を指定します。

lacp max-bundle *number*

例：

```
ciscoasa(config-if)# lacp max-bundle 6
```

number には、1 ～ 16 の範囲内の値を入力します。デフォルトは 16 です。スイッチが 16 個のアクティブインターフェイスをサポートしていない場合、このコマンドは必ず8以下に設定する必要があります。

ステップ 3 ポートチャネルインターフェイスがアクティブになるために必要な、アクティブインターフェイスの最小数を指定します。

port-channel min-bundle *number*

例：

```
ciscoasa(config-if)# port-channel min-bundle 2
```

number には、1 ～ 16 の範囲内の値を入力します。デフォルトは 1 です。チャネル グループ内のアクティブ インターフェイス数がこの値よりも小さい場合、ポートチャネル インターフェイスがダウンし、デバイスレベル フェールオーバーが開始されます。

ステップ 4 ロード バランシング アルゴリズムを設定します。

port-channel load-balance {**dst-ip** | **dst-ip-port** | **dst-mac** | **dst-port** | **src-dst-ip** | **src-dst-ip-port** | **src-dst-mac** | **src-dst-port** | **src-ip** | **src-ip-port** | **src-mac** | **src-port** | **vlan-dst-ip** | **vlan-dst-ip-port** | **vlan-only** | **vlan-src-dst-ip** | **vlan-src-dst-ip-port** | **vlan-src-ip** | **vlan-src-ip-port**}

例：

```
ciscoasa(config-if)# port-channel load-balance src-dst-mac
```

デフォルトでは、ASA はパケットの送信元および宛先 IP アドレス（**src-dst-ip**）に従ってインターフェイスでのパケットの負荷を分散します。パケットの分類の基準となるプロパティを変更する場合は、このコマンドを使用します。たとえば、トラフィックが同じ送信元および宛先 IP アドレスに大きく偏っている場合、EtherChannel 内のインターフェイスに対するトラフィックの割り当てがアンバランスになります。別のアルゴリズムに変更すると、トラフィックはより均等に分散される場合があります。

ステップ 5 LACP システム プライオリティを設定します。

lacp system-priority *number*

例：

```
ciscoasa(config)# lacp system-priority 12345
```

number には、1 ～ 65535 の範囲内の値を入力します。デフォルトは 32768 です。数字が大きいほど、プライオリティは低くなります。このコマンドは、ASA に対してグローバルです。

EtherChannel の反対の端にあるデバイスのポート プライオリティが衝突している場合、システム プライオリティを使用して使用するポート プライオリティが決定されます。EtherChannel 内でのインターフェイス プライオリティについては、**lacp port-priority** コマンドを参照してください。

関連トピック

ロード バランシング （482 ページ）
EtherChannel へのインターフェイスの追加 （489 ページ）

EtherChannel および冗長インターフェイスのモニタリング

次のコマンドを参照してください。

- **show interface**

  インターフェイス統計情報を表示します。

- **show interface ip brief**

  インターフェイスの IP アドレスとステータスを表示します。

- **show lacp**{[*channel_group_number*] {**counters** | **internal** | **neighbor**} | **sys-id**}

  EtherChannel の場合は、LACP 情報（トラフィック統計情報、システム ID、ネイバーの詳細など）が表示されます。

- **show port-channel** [*channel_group_number*] [**brief** | **detail** | **port** | **protocol** | **summary**]

  EtherChannel の場合は、EtherChannel 情報が、詳細な 1 行サマリー形式で表示されます。このコマンドは、ポートとポートチャネルの情報も表示します。

- **show port-channel** *channel_group_number* **load-balance** [**hash-result** {**ip** | **ipv6** | **l4port** | **mac** | **mixed** | **vlan-only**} *parameters*]

  EtherChannel の場合は、ポートチャネル負荷分散情報が、指定のパラメータ セットに対するハッシュ結果および選択されたメンバー インターフェイスとともに表示されます。

EtherChannel インターフェイスと冗長インターフェイスの例

次の例では、3 つのインターフェイスを EtherChannel の一部として設定します。また、システム プライオリティをより高く設定するとともに、GigabitEthernet 0/2 のプライオリティを他のインターフェイスよりも高く設定します。これは、8 個を超えるインターフェイスが EtherChannel に割り当てられた場合に備えるためです。

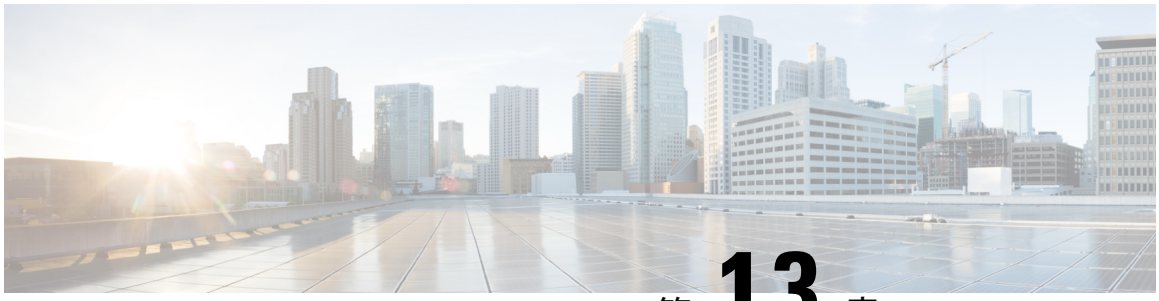
```
lacp system-priority 1234
interface GigabitEthernet0/0
  channel-group 1 mode active
interface GigabitEthernet0/1
  channel-group 1 mode active
interface GigabitEthernet0/2
  lacp port-priority 1234
  channel-group 1 mode passive
interface Port-channel1
  lacp max-bundle 4
  port-channel min-bundle 2
  port-channel load-balance dst-ip
```

EtherChannel インターフェイスと冗長インターフェイスの履歴

表 *17 : EtherChannel* インターフェイスと冗長インターフェイスの履歴

機能名	リリース	機能情報
冗長インターフェイス	8.0(2)	論理冗長インターフェイスは、アクティブとスタンバイの物理インターフェイスからなるペアです。アクティブインターフェイスで障害が発生すると、スタンバイインターフェイスがアクティブになって、トラフィックを通過させ始めます。冗長インターフェイスを設定して ASA の信頼性を高めることができます。この機能は、デバイスレベルのフェールオーバーとは別個のものですが、必要な場合はフェールオーバーとともに冗長インターフェイスも設定できます。最大 8 個の冗長インターフェイスペアを設定できます。
EtherChannel サポート	8.4(1)	最大 48 個の 802.3ad EtherChannel（1 つあたりのアクティブインターフェイス 8 個）を設定できます。 **channel-group**、**lacp port-priority**、**interface port-channel**、**lacp max-bundle**、**port-channel min-bundle**、**port-channel load-balance**、**lacp system-priority**、**clear lacp counters**、**show lacp**、**show port-channel** の各コマンドが導入されました。 （注） EtherChannel は ASA 5505 ではサポートされません。

機能名	リリース	機能情報
EtherChannel あたり 16 個のアクティブ リンクのサポート	9.2(1)	EtherChannel あたり最大で 16 個のアクティブ リンクを設定できるようになりました。これまでは、8 個のアクティブ リンクと 8 個のスタンバイ リンクが設定できました。スイッチは、16 個のアクティブ リンクをサポート可能である必要があります（たとえば、Cisco Nexus 7000 と F2 シリーズ 10 ギガビット イーサネット モジュール）。 （注） 旧バージョンの ASA からアップグレードする場合、互換性を得るために、アクティブなインターフェイスの最大数を 8 に設定します（**lacp max-bundle** コマンド）。 次のコマンドが変更されました。**lacp max-bundle** および **port-channel min-bundle**。



第 13 章

VLAN サブインターフェイス

この章では、VLAN サブインターフェイスを設定する方法について説明します。

（注） マルチコンテキストモードでは、この項のすべてのタスクをシステム実行スペースで実行してください。コンテキストからシステム実行スペースに切り替えるには、**changeto system** コマンドを入力します。。

VLAN サブインターフェイスについて

VLAN サブインターフェイスを使用すると、1 つの物理インターフェイス、冗長インターフェイス、または EtherChannel インターフェイスを、異なる VLAN ID でタグ付けされた複数の論理インターフェイスに分割できます。VLAN サブインターフェイスが 1 つ以上あるインターフェイスは、自動的に 802.1Q トランクとして設定されます。VLAN では、所定の物理インターフェイス上でトラフィックを分離しておくことができるため、物理インターフェイスまたは ASA を追加しなくても、ネットワーク上で使用できるインターフェイスの数を増やすことができます。この機能は、各コンテキストに固有のインターフェイスを割り当てることができるので、マルチ コンテキスト モードで特に便利です。

VLAN サブインターフェイスのライセンス

モデル	ライセンス要件
Firepower 9300	標準ライセンス：1024
ASAv5	標準ライセンス：25
ASAv10	標準ライセンス：50
ASAv30	標準ライセンス：200
ASA 5506-X ASA 5506W-X ASA 5506H-X	基本ライセンス：5 Security Plus ライセンス：30
ASA 5508-X	基本ライセンス：50
ASA 5512-X	基本ライセンス：50 Security Plus ライセンス：100
ASA 5515-X	基本ライセンス：100
ASA 5516-X	基本ライセンス：50
ASA 5525-X	基本ライセンス：200
ASA 5545-X	基本ライセンス：300
ASA 5555-X	基本ライセンス：500
ASA 5585-X	基本ライセンスと Security Plus ライセンス：1024
ASASM	サポートしない
ISA 3000	基本ライセンス：5 Security Plus ライセンス：25

（注） VLAN 制限の対象としてカウントするインターフェイスに、VLAN を割り当てます。 たとえば、次のようになります。

```
interface gigabitethernet 0/0.100
  vlan 100
```

VLAN サブインターフェイスのガイドラインと制限事項

モデルのサポート

- ASASM：VLAN サブインターフェイスは、ASASM ではサポートされません。ASASM のインターフェイスは、すでにスイッチから割り当てられた VLAN インターフェイスです。

その他のガイドライン

- 物理インターフェイス上のタグなしパケットの禁止：サブインターフェイスを使用する場合、物理インターフェイスでトラフィックを通過させないようにすることもよくあります。物理インターフェイスはタグのないパケットを通過させることができるためです。この特性は、冗長インターフェイスペアのアクティブな物理インターフェイスと EtherChannel リンクにも当てはまります。トラフィックがサブインターフェイスを通過するには、物理インターフェイス、冗長インターフェイス、または EtherChannel インターフェイスがイネーブルになっている必要があるため、トラフィックが物理インターフェイス、冗長インターフェイス、または EtherChannel インターフェイスを通過しないように、**nameif** コマンドを除外してください。物理インターフェイス、冗長インターフェイス、または EtherChannel インターフェイスでタグのないパケットを通過させる場合は、通常通り **nameif** コマンドを設定できます。
- 多くのモデルでは、管理インターフェイスのサブインターフェイスを設定できません。サブインターフェイスのサポートについては、管理スロット/ポートインターフェイス（466 ページ）を参照してください。
- ASA は Dynamic Trunking Protocol（DTP）をサポートしていないため、接続されているスイッチポートを無条件にトランキングするように設定する必要があります。
- 親インターフェイスの同じ Burned-In MAC Address を使用するので、ASA で定義されたサブインターフェイスに一意の MAC アドレスを割り当てることもできます。たとえば、サービス プロバイダーによっては、MAC アドレスに基づいてアクセス コントロールを実行する場合があります。また、IPv6 リンクローカル アドレスは MAC アドレスに基づいて生成されるため、サブインターフェイスに一意の MAC アドレスを割り当てることで、一意の IPv6 リンクローカル アドレスが可能になり、ASA で特定のインスタンスでのトラフィックの中断を避けることができます。

VLAN サブインターフェイスのデフォルト設定

この項では、工場出荷時のデフォルト コンフィギュレーションが設定されていない場合のインターフェイスのデフォルト設定を示します。

インターフェイスのデフォルトの状態

インターフェイスのデフォルトの状態は、そのタイプおよびコンテキストモードによって異なります。

マルチ コンテキスト モードでは、システム実行スペース内でのインターフェイスの状態にかかわらず、すべての割り当て済みのインターフェイスがデフォルトでイネーブルになっています。ただし、トラフィックがインターフェイスを通過するためには、そのインターフェイスもシステム実行スペース内でイネーブルになっている必要があります。インターフェイスをシステム実行スペースでシャットダウンすると、そのインターフェイスは、それを共有しているすべてのコンテキストでダウンします。

シングルモードまたはシステム実行スペースでは、インターフェイスのデフォルトの状態は次のとおりです。

- 物理インターフェイス：ディセーブル。
- VLANサブインターフェイス：イネーブル。ただし、トラフィックがサブインターフェイスを通過するためには、物理インターフェイスもイネーブルになっている必要があります。

VLAN サブインターフェイスと 802.1Q トランキングの設定

VLAN サブインターフェイスを物理インターフェイス、冗長インターフェイス、または EtherChannel インターフェイスに追加します。

始める前に

マルチ コンテキスト モードでは、システム実行スペースで次の手順を実行します。コンテキストからシステム実行スペースに切り替えるには、**changeto system** コマンドを入力します。

手順

ステップ 1 新しいサブインターフェイスを指定します。

interface {*physical_interface* | **redundant** *number* | **port-channel** *number*}.*subinterface*

例：

```
ciscoasa(config)# interface gigabitethernet 0/1.100
```

redundant *number* 引数には、冗長インターフェイス ID（**redundant 1** など）を指定します。

port-channel *number* 引数は、**port-channel 1** などの EtherChannel インターフェイス ID です。

subinterface ID は、1 ～ 4294967293 の整数です。

ステップ 2 サブインターフェイスの VLAN を指定します。

vlan *vlan_id*

例：

```
ciscoasa(config-subif)# vlan 101
```

vlan_id は、1 ～ 4094 の整数です。VLAN ID には、接続されているスイッチで予約されているものがあります。詳細については、スイッチのマニュアルを参照してください。

単一の VLAN のみをサブインターフェイスに割り当てることはできません。同じ VLAN を複数のサブインターフェイスに関連付けることはできません。VLAN を物理インターフェイスに割り当てることはできません。トラフィックがサブインターフェイスを通過するには、各サブインターフェイスに VLAN ID が必要となります。VLAN ID を変更するために **no** オプションで古い VLAN ID を削除する必要はありません。別の VLAN ID を指定して **vlan** コマンドを入力すると、ASA によって古い ID が変更されます。

関連トピック

VLAN サブインターフェイスのライセンス （498 ページ）

VLAN サブインターフェイスのモニタリング

次のコマンドを参照してください。

- **show interface**

  インターフェイス統計情報を表示します。

- **show interface ip brief**

  インターフェイスの IP アドレスとステータスを表示します。

VLAN のサブインターフェイスの例

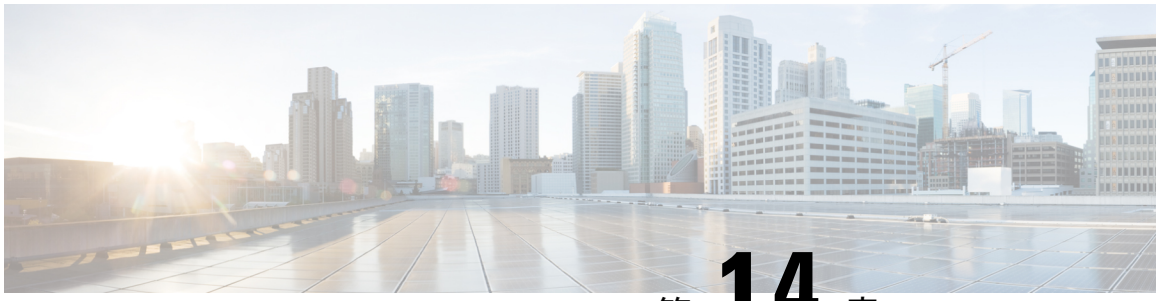
次に、シングル モードでサブインターフェイスのパラメータを設定する例を示します。

```
interface gigabitethernet 0/1
  no nameif
  no security-level
  no ip address
  no shutdown
interface gigabitethernet 0/1.1
  vlan 101
  nameif inside
  security-level 100
  ip address 192.168.6.6 255.255.255.0
  no shutdown
```

VLAN サブインターフェイスの履歴

表 *18 : VLAN* サブインターフェイスの履歴

機能名	バージョン	機能情報
VLAN 数の増加	7.0(5)	次の制限値が増加されました。 • ASA 5510 基本ライセンスの VLAN 数が 0 から 10 に増えました。 • ASA 5510 Security Plus ライセンスの VLAN 数が 10 から 25 に増えました。 • ASA 5520 の VLAN 数が 25 から 100 に増えました。 • ASA 5540 の VLAN 数が 100 から 200 に増えました。
VLAN 数の増加	7.2(2)	VLAN の制限値が変更されました。ASA 5510 の基本ライセンスでは 10 から 50 に、Security Plus ライセンスでは 25 から 100 に、ASA 5520 では 100 から 150 に、ASA 5550 では 200 から 250 に増えています。
ASA 5580 の VLAN 数の増加	8.1(2)	ASA 5580 上でサポートされる VLAN 数が 100 から 250 に増加されました。



第 14 章

VXLAN インターフェイス

この章では、仮想拡張 LAN（VXLAN）インターフェイスを設定する方法について説明します。VXLAN は、レイヤ 2 ネットワークを拡張するためにレイヤ 3 物理ネットワーク上のレイヤ 2 仮想ネットワークとして機能します。

VXLAN インターフェイスの概要

VXLAN は、VLAN の場合と同じイーサネット レイヤ 2 ネットワーク サービスを提供しますが、より優れた拡張性と柔軟性を備えています。VLAN と比較して、VXLAN には次の利点があります。

- データセンター全体でのマルチテナント セグメントの柔軟な配置。
- より多くのレイヤ 2 セグメント（最大 1600 万の VXLAN セグメント）に対応するための高度なスケーラビリティ。

ここでは、VXLAN の動作について説明します。詳細については、RFC 7348 を参照してください。

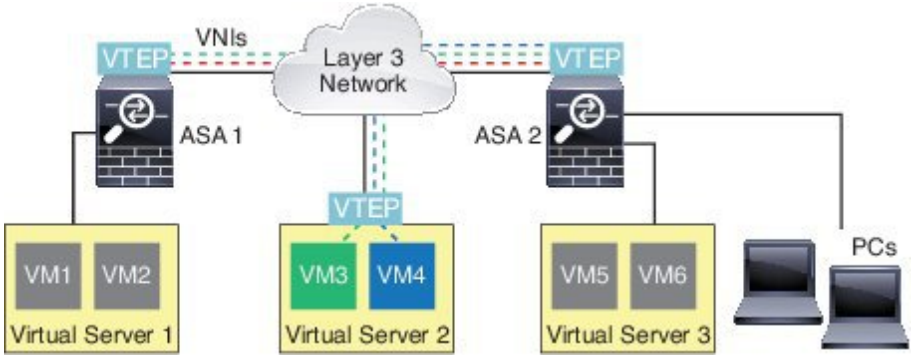
VXLAN カプセル化

VXLAN は、レイヤ 3 ネットワーク上のレイヤ 2 オーバーレイ方式です。VXLAN は、MAC Address-in-User Datagram Protocol（MAC-in-UDP）のカプセル化を使用します。元のレイヤ 2 フレームに VXLAN ヘッダーが追加され、UDP-IP パケットに置かれます。

VXLAN トンネル エンドポイント

VXLAN トンネルエンドポイント（VTEP）デバイスは、VXLAN のカプセル化およびカプセル化解除を実行します。各 VTEP には 2 つのインターフェイス タイプ（セキュリティ ポリシーを適用する VXLAN Network Identifier（VNI）インターフェイスと呼ばれる 1 つ以上の仮想インターフェイスと、 VTEP 間に VNI をトンネリングする VTEP 送信元インターフェイスと呼ばれる通常のインターフェイス）があります。VTEP 送信元インターフェイスは、VTEP 間通信のトランスポート IP ネットワークに接続されます。

次の図に、レイヤ 3 ネットワークで VTEP として機能し、サイト間の VNI 1、2、3 を拡張する 2 つの ASA と仮想サーバ 2 を示します。ASA は、VXLAN と VXLAN 以外のネットワークの間のブリッジまたはゲートウェイとして機能します。



VTEP 間の基盤となる IP ネットワークは、VXLAN オーバーレイに依存しません。カプセル化されたパケットは、発信元 IP アドレスとして開始 VTEP を持ち、宛先 IP アドレスとして終端 VTEP を持っており、外部 IP アドレス ヘッダーに基づいてルーティングされます。宛先 IP アドレスは、リモート VTEP が不明な場合、マルチキャスト グループにすることができます。デフォルトでは、宛先ポートは UDP ポート 4789 です（ユーザ設定可能）。

VTEP 送信元インターフェイス

VTEP 送信元インターフェイスは、すべての VNI インターフェイスに関連付けられる予定の標準の ASA インターフェイス（物理、冗長、EtherChannel、または VLAN）です。ASA/セキュリティ コンテキストごとに 1 つの VTEP 送信元インターフェイスを設定できます。

VTEP 送信元インターフェイスは、VXLAN トラフィック専用にすることができますが、その使用に制限されません。必要に応じて、インターフェイスを通常のトラフィックに使用し、そのトラフィックのインターフェイスにセキュリティポリシーを適用できます。ただし、VXLAN トラフィックの場合は、すべてのセキュリティ ポリシーを VNI インターフェイスに適用する必要があります。VTEP インターフェイスは、物理ポートとしてのみ機能します。

トランスペアレント ファイアウォール モードでは、VTEP 送信元インターフェイスは、BVI の一部ではないため、その IP アドレスを設定しません。このインターフェイスは、管理インターフェイスが処理される方法に似ています。

VNI インターフェイス

VNI インターフェイスは VLAN インターフェイスに似ています。VNI インターフェイスは、タギングを使用して特定の物理インターフェイスでのネットワーク トラフィックの分割を維持する仮想インターフェイスです。各VNI インターフェイスにセキュリティ ポリシーを直接適用します。

すべての VNI インターフェイスは、同じ VTEP インターフェイスに関連付けられます。

VXLAN パケット処理

VTEP 送信元インターフェイスを出入りするトラフィックは、VXLAN 処理、特にカプセル化または非カプセル化の対象となります。

カプセル化処理には、次のタスクが含まれます。

- VTEP送信元インターフェイスにより、VXLANヘッダーが含まれている内部MACフレームがカプセル化されます。
- UDP チェックサム フィールドがゼロに設定されます。
- 外部フレームの送信元 IP がVTEP インターフェイスの IP に設定されます。
- 外部フレームの宛先 IP がリモート VTEP IP ルックアップによって決定されます。

カプセル化解除については、次の場合に ASA によって VXLAN パケットのみがカプセル化解除されます。

- これが、宛先ポートが 4789 に設定された UDP パケットである場合（この値はユーザ設定可能です）。
- 入力インターフェイスが VTEP 送信元インターフェイスである場合。
- 入力インターフェイスの IP アドレスが宛先 IP アドレスと同じになります。
- VXLAN パケット形式が標準に準拠します。

ピア VTEP

ASA がピア VTEP の背後にあるデバイスにパケットを送信する場合、ASA には次の 2 つの重要な情報が必要です。

- リモート デバイスの宛先 MAC アドレス
- ピア VTEP の宛先 IP アドレス

ASA がこの情報を検出するには 2 つの方法あります。

- 単一のピア VTEP IP アドレスを ASA に静的に設定できます。

  手動で複数のピアを定義することはできません。

ASA が VXLAN カプセル化 ARP ブロードキャストを VTEP に送信し、エンド ノードの MAC アドレスを取得します。

- マルチキャスト グループは、VNI インターフェイスごとに（または VTEP 全体に）設定できます。

  ASA は、IP マルチキャスト パケット内の VXLAN カプセル化 ARP ブロードキャスト パケットを VTEP 送信元インターフェイスを経由して送信します。この ARP 要求への応答により、ASA はリモート VTEP の IP アドレスと、リモート エンド ノードの宛先 MAC アドレスの両方を取得することができます。

ASA は VNI インターフェイスのリモート VTEP IP アドレスに対する宛先 MAC アドレスのマッピングを維持します。

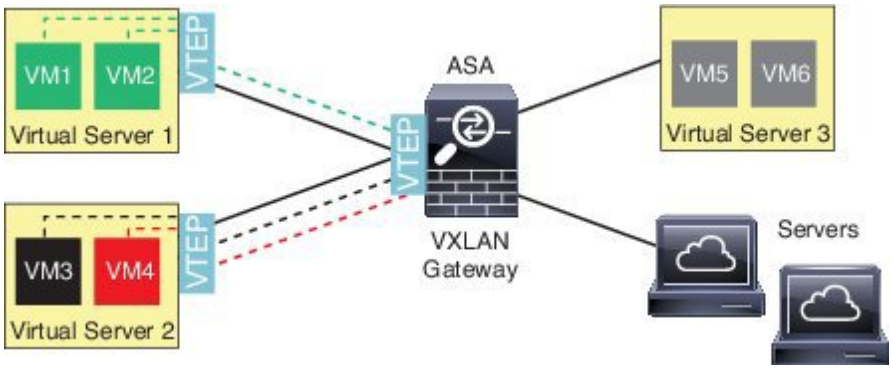
VXLAN 使用例

ここでは、ASA 上への VXLAN の実装事例について説明します。

VXLAN ブリッジまたはゲートウェイの概要

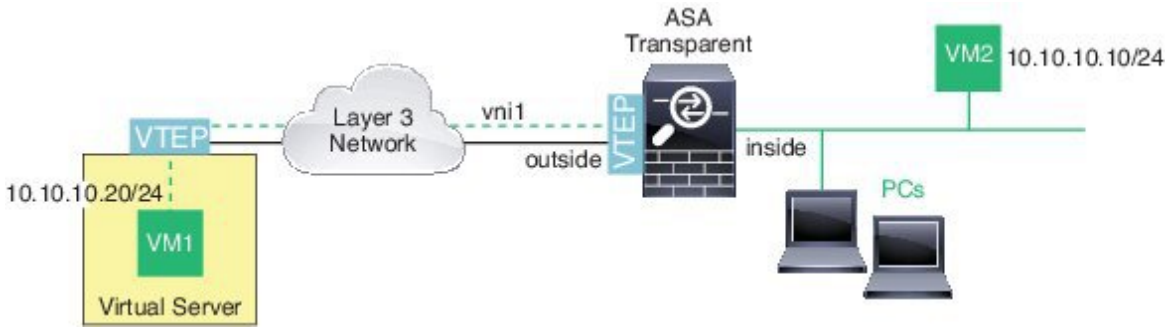
各 ASA の VTEP は、VM、サーバ、PC、VXLAN のオーバーレイ ネットワークなどのエンド ノードの間のブリッジまたはゲートウェイとして機能します。VTEP 送信元インターフェイス経由の VXLAN カプセル化を使用して受信された着信フレームの場合は、ASA が VXLAN ヘッダーを抽出して、内部イーサネット フレームの宛先 MAC アドレスに基づいて非 VXLAN ネットワークに接続された物理インターフェイスにその着信フレームを転送します。

ASA は、常に VXLAN パケットを処理します。未処理の VXLAN パケットを他の 2 つの VTEP 間でそのまま転送しません。



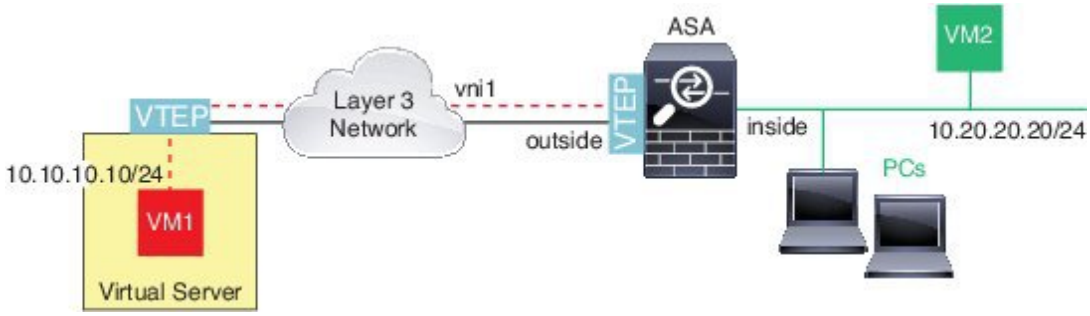
VXLAN ブリッジ（トランスペアレント モード）

ブリッジグループを使用する場合（トランスペアレント ファイアウォール モード）、ASA は、同じネットワークに存在する VXLAN セグメント（リモート）とローカル セグメント間の VXLAN ブリッジとして機能できます。この場合、ブリッジグループのメンバーは通常インターフェイス 1 つのメンバーが通常のインターフェイスで、もう 1 つのメンバーが VNI インターフェイスです。



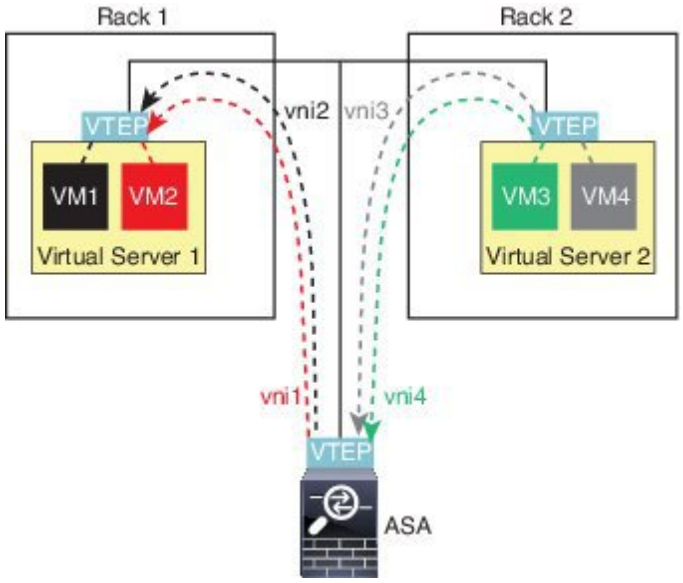
VXLAN ゲートウェイ（ルーテッド モード）

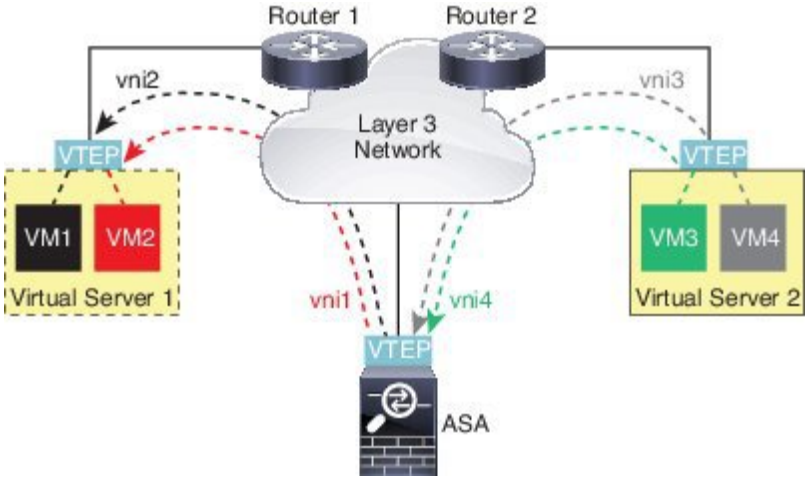
ASA は、VXLAN ドメインと VXLAN 以外のドメインの間のルータとして機能し、異なるネットワーク上のデバイスを接続できます。



VXLAN ドメイン間のルータ

VXLAN 拡張レイヤ 2 ドメインを使用すると、VM は、ASA が同じラックにないとき、あるいは ASA がレイヤ 3 ネットワーク上の離れた場所にあるときに、ゲートウェイとして ASA を指し示すことができます。





このシナリオに関する次の注意事項を参照してください。

1. VM3 から VM1 へのパケットでは、ASA がデフォルト ゲートウェイであるため、宛先 MAC アドレスは ASA の MAC アドレスです。
2. 仮想サーバ 2 の VTEP 送信元インターフェイスは、VM3 からパケットを受信してから、VNI 3 の VXLAN タグでパケットをカプセル化して ASA に送信します。
3. ASA は、パケットを受信すると、パケットをカプセル化解除して内部フレームを取得します。
4. ASA は、ルート ルックアップに内部フレームを使用して、宛先が VNI 2 上であることを認識します。VM1 のマッピングがまだない場合、ASA は VNI 2 カプセル化された ARP ブロードキャストを VNI 2 のマルチキャスト グループ IP で送信します。

（注） このシナリオでは複数の VTEP ピアがあるため、ASA は複数のダイナミック VTEP ピア ディスカバリを使用する必要があります。

5. ASA は VNI 2 の VXLAN タグでパケットを再度カプセル化し、仮想サーバ 1 に送信します。カプセル化の前に、ASA は内部フレームの宛先 MAC アドレスを変更して VM1 の MAC にします（ASA で VM1 の MAC アドレスを取得するためにマルチキャスト カプセル化 ARP が必要な場合があります）。
6. 仮想サーバ 1 は、VXLAN パケットを受信すると、パケットをカプセル化解除して内部フレームを VM1 に配信します。

VXLAN インターフェイスのガイドライン

IPv6

- VNI インターフェイスでは、IPv6 トラフィックをサポートしますが、VTEP 送信元インターフェイス IP アドレスでは、IPv4 のみをサポートします。
- IPv6 OSPF インターフェイス設定はサポートされていません。

クラスタ

ASA クラスタリングでは、個別インターフェイス モードの VXLAN をサポートしません。Spanned EtherChannel モードでのみ VXLAN をサポートします。

Routing

- VNI インターフェイスでは、スタティック ルーティングのみをサポートします。ダイナミック ルーティング プロトコルはサポートされません。
- ポリシーベース ルーティングはサポートされません。

MTU

送信元インターフェイスの MTU が 1554 バイト未満の場合、ASA は自動的に MTU を 1554 バイトに増やします。この場合、イーサネット データグラム全体がカプセル化されるため、新しいパケットのサイズが大きくなるため、より大きな MTU が必要になります。他のデバイスが使用する MTU の方が大きい場合、送信元インターフェイス MTU を、ネットワーク MTU + 54 バイトに設定する必要があります。この MTU は、ジャンボ フレーム予約を有効にする必要があります。ジャンボ フレーム サポートの有効化 （474 ページ） を参照してください。

VXLAN インターフェイスのデフォルト設定

デフォルトでは、VNI インターフェイスはイネーブルになっています。

VXLAN インターフェイスの設定

VXLAN を設定するには、次の手順を実行します。

手順

ステップ 1 VTEP 送信元インターフェイスの設定 （510 ページ）。

ステップ 2 VNI インターフェイスの設定 （512 ページ）

ステップ 3 （オプション）VXLAN UDP ポートの変更 （513 ページ）を使用して無効にすることができます。

VTEP 送信元インターフェイスの設定

ASA ごと、またはセキュリティ コンテキストごとに 1 つの VTEP 送信元インターフェイスを設定できます。VTEP は、ネットワーク仮想化エンドポイント（NVE）として定義されます。VXLAN VTEP が現時点でサポートされている NVE です。

始める前に

マルチ コンテキスト モードでは、この項のタスクをコンテキスト実行スペースで実行してください。設定したいコンテキストを変更するには、**changeto context***name* コマンドを入力します。

手順

ステップ 1 （トランスペアレント モード）送信元インターフェイスが NVE 専用であることを指定します。

interface *id*

nve-only

例：

```
ciscoasa(config)# interface gigabitethernet 1/1
ciscoasa(config-if)# nve-only
```

この設定により、インターフェイスの IP アドレスを設定することができます。このコマンドは、この設定によってトラフィックがこのインターフェイスの VXLAN および共通の管理トラフィックのみに制限されるルーテッド モードではオプションです。

ステップ 2 送信元インターフェイス名と IPv4 アドレスを設定します。

例：

（ルーテッド モード）

```
ciscoasa(config)# interface gigabitethernet 1/1
ciscoasa(config-if)# nameif outside
ciscoasa(config-if)# ip address 10.1.1.1 255.255.255.0
```

例：

（トランスペアレント モード）

```
ciscoasa(config)# interface gigabitethernet 1/1
ciscoasa(config-if)# nve-only
```

```
ciscoasa(config-if)# nameif outside
ciscoasa(config-if)# ip address 10.1.1.1 255.255.255.0
```

ステップ 3 NVE インスタンスを指定します。

nve 1

ID 1 で NVE インスタンスを 1 つだけ指定できます。

（注） **encapsulation vxlan** コマンドが NVE インスタンスのデフォルトにより追加されます。明示的に追加する必要はありません。

ステップ 4 ステップ 2 で設定した送信元インターフェイス名を指定します。

source-interface *interface-name*

例：

```
ciscoasa(cfg-nve)# source-interface outside
```

（注） 送信元インターフェイスの MTU が 1554 バイト未満の場合、ASA は自動的に MTU を 1554 バイトに増やします。

ステップ 5 （マルチ コンテキスト モード（シングル モードではオプション）手動でピア VTEP の IP アドレスを指定します。

peer ip *ip_address*

例：

```
ciscoasa(cfg-nve)# peer ip 10.1.1.2
```

ピア IP アドレスを指定した場合、マルチキャスト グループ ディスカバリは使用できません。マルチキャストは、マルチ コンテキスト モードではサポートされていないため、手動設定が唯一のオプションです。VTEP には 1 つのピアのみを指定できます。

ステップ 6 （オプション、シングル モードのみ）関連付けられたすべての VNI インターフェイスにデフォルトのマルチキャスト グループを指定します。

default-mcast-group *mcast_ip*

例：

```
ciscoasa(cfg-nve)# default-mcast-group 236.0.0.100
```

VNI インターフェイスごとにマルチキャスト グループを設定していない場合は、このグループが使用されます。その VNI インターフェイス レベルでグループを設定している場合は、そのグループがこの設定よりも優先されます。

VNI インターフェイスの設定

VNI インターフェイスを追加してそれを VTEP 送信元インターフェイスに関連付けて、基本インターフェイス パラメータを設定します。

手順

ステップ 1 VNI インターフェイスを作成します。

interface vni *vni_num*

例：

```
ciscoasa(config)# interface vni 1
```

1 ～ 10000 の範囲で ID を設定します。この ID は内部インターフェイス識別子です。

ステップ 2 VXLAN セグメント ID を指定します。

segment-id *id*

例：

```
ciscoasa(config-if)# segment-id 1000
```

1 ～ 16777215 の範囲で ID を設定します。セグメント ID は VXLAN タギングに使用されます。

ステップ 3 （トランスペアレント モードの場合は必須）このインターフェイスを関連付けるブリッジ グループを指定します。

bridge-group *number*

例：

```
ciscoasa(config-if)# bridge-group 1
```

BVI インターフェイスを設定して通常のインターフェイスをこのブリッジ グループに関連付けるには、トランスペアレント モードの□ブリッジ グループ インターフェイスの設定（531 ページ）を参照してください。

ステップ 4 このインターフェイスを VTEP 送信元インターフェイスに関連付けます。

vtep-nve 1

ステップ 5 インターフェイスの名前を指定します。

nameif *vni_interface_name*

例：

```
ciscoasa(config-if)# nameif vxlan1000
```

name は最大 48 文字のテキスト文字列です。大文字と小文字は区別されません。名前を変更するには、このコマンドで新しい値を再入力します。その名前を参照するすべてのコマンドが削除されるため、**no** 形式は入力しないでください。

ステップ 6 （ルーテッド モード）IPv4 アドレスと IPv6 アドレスの一方または両方を割り当てます。

ip address {*ip_address* [*mask*] [**standby** *ip_address*] | **dhcp** [**setroute**] | **pppoe** [**setroute**]}

ipv6 address {**autoconfig** | *ipv6-address*/*prefix-length* [**standby** *ipv6-address*]}

例：

```
ciscoasa(config-if)# ip address 10.1.1.1 255.255.255.0 standby 10.1.1.2
ciscoasa(config-if)# ipv6 address 2001:0DB8::BA98:0:3210/48
```

ステップ 7 セキュリティ レベルを設定します。

security-level *level*

例：

```
ciscoasa(config-if)# security-level 50
```

number には、0（最下位）～ 100（最上位）の整数を指定します。

ステップ 8 （シングル モード）マルチキャスト グループ アドレスを設定します。

mcast-group *multicast_ip*

例：

```
ciscoasa(config-if)# mcast-group 236.0.0.100
```

VNI インターフェイスに対してマルチキャスト グループを設定しない場合は、VTEP 送信元インターフェイス設定のデフォルト グループが使用されます（使用可能な場合）。VTEP 送信元インターフェイスに対して手動でVTEP ピア IP を設定した場合、VNI インターフェイスに対してマルチキャスト グループを指定することはできません。マルチキャストは、マルチ コンテキスト モードではサポートされていません。

（オプション）VXLAN UDP ポートの変更

デフォルトでは、VTEP 送信元インターフェイスは UDP ポート 4789 への VXLAN トラフィックを受け入れます。ネットワークで標準以外のポートを使用する場合は、それを変更できます。

始める前に

マルチ コンテキスト モードでは、システム実行スペースで次のタスクを実行します。コンテキストからシステム実行スペースに切り替えるには、**changeto system** コマンドを入力します。

手順

VXLAN UDP ポートを設定します。

vxlan *port number*

例：

```
ciscoasa(config)# vxlan port 5678
```

VXLAN インターフェイスのモニタリング

VTEP インターフェイスおよび VNI インターフェイスをモニタするには、次のコマンドを参照してください。

- **show nve** [*id*] [**summary**]

  このコマンドは、NVE インターフェイスのパラメータ、ステータス、および統計情報とキャリア インターフェイス（送信元インターフェイス）のステータス、この NVE を VXLAN VTEP として使用する VNI、ならびにこの NVE インターフェイスに関連付けられているピア VTEP IP アドレスを表示します。**summary** オプションを指定すると、このコマンドは、the status of the NVE インターフェイスのステータス、NVE インターフェイスの背後にある VNI の数、 検出された VTEP の数を表示します。

  show nve 1 コマンドについては、次の出力を参照してください。

```
ciscoasa# show nve 1
ciscoasa(config-if)# show nve
nve 1, source-interface "inside" is up
IP address 15.1.2.1, subnet mask 255.255.255.0
Encapsulation: vxlan
Encapsulated traffic statistics:
6701004 packets input, 3196266002 bytes
6700897 packets output, 3437418084 bytes
1 packets dropped
Number of configured static peer VTEPs: 0
Number of discovered peer VTEPs: 1
Discovered peer VTEPs:
IP address 15.1.2.3
Number of VNIs attached to nve 1: 2
VNIs attached:
vni 2: segment-id 5002, mcast-group 239.1.2.3
vni 1: segment-id 5001, mcast-group 239.1.2.3
```

  show nve 1 summary コマンドについては、次の出力を参照してください。

```
ciscoasa# show nve 1 summary
nve 1, source-interface "inside" is up
Encapsulation: vxlan
Number of configured static peer VTEPs: 0
Number of discovered peer VTEPs: 1
```

```
Default multicast group: 239.1.2.3
Number of VNIs attached to nve 1: 2
```

- **show interface vni** *id* [**summary**]

  このコマンドは、VNIインターフェイスのパラメータ、ステータス、および統計情報と、ブリッジされているインターフェイス（設定されている場合）のステータス、ならびに関連付けられているNVEインターフェイスを表示します。**summary** オプションを指定すると、VNIインターフェイスのパラメータのみが表示されます。

  show interface vni 1 コマンドについては、次の出力を参照してください。

```
ciscoasa# show interface vni 1
Interface vni1 "vni-inside", is up, line protocol is up
VTEP-NVE 1
Segment-id 5001
Tag-switching: disabled
MTU: 1500
MAC: aaaa.bbbb.1234
IP address 192.168.0.1, subnet mask 255.255.255.0
Multicast group 239.1.3.3
Traffic Statistics for "vni-inside":
235 packets input, 23606 bytes
524 packets output, 32364 bytes
14 packets dropped
1 minute input rate 0 pkts/sec, 0 bytes/sec
1 minute output rate 0 pkts/sec, 2 bytes/sec
1 minute drop rate, 0 pkts/sec
5 minute input rate 0 pkts/sec, 0 bytes/sec
5 minute output rate 0 pkts/sec, 0 bytes/sec
5 minute drop rate, 0 pkts/sec
```

  show interface vni 1 summary コマンドについては、次の出力を参照してください。

```
ciscoasa# show interface vni 1 summary
Interface vni1 "vni-inside", is up, line protocol is up
VTEP-NVE 1
Segment-id 5001
Tag-switching: disabled
MTU: 1500
MAC: aaaa.bbbb.1234
IP address 192.168.0.1, subnet mask 255.255.255.0
Multicast group not configured
```

- **show vni vlan-mapping**

  このコマンドは、VNIセグメントIDと、VLANインターフェイスまたは物理インターフェイス間のマッピングを表示します。このコマンドは、ルーテッドモードでは、VXLANとVLAN間ののマッピングに表示する値を大量に含めることができるため、トランスペアレント ファイアウォール モードでのみ有効です。

  show vni vlan-mapping コマンドについては、次の出力を参照してください。

```
ciscoasa# show vni vlan-mapping
vni1: segment-id: 6000, interface: 'g0110', vlan 10, interface: 'g0111', vlan 11
vni2: segment_id: 5000, interface: 'g01100', vlan 1, interface: 'g111', vlan 3,
```

```
interface: 'g112', vlan 4
```

- **show arp vtep-mapping**

  このコマンドは、リモート セグメント ドメインにある IP アドレスとリモート VTEP IP アドレス用の VNI インターフェイスにキャッシュされた MAC アドレスを表示します。

  show arp vtep-mapping コマンドについては、次の出力を参照してください。

```
ciscoasa# show arp vtep-mapping
vni-outside 192.168.1.4 0012.0100.0003 577 15.1.2.3
vni-inside 192.168.0.4 0014.0100.0003 577 15.1.2.3
```

- **show mac-address-table vtep-mapping**

  このコマンドは、リモート VTEP IP アドレスが設定された VNI インターフェイス上のレイヤ 2 転送テーブル（MAC アドレス テーブル）を表示します。

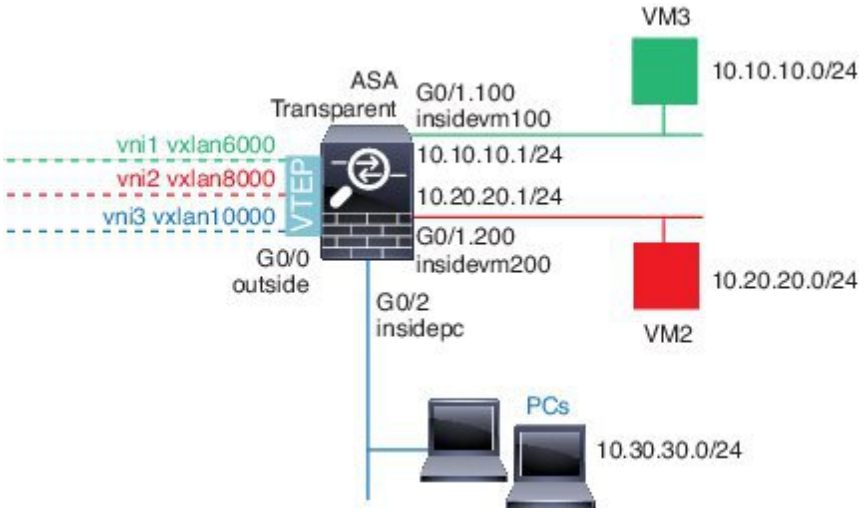
  show mac-address-table vtep-mapping コマンドについては、次の出力を参照してください。

```
ciscoasa# show mac-address-table vtep-mapping
interface                  mac  address       type     Age(min)   bridge-group
VTEP
-------------------------------------------------------------------------------------------
vni-outside                00ff.9200.0000      dynamic      5         1
10.9.1.3
vni-inside                0041.9f00.0000     dynamic     5         1      10.9.1.3
```

VXLAN インターフェイスの例

次の VXLAN の設定例を参照してください。

トランスペアレント VXLAN ゲートウェイの例



この例の次の説明を参照してください。

- GigabitEthernet 0/0 の外部インターフェイスは、VTEP 送信元インターフェイスとして使用され、レイヤ 3 ネットワークに接続されます。
- GigabitEthernet 0/1.100 の insidevm100 VLAN サブインターフェイスは、VM3 が存在する 10.10.10.0/24 ネットワークに接続されます。VM3 が VM1 と通信する場合（表示されません。両方とも、10.10.10.0/24 の IP アドレスを持つ）、ASA は VXLAN タグ 6000 を使用します。
- GigabitEthernet 0/1.200 の insidevm200 VLAN サブインターフェイスは、VM2 が存在する 10.20.20.0/24 ネットワークに接続されます。VM2 が VM4 と通信する場合（表示されません。両方とも、10.20.20.0/24 の IP アドレスを持つ）、ASA は VXLAN タグ 8000 を使用します。
- GigabitEthernet 0/2 の insidepc インターフェイスは、数台の PC が存在する 10.30.30.0/24 ネットワークに接続されます。それらの PC が、同じネットワーク（すべて 10.30.30.0/24 の IP アドレスを持つ）に属するリモート VTEP の裏の VMs/PCs（表示されません）と通信する場合、ASA は VXLAN タグ 10000 を使用します。

ASA の設定

```
firewall transparent
vxlan port 8427
!
interface gigabitethernet0/0
  nve-only
  nameif outside
  ip address 192.168.1.30 255.255.255.0
  no shutdown
!
nve 1
  encapsulation vxlan
```

```
  source-interface outside
!
interface vni1
  segment-id 6000
  nameif vxlan6000
  security-level 0
  bridge-group 1
  vtep-nve 1
  mcast-group 235.0.0.100
!
interface vni2
  segment-id 8000
  nameif vxlan8000
  security-level 0
  bridge-group 2
  vtep-nve 1
  mcast-group 236.0.0.100
!
interface vni3
  segment-id 10000
  nameif vxlan10000
  security-level 0
  bridge-group 3
  vtep-nve 1
  mcast-group 236.0.0.100
!
interface gigabitethernet0/1.100
  nameif insidevm100
  security-level 100
  bridge-group 1
!
interface gigabitethernet0/1.200
  nameif insidevm200
  security-level 100
  bridge-group 2
!
interface gigabitethernet0/2
  nameif insidepc
  security-level 100
  bridge-group 3
!
interface bvi 1
  ip address 10.10.10.1 255.255.255.0
!
interface bvi 2
  ip address 10.20.20.1 255.255.255.0
!
interface bvi 3
  ip address 10.30.30.1 255.255.255.0
```

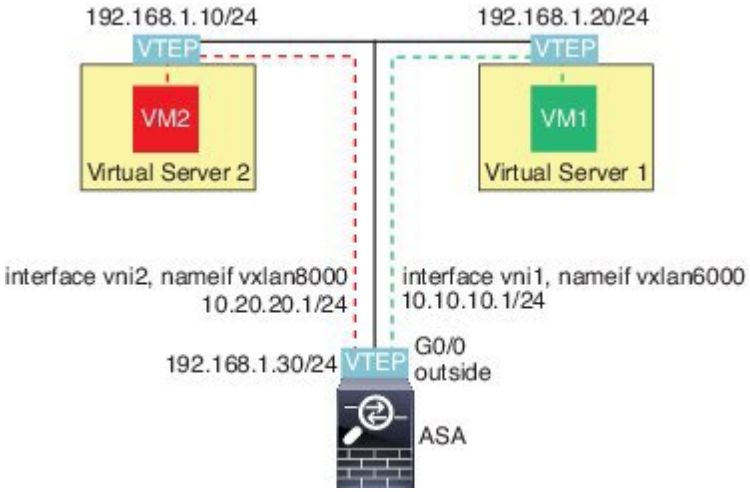
注意

- VNI インタフェース vni1 と vni2 の場合、カプセル化時に内部 VLAN タグが削除されます。
- VNI インターフェイス vni2 と vni3 は、マルチキャストでカプセル化された ARP に対して同じマルチキャスト IP アドレスを共有します。この共有は許可されます。
- ASA は、上記の BVI とブリッジグループ設定に基づいて VXLAN トラフィックを非 VXLAN でサポートされているインターフェイスにブリッジします。拡張されたレイヤ 2 ネット

ワークの各セグメント（10.10.10.0/24、10.20.20.0/24、10.30.30.0/24）の場合、ASA はブリッジとして機能します。

- 複数の VNI または複数の通常のインターフェイス（VLAN または単に物理インターフェイス）をブリッジ グループに設定できます。VXLAN セグメント ID から VLAN ID（物理インターフェイス）の転送または関連付けは、宛先 MAC アドレスによって決定され、どちらかのインターフェイスが宛先に接続されます。
- VTEP 送信元インターフェイスは、インターフェイス設定で **nve-only** によって示されるトランスペアレント ファイアウォール モードのレイヤ 3 インターフェイスです。VTEP 送信元インターフェイスは、BVI インターフェイスまたは管理インターフェイスではありませんが、IP アドレスがあり、ルーティング テーブルを使用します。

VXLAN ルーティングの例



この例の次の説明を参照してください。

- VM1（10.10.10.10）は仮想サーバ 1 にホストされ、VM2（10.20.20.20）は仮想サーバ 2 にホストされます。
- VM1 のデフォルト ゲートウェイは ASA であり、仮想サーバ 1 と同じのポッドにありませんが、VM1 はそれを認識しません。VM1 は、そのデフォルト ゲートウェイの IP アドレスが 10.10.10.1 であることだけを認識します。同様に、VM2 はデフォルト ゲートウェイの IP アドレスが10.20.20.1 であることだけを認識します。
- 仮想サーバ 1 および 2 の VTEP サポート型ハイパーバイザは、同じサブネットまたはレイヤ 3 ネットワーク（表示なし。この場合、ASA と仮想サーバのアップリンクに異なるネットワーク アドレスがある）経由で ASA と通信できます。
- VM1 のパケットは、そのハイパーバイザの VTEP によってカプセル化され、VXLAN トンネリングを使用してそのデフォルト ゲートウェイに送信されます。

- VM1 がパケットを VM2 に送信すると、パケットはその観点からデフォルト ゲートウェイ 10.10.10.1 を介して送信されます。仮想サーバ 1 は 10.10.10.1 がローカルにないことを認識しているので、VTEP は VXLAN 経由でパケットをカプセル化し、ASA の VTEP に送信します。
- ASA で、パケットはカプセル化解除されます。VXLAN セグメント ID は、カプセル化解除時に取得されます。次に、ASA は、VXLAN セグメント ID に基づいて、VNI インターフェイス（vni1）に対応する内部フレームを再投入します。その後に、ASA はルート ルックアップを実行し、別の VNI インターフェイス（vni2）経由で内部パケットを送信します。vni2 を経由するすべての出力パケットは、VXLAN セグメント 8000 でカプセル化され、VTEP 経由で外部に送信されます。
- 最後に、カプセル化されたパケットが仮想サーバ 2 の VTEP によって受信され、カプセル化解除され、VM2 に転送されます。

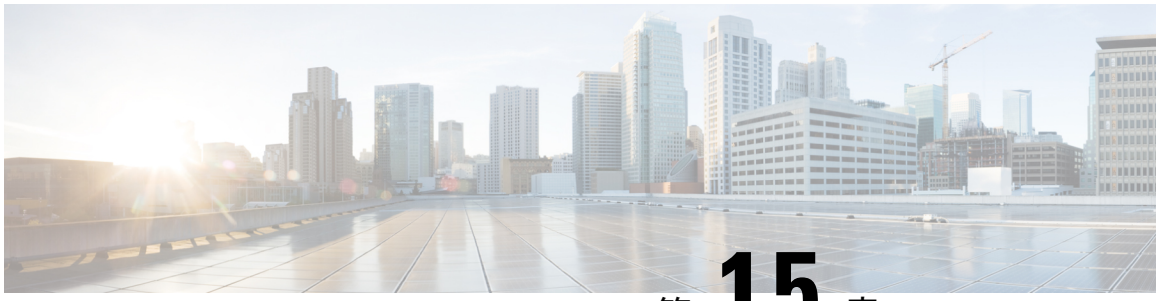
ASA の設定

```
interface gigabitethernet0/0
  nameif outside
  ip address 192.168.1.30 255.255.255.0
  no shutdown
!
nve 1
  encapsulation vxlan
  source-interface outside
  default-mcast-group 235.0.0.100
!
interface vni1
  segment-id 6000
  nameif vxlan6000
  security-level 0
  vtep-nve 1
  ip address 10.20.20.1 255.255.255.0
!
interface vni2
  segment-id 8000
  nameif vxlan8000
  security-level 0
  vtep-nve 1
  ip address 10.10.10.1 255.255.255.0
!
```

VXLAN インターフェイスの履歴

表 *19 : VXLAN* インターフェイスの履歴

機能名	リリース	機能情報
VXLAN のサポート	9.4(1)	VXLAN のサポートが追加されました（VXLAN トンネル エンドポイント（VTEP）のサポートを含む）。ASA またはセキュリティ コンテキストごとに 1 つの VTEP 送信元インターフェイスを定義できます。 次のコマンドが導入されました。**debug vxlan**、**default-mcast-group**、**encapsulation vxlan**、**inspect vxlan**、**interface vni**、**mcast-group**、**nve**、**nve-only**、**peer ip**、**segment-id**、**show arp vtep-mapping**、**show interface vni**、**show mac-address-table vtep-mapping**、**show nve**、**show vni vlan-mapping**、**source-interface**、**vtep-nve**、**vxlan port**



第 15 章

ルーテッド モード インターフェイスとトランスペアレント モード インターフェイス

この章では、ルーテッド ファイアウォール モードおよびトランスペアレント ファイアウォール モードですべてのモデルのインターフェイス コンフィギュレーションを実行するためのタスクについて説明します。

（注） マルチ コンテキスト モードでは、この項のタスクをコンテキスト実行スペースで実行してください。設定したいコンテキストを変更するには、**changeto context***name* コマンドを入力します。

ルーテッドモードインターフェイスとトランスペアレント モード インターフェイスについて

ASA は、ルーテッドおよびブリッジという 2 つのタイプのインターフェイスをサポートします。

各レイヤ3ルーテッドインターフェイスは一意のサブネット上にIPアドレスを必要とします。

ブリッジインターフェイスはブリッジグループに属し、すべてのインターフェイスは同じネットワーク内にあります。ブリッジ グループはブリッジ ネットワーク上に IP アドレスを持つブリッジ仮想インターフェイス（BVI）で表されます。ルーテッドモードはルーテッドインターフェイスのみサポートします。トランスペアレント ファイアウォール モードでは、ブリッジグループと BVI インターフェイスのみがサポートされます。

セキュリティ レベル

ブリッジグループ メンバーインターフェイスを含む各インターフェイスには、0（最下位）～100（最上位）のセキュリティ レベルを設定する必要があります。たとえば、内部ホスト ネットワークなど、最もセキュアなネットワークにはレベル100を割り当てる必要があります。一方、インターネットなどに接続する外部ネットワークにはレベル0が割り当てられる場合があります。DMZ など、その他のネットワークはその中間に設定できます。複数のインターフェイスを同じセキュリティ レベルに割り当てることができます。

トランスペアレントモードでは、BVIインターフェイスはインターフェイス間のルーティングに参加しないため、BVI インターフェイスにはセキュリティ レベルが割り当てられていません。

レベルによって、次の動作が制御されます。

- ネットワーク アクセス：デフォルトで、高いセキュリティ レベルのインターフェイスから低いセキュリティ レベルのインターフェイスへの通信（発信）は暗黙的に許可されます。高いセキュリティ レベルのインターフェイス上のホストは、低いセキュリティ レベルのインターフェイス上の任意のホストにアクセスできます。ACLをインターフェイスに適用して、アクセスを制限できます。

  同じセキュリティ レベルのインターフェイスの通信をイネーブルにすると、同じセキュリティ レベルまたはそれより低いセキュリティ レベルの他のインターフェイスにアクセスするインターフェイスは、暗黙的に許可されます。

- インスペクション エンジン：一部のアプリケーション インスペクション エンジンはセキュリティ レベルに依存します。同じセキュリティ レベルのインターフェイス間では、インスペクション エンジンは発信と着信のいずれのトラフィックに対しても適用されます。

  - NetBIOS インスペクション エンジン：発信接続に対してのみ適用されます。

- SQL*Net インスペクション エンジン：SQL*Net（旧称 OraServ）ポートとの制御接続が一対のホスト間に存在する場合、着信データ接続だけが ASA を通過することが許可されます。

デュアル IP スタック（IPv4 および IPv6）

ASA は、インターフェイスで IPv6 アドレスと IPv4 アドレスの両方をサポートしています。IPv4 と IPv6 の両方で、デフォルト ルートを設定してください。

ルーテッドモードおよびトランスペアレントモードのインターフェイスのガイドラインおよび要件

コンテキスト モード

- マルチ コンテキスト モードで設定できるのは、マルチ コンテキストの設定 （215 ページ）に従ってシステム コンフィギュレーションでコンテキストにすでに割り当てられているコンテキスト インターフェイスだけです。
- PPPoE は、マルチ コンテキスト モードではサポートされていません。
- トランスペアレント モードのマルチ コンテキスト モードでは、各コンテキストが別個のインターフェイスを使用する必要があります。コンテキスト間でインターフェイスを共有することはできません。
- トランスペアレント モードのマルチ コンテキスト モードでは、通常、各コンテキストが別個のサブネットを使用します。重複するサブネットを使用することもできますが、ルーティング スタンドポイントから可能にするため、ネットワーク トポロジにルータと NAT コンフィギュレーションが必要です。

フェールオーバー

- フェールオーバー リンクは、この章の手順で設定しないでください。詳細については、フェールオーバーの章も参照してください。
- フェールオーバーを使用する場合、データ インターフェイスの IP アドレスとスタンバイ アドレスを手動で設定する必要があります。DHCP および PPPoE はサポートされません。

IPv6

- IPv6 はすべてのインターフェイスでサポートされます。
- トランスペアレント モードでは、IPv6 アドレスは手動でのみ設定できます。
- ASAは、IPv6 エニーキャスト アドレスはサポートしません。

サポート モデル

- ASASM では、PPPoE および DHCP はサポートされません。

ASASM の VLAN ID

コンフィギュレーションにはあらゆる VLAN ID を追加できますが、トラフィックを転送できるのはスイッチによって ASA に割り当てられた VLAN だけです。ASA に割り当てられたすべての VLAN を表示するには、**show vlan** コマンドを使用します。

スイッチによって ASA にまだ割り当てられていない VLAN にインターフェイスを追加した場合、そのインターフェイスはダウン ステートになります。ASA に VLAN を割り当てた時点で、インターフェイスはアップ ステートに変化します。インターフェイス ステートの詳細については、**show interface** コマンドを参照してください。

トランスペアレント モードとブリッジ グループのガイドライン

- 4 のインターフェイスをもつブリッジ グループを 250 まで作成できます。
- 直接接続された各ネットワークは同一のサブネット上にある必要があります。
- ASA では、セカンダリ ネットワーク上のトラフィックはサポートされていません。BVI IP アドレスと同じネットワーク上のトラフィックだけがサポートされています。
- IPv4 の場合は、管理トラフィックと、ASA を通過するトラフィックの両方の各ブリッジ グループに対し、BVI の IP アドレスが必要です。IPv6 アドレスは BVI でサポートされますが必須ではありません。
- IPv6 アドレスは手動でのみ設定できます。
- BVI IP アドレスは、接続されたネットワークと同じサブネット内にある必要があります。サブネットにホスト サブネット（255.255.255.255）を設定することはできません。
- 管理インターフェイスはブリッジ グループのメンバーとしてサポートされません。
- トランスペアレント モードでは、少なくとも 1 つのブリッジ グループを使用し、データ インターフェイスがブリッジ グループに属している必要があります。
- トランスペアレント モードでは、接続されたデバイス用のデフォルト ゲートウェイとして BVI IP アドレスを指定しないでください。デバイスは ASA の他方側のルータをデフォルト ゲートウェイとして指定する必要があります。
- トランスペアレント モードでは、管理トラフィックの戻りパスを指定するために必要な *default* ルートは、1 つのブリッジ グループ ネットワークからの管理トラフィックにだけ適用されます。これは、デフォルト ルートはブリッジ グループのインターフェイスとブリッジ グループ ネットワークのルータ IP アドレスを指定しますが、ユーザは 1 つのデフォルト ルートしか定義できないためです。複数のブリッジ グループ ネットワークからの管理トラフィックが存在する場合は、管理トラフィックの発信元ネットワークを識別する標準のスタティック ルートを指定する必要があります。

- トランスペアレント モードでは、PPPoE は 管理 インターフェイスでサポートされません。
- Bidirectional Forwarding Detection（BFD）エコー パケットは、ブリッジ グループ メンバを使用するときに、ASA を介して許可されません。BFD を実行している ASA の両側に 2 つのネイバーがある場合、ASA は BFD エコー パケットをドロップします。両方が同じ送信元および宛先 IP アドレスを持ち、LAND 攻撃の一部であるように見えるからです。

デフォルトのセキュリティ レベル

デフォルトのセキュリティ レベルは 0 です。インターフェイスに「inside」という名前を付けて、明示的にセキュリティ レベルを設定しないと、ASA はセキュリティ レベルを 100 に設定します。

（注） インターフェイスのセキュリティ レベルを変更したときに、既存の接続がタイムアウトするまで待機せずに新しいセキュリティ情報を使用する必要がある場合は、**clear local-host** コマンドを使用して接続をクリアできます。

ルーテッド モードのインターフェイスの設定

ルーテッド モードのインターフェイスを設定するには、次の手順を実行します。

ルーテッド モードの一般的なインターフェイス パラメータの設定

この手順では、名前、セキュリティ レベル、IPv4 アドレス、およびその他のオプションを設定する方法について説明します。

始める前に

マルチ コンテキスト モードでは、コンテキスト実行スペースで次の手順を実行します。システム コンフィギュレーションからコンテキスト コンフィギュレーションに切り替えるには、**changeto context** *name* コマンドを入力します。

手順

ステップ 1 インターフェイス コンフィギュレーション モードを開始します。

interface *id*

例：

```
ciscoasa(config)# interface gigabithethernet 0/0
```

インターフェイス ID には、次のものがあります。

- **冗長**
- **port-channel**
- *physical*：**ethernet**、**gigabitethernet**、**tengigabitethernet**、**management** など。インターフェイス名については、使用しているモデルのハードウェア インストール ガイドを参照してください。
- *physical.subinterface*：**gigabitethernet0/0.100** など。
- **vni**
- **vlan**
- *mapped_name*：マルチ コンテキスト モードの場合。

ステップ 2 インターフェイスの名前を指定します。

nameif *name*

例：

```
ciscoasa(config-if)# nameif inside
```

name は最大 48 文字のテキスト文字列です。大文字と小文字は区別されません。名前を変更するには、このコマンドで新しい値を再入力します。その名前を参照するすべてのコマンドが削除されるため、**no** 形式は入力しないでください。

ステップ 3 次のいずれかの方法を使用して IP アドレスを設定します。

- IP アドレスを手動で設定します。

  ip address *ip_address* [*mask*] [**standby** *ip_address*]

  例：

  ```
  ciscoasa(config-if)# ip address 10.1.1.1 255.255.255.0 standby 10.1.1.2
  ```

  （注） フェールオーバーを使用する場合、IP アドレスとスタンバイ アドレスを手動で設定する必要があります。DHCP および PPPoE はサポートされません。

  standby *ip_address* 引数は、フェールオーバーで使用します。スタンバイ IP アドレスを設定しない場合、アクティブ ユニットはネットワーク テストを使用してスタンバイ インターフェイスをモニタできず、リンク ステートをトラックすることしかできません。

  ip_address 引数および *mask* 引数には、インターフェイスの IP アドレスとサブネット マスクを設定します。

- DHCP サーバから IP アドレスを取得します。

  ip address dhcp [**setroute**]

例：

```
ciscoasa(config-if)# ip address dhcp
```

setroute キーワードを指定すると、ASA が DHCP サーバから渡されたデフォルト ルートを使用できるようになります。

DHCP リースをリセットし、新規リースを要求するには、このコマンドを再入力します。

（注） **ip address dhcp** コマンドを入力する前に、**no shutdown** コマンドを使用してインターフェイスを有効化していない場合、一部の DHCP 要求が送信されないことがあります。

- PPPoE サーバから IP アドレスを取得します。

  ip address pppoe [**setroute**]

  例：

  ```
  ciscoasa(config-if)# ip address pppoe setroute
  ```

  または、IP アドレスを手動で入力して PPPoE を有効化することができます。

  ip address *ip_address mask* **pppoe**

  例：

  ```
  ciscoasa(config-if)# ip address 10.1.1.78 255.255.255.0 pppoe
  ```

  setroute オプションを指定すると、PPPoE クライアントが接続をまだ確立していない場合に、デフォルトルートが設定されます。**setroute** オプションを使用する場合は、スタティックに定義されたルートをコンフィギュレーションに含めることはできません。

  （注） 2 つのインターフェイス（プライマリとバックアップのインターフェイスなど）で PPPeE が有効化されているときに、デュアル ISP サポートを設定しない場合、ASA では、最初のインターフェイスに限り、IP アドレスを取得するためにトラフィックを送信できます。

ステップ 4 セキュリティ レベルを設定します。

security-level *number*

例：

```
ciscoasa(config-if)# security-level 50
```

number には、0（最下位）～ 100（最上位）の整数を指定します。

ステップ 5 （オプション）インターフェイスを管理専用モードに設定してトラフィックが通過しないようにします。

management-only

デフォルトでは、管理インターフェイスは管理専用として設定されます。

例

次に、VLAN 101 のパラメータの設定例を示します。

```
ciscoasa(config)# interface vlan 101
ciscoasa(config-if)# nameif inside
ciscoasa(config-if)# security-level 100
ciscoasa(config-if)# ip address 10.1.1.1 255.255.255.0
```

次に、マルチコンテキストモードでコンテキストコンフィギュレーションにパラメータを設定する例を示します。インターフェイス ID はマップ名です。

```
ciscoasa/contextA(config)# interface int1
ciscoasa/contextA(config-if)# nameif outside
ciscoasa/contextA(config-if)# security-level 100
ciscoasa/contextA(config-if)# ip address 10.1.2.1 255.255.255.0
```

関連トピック

IPv6 アドレスの設定 （537 ページ）
物理インターフェイスのイネーブル化およびイーサネット パラメータの設定 （471 ページ）
PPPoE の設定 （530 ページ）

PPPoE の設定

インターフェイスが DSL、ケーブル モデム、またはその他の手段で ISP に接続されていて、ISP が PPPoE を使用して IP アドレスを割り当てる場合は、次のパラメータを設定します。

手順

ステップ 1 この接続を表す任意のバーチャルプライベート ダイヤルアップ ネットワーク（VPDN）グループ名を定義します。

vpdn group *group_name* **request dialout pppoe**

例：

```
ciscoasa(config)# vpdn group pppoe-sbc request dialout pppoe
```

ステップ 2 ISP が認証を要求する場合は、認証プロトコルを選択します。

vpdn group *group_name* **ppp authentication** {**chap** | **mschap** | **pap**}

例：

```
ciscoasa(config)# vpdn group pppoe-sbc ppp authentication chap
```

ISP で使用する認証方式に応じた適切なキーワードを入力します。

CHAP または MS-CHAP を使用する場合は、ユーザ名がリモート システム名として参照され、パスワードが CHAP シークレットとして参照されます。

ステップ 3 ISP で割り当てられたユーザ名を VPDN グループに関連付けます。

vpdn group *group_name* **localname** *username*

例：

```
ciscoasa(config)# vpdn group pppoe-sbc localname johncrichton
```

ステップ 4 PPPoE 接続用のユーザ名とパスワードのペアを作成します。

vpdn username *username* **password** *password* [**store-local**]

例：

```
ciscoasa(config)# vpdn username johncrichton password moya
```

store-local オプションを指定すると、ユーザ名とパスワードが ASA の NVRAM の特別な場所に保存されます。Auto Update Server が **clear config** コマンドを ASA に送信し、その後に接続が中断された場合、ASA は、ユーザ名とパスワードを NVRAM から読み取り、アクセス コンセントレータに対して再認証できます。

トランスペアレントモードの ブリッジグループインターフェイスの設定

ブリッジ グループは、ASA がルーティングではなくブリッジするインターフェイスのグループです。 ブリッジグループはトランスペアレント ファイアウォール モードでのみサポートされています。ブリッジグループの詳細については、ブリッジグループについて（177 ページ）を参照してください。

ブリッジ グループと関連インターフェイスを設定するには、次の手順を実行します。

ブリッジ仮想インターフェイス（BVI）の設定

ブリッジ グループごとに、IP アドレスを設定する BVI が必要です。ASA は、ブリッジ グループから発信されるパケットの送信元アドレスとしてこの IP アドレスを使用します。BVI IP ア

ドレスは、接続されているネットワークと同じサブネット上になければなりません。IPv4 トラフィックの場合、すべてのトラフィックを通過させるには、BVI IP アドレスが必要です。IPv6 トラフィックの場合は、少なくとも、トラフィックを通過させるリンクローカルアドレスを設定する必要があります。リモート管理などの管理操作を含めたフル機能を実現するために、グローバル管理アドレスを設定することを推奨します。

一部のモデルでは、デフォルト コンフィギュレーションにブリッジ グループと BVI が含まれています。追加のブリッジグループおよびBVIを作成して、グループの間でメンバーインターフェイスを再割り当てすることもできます。

（注） トランスペアレントモードの個別の管理インターフェイスでは（サポートされているモデルの場合）、設定できないブリッジグループ（ID 301）がコンフィギュレーションに自動的に追加されます。このブリッジ グループはブリッジ グループの制限に含まれません。

手順

ステップ 1 BVI を作成します。

interface bvi *bridge_group_number*

例：

```
ciscoasa(config)# interface bvi 2
```

bridge_group_number は、1 ～ 250 の整数です。このブリッジ グループ メンバーには、後で物理インターフェイスを割り当てます。

ステップ 2 BVI の IP アドレスを指定します。

ip address *ip_address* [*mask*] [**standby** *ip_address*]

例：

```
ciscoasa(config-if)# ip address 10.1.3.1 255.255.255.0 standby 10.1.3.2
```

BVI にはホスト アドレス（/32 または 255.255.255.255）を割り当てないでください。また、/30 サブネットなど（255.255.255.252）、ホストアドレスが 3 つ未満の他のサブネットを使用しないでください（ホストアドレスは、アップストリーム ルータ、ダウンストリーム ルータ、BVI にそれぞれ 1 つずつです）。ASA は、サブネットの先頭アドレスと最終アドレスで送受信されるすべての ARP パケットをドロップします。このため、/30 サブネットを使用し、このサブネットからアップストリーム ルータに予約済みアドレスを割り当てると、ASA はダウンストリーム ルータからアップストリーム ルータへの ARP 要求をドロップします。

フェールオーバーには、**standby** キーワードおよびアドレスを使用します。

例

次の例では、BVI 2 アドレスとスタンバイ アドレスを設定します。

```
ciscoasa(config)# interface bvi 2
ciscoasa(config-if)# ip address 10.1.3.1 255.255.255.0 standby 10.1.3.2
```

ブリッジ グループ メンバーの一般的なインターフェイス パラメータの設定

この手順は、ブリッジ グループ メンバー インターフェイスの名前、セキュリティ レベル、およびブリッジ グループを設定する方法について説明します。

始める前に

- 同じブリッジグループで、さまざまな種類のインターフェイス（物理インターフェイス、VLAN サブインターフェイス、VNI インターフェイス、EtherChannel、冗長インターフェイス）を含めることができます。管理インターフェイスはサポートされていません。
- マルチ コンテキスト モードでは、コンテキスト実行スペースで次の手順を実行します。システム コンフィギュレーションからコンテキスト コンフィギュレーションに切り替えるには、**changeto context** *name* コマンドを入力します。
- トランスペアレント モードの場合、管理インターフェイスにはこの手順を使用しないでください。管理インターフェイスを設定する場合は、トランスペアレント モードの管理インターフェイスの設定 （534 ページ）を参照してください。

手順

ステップ 1 インターフェイス コンフィギュレーション モードを開始します。

interface *id*

例：

```
ciscoasa(config)# interface gigabitethernet 0/0
```

インターフェイス ID には、次のものがあります。

- **冗長**
- **port-channel**
- *physical*：**ethernet**、**gigabitethernet**、**tengigabitethernet** など。管理インターフェイスはサポートされていません。インターフェイス名については、使用しているモデルのハードウェア インストール ガイドを参照してください。

- *physical*.*subinterface*：**gigabitethernet0/0.100** など。
- **vni**
- **vlan**
- *mapped_name*：マルチ コンテキスト モードの場合。

ステップ 2 インターフェイスをブリッジ グループに割り当てます。

bridge-group *number*

例：

```
ciscoasa(config-if)# bridge-group 1
```

number は 1 ~ 250 の整数で、BVI インターフェイス番号に一致する必要があります。ブリッジ グループには最大 4 個のインターフェイスを割り当てることができます。同一インターフェイスを複数のブリッジ グループに割り当てることはできません。

ステップ 3 インターフェイスの名前を指定します。

nameif *name*

例：

```
ciscoasa(config-if)# nameif inside1
```

name は最大 48 文字のテキスト文字列です。大文字と小文字は区別されません。名前を変更するには、このコマンドで新しい値を再入力します。その名前を参照するすべてのコマンドが削除されるため、**no** 形式は入力しないでください。

ステップ 4 セキュリティ レベルを設定します。

security-level *number*

例：

```
ciscoasa(config-if)# security-level 50
```

number には、0（最下位）～ 100（最上位）の整数を指定します。

関連トピック

MTUおよび TCP MSS の設定 （560 ページ）

トランスペアレント モードの管理インターフェイスの設定

トランスペアレント ファイアウォール モードでは、すべてのインターフェイスがブリッジ グループに属している必要があります。唯一の例外は管理インターフェイス（物理インターフェイス、サブインターフェイス（ご使用のモデルでサポートされている場合）、または管理イン

ターフェイスを構成するEtherChannelインターフェイス（複数の管理インターフェイスがある場合）のいずれか）です。管理インターフェイスは個別の管理インターフェイスとして設定できます。Firepower 9300 シャーシ では、管理インターフェイス ID は ASA 論理デバイスに割り当てた mgmt タイプ インターフェイスに基づいています。他のインターフェイス タイプは管理インターフェイスとして使用できません。シングルモードまたはコンテキストごとに1つの管理インターフェイスを設定できます。詳細については、トランスペアレントモードの管理インターフェイス （468 ページ）を参照してください。

始める前に

- このインターフェイスをブリッジ グループに割り当てないでください。設定できないブリッジグループ（ID 301）は、コンフィギュレーションに自動的に追加されます。このブリッジ グループはブリッジ グループの制限に含まれません。
- モデルに管理インターフェイスが含まれていない場合、データ インターフェイスからトランスペアレント ファイアウォールを管理する必要があります。この手順はスキップします。（たとえば、ASASM の場合。）Firepower 9300 シャーシ では、管理インターフェイス ID は ASA 論理デバイスに割り当てた mgmt-type インターフェイスに基づいています。
- マルチ コンテキスト モードでは、どのインターフェイスも（これには管理インターフェイスも含まれます）、コンテキスト間で共有させることはできません。データ インターフェイスに接続する必要があります。
- マルチ コンテキスト モードでは、コンテキスト実行スペースで次の手順を実行します。システムからコンテキスト コンフィギュレーションに変更するには、**changeto context** *name* コマンドを入力します。

手順

ステップ 1 インターフェイス コンフィギュレーション モードを開始します。

interface {{**port-channel** *number* | **management** *slot*/*port* | *mgmt-type_interface_id* }[**.** *subinterface*] | *mapped_name*}

例：

```
ciscoasa(config)# interface management 0/0.1
```

port-channel *number* 引数は、**port-channel 1** などの EtherChannel インターフェイス ID です。EtherChannelインターフェイスには、管理メンバーインターフェイスのみが設定されている必要があります。

冗長インターフェイスは、Management *slot*/*port* インターフェイスをメンバとしてサポートしません。ただし、管理インターフェイス以外の複数インターフェイスからなる冗長インターフェイスを、管理専用として設定できます。

マルチ コンテキスト モードで、**allocate-interface** コマンドを使用して割り当てた場合、*mapped_name* を入力します。

Firepower 9300 シャーシでは、ASA 論理デバイスに割り当てた mgmt タイプ インターフェイス（個別インターフェイスまたは EtherChannel インターフェイス）のインターフェイス ID を指定します。

ステップ 2 インターフェイスの名前を指定します。

nameif *name*

例：

```
ciscoasa(config-if)# nameif management
```

name は最大 48 文字のテキスト文字列です。大文字と小文字は区別されません。名前を変更するには、このコマンドで新しい値を再入力します。その名前を参照するすべてのコマンドが削除されるため、**no** 形式は入力しないでください。

ステップ 3 次のいずれかの方法を使用して IP アドレスを設定します。

- IP アドレスを手動で設定します。

  フェールオーバーとともに使用する場合は、IP アドレスとスタンバイ アドレスを手動で設定する必要があります。DHCP はサポートされません。

  ip_address 引数および *mask* 引数には、インターフェイスの IP アドレスとサブネット マスクを設定します。

  standby *ip_address* 引数は、フェールオーバーで使用します。

  ip address *ip_address* [*mask*] [**standby** *ip_address*]

  例：

  ```
  ciscoasa(config-if)# ip address 10.1.1.1 255.255.255.0 standby 10.1.1.2
  ```

- DHCP サーバから IP アドレスを取得します。

  ip address dhcp [**setroute**]

  例：

  ```
  ciscoasa(config-if)# ip address dhcp
  ```

  setroute キーワードを指定すると、ASA が DHCP サーバから渡されたデフォルト ルートを使用できるようになります。

  DHCP リースをリセットし、新規リースを要求するには、このコマンドを再入力します。

  ip address dhcp コマンドを入力する前に、no shutdown コマンドを使用してインターフェイスを有効化していない場合、一部の DHCP 要求が送信されないことがあります。

ステップ 4 セキュリティ レベルを設定します。

security-level *number*

例：

```
ciscoasa(config-if)# security-level 100
```

number には、0（最下位）～ 100（最上位）の整数を指定します。

IPv6 アドレスの設定

この項では、IPv6 アドレッシングを設定する方法について説明します。

IPv6 について

このセクションには、IPv6 に関する情報が含まれています。

IPv6 アドレス指定

次の 2 種類の IPv6 のユニキャスト アドレスを設定できます。

- グローバル：グローバル アドレスは、パブリック ネットワークで使用可能なパブリック アドレスです。ブリッジ グループの場合、このアドレスは各メンバー インターフェイスごとに設定するのではなく、BVI用に設定する必要があります。また、トランスペアレント モードで管理インターフェイスのグローバルな IPv6 アドレスを設定することもできます。
- リンクローカル：リンクローカルアドレスは、直接接続されたネットワークだけで使用できるプライベート アドレスです。ルータは、リンクローカル アドレスを使用してパケットを転送するのではなく、特定の物理ネットワーク セグメント上で通信だけを行います。ルータは、アドレス設定またはアドレス解決などの Neighbor Discovery 機能に使用できます。ブリッジ グループでは、メンバー インターフェイスのみがリンクローカル アドレスを所有しています。BVI にはリンクローカル アドレスはありません。

最低限、IPv6 が動作するようにリンクローカル アドレスを設定する必要があります。グローバル アドレスを設定すると、リンクローカル アドレスがインターフェイスに自動的に設定されるため、リンクローカル アドレスを個別に設定する必要はありません。ブリッジ グループ インターフェイスでは、BVI でグローバル アドレスを設定した場合、ASA が自動的にメンバー インターフェイスのリンクローカル アドレスを生成します。グローバル アドレスを設定しない場合は、リンクローカル アドレスを自動的にするか、手動で設定する必要があります。

（注） リンクローカル アドレスの設定だけを行う場合は、コマンド リファレンスの **ipv6 enable** コマンド（自動設定）または **ipv6 address link-local** コマンド（手動設定）を参照してください。

Modified EUI-64 インターフェイス ID

RFC 3513「Internet Protocol Version 6 (IPv6) Addressing Architecture」（インターネット プロトコル バージョン 6 アドレッシング アーキテクチャ）では、バイナリ値 000 で始まるものを除き、すべてのユニキャスト IPv6 アドレスのインターフェイス識別子部分は長さが 64 ビットで、Modified EUI-64 形式で組み立てることが要求されています。ASA では、ローカル リンクに接続されたホストにこの要件を適用できます。

この機能がインターフェイスでイネーブルになっていると、そのインターフェイス ID が Modified EUI-64 形式を採用していることを確認するために、インターフェイスで受信した IPv6 パケットの送信元アドレスが送信元 MAC アドレスに照らして確認されます。IPv6 パケットがインターフェイス ID に Modified EUI-64 形式を採用していない場合、パケットはドロップされ、次のシステム ログ メッセージが生成されます。

```
325003: EUI-64 source address check failed.
```

アドレス形式の確認は、フローが作成される場合にのみ実行されます。既存のフローからのパケットは確認されません。また、アドレスの 確認はローカル リンク上のホストに対してのみ実行できます。

グローバル IPv6 アドレスの設定

ルーテッド モードの任意のインターフェイスとトランスペアレント モードの BVI に対してグローバル IPv6 アドレスを設定するには、次の手順を実行します。

（注） グローバルアドレスを設定すると、リンクローカルアドレスは自動的に設定されるため、別々に設定する必要はありません。

サブインターフェイスの場合、親インターフェイスの同じ Burned-In MAC Address を使用するので、MAC アドレスも手動で設定することをお勧めします。IPv6 リンクローカル アドレスは MAC アドレスに基づいて生成されるため、サブインターフェイスに一意の MAC アドレスを割り当てることで、一意の IPv6 リンクローカル アドレスが可能になり、ASA で特定のインスタンスでのトラフィックの中断を避けることができます。を参照してください。MAC アドレスの手動設定 （557 ページ）

始める前に

- マルチ コンテキスト モードでは、コンテキスト実行スペースで次の手順を実行します。システム コンフィギュレーションからコンテキスト コンフィギュレーションに切り替えるには、**changeto context** *name* コマンドを入力します。

手順

ステップ 1 インターフェイス コンフィギュレーション モードを開始します。

interface *id*

例：

```
ciscoasa(config)# interface gigabithethernet 0/0
```

トランスペアレント モードの場合、BVI を指定します。

例：

```
ciscoasa(config)# interface bvi 1
```

トランスペアレントモードでは、BVIに加え、管理インターフェイスを指定することもできます。

例：

```
ciscoasa(config)# interface management 1/1
```

ステップ 2 （ルーテッド インターフェイス）次のいずれかの方法を使用して IP アドレスを設定します。

- インターフェイスでステートレスな自動設定をイネーブルにします。

  ipv6 address autoconfig

  インターフェイスでステートレスな自動設定をイネーブルにすると、ルータ アドバタイズメント メッセージで受信したプレフィックスに基づいて IPv6 アドレスが設定されます。ステートレスな自動設定がイネーブルになっている場合、インターフェイスのリンクローカル アドレスは、Modified EUI-64 インターフェイス ID に基づいて自動的に生成されます。

  （注） RFC 4862 では、ステートレスな自動設定に設定されたホストはルータ アドバタイズメントメッセージを送信しないと規定していますが、ASAはこの場合、ルータ アドバタイズメント メッセージを送信します。メッセージを抑制するには、**ipv6 nd suppress-ra** コマンドを参照してください。

- インターフェイスに手動でグローバル アドレスを割り当てます。

  ipv6 address *ipv6_address*/*prefix-length* [**standby** *ipv6_address*]

  例：

  ```
  ciscoasa(config-if)# ipv6 address 2001:0DB8:BA98::3210/64 standby 2001:0DB8:BA98::3211
  ```

  グローバル アドレスを割り当てると、インターフェイスのリンクローカル アドレスが自動的に作成されます。

standbyは、フェールオーバーペアのセカンダリ ユニットまたはフェールオーバー グループで使用されるインターフェイス アドレスを指定します。

- Modified EUI-64 形式を使用してインターフェイスの MAC アドレスから生成されたインターフェイス ID と、指定されたプレフィックスを結合することによって、インターフェイスにグローバル アドレスを割り当てます。

  ipv6 address *ipv6-prefix*/*prefix-length* **eui-64**

  例：

  ```
  ciscoasa(config-if)# ipv6 address 2001:0DB8:BA98::/64 eui-64
  ```

  グローバル アドレスを割り当てると、インターフェイスのリンクローカル アドレスが自動的に作成されます。

  スタンバイ アドレスを指定する必要はありません。インターフェイス ID が自動的に生成されます。

ステップ 3 （BVIインターフェイス）BVIに手動でグローバルアドレスを割り当てます。トランスペアレント モードの管理インターフェイスでも、この方法を使用します。

ipv6 address *ipv6_address*/*prefix-length* [**standby** *ipv6_address*]

例：

```
ciscoasa(config-if)# ipv6 address 2001:0DB8::BA98:0:3210/48
```

グローバル アドレスを割り当てると、インターフェイスのリンクローカル アドレスが自動的に作成されます。

standby は、フェールオーバー ペアのセカンダリ ユニットまたはフェールオーバー グループで使用されるインターフェイス アドレスを指定します。

ステップ 4 （オプション）ローカル リンクの IPv6 アドレスに Modified EUI-64 形式のインターフェイス識別子の使用を適用します。

ipv6 enforce-eui64 *if_name*

例：

```
ciscoasa(config)# ipv6 enforce-eui64 inside
```

if_name 引数には、**nameif** コマンドで指定したインターフェイスの名前を指定します。このインターフェイスに対してアドレス形式を適用できます。

IPv6 ネイバー探索の設定

IPv6 ネイバー探索プロセスは、ICMPv6 メッセージおよび送信要求ノード マルチキャスト アドレスを使用して、同じネットワーク（ローカル リンク）上のネイバーのリンク層アドレスを決定し、ネイバーの読み出し可能性を確認し、隣接ルータを追跡します。

ノード（ホスト）はネイバー探索を使用して、接続リンク上に存在することがわかっているネイバーのリンク層アドレスの特定や、無効になったキャッシュ値の迅速なパージを行います。また、ホストはネイバー探索を使用して、ホストに代わってパケットを転送しようとしている隣接ルータを検出します。さらに、ノードはこのプロトコルを使用して、どのネイバーが到達可能でどのネイバーがそうでないかをアクティブに追跡するとともに、変更されたリンク層アドレスを検出します。ルータまたはルータへのパスが失敗すると、ホストは機能している代替ルータまたは代替パスをアクティブに検索します。

-

手順

ステップ 1 設定する IPv6 インターフェイスを指定します。

interface *name*

例：

```
ciscoasa(config)# interface gigabitethernet 0/0
ciscoasa(config-if)#
```

ステップ 2 重複アドレス検出（DAD）の試行回数を指定します。

ipv6 nd dad attempts *value*

value 引数の有効な値の範囲は 0 ～ 600 です。この値が 0 の場合、指定されたインターフェイスでの DAD 処理が無効化されます。デフォルト値は 1 件です。

DAD は、割り当てられる前に、新しいユニキャスト IPv6 アドレスの一意性を確認し、ネットワークに重複する IPv6 アドレスが検出されていないかをリンク ベースで確認します。ASA は、ネイバー送信要求メッセージを使用して、DAD を実行します。

重複アドレスが検出されると、そのアドレスの状態は DUPLICATE に設定され、アドレスは使用対象外となり、次のエラー メッセージが生成されます。

```
325002: Duplicate address ipv6_address/MAC_address on interface
```

重複アドレスがインターフェイスのリンクローカルアドレスであれば、インターフェイス上で IPv6 パケットの処理はディセーブルになります。重複アドレスがグローバル アドレスであれば、そのアドレスは使用されません。

例：

```
ciscoasa(config-if)# ipv6 nd dad attempts 20
```

ステップ 3 IPv6 ネイバー送信要求の再送信する間隔を設定します。

ipv6 nd ns-interval *value*

value 引数の有効な値は、1000 ～ 3600000 ミリ秒です。

ローカル リンク上にある他のノードのリンクレイヤ アドレスを検出するため、ノードからネイバー送信要求メッセージ（ICMPv6 Type 135）がローカル リンクに送信されます。ネイバー送信要求メッセージを受信すると、宛先ノードは、ネイバー アドバタイズメント メッセージ（ICPMv6 Type 136）をローカル リンク上に送信して応答します。

送信元ノードがネイバーアドバタイズメントを受信すると、送信元ノードと宛先ノードが通信できるようになります。ネイバー送信要求メッセージは、ネイバーのリンク層アドレスが識別された後に、ネイバーの到達可能性の確認にも使用されます。ノードがネイバーの到達可能性を確認するときに、ネイバー送信要求メッセージの宛先アドレスは、ネイバーのユニキャストアドレスです。

ネイバー アドバタイズメント メッセージは、ローカル リンク上のノードのリンク層アドレスが変更されたときにも送信されます。

例：

```
ciscoasa(config-if)# ipv6 nd ns-interval 9000
```

ステップ 4 リモートの IPv6 ノードに到達可能な時間を設定します。

ipv6 nd reachable-time *value*

value 引数の有効な値は、0 ～ 3600000 ミリ秒です。value に 0 を使用すると、到達可能時間が判定不能として送信されます。到達可能時間の値を設定し、追跡するのは、受信デバイスの役割です。

ネイバー到達可能時間を設定すると、使用できないネイバーを検出できます。時間を短く設定すると、使用できないネイバーをより早く検出できます。ただし、時間を短くするほど、IPv6 ネットワーク帯域幅とすべての IPv6 ネットワーク デバイスの処理リソースの消費量が増えます。通常の IPv6 の運用では、あまり短い時間設定は推奨できません。

例：

```
ciscoasa config-if)# ipv6 nd reachable-time 1700000
```

ステップ 5 IPv6 ルータ アドバタイズメントの送信間隔を設定します。

ipv6 nd ra-interval [**msec**] *value*

msec キーワードは、この値がミリ秒単位で指定されることを示します。このキーワードが存在しない場合、値は秒単位で指定されます。*value* 引数の有効な値の範囲は 3 ～ 1800 秒、**msec** キーワードが指定されている場合は 500 ～ 1800000 ミリ秒です。デフォルトは 200 秒です。

送信間隔の値は、このインターフェイスから送信されるすべての IPv6 ルータ アドバタイズメントに含まれます。

ASA がデフォルト ルータとして設定されている場合、送信間隔は IPv6 ルータ アドバタイズメント ライフタイム以下にする必要があります。他の IPv6 ノードと同期しないようにするには、使用する実際値を必要値の 20 % 以内にランダムに調整します。

例：

```
ciscoasa(config-if)# ipv6 nd ra-interval 201
```

ステップ 6 ローカル リンク上のノードが、ASA をリンク上のデフォルト ルータと見なす時間の長さを指定します。

ipv6 nd ra-lifetime [**msec**] *value*

オプションの **msec** キーワードは、この値がミリ秒単位で指定されることを示します。このキーワードを指定しない場合、値は秒単位です。*value* 引数の有効な値は 0 ～ 9000 秒です。0 を入力すると、ASA は選択したインターフェイスのデフォルト ルータと見なされません。

ルータの有効期間の値は、このインターフェイスから送信されるすべての IPv6 ルータ アドバタイズメントに含まれます。この値は、このインターフェイス上のデフォルト ルータとしての ASA の有用性を示します。

例：

```
ciscoasa(config-if)# ipv6 nd ra-lifetime 2000
```

ステップ 7 ルータ アドバタイズメントを抑制します。

ipv6 nd suppress-ra

ルータ要請メッセージ（ICMPv6 Type 133）に応答して、ルータ アドバタイズメント メッセージ（ICMPv6 Type 134）が自動的に送信されます。ルータ送信要求メッセージは、ホストからシステムの起動時に送信されるため、ホストは、次にスケジュールされているルータ アドバタイズメント メッセージを待つことなくただちに自動設定を行うことができます。

ASA で IPv6 プレフィックスを提供する必要がないインターフェイス（外部インターフェイスなど）では、これらのメッセージをディセーブルにできます。

このコマンドを入力すると、ASA がリンク上では IPv6 ルータではなく、通常の IPv6 ネイバーのように見えるようになります。

ステップ 8 取得されるステートレス自動設定のアドレス以外の IPv6 アドレスの取得に DHCPv6 を使用するように IPv6 自動設定クライアントに通知するには、IPv6 ルータ アドバタイズメントにフラグを追加します。

ipv6 nd managed-config-flag

このオプションは、IPv6 ルータ アドバタイズメント パケットの管理対象アドレス設定フラグを設定します。

ステップ 9 DNS サーバ アドレスや他の情報の取得に DHCPv6 を使用するように IPv6 自動設定クライアントに通知するには、IPv6 ルータ アドバタイズメントにフラグを追加します。

ipv6 nd other-config-flag

このオプションは、IPv6 ルータ アドバタイズメント パケットのその他のアドレス設定フラグを設定します。

ステップ 10 IPv6 ルータ アドバタイズメントに含める IPv6 プレフィックスを設定します。

ipv6 nd prefix {*ipv6_prefix*/*prefix_length* |**default**} [*valid_lifetime preferred_lifetime* | **at** *valid_date preferred_date*] [**no-advertise**] [**no-autoconfig**] [ ] [**off-link**]

ネイバー デバイスは、プレフィックス アドバタイズメントを使用して、そのインターフェイス アドレスを自動設定できます。ステートレス自動設定では、ルータ アドバタイズメント メッセージで提供される IPv6 プレフィックスを使用して、リンクローカル アドレスからグローバル ユニキャスト アドレスを作成します。

デフォルトでは、**ipv6 address** コマンドを使用してインターフェイスにアドレスとして設定されるプレフィックスは、ルータ アドバタイズメントでアドバタイズされます。**ipv6 nd prefix** コマンドを使用してプレフィックスをアドバタイズメント用に設定すると、これらのプレフィックスだけがアドバタイズされます。

ステートレス自動設定が正しく機能するには、ルータ アドバタイズメント メッセージでアドバタイズされるプレフィックス長が常に 64 ビットでなければなりません。

- **default**: デフォルトのプレフィックスが使用されていることを示します。
- *valid_lifetime preferred_lifetime* ：指定した IPv6 プレフィックスを有効かつ優先されるものとしてアドバタイズする時間を指定します。優先の有効期間中には、アドレスの制限はありません。優先有効期間を過ぎると、アドレスは廃止状態になります。廃止状態のアドレスの使用は推奨されませんが、固く禁じられているわけではありません。有効期間の期限が切れた後に、アドレスは無効になり、使用できません。有効ライフタイムは優先ライフタイムと同じかそれより長い必要があります。値の範囲は 0 ～ 4294967295 秒です。最大値は無限ですが、これは **infinite** キーワードを使用して指定することもできます。デフォルトの有効期間は 2592000（30 日間）です。デフォルトの優先有効期間は 604800（7 日間）です。
- **at** *valid_date preferred_date*：プレフィックスの有効期限が切れる特定の日付と時刻を示します。日付は *month_name day hh*:*mm* と指定します。たとえば、**dec 1 13:00** と入力します。
- **no-advertise**：プレフィックスのアドバタイズメントを無効にします。
- **no-autoconfig**：プレフィックスは IPv6 自動設定には使用できないことを指定します。
- **off-link**：指定したプレフィックスをオフリンクとして設定します。プレフィクスはLビットクリアでアドバタイズされます。プレフィックスは、接続されたプレフィックスとしてルーティング テーブルに挿入されません。

onlink がオン（デフォルト）のときは、指定されたプレフィックスがそのリンクに割り当てられます。指定されたプレフィックスを含むそのようなアドレスにトラフィックを送信するノードは、宛先がリンク上でローカルに到達可能であると見なします。

例：

```
ciscoasa(config-if)# ipv6 nd prefix 2001:DB8::/32 1000 900
```

ステップ 11 IPv6 ネイバー探索キャッシュのスタティック エントリを設定します。

ipv6 neighbor *ipv6_address if_name mac_address*

次のガイドラインと制限事項は、スタティック IPv6 ネイバーの設定に適用されます。

- **ipv6 neighbor** コマンドは **arp** コマンドに似ています。IPv6 ネイバー探索プロセスによる学習を通して、指定された IPv6 アドレスのエントリがネイバー探索キャッシュにすでに存在する場合、エントリは自動的にスタティック エントリに変換されます。これらのエントリは、copy コマンドを使用して設定を保存するときに設定に保存されます。
- IPv6 ネイバー探索キャッシュのスタティック エントリを表示するには、**show ipv6 neighbor** コマンドを使用します。
- **clear ipv6 neighbor** コマンドにより、スタティック エントリを除く、IPv6 ネイバー探索キャッシュ内のすべてのエントリを削除します。**no ipv6 neighbor** コマンドは、指定したスタティック エントリをネイバー探索キャッシュから削除します。このコマンドは、IPv6 ネイバー探索プロセスから認識されるエントリであるダイナミック エントリはキャッシュから削除しません。**no ipv6 enable** コマンドを使用してインターフェイスで IPv6 をディセーブルにすると、スタティック エントリを除いて、そのインターフェイス用に設定されたすべての IPv6 ネイバー探索キャッシュ エントリが削除されます（エントリの状態が INCMP [Incomplete] に変更されます）。
- IPv6 ネイバー探索キャッシュ内のスタティック エントリがネイバー探索プロセスによって変更されることはありません。
- **clear ipv6 neighbor** コマンドを実行しても、スタティック エントリが IPv6 ネイバー探索キャッシュから削除されることはありません。ダイナミック エントリのクリアだけが行われます。
- 生成された ICMP syslog は、IPv6 ネイバー エントリの定期的な更新に起因します。IPv6 ネイバー エントリの ASA デフォルト タイマーは 30 秒であるため、ASA は 30 秒おきに ICMPv6 ネイバー探索および応答パケットを生成します。ASA にフェールオーバー LAN および IPv6 アドレスで設定された状態インターフェイスの両方がある場合は、30 秒ごとに、ICMPv6 ネイバー探索および応答パケットが、設定済みのリンクローカル IPv6 アドレスの 両方の ASA で生成されます。また、各パケットは複数の syslog（ICMP 接続およびローカル ホストの作成またはティアダウン）を生成するため、連続 ICMP syslog が生成されているように見えることがあります。IPV6 ネイバー エントリのリフレッシュ時間は、通常のデータ インターフェイスに設定可能ですが、フェールオーバー インターフェイスでは設定可能ではありません。ただし、この ICMP ネイバー探索トラフィックの CPU の影響はわずかです。

例：

```
ciscoasa(config)# ipv6 neighbor 3001:1::45A inside 002.7D1A.9472
```

ルーテッドモードおよびトランスペアレントモードのインターフェイスのモニタリング

インターフェイスの統計情報、ステータス、PPPoE をモニタできます。

インターフェイス統計情報

- **show interface**

  インターフェイス統計情報を表示します。

- **show interface ip brief**

  インターフェイスの IP アドレスとステータスを表示します。

- **show bridge-group**

  指定されたインターフェイス、MAC アドレスと IP アドレスなどのブリッジグループ情報を表示します。

PPPoE

- **show ip address** *interface_name* **pppoe**

  現在の PPPoE クライアントの設定情報を表示します。

- **debug pppoe** {**event** | **error** | **packet**}

  PPPoE クライアントのデバッグをイネーブルにします。

- **show vpdn session**[**l2tp** |**pppoe**] [**id** *sess_id* |**packets** |**state** | **window**]

  PPPoE セッションのステータスを表示します。

  次に、このコマンドで提供される情報例を示します。

```
ciscoasa# show vpdn

Tunnel id 0, 1 active sessions
     time since change 65862 secs
     Remote Internet Address 10.0.0.1
    Local Internet Address 199.99.99.3
     6 packets sent, 6 received, 84 bytes sent, 0 received
Remote Internet Address is 10.0.0.1
     Session state is SESSION_UP
```

```
       Time since event change 65865 secs, interface outside
       PPP interface id is 1
       6 packets sent, 6 received, 84 bytes sent, 0 received
ciscoasa#
ciscoasa# show vpdn session
PPPoE Session Information (Total tunnels=1 sessions=1)
Remote Internet Address is 10.0.0.1
  Session state is SESSION_UP
    Time since event change 65887 secs, interface outside
    PPP interface id is 1
    6 packets sent, 6 received, 84 bytes sent, 0 received
ciscoasa#
ciscoasa# show vpdn tunnel
PPPoE Tunnel Information (Total tunnels=1 sessions=1)
Tunnel id 0, 1 active sessions
   time since change 65901 secs
   Remote Internet Address 10.0.0.1
   Local Internet Address 199.99.99.3
   6 packets sent, 6 received, 84 bytes sent, 0 received
ciscoasa#
```

IPv6 ネイバー探索

IPv6 ネイバー探索パラメータをモニタするには、次のコマンドを入力します。

- **show ipv6 interface**

  このコマンドは、「外部」などのインターフェイス名を含む、IPv6 用に設定されているインターフェイスのユーザビリティ状態を表示し、指定されたインターフェイスの設定を表示します。しかし、このコマンドは名前を除外し、IPv6 が有効になっているすべてのインターフェイスの設定を表示します。コマンドの出力では、次の項目が表示されます。

  - インターフェイスの名前とステータス
  - リンクローカルおよびグローバルなユニキャスト アドレス
  - インターフェイスが属するマルチキャスト グループ
  - ICMP リダイレクトおよびエラー メッセージの設定
  - ネイバー探索の設定
  - コマンドが 0 に設定されているときの実際の時間
  - 使用されているネイバー探索の到達可能時間

ルーテッドモードおよびトランスペアレントモードのインターフェイスの例

2 つのブリッジグループを含むトランスペアレント モードの例

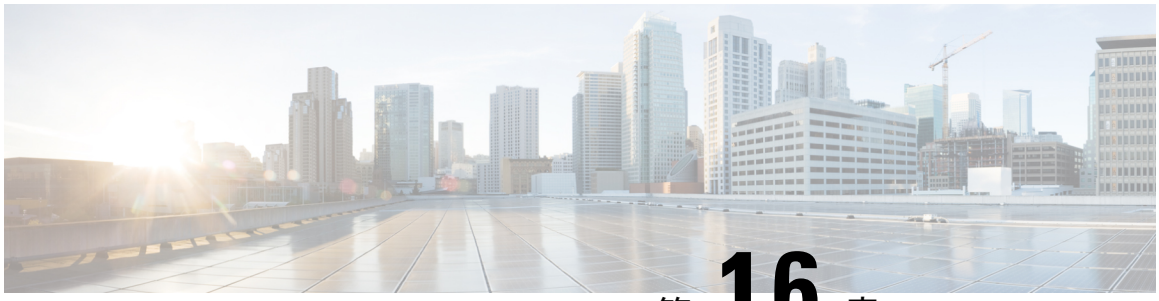
トランスペアレント モードの次の例では、3 つのインターフェイスそれぞれの 2 つのブリッジグループと管理専用インターフェイスを示します。

```
interface gigabitethernet 0/0
  nameif inside1
  security-level 100
  bridge-group 1
  no shutdown
interface gigabitethernet 0/1
  nameif outside1
  security-level 0
  bridge-group 1
  no shutdown
interface gigabitethernet 0/2
  nameif dmz1
  security-level 50
  bridge-group 1
  no shutdown
interface bvi 1
  ip address 10.1.3.1 255.255.255.0 standby 10.1.3.2

interface gigabitethernet 1/0
  nameif inside2
  security-level 100
  bridge-group 2
  no shutdown
interface gigabitethernet 1/1
  nameif outside2
  security-level 0
  bridge-group 2
  no shutdown
interface gigabitethernet 1/2
  nameif dmz2
  security-level 50
  bridge-group 2
  no shutdown
interface bvi 2
  ip address 10.3.5.8 255.255.255.0 standby 10.3.5.9

interface management 0/0
  nameif mgmt
  security-level 100
  ip address 10.2.1.1 255.255.255.0 standby 10.2.1.2
  no shutdown
```

ルーテッドモードおよびトランスペアレントモードのインターフェイスの履歴

機能名	プラットフォーム リリース	機能情報
IPv6 ネイバー探索	7.0(1)	この機能が導入されました。 **ipv6 nd ns-interval**、**ipv6 nd ra-lifetime**、**ipv6 nd suppress-ra**、**ipv6 neighbor**、**ipv6 nd prefix**、**ipv6 nd dad-attempts**、**ipv6 nd reachable-time**、**ipv6 address**、および **ipv6 enforce-eui64** コマンドが導入されました。
トランスペアレント モードの IPv6 のサポート	8.2(1)	トランスペアレント ファイアウォール モードの IPv6 サポートが導入されました。
トランスペアレント モードのブリッジ グループ	8.4(1)	セキュリティ コンテキストのオーバーヘッドを避けたい場合、またはセキュリティ コンテキストを最大限に使用したい場合、インターフェイスをブリッジ グループにグループ化し、各ネットワークに 1 つずつ複数のブリッジ グループを設定できます。ブリッジ グループのトラフィックは他のブリッジ グループから隔離されます。シングル モードまたはコンテキストごとに、それぞれ 4 つのインターフェイスからなる最大 8 個のブリッジ グループを設定できます。 次のコマンドが導入されました。**interface bvi**、**show bridge-group**
IPv6 DHCP リレーのアドレス設定フラグ	9.0(1)	コマンド **ipv6 nd managed-config-flag**、**ipv6 nd other-config-flag** が導入されました。

機能名	プラットフォーム リリース	機能情報
トランスペアレントモードのブリッジグループの最大数が 250 に増加	9.3(1)	ブリッジグループの最大数が 8 個から 250 個に増えました。シングル モードでは最大 250 個、マルチ モードではコンテキストあたり最大 8 個のブリッジグループを設定でき、各ブリッジ グループには最大 4 個のインターフェイスを追加できます。 **interface bvi** および **bridge-group** コマンドが変更されました。



第 16 章

高度なインターフェイス設定

この章では、インターフェイスのMACアドレスを設定する方法、最大伝送ユニット（MTU）を設定する方法、TCP最大セグメントサイズ（TCP MSS）を設定する方法、および同じセキュリティ レベルの通信を許可する方法について説明します。最高のネットワーク パフォーマンスを実現するには、正しい MTU と最大 TCP セグメント サイズの設定が不可欠です。

高度なインターフェイス設定について

この項では、インターフェイスの高度な設定について説明します。

MAC アドレスについて

手動で MAC アドレスを割り当ててデフォルトをオーバーライドできます。マルチコンテキストモードでは、（コンテキストに割り当てられているすべてのインターフェイスの）一意の MAC アドレスと。

（注） 親インターフェイスと同じ組み込みのMACアドレスを使用するので、ASA で定義されたサブインターフェイスに一意の MAC アドレスを割り当てることもできます。たとえば、サービスプロバイダーによっては、MAC アドレスに基づいてアクセス コントロールを実行する場合があります。また、IPv6 リンクローカル アドレスはMACアドレスに基づいて生成されるため、サブインターフェイスに一意のMACアドレスを割り当てることで、一意のIPv6リンクローカル アドレスが可能になり、ASA で特定のインスタンスでのトラフィックの中断を避けることができます。

デフォルトの MAC アドレス

デフォルトの MAC アドレスの割り当ては、インターフェイスのタイプによって異なります。

- 物理インターフェイス：物理インターフェイスは、Burned-in MAC Address を使用します。
- 冗長インターフェイス：冗長インターフェイスでは、最初に追加された物理インターフェイスの MAC アドレスが使用されます。構成でメンバー インターフェイスの順序を変更すると、MAC アドレスがリストの先頭にあるインターフェイスの MAC アドレスと一致するように変更されます。冗長インターフェイスに MAC アドレスを割り当てると、メンバー インターフェイスの MAC アドレスに関係なく、割り当てた MAC アドレスが使用されます。
- EtherChannel（Firepower Models）：EtherChannel の場合は、そのチャネル グループに含まれるすべてのインターフェイスが同じ MAC アドレスを共有します。この機能によって、EtherChannel はネットワーク アプリケーションとユーザに対してトランスペアレントになります。ネットワーク アプリケーションやユーザから見えるのは 1 つの論理接続のみであり、個々のリンクのことは認識しないからです。ポート チャネル インターフェイスは、プールからの一意の MAC アドレスを使用します。インターフェイスのメンバーシップは、MAC アドレスには影響しません。
- EtherChannel（ASA モデル）：ポート チャネル インターフェイスは、最も小さいチャネル グループ インターフェイスの MAC アドレスをポート チャネル MAC アドレスとして使用します。または、ポート チャネル インターフェイスの MAC アドレスを設定することもできます。グループ チャネル インターフェイスのメンバーシップが変更された場合に備えて、一意の MAC アドレスを設定することを推奨します。ポートチャネル MAC アドレスを提供していたインターフェイスを削除すると、そのポートチャネルの MAC アドレスは次に番号が小さいインターフェイスに変わるため、トラフィックが分断されます。
- サブインターフェイス：物理インターフェイスのすべてのサブインターフェイスは同じ Burned-In MAC Address を使用します。サブインターフェイスに一意の MAC アドレスを割り当てることが必要になる場合があります。たとえば、サービス プロバイダーによっては、MAC アドレスに基づいてアクセス コントロールを実行する場合があります。また、IPv6 リンクローカル アドレスは MAC アドレスに基づいて生成されるため、サブインターフェイスに一意の MAC アドレスを割り当てることで、一意の IPv6 リンクローカル アドレスが可能になり、ASA で特定のインスタンスでのトラフィックの中断を避けることができます。
- ASASM VLAN：ASASM では、すべての VLAN がバックプレーンから提供される同じ MAC アドレスを使用します。

自動 MAC アドレス

マルチ コンテキスト モードでは、自動生成によって一意の MAC アドレスがコンテキストに割り当てられているすべてのインターフェイスに割り当てられます。

MAC アドレスを手動で割り当てた場合、自動生成がイネーブルになっていても、手動で割り当てた MAC アドレスが使用されます。後で手動 MAC アドレスを削除すると、自動生成されたアドレスが使用されます（有効になっている場合）。

生成した MAC アドレスがネットワーク内の別のプライベート MAC アドレスと競合することがまれにあります。この場合は、インターフェイスの MAC アドレスを手動で設定できます。

自動生成されたアドレス（プレフィックスを使用するとき）は A2 で始まるため、自動生成も使用する予定のときは手動 MAC アドレスを A2 で始めることはできません。

ASA は、次の形式を使用して MAC アドレスを生成します。

A2*xx.yyzz.zzzz*

xx.yy はユーザ定義プレフィックスまたはインターフェイス MAC アドレスの最後の 2 バイトに基づいて自動生成されるプレフィックスです。*zz.zzzz* は ASA によって生成される内部カウンタです。スタンバイ MAC アドレスの場合、内部カウンタが 1 増えることを除けばアドレスは同じです。

プレフィックスの使用方法を示す例の場合、プレフィックス 77 を設定すると、ASA は 77 を 16 進数値 004D（*yyxx*）に変換します。MAC アドレスで使用すると、プレフィックスは ASA ネイティブ形式に一致するように逆にされます（*xxyy*）。

A24**D.00***zz.zzzz*

プレフィックス 1009（03F1）の場合、MAC アドレスは次のようになります。

A2**F1.03***zz.zzzz*

（注） プレフィックスのない MAC アドレス形式は従来のバージョンです。従来の形式に関する詳細については、コマンド リファレンスの **mac-address auto** コマンドを参照してください。

MTU について

MTU は、ASA が特定のイーサネット インターフェイスで送信する最大フレームペイロードサイズを指定します。MTU の値は、イーサネット ヘッダー、VLAN タギング、他のオーバーヘッドを含まないフレーム サイズです。たとえば、MTU を 1500 に設定すると、予想されるフレーム サイズは、ヘッダーを含めて 1518 バイトです。または、VLAN を使用している場合は、1522 バイトです。これらのヘッダーに対応するために MTU 値を高く設定しないでください。

VXLAN については、イーサネット データグラム全体がカプセル化されるため、新しい IP パケットにより大きな MTU が必要です。ASA VTEP 送信元インターフェイスの MTU を 54 バイト以上のネットワーク MTU に設定する必要があります。

『Path MTU Discovery』

ASA は、Path MTU Discovery（RFC 1191 の定義に従う）をサポートします。つまり、2 台のホスト間のネットワーク パス内のすべてのデバイスで MTU を調整できます。したがってパスの最小 MTU の標準化が可能です。

デフォルト MTU

ASA のデフォルト MTU は、1500 バイトです。この値には、イーサネット ヘッダー、VLAN タギングや他のオーバーヘッドのための 18～22 バイト以上は含まれません。

VTEP 送信元インターフェイスの VXLAN を有効にし、MTU が 1554 バイト未満の場合、ASA は自動的に MTU を 1554 バイトに増やします。この場合、イーサネット データグラム全体がカプセル化されるため、新しいパケットにはより大きな MTU が必要です。一般的には、ASA ソースインターフェイス MTU をネットワーク MTU + 54 バイトに設定する必要があります。

MTU とフラグメンテーション

IPv4 では、出力 IP パケットが指定された MTU より大きい場合、2 つ以上のフレームにフラグメント化されます。フラグメントは送信先（場合によっては中継先）で組立て直されますが、フラグメント化はパフォーマンス低下の原因となります。IPv6 では、通常、パケットはフラグメント化を許可されていません。したがってフラグメント化を避けるために、IP パケットを MTU サイズ以内に収める必要があります。

TCP パケットでは、通常、エンドポイントは MTU を使用して TCP の最大セグメント サイズ（たとえば、MTU - 40）を判別します。途中で追加の TCP ヘッダーが追加された場合（たとえば、サイト間 VPN トンネル）、TCP MSS はトンネリング エンティティで下方調整しないといけない場合があります。TCP MSS について （555 ページ）を参照してください。

UDP または ICMP では、フラグメンテーションを回避するために、アプリケーションは MTU を考慮する必要があります。

（注） ASA はメモリに空きがある限り、設定された MTU よりも大きいフレームを受信できます。

MTU とジャンボ フレーム

より大きな MTU は、より大きなパケットの送信が可能です。より大きなパケットは、ネットワークにとってより効率的な場合があります。次のガイドラインを参照してください。

- トラフィック パスの MTU の一致：すべての ASA インターフェイスとトラフィック パス内のその他のデバイスのインターフェイスでは、MTU が同じになるように設定することを推奨します。MTU の一致により、中間デバイスでのパケットのフラグメント化が回避できます。
- ジャンボ フレームに対応する：ジャンボ フレームを有効にすると、MTU を最大 9198 バイトに設定できます。最大値は、Firepower 9300 シャーシ の ASAv で 9000、ASA です。

（注） ASA 5585-X とFirepower 9300では、VLAN タギングを使用している場合、最大 MTU は 4 バイト小さいです：ASA 5585-X では 9194、Firepower 9300 では 8996 です。

TCP MSS について

最大セグメント サイズ（TCP MSS）とは、あらゆる TCP および IP ヘッダーが追加される前の TCP ペイロードのサイズです。UDP パケットは影響を受けません。接続を確立するときのスリーウェイ ハンドシェイク中に、クライアントとサーバは TCP MSS 値を交換します。

を参照してください。デフォルトでは、最大 TCP MSS は 1380 バイトに設定されます。この設定は、ASA が IPsec VPN カプセル化のパケットサイズを追加する必要がある場合に役立ちます。ただし、非 IPsec エンドポイントでは、ASA の最大 TCP MSS を無効にする必要があります。

最大 TCP MSS を設定している場合、接続のいずれかのエンドポイントが ASA に設定された値を超える TCP MSS を要求すると、ASA は要求パケット内の TCP MSS を ASA の最大サイズで上書きします。ホストまたはサーバが TCP MSS を要求しない場合、ASA は RFC 793 のデフォルト値 536 バイト（IPv4）または 1220 バイト（IPv6）を想定しますが、パケットは変更しません。たとえば、MTU をデフォルトの 1500 バイトのままにします。ホストは、1500 バイトの MSS から TCP および IP のヘッダー長を減算して、MSS を 1460 バイトに設定するように要求します。ASA の最大 TCP MSS が 1380（デフォルト）の場合、ASA は TCP 要求パケットの MSS 値を 1380 に変更します。その後、サーバは、1380 バイトのペイロードを含むパケットを送信します。ASA は、最大 120 バイトのヘッダーをパケットに追加しても、1500 バイトの MTU サイズに適応することができます。

TCP の最小 MSS も設定できます。ホストまたはサーバが非常に小さい TCP MSS を要求した場合、ASAは値を調整します。デフォルトでは、最小 TCP MSS は有効ではありません。

SSL VPN 接続用を含め、to-the-box トラフィックの場合、この設定は適用されません。ASA は MTU を使用して、TCP MSS を導き出します。MTU - 40（IPv4）または MTU - 60（IPv6）となります。

デフォルト TCP MSS

デフォルトでは、ASA の最大 TCP MSS は 1380 バイトです。このデフォルトは、ヘッダーが最大 120 バイトの IPv4 IPsec VPN 接続に対応しています。この値は、MTU の デフォルトの 1500 バイト内にも収まっています。

TCP MSS の推奨最大設定

デフォルトでは TCP MSS は、ASA が IPv4 IPsec VPN エンドポイントとして機能し、MTU が 1500 バイトであることを前提としています。ASA が IPv4 IPsec VPN エンドポイントとして機能している場合は、最大 120 バイトの TCP および IP ヘッダーに対応する必要があります。

MTU 値を変更して、IPv6 を使用するか、または IPsec VPN エンドポイントとして ASA を使用しない場合は、FlexConfig の Sysopt_Basic オブジェクトを使用して TCP MSS 設定を参照してください。次のガイドラインを参照してください。

- 通常のトラフィック：TCP MSS の制限を無効にし、接続のエンドポイント間で確立された値を受け入れます。通常、接続エンドポイントは MTU から TCP MSS を取得するため、非 IPsec パケットは通常この TCP MSS を満たしています。

- IPv4 IPsec エンドポイント トラフィック：最大 TCP MSS を MTU - 120 に設定します。たとえば、ジャンボ フレームを使用しており、MTU を 9000 に設定すると、新しい MTU を使用するために、TCP MSS を 8880 に設定する必要があります。
- IPv6 IPsec エンドポイント トラフィック：最大 TCP MSS を MTU - 140 に設定します。

インターフェイス間通信

同じセキュリティ レベルのインターフェイスで相互通信を許可する利点としては、次のものがあります。

- 101 より多い数の通信インターフェイスを設定できます。

  各インターフェイスで異なるセキュリティ レベルを使用したときに、同一のセキュリティ レベルにインターフェイスを割り当てないと、各レベル（0 ～ 100）に 1 つのインターフェイスしか設定できません。

- ACL がなくても同じセキュリティ レベルのインターフェイスすべての間で自由にトラフィックが流れるようにできます。

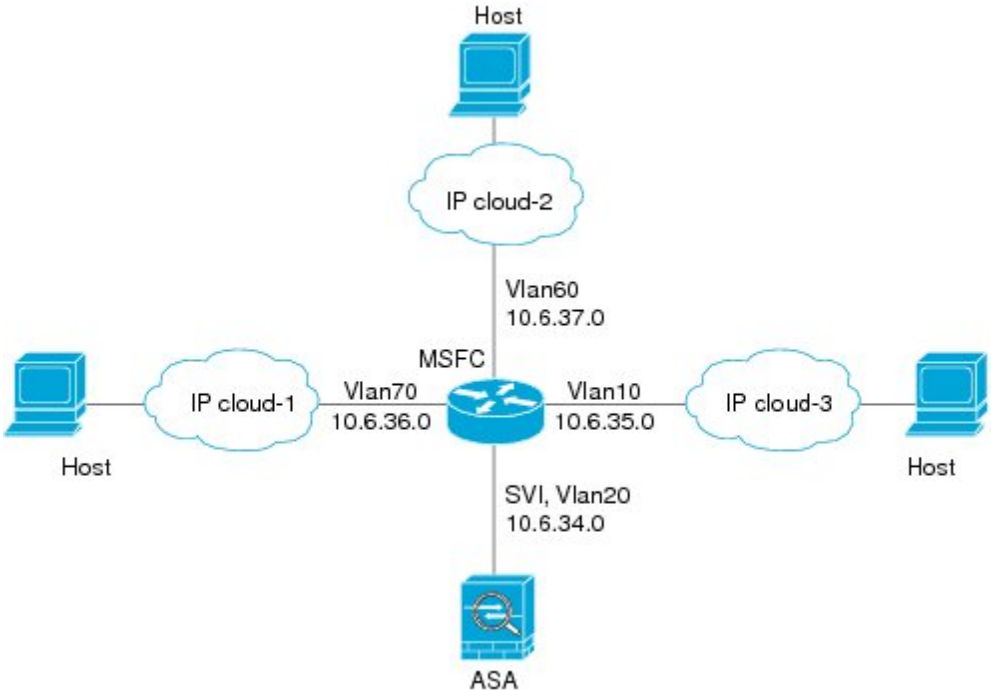
同じセキュリティ インターフェイス通信をイネーブルにした場合でも、異なるセキュリティ レベルで通常どおりインターフェイスを設定できます。

インターフェイス内通信（ルーテッド ファイアウォール モード）

インターフェイス内通信は、インターフェイスに入ってくる VPN トラフィックに対して使用できますが、その場合は同じインターフェイスのルートから外されます。この場合、VPN トラフィックは暗号化解除されたり、別の VPN 接続のために再度暗号化されたりする場合があります。たとえば、ハブアンドスポーク VPN ネットワークがあり、ASA がハブ、リモート VPN ネットワークがスポークの場合、あるスポークが別のスポークと通信するためには、トラフィックは ASA に入ってから他のスポークに再度ルーティングされる必要があります。

（注） この機能で許可されたすべてのトラフィックは、引き続きファイアウォール規則に従います。リターン トラフィックが ASA を通過できない原因となるため、非対称なルーティング状態にしないよう注意してください。

ASASM の場合、この機能をイネーブルにするには、まず、パケットがスイッチ経由で宛先ホストに直接送信されるのではなく、ASA の MAC アドレスに送信されるように、MSFC を正しく設定する必要があります。次の図に、同一インターフェイス上のホストが通信する必要があるネットワークを示します。



次の設定例では、 次の図に示すネットワークのポリシー ルーティングをイネーブルにするために使用される Cisco IOS **route-map** コマンドを示します。

```
route-map intra-inter3 permit 0
  match ip address 103
  set interface Vlan20
  set ip next-hop 10.6.34.7
!
route-map intra-inter2 permit 20
  match ip address 102
  set interface Vlan20
  set ip next-hop 10.6.34.7
!
route-map intra-inter1 permit 10
  match ip address 101
  set interface Vlan20
  set ip next-hop 10.6.34.7
```

MAC アドレスの手動設定

MAC アドレスを手動で割り当てる必要がある場合は、この手順を使用して実行できます。

親インターフェイスと同じ組み込みの MAC アドレスを使用するので、ASA で定義されたサブインターフェイスに一意の MAC アドレスを割り当てることもできます。たとえば、サービス プロバイダーによっては、MAC アドレスに基づいてアクセス コントロールを実行する場合があります。また、IPv6 リンクローカル アドレスは MAC アドレスに基づいて生成されるため、サブインターフェイスに一意の MAC アドレスを割り当てることで、一意の IPv6 リンクローカ

ル アドレスが可能になり、ASA で特定のインスタンスでのトラフィックの中断を避けることができます。

始める前に

マルチ コンテキスト モードでは、コンテキスト実行スペースで次の手順を実行します。システム コンフィギュレーションからコンテキスト コンフィギュレーションに切り替えるには、**changeto context** *name* コマンドを入力します。

手順

ステップ 1 インターフェイス コンフィギュレーション モードを開始します。

interface *id*

例：

```
ciscoasa(config)# interface gigabithethernet 0/0
```

ステップ 2 プライベート MAC アドレスをこのインターフェイスに割り当てます。

mac-address *mac_address* [**standby** *mac_address*]

例：

```
ciscoasa(config-if)# mac-address 000C.F142.4CDE
```

mac_address は、H.H.H 形式で指定します。H は 16 ビットの 16 進数です。たとえば、MAC アドレス 00-0C-F1-42-4C-DE は、000C.F142.4CDE と入力します。MAC アドレスはマルチキャスト ビット セットを持つことはできません。つまり、左から 2 番目の 16 進数字を奇数にすることはできません。

自動生成された MAC アドレスも使用する場合、手動で割り当てる MAC アドレスの最初の 2 バイトには A2 を使用できません。

フェールオーバーで使用する場合は、**スタンバイ** MAC アドレスを設定します。アクティブ装置がフェールオーバーし、スタンバイ装置がアクティブになると、新しいアクティブ装置はアクティブな MAC アドレスの使用を開始して、ネットワークの切断を最小限に抑えます。一方、古いアクティブ装置はスタンバイ アドレスを使用します。

マルチ コンテキスト モードでの MAC アドレスの自動割り当て

この項では、MAC アドレスの自動生成の設定方法について説明します。マルチ コンテキスト モードの場合、この機能によって、コンテキストに割り当てられたすべてのインターフェイス タイプに一意の MAC アドレスが割り当てられます。

始める前に

- インターフェイスの **nameif** コマンドを設定すると、ただちに新規 MAC アドレスが生成されます。インターフェイスを設定した後でこの機能をイネーブルにした場合は、イネーブルにした直後に、すべてのインターフェイスの MAC アドレスが生成されます。この機能をディセーブルにすると、各インターフェイスの MAC アドレスはデフォルトの MAC アドレスに戻ります。たとえば、GigabitEthernet 0/1 のサブインターフェイスは GigabitEthernet 0/1 の MAC アドレスを使用するようになります。
- 生成した MAC アドレスがネットワーク内の別のプライベート MAC アドレスと競合することがまれにあります。この場合は、インターフェイスの MAC アドレスを手動で設定できます。
- マルチ コンテキスト モードでは、システム実行スペースで次の手順を実行します。コンテキストからシステム実行スペースに切り替えるには、**changeto system** コマンドを入力します。

手順

プライベート MAC アドレスを各インターフェイスに自動的に割り当てます。

mac-address auto [**prefix** *prefix*]

プレフィックスを入力しない場合は、ASA によって、インターフェイス MAC アドレスの最後の 2 バイトに基づいてプレフィックスが自動生成されます。

手動でプレフィックスを入力する場合は、*prefix* に 0 ～ 65535 の 10 進数値を指定します。このプレフィックスは 4 桁の 16 進数値に変換され、MAC アドレスの一部として使用されます。

例：

```
ciscoasa(config)# mac-address auto prefix 19
```

MTUおよび TCP MSS の設定

始める前に

- マルチ コンテキスト モードでは、コンテキスト実行スペースで次の手順を実行します。システム コンフィギュレーションからコンテキスト コンフィギュレーションに切り替えるには、**changeto context** *name* コマンドを入力します。
- MTU を 1500 より多く増やすには、ジャンボ フレーム サポートの有効化 （474 ページ）に従って、ジャンボ フレームをイネーブルにします。 ジャンボ フレームはデフォルトで ASASM でサポートされるため、この機能をイネーブルにする必要はありません。

手順

ステップ 1 MTU を 300 ～ 9198（ASAv の場合は 9000、Firepower 9300 シャーシ の場合は ）バイトの範囲で設定します

mtu *interface_name bytes*

例：

```
ciscoasa(config)# mtu inside 9000
```

デフォルトは 1500 バイトです。

（注） 冗長インターフェイスまたはポートチャネル インターフェイスに MTU を設定すると、ASA は、この設定をすべてのメンバー インターフェイスに適用します。

ジャンボ フレームをサポートする多くのモデルでは、インターフェイスに 1500 よりも大きな値を入力する場合、ジャンボ フレームのサポートをイネーブルにする必要があります。「ジャンボ フレーム サポートの有効化 （474 ページ）」を参照してください。

（注） VLAN タギングを使用する場合、ASA 5585-X および Firepower 9300 シャーシ の最大値は 4 バイト少なくなります。したがって、ASA 5585-X の場合は 9194、Firepower 9300 シャーシ の場合は 8996 になります。ASA では MTU の値を 9195 ～ 9198 に設定できますが、実際のペイロードのサイズは 9194 になります。

ステップ 2 最大 TCP セグメント サイズをバイト単位で設定します（48 ～任意の最大値）。

sysopt connection tcpmss [**minimum**] *bytes*

例：

```
ciscoasa(config)# sysopt connection tcpmss 8500
ciscoasa(config)# sysopt connection tcpmss minimum 1290
```

デフォルト値は1380バイトです。この機能は、0バイトに設定することによってディセーブルにできます。

minimal キーワードには、48 ～ 65535 の間のバイト数未満にならないように最大セグメントサイズを設定します。minimum 機能は、デフォルトでディセーブルです（0 に設定）。

ステップ 3 [ASA Cluster] 設定については、マスターユニットでのインターフェイスの設定（362 ページ）を参照してください。

例

下記の例では、ジャンボ フレームをイネーブルにし、すべてのインターフェイスの MTU を増加し、非 VPN トラフィックの TCP MSS をディセーブルにします（TCP MSS を 0 に設定、すなわち無制限とすることによって行います）。

```
jumbo frame-reservation
mtu inside 9198
mtu outside 9198
sysopt connection tcpmss 0
```

下記の例では、ジャンボ フレームをイネーブルにし、すべてのインターフェイスの MTU を増加し、VPN トラフィックの TCP MSS を 9078 に変更します（MTU から 120 を差し引きます）。

```
jumbo frame-reservation
mtu inside 9198
mtu outside 9198
sysopt connection tcpmss 9078
```

同一のセキュリティ レベル通信の許可

デフォルトでは、同じセキュリティ レベルのインターフェイスは相互に通信することができません。また、パケットは同じインターフェイスを出入りすることができません。この項では、複数のインターフェイスが同じセキュリティ レベルの場合にインターフェイス間通信をイネーブルにする方法と、インターフェイス内通信をイネーブルにする方法について説明します。

手順

ステップ 1 相互通信を可能にするために同じセキュリティ レベルのインターフェイスをイネーブルにします。

same-security-traffic permit inter-interface

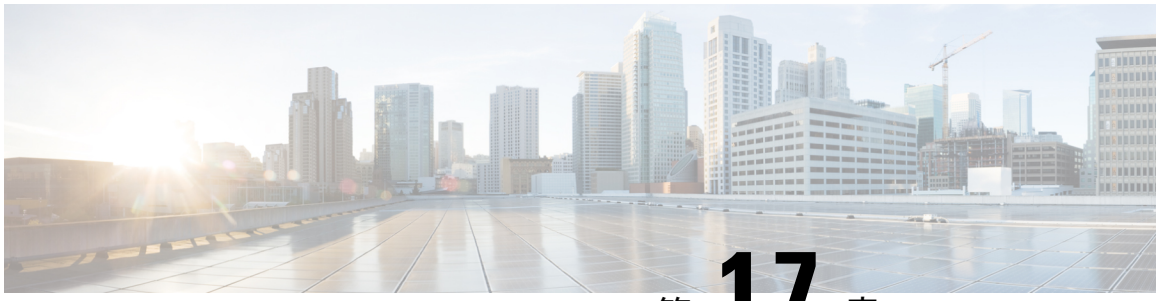
ステップ 2 同じインターフェイスに接続されたホスト間の通信をイネーブルにします。

same-security-traffic permit intra-interface

インターフェイスの詳細設定の履歴

表 *20*：インターフェイスの詳細設定の履歴

機能名	リリース	機能情報
最大 MTU が 9198 バイトになりました	9.1(6)、9.2(1)	ASA で使用できる最大の MTU は 9198 バイトです（CLI のヘルプでご使用のモデルの正確な最大値を確認してください）。この値にはレイヤ 2 ヘッダーは含まれません。以前は、ASA で 65535 バイトの最大 MTU を指定できましたが、これは不正確であり、問題が発生する可能性がありました。9198 よりも大きいサイズに MTU を設定している場合は、アップグレード時に MTU のサイズが自動的に削減されます。場合によっては、この MTU の変更により MTU の不一致が発生する可能性があります。接続している機器が新しい MTU 値を使用するように設定されていることを確認してください。 次のコマンドが変更されました。**mtu**



第 17 章

トラフィック ゾーン

トラフィック ゾーンに複数のインターフェイスを割り当てることができます。これにより、既存のフローのトラフィックがゾーン内のインターフェイスで ASA に出入りできるようになります。この機能により、ASA 上での等コスト マルチパス（ECMP）のルーティングや、ASA へのトラフィックの複数のインターフェイスにわたる外部ロードバランシングが可能になります。

トラフィック ゾーンの概要

この項では、ネットワークでトラフィック ゾーンを使用する方法について説明します。

ゾーン分割されていない動作

アダプティブセキュリティアルゴリズムは、トラフィックの許可または拒否を決定する際に、パケットの状態を考慮します。フローに適用されたパラメータの1つは、トラフィックが同じインターフェイスに出入りすることです。異なるインターフェイスに入る既存のフローのトラフィックは、ASA によってドロップされます。

トラフィック ゾーンにより、複数のインターフェイスを 1 つにまとめることができるため、ゾーン内の任意のインターフェイスに出入りするトラフィックがアダプティブ セキュリティ アルゴリズムのセキュリティ チェックを満たすことができるようになります。

関連トピック

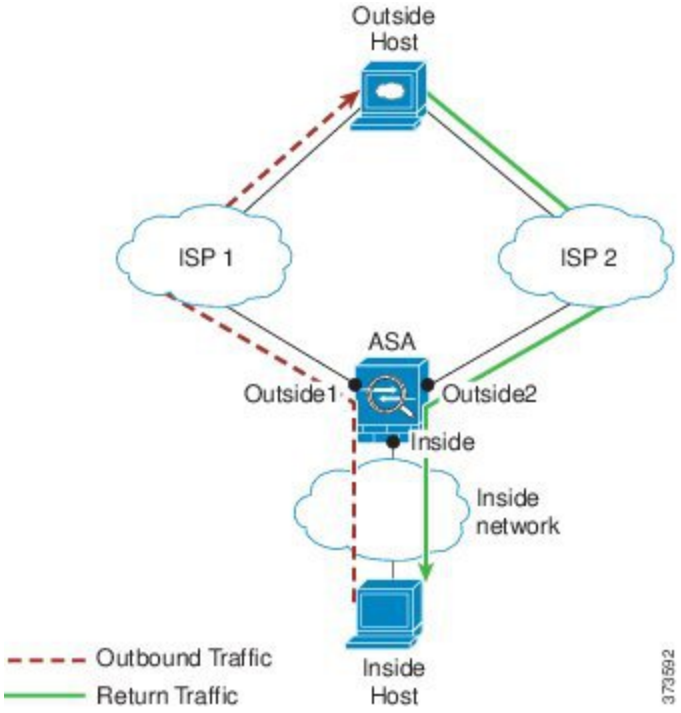
ステートフル インスペクションの概要 （17 ページ）

ゾーンを使用する理由

ゾーンを使用して、複数のルーティングのシナリオに対応することができます。

非対称ルーティング

次のシナリオでは、Outside1 インターフェイスの ISP 1 を経由する内部ホストと外部ホストの間に接続が確立されています。宛先ネットワークの非対称ルーティングが原因で、Outside2 インターフェイスの ISP 2 からリターン トラフィックが到達しています。

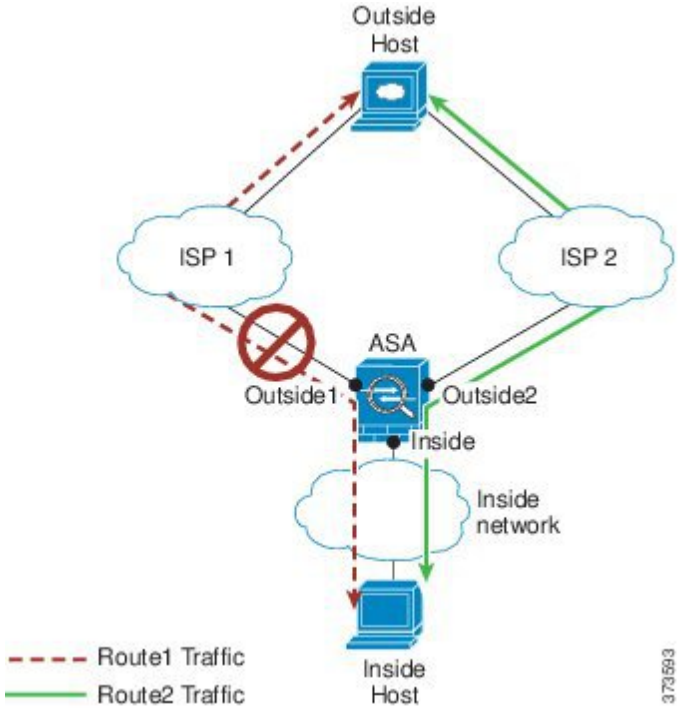


ゾーン分割されていない場合の問題：ASA は、インターフェイスごとに接続テーブルを保持します。リターン トラフィックが Outside2 に到達すると、そのトラフィックは、接続テーブルに一致しないため、ドロップされます。ASA クラスタに関しては、クラスタが同一ルータに対して複数の隣接関係（アジャセンシー）を持つ場合、非対称ルーティングは許容できないトラフィック紛失の原因となることがあります。

ゾーン分割されたソリューション：ASAは、ゾーンごとに接続テーブルを保持します。Outside1 と Outside2 を 1 つのゾーンにグループ化した場合、リターン トラフィックが Outside2 に到達すると、ゾーンごとの接続テーブルに一致するため、接続が許可されます。

紛失したルート

次のシナリオでは、Outside1 インターフェイスの ISP 1 を経由する内部ホストと外部ホストの間に接続が確立されています。Outside1 と ISP 1 間でルートが紛失または移動したため、トラフィックは ISP 2 を経由する別のルートを通る必要があります。

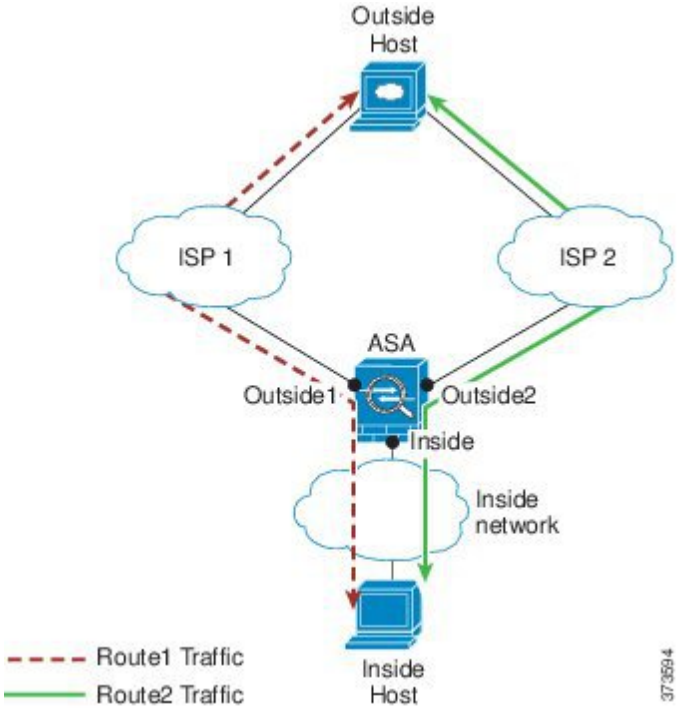


ゾーン分割されていない場合の問題：内部ホストと外部ホスト間の接続が削除されるため、新しい次善のルートを使用して新しい接続を確立する必要があります。UDP の場合、1 つのパケットがドロップダウンすると新しいルートが使用され、UDP がない場合は、新しい接続を再確立する必要があります。

ゾーン分割されたソリューション：ASA は、紛失したルートを検出し、フローを ISP 2 経由の新しいパスに切り替えます。トラフィックは、パケットがドロップすることなくシームレスに転送されます。

ロード バランシング

次のシナリオでは、Outside1 インターフェイスの ISP 1 を経由する内部ホストと外部ホストの間に接続が確立されています。2 番目の接続が Outside2 の ISP 2 を経由する等コスト ルートを介して確立されています。



ゾーン分割されていない場合の問題：インターフェイス間でロードバランシングを行うことができません。可能なのは、1つのインターフェイスの等コストルートによるロードバランスだけです。

ゾーン分割されたソリューション：ASAは、ゾーン内のすべてのインターフェイスで最大8つの等コスト ルート間の接続をロードバランスすることができます。

ゾーンごとの接続テーブルおよびルーティング テーブル

ASAは、トラフィックがゾーンのインターフェイスのいずれかに到達できるようにゾーンごとの接続テーブルを保持します。また、ASAは、ECMPサポート用にゾーンごとのルーティングテーブルも保持します。

ECMP ルーティング

ASA では、等コスト マルチパス（ECMP）ルーティングをサポートしています。

ゾーン分割されていない ECMP サポート

ゾーンがない場合は、インターフェイスごとに最大8つの等コストのスタティック ルートタまたはダイナミック ルートを設定できます。たとえば、次のように異なるゲートウェイを指定する外部インターフェイスに 3 つのデフォルト ルートを設定できます。

```
route outside 0 0 10.1.1.2
route outside 0 0 10.1.1.3
```

```
route outside 0 0 10.1.1.4
```

この場合、トラフィックは、10.1.1.2、10.1.1.3 と 10.1.1.4 間の外部インターフェイスでロードバランスされます。トラフィックは、送信元 IP アドレスおよび宛先 IP アドレスをハッシュするアルゴリズムに基づいて、指定したゲートウェイ間に分配されます。

ECMP は複数のインターフェイス間ではサポートされないため、異なるインターフェイスで同じ宛先へのルートを定義することはできません。上記のルートのいずれかを設定すると、次のルートは拒否されます。

```
route outside2 0 0 10.2.1.1
```

ゾーン分割された ECMP サポート

ゾーンがある場合は、ゾーン内の最大 8 つのインターフェイス間に最大 8 つの等コストのスタティック ルートまたはダイナミック ルートを設定できます。たとえば、次のようにゾーン内の 3 つのインターフェイ間に 3 つのデフォルト ルートを設定できます。

```
route outside1 0 0 10.1.1.2
route outside2 0 0 10.2.1.2
route outside3 0 0 10.3.1.2
```

同様に、ダイナミック ルーティング プロトコルは、自動的に等コスト ルートを設定できます。ASA では、より堅牢なロード バランシング メカニズムを使用してインターフェイス全体でトラフィックをロードバランスします。

ルートが紛失した場合、ASA はフローをシームレスに別のルートに移動させます。

接続のロード バランス方法

ASA では、パケットの 6 タプル（送信元 IP アドレス、宛先 IP アドレス、送信元ポート、宛先ポート、プロトコル、入力インターフェイス）から生成されたハッシュを使用して、等コスト ルート間の接続をロードバランスします。ルートが紛失しない限り、接続は接続期間中、インターフェイスで継続されます。

接続内のパケットは、ルート間でロードバランスされません。接続では、そのルートが紛失しない限り、単一ルートを使用します。

ASA では、ロード バランシング時にインターフェイス帯域幅やその他のパラメータを考慮しません。同じゾーン内のすべてのインターフェイスが MTU、帯域幅などの同じ特性を持つことを確認します。

ロード バランシング アルゴリズムは、ユーザ設定可能ではありません。

別のゾーンのルートへのフォール バック

ルートがインターフェイスで紛失したときにゾーン内で使用可能な他のルートがない場合、ASA では、異なるインターフェイス/ゾーンからのルートを使用します。このバックアップ

ルートを使用した場合、ゾーン分割されていないルーティングのサポートと同様にパケットのドロップが発生することがあります。

インターフェイスベースのセキュリティ ポリシーの設定

ゾーンを使用すると、トラフィックはゾーン内のすべてのインターフェイスで出入りを許可されますが、セキュリティ ポリシー自体（アクセス ルール、NAT など）は、ゾーン単位ではなく、インターフェイス単位で適用されます。ゾーン内のすべてのインターフェイスに同じセキュリティ ポリシーを設定すると、そのトラフィックの ECMP およびロード バランシングを適切に実装できます。必須のパラレルインターフェイス設定の詳細については、トラフィック ゾーンの前提条件 （570 ページ）を参照してください。

トラフィック ゾーンでサポートされるサービス

次のサービスがゾーンでサポートされています。

- アクセル ルール
- NAT
- QoS トラフィック ポリシングを除くサービス ルール。
- Routing

完全にゾーン分割されたサポートは利用できませんが、To-the-Box および From-the-Box トラフィック （569 ページ）に示した to-the-box サービスおよび from-the-box サービスを設定することもできます。

トラフィック ゾーンのインターフェイスに他のサービス（VPN、ボットネット トラフィック フィルタなど）を設定しないでください。これらのサービスは、想定どおりに機能または拡張しないことがあります。

（注） セキュリティ ポリシーの設定方法の詳細については、トラフィック ゾーンの前提条件 （570 ページ）を参照してください。

セキュリティ レベル

ゾーンに最初に追加するインターフェイスによってゾーンのセキュリティ レベルが決まります。追加のインターフェイスは、すべて同じセキュリティ レベルにする必要があります。ゾーン内のインターフェイスのセキュリティ レベルを変更するには、1 つのインターフェイスを除くすべてのインターフェイスを削除してからセキュリティ レベルを変更し、インターフェイスを再度追加します。

フローのプライマリおよび現在のインターフェイス

各接続フローは、最初の入出力インターフェイスに基づいて構築されます。これらのインターフェイスは、プライマリ インターフェイスです。

ルート変更または非対称ルーティングにより、新しい出力インターフェイスが使用されている場合は、新しいインターフェイスが現在のインターフェイスになります。

ゾーンの追加または削除

ゾーンにインターフェイスを割り当てる場合、そのインターフェイスのすべての接続が削除されます。接続を再確立する必要があります。

ゾーンからインターフェイスを削除する場合、そのインターフェイスをプライマリ インターフェイスとしているすべての接続が削除されます。接続を再確立する必要があります。そのインターフェイスが現在のインターフェイスの場合、ASA は接続をプライマリ インターフェイスに戻します。ゾーンのルート テーブルも更新されます。

ゾーン内トラフィック

トラフィックがあるインターフェイスに入り、同じゾーンの別のインターフェイスから出ることができるようにするには、**same-security permit intra-interface** コマンドをイネーブルにしてトラフィックが同じインターフェイスを出入りできるようにし、さらに、**same-security permit inter-interface** コマンドをイネーブルにして same-security インターフェイス間のトラフィックを許可します。このように設定しない場合、フローは同じゾーンの2つのインターフェイス間をルーティングできません。

To-the-Box および From-the-Box トラフィック

- management-only インターフェイスまたは management-access インターフェイスをゾーンに追加することはできません。
- ゾーンの通常のインターフェイスでの管理トラフィックでは、既存のフローの非対称ルーティングのみがサポートされます。ECMP サポートはありません。
- 1つのゾーン インターフェイスにのみ管理サービスを設定できますが、非対称ルーティング サポートを利用するには、すべてのインターフェイスでそれを設定する必要があります。構成がすべてのインターフェイスでパラレルである場合でも、ECMP はサポートされません。
- ASA は、ゾーンで次の To-the-Box および From-the-Box サービスをサポートします。
  - Telnet
  - SSH
  - HTTPS
  - SNMP

- Syslog

ゾーン内の IP アドレスのオーバーラップ

ゾーン分割されていないインターフェイスの場合、ASA では、NAT が正しく設定されていれば、インターフェイスでの IP アドレス ネットワークのオーバーラップをサポートします。ただし、同じゾーンのインターフェイスでは、ネットワークのオーバーラップはサポートされていません。

トラフィック ゾーンの前提条件

- 名前、IPアドレス、およびセキュリティ レベルを含むすべてのインターフェイスパラメータを設定します。ゾーンのすべてのインターフェイスでセキュリティ レベルが一致する必要があることに注意してください。帯域幅および他のレイヤ2のプロパティについては、インターフェイスのようにグループ化する計画を立てる必要があります。
- 次のサービスをゾーンのすべてのインターフェイスで一致するように設定します。
  - アクセス ルール：同じアクセス ルールをゾーンのすべてのメンバー インターフェイスに適用するか、グローバル アクセス ルールを使用します。

    次に例を示します。

    ```
    access-list ZONE1 extended permit tcp any host WEBSERVER1 eq 80
    access-group ZONE1 in interface outside1
    access-group ZONE1 in interface outside2
    access-group ZONE1 in interface outside3
    ```

  - NAT：ゾーンのすべてのメンバー インターフェイスで同じ NAT ポリシーを設定するか、グローバル NAT ルールを使用します（つまり、「any」を使用して NAT ルールでゾーンのインターフェイスを表します）。

    インターフェイス PAT はサポートされていません。

    次に例を示します。

    ```
    object network WEBSERVER1
      host 10.9.9.9 255.255.255.255
      nat (inside,any) static 209.165.201.9
    ```

（注） インターフェイス固有の NAT および PAT プールを使用したときに元のインターフェイスの障害が発生した場合、ASA は接続を切り替えることはできません。

インターフェイス固有の PAT プールを使用する場合、同じホストからの複数の接続は、別のインターフェイスにロードバランスし、別のマッピング IP アドレスを使用することがあります。この場合、複数の同時接続を使用するインターネット サービスが正しく機能しないことがあります。

- サービス ルール：グローバル サービス ポリシーを使用するか、ゾーンの各インターフェイスに同じポリシーを割り当てます。

  QoS トラフィック ポリシングはサポートされていません。

  次に例を示します。

```
service-policy outside_policy interface outside1
service-policy outside_policy interface outside2
service-policy outside_policy interface outside3
```

（注） VoIP インスペクションでは、ゾーンのロード バランシングにより、順序が正しくないパケットが増加する可能性があります。この状況は、異なるパスを通る先行パケットの前に後行パケットが ASA に到達する可能性があるために発生することがあります。順序が正しくないパケットには、次のような症状があります。

  - キューイングを使用した場合に、中間ノード（ファイアウォールと IDS）および受信エンド ノードでメモリ使用率が高い。
  - ビデオまたは音声の品質が低い。

  これらの影響を軽減するには、VoIP トラフィックのロード分散にのみ IP アドレスを使用することを推奨します。

- ECMP ゾーン機能を考慮してルーティングを設定します。

トラフィック ゾーンのガイドライン

ファイアウォール モード

ルーテッド ファイアウォール モードでだけサポートされています。トランスペアレント ファイアウォール モード。

フェールオーバー

- フェールオーバー リンクまたはステート リンクをゾーンに追加することはできません。
- アクティブ/アクティブ フェールオーバー モードでは、各コンテキストのインターフェイスを非対称ルーティング（ASR）グループに割り当てることができます。このサービスにより、ピア装置の同様のインターフェイスに戻るトラフィックを元の装置に復元することができます。コンテキスト内に ASR グループとトラフィック ゾーンの両方を設定することはできません。コンテキスト内にゾーンを設定した場合、どのコンテキスト インターフェイスも ASR グループに含めることはできません。ASR グループに関する詳細については、非対称にルーティングされたパケットのサポートの設定（アクティブ/アクティブ モード）（302 ページ）を参照してください。
- 各接続のプライマリ インターフェイスのみがスタンバイ装置に 複製されます。現在のインターフェイスは複製されません。スタンバイ装置がアクティブになると、その装置によって必要に応じて現在の新しいインターフェイスが割り当てられます。

クラスタ

- クラスタ制御リンクをゾーンに追加することはできません。

その他のガイドライン

- 最大 256 ゾーンを作成できます。
- 次のタイプのインターフェイスをゾーンに追加できます。
  - 物理
  - VLAN
  - EtherChannel
  - Redundant
- 次のタイプのインターフェイスは追加できません。
  - 管理専用
  - 管理アクセス
  - フェールオーバーまたはステート リンク

- クラスタ制御リンク
- EtherChannelインターフェイスまたは冗長インターフェイスのメンバーインターフェイス
- VNI（さらに、通常のデータ インターフェイスが nve 専用としてマークされている場合、ゾーンのメンバーにすることはできません）
- BVI、またはブリッジグループ メンバー インターフェイス。

- 1 つのインターフェイスがメンバーになることができるゾーンは 1 つだけです。
- ゾーンごとに最大 8 つのインターフェイスを含めることができます。
- ECMP の場合、ゾーンのすべてのインターフェイス間で、ゾーンごとに最大 8 つの等コスト ルートを追加できます。また、8 ルート制限の一部として 1 つのインターフェイスに複数のルートを設定することもできます。
- ゾーンにインターフェイスを追加すると、それらのインターフェイスのすべてのスタティック ルートが削除されます。
- ゾーン内のインターフェイスで DHCP リレー を有効にできません。

トラフィック ゾーンの設定

名前を付けたゾーンを設定し、インターフェイスをそのゾーンに割り当てます。

手順

ステップ 1 ゾーンを追加します。

zone *name*

例：

```
zone outside
```

ゾーン名は最大 48 文字です。

ステップ 2 インターフェイスをゾーンに追加します。

interface *id* **zone-member** *zone_name*

例：

```
interface gigabitethernet0/0
  zone-member outside
```

ステップ 3 インターフェイスをさらにゾーンに追加します。これらのインターフェイスのセキュリティ レベルが、追加した最初のインターフェイスのセキュリティ レベルと同じであることを確認します。

例：

```
interface gigabitethernet0/1
  zone-member outside
interface gigabitethernet0/2
  zone-member outside
interface gigabitethernet0/3
  zone-member outside
```

例

次の例では、4 つのメンバー インターフェイスを含む外部ゾーンを設定します。

```
zone outside
interface gigabitethernet0/0
  zone-member outside
interface gigabitethernet0/1
  zone-member outside
interface gigabitethernet0/2
  zone-member outside
interface gigabitethernet0/3
  zone-member outside
```

トラフィック ゾーンのモニタリング

この項では、トラフィック ゾーンをモニタする方法について説明します。

ゾーン情報

- **show zone** [*name*]

  ゾーン ID、コンテキスト、セキュリティ レベル、およびメンバーを表示します。

  show zone コマンドについては、次の出力を参照してください。

```
ciscoasa# show zone outside-zone

Zone: zone-outside id: 2
Security-level: 0
Context: test-ctx
 Zone Member(s) : 2
  outside1       GigabitEthernet0/0
  outside2       GigabitEthernet0/1
```

- **show nameif zone**

  インターフェイス名およびゾーン名を表示します。

  show nameif zone コマンドについては、次の出力を参照してください。

```
ciscoasa# show nameif zone
Interface                Name                    zone-name      Security
GigabitEthernet0/0       inside-1                inside-zone     100
GigabitEthernet0/1.21    inside                  inside-zone     100
GigabitEthernet0/1.31    4                                         0
GigabitEthernet0/2       outside                 outside-zone   0
Management0/0            lan                                       0
```

ゾーン接続

- **show conn** [**long** | **detail**] [**zone** *zone_name* [**zone** *zone_name*] [...]]

  show conn zone コマンドは、ゾーンの接続を表示します。**long** キーワードと **detail** キーワードは、接続が構築されたプライマリ インターフェイスと、トラフィックの転送に使用される現在のインターフェイスを表示します。

  show conn long zone コマンドの次の出力を参照してください。

```
ciscoasa# show conn long zone zone-inside zone zone-outside

TCP outside-zone:outside1(outside2): 10.122.122.1:1080
inside-zone:inside1(inside2): 10.121.121.1:34254, idle 0:00:02, bytes 10, flags UO
```

- **show asp table zone**

  デバッグ目的で高速セキュリティ パス テーブルを表示します。

- **show local-host** [**zone** *zone_name* [**zone** *zone_name*] [...]]

  ゾーン内のローカル ホストのネットワーク状態を表示します。

  show local-host zone コマンドについては、次の出力を参照してください。プライマリ インターフェイスが最初に表示され、現在のインターフェイスがカッコに囲まれています。

```
ciscoasa# show local-host zone outside-zone

Zone:outside-zone: 4 active, 5 maximum active, 0 denied
local host: <10.122.122.1>,
    TCP flow count/limit = 3/unlimited
    TCP embryonic count to host = 0
    TCP intercept watermark = unlimited
    UDP flow count/limit = 0/unlimited

  Conn:
 TCP outside-zone:outside1(outside2): 10.122.122.1:1080
inside-zone:inside1(inside2): 10.121.121.1:34254, idle 0:00:02, bytes 10, flags UO
```

ゾーン ルーティング

- **show route zone**

  ゾーン インターフェイスのルートを表示します。

  show route zone コマンドについては、次の出力を参照してください。

```
ciscoasa# show route zone

Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

S    192.168.105.1 255.255.255.255 [1/0] via 172.16.1.1, outside-zone:outside1
C    192.168.212.0 255.255.255.0 is directly connected, lan-zone:inside,
C    172.16.1.0 255.255.255.0 is directly connected, wan-zone:outside2
S    10.5.5.0 255.255.255.0 [1/0] via 172.16.1.1, wan-zone:outside2
O    10.2.2.1 255.255.255.255 [110/11] via 192.168.212.3, 2:09:24, lan-zone:inside
O    10.1.1.1 255.255.255.255 [110/11] via 192.168.212.2, 2:09:24, lan-zone:inside
```

- **show asp table routing**

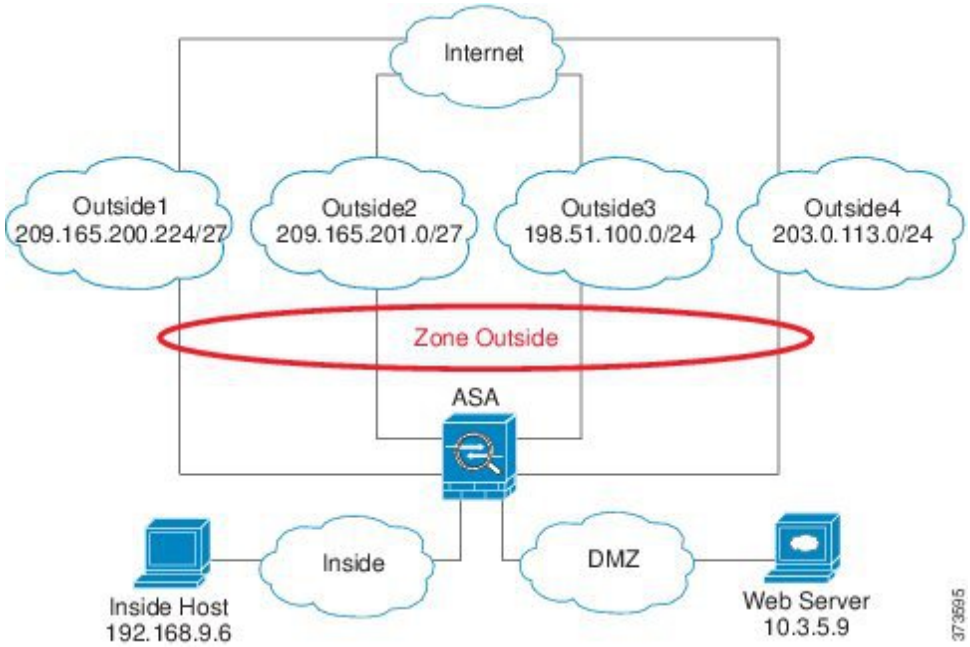
  デバッグ目的で高速セキュリティ パス テーブルを表示し、各ルートに関連付けられたゾーンを表示します。

  show asp table routing コマンドについては次の出力を参照してください。

```
ciscoasa# show asp table routing
route table timestamp: 60
in   255.255.255.255 255.255.255.255 identity
in   10.1.0.1       255.255.255.255 identity
in   10.2.0.1       255.255.255.255 identity
in   10.6.6.4         255.255.255.255 identity
in   10.4.4.4         255.255.255.255 via 10.4.0.10 (unresolved, timestamp: 49)
in   172.0.0.67       255.255.255.255 identity
in   172.0.0.0       255.255.255.0   wan-zone:outside2
in   10.85.43.0      255.255.255.0   via 10.4.0.3 (unresolved, timestamp: 50)
in   10.85.45.0      255.255.255.0   via 10.4.0.20 (unresolved, timestamp: 51)
in   192.168.0.0        255.255.255.0   mgmt
in   192.168.1.0       255.255.0.0     lan-zone:inside
out  255.255.255.255 255.255.255.255 mgmt
out  172.0.0.67       255.255.255.255 mgmt
out  172.0.0.0        255.255.255.0   mgmt
out  10.4.0.0       240.0.0.0       mgmt
out  255.255.255.255 255.255.255.255 lan-zone:inside
out  10.1.0.1       255.255.255.255 lan-zone:inside
out  10.2.0.0       255.255.0.0     lan-zone:inside
out  10.4.0.0       240.0.0.0       lan-zone:inside
```

トラフィック ゾーンの例

次に、4 つの VLAN インターフェイスを外部ゾーンに割り当てて、4 つの等コストのデフォルト ルートを設定する例を示します。PAT は内部インターフェイスに設定され、Web サーバはスタティック NAT を使用して DMZ インターフェイスで使用できます。




```
interface gigabitethernet0/0
  no shutdown
  description outside switch 1
interface gigabitethernet0/1
  no shutdown
  description outside switch 2

interface gigabitethernet0/2
  no shutdown
  description inside switch

zone outside

interface gigabitethernet0/0.101
  vlan 101
  nameif outside1
  security-level 0
  ip address 209.165.200.225 255.255.255.224
  zone-member outside
  no shutdown

interface gigabitethernet0/0.102
  vlan 102
  nameif outside2
  security-level 0
  ip address 209.165.201.1 255.255.255.224
  zone-member outside
```

```
  no shutdown

interface gigabitethernet0/1.201
  vlan 201
  nameif outside3
  security-level 0
  ip address 198.51.100.1 255.255.255.0
  zone-member outside
  no shutdown

interface gigabitethernet0/1.202
  vlan 202
  nameif outside4
  security-level 0
  ip address 203.0.113.1 255.255.255.0
  zone-member outside
  no shutdown

interface gigabitethernet0/2.301
  vlan 301
  nameif inside
  security-level 100
  ip address 192.168.9.1 255.255.255.0
  no shutdown

interface gigabitethernet0/2.302
  vlan 302
  nameif dmz
  security-level 50
  ip address 10.3.5.1 255.255.255.0
  no shutdown

# Static NAT for DMZ web server on any destination interface
object network WEBSERVER
  host 10.3.5.9 255.255.255.255
  nat (dmz,any) static 209.165.202.129 dns

# Dynamic PAT for inside network on any destination interface
object network INSIDE
  subnet 192.168.9.0 255.255.255.0
  nat (inside,any) dynamic 209.165.202.130

# Global access rule for DMZ web server
access-list WEB-SERVER extended permit tcp any host WEBSERVER eq 80
access-group WEB-SERVER global

# 4 equal cost default routes for outside interfaces
route outside1 0 0 209.165.200.230
route outside2 0 0 209.165.201.10
route outside3 0 0 198.51.100.99
route outside4 0 0 203.0.113.87
# Static routes for NAT addresses - see redistribute static command
route dmz 209.165.202.129 255.255.255.255 10.3.5.99
route inside 209.165.202.130 255.255.255.255 192.168.9.99

# The global service policy
class-map inspection_default
  match default-inspection-traffic
policy-map type inspect dns preset_dns_map
  parameters
    message-length maximum client auto
    message-length maximum 512
    dns-guard
    protocol-enforcement
```

```
    nat-rewrite
policy-map global_policy
  class inspection_default
    inspect dns preset_dns_map
    inspect ftp
    inspect h323 h225 _default_h323_map
    inspect h323 ras _default_h323_map
    inspect ip-options _default_ip_options_map
    inspect netbios
    inspect rsh
    inspect rtsp
    inspect skinny
    inspect esmtp _default_esmtp_map
    inspect sqlnet
    inspect sunrpc
    inspect tftp
    inspect sip
    inspect xdmcp
service-policy global_policy global
```

トラフィック ゾーンの履歴

機能名	プラットフォーム リリース	説明
トラフィック ゾーン	9.3(2)	インターフェイスをトラフィック ゾーンにグループ化することで、トラフィックのロードバランシング（等コスト マルチパス（ECMP）ルーティングを使用）、ルートの冗長性、および複数のインターフェイス間での非対称ルーティングを実現できます。 （注） 名前付きゾーンにはセキュリティ ポリシーを適用できません。セキュリティポリシーはインターフェイスに基づきます。ゾーン内のインターフェイスが同じアクセスルール、NAT、およびサービス ポリシーを使用して設定されていれば、ロード バランシングおよび非対称ルーティングは正しく動作します。 **zone**、**zone-member**、**show running-config zone**、**clear configure zone**、**show zone**、**show asp table zone**、**show nameif zone**、**show conn long**、**show local-host zone**、**show route zone**、**show asp table routing**、**clear conn zone**、**clear local-host zone** の各コマンドが導入または変更されました。

第 IV 部

基本設定

第 18 章

基本設定

この章では、ASA 上でコンフィギュレーションを機能させるために通常必要な基本設定を行う方法について説明します。

ホスト名、ドメイン名、およびイネーブルパスワードと Telnet パスワードの設定

ホスト名、ドメイン名、イネーブル パスワード、Telnet パスワードを設定するには、次の手順を実行します。

始める前に

ホスト名、ドメイン名、イネーブル パスワード、Telnet パスワードを設定する前に、次の要件を確認します。

- マルチ コンテキスト モードでは、コンテキスト実行スペースとシステム実行スペースの両方のホスト名とドメイン名を設定できます。
- イネーブル パスワードと Telnet パスワードは、各コンテキストで設定します。システムでは使用できません。 マルチ コンテキスト モードのスイッチから ASASM へのセッションを実行する場合、ASASM は管理コンテキストで設定したログイン パスワードを使用します。

- システム コンフィギュレーションからコンテキスト コンフィギュレーションに切り替えるには、**changeto context** *name* コマンドを入力します。

手順

ステップ 1 ASA またはコンテキストのホスト名を指定します。デフォルトのホスト名は「asa」です。

hostname *name*

例：

```
ciscoasa(config)# hostname myhostnamexample12345
```

名前には、63 文字以下の文字を使用できます。ホスト名はアルファベットまたは数字で開始および終了する必要があります。使用できるのはアルファベット、数字、ハイフンのみです。

ASA のホスト名を設定すると、そのホスト名がコマンドラインのプロンプトに表示されます。このホスト名によって、複数のデバイスとのセッションを確立する場合に、コマンドを入力する場所が常に把握できます。

マルチ コンテキスト モードでは、システム実行スペースに設定したホスト名がすべてのコンテキストのコマンドラインプロンプトに表示されます。コンテキスト内で任意に設定したホスト名はコマンドラインには表示されませんが、**banner** コマンド**$(hostname)** トークンによって使用できます。

ステップ 2 ASA のドメイン名を指定します。デフォルト ドメイン名は default.domain.invalid です。

domain-name *name*

例：

```
ciscoasa(config)# domain-name example.com
```

ASA は、修飾子を持たない名前のサフィックスとして、ドメイン名を追加します。たとえば、ドメイン名を「example.com」に設定し、syslog サーバとして非修飾名「jupiter」を指定した場合は、ASA によって名前が修飾されて「jupiter.example.com」となります。

ステップ 3 イネーブル パスワードを変更します。デフォルトではイネーブル パスワードは空白ですが。

enable password *password*

例：

```
ciscoasa(config)# enable password Pa$$w0rd
```

enable 認証を設定しない場合、イネーブル パスワードによって特権 EXEC モードが開始されます。HTTP 認証を設定しない場合、イネーブル パスワードによって空のユーザ名で ASDM にログインできます。

password 引数は、大文字と小文字が区別される 3 ～ 32 文字のパスワードです。スペースと疑問符を除く任意の ASCII 印刷可能文字（文字コード 32 ～ 126）を組み合わせることができます。

このコマンドによって最高の特権レベル（15）のパスワードが変更されます。ローカル コマンド許可を設定すると、次の構文を使用して 0 ～ 15 の各特権レベルにイネーブル パスワードを設定できます。

enable password *password* **level** *number*

encrypted キーワードは、（MD5 ベースのハッシュまたは PBKDF2（Password-Based Key Derivation Function 2）ハッシュを使用して）パスワードが暗号化されていることを示します。**enable password** コマンドのパスワードを定義すると、ASA はセキュリティを維持するために、そのパスワードを設定に保存するときに暗号化します。**show running-config** コマンドを入力すると、**enable password** コマンドでは実際のパスワードは示されません。暗号化されたパスワードとそれに続けて **encrypted** キーワードが示されます。たとえば、パスワードに「test」と入力すると、**show running-config** コマンドの出力には次のように表示されます。

```
username user1 password DLaUiAX3l78qgoB5c7iVNw== encrypted
```

実際に CLI で **encrypted** キーワードを入力するのは、同じパスワードを使用して、ある設定ファイルを他の ASA で使用するためにカット アンド ペーストする場合だけです。

パスワードを指定せずに **enable password** コマンドを入力すると、パスワードはデフォルトの空白に設定されます。

ステップ 4 Telnet アクセスのためのログイン パスワードを設定します。デフォルトのパスワードはありません。

Telnet 認証を設定しない場合、ログイン パスワードは Telnet アクセスに使用されます。**session** コマンドを使用してスイッチから ASASM にアクセスする場合にも、このパスワードを使用します。

{**passwd** | **password**} *password* [**encrypted**]

例：

```
ciscoasa(config)# password cisco12345
```

passwd または **password** と入力できます。*password* は、大文字と小文字が区別されるパスワードです。英数字と特殊記号を 16 文字まで使用できます。パスワードには、疑問符とスペースを除いて、任意の文字を使用できます。

パスワードは暗号化された形式でコンフィギュレーションに保存されるため、パスワードの入力後に元のパスワードを表示することはできません。何らかの理由で別の ASA にパスワードをコピーする必要があるが、元のパスワードがわからない場合、暗号化されたパスワードと、**encrypted** キーワードを指定して **passwd** コマンドを入力できます。通常、このキーワードは、**show running-config passwd** コマンドを入力するときにだけ表示されます。

日時の設定

（注） ASASM または Firepower 2100、4100、または 9300 の日時を設定しないでください。ASA はシャーシから日時の設定を受信します。

タイムゾーンと夏時間の日付の設定

タイムゾーンおよび夏時間の日付範囲を設定するには、次の手順を実行します。

手順

ステップ 1 タイム ゾーンを設定します。デフォルトでは、タイムゾーンは UTC です。

- **clock timezone** *zone* [-]*hours* [*minutes*]
  - *zone*：タイムゾーンを文字列で指定します（太平洋標準時の PST など）。
  - [-]*hours*：UTC からのオフセットの時間数を設定します。たとえば、PST は -8 時間です。
  - *minutes*：UTC からのオフセットの分数を設定します。

例：

```
ciscoasa(config)# clock timezone PST -8
```

ステップ 2 次のいずれかのコマンドを入力して、夏時間の日付範囲をデフォルトから変更します。デフォルトの定期的な日付範囲は、3 月の第 2 日曜日の午前 2 時～ 11 月の第 1 日曜日の午前 2 時です。

- 夏時間の開始日と終了日を、特定の年の特定の日付として指定します。このコマンドを使用する場合は、日付を毎年再設定する必要があります。

  clock summer-time *zone* **date** {*day month* | *month day*} *year hh*:*mm* {*day month* | *month day*} *year hh*:*mm* [*offset*]
  - *zone*：タイムゾーンを文字列で指定します（太平洋夏時間の PDT など）。
  - *day*：1 ～ 31 の日付を設定します。標準の日付形式に応じて、月日を **April 1** または 1 April のように入力できます。
  - *month*：月を文字列で設定します。標準の日付形式に応じて、月日を April 1 または 1 April のように入力できます。
  - *year*：年を 4 桁で設定します（2004 など）。年の範囲は 1993 ～ 2035 です。

- *hh:mm*：時間と分を 24 時間形式で設定します。
- *offset*：夏時間用に時間を変更する分数を設定します。デフォルト値は 60 分です。

例：

```
ciscoasa(config)# clock summer-time PDT 1 April 2010 2:00 60
```

- 夏時間の開始日と終了日を、年の特定の日付ではなく、月の日時の形式で指定します。このコマンドを使用すると、毎年変更する必要がない、繰り返される日付範囲を設定できます。

  clock summer-time *zone* **recurring** [*week weekday month hh*:*mm week weekday month hh*:*mm*] [*offset*]

  - *zone*：タイムゾーンを文字列で指定します（太平洋夏時間の PDT など）。
  - *week*：月の特定の週を 1 から 4 までの整数で指定するか、first または last という単語で指定します。たとえば、日付が 5 週目に当たる場合は、last を指定します。
  - *weekday*：Monday、Tuesday、Wednesday などのように曜日を指定します。
  - *month*：月を文字列で設定します。
  - *hh:mm*：時間と分を 24 時間形式で設定します。
  - *offset*：夏時間用に時間を変更する分数を設定します。デフォルト値は 60 分です。

  例：

```
ciscoasa(config)# clock summer-time PDT recurring first Monday April 2:00 60
```

NTP サーバを使用した日付と時刻の設定

NTP を利用して階層的なサーバ システムを実現し、ネットワーク システム間の時刻を正確に同期します。このような精度は、CRL の検証など正確なタイム スタンプを含む場合など、時刻が重要な操作で必要になります。複数の NTP サーバを設定できます。ASA は、データ信頼度の尺度となる一番下のストラタムのサーバを選択します。

手動で設定した時刻はすべて、NTP サーバから取得された時刻によって上書きされます。

始める前に

マルチ コンテキスト モードでは、時刻はシステム コンフィギュレーションに対してだけ設定できます。

手順

ステップ 1 （任意） NTP サーバによる MD5 認証を有効にします。

a) 認証をイネーブルにします。

ntp authenticate

例：

```
ciscoasa(config)# ntp authenticate
```

NTP 認証を有効にする場合は、さらに **ntp trusted-key** コマンドでキー ID を指定し、そのキーを **ntp server key** コマンドでサーバに関連付ける必要があります。**ntp authentication-key** コマンドを使用して ID の実際のキーを設定します。複数のサーバがある場合は、サーバごとに個別の ID を設定します。

b) 認証キー ID が信頼できるキーであると指定します。この信頼できるキーは、NTP サーバでの認証に必要です。

ntp trusted-key *key_id*

例：

```
ciscoasa(config)# ntp trusted-key 1
ciscoasa(config)# ntp trusted-key 2
ciscoasa(config)# ntp trusted-key 3
ciscoasa(config)# ntp trusted-key 4
```

key_id 引数は、1 ～ 4294967295 の値です。複数のサーバで使用できるように複数の信頼できるキーを入力できます。

c) NTP サーバの認証を行うためのキーを設定します。

ntp authentication-key *key_id* **md5** *key*

例：

```
ciscoasa(config)# ntp authentication-key 1 md5 aNiceKey1
ciscoasa(config)# ntp authentication-key 2 md5 aNiceKey2
ciscoasa(config)# ntp authentication-key 3 md5 aNiceKey3
ciscoasa(config)# ntp authentication-key 4 md5 aNiceKey4
```

- *key_id*：**ntp trusted-key** コマンドを使用して設定した ID を設定します。
- **md5** *key*：MD5 キーを最大 32 文字の文字列で設定します。

ステップ 2 NTP サーバを指定します。

ntp server*ipv4_address* [**key** *key_id*] [**source** *interface_name*] [**prefer**]

例：

```
ciscoasa(config)# ntp server 10.1.1.1 key 1 prefer
```

```
ciscoasa(config)# ntp server 10.2.1.1 key 2
```

NTP 認証（**ntp authenticate**）をイネーブルにした場合は、**ntp trusted-key** コマンドを使って設定した ID を使用して **key** *keykey_id* 引数を指定する必要があります。

source *interface_name* キーワード引数ペアは、NTP パケットの発信インターフェイスを識別します（ルーティングテーブル内のデフォルトのインターフェイスを使用しない場合）。マルチコンテキストモードではシステムにインターフェイスが含まれないため、管理コンテキストに定義されているインターフェイス名を指定します。

prefer キーワードは、精度が類似する複数のサーバがある場合に、このNTPサーバを優先サーバに設定します。NTPでは、どのサーバの精度が最も高いかを判断するためのアルゴリズムを使用し、そのサーバに同期します。サーバの精度に差がない場合は、**prefer** キーワードで使用するサーバを指定します。ただし、優先サーバよりも精度が大幅に高いサーバがある場合、ASA は精度の高いそのサーバを使用します。たとえば、ASA は優先サーバであるストラタム 3 のサーバよりもストラタム 2 のサーバを優先的に使用します。

複数のサーバを指定できます。その中から ASA は最も精度の高いサーバを使用します。

手動での日時の設定

日付と時刻を手動で設定するには、次の手順を実行します。

始める前に

マルチ コンテキスト モードでは、時刻はシステム コンフィギュレーションに対してだけ設定できます。

手順

日付と時刻を手動で設定します。

clock set *hh*:*mm*:*ss* {*month day* | *day month*} *year*

例：

```
ciscoasa# clock set 20:54:00 april 1 2004
```

hh:*mm*:*ss* 引数には、時、分、秒を 24 時間形式で設定します。たとえば、午後 8:54 の場合は、20:54:00 と入力します。

day 値は、月の日付として 1 ～ 31 を設定します。標準の日付形式に応じて、月日を april 1 または 1 april のように入力できます。

month 値は、月を設定します。標準の日付形式に応じて、月日を april 1 または 1 april のように入力できます。

year 値は、4 桁で年を設定します（2004 など）。年の範囲は 1993 ～ 2035 です。

デフォルトの時間帯は UTC です。**clock timezone** コマンドを使用して、 **clock set** コマンドの入力後に時間帯を変更した場合、時間は自動的に新しい時間帯に調整されます。

このコマンドはハードウェア チップ内の時間を設定しますが、コンフィギュレーション ファイル内の時間は保存しません。この時間はリブート後も保持されます。他の **clock** コマンドとは異なり、このコマンドは特権 EXEC コマンドです。クロックをリセットするには、clock set コマンドを使用して新しい時刻を設定する必要があります。

マスター パスフレーズの設定

マスター パスフレーズを利用すると、プレーン テキストのパスワードが安全に、暗号化形式で保存され、1 つのキーを使用してすべてのパスワードを一様に暗号化またはマスキングできるようになります。このようにしても、機能は一切変更されません。マスターパスフレーズを使用する機能としては、次のものがあります。

- OSPF
- EIGRP
- VPN ロード バランシング
- VPN (リモート アクセスおよびサイトツーサイト)
- フェールオーバー
- AAA サーバ
- Logging
- 共有ライセンス

マスター パスフレーズの追加または変更

マスター パスフレーズを追加または変更するには、次の手順を実行します。

始める前に

- この手順を実行できるのは、コンソール、SSH、HTTPS 経由の ASDM などによるセキュア セッションにおいてのみです。
- フェールオーバーがイネーブルであっても、フェールオーバー共有キーが設定されていない場合に、マスター パスフレーズを変更すると、エラー メッセージが表示されます。このメッセージには、マスター パスフレーズの変更がプレーン テキストとして送信されないよう、フェールオーバー共有キーを入力する必要があることが示されます。

- アクティブ/スタンバイ フェールオーバーでパスワードの暗号化を有効化または変更すると、**write standby** が実行されます。これは、アクティブな構成をスタンバイ ユニットに複製します。この複製が行われない場合、スタンバイ ユニットの暗号化されたパスワードは、同じパスフレーズを使用している場合でも異なるものになります。構成を複製することで、構成が同じであることが保証されます。アクティブ/アクティブ フェールオーバーの場合は、手動で **write standby** を入力する必要があります。**write standby** は、アクティブ/アクティブ モードでトラフィックの中断を引き起こす場合があります。これは、新しい構成が同期される前に、セカンダリ ユニットで構成が消去されるためです。**failover active group 1** および **failover active group 2** コマンドを使用してプライマリ ASA ですべてのコンテキストをアクティブにし、**write standby** を入力してから、**no failover active group 2** コマンドを使用してセカンダリ ユニットにグループ 2 コンテキストを復元する必要があります。

手順

ステップ 1 暗号キーの生成に使用されるパスフレーズを設定します。パスフレーズの長さは、8 ～ 128 文字にする必要があります。パスフレーズには、バックスペースと二重引用符を除くすべての文字を使用できます。コマンドに新しいパスフレーズを入力しないと、入力を求めるプロンプトが表示されます。パスフレーズを変更するには、古いパスフレーズを入力する必要があります。

key config-key password-encryption [*new_passphrase* [*old_passphrase*]]

例：

```
ciscoasa(config)# key config-key password-encryption
Old key: bumblebee
New key: haverford
Confirm key: haverford
```

（注） インタラクティブ プロンプトを使用してパスワードを入力し、パスワードがコマンド履歴バッファに記録されないようにします。

暗号化されたパスワードがプレーン テキスト パスワードに変換されるため、**no key config-key password-encrypt** コマンドは注意して使用してください。パスワードの暗号化がサポートされていないソフトウェア バージョンにダウングレードするときは、このコマンドの **no** 形式を使用できます。

ステップ 2 パスワード暗号化をイネーブルにします。

password encryption aes

例：

```
ciscoasa(config)# password encryption aes
```

パスワードの暗号化がイネーブルになり、マスターパスワードが使用可能になると、ただちにすべてのユーザパスワードが暗号化されます。実行コンフィギュレーションには、パスワードは暗号化された形式で表示されます。

パスワードの暗号化をイネーブルにしたときに、パスフレーズが設定されていない場合、パスフレーズが将来的に使用可能になるものとしてコマンドは正常に実行されます。

後から **no password encryption aes** コマンドを使用してパスワードの暗号化をディセーブルにすると、暗号化された既存のパスワードは変更されず、マスター パスフレーズが存在する限り、暗号化されたパスワードはアプリケーションによって必要に応じて復号化されます。

ステップ 3 マスター パスフレーズのランタイム値と結果のコンフィギュレーションを保存します。

write memory

例：

```
ciscoasa(config)# write memory
```

このコマンドを入力しなければ、スタートアップ コンフィギュレーションのパスワードは引き続き可読状態となります（過去に暗号化された状態で保存されていない場合）。また、マルチ コンテキスト モードでは、マスター パスフレーズはシステム コンテキスト コンフィギュレーション内で変更されます。その結果、すべてのコンテキスト内のパスワードが影響を受けます。すべてのユーザ コンテキストではなく、システム コンテキスト モードで write memory コマンドを入力しないと、ユーザ コンテキストで暗号化されたパスワードは失効する可能性があります。また、すべての設定を保存するには、システム コンテキストで write memory all コマンドを使用します。

例

次の例は、これまでにキーが何も存在していないことを示します。

```
ciscoasa(config)# key config-key password-encryption 12345678
```

次の例は、キーがすでに存在することを示します。

```
ciscoasa(config)# key config-key password-encryption 23456789
Old key: 12345678
```

次の例では、パラメータを指定しないでコマンドを入力して、キーの入力を求めるプロンプトが表示されるようにします。キーがすでに存在するため、入力を求めるプロンプトが表示されます。

```
ciscoasa(config)# key config-key password-encryption
Old key: 12345678
New key: 23456789
Confirm key: 23456789
```

次の例では、既存のキーがないため、入力を求めるプロンプトが表示されません。

```
ciscoasa(config)# key config-key password-encryption
New key: 12345678
Confirm key: 12345678
```

マスター パスフレーズの無効化

マスター パスフレーズをディセーブルにすると、暗号化されたパスワードがプレーン テキストパスワードに戻ります。暗号化されたパスワードをサポートしていない以前のソフトウェアバージョンにダウングレードする場合は、パスフレーズを削除しておくと便利です。

始める前に

- ディセーブルにする現在のマスターパスフレーズがわかっていなければなりません。パスフレーズが不明の場合は、マスターパスフレーズの削除（594 ページ）を参照してください。
- この手順が機能するのは、HTTPS を介した Telnet、SSH、または ASDM によるセキュアセッションだけです。

  マスター パスフレーズをディセーブルにするには、次の手順を実行します。

手順

ステップ 1 マスターパスフレーズを削除します。コマンドにパスフレーズを入力しないと、入力を求めるプロンプトが表示されます。

no key config-key password-encryption [*old_passphrase*]]

例：

```
ciscoasa(config)# no key config-key password-encryption

Warning! You have chosen to revert the encrypted passwords to plain text.
This operation will expose passwords in the configuration and therefore
exercise caution while viewing, storing, and copying configuration.

Old key: bumblebee
```

ステップ 2 マスター パスフレーズのランタイム値と結果のコンフィギュレーションを保存します。

write memory

例：

```
ciscoasa(config)# write memory
```

パスフレーズを含む不揮発性メモリは消去され、0xFF パターンで上書きされます。

マルチ モードでは、システム コンテキスト コンフィギュレーション内のマスター パスフレーズが変更されます。その結果、すべてのコンテキスト内のパスワードが影響を受けます。すべてのユーザ コンテキストではなく、システム コンテキスト モードで write memory コマンドを入力すると、ユーザ コンテキストで暗号化されたパスワードは失効する可能性があります。また、すべての設定を保存するには、システム コンテキストで write memory all コマンドを使用します。

マスター パスフレーズの削除

マスター パスフレーズは回復できません。マスター パスフレーズがわからなくなった場合や不明な場合は、削除できます。

マスター パスフレーズを削除するには、次の手順を実行します。

手順

ステップ 1 マスターキーと、暗号化されたパスワードが含まれているコンフィギュレーションを削除します。

write erase

例：

```
ciscoasa(config)# write erase
```

ステップ 2 マスター キーや暗号化パスワードのないスタートアップ コンフィギュレーションを使用して ASA をリロードします。

reload

例：

```
ciscoasa(config)# reload
```

DNS サーバの設定

DNS サーバを設定して、ASA がホスト名を IP アドレスに解決できるようにする必要があります。また、アクセス ルールに完全修飾ドメイン名（FQDN）ネットワーク オブジェクトを使用するように、DNS サーバを設定する必要があります。

一部の ASA 機能では、ドメイン名で外部サーバにアクセスするために DNS サーバを使用する必要があります。たとえば、ボットネット トラフィック フィルタ機能では、ダイナミック デー

タベース サーバにアクセスして、スタティック データベースのエントリを解決するためにDNSサーバが必要です。他の機能（**ping** コマンドや **traceroute** コマンドなど）では、ping やtracerouteを実行する名前を入力できるため、ASA はDNS サーバと通信することで名前を解決できます。名前は、多くの SSL VPN コマンドおよび certificate コマンドでもサポートされます。

（注） ASA では、機能に応じて DNS サーバの使用が限定的にサポートされます。たとえば、ほとんどのコマンドでは、IP アドレスを入力する必要があります。名前を使用できるのは、名前と IP アドレスを関連付けるように **name** コマンドを手動で設定し、names コマンドを使用して名前の使用を有効にした場合だけです。

始める前に

DNS ドメイン ルックアップをイネーブルにするすべてのインターフェイスに対して適切なルーティングおよびアクセス ルールを設定し、DNS サーバに到達できるようにしてください。

手順

ステップ 1 サポートされているコマンドに対してネーム ルックアップを実行するために、ASA が DNS サーバに DNS 要求を送信できるようにします。

dns domain-lookup *interface_name*

例：

```
ciscoasa(config)# dns domain-lookup inside
```

ステップ 2 ASA が発信要求に使用する DNS サーバ グループを指定します。

dns server-group DefaultDNS

例：

```
ciscoasa(config)# dns server-group DefaultDNS
```

PN トンネル グループ用に他の DNS サーバ グループを設定できます。詳細については、コマンド リファレンスの **tunnel-group** コマンドを参照してください。

ステップ 3 1つまたは複数のDNSサーバを指定します。同じコマンドで6つのIPアドレスすべてをスペースで区切って入力するか、各コマンドを別々に入力できます。ASAでは、応答を受信するまで各 DNS サーバを順に試します。

name-server *ip_address* [*ip_address2*] [...] [*ip_address6*]

例：

```
ciscoasa(config-dns-server-group)# name-server 10.1.1.5 192.168.1.67 209.165.201.6 dmz
```

ステップ 4 ホスト名に追加するドメイン名を設定します（完全修飾されていない場合）。

domain-name *name*

例：

```
ciscoasa(config-dns-server-group)# domain-name example.com
```

ステップ 5 （任意）DNS サーバ グループの追加プロパティを設定します。

デフォルト設定がネットワークに適さない場合は、次のコマンドを使用してグループの特性を変更します。

- **timeout** *seconds*：次の DNS サーバを試行する前に待機する秒数（1 ～ 30）。デフォルト値は 2 秒です。ASA がサーバのリストを再試行するたびに、このタイムアウトは倍増します。
- **retries** *number*：ASA が応答を受信しないときに、DNS サーバのリストを再試行する回数（0 ～ 10）。
- **expire-entry-timer minutes** *number*：DNS エントリの期限が切れた（TTL が経過した）後、そのエントリが DNS ルックアップ テーブルから削除されるまでの分数。エントリを削除するとテーブルの再コンパイルが必要になります。このため、頻繁に削除するとデバイスの処理負荷が大きくなる可能性があります。DNS エントリによっては TTL が極端に短い（3 秒程度）場合があるため、この設定を使用して TTL を実質的に延長できます。デフォルトは 1 分です（つまり、TTL が経過してから 1 分後にエントリが削除されます）。指定できる範囲は 1 ～ 65535 分です。このオプションは、FQDN ネットワーク オブジェクトの解決時にのみ使用されます。
- **poll-timer minutes** *number*：FQDN ネットワーク/ホスト オブジェクトを IP アドレスに解決するために使用されるポーリング サイクルの時間（分単位）。FQDN オブジェクトはファイアウォール ポリシーで使用される場合にのみ解決されます。タイマーによって解決間隔の最大時間が決まります。IP アドレス解決に対して更新するタイミングの決定には DNS エントリの存続可能時間（TTL）値も使用されるため、個々の FQDN がポーリング サイクルよりも頻繁に解決される場合があります。デフォルトは 240（4 時間）です。指定できる範囲は 1 ～ 65535 分です。

ハードウェア バイパス（Cisco ISA 3000）の設定

ハードウェア バイパスを有効化して、停電時にもインターフェイス ペア間のトラフィックのフローを継続することができます。サポートされているインターフェイス ペアは、銅線 GigabitEthernet 1/1 と 1/2 および GigabitEthernet 1/3 と 1/4 です。ハードウェア バイパスがアクティブな場合はファイアウォール機能が設定されていません。したがって、トラフィックの通過を許可しているリスクをご自身が理解していることを確認してください。次のハードウェア バイパスのガイドラインを参照してください。

- この機能は、Cisco ISA 3000 アプライアンスのみで使用できます。
- 光ファイバ イーサネット モデルがある場合は、銅線イーサネット ペア（GigabitEthernet 1/1 および 1/2）のみがハードウェア バイパスをサポートします。
- ISA 3000 への電源が切断され、ハードウェア バイパス モードに移行すると、通信できるのはサポートされているインターフェイス ペアだけになります。つまり、デフォルトの設定を使用している場合、inside1 と inside2 間および outside1 と outside2 間は通信できなくなります。これらのインターフェイス間の既存の接続がすべて失われます。
- シスコでは、TCP シーケンスのランダム化を無効にすることを推奨しています（下記の手順を参照）。ランダム化が有効化されている場合（デフォルト）、ハードウェア バイパスを有効化するときに TCP セッションを再確立する必要があります。デフォルトでは、ISA 3000 を通過する TCP 接続の最初のシーケンス番号（ISN）が乱数に書き換えられます。ハードウェア バイパスが有効化されると、ISA 3000 はデータ パスに存在しなくなり、シーケンス番号を変換しません。受信するクライアントは予期しないシーケンス番号を受信し、接続をドロップします。TCP シーケンスのランダム化が無効になっていても、スイッチオーバーの際に一時的にダウンしたリンクのために、一部の TCP 接続は再確立される必要があります。
- ハードウェアのバイパス インターフェイスでの Cisco TrustSec の接続は、ハードウェアのバイパスが有効化されているときにはドロップされます。ISA 3000 の電源がオンになり、ハードウェアのバイパスが非アクティブ化されている場合、接続は再ネゴシエートされます。
- ハードウェア バイパスを非アクティブ化し、トラフィックが ISA 3000 のデータ パスを経由することを再開した場合、スイッチオーバー時に一時的にダウンしたリンクがあるために、既存の TCP セッションの一部を再確立する必要があります。
- ハードウェア バイパスをアクティブにすると、イーサネット PHY が切断され、ASA はインターフェイスのステータスを判断できなくなります。インターフェイスはダウン状態であるかのように表示されます。

始める前に

- ハードウェア バイパス インターフェイスはスイッチのアクセス ポートに接続する必要があります。トランク ポートには接続しないでください。

手順

ステップ 1 停電時にハードウェア バイパスが有効化されるように設定します。

hardware-bypass GigabitEthernet {**1/1-1/2** | **1/3-1/4**} [**sticky**]

例：

```
ciscoasa(config)# hardware-bypass GigabitEthernet 1/1-1/2
ciscoasa(config)# hardware-bypass GigabitEthernet 1/3-1/4
```

sticky キーワードによって、電源が回復してアプライアンスが起動した後に、アプライアンスがハードウェア バイパス モードに保たれます。この場合、準備が整った時点でハードウェア バイパスを手動でオフにする必要があります。このオプションを使用すると、トラフィックへの短時間の割り込みがいつ発生するかを制御できます。

ステップ 2 手動でハードウェア バイパスを有効化または非アクティブ化します。

[**no**] **hardware-bypass manual GigabitEthernet** {**1/1-1/2** |**1/3-1/4**}

例：

```
ciscoasa# hardware-bypass manual GigabitEthernet 1/1-1/2
ciscoasa# no hardware-bypass manual GigabitEthernet 1/1-1/2
```

ステップ 3 （任意）ハードウェア バイパスを設定して、ASA FirePOWER モジュールが起動するまでアクティブに維持します。

hardware-bypass boot-delay module-up sfr

ブート遅延が動作するには、**sticky** オプションを使用せずにハードウェア バイパスを有効化する必要があります。**hardware-bypass boot-delay** を使用しないと、ASA FirePOWER モジュールが起動を完了する前にハードウェア バイパスが非アクティブになる可能性があります。たとえば、モジュールをフェールクローズに設定していた場合、このような状況では、トラフィックがドロップされる可能性があります。

ステップ 4 TCP シーケンスのランダム化のディセーブルこの例では、デフォルト設定に設定を追加することによって、すべてのトラフィックのランダム化を無効化する方法を示します。

policy-map global_policy

class sfrclass

set connection random-sequence-number disable

後でオンに戻す場合は、「disable」を **enable** に置き換えます。

ASP（高速セキュリティ パス）のパフォーマンスと動作の調整

ASP はポリシーおよび設定を利用可能にする実装レイヤです。Cisco Technical Assistance Center とのトラブルシューティング時以外は直接影響することはありません。ただし、パフォーマンスと信頼性に関連するいくつかの動作を調節することができます。

ルール エンジンのトランザクション コミット モデルの選択

デフォルトでは、ルールベースのポリシー（アクセス ルールなど）を変更した場合、変更はただちに有効になります。ただし、この即時性によりパフォーマンスにわずかな負担がかかりま

す。パフォーマンス コストは、1秒あたりの接続数が多い環境で大量のルール リストがある場合に顕著です。たとえば、ASAが1秒あたり18,000個の接続を処理しながら、25,000個のルールがあるポリシーを変更する場合などです。

ルール エンジンはさらに迅速なルール ルックアップを実現するためにルールをコンパイルするため、パフォーマンスに影響します。デフォルトでは、システムは接続試行の評価時にコンパイルされていないルールも検索して、新しいルールが適用されるようにします。ルールがコンパイルされていないため、検索に時間がかかります。

この動作を変更して、ルール エンジンがトランザクション モデルを使用してルールの変更を導入し、新しいルールがコンパイルされて使用可能な状態になるまで古いルールを引き続き使用するようにできます。トランザクション モデルを使用することで、ルールのコンパイル中にパフォーマンスが落ちることはありません。次の表は、その動作の違いを明確にします。

モデル	コンパイル前	コンパイル中	コンパイル後
デフォルト	古いルールに一致します。	新しいルールに一致します （接続数/秒のレートは減少します）。	新しいルールに一致します。
トランザクション	古いルールに一致します。	古いルールに一致します （接続数/秒のレートは影響を受けません）。	新しいルールに一致します。

トランザクション モデルのその他のメリットには、インターフェイス上の ACL を交換するときに、古い ACL を削除して新しいポリシーを適用するまでに時間差がないことがあります。この機能により受け入れ可能な接続が操作中にドロップされる可能性が削減されます。

ヒント ルール タイプのトランザクション モデルをイネーブルにする場合、コンパイルの先頭と末尾をマークする Syslog が生成されます。これらの Syslog には 780001 ～ 780004 までの番号が付けられます。

ルール エンジンのトランザクション コミット モデルを有効にするには、次の手順を使用します。

手順

ルール エンジンのトランザクション コミット モデルを有効にします。

asp rule-engine transactional-commit *option*

オプションは次のとおりです。

- **access-group**：グローバルにまたはインターフェイスに適用されるアクセス ルール。

- **nat**：ネットワーク アドレス変換ルール。

例：

```
ciscoasa(config)# asp rule-engine transactional-commit access-group
```

ASP ロード バランシングの有効化

ASP のロード バランシング機能によって、次の問題を回避しやすくなります。

- フロー上での突発的なトラフィックの増加によって発生するオーバーラン
- 特定のインターフェイス受信リングをオーバーサブスクライブするバルク フローによるオーバーラン
- 比較的高過負荷のインターフェイス受信リングによるオーバーラン（シングル コアでは負荷を維持できません）

ASP ロード バランシングにより、1 つのインターフェイス受信リングから受信したパケットを複数のコアが同時に処理できます。システムがパケットをドロップし、**show cpu** コマンドの出力が 100% を大きく下回る場合、互いに関連のない多数の接続にパケットが属しているのであれば、この機能によってスループットが向上することがあります。

手順

ステップ 1 ASP ロード バランシングの自動オン/オフ切り替えを次のようにイネーブルにします。

asp load-balance per-packet auto

ASAv では **auto** キーワードを使用できません。手動で ASP ロード バランシングを有効化または無効化する必要があります。

ステップ 2 次のように手動で ASP ロード バランシングをイネーブルにします。

asp load-balance per-packet

ASP ロード バランシングは、**auto** コマンドを有効にしている場合でも、手動で無効化するまでは有効です。

ステップ 3 次のように ASP ロード バランシングを手動でディセーブルにします。

no asp load-balance per-packet

このコマンドは、手動で ASP ロード バランシングをイネーブルにした場合にのみ適用されます。**auto** コマンドも有効にしている場合、ASP ロード バランシングは自動的に有効または無効な状態に戻ります。

DNS キャッシュのモニタリング

ASA では、特定のクライアントレス SSL VPN および certificate コマンドに送信された外部 DNS クエリーの DNS 情報のローカル キャッシュを提供します。各 DNS 変換要求は、ローカル キャッシュで最初に検索されます。ローカル キャッシュに情報がある場合、結果の IP アドレスが戻されます。ローカルキャッシュで要求を解決できない場合、設定されているさまざまな DNS サーバに DNS クエリーが送信されます。外部 DNS サーバによって要求が解決された場合、結果の IP アドレスが、対応するホスト名とともにローカル キャッシュに格納されます。

DNS キャッシュのモニタリングについては、次のコマンドを参照してください。

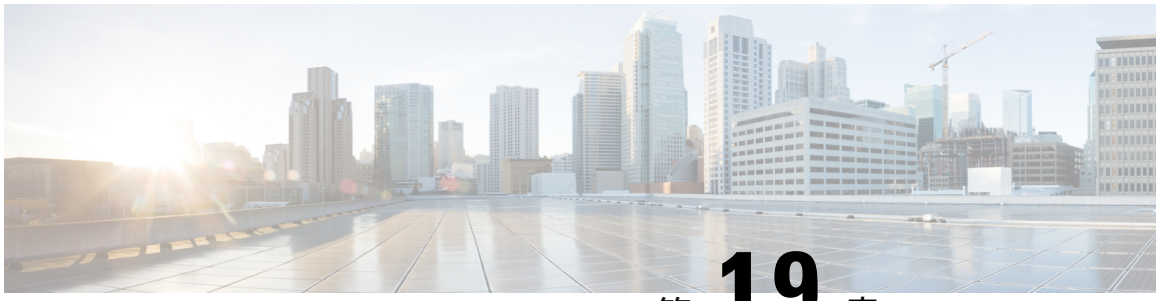
- **show dns-hosts**

  DNS キャッシュを表示します。これには、DNS サーバからダイナミックに学習したエントリと name コマンドを使用して手動で入力された名前および IP アドレスが含まれます。

基本設定の履歴

機能名	プラットフォーム リリース	説明
ISA 3000 ハードウェア バイパス	9.4(1.225)	ISA 3000 は、トラフィックが電源喪失時にアプライアンスを通過し続けるようにするハードウェア バイパス機能をサポートします。 次のコマンドが導入されました。**hardware-bypass**、**hardware-bypass manual**、**hardware-bypass boot-delay**、**show hardware-bypass**
自動 ASP ロード バランシング	9.3(2)	ASP ロードバランシング機能の自動切替を有効または無効に設定できるようになりました。 （注） 自動機能は ASAv ではサポートされません。手動による有効化または無効化のみがサポートされます。 次のコマンドが導入されました。**asp load-balance per-packet-auto**

機能名	プラットフォーム リリース	説明
デフォルトの Telnet パスワードの削除	9.0(2)、9.1(2)	ASA への管理アクセスのセキュリティ向上のために、Telnet のデフォルト ログイン パスワードが削除されました。Telnet を使用してログインする前に、パスワードを手動で設定する必要があります。 （注） ログイン パスワードが使用されるのは、Telnet ユーザ認証（**aaa authentication telnet console** コマンド）を設定しない場合の Telnet に対してのみです。 以前はパスワードをクリアすると、ASA がデフォルト「cisco」を復元していました。今ではパスワードをクリアすると、パスワードは削除されるようになりました。 ログイン パスワードは、スイッチから ASASM への Telnet セッションでも使用されます（**session** コマンドを参照）。最初 ASASM のアクセスでは、ログイン パスワードを設定するまで、**service-module session** コマンドを使用します。 **password** コマンドが変更されました。
パスワード暗号化の可視性	8.4(1)	**show password encryption** コマンドが変更されました。
マスター パスフレーズ	8.3(1)	この機能が導入されました。マスター パスフレーズを利用すると、プレーン テキストのパスワードが安全に、暗号化形式で保存され、1 つのキーを使用してすべてのパスワードを一様に暗号化またはマスキングできるようになります。このようにしても、機能は一切変更されません。 次のコマンドが導入されました。**key config-key password-encryption**、**password encryption aes**、**clear configure password encryption aes**、**show running-config password encryption aes**、**show password encryption**



第 19 章

DHCP サービスと DDNS サービス

この章では、ダイナミック DNS（DDNS）のアップデート方式のほか、DHCP サーバまたは DHCP リレーを設定する方法について説明します。

DHCP サービスと DDNS サービスについて

次の項では、DHCP サーバ、DHCP リレー エージェント、および DDNS 更新について説明します。

DHCPv4 サーバについて

DHCP は、IP アドレスなどのネットワーク コンフィギュレーション パラメータを DHCP クライアントに提供します。ASAはASAインターフェイスに接続されている DHCP クライアントに、DHCP サーバを提供します。DHCP サーバは、ネットワーク コンフィギュレーション パラメータを DHCP クライアントに直接提供します。

IPv4 DHCP クライアントは、サーバに到達するために、マルチキャストアドレスよりもブロードキャストを使用します。DHCP クライアントは UDP ポート 68 でメッセージを待ちます。DHCP サーバは UDP ポート 67 でメッセージを待ちます。

IPv6 の DHCP サーバはサポートされていません。ただし、IPv6 トラフィックの DHCP リレーを有効にできます。

DHCP オプション

DHCP は、TCP/IP ネットワーク上のホストに設定情報を渡すフレームワークを提供します。設定パラメータは DHCP メッセージの Options フィールドにストアされているタグ付けされたアイテムにより送信され、このデータはオプションとも呼ばれます。ベンダー情報も Options に保存され、ベンダー拡張情報はすべて DHCP オプションとして使用できます。

たとえば、Cisco IP Phone が TFTP サーバから設定をダウンロードする場合を考えます。Cisco IP Phone の起動時に、IP アドレスと TFTP サーバの IP アドレスの両方が事前に設定されていない場合、Cisco IP Phone ではオプション 150 または 66 を伴う要求を DHCP サーバに送信して、この情報を取得します。

- DHCP オプション 150 では、TFTP サーバのリストの IP アドレスが提供されます。
- DHCP オプション 66 では、1 つの TFTP サーバの IP アドレスまたはホスト名が与えられます。
- DHCP オプション 3 はデフォルト ルートを設定します。

1 つの要求にオプション 150 と 66 の両方が含まれている場合があります。この場合、両者が ASA ですでに設定されていると、ASA の DHCP サーバは、その応答で両方のオプションに対する値を提供します。

高度な DHCP オプションにより、DNS、WINS、ドメインネームパラメータを DHCP クライアントに提供できます。DNS ドメインサフィックスは DHCP オプション 15 を使用します。これらの値は DHCP 自動設定により、または手動で設定できます。この情報の定義に 2 つ以上の方法を使用すると、次の優先順位で情報が DHCP クライアントに渡されます。

1. 手動で行われた設定
2. 高度な DHCP オプションの設定
3. DHCP 自動コンフィギュレーションの設定

たとえば、DHCP クライアントが受け取るドメイン名を手動で定義し、次に DHCP 自動コンフィギュレーションをイネーブルにできます。DHCP 自動構成によって、DNS サーバおよび WINS サーバとともにドメインが検出されても、手動で定義したドメイン名が、検出された DNS サーバ名および WINS サーバ名とともに DHCP クライアントに渡されます。これは、DHCP 自動構成プロセスで検出されたドメイン名よりも、手動で定義されたドメイン名の方が優先されるためです。

DHCP リレー エージェントについて

インターフェイスで受信した DHCP 要求を 1 つまたは複数の DHCP サーバに転送するように DHCP リレー エージェントを設定できます。DHCP クライアントは、最初の DHCPDISCOVER メッセージを送信するために UDP ブロードキャストを使用します。接続されたネットワークについての情報がクライアントにはないためです。サーバを含まないネットワーク セグメントにクライアントがある場合、ASA はブロードキャスト トラフィックを転送しないため、UDP ブロードキャストは通常転送されません。DHCP リレー エージェントを使用して、ブロード

キャストを受信している ASA のインターフェイスが DHCP 要求を別のインターフェイスの DHCP サーバに転送するように設定できます。

DDNS の概要

DDNS アップデートでは、DNS を DHCP に組み込みます。これら 2 つのプロトコルは相互補完します。DHCP は、IP アドレス割り当てを集中化および自動化します。DDNS アップデートは、割り当てられたアドレスとホスト名の間のアソシエーションを事前定義された間隔で自動的に記録します。DDNS は、頻繁に変わるアドレスとホスト名のアソシエーションを頻繁にアップデートできるようにします。これにより、たとえばモバイルホストは、ユーザまたは管理者が操作することなく、ネットワーク内を自由に移動できます。DDNS は、DNS サーバ上で、名前からアドレスへのマッピングと、アドレスから名前へのマッピングをダイナミックにアップデートして、同期化します。

DDNS の名前とアドレスのマッピングは、DHCP サーバ上で 2 つのリソース レコード（RR）で行われます。A RR では、名前から IP アドレスへのマッピングが保持され、PTR RR では、アドレスから名前へのマッピングが行われます。DDNS 更新を実行するための 2 つの方式（RFC 2136 で規定されている IETF 標準規格、および一般的な HTTP 方式）のうち、ASA では、IETF 方式をサポートしています。

（注） DDNS は BVI またはブリッジ グループのメンバー インターフェイスではサポートされません。

DDNS アップデート コンフィギュレーション

2 つの最も一般的な DDNS アップデート コンフィギュレーションは次のとおりです。

- DHCP クライアントは A RR をアップデートし、DHCP サーバは PTR RR をアップデートします。
- DHCP サーバは、A RR と PTR RR の両方をアップデートします。

通常、DHCP サーバはクライアントの代わりに DNS PTR RR を保持します。クライアントは、必要なすべての DNS アップデートを実行するように設定できます。サーバは、これらのアップデートを実行するかどうかを設定できます。DHCP サーバは、PTR RR をアップデートするクライアントの完全修飾ドメイン名（FQDN）を認識している必要があります。クライアントは Client FQDN と呼ばれる DHCP オプションを使用して、サーバに FQDN を提供します。

UDP パケット サイズ

DDNS は、DNS 要求者が UDP パケットのサイズをアドバタイズできるようにし、512 オクテットより大きいパケットの転送を容易にします。DNS サーバは UDP 上で要求を受信すると、OPT RR から UDP パケット サイズを識別し、要求者により指定された最大 UDP パケット サイズにできるだけ多くのリソース レコードを含めることができるよう、応答のサイズを調整します。DNS パケットのサイズは、BIND の場合は最大 4096 バイト、Windows 2003 DNS サーバの場合は 1280 バイトです。

次に示す追加の **message-length maximum** コマンドを使用できます。

- 既存のグローバル制限：**message-length maximum 512**
- クライアントまたはサーバ固有の制限：**message-length maximum client 4096** および message-length maximum server 4096
- OPT RR フィールドで指定されたダイナミック値：**message-length maximum client auto**

3つのコマンドが同時に存在する場合、ASAは、設定されたクライアントまたはサーバ制限まで長さの自動設定を可能にします。他のすべてのDNSトラフィックについては、message-length maximum が使用されます。

DHCP サービスと DDNS サービスのガイドライン

この項では、DHCPおよびDDNSサービスを設定する前に確認する必要のあるガイドラインおよび制限事項について説明します。

ファイアウォール モード

- DHCP リレーは、トランスペアレント ファイアウォール モード。
- DHCP サーバは、ブリッジグループ メンバー インターフェイス上のトランスペアレント ファイアウォール モードでサポートされます。
- DDNS は、トランスペアレント ファイアウォール モード。

IPv6

DHCP サーバの IPv6 はサポートされません。DHCP リレー の IPv6 は、。

DHCPv4 サーバ

- 使用可能な DHCP の最大プールは 256 アドレスです。
- インターフェイスごとに 1 つの DHCP サーバのみを設定できます。各インターフェイスは、専用のアドレス プールのアドレスを使用できます。しかし、DNS サーバ、ドメイン名、オプション、ping のタイムアウト、WINS サーバなど他の DHCP 設定はグローバルに設定され、すべてのインターフェイス上の DHCP サーバによって使用されます。
- DHCP クライアントや DHCP リレー サービスは、サーバがイネーブルになっているインターフェイス上では設定できません。また、DHCPクライアントは、サーバがイネーブルになっているインターフェイスに直接接続する必要があります。
- ASA は、QIP DHCP サーバと DHCP プロキシ サービスとの併用をサポートしません。
- DHCPサーバもイネーブルになっている場合、リレーエージェントをイネーブルにすることはできません。
- DHCP サーバは、BOOTP 要求をサポートしません。

DHCP リレー

- シングルモードとコンテキストごとに、グローバルおよびインターフェイス固有のサーバを合わせて 10 台までの DHCPv4 リレー サーバを設定できます。インターフェイスごとには、4 台まで設定できます。
- シングル モードとコンテキストごとに、10 台までの DHCPv6 リレー サーバを設定できます。IPv6 のインターフェイス固有のサーバはサポートされません。
- DHCP サーバもイネーブルになっている場合、リレーエージェントをイネーブルにできません。
- DHCP リレー サービスは、トランスペアレント ファイアウォール モード。ただし、アクセス ルールを使用して DHCP トラフィックを通過させることはできます。DHCP 要求と応答がASAを通過できるようにするには、2 つのアクセス ルールを設定する必要があります。1 つは内部インターフェイスから外部（UDP 宛先ポート 67）への DCHP 要求を許可するもので、もう 1 つは逆方向（UDP 宛先ポート 68）に向かうサーバからの応答を許可するためのものです。
- IPv4 の場合、クライアントは直接 ASA に接続する必要があり、他のリレー エージェントやルータを介して要求を送信できません。IPv6 の場合、ASA は別のリレー サーバからのパケットをサポートします。
- DHCP クライアントは、ASA が要求をリレーする DHCP サーバとは別のインターフェイスに存在する必要があります。
- トラフィック ゾーン内のインターフェイスで DHCP リレーを有効にできません。

DHCP サーバの設定

ここでは、ASA の DHCP サーバを設定する方法について説明します。

手順

ステップ 1 DHCPv4 サーバの有効化 （607 ページ）。
ステップ 2 高度な DHCPv4 オプションの設定 （610 ページ）。

DHCPv4 サーバの有効化

ASA のインターフェイスで DHCP サーバをイネーブルにするには、次の手順を実行します。

手順

ステップ 1 インターフェイスの DHCP アドレス プールを作成します。ASA は各クライアントにこのプールのアドレスを 1 つ割り当て、このアドレスを一定時間だけ使用できます。これらのアドレスは、直接接続されているネットワークのための、変換されていないローカル アドレスです。

dhcpd address *ip_address_start-ip_address_end if_name*

例：

```
ciscoasa(config)# dhcpd address 10.0.1.101-10.0.1.110 inside
```

アドレス プールは、ASA インターフェイスと同じサブネット内にある必要があります。トランスペアレント モードでは、ブリッジ グループ メンバー インターフェイスを指定します。

ステップ 2 （任意）（ルーテッド モード）DHCP または PPPoE クライアントを実行するインターフェイスから、または VPN サーバから取得される DNS、WINS、およびドメイン名の値を自動的に構成します。

dhcpd auto_config *client_if_name* [[**vpnclient-wins-override**] **interface** *if_name*]

例：

```
ciscoasa(config)# dhcpd auto_config outside interface inside
```

次のコマンドを使用して DNS、WINS、またはドメイン名パラメータを指定した場合、自動設定で取得されたパラメータが上書きされます。

ステップ 3 （オプション）DNS サーバの IP アドレスを指定します。

dhcpd dns *dns1* [*dns2*]

例：

```
ciscoasa(config)# dhcpd dns 209.165.201.2 209.165.202.129
```

ステップ 4 （オプション）WINS サーバの IP アドレスを指定します。WINS サーバは最大 2 つまでです。

dhcpd wins *wins1* [*wins2*]

例：

```
ciscoasa(config)# dhcpd wins 209.165.201.5
```

ステップ 5 （任意）クライアントに許可するリース期間を変更します。リース期間とは、割り当てられた IP アドレスをクライアントが使用できる時間の長さ（秒）であり、この時間が経過するとリースは失効します。0 ～ 1,048,575 の範囲の数を入力してください。デフォルト値は 3600 秒です。

dhcpd lease *lease_length*

例：

```
ciscoasa(config)# dhcpd lease 3000
```

ステップ 6 （オプション）ドメイン名を設定します。

dhcpd domain *domain_name*

例：

```
ciscoasa(config)# dhcpd domain example.com
```

ステップ 7 （オプション）ICMP パケットの DHCP ping タイムアウト値を設定します。アドレスの競合を避けるために、ASA はアドレスを DHCP クライアントに割り当てる前に 2 つの ICMP ping パケットをそのアドレスに送信します。デフォルト値は 50 ミリ秒です。

dhcpd ping timeout *milliseconds*

例：

```
ciscoasa(config)# dhcpd ping timeout 20
```

ステップ 8 DHCP クライアントに送信するデフォルト ゲートウェイを定義します。ルーテッド モードで **dhcpd option 3 ip** コマンドを使用しない場合、ASA は、DHCP サーバがイネーブルになっているインターフェイス IP アドレスをデフォルト ゲートウェイとして送信します。トランスペアレント モードでデフォルト ゲートウェイを設定する場合には **dhcpd option 3 ip** を設定する必要があります。ASA 自体はデフォルト ゲートウェイとして動作できません。

dhcpd option 3 ip *gateway_ip*

例：

```
ciscoasa(config)# dhcpd option 3 ip 10.10.1.1
```

ステップ 9 ASA内のDHCPデーモンをイネーブルにし、イネーブルになったインターフェイス上でDHCPクライアント要求をリッスンします。

dhcpd enable *interface_name*

例：

```
ciscoasa(config)# dhcpd enable inside
```

dhcpd address 範囲と同じインターフェイスを指定します。

高度な DHCPv4 オプションの設定

ASA は、RFC 2132、RFC 2562、および RFC 5510 に記載されている情報を送信する DHCP オプションをサポートしています。オプション 1、12、50 ～ 54、58 ～ 59、61、67、82 を除き、すべての DHCP オプション（1 ～ 255）がサポートされています。

手順

ステップ 1 1 つまたは 2 つの IP アドレスを返す DHCP オプションを設定します。

dhcpd option *code* **ip** *addr_1* [*addr_2*]

例：

```
ciscoasa(config)# dhcpd option 150 ip 10.10.1.1
ciscoasa(config)# dhcpd option 3 ip 10.10.1.10
```

オプション 150 では、Cisco IP Phone で使用する 1 台または 2 台の TFTP サーバの IP アドレスまたは名前を指定します。オプション 3 では、Cisco IP Phone のデフォルト ルートを設定します。

ステップ 2 テキスト文字列を返す DHCP オプションを設定します。

dhcpd option *code* **ascii** *text*

例：

```
ciscoasa(config)# dhcpd option 66 ascii exampleserver
```

オプション 66 では、Cisco IP Phone で使用する TFTP サーバの IP アドレスまたは名前を指定します。

ステップ 3 16 進数値を返す DHCP オプションを設定します。

dhcpd option code hex *value*

例：

```
ciscoasa(config)# dhcpd option 2 hex 22.0011.01.FF1111.00FF.0000.AAAA.1111.1111.1111.11
```

（注） ASA は、指定されたオプションのタイプおよび値が、RFC 2132 に定義されているオプション コードに対して期待されているタイプおよび値と一致するかどうかは確認しません。たとえば、**dhcpd option 46 ascii hello** というコマンドを入力することは可能であり、ASA はこのコンフィギュレーションを受け入れますが、RFC 2132 の定義では、オプション 46 には 1 桁の 16 進数値を指定することになっています。オプション コードと、コードに関連付けられたタイプおよび期待値の詳細については、RFC 2132 を参照してください。

次の表に、**dhcpd option** コマンドでサポートされていない DHCP オプションを示します。

表 *21* : サポートされていない *DHCP* オプション

オプション コード	説明
0	DHCPOPT_PAD
1	HCPOPT_SUBNET_MASK
12	DHCPOPT_HOST_NAME
50	DHCPOPT_REQUESTED_ADDRESS
51	DHCPOPT_LEASE_TIME
52	DHCPOPT_OPTION_OVERLOAD
53	DHCPOPT_MESSAGE_TYPE
54	DHCPOPT_SERVER_IDENTIFIER
58	DHCPOPT_RENEWAL_TIME
59	DHCPOPT_REBINDING_TIME
61	DHCPOPT_CLIENT_IDENTIFIER
67	DHCPOPT_BOOT_FILE_NAME
82	DHCPOPT_RELAY_INFORMATION
255	DHCPOPT_END

DHCP リレー エージェントの設定

インターフェイスに DHCP 要求が届くと、ユーザの設定に基づいて、ASA からその要求がリレーされる DHCP サーバが決定されます。設定できるサーバのタイプは次のとおりです。

- インターフェイス固有の DHCP サーバ：特定のインターフェイスに DHCP 要求が届くと、ASA はその要求をインターフェイス固有のサーバにだけリレーします。
- グローバル DHCP サーバ：インターフェイス固有のサーバが設定されていないインターフェイスに DHCP 要求が届くと、ASA はその要求をすべてのグローバル サーバにリレーします。インターフェイスにインターフェイス固有のサーバが設定されている場合、グローバル サーバは使用されません。

DHCPv4 リレー エージェントの設定

DHCP 要求がインターフェイスに届くと、ASA はその要求を DHCP サーバにリレーします。

手順

ステップ 1 次のいずれかまたは両方を実行します。

- グローバル DHCP サーバの IP アドレスおよびそのサーバに到達可能なインターフェイスを指定します。

  dhcprelay server *ip_address if_name*

  例：

```
ciscoasa(config)# dhcprelay server 209.165.201.5 outside
ciscoasa(config)# dhcprelay server 209.165.201.8 outside
ciscoasa(config)# dhcprelay server 209.165.202.150 it
```

- DHCP クライアント ネットワークに接続されているインターフェイス ID、およびそのインターフェイスで受信した DHCP 要求に対して使用される DHCP サーバの IP アドレスを指定します。

```
interface interface_id
  dhcprelay server ip_address
```

  例：

```
ciscoasa(config)# interface gigabitethernet 0/0
ciscoasa(config)# dhcprelay server 209.165.201.6
ciscoasa(config)# dhcprelay server 209.165.201.7
ciscoasa(config)# interface gigabitethernet 0/1
ciscoasa(config)# dhcprelay server 209.165.202.155
ciscoasa(config)# dhcprelay server 209.165.202.156
```

  グローバル **dhcprelay server** コマンドとは異なり、要求の出力インターフェイスは指定しないことに注意してください。代わりに、ASA はルーティング テーブルを使用して出力インターフェイスを決定します。

ステップ 2 DHCP クライアントに接続されたインターフェイス上で DHCP リレー サービスをイネーブルにします。複数のインターフェイス上で DHCP リレーをイネーブルにできます。

dhcprelay enable *interface*

例：

```
ciscoasa(config)# dhcprelay enable inside
ciscoasa(config)# dhcprelay enable dmz
ciscoasa(config)# dhcprelay enable eng1
ciscoasa(config)# dhcprelay enable eng2
ciscoasa(config)# dhcprelay enable mktg
```

ステップ 3 （オプション）DHCP リレーのアドレス処理のために許容する時間を秒数で設定します。

dhcprelay timeout *seconds*

例：

```
ciscoasa(config)# dhcprelay timeout 25
```

ステップ 4 （オプション）DHCP サーバから送信されたパケットの最初のデフォルト ルータ アドレスを、ASA インターフェイスのアドレスに変更します。

dhcprelay setroute *interface_name*

例：

```
ciscoasa(config)# dhcprelay setroute inside
```

このアクションを行うと、クライアントは、自分のデフォルト ルートを設定して、DHCP サーバで異なるルータが指定されている場合でも、ASA をポイントすることができます。

パケット内にデフォルトのルータ オプションがなければ、ASA は、そのインターフェイスのアドレスを含んでいるデフォルト ルータを追加します。

ステップ 5 （オプション）インターフェイスを信頼できるインターフェイスとして設定します。次のいずれかを実行します。

- 信頼する DHCP クライアント インターフェイスを指定します。

```
interface interface_id
  dhcprelay information trusted
```

例：

```
ciscoasa(config)# interface gigabitethernet 0/0
ciscoasa(config-if)# dhcprelay information trusted
```

DHCP Option 82 を維持するために、インターフェイスを信頼できるインターフェイスとして設定できます。DHCP Option 82 は、DHCP スヌーピングおよび IP ソース ガードのために、ダウンストリームのスイッチおよびルータによって使用されます。通常、ASA DHCP リレー エージェントが Option 82 をすでに設定した DHCP パケットを受信しても、giaddr フィールド（サーバにパケットを転送する前に、リレー エージェントによって設定された DHCP リレー エージェント アドレスを指定するフィールド）が 0 に設定されている場合は、ASA はそのパケットをデフォルトで削除します。インターフェイスを信頼できるインターフェイスとして指定することで、Option 82 を維持したままパケットを転送できます。

- すべてのクライアント インターフェイスを信頼するインターフェイスとして設定します。

dhcprelay information trust-all

例：

```
ciscoasa(config)# dhcprelay information trust-all
```

DHCPv6 リレー エージェントの設定

インターフェイスに DHCPv6 要求が届くと、ASA はその要求をすべての DHCPv6 グローバル サーバにリレーします。

手順

ステップ 1 クライアント メッセージの転送先となる IPv6 DHCP サーバの宛先アドレスを指定します。

ipv6 dhcprelay server *ipv6_address* [*interface*]

例：

```
ciscoasa(config)# ipv6 dhcprelay server 3FFB:C00:C18:6:A8BB:CCFF:FE03:2701
```

ipv6-address 引数には、リンク スコープのユニキャスト、マルチキャスト、サイト スコープのユニキャスト、またはグローバル IPv6 アドレスを指定できます。リレー宛先の指定は必須です。ループバックやノードローカルのマルチキャスト アドレスは指定できません。オプションの *interface* 引数では、宛先に対する出力インターフェイスを指定します。クライアントのメッセージは、この出力インターフェイスが接続されたリンクを経由して宛先アドレスに転送されます。指定したアドレスがリンク スコープのアドレスである場合は、インターフェイスを指定する必要があります。

ステップ 2 インターフェイス上で DHCPv6 リレー サービスをイネーブルにします。

ipv6 dhcprelay enable *interface*

例：

```
ciscoasa(config)# ipv6 dhcprelay enable inside
```

ステップ 3 （オプション）リレー アドレスの処理のために、リレー バインディングを通して DHCPv6 サーバからの応答を DHCPv6 クライアントに渡すときに許容する時間を秒数で指定します。

ipv6 dhcprelay timeout *seconds*

例：

```
ciscoasa(config)# ipv6 dhcprelay timeout 25
```

seconds 引数の有効な値の範囲は 1 ～ 3600 です。デフォルトは 60 秒です。

DDNS の設定

ここでは、DDNS の設定方法について説明します。

スタティック IP アドレスの A RR と PTR RR の両方のアップデート

クライアントを設定して、スタティック IP アドレスの A RR と PTR RR の両方をアップデートするように要求するには、次の手順を実行します。

手順

ステップ 1 DNS RR を動的にアップデートする DDNS アップデート方式を作成します。

ddns update method *name*

例：

```
ciscoasa(config)# ddns update method ddns-2
```

ステップ 2 クライアントが DNS の A RR と PTR RR の両方をアップデートすることを指定します。

ddns both

例：

```
ciscoasa(DDNS-update-method)# ddns both
```

ステップ 3 インターフェイスを設定し、インターフェイスの設定モードを開始します。

interface *mapped_name*

例：

```
ciscoasa(DDNS-update-method)# interface eth1
```

ステップ 4 DDNS 方式とインターフェイスおよびアップデート ホスト名を関連付けます。

ddns update [*method-name* | **hostname** *hostname*]

例：

```
ciscoasa(config-if)# ddns update ddns-2
ciscoasa(config-if)# ddns update hostname asa.example.com
```

ステップ 5 インターフェイスのスタティック IP アドレスを設定します。

ip address *ip_address* [*mask*] [*standby ip_address*]

例：

```
ciscoasa(config-if)# ip address 10.0.0.40 255.255.255.0
```

A RR と PTR RR の両方のアップデート

DHCP クライアントを設定して、A RR と PTR RR の両方をアップデートするように要求するとともに、DHCPサーバがこれらの要求を受け取るように要求するには、次の手順を実行します。

手順

ステップ 1 DHCPサーバがアップデートを実行しないことを要求するようにDHCPクライアントを設定します。

dhcp-client update dns [**server** {**both** |**none**}]

例：

```
ciscoasa(config)# dhcp-client update dns server none
```

ステップ 2 DNS RR を動的にアップデートする DDNS アップデート方式を作成します。

ddns update method *name*

例：

```
ciscoasa(config)# ddns update method ddns-2
```

ステップ 3 クライアントが DNS の A RR と PTR RR の両方をアップデートすることを指定します。

ddns both

例：

例：

```
ciscoasa(DDNS-update-method)# ddns both
```

ステップ 4 インターフェイスを設定し、インターフェイスの設定モードを開始します。

interface *mapped_name*

例：

```
ciscoasa(DDNS-update-method)# interface Ethernet0
```

ステップ 5 DDNS 方式とインターフェイスおよびアップデート ホスト名を関連付けます。

ddns update [*method-name* | **hostname** *hostname*]

例：

```
ciscoasa(config-if)# ddns update ddns-2
ciscoasa(config-if)# ddns update hostname asa.example.com
```

ステップ 6 DHCP を使用して インターフェイスの IP アドレスを取得します。

ip address dhcp

例：

```
ciscoasa(if-config)# ip address dhcp
```

ステップ 7 DDNS アップデートを実行するように DHCP サーバを設定します。

dhcpd update dns [**both**] [**override**] [**interface** *srv_ifc_name*]

例：

```
ciscoasa(if-config)# dhcpd update dns
```

両方の RR へのアップデートを無視

DHCP クライアントを設定して、DHCP サーバに A と PTR のどちらのアップデートも受け取らないように指示する FQDN オプションを含めるには、次の手順を実行します。

手順

ステップ 1 DNS RR を動的にアップデートする DDNS アップデート方式を作成します。

ddns update method *name*

例：

```
ciscoasa(config)# ddns update method ddns-2
```

ステップ 2 クライアントが DNS の A RR と PTR RR の両方をアップデートすることを指定します。

ddns both

例：

```
ciscoasa(DDNS-update-method)# ddns both
```

ステップ 3 インターフェイスを設定し、インターフェイスの設定モードを開始します。

interface *mapped_name*

例：

```
ciscoasa(DDNS-update-method)# interface Ethernet0
```

ステップ 4 DDNS 方式とインターフェイスおよびアップデート ホスト名を関連付けます。

ddns update [*method-name* | **hostname** *hostname*]

例：

```
ciscoasa(config-if)# ddns update ddns-2
ciscoasa(config-if)# ddns update hostname asa.example.com
```

ステップ 5 DHCP サーバがアップデートを実行しないことを要求するように DHCP クライアントを設定します。

dhcp-client update dns [**server** {**both** |**none**}]

例：

```
ciscoasa(config)# dhcp-client update dns server none
```

ステップ 6 DHCP を使用して インターフェイスの IP アドレスを取得します。

ip address dhcp

例：

```
ciscoasa(if-config)# ip address dhcp
```

ステップ 7 クライアントのアップデート要求を上書きするように DHCP サーバを設定します。

dhcpd update dns [**both**] [**override**] [**interface** *srv_ifc_name*]

例：

```
ciscoasa(if-config)# dhcpd update dns both override
```

PTR RR のみのアップデート

サーバを設定して、デフォルトで PTR RR のアップデートのみを実行するには、次の手順を実行します。

手順

ステップ 1 インターフェイスを設定します。

interface *mapped_name*

例：

```
ciscoasa(config)# interface Ethernet0
```

ステップ 2 DHCP サーバが DNS の A RR と PTR RR の両方をアップデートすることを要求します。

dhcp-client update dns [**server** {**both** |**none**}]

例：

```
ciscoasa(config-if)# dhcp-client update dns both
```

ステップ 3 設定されたインターフェイスで DHCP クライアントを設定します。

ddns update [*method-name* | **hostname** *hostname*]

例：

```
ciscoasa(config-if)# ddns update hostname asa
```

ステップ 4 DDNS アップデートを実行するように DHCP サーバを設定します。

dhcpd update dns [**both**] [**override**] [**interface** *srv_ifc_name*]

例：

```
ciscoasa(config-if)# dhcpd update dns
```

ステップ 5 DHCP クライアントの DNS ドメイン名を定義します。

dhcpd domain *domain_name* [**interface** *if_name*]

例：

```
ciscoasa(config-if)# dhcpd domain example.com
```

クライアントでの RR のアップデートとサーバでの PTR RR のアップデート

クライアントを設定して A リソース レコードをアップデートするとともに、サーバを設定して PTR レコードをアップデートするには、次の手順を実行します。

手順

ステップ 1 DNS RR を動的にアップデートする DDNS アップデート方式を作成します。

ddns update method *name*

例：

```
ciscoasa(config)# ddns update method ddns-2
```

ステップ 2 DDNS のアップデート方式を指定します。

ddns both

例：

```
ciscoasa(DDNS-update-method)# ddns both
```

ステップ 3 インターフェイスを設定します。

interface *mapped_name*

例：

```
ciscoasa(DDNS-update-method)# interface Ethernet0
```

ステップ 4 DHCP クライアントが DHCP サーバに渡すアップデート パラメータを設定します。

dhcp-client update dns [**server** {**both** | **none**}]

例：

```
ciscoasa(config-if)# dhcp-client update dns
```

ステップ 5 DDNS 方式とインターフェイスおよびアップデート ホスト名を関連付けます。

ddns update [*method-name* | **hostname** *hostname*]

例：

```
ciscoasa(config-if)# ddns update ddns-2
ciscoasa(config-if)# ddns update hostname asa
```

ステップ 6 DDNS アップデートを実行するように DHCP サーバを設定します。

dhcpd update dns [**both**] [**override**] [**interface** *srv_ifc_name*]

例：

```
ciscoasa(if-config)# dhcpd update dns
```

ステップ 7 DHCP クライアントの DNS ドメイン名を定義します。

dhcpd domain *domain_name* [**interface** *if_name*]

例：

```
ciscoasa(config-if)# dhcpd domain example.com
```

DHCP および DDNS サービスのモニタリング

この項では、DHCP および DDNS の両方のサービスをモニタする手順について説明します。

DHCP サービスのモニタリング

- **show dhcpd** {**binding** [*IP_address*] | **state** | **statistics**}

  このコマンドは、現在の DHCP サーバ クライアント バインディング、状態と統計情報を示します。

- **show dhcprelay** {**state** | **statistics**}

  このコマンドは、DHCP リレー ステータスと統計情報を表示します。

- **show ipv6 dhcprelay binding**

  このコマンドは、リレー エージェントによって作成されたリレー バインディング エントリを表示します。

- **show ipv6 dhcprelay statistics**

  このコマンドは、IPv6 の DHCP リレー エージェントの統計情報を表示します。

DDNS ステータスのモニタリング

DDNS ステータスのモニタリングについては、次のコマンドを参照してください。

- **show running-config ddns**

  このコマンドは、現在の DDNS コンフィギュレーションを表示します。

- **show running-config dns server-group**

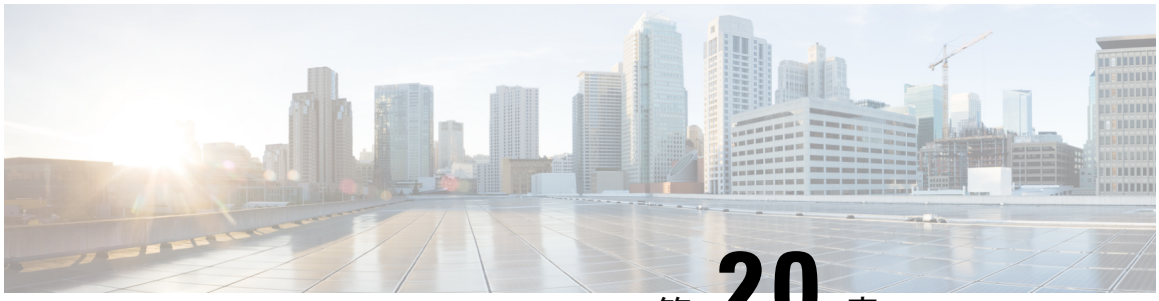
  このコマンドは、現在の DNS サーバ グループのステータスを表示します。

DHCP および DDNS サービスの履歴

機能名	プラットフォーム リリース	説明
DHCP	7.0(1)	ASA は、DHCP サーバまたは DHCP リレー サービスを ASA のインターフェイスに接続されている DHCP クライアントに提供することができます。 次のコマンドを導入しました。**dhcp client update dns**、 **dhcpd address**、**dhcpd domain**、**dhcpd enable**、 **dhcpd lease**、**dhcpd option**、**dhcpd ping timeout**、**dhcpd update dns**、**dhcpd wins**、**dhcp-network-scope**、**dhcprelay enable**、**dhcprelay server**、**dhcprelay setroute**、**dhcp-server**、**show running-config dhcpd**、および **show running-config dhcprelay**。
DDNS	7.0(1)	この機能が導入されました。 **ddns**、**ddns update**、**dhcp client update dns**、**dhcpd update dns**、**show running-config ddns**、および **show running-config dns server-group** の各コマンドが導入されました。
DHCP relay for IPv6 (DHCPv6)	9.0(1)	DHCP リレーに IPv6 サポートが追加されました。 **ipv6 dhcprelay server**、**ipv6 dhcprelay enable**、**ipv6 dhcprelay timeout**、**clear config ipv6 dhcprelay**、**ipv6 nd managed-config-flag**、**ipv6 nd other-config-flag**、**debug ipv6 dhcp**、**debug ipv6 dhcprelay**、**show ipv6 dhcprelay binding**、**clear ipv6 dhcprelay binding**、**show ipv6 dhcprelay statistics**、**clear ipv6 dhcprelay statistics** の各コマンドが導入されました。

機能名	プラットフォーム リリース	説明
インターフェイスごとのDHCPリレーサーバ（IPv4 のみ）	9.1(2)	DHCP リレー サーバをインターフェイスごとに設定できるようになりました。特定のインターフェイスに届いた要求は、そのインターフェイス用に指定されたサーバに対してのみリレーされます。インターフェイス単位の DHCP リレーでは、IPv6 はサポートされません。 **dhcprelay server**（インターフェイス設定モード）、**clear configure dhcprelay**、**show running-config dhcprelay** の各コマンドが導入または変更されました。
DHCP の信頼できるインターフェイス	9.1(2)	DHCP Option 82 を維持するために、インターフェイスを信頼できるインターフェイスとして設定できるようになりました。DHCP Option 82 は、DHCP スヌーピングおよび IP ソース ガードのために、ダウンストリームのスイッチおよびルータによって使用されます。通常、ASA DHCP リレー エージェントが Option 82 をすでに設定した DHCP パケットを受信しても、giaddr フィールド（サーバにパケットを転送する前に、リレー エージェントによって設定された DHCP リレー エージェント アドレスを指定するフィールド）が 0 に設定されている場合は、ASA はそのパケットをデフォルトで削除します。インターフェイスを信頼できるインターフェイスとして指定することで、Option 82 を維持したままパケットを転送できます。 **dhcprelay information trusted**、**dhcprelay information trust-all**、**show running-config dhcprelay** の各コマンドが導入または変更されました。

機能名	プラットフォーム リリース	説明
DHCP 再バインド機能	9.1(4)	DHCP再バインドフェーズに、クライアントはトンネル グループ リスト内の他のDHCPサーバへの再バインドを試みるようになりました。このリリース以前には、DHCP リースの更新に失敗した場合、クライアントは代替サーバへ再バインドしませんでした。 導入または変更されたコマンドはありません。
DHCP リレー サーバは、応答用の DHCP サーバ識別子を確認します。	9.2(4)/ 9.3(3)	ASA DHCP リレー サーバが不適切な DHCP サーバから応答を受信すると、応答を処理する前に、その応答が適切なサーバからのものであることを確認するようになりました。導入または変更されたコマンドはありません。変更された ASDM 画面はありません。 導入または変更されたコマンドはありません。
DHCPv6 モニタリング	9.4(1)	IPv6 の DHCP 統計情報および IPv6 の DHCP バインディングをモニタできます。



第 20 章

デジタル証明書

この章では、デジタル証明書の設定方法について説明します。

デジタル証明書の概要

デジタル証明書は、認証に使用されるデジタル ID を保持しています。デジタル証明書には、名前、シリアル番号、会社、部門、または IP アドレスなど、ユーザまたはデバイスを識別する情報が含まれます。CA は、証明書に「署名」してその認証を確認することで、デバイスまたはユーザのアイデンティティを保証する、信頼できる機関です。CA は、公開キーまたは秘密キーの暗号化を使用してセキュリティを保証する PKI コンテキストで、デジタル証明書を発行します。

デジタル証明書を使用して認証を行う場合は、ASA に 1 つ以上の ID 証明書と、その発行元の CA 証明書が必要です。この設定では、複数のアイデンティティ、ルート、および証明書の階層が許可されます。ASA では CRL（認証局の失効リストとも呼ばれます）に照らしてサードパーティの証明書を検証します。検証は、ID 証明書から下位証明書チェーンの認証局までさかのぼって行われます。

次に、使用可能な各種デジタル証明書について説明します。

- CA 証明書は、他の証明書に署名するために使用されます。これは自己署名され、ルート証明書と呼ばれます。別の CA 証明書により発行される証明書は、下位証明書と呼ばれます。
- ID 証明書は、特定のシステムまたはホストの証明書です。この証明書も CA により発行されます。

- コード署名者証明書は、コードに署名するためのデジタル署名を作成する際に使用される特殊な証明書であり、署名されたコードそのものが証明書の作成元を示しています。

ローカルCAは、ASAの独立認証局機能を統合したもので、証明書の配布と、発行された証明書に対するセキュアな失効チェックを行います。Web サイトのログイン ページからユーザ登録を行う場合には、ローカル CA により実現されるセキュアで設定可能な内部認証局機能によって、証明書の認証を行うことができます。

（注） CA 証明書および ID 証明書は、サイトツーサイト VPN 接続およびリモート アクセス VPN 接続の両方に適用されます。このマニュアルに記載の手順は、ASDM GUI でリモート アクセス VPN を使用する場合の手順です。

デジタル証明書は、認証に使用されるデジタル ID を保持しています。デジタル証明書には、名前、シリアル番号、会社、部門、または IP アドレスなど、ユーザまたはデバイスを識別する情報が含まれます。CA は、証明書に「署名」してその認証を確認することで、デバイスまたはユーザのアイデンティティを保証する、信頼できる機関です。CA は、公開キーまたは秘密キーの暗号化を使用してセキュリティを保証する PKI コンテキストで、デジタル証明書を発行します。

デジタル証明書を使用して認証を行う場合は、ASA に 1 つ以上の ID 証明書と、その発行元の CA 証明書が必要です。この設定では、複数のアイデンティティ、ルート、および証明書の階層が許可されます。次に、使用可能な各種デジタル証明書について説明します。

- CA 証明書は、他の証明書に署名するために使用されます。これは自己署名され、ルート証明書と呼ばれます。
- 別の CA 証明書により発行される証明書は、下位証明書と呼ばれます。

CA は、証明書要求の管理とデジタル証明書の発行を行います。デジタル証明書には、名前、シリアル番号、会社、部門、または IP アドレスなど、ユーザまたはデバイスを識別する情報が含まれます。デジタル証明書には、ユーザまたはデバイスの公開キーのコピーも含まれています。CA は、信頼できるサードパーティ（VeriSign など）の場合もあれば、組織内に設置したプライベート CA（インハウス CA）の場合もあります。

ヒント 証明書コンフィギュレーションおよびロード バランシングの例は、次の URL を参照してください。https://supportforums.cisco.com/docs/DOC-5964

公開キー暗号化

デジタル署名は、公開キー暗号化によってイネーブルになり、デバイスおよびユーザを認証する手段です。RSA 暗号化システムなどの Public Key Cryptography では、各ユーザは、公開キーと秘密キーの両方を含むキーペアを使用します。これらのキーは、補足として機能し、一方で暗号化されたものは、もう一方で復号化できます。

簡単に言えば、データが秘密キーで暗号化されたとき、署名が形成されます。署名はデータに付加されて受信者に送信されます。受信者は送信者の公開キーをデータに適用します。データとともに送信された署名が、公開キーをデータに適用した結果と一致した場合、メッセージの有効性が確立されます。

このプロセスは、受信者が送信者の公開キーのコピーを持っていること、およびその公開キーが送信者になりすました別人のものではなく、送信者本人のものであることを受信者が強く確信していることに依存しています。

通常、送信者の公開キーは外部で取得するか、インストール時の操作によって取得します。たとえば、ほとんどの Web ブラウザでは、いくつかの CA のルート証明書がデフォルトで設定されています。VPN の場合、IKE プロトコルは IPsec のコンポーネントであり、デジタル署名を使用してピア デバイスを認証した後で、セキュリティ アソシエーションをセットアップできます。

証明書のスケーラビリティ

デジタル証明書がない場合、通信するピアごとに各 IPsec ピアを手動で設定する必要があります。そのため、ネットワークにピアを新たに追加するたびに、安全に通信するために各ピアで設定変更を行わなければなりません。

デジタル証明書を使用している場合、各ピアは CA に登録されます。2 つのピアは、通信を試みるときに、証明書とデジタル署名されたデータを交換して、相互の認証を行います。新しいピアがネットワークに追加された場合は、そのピアを CA に登録するだけで済みます。他のピアを修正する必要はありません。新しいピアが IPSec 接続を試みると、証明書が自動的に交換され、そのピアの認証ができます。

CA を使用した場合、ピアはリモート ピアに証明書を送り、公開キー暗号化を実行することによって、そのリモート ピアに対して自分自身を認証します。各ピアから、CA によって発行された固有の証明書が送信されます。このプロセスが機能を果たすのは、関連付けられているピアの公開キーが各証明書にカプセル化され、各証明書が CA によって認証され、参加しているすべてのピアによって CA が認証権限者として認識されるためです。このプロセスは、RSA 署名付きの IKE と呼ばれます。

ピアは、証明書が期限満了になるまで、複数の IPSec セッションに対して、および複数の IPSec ピア宛てに証明書を送り続けることができます。証明書が期限満了になったときは、ピアの管理者は新しい証明書を CA から入手する必要があります。

CA は、IPSec に参加しなくなったピアの証明書を無効にすることもできます。無効にされた証明書は、他のピアからは有効な証明書とは認識されなくなります。無効にされた証明書は CRL に記載され、各ピアは別のピアの証明書を受け取る前に、CRL をチェックします。

CA の中には、実装の一部として RA を持つものもあります。RA は CA のプロキシの役割を果たすサーバであるため、CA が使用できないときも CA 機能は継続しています。

キーペア

キー ペアは、RSA または楕円曲線署名アルゴリズム（ECDSA）キーであり、次の特性があります。

- RSA キーは SSH や SSL に使用できます。
- SCEP 登録は、RSA キーの証明書をサポートしています。
- RSA キー サイズの最大値は 4096 で、デフォルトは 2048 です。
- ECDSA キー長の最大値は 521 で、デフォルトは 384 です。
- 署名にも暗号化にも使用できる汎用 RSA キー ペアを生成することも、署名用と暗号化用に別々の RSA キー ペアを生成することもできます。SSL では署名用ではなく暗号化用のキーが使用されるので、署名用と暗号化用にキーを分けると、キーが公開される頻度を少なくすることができます。ただし、IKE では暗号化用ではなく署名用のキーが使用されます。キーを用途別に分けることで、キーの公開頻度が最小化されます。

トラストポイント

トラストポイントを使用すると、CA と証明書の管理とトレースができます。トラストポイントとは、CA または ID ペアを表現したものです。トラストポイントには、CA の ID、CA 固有のコンフィギュレーション パラメータ、登録されている ID 証明書とのアソシエーションが含まれています。

トラストポイントの定義が完了したら、CA の指定を必要とするコマンドで、名前によってトラストポイントを参照できます。トラストポイントは複数設定できます。

（注） Cisco ASA に同じ CA を共有するトラストポイントが複数ある場合、CA を共有するトラストポイントのうち、ユーザ証明書の検証に使用できるのは 1 つだけです。CA を共有するどのトラストポイントを使用して、その CA が発行したユーザ証明書を検証するかを制御するには、**support-user-cert-validation** コマンドを使用します。

自動登録の場合は、登録 URL がトラストポイントに設定されている必要があり、また、トラストポイントが示す CA がネットワーク上で使用可能であり、SCEP をサポートしている必要があります。

キーペアと、トラストポイントに関連付けられている発行済み証明書は、PKCS12 形式でエクスポートとインポートができます。この形式は、異なる ASA 上のトラストポイント コンフィギュレーションを手動でコピーする場合に便利です。

認証登録

ASA は、トラストポイントごとに 1 つの CA 証明書が必要で、セキュリティ アプライアンス自体には、トラストポイントで使用するキーのコンフィギュレーションに応じて 1 つまたは 2 つの証明書が必要です。トラストポイントが署名と暗号化に別々の RSA キーを使用する場合、

ASA には署名用と暗号化用の 2 つの証明書が必要になります。署名用と暗号化用のキーが同じである場合、必要な証明書は 1 つだけです。

ASA は、SCEP を使用した自動登録と、base-64-encoded 証明書を直接端末に貼り付けられる手動登録をサポートしています。サイトツーサイト VPN の場合は、各 ASA を登録する必要があります。リモート アクセス VPN の場合は、各 ASA と各リモート アクセス VPN クライアントを登録する必要があります。

SCEP 要求のプロキシ

ASA は、AnyConnect とサードパーティ CA 間の SCEP 要求のプロキシとして動作することができます。プロキシとして動作する場合に必要なのは CA が ASA からアクセス可能であることのみです。ASA のこのサービスが機能するには、ASA が登録要求を送信する前に、ユーザが AAA でサポートされているいずれかの方法を使用して認証されている必要があります。また、ホスト スキャンおよびダイナミック アクセス ポリシーを使用して、登録資格のルールを適用することもできます。

ASA は、AnyConnect SSL または IKEv2 VPN セッションでのみこの機能をサポートしています。これは、Cisco IOS CS、Windows Server 2003 CA、および Windows Server 2008 CA を含む、すべての SCEP 準拠 CA をサポートしています。

クライアントレス（ブラウザベース）でのアクセスは SCEP プロキシをサポートしていませんが、WebLaunch（クライアントレス起動 AnyConnect）はサポートしていません。

ASA は、証明書のポーリングはサポートしていません。

ASA はこの機能に対するロード バランシングをサポートしています。

失効チェック

証明書は発行されると、一定期間有効です。CA は、安全上の問題や名前またはアソシエーションの変更などの理由で、期限が切れる前に証明書を無効にすることがあります。CA は、無効になった証明書の署名付きリストを定期的に発行します。失効確認を有効にすることにより、CA が認証にその証明書を使用するたびに、その証明書が無効にされていないかどうか、ASA によってチェックされます。

失効確認を有効にすると、PKI 証明書検証プロセス時に ASA によって証明書の失効ステータスがチェックされます。これには、CRL チェック、OCSP、またはその両方が使用されます。OCSP は、最初の方式がエラーを返した場合に限り使用されます（たとえば、サーバが使用不可であることを示すエラー）。

CRL チェックを使用すると、ASA によって、無効になった（および失効解除された）証明書とその証明書シリアル番号がすべてリストされている CRL が取得、解析、およびキャッシュされます。ASA は CRL（認証局の失効リストとも呼ばれます）に基づいて証明書を検証します。検証は、ID 証明書から下位証明書チェーンの認証局までさかのぼって行われます。

OCSP は、検証局に特定の証明書のステータスを問い合わせ、チェックを検証局が扱う範囲に限定するため、よりスケーラブルな方法を提供します。

サポート対象の CA サーバ

ASA は次の CA サーバをサポートしています。

Cisco IOS CS、ASA ローカル CA、およびサードパーティの X.509 準拠 CA ベンダー（次のベンダーが含まれますが、これらに限定はされません）。

- Baltimore Technologies
- Entrust
- Digicert
- Geotrust
- GoDaddy
- iPlanet/Netscape
- Microsoft Certificate Services
- RSA Keon
- Thawte
- VeriSign

CRL

CRL は、有効期間内の証明書が発行元の CA によって無効にされているかどうかを ASA が判断するための 1 つの方法です。CRL コンフィギュレーションは、トラストポイントのコンフィギュレーションの一部です。

証明書を認証するときに必ず **revocation-check crl** コマンドを使用して CRL チェックを行うように、ASA を設定できます。また、**revocation-check crl none** コマンドを使用して、CRL チェックをオプションにすることもできます。オプションにすると、更新された CRL データが CA から提供されない場合でも、証明書認証は成功します。

ASA は HTTP、SCEP、または LDAP を使用して、CA から CRL を取得できます。トラストポイントごとに取得された CRL は、トラストポイントごとに設定可能な時間だけキャッシュされます。

CRL のキャッシュに設定された時間を超過して ASA にキャッシュされている CRL がある場合、ASA はその CRL を、古すぎて信頼できない、つまり「失効した」と見なします。ASA は、次回の証明書認証で失効した CRL のチェックが必要な場合に、より新しいバージョンの CRL を取得しようとします。

CRL のエントリ制限を超えると、ユーザ接続/証明書で失効チェックエラーが表示されることがあります。CRL あたりの最大エントリ数が 65534 を超えている場合、処理するエントリ数が多すぎることを示すメッセージが syslog から返されます。

ASA によって CRL がキャッシュされる時間は、次の 2 つの要素によって決まります。

- **cache-time** コマンドで指定される分数。デフォルト値は 60 分です。

- 取得した CRL 中の NextUpdate フィールド。このフィールドが CRL にない場合もあります。ASA が NextUpdate フィールドを必要とするかどうか、およびこのフィールドを使用するかどうかは、**enforcenextupdate** コマンドで制御します。

ASA では、これらの 2 つの要素が次のように使用されます。

- NextUpdate フィールドが不要の場合、**cache-time** コマンドで指定された時間が経過すると、ASA は CRL に失効のマークを付けます。
- NextUpdate フィールドが必要な場合、ASA は、**cache-time** コマンドと NextUpdate フィールドで指定されている 2 つの時間のうち短い方の時間で、CRL に失効のマークを付けます。たとえば、**cache-time** コマンドによってキャッシュ時間が 100 分に設定され、NextUpdate フィールドによって次のアップデートが 70 分後に指定されている場合、ASA は 70 分後に CRL に失効のマークを付けます。

ASA がメモリ不足で、特定のトラストポイント用にキャッシュされた CRL をすべて保存することができない場合、使用頻度が最も低い CRL が削除され、新しく取得した CRL 用の空き領域が確保されます。

OCSP

OCSP は、有効期間内の証明書が発行元の CA によって無効にされているかどうかを ASA が判断するための 1 つの方法です。OCSP のコンフィギュレーションは、トラストポイントのコンフィギュレーションの一部です。

OCSP によって、証明書のステータスをチェックする範囲が検証局（OCSP サーバ、応答側とも呼ばれます）に限定され、ASA によって検証局に特定の証明書のステータスに関する問い合わせが行われます。これは、CRL チェックよりもスケーラブルで、最新の失効ステータスを確認できる方法です。この方法は、PKI の導入規模が大きい場合に便利で、安全なネットワークを拡大できます。

（注） ASA では、OCSP 応答に 5 秒間のスキューを許可します。

証明書を認証するときに必ず **revocation-check ocsp** コマンドを使用して OCSP チェックを行うように、ASA を設定できます。また、**revocation-check ocsp none** コマンドを使用して、OCSP チェックをオプションにすることもできます。オプションにすると、更新された OCSP データが検証局から提供されない場合でも、証明書認証は成功します。

OCSP を利用すると、OCSP サーバの URL を 3 つの方法で定義できます。ASA は、これらのサーバを次の順に使用します。

1. **match certificate** コマンドの使用による証明書の照合の上書きルールで定義されている OCSP サーバの URL
2. **ocsp url** コマンドを使用して設定されている OCSP サーバの URL
3. クライアント証明書の AIA フィールド

（注） トラストポイントでOCSPの応答側の自己署名した証明書を検証するように設定するには、信頼できるCA証明書として、この自己署名した応答側の証明書をそのトラストポイントにインポートします。次に、クライアント証明書を検証するトラストポイントで **match certificate** コマンドを設定して、応答側の証明書を検証するために、OCSP の応答側の自己署名された証明書を含むトラストポイントを使用するようにします。クライアント証明書の検証パスの外部にある応答側の証明書を検証する場合も、同じ手順で設定します。

通常、OCSP サーバ（応答側）の証明書によって、OCSP 応答が署名されます。ASA が応答を受け取ると、応答側の証明書を検証しようとします。通常、CA は、侵害される危険性を最小限に抑えるために、OCSP レスポンダ証明書のライフタイムを比較的短い期間に設定します。CA は一般に、応答側証明書に ocsp-no-check 拡張を含めて、この証明書では失効ステータスチェックが必要ないことを示します。ただし、この拡張がない場合、ASAはトラストポイントで指定されている方法で失効ステータスをチェックします。応答側の証明書を検証できない場合、失効ステータスをチェックできなくなります。この可能性を防ぐには、**revocation-check none** コマンドを使用して応答側の証明書を検証するトラストポイントを設定し、**revocation-check ocsp** コマンドを使用してクライアント証明書を設定します。

ローカル CA

ローカル CA では、次のタスクが実行されます。

- ASA で基本的な証明機関動作を統合する。
- 証明書を導入する。
- 発行済み証明書のセキュアな失効チェックを実行する。
- ブラウザベースとクライアントベースの両方で SSL VPN 接続とともに使用するために、ASA 上に認証局を提供する。
- 外部の証明書認証に依存することなく、ユーザに信頼できるデジタル証明書を提供する。
- 証明書認証のためのセキュアな内部認証局を提供し、Web サイト ログインを使用した簡単なユーザ登録を実現する。

ローカル CA ファイル用のストレージ

ASA では、ユーザ情報、発行済み証明書、および失効リストへのアクセスと実装にローカル CAデータベースが使用されます。このデータベースは、デフォルトでローカル フラッシュ メモリに存在するか、または、マウントされて ASA にアクセス可能な外部のファイル システム上に設定することもできます。

ローカルCAユーザデータベースに保存できるユーザの数に制限はありませんが、フラッシュ メモリ ストレージに問題がある場合、管理者に対策を取るように警告するsyslogが作成され、ローカル CA はストレージの問題が解決されるまでディセーブルになることがあります。フ

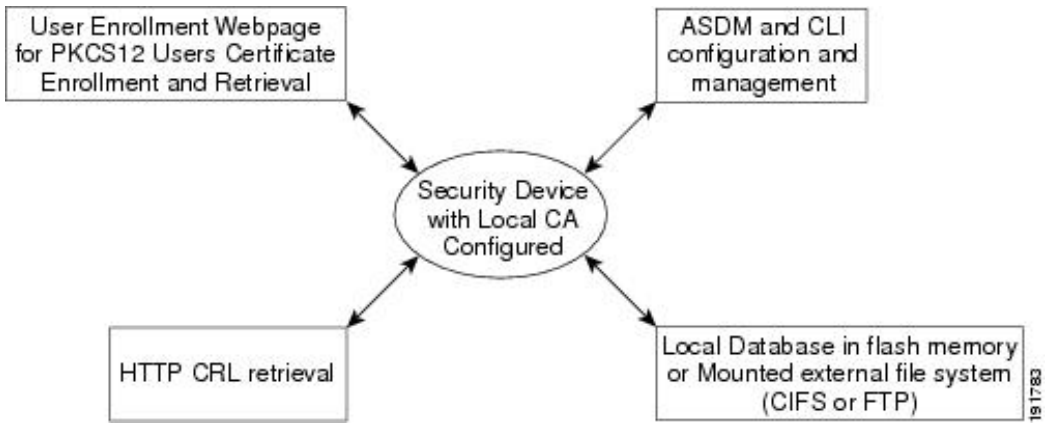
ラッシュ メモリは、3500 人以下のユーザを持つデータベースを保存できますが、ユーザの数がそれを超えるデータベースでは外部ストレージが必要になります。

ローカル CA サーバ

ASA にローカル CA サーバを設定すると、ユーザは、Web サイトにログインし、ユーザの登録資格を検証するためにローカル CA 管理者によって与えられたユーザ名とワンタイム パスワードを入力することで、証明書を登録できます。

次の図に示すように、ローカル CA サーバは ASA に常駐し、Web サイト ユーザからの登録要求や、その他の証明書を検証するデバイスおよび ASA から発信された CRL の問い合わせを処理します。ローカル CA データベースおよびコンフィギュレーション ファイルは、ASA のフラッシュ メモリ（デフォルトのストレージ）または個別のストレージ デバイスに保持されます。

図 *51* : ローカル *CA*



証明書とユーザ ログイン クレデンシャル

この項では、認証と認可に証明書およびユーザ ログイン クレデンシャル（ユーザ名とパスワード）を使用する、さまざまな方法について説明します。これらの方式は、IPSec、AnyConnect、およびクライアントレス SSL VPN に適用されます。

すべての場合において、LDAP 認可では、パスワードをクレデンシャルとして使用しません。RADIUS 認可では、すべてのユーザの共通パスワードまたはユーザ名のいずれかを、パスワードとして使用します。

ユーザ ログイン クレデンシャル

認証および認可のデフォルトの方法では、ユーザ ログイン クレデンシャルを使用します。

- 認証
  - トンネル グループ（ASDM 接続プロファイルとも呼ばれます）の認証サーバ グループ設定によりイネーブルにされます。

- ユーザ名とパスワードをクレデンシャルとして使用します。

- 認証
  - トンネル グループ（ASDM 接続プロファイルとも呼ばれます）の認可サーバ グループ設定によりイネーブルにされます。
  - ユーザ名をクレデンシャルとして使用します。

証明書

ユーザ デジタル証明書が設定されている場合、ASA によって最初に証明書が検証されます。ただし、証明書の DN は認証用のユーザ名として使用されません。

認証と認可の両方がイネーブルになっている場合、ASAによって、ユーザの認証と認可の両方にユーザ ログイン クレデンシャルが使用されます。

- 認証
  - 認証サーバ グループ設定によってイネーブルにされます。
  - ユーザ名とパスワードをクレデンシャルとして使用します。

- 認証
  - 認可サーバ グループ設定によってイネーブルにされます。
  - ユーザ名をクレデンシャルとして使用します。

認証がディセーブルで認可がイネーブルになっている場合、ASA によって認可にプライマリ DN のフィールドが使用されます。

- 認証
  - 認証サーバ グループ設定によってディセーブル（[None] に設定）になります。
  - クレデンシャルは使用されません。

- 認証
  - 認可サーバ グループ設定によってイネーブルにされます。
  - 証明書のプライマリ DN フィールドのユーザ名の値をクレデンシャルとして使用します。

（注） 証明書にプライマリ DN のフィールドが存在しない場合、ASA では、セカンデリ DN のフィールド値が認可要求のユーザ名として使用されます。

次のサブジェクト DN フィールドと値が含まれるユーザ証明書を例に挙げます。

```
Cn=anyuser,OU=sales;O=XYZCorporation;L=boston;S=mass;C=us;ea=anyuser@example.com
```

プライマリ DN = EA（電子メール アドレス）およびセカンデリ DN = CN（一般名）の場合、許可要求で使われるユーザ名は anyuser@example.com になります。

デジタル証明書のガイドライン

この項では、デジタル証明書を設定する前に確認する必要のあるガイドラインおよび制限事項について説明します。

コンテキスト モードのガイドライン

- サードパーティ CA ではシングル コンテキスト モードでのみサポートされています。

フェールオーバーのガイドライン

- ステートフル フェールオーバーではセッションの複製はサポートされません。
- ローカル CA のフェールオーバーはサポートされません。

IPv6 のガイドライン

IPv6 はサポートされません。

ローカル CA 証明書

- 証明書をサポートするように ASA が正しく設定されていることを確認します。ASA の設定が正しくないと、登録に失敗したり、不正確な情報を含む証明書が要求されたりする可能性があります。
- ASA のホスト名とドメイン名が正しく設定されていることを確認します。現在設定されているホスト名とドメイン名を表示するには、**show running-config** コマンドを入力します。
- CA を設定する前に、ASA のクロックが正しく設定されていることを確認します。証明書には、有効になる日時と満了になる日時が指定されています。ASA が CA に登録して証明書を取得するとき、ASA は現在の時刻が証明書の有効期間の範囲内であるかどうかをチェックします。現在の時刻が有効期間の範囲外の場合、登録は失敗します。
- ローカル CA 証明書の有効期限の 30 日前に、ロールオーバー代替証明書が生成され、syslog メッセージ情報で管理者にローカル CA のロールオーバーの時期であることが知らされます。新しいローカル CA 証明書は、現在の証明書が有効期限に達する前に、必要なすべてのデバイスにインポートする必要があります。管理者が、新しいローカル CA 証明書としてロールオーバー証明書をインストールして応答しない場合、検証が失敗する可能性があります。
- ローカル CA 証明書は、同じキー ペアを使用して期限満了後に自動的にロールオーバーします。ロールオーバー証明書は、base 64 形式でエクスポートに使用できます。

次に、base 64 で符号化されたローカル CA 証明書の例を示します。

```
MIIXlwIBAzCCF1EGCSqGSIb3DQEHAaCCF0IEghc+MIIXOjCCFzYGCSqGSIb3DQEHBqCCFycwghcjAgEAMIIXHA
YJKoZIhvcNAQcBMBsGCiqGSIb3DQEMAQMwDQQIjph4SxJoyTgCAQGAghbw3v4bFy+GGG2dJnB4OLphsUM+IG3S
DOiDwZG9n1SvtMieoxd7Hxknxbum06JDrujWKtHBIqkrm+td34qlNE1iGeP2YC94/NQ2z+4kS+uZzwcRhl1KEZ
TS1E4L0fSaC3uMTxJq2NUHYWmoc8pi4CIeLj3h7VVMy6qbx2AC8I+q57+QG5vG5l5Hi5imwtYfaWwPEdPQxaWZ
PrzoG1J8BFqdPa1jBGhAzzuSmElm3j/2dQ3Atro1G9nIsRHgV39fcBgwz4fEabHG7/Vanb+fj81d5nlOiJjDYY
bP86tvbZ2yOVZR6aKFVI0b2AfCr6PbwfC9U8Z/aF3BCyM2sN2xPJrXva94CaYrqyotZdAkSYA5KWScyEcgdqmu
BeGDKOncTknfgy0XM+fG5rb3qAXy1GkjyFI5Bm9Do6RUROoG1DSrQrKeq/hj….

END OF CERTIFICATE
```

SCEP プロキシ サポート

- ASA と Cisco ISE ポリシー ノードが、同じ NTP サーバを使用して同期されていることを確認します。
- AnyConnect セキュア モビリティ クライアント 3.0 以降がエンドポイントで実行中である必要があります。
- グループ ポリシーの接続プロファイルで設定される認証方式は、AAA 認証と証明書認証の両方を使用するように設定する必要があります。
- SSL ポートが、IKEv2 VPN 接続用に開いている必要があります。
- CA は、自動許可モードになっている必要があります。

ローカル CA 証明書データベース

ローカル CA 証明書データベースを維持するため、データベースに変更が加えられるたびに **write memory** コマンドを使用して、証明書データベース ファイル LOCAL-CA-SERVER.cdb を保存してください。ローカル CA 証明書データベースには、次のファイルが含まれます。

- LOCAL-CA-SERVER.p12 は、ローカル CA サーバを最初にイネーブルにしたときに生成されたローカル CA 証明書とキー ペアのアーカイブです。
- LOCAL-CA-SERVER.crl ファイルは、実際の CRL です。
- LOCAL-CA-SERVER.ser ファイルでは、発行済み証明書のシリアル番号が追跡されます。

その他のガイドライン

- ASA が CA サーバまたはクライアントとして設定されている場合、推奨される終了日（2038 年 1 月 19 日 03:14:08 UTC）を超えないよう、証明書の有効期を制限してください。このガイドラインは、サードパーティ ベンダーからインポートした証明書にも適用されます。
- フェールオーバーがイネーブルになっている場合、ローカル CA は設定できません。ローカル CA サーバを設定できるのは、フェールオーバーのないスタンドアロン ASA のみです。詳細については、「CSCty43366」を参照してください。

- 証明書の登録が完了すると、ASA により、ユーザのキー ペアと証明書チェーンを含む PKCS12 ファイルが保存されます。これには、登録ごとに約 2 KB のフラッシュ メモリまたはディスク領域が必要です。実際のディスク領域の量は、設定されている RSA キー サイズと証明書フィールドによって異なります。使用できるフラッシュ メモリの量が限られている ASA に、保留中の証明書登録を多数追加する場合には、このガイドラインに注意してください。これらの PKCS12 ファイルは、設定されている登録の取得タイムアウトの間、フラッシュ メモリに保存されます。キー サイズは 2048 以上を使用することをお勧めします。
- **lifetime ca-certificate** コマンドは、ローカル CA サーバ証明書の初回生成時（初めてローカル CA サーバを設定し、**no shutdown** コマンドを発行するとき）に有効になります。CA 証明書の期限が切れると、設定されたライフタイム値を使用して新しい CA 証明書が生成されます。既存の CA 証明書のライフタイム値は変更できません。
- 管理インターフェイスへの ASDM トラフィックと HTTPS トラフィックを保護するために、アイデンティティ証明書を使用するよう ASA を設定する必要があります。SCEP により自動的に生成される ID 証明書はリブートのたびに再生成されるため、必ず独自の ID 証明書を手動でインストールしてください。SSL のみに適用されるこのプロシージャの例については、次の URL を参照してください。
http://www.cisco.com/en/US/products/ps6120/products_configuration_example09186a00809fcf91.shtml。
- ASA および AnyConnect クライアントで検証できるのは、[X520Serialnumber] フィールド（[Subject Name] のシリアル番号）が PrintableString 形式である証明書のみです。シリアル番号の形式に UTF8 などのエンコーディングが使用されている場合、証明書認証は失敗します。
- ASA でのインポート時は、有効な文字と値だけを証明書パラメータに使用してください。
- ワイルドカード（*）記号を使用するには、文字列値でこの文字を使用できるエンコードを CA サーバで使用していることを確認してください。RFC 5280 では UTF8String または PrintableString を使用することを推奨していますが、PrintableString ではこのワイルドカード文字を有効であると認識しないため UTF8String を使用する必要があります。ASA は、インポート中に無効な文字または値が見つかると、インポートした証明書を拒否します。次に例を示します。

```
ERROR: Failed to parse or verify imported certificate ciscoasa(config)# Read 162*H÷ytes
 as CA certificate:0U0= \Ivr"phÕV°3é¼þ0 CRYPTO_PKI(make trustedCerts list)
CERT-C: E ../cert-c/source/certlist.c(302): Error #711h
CRYPTO_PKI: Failed to verify the ID certificate using the CA certificate in trustpoint
 mm.
CERT-C: E ../cert-c/source/p7contnt.c(169): Error #703h
crypto_certc_pkcs7_extract_certs_and_crls failed (1795):
crypto_certc_pkcs7_extract_certs_and_crls failed
CRYPTO_PKI: status = 1795: failed to verify or insert the cert into storage
```

デジタル証明書の設定

ここでは、デジタル証明書の設定方法について説明します。

キーペアの設定

キー ペアを作成または削除するには、次の手順を実行します。

手順

ステップ 1 1 つのデフォルト汎用 RSA キー ペアを生成します。

crypto key generate rsa modulus 2048

例：

```
ciscoasa(config)# crypto key generate rsa modulus 2048
```

デフォルト キー モジュラスは 2048 ですが、必要なサイズを確実に取得するために、明示的にモジュラスを指定する必要があります。キーの名前は Default-RSA-Key になります。

楕円曲線デジタル署名アルゴリズム（ECDSA）キーも必要な場合は、Default-ECDSA-Key を生成できます。デフォルトの長さは 384 ですが、256 または 521 も使用できます。

crypto key generate ecdsa elliptic-curve 384

ステップ 2 （オプション）一意の名前で追加のキーを作成します。

crypto key generate rsa label *key-pair-label* **modulus** *size*

crypto key generate ecdsa label *key-pair-label* **elliptic-curve** *size*

例：

```
ciscoasa(config)# crypto key generate rsa label exchange modulus 2048
```

このラベルは、キー ペアを使用するトラストポイントによって参照されます。

RSA キーの場合、モジュラスは 512、768、1024、2048、4096 ビットのいずれかです。

ECDSA キーの場合、楕円曲線は 256、384、521 ビットのいずれかです。

ステップ 3 生成したキー ペアを検証します。

show crypto key mypubkey {**rsa** | **ecdsa**}

例：

```
ciscoasa/contexta(config)# show crypto mypubkey key rsa
```

ステップ 4 生成したキー ペアを保存します。

write memory

例：

```
ciscoasa(config)# write memory
```

ステップ 5 必要に応じて、新しいキー ペアを生成できるように既存のキー ペアを削除します。

crypto key zeroize {**rsa** | **ecdsa**}

例：

```
ciscoasa(config)# crypto key zeroize rsa
```

ステップ 6 （オプション）ローカル CA サーバ証明書およびキー ペアをアーカイブします。

copy

例：

```
ciscoasa# copy LOCAL-CA-SERVER_0001.pl2 tftp://10.1.1.22/user6/
```

このコマンドは、FTP または TFTP を使用して、ローカル CA サーバ証明書とキー ペア、および ASA からのすべてのファイルをコピーします。

（注） すべてのローカル CA ファイルをできるだけ頻繁にバックアップしてください。

例

次に、キー ペアを削除する例を示します。

```
ciscoasa(config)# crypto key zeroize rsa
WARNING: All RSA keys will be removed.
WARNING: All device certs issued using these keys will also be removed.

Do you really want to remove these keys? [yes/no] y
```

トラストポイントの設定

トラストポイントを設定するには、次の手順を実行します。

手順

ステップ 1 ASA が証明書を受け取る必要のある CA に対応するトラストポイントを作成します。

crypto ca trustpoint *trustpoint-name*

例：

```
ciscoasa/contexta(config)# crypto ca trustpoint Main
```

crypto ca トラストポイント コンフィギュレーション モードに入り、ステップ 3 から設定できる CA 固有のトラストポイント パラメータを制御します。

ステップ 2 次のいずれかのオプションを選択します。

- SCEP と指定のトラストポイントを使用して自動登録を要求し、登録用 URL を設定します。

  enrollment protocol scep *url*

  例：

```
ciscoasa/contexta(config-ca-trustpoint)# enrollment protocol scep url
http://10.29.67.142:80/certsrv/mscep/mscep.dll
```

- CMP と指定のトラストポイントを使用して自動登録を要求し、登録用 URL を設定します。

  enrollment protocol cmp*url*

  例

```
ciscoasa/ contexta(config-ca-trustpoint)# enrollment protocol cmp url
http://10.29.67.142:80/certsrv/mscep/mscep.dll
```

- CA から取得した証明書を端末に貼り付けることによって、指定したトラストポイントで手動登録を要求します。

  enrollment terminal

```
ciscoasa/contexta(config-ca-trustpoint)# enrollment terminal
```

- 自己署名証明書を要求します。

  enrollment self

ステップ 3 使用可能な CRL コンフィギュレーション オプションを指定します。

revocation-check crl none

例：

```
ciscoasa/contexta(config-ca-trustpoint)# revocation-check crl none
ciscoasa/contexta(config-ca-trustpoint)# revocation-check crl
ciscoasa/contexta(config-ca-trustpoint)# revocation-check none
```

（注） 必須または任意の CRL チェックをイネーブルにするには、証明書を取得してから、CRL 管理用のトラストポイントを設定します。

ステップ 4 基本制約の拡張および CA フラグを有効または無効にします。

[**no**] **ca-check**

基本制約の拡張によって、証明書のサブジェクトが認証局（CA）かどうかが識別されます。この場合、証明書を使用して他の証明書に署名することができます。CA フラグは、この拡張の一部です。これらの項目が証明書に存在することは、証明書の公開キーを使用して証明書の署名を検証できることを示します。

ca-check コマンドはデフォルトで有効になっているため、このコマンドは、基本制約と CA フラグを無効にする場合にのみ入力する必要があります。

例：

```
ciscoasa/contexta(config-ca-trustpoint)# no ca-check
```

ステップ 5 登録時に、指定された電子メール アドレスを、証明書の Subject Alternative Name 拡張子に含めるように CA に要求します。

email *address*

例：

```
ciscoasa/contexta(config-ca-trustpoint)# email example.com
```

ステップ 6 （オプション）再試行間隔を分単位で指定し、SCEP 登録だけに適用します。

enrollment retry period

例：

```
ciscoasa/contexta(config-ca-trustpoint)# enrollment retry period 5
```

ステップ 7 （オプション）許可される再試行の最大数を指定し、SCEP 登録だけに適用します。

enrollment retry count

例：

```
ciscoasa/contexta(config-ca-trustpoint)# enrollment retry period 2
```

ステップ 8 登録時に、指定された完全修飾ドメイン名を証明書の Subject Alternative Name 拡張子に含めるように CA に要求します。

fqdn *fqdn*

例：

```
ciscoasa/contexta(config-ca-trustpoint)# fqdn example.com
```

ステップ 9 登録時に、ASA の IP アドレスを証明書に含めるように CA に要求します。

ip-address *ip-address*

例：

```
ciscoasa/contexta(config-ca-trustpoint)# ip-address 10.10.100.1
```

ステップ 10 公開キーが認証の対象となるキー ペアを指定します。

keypair *name*

例：

```
ciscoasa/contexta(config-ca-trustpoint)# keypair exchange
```

ステップ 11 OCSP の URL の上書きと、OCSP の応答側の証明書の検証に使用するトラストポイントを設定します。

match certificate map-name override ocsp

例：

```
ciscoasa/contexta(config-ca-trustpoint)# match certificate examplemap override ocsp
```

ステップ 12 OCSP 要求の nonce 拡張をディセーブルにします。nonce 拡張は、リプレイ攻撃を防ぐために、要求と応答を暗号化してバインドします。

ocsp disable-nonce

例：

```
ciscoasa/contexta(config-ca-trustpoint)# ocsp disable-nonce
```

ステップ 13 ASA で、トラストポイントに関連するすべての証明書をチェックするときに使用する OCSP サーバを設定します。クライアント証明書の AIA 拡張で指定されているサーバは使用しません。

ocsp url

例：

```
ciscoasa/contexta(config-ca-trustpoint)# ocsp url
```

ステップ 14 登録時に CA に登録されるチャレンジ フレーズを指定します。CA は、通常、このフレーズを使用して、その後の失効要求を認証します。

password *string*

例：

```
ciscoasa/contexta(config-ca-trustpoint)# password mypassword
```

ステップ 15 失効チェックの方法（CRL、OCSP、および none）を 1 つまたは複数設定します。

revocation check

例：

```
ciscoasa/contexta(config-ca-trustpoint)# revocation check
```

ステップ 16 登録時に、指定されたサブジェクト DN を証明書に含めるように CA に要求します。DN 文字列にカンマが含まれている場合、この値文字列を二重引用符で囲みます（例：O="Company, Inc."）。

subject-name *X.500 name*

例：

```
ciscoasa/contexta(config-ca-trustpoint)# myname X.500 examplename
```

ステップ 17 登録時に、ASA のシリアル番号を証明書に含めるように CA に要求します。

serial-number

例：

```
ciscoasa/contexta(config-ca-trustpoint)# serial number JMX1213L2A7
```

ステップ 18 実行コンフィギュレーションを保存します。

write memory

例：

```
ciscoasa/contexta(config)# write memory
```

トラストポイントの CRL の設定

証明書の認証時に必須またはオプションの CRL チェックを行うには、トラストポイントごとに CRL を設定する必要があります。トラストポイントの CRL を設定するには、次の手順を実行します。

手順

ステップ 1 CRL コンフィギュレーションを変更するトラストポイントに対して、crypto ca trustpoint コンフィギュレーション モードに入ります。

crypto ca trustpoint *trustpoint-name*

例：

```
ciscoasa (config)# crypto ca trustpoint Main
```

（注） このコマンドを入力する前に、CRL がイネーブルであることを確認してください。また、認証が成功するためには、CRL が使用可能である必要があります。

ステップ 2 現在のトラストポイントで、crl コンフィギュレーション モードを開始します。

crl configure

例：

```
ciscoasa(config-ca-trustpoint)# crl configure
```

ヒント　すべてのCRLコンフィギュレーションのパラメータをデフォルト値に設定するには、**default** コマンドを使用します。CRL の設定中は、いつでもこのコマンドを入力して手順をやり直すことができます。

ステップ 3　取得ポリシーを設定するには、次のいずれかを選択します。

- CRL は、認証済みの証明書で指定されている CRL 分散ポイントだけから取得できます。

  policy cdp

  ```
  ciscoasa(config-ca-crl)# policy cdp
  ```

  （注）　SCEP の取得は、証明書で指定されている分散ポイントではサポートされていません。

- CRL は、設定した URL だけから取得できます。

  policy static

  ```
  ciscoasa(config-ca-crl)# policy static
  ```

- CRL は、認証済みの証明書で指定されている CRL 分散ポイントと、設定した URL の両方から取得できます。

  policy both

  ```
  ciscoasa(config-ca-crl)# policy both
  ```

ステップ 4　CRL ポリシーの設定時に **static** または **both** キーワードを使用する場合、CRL 取得用の URL を設定する必要があります。1 ～ 5 のランクを付けて、最大 5 つの URL を入力できます。*n* 引数は、URL に割り当てるランクです。

url *n url*

例：

```
ciscoasa (config-ca-crl)# url 2 http://www.example.com
```

URL を削除するには、**no url** *n* コマンドを使用します。

ステップ 5　CRL 取得方式として HTTP、LDAP、または SCEP を指定します。

protocol http | **ldap** | **scep**

例：

```
ciscoasa(config-ca-crl)# protocol http
```

ステップ 6 ASA が現在のトラストポイントの CRL をキャッシュしている時間を設定します。*refresh-time* 引数は、CRL を失効と判断するまで ASA が待機する時間（分）です。

cache-time *refresh-time*

例：

```
ciscoasa(config-ca-crl)# cache-time 420
```

ステップ 7 次のいずれかを選択します。

- CRL に NextUpdate フィールドが存在する必要があります。これがデフォルト設定です。

  enforcenextupdate

  ```
  ciscoasa(config-ca-crl)# enforcenextupdate
  ```

- CRL に NextUpdate フィールドが存在しないことを許可します。

  no enforcenextupdate

  ```
  ciscoasa(config-ca-crl)# no enforcenextupdate
  ```

ステップ 8 LDAP が取得プロトコルとして指定されている場合に ASA に LDAP サーバを指定します。LDAP サーバは、DNS ホスト名または IP アドレスで指定できます。LDAP サーバがデフォルトの 389 以外のポートで LDAP クエリーを受信する場合は、ポート番号も指定できます。

ldap-defaults *server*

例：

```
ciscoasa (config-ca-crl)# ldap-defaults ldap1
```

（注） LDAP サーバを指定するために、IP アドレスの代わりにホスト名を使用する場合は、ASA が DNS を使用するように設定されていることを確認します。

ステップ 9 LDAP サーバでクレデンシャルを必要としている場合に、CRL の取得を許可します。

ldap-dn *admin-DN password*

例：

```
ciscoasa (config-ca-crl)# ldap-dn cn=admin,ou=devtest,o=engineering c00lRunZ
```

ステップ 10 指定したトラストポイントによって示される CA から現在の CRL を取得し、現在のトラストポイントの CRL コンフィギュレーションをテストします。

crypto ca crl request *trustpoint*

例：

```
ciscoasa (config-ca-crl)# crypto ca crl request Main
```

ステップ 11 実行コンフィギュレーションを保存します。

write memory

例：

```
ciscoasa (config)# write memory
```

トラストポイント設定のエクスポートまたはインポート

トラストポイント設定をエクスポート/インポートするには、次の手順を実行します。

手順

ステップ 1 トラストポイント設定を関連するすべてのキーとPKCS12形式の証明書とともにエクスポートします。

crypto ca export *trustpoint*

例：

```
ciscoasa(config)# crypto ca export Main
```

ASAはPKCS12データを端末に表示します。この表示されたデータはコピーできます。トラストポイントデータはパスワードで保護されますが、このデータをファイルに保存する場合は、そのファイルがセキュアな場所にあることを確認してください。

ステップ 2 キー ペアと、トラスト ポイント設定に関連付けられている発行済み証明書をインポートします。

crypto ca import *trustpoint* **pkcs12**

例：

```
ciscoasa(config)# crypto ca import Main pkcs12
```

Base-64形式で端末にテキストを貼り付けるようASAによって促されます。トラストポイントとともにインポートされるキーペアには、作成するトラストポイントの名前と一致するラベルが割り当てられます。

（注） 同じ CA を共有するトラストポイントが ASA 内に複数ある場合、CA を共有するトラストポイントのうち 1 つだけを使用してユーザ証明書を検証できます。CA を共有するどのトラストポイントを使用して、その CA が発行したユーザ証明書を検証するかを制御するには、**support-user-cert-validation** キーワードを使用します。

例

次の例では、トラストポイント Main の PKCS12 データをパスフレーズ Wh0zits とともにエクスポートしています。

```
ciscoasa(config)# crypto ca export Main pkcs12 Wh0zits

Exported pkcs12 follows:

[ PKCS12 data omitted ]

---End - This line not part of the pkcs12---
```

次の例では、パスフレーズ Wh0zits とともに PKCS12 データを手動でトラストポイント Main にインポートしています。

```
ciscoasa (config)# crypto ca import Main pkcs12 Wh0zits

Enter the base 64 encoded pkcs12.
End with a blank line or the word "quit" on a line by itself:
[ PKCS12 data omitted ]
quit
INFO: Import PKCS12 operation completed successfully
```

次に、トラストポイント Main の証明書を手動でインポートする例を示します。

```
ciscoasa (config)# crypto ca import Main certificate
% The fully-qualified domain name in the certificate will be: securityappliance.example.com

Enter the base 64 encoded certificate.
End with a blank line or the word “quit” on a line by itself
[ certificate data omitted ]
quit
INFO: Certificate successfully imported
```

CA 証明書マップ ルールの設定

証明書の [Issuer] フィールドと [Subject] フィールドに基づいて、ルールを設定できます。作成したルールを使用すると、**tunnel-group-map** コマンドによって、IPsec ピアの証明書をトンネル グループにマッピングできます。

CA 証明書マップ規則を設定するには、次の手順を実行します。

手順

ステップ 1 設定するルールの CA 証明書マップ コンフィギュレーション モードを開始し、ルールのシーケンス番号を指定します。

crypto ca certificate map [*map_name*]*sequence-number*

例：

```
ciscoasa(config)# crypto ca certificate map test-map 10
```

マップ名を指定しない場合、ルールはデフォルト マップ（DefaultCertificateMap）に追加されます。ルール番号ごとに、一致させるフィールドを 1 つ以上指定できます。

ステップ 2 発行元の名前またはサブジェクト名を指定します。

{**issuer-name** | **subject-name**} [**attr** *attribute*] *operator string*

例：

```
ciscoasa(config-ca-cert-map)# issuer-name cn=asa.example.com
ciscoasa(config-ca-cert-map)# subject-name attr cn eq mycert
ciscoasa(config-ca-cert-map)# subject-name attr uid eq jcrichton
```

値全体と一致させることも、一致させる属性を指定することもできます。有効な値は次のとおりです。

- c：国
- cn：共通名
- dc：ドメイン コンポーネント
- dnq：DN 修飾子
- ea：電子メール アドレス
- genq：世代修飾子
- gn：名
- i：イニシャル
- ip：IP アドレス
- l：局所性
- n：名前
- o：組織名
- ou：組織単位
- ser：シリアル番号

- sn：姓
- sp：都道府県
- t：役職
- uid：ユーザ ID
- uname：非構造化名

有効な演算子は次のとおりです。

- eq：フィールドまたは属性が所定の値と一致する。
- ne：フィールドまたは属性が所定の値と一致しない。
- co：フィールドまたは属性の一部または全部が所定の値と一致する。
- nc：フィールドまたは属性の全部が所定の値と一致しない。

ステップ 3 サブジェクト代替名を指定します。

alt-subject-name *operator string*

例：

```
ciscoasa(config-ca-cert-map)# alt-subject-name eq happydays
```

有効な演算子は次のとおりです。

- eq：フィールドが所定の値と一致する。
- ne：フィールドが所定の値と一致しない。
- co：フィールドの一部または全部が所定の値と一致する。
- nc：フィールドの全部が所定の値と一致しない。

ステップ 4 拡張キーの使用法を指定します。

extended-key-usage *operator OID_string*

例：

```
ciscoasa(config-ca-cert-map)# extended-key-usage nc clientauth
```

有効な演算子は次のとおりです。

- co：フィールドの一部または全部が所定の値と一致する。
- nc：フィールドの全部が所定の値と一致しない。

有効な OID 文字列は次のとおりです。

- [string]：ユーザ定義の文字列。

- clientauth：クライアント認証（1.3.6.1.5.5.7.3.2）
- codesigning：コード署名（1.3.6.1.5.5.7.3.3）
- emailprotection：セキュア電子メール保護（1.3.6.1.5.5.7.3.4）
- ocspsigning：OCSP 署名（1.3.6.1.5.5.7.3.9）
- serverauth：サーバ認証（1.3.6.1.5.5.7.3.1）
- timestamping：タイムスタンプ（1.3.6.1.5.5.7.3.8）

手動での証明書の取得

証明書を手動で取得するには、次の手順を実行します。

始める前に

トラストポイントで示されている CA から、base-64 encoded CA 証明書を取得しておく必要があります。

手順

ステップ 1 設定したトラストポイントの CA 証明書をインポートします。

crypto ca authenticate *trustpoint*

例：

```
ciscoasa(config)# crypto ca authenticate Main
Enter the base 64 encoded CA certificate.
End with a blank line or the word "quit" on a line by itself
MIIDRTCCAu+gAwIBAgIQKVcqP/KW74VP0NZzL+JbRTANBgkqhkiG9w0BAQUFADCB
[ certificate data omitted ]
/7QEM8izy0EOTSErKu7Nd76jwf5e4qttkQ==
quit

INFO: Certificate has the following attributes:
Fingerprint:     24b81433 409b3fd5 e5431699 8d490d34
Do you accept this certificate? [yes/no]: y
Trustpoint CA certificate accepted.

% Certificate successfully imported
```

トラストポイントの証明書を手動で取得する必要があるかどうかは、そのトラストポイントの設定時に **enrollment terminal** コマンドを使用するかどうかによって決まります。

ステップ 2 このトラストポイントを持つ ASA を登録します。

crypto ca enroll *trustpoint*

例：

```
ciscoasa(config)# crypto ca enroll Main
% Start certificate enrollment ..

% The fully-qualified domain name in the certificate will be: securityappliance.example.com

% Include the device serial number in the subject name? [yes/no]: n

Display Certificate Request to terminal? [yes/no]: y
Certificate Request follows:

MIIBoDCCAQkCAQAwIzEhMB8GCSqGSIb3DQEJAhYSRmVyYWxQaXguY2lzY28uY29t
[ certificate request data omitted ]
jF4waw68eOxQxVmdgMWeQ+RbIOYmvt8g6hnBTrd0GdqjjVLt

---End - This line not part of the certificate request---

Redisplay enrollment request? [yes/no]: n
```

このコマンドは、署名データの証明書を生成し、設定したキーのタイプによっては暗号化データの証明書も生成します。署名と暗号化に別々の RSA キーを使用する場合、**crypto ca enroll** コマンドは 2 つの証明書要求（キーごとに 1 つ）を表示します。署名と暗号化の両方に汎用の RSA キーを使用する場合、**crypto ca enroll** コマンドでは証明書要求が 1 つ表示されます。

登録を完了するには、該当するトラストポイントで示される CA から **crypto ca enroll** コマンドで生成されたすべての証明書要求に対する証明書を取得します。証明書が base-64 形式であることを確認してください。

ステップ 3 CA から受信する各証明書をインポートして、証明書を base-64 形式で端末に貼り付けていることを確認します。

crypto ca import *trustpoint* **certificate**

例：

```
ciscoasa (config)# crypto ca import Main certificate
% The fully-qualified domain name in the certificate will be: securityappliance.example.com

Enter the base 64 encoded certificate.
End with a blank line or the word "quit" on a line by itself
[ certificate data omitted ]
quit
INFO: Certificate successfully imported
```

ステップ 4 ASA に発行された証明書の詳細とトラストポイントの CA 証明書を表示して、登録プロセスが成功したことを確認します。

show crypto ca certificate

例：

```
ciscoasa(config)# show crypto ca  certificate Main
```

ステップ 5 実行コンフィギュレーションを保存します。

write memory

例：

```
ciscoasa(config)# write memory
```

ステップ 6 手動登録を設定したトラストポイントごとに、これらの手順を繰り返します。

SCEP を使用した証明書の自動取得

この項では、SCEP を使用して証明書を自動的に取得する方法について説明します。

始める前に

トラストポイントで示されている CA から、base-64 encoded CA 証明書を取得しておく必要があります。

手順

ステップ 1 設定したトラストポイントの CA 証明書を取得します。

crypto ca authenticate *trustpoint*

例：

```
ciscoasa/contexta(config)# crypto ca authenticate Main
```

トラストポイントを設定するときに、**enrollment url** コマンドを使用すると、SCEP を使用して証明書を自動的に取得する必要があるかどうかを判断できます。

ステップ 2 このトラストポイントを持つ ASA を登録します。このコマンドは、署名データの証明書を取得し、設定したキーのタイプによっては暗号化データの証明書も取得します。CA の管理者は、CA が証明書を付与する前に手動で登録要求を認証しなければならない場合があるため、このコマンドを入力する前に CA の管理者に連絡してください。

crypto ca enroll *trustpoint*

例：

```
ciscoasa/contexta(config)# crypto ca enroll Main
```

ASA が証明書要求を送信してから 1 分（デフォルト）以内に CA から証明書を受け取らなかった場合は、証明書要求が再送信されます。ASA によって、証明書を受信するまで 1 分ごとに証明書要求が送信されます。

トラストポイントの完全修飾ドメイン名が ASA の完全修飾ドメイン名と一致しなかった場合（完全修飾ドメイン名が文字の場合も含む）、警告が表示されます。この問題を解決するに

は、登録プロセスを終了し、必要な修正を行ってから、**crypto ca enroll** コマンドを再入力します。

（注） **crypto ca enroll** コマンドを発行した後、証明書を受信する前に ASA がリブートされた場合は、**crypto ca enroll** コマンドを再入力して、CA 管理者に連絡してください。

ステップ 3 ASAに発行された証明書の詳細とトラストポイントのCA証明書を表示して、登録プロセスが成功したことを確認します。

show crypto ca certificate

例：

```
ciscoasa/contexta(config)# show crypto ca certificate Main
```

ステップ 4 実行コンフィギュレーションを保存します。

write memory

例：

```
ciscoasa/contexta(config)# write memory
```

SCEP 要求のプロキシ サポートの設定

サードパーティの CA を使用してリモート アクセスのエンド ポイントを認証するように ASA を設定するには、次の手順を実行します。

手順

ステップ 1 トンネル グループ ipsec 属性コンフィギュレーション モードを開始します。

tunnel-group *name* **ipsec-attributes**

例：

```
ciscoasa(config)# tunnel-group remotegrp ipsec-attributes
```

ステップ 2 クライアント サービスをイネーブルにします。

crypto ikev2 enable outside client-services port *portnumber*

例：

```
ciscoasa(config-tunnel-ipsec)# crypto ikev2 enable outside client-services
```

デフォルトのポート番号は 443 です。

（注）　このコマンドは、IKEv2 をサポートする場合にのみ必要です。

ステップ 3　トンネル グループ general 属性コンフィギュレーション モードを開始します。

tunnel-group *name* **general-attributes**

例：

```
ciscoasa(config)# tunnel-group 209.165.200.225 general-attributes
```

ステップ 4　トンネル グループの SCEP 登録をイネーブルにします。

scep-enrollment enable

例：

```
ciscoasa(config-tunnel-general)# scep-enrollment enable
INFO: 'authentication aaa certificate' must be configured to complete setup of this
option.
```

ステップ 5　グループ ポリシー属性コンフィギュレーション モードを開始します。

group-policy *name* **attributes**

例：

```
ciscoasa(config)# group-policy FirstGroup attributes
```

ステップ 6　グループ ポリシー用の SCEP CA を登録します。このコマンドは、サードパーティのデジタル証明書をサポートするグループ ポリシーごとに 1 回入力します。

scep-forwarding-url value *URL*

例：

```
ciscoasa(config-group-policy)# scep-forwarding-url value http://ca.example.com:80/
```

URL は CA の SCEP URL です。

ステップ 7　証明書が SCEP プロキシの WebLaunch のサポートに使用できない場合は、共通のセカンデリ パスワードを使用します。

secondary-pre-fill-username clientless hide use-common-password *password*

例：

```
ciscoasa(config)# tunnel-group remotegrp webvpn-attributes
ciscoasa(config-tunnel-webvpn)# secondary-pre-fill-username clientless hide
use-common-password secret
```

SCEP プロキシをサポートするには、**hide** キーワードを使用する必要があります。

たとえば、証明書は、それを要求するエンド ポイントでは使用できません。エンド ポイントに証明書が存在する場合、AnyConnect は ASA への接続を切断し、その後再接続して、内部ネットワーク リソースへのアクセスを提供する DAP ポリシーに適合するようにします。

ステップ 8 AnyConnect VPN セッションの事前入力されているセカンデリ ユーザ名を非表示にします。

secondary-pre-fill-username ssl-client hide use-common-password *password*

例：

```
ciscoasa(config-tunnel-webvpn)# secondary-pre-fill-username ssl-client hide
use-common-password secret
```

以前のリリースから継承した **ssl-client** キーワードに関係なく、IKEv2 または SSL を使用する AnyConnect セッションをサポートするには、このコマンドを使用します。

SCEP プロキシをサポートするには、**hide** キーワードを使用する必要があります。

ステップ 9 証明書が使用できないときにはユーザ名を指定します。

secondary-username-from-certificate {**use-entire-name** | **use-script** | {*primary_attr* [*secondary-attr*]}} [**no-certificate-fallback cisco-secure-desktop machine-unique-id**]

例：

```
ciscoasa(config-tunnel-webvpn)# secondary-username-from-certificate CN
no-certificate-fallback cisco-secure-desktop machine-unique-id
```

CA 証明書のライフタイムの設定

ローカル CA サーバ証明書のライフタイムを設定するには、次の手順を実行します。

手順

ステップ 1 ローカル CA サーバ コンフィギュレーション モードに入ります。

crypto ca server

例：

```
ciscoasa(config)# crypto ca server
```

ステップ 2 証明書に含める有効期限を決定します。ローカル CA 証明書のデフォルトのライフタイムは 3 年間です。

lifetime ca-certificate *time*

例：

```
ciscoasa(config-ca-server)# lifetime ca-certificate 365
```

推奨される終了日（2038 年 1 月 19 日 03:14:08 UTC）を超えないよう、証明書の有効期間を制限します。

ステップ 3 （オプション）ローカル CA 証明書のライフタイムをデフォルト値の 3 年にリセットします。

no lifetime ca-certificate

例：

```
ciscoasa(config-ca-server)# no lifetime ca-certificate
```

ローカル CA サーバでは、CA 証明書の期限が切れる 30 日前に後継の CA 証明書が自動的に生成されます。この証明書をエクスポートし、他のデバイスにインポートすることにより、ローカル CA 証明書が発行したユーザ証明書のローカル CA 証明書検証を、期限が切れた後に行うことができます。次のような pre-expiration syslog メッセージが生成されます。

```
%ASA-1-717049: Local CA Server certificate is due to expire in days days and a replacement
 certificate is available for export.
```

（注） この自動ロールオーバーが通知されたら、管理者は、新しいローカル CA 証明書が有効期限の前に必要なすべてのデバイスにインポートされるようにする必要があります。

ユーザ証明書のライフタイムの設定

ユーザ証明書のライフタイムを設定するには、次の手順を実行します。

手順

ステップ 1 ローカル CA サーバ コンフィギュレーション モードに入ります。

crypto ca server

例：

```
ciscoasa(config)# crypto ca server
```

ステップ 2 ユーザ証明書の有効期間の時間の長さを設定します。

lifetime certificate *time*

例：

```
ciscoasa(config-ca-server)# lifetime certificate 60
```

（注） ユーザ証明書の期限が満了になる前に、ローカル CA サーバは、証明書の有効期限の数日前にそのユーザに登録特権を付与し、更新の注意を設定し、証明書更新用の登録ユーザ名および OTP を電子メールで配信することで、証明書の更新プロセスを自動的に開始します。推奨される終了日（2038 年 1 月 19 日 03:14:08 UTC）を超えないよう、証明書の有効期間を制限します。

CRL のライフタイムの設定

CRL ライフタイムを設定するには、次の手順を実行します。

手順

ステップ 1 ローカル CA サーバ コンフィギュレーション モードに入ります。

crypto ca server

例：

```
ciscoasa(config)# crypto ca server
```

ステップ 2 CRL の有効期間の時間の長さを設定します。

lifetime crl *time*

例：

```
ciscoasa(config-ca-server)# lifetime crl 10
```

ローカル CA では、ユーザ証明書が失効または失効解除されるたびに CRL をアップデートおよび再発行しますが、失効状態に変更がない場合、CRL の再発行は、そのライフタイムの中で 1 回だけ自動的に行われます。CRL のライフタイムを指定しない場合、デフォルトの期間は 6 時間になります。

ステップ 3 CRL を任意のタイミングで強制的に発行します。現在の CRL がただちに更新および再生成され、既存の CRL が上書きされます。

crypto ca server crl issue

例：

```
ciscoasa(config-ca-server)# crypto ca server crl issue

A new CRL has been issued.
```

（注） CRL ファイルがエラーで削除されたり、壊れたりして、再生成が必要になった場合以外は、このコマンドを使用しないでください。

サーバのキーサイズの設定

サーバのキーサイズを設定するには、次の手順を実行します。

手順

ステップ 1 ローカル CA サーバ コンフィギュレーション モードに入ります。

crypto ca server

例：

```
ciscoasa(config)# crypto ca server
```

ステップ 2 ユーザ証明書登録で生成される公開キーと秘密キーのサイズを指定します。

keysize server

例：

```
ciscoasa(config-ca-server)# keysize server 2048
```

キーペア サイズのオプションは 512、768、1024、2048、4096 ビットで、デフォルト値は 1024 ビットです。

（注） ローカル CA をイネーブルにした後でローカル CA のキーサイズを変更することはできません。発行済み証明書すべてが無効になるためです。ローカル CA キーサイズを変更するには、現在のローカル CA を削除して新しいローカル CA を再設定する必要があります。

例

次は、データベースの 2 つのユーザ証明書の出力例です。

```
Username: user1
Renewal allowed until: Not Allowed
Number of times user notified: 0
PKCS12 file stored until: 12:45:52 UTC Fri Jan 4 2017
Certificates Issued:
serial:   0x71
issued:   12:45:52 UTC Thu Jan 3 2008
expired:  12:17:37 UTC Sun Dec 31 2017
```

```
status:   Not Revoked
Username: user2
Renewal allowed until: Not Allowed
Number of times user notified: 0
PKCS12 file stored until: 12:27:59 UTC Fri Jan 4 2008
Certificates Issued:
serial:   0x2
issued:   12:27:59 UTC Thu Jan 3 2008
expired:  12:17:37 UTC Sun Dec 31 2017
status:   Not Revoked
<--- More --->
```

特定の証明書タイプの設定方法

信頼できる証明書を確立すると、アイデンティティ証明書の確立などの基本的なタスクや、ローカル CA 証明書やコード署名証明書の確立などのさらに高度な設定を行なえるようになります。

始める前に

デジタル証明書情報に目を通し、信頼できる証明書を確立します。秘密キーが設定されていない CA 証明書は、すべての VPN プロトコルと webvpn で使用され、トラストポイントで着信クライアント証明書を検証するように設定されています。また、トラストポイントとは、HTTPS サーバにプロキシ接続された接続を検証し、smart-call-home 証明書を検証する、webvpn 機能によって使用される信頼できる証明書の一覧のことです。

手順

ローカル CA を設定すると、VPN クライアントが ASA から証明書を直接登録できるようになります。この高度な設定により、ASA は CA に変換されます。CA を設定するには、CA 証明書 （659 ページ） を参照してください。

次のタスク

証明書の有効期限にアラートを設定するか、デジタル証明書や証明書の管理履歴をモニタします。

CA 証明書

このページで、CA 証明書を管理します。次のトピックでは、実行できることについて説明します。

ローカル CA サーバの設定

ローカル CA サーバを設定にするには、次の手順を実行します。

手順

ステップ 1 ローカル CA サーバ コンフィギュレーション モードに入ります。

crypto ca server

例：

```
ciscoasa(config)# crypto ca server
```

ステップ 2 SMTP from-address を指定します。これはローカル CA がユーザに登録案内用のワンタイム パスワード（OTP）を送る電子メール メッセージを送信するときに、発信元アドレスとして使用する有効な電子メール アドレスです。

smtp from-address *e-mail_address*

例：

```
ciscoasa(config-ca-server) # smtp from-address SecurityAdmin@example.com
```

ステップ 3 （オプション）発行された証明書のユーザ名に付加する subject-name DN を指定します。

subject-name-default *dn*

例：

```
ciscoasa(config-ca-server)# subject-name-default cn=engineer, o=asc systems, c="US"
```

subject-name DN とユーザ名は結合して、ローカル CA サーバによって発行されたすべてのユーザ証明書の DN を形成します。subject-name DN を指定しない場合、ユーザ データベースにユーザを追加するたびに、ユーザ証明書に含めるサブジェクト名 DN を正確に指定する必要があります。

（注） ローカル CA をイネーブルにした後は、issuer-name 値および keysize server 値は変更できないため、設定したローカル CA をイネーブルにする前に、オプションのすべてのパラメータを慎重に見直してください。

ステップ 4 自己署名した証明書を作成し、ASA のローカル CA に関連付けます。

no shutdown

例：

```
ciscoasa(config-ca-server)# no shutdown
```

自己署名した証明書のキーの使用拡張には、キー暗号化、キー シグニチャ、CRL 署名、および証明書署名機能があります。

（注） 自己署名したローカル CA 証明書が生成された後、特性を変更するには、既存のローカル CA サーバを削除して、完全に作成し直す必要があります。

ローカル CA サーバはユーザ証明書を把握しているため、管理者は、必要に応じて特権を無効にしたり元に戻したりできます。

例

次の例は、必要なパラメータすべてで事前定義済みのデフォルト値を使用してローカル CA サーバを設定する方法を示しています。

```
ciscoasa(config)# crypto ca server
ciscoasa(config-ca-server)# smtp from-address SecurityAdmin@example.com
ciscoasa(config-ca-server)# subject-name-default cn=engineer, o=asc Systems, c=US
ciscoasa(config-ca-server)# no shutdown
```

CA サーバ管理

ローカル CA サーバの削除

既存のローカル CA サーバ（イネーブル状態またはディセーブル状態）を削除するには、次の手順を実行します。

手順

次のコマンドの 1 つを入力して、既存のローカル CA サーバ（イネーブル状態またはディセーブル状態）を削除します。

- **no crypto ca server**

  例

  ```
  ciscoasa(config)# no crypto ca server
  ```

- **clear configure crypto ca server**

  例

  ```
  ciscoasa(config)# clear config crypto ca server
  ```

（注） ローカル CA サーバを削除すると、ASA からコンフィギュレーションが削除されます。削除されたコンフィギュレーションは元に戻せません。

関連付けられたローカルCAサーバのデータベースとコンフィギュレーションファイル（つまり、ワイルドカード名が LOCAL-CA-SERVER.* のすべてのファイル）も必ず削除してください。

ユーザ証明書の管理

証明書のステータスを変更するには、次の手順を実行します。

手順

ステップ 1 [Manage User Certificates] ペインで、ユーザ名または証明書のシリアル番号で特定の証明書を選択します。

ステップ 2 次のいずれかのオプションを選択します。

- ユーザ証明書のライフタイム期間が終了した場合、[Revoke] をクリックしてユーザアクセスを削除します。また、ローカル CA により、証明書データベース内にあるその証明書に失効のマークが付けられ、情報が自動的に更新されて、CRL が再発行されます。
- 失効した証明書を選択して [Unrevoke] をクリックすると、その証明書に再びアクセスできるようになります。また、ローカル CA により、証明書データベース内にあるその証明書に失効解除のマークが付けられ、証明書の情報が自動的に更新された後、更新されたCRLが再発行されます。

ステップ 3 完了したら [Apply] をクリックして、変更を保存します。

ローカル CA サーバのイネーブル化

ローカル CA サーバをイネーブルにするには、次の手順を実行します。

始める前に

ローカル CA サーバをイネーブルにする前に、7 文字以上からなるパスフレーズを作成して、生成されるローカルCA証明書とキーペアを含むPKCS12ファイルを符号化し、アーカイブしておく必要があります。CA 証明書またはキーペアが失われた場合は、パスフレーズを使用して PKCS12 アーカイブをロック解除します。

手順

ステップ 1 ローカル CA サーバ コンフィギュレーション モードに入ります。

crypto ca server

例：

```
ciscoasa(config)# crypto ca server
```

ステップ 2 ローカル CA サーバをイネーブルにします。

no shutdown

例：

```
ciscoasa(config-ca-server)# no shutdown
```

このコマンドは、ローカル CA サーバの証明書、キー ペア、および必要なデータベース ファイルを生成し、ローカル CA サーバの証明書とキー ペアを PKCS12 ファイルにアーカイブします。英数字で 8 ～ 65 文字のパスワードを入力する必要があります。初期スタートアップ後、パスワードを求めるプロンプトを表示せずにローカル CA をディセーブルにすることができます。

ステップ 3 コンフィギュレーションを保存して、リブート後にローカル CA 証明書とキーペアが失われないようにします。

write memory

例：

```
ciscoasa(config)# write memory
```

例

次の例では、ローカル CA サーバをイネーブルにします。

```
ciscoasa(config)# crypto ca server
ciscoasa(config-ca-server)# no shutdown

% Some server settings cannot be changed after CA certificate generation.
% Please enter a passphrase to protect the private key
% or type Return to exit

Password: caserver

Re-enter password: caserver

Keypair generation process begin. Please wait...
```

次に、ローカル CA サーバのコンフィギュレーションとステータスを表示するサンプル出力を示します。

```
Certificate Server LOCAL-CA-SERVER:
    Status: enabled
    State: enabled
    Server's configuration is locked (enter “shutdown” to unlock it)
    Issuer name: CN=wz5520-1-16
```

```
CA certificate fingerprint/thumbprint: (MD5)
    76dd1439 ac94fdbc 74a0a89f cb815acc
CA certificate fingerprint/thumbprint: (SHA1)
    58754ffd 9f19f9fd b13b4b02 15b3e4be b70b5a83
Last certificate issued serial number: 0x6
CA certificate expiration timer: 14:25:11 UTC Jan 16 2008
CRL NextUpdate timer: 16:09:55 UTC Jan 24 2007
Current primary storage dir: flash:
```

ローカル CA サーバのカスタマイズ

カスタマイズされたローカル CA グループ サーバを設定するには、次の手順を実行します。

手順

ステップ 1 ローカル CA サーバ コンフィギュレーション モードに入ります。

crypto ca server

例：

```
ciscoasa(config)# crypto ca server
```

ステップ 2 デフォルト値のないパラメータを指定します。

issuer-name *DN-string*

例：

```
ciscoasa(config-ca-server)# issuer-name cn=xx5520,cn=30.132.0.25,ou=DevTest,ou=QA,o=ASC
 Systems
```

ステップ 3 ローカル CA サーバによって生成されるすべての電子メールの [From:] フィールドに使用する電子メール アドレスを指定します。

smtp from-address *e-mail_address*

例：

```
ciscoasa(config-ca-server)# smtp from-address SecurityAdmin@example.com
```

ステップ 4 ローカル CA サーバから送信されるすべての電子メールの件名フィールドに表示するテキストをカスタマイズします。

smtp subject *subject-line*

例：

```
ciscoasa(config-ca-server)# smtp subject Priority E-Mail: Enclosed Confidential Information
 is Required for Enrollment
```

ステップ 5 発行された証明書のユーザ名に追加するオプションの subject-name DN を指定します。

subject-name-default *dn*

例：

```
ciscoasa(config-ca-server)# subject-name default cn=engineer, o=ASC Systems, c=US
```

デフォルトの subject-name DN は、ローカル CA サーバによって発行されたすべてのユーザ証明書でユーザ名の一部になります。

許可される DN 属性キーワードは次のとおりです。

- C = 国
- CN = 通常名
- EA = 電子メール アドレス
- L = 地名
- O = 組織名
- OU = 組織ユニット
- ST = 州/都道府県
- SN = 姓名の姓
- ST = 州/都道府県

（注） subject-name-default を標準の subject-name のデフォルト値として機能するように指定しない場合、ユーザを追加するたびに DN を指定する必要があります。

ローカル CA サーバのディセーブル化

ローカル CA サーバをディセーブルにするには、次の手順を実行します。

手順

ステップ 1 ローカル CA サーバ コンフィギュレーション モードに入ります。

crypto ca server

例：

```
ciscoasa(config)# crypto ca server
```

ステップ 2 ローカル CA サーバをディセーブルにします。

shutdown

例：

```
ciscoasa(config-ca-server)# shutdown
INFO: Local CA Server has been shutdown.
```

このコマンドは、Web サイト登録をディセーブルにして、ローカル CA サーバ コンフィギュレーションの修正を可能にし、現在のコンフィギュレーションと関連付けられたファイルを保存します。初期スタートアップ後、パスワードを求めるプロンプトを表示せずにローカル CA を再びイネーブルにすることができます。

外部ローカル CA ファイル ストレージの設定

外部ローカル CA ファイル ストレージを設定するには、次の手順を実行します。

手順

ステップ 1 特定のファイル システム タイプでコンフィギュレーション モードにアクセスします。

mount *name* **type**

例：

```
ciscoasa(config)# mount mydata type cifs
```

ステップ 2 CIFS ファイル システムをマウントします。

mount *name* **type cifs**

例：

```
ciscoasa(config-mount-cifs)# mount mydata type cifs
server 10.1.1.10 share myshare
domain example.com
username user6
password ********
status enable
```

（注） ファイル システムをマウントするユーザだけが、**no mount** コマンドを使ってアンマウントできます。

ステップ 3 ローカル CA サーバ コンフィギュレーション モードに入ります。

crypto ca server

例：

```
ciscoasa(config)# crypto ca server
```

ステップ 4 ローカル CA サーバ データベースで使用するマウント済みの CIFS ファイル システムである *mydata* の場所を指定します。

database path *mount-name directory-path*

例：

```
ciscoasa(config-ca-server)# database path mydata:newuser
```

このコマンドは、サーバへのパスを確立して、ストレージおよび取得に使用するローカル CA ファイルまたはフォルダ名を指定します。ローカル CA ファイル ストレージを ASA フラッシュ メモリに戻すには、**no database path** コマンドを使用します。

（注） 外部サーバに保存されているローカル CA ファイルは、ユーザ名とパスワードが保護されているファイル タイプが CIFS または FTP のマウント済みファイル システムが必要です。

ステップ 5 実行コンフィギュレーションを保存します。

write memory

例：

```
ciscoasa(config)# write memory
```

外部ローカル CA ファイル ストレージでは、ASA 設定を保存するたびに、ユーザ情報が ASA からマウント済みファイル システムおよびファイル場所 *mydata:newuser* に保存されます。

フラッシュ メモリ ストレージの場合、ユーザ情報は、スタートアップ コンフィギュレーションのデフォルトの場所に自動的に保存されます。

例

次の例は、フラッシュ メモリまたは次の外部ストレージに表示されるローカル CA ファイルの例です。

```
ciscoasa(config-ca-server)# dir LOCAL* //
Directory of disk0:/LOCAL*

75      -rwx  32          13:07:49 Jan 20 2007  LOCAL-CA-SERVER.ser
77      -rwx  229         13:07:49 Jan 20 2007  LOCAL-CA-SERVER.cdb
69      -rwx  0           01:09:28 Jan 20 2007  LOCAL-CA-SERVER.udb
81      -rwx  232         19:09:10 Jan 20 2007  LOCAL-CA-SERVER.crl
72      -rwx  1603        01:09:28 Jan 20 2007  LOCAL-CA-SERVER.p12

127119360 bytes total (79693824 bytes free)
```

CRL のダウンロードおよび保存

CEM コントローラをダウンロードおよび保存するには、次の手順を実行します。

手順

ステップ 1 ローカル CA サーバ コンフィギュレーション モードに入ります。

crypto ca server

例：

```
ciscoasa(config)# crypto ca server
```

ステップ 2 インターフェイスのポートを開き、CRL をそのインターフェイスからアクセスできるようにします。指定したインターフェイスおよびポートを使用して、CRL の着信要求をリッスンします。

publish-crl interface *interface* **port** *portnumber*

例：

```
ciscoasa(config-ca-server)# publish-crl outside 70
```

選択できるインターフェイスと任意のポートは、次のとおりです。

- inside：interface/GigabitEthernet0/1 の名前
- management：interface/Management0/0 の名前
- outside：interface/GigabitEthernet0/0 の名前
- ポート番号の範囲は 1 ～ 65535 です。TCP ポート 80 は、HTTP のデフォルト ポート番号です。

（注） インターフェイスを開いて CRL ファイルをダウンロードするにはこのコマンドが必要であるため、このコマンドを指定しないと、CDP の場所から CRL にアクセスできません。

CDP URL でインターフェイスの IP アドレスを使用するように設定し、CDP URL およびファイル名のパスも設定できます（http://10.10.10.100/user8/my_crl_file など）。

この場合、その IP アドレスが設定されたインターフェイスだけが CRL 要求をリッスンします。要求を受信すると、ASA によってパス /user8/my_crl_file と設定済み CDP URL が照合されます。パスが一致すると、ASA から、保存されている CRL ファイルが返されます。

（注） プロトコルは必ず HTTP にします。したがって、プレフィックスは http:// です。

ステップ 3 対象となるすべての証明書に含まれる CDP を指定します。CDP に特定の場所を設定しない場合、デフォルトの URL は http://*hostname.domain*/+CSCOCA+/asa_ca.crl になります。

cdp-url *url*

例：

```
ciscoasa(config-ca-server)# cdp-url http://172.16.1.1/pathname/myca.crl
```

ローカルCAは、ユーザ証明書が無効化または無効化解除されるたびに、CRLを更新および再発行します。無効化に変更がない場合、CRLのライフタイムごとに1回CRLが再発行されます。

このコマンドがローカルCA ASAからCRLを直接処理するように設定されている場合に、そのインターフェイスからCRLにアクセスできるようにインターフェイスのポートを開く手順については、CRLのダウンロードおよび保存を参照してください。

CRLは、ローカルCAによって発行された証明書の失効を検証する他のデバイスのためにあります。また、ローカルCAは、自らの証明書データベース内にあるすべての発行済み証明書とステータスを追跡します。検証する機関が、外部サーバから失効ステータスを取得してユーザ証明書を検証する必要がある場合、失効チェックが行われます。この場合、外部サーバは、証明書を発行したCA、またはCAが指定したサーバである可能性があります。

登録とユーザ管理

登録パラメータの設定

登録パラメータを設定するには、次の手順を実行します。

手順

ステップ1 ローカルCAサーバ コンフィギュレーション モードに入ります。

crypto ca server

例：

```
ciscoasa(config)# crypto ca server
```

ステップ2 ローカルCA登録ページに対して発行されたOTPが有効である期間を時間数で指定します。デフォルトの有効期間は72時間です。

otp expiration *timeout*

例：

```
ciscoasa(config-ca-server)# otp expiration 24
```

（注） 登録Webサイトで証明書に登録するためのユーザOTPをパスワードとして使用して、指定したユーザの発行済み証明書およびキーペアが含まれるPKCS12ファイルをロック解除することもできます。

ステップ 3 登録されたユーザが PKCS12 登録ファイルを取得できる時間数を指定します。

enrollment-retrieval *timeout*

例：

```
ciscoasa(config-ca-server)# enrollment-retrieval 120
```

この期間は、ユーザが正常に登録されたときに開始します。デフォルトの取得期間は 24 時間です。取得期間の有効値の範囲は 1 ～ 720 時間です。登録取得期間は、OTP の有効期間とは関係ありません。

登録取得期間が過ぎた後、ユーザ証明書とキーペアは無効になります。ユーザが証明書を受け取る唯一の方法は、管理者が証明書の登録を再開し、ユーザの再ログインを許可することです。

ユーザの追加と登録

ローカル CA データベースに登録できるユーザを追加するには、次の手順を実行します。

手順

ステップ 1 ローカル CA サーバ ユーザ データベースに新規ユーザを追加します。

crypto ca server user-db add *username* [**dn** *dn*] [**email** *emailaddress*]

例：

```
ciscoasa(config-ca-server)# crypto ca server user-db add user1 dn user1@example.com,
Engineer, Example Company, US, email user1@example.com
```

username 引数は、4 ～ 64 文字の文字列で、追加するユーザの単純なユーザ名です。ユーザ名には、電子メール アドレスを指定できます。この電子メール アドレスを使用して、登録案内の際に必要に応じてユーザに連絡を取ることができます。

dn 引数は、識別名で、OSI ディレクトリ（X.500）内のグローバルな正規のエントリ名です（たとえば、cn=user1@example.com, cn=Engineer, o=Example Company, c=US のようになります）。

e-mail-address 引数は、OTP および通知が送信される、新しいユーザの電子メール アドレスです。

ステップ 2 新たに追加したユーザにユーザ特権を付与します。

crypto ca server user-db allow *user*

例：

```
ciscoasa(config-ca-server)# crypto ca server user-db allow user
```

ステップ 3 ローカル CA データベースのユーザに、ユーザ証明書を登録およびダウンロードするように通知します。そのユーザには、OTP が自動的に電子メールで送信されます。

crypto ca server user-db email-otp *username*

例：

```
ciscoasa(config-ca-server)# crypto ca server user-db email-otp exampleuser1
```

（注） 管理者は、電子メールでのユーザ通知が必要である場合、ユーザを追加するときに、ユーザ名フィールドまたは電子メール フィールドに電子メール アドレスを指定する必要があります。

ステップ 4 対象の OTP を表示します。

crypto ca server user-db show-otp

例：

```
ciscoasa(config-ca-server)# crypto ca server user-db show-otp
```

ステップ 5 登録の時間制限を時間単位で設定します。デフォルトの有効期間は 72 時間です。

otp expiration *timeout*

例：

```
ciscoasa(config-ca-server)# otp expiration 24
```

このコマンドは、OTP がユーザ登録に有効な期間を定義します。この期間は、ユーザが登録を許可されたときに開始します。

ユーザが正しい OTP を使って時間制限内に正常に登録すると、ローカル CA サーバによって PKCS12 ファイルが作成されます。これには、そのユーザのキーペア、生成されたキーペアの公開キーに基づいたユーザ証明書、およびユーザを追加したときに指定した subject-name DN が含まれます。PKCS12 ファイルの内容は、OTP と呼ばれるパスフレーズによって保護されます。OTP は手動で処理できます。または、管理者が登録を許可した後、このファイルをローカル CA からユーザに電子メールで送信し、ダウンロードすることもできます。

PKCS12 ファイルは、*username.p12* という名前で一時的なストレージに保存されます。ストレージ内の PKCS12 ファイルを使用して、登録取得期間内に戻り、PKCS12 ファイルを必要な回数だけダウンロードすることができます。登録取得期間が過ぎると、PKCS12 ファイルがストレージから自動的に削除され、ダウンロードできなくなります。

（注） ユーザ証明書が含まれる PKCS12 ファイルを取得する前に登録の有効期間が切れた場合、登録は許可されません。

ユーザの更新

更新通知のタイミングを指定するには、次の手順を実行します。

手順

ステップ 1 ローカル CA サーバ コンフィギュレーション モードに入ります。

crypto ca server

例：

```
ciscoasa(config)# crypto ca server
```

ステップ 2 ローカル CA 証明書の有効期限までの日数（1 ～ 90）を指定します。この日数が経過すると、再登録に関する最初の通知が証明書所有者に送信されます。

renewal-reminder *time*

例：

```
ciscoasa(config-ca-server)# renewal-reminder 7
```

証明書は、有効期限を過ぎると無効になります。電子メールでユーザに送信される更新通知のタイプや送信時機の設定は各種あり、ローカル CA サーバの設定中に管理者が設定できます。

3 種類の通知が送信されます。ユーザ データベースに電子メール アドレスが指定されている場合、3 種類ある通知ごとに、電子メールが自動的に証明書所有者に送信されます。ユーザの電子メール アドレスを指定していない場合、syslog メッセージが更新要件を警告します。

ユーザがユーザ データベース内に存在する限り、ASA によって、有効期限間近の有効な証明書を持つすべてのユーザに、証明書の更新特権が自動的に付与されます。したがって、管理者がユーザに自動更新を許可しない場合、更新期間の前にそのユーザをデータベースから削除する必要があります。

ユーザの復元

ローカル CA サーバによって発行され、以前無効にした証明書とユーザを復元するには、次の手順を実行します。

手順

ステップ 1 ローカル CA サーバ コンフィギュレーション モードに入ります。

crypto ca server

例：

```
ciscoasa(config)# crypto ca server
```

ステップ 2 ユーザを復元し、ローカル CA サーバによって発行され、以前無効にした証明書を無効化解除します。

crypto ca server unrevoke *cert-serial-no*

例：

```
ciscoasa(config-ca-server)# crypto ca server unrevoke 782ea09f
```

ローカルCAでは、CRLは、無効になったすべてのユーザ証明書のシリアル番号で保持されます。このリストは外部デバイスで使用でき、**cdp-url** コマンドや **publish-crl** コマンドなどで設定されている場合に、ローカルCAから直接取得することができます。証明書のシリアル番号で、現在の証明書を無効化（または無効化解除）すると、CRLにはそれらの変更が自動的に反映されます。

ユーザの削除

ユーザ データベースからユーザ名によってユーザを削除するには、次の手順を実行します。

手順

ステップ 1 ローカル CA サーバ コンフィギュレーション モードに入ります。

crypto ca server

例：

```
ciscoasa(config)# crypto ca server
```

ステップ 2 ユーザデータベースからユーザを削除し、そのユーザに発行された有効な証明書の無効化を許可します。

crypto ca server user-db remove *username*

例：

```
ciscoasa(config-ca-server)# crypto ca server user-db remove user1
```

証明書の無効化

ユーザ証明書を無効にするには、次の手順を実行します。

手順

ステップ 1 ローカル CA サーバ コンフィギュレーション モードに入ります。

crypto ca server

例：

```
ciscoasa(config)# crypto ca server
```

ステップ 2 16 進数の形式で証明書のシリアル番号を入力します。

crypto ca server revoke *cert-serial-no*

例：

```
ciscoasa(config-ca-server)# crypto ca server revoke 782ea09f
```

このコマンドは、ローカル CA サーバ上の証明書データベースと CRL で証明書に無効のマークを付けます。CRL は、自動的に再発行されます。

（注） ASA の証明書を無効にするには、パスワードも必要なので、パスワードを必ず記録し、安全な場所に保管してください。

証明書の有効期限アラートの設定（ID 証明書または CA 証明書用）

ASA は、トラストポイントの CA 証明書および ID 証明書について有効期限を24時間ごとに 1 回チェックします。証明書の有効期限がまもなく終了する場合、syslog がアラートとして発行されます。

リマインダおよび繰り返し間隔を設定するためにCLIが提供されます。デフォルトでは、リマインダは有効期限の 60 日前に開始され、7 日ごとに繰り返されます。次のコマンドを使用して、最初のアラートが送信される有効期限までの日数を設定し、リマインダが送信される間隔を設定します。

```
[no] crypto ca alerts expiration [begin <days before expiration>] [repeat <days>]
```

アラートの設定に関係なく、有効期限の直前の週はリマインダが毎日送信されます。次の **show** コマンドと **clear** コマンドも追加されています。

```
clear conf crypto ca alerts
show run crypto ca alerts
```

更新リマインダに加え、コンフィギュレーションに期限が切れた証明書が見つかった場合、その証明書を更新するか、または削除することで、コンフィギュレーションを修正するために syslog が毎日 1 回生成されます。

たとえば、有効期限アラートが 60 日に開始され、その後 6 日ごとに繰り返すように設定されているとします。ASAが 40 日に再起動されると、アラートはその日に送信され、次のアラートは 36 日目に送信されます。

（注） 有効期限チェックは、トラストプールの証明書では実行されません。ローカルCA トラストポイントは、有効期限チェックの通常のトラストポイントとしても扱われます。

デジタル証明書のモニタリング

デジタル証明書ステータスのモニタリングについては、次のコマンドを参照してください。

- **show crypto ca server**

  このコマンドは、ローカル CA のコンフィギュレーションとステータスを表示します。

- **show crypto ca server cert-db**

  このコマンドは、ローカル CA によって発行されたユーザ証明書を表示します。

- **show crypto ca server certificate**

  このコマンドは、コンソールに base 64 形式でローカル CA 証明書を表示し、使用可能な場合は、他のデバイスへのインポート時に新しい証明書の検証に使うためのロールオーバー証明書のサムプリントを含むロールオーバー証明書の情報を表示します。

- **show crypto ca server crl**

  このコマンドは、CRL を表示します。

- **show crypto ca server user-db**

  このコマンドは、ユーザとユーザのステータスを表示します。この情報に次の修飾子を使用して、表示されるレコード数を減らすことができます。

  - allowed：現在登録が許可されているユーザだけを表示します。
  - enrolled：登録され、有効な証明書を持つユーザだけを表示します。
  - expired：期間満了になった証明書を持つユーザだけを表示します。
  - on-hold：証明書を持たず現在登録が許可されていないユーザだけを表示します。

- **show crypto ca server user-db allowed**

  このコマンドは、登録できるユーザを表示します。

- **show crypto ca server user-db enrolled**

このコマンドは、有効な証明書を持つ登録済みユーザを表示します。

- **show crypto ca server user-db expired**

  このコマンドは、期間満了した証明書を持つユーザを表示します。

- **show crypto ca server user-db on-hold**

  このコマンドは、証明書がなく、登録が許可されていないユーザを表示します。

- **show crypto key** *name of key*

  このコマンドは、生成したキー ペアを表示します。

- **show running-config**

  このコマンドは、ローカル CA 証明書マップ ルールを表示します。

例

次の例では、汎用 RSA キーを表示します。

```
ciscoasa/contexta(config)# show crypto key mypubkey rsa
Key pair was generated at: 16:39:47 central Feb 10 2010
Key name: <Default-RSA-Key>
 Usage: General Purpose Key
 Modulus Size (bits): 2048
 Storage: config
 Key Data:

  30820122 300d0609 2a864886 f70d0101 01050003 82010f00 3082010a 02820101
  00ea2c38 df9c606e ddb7b08a e8b0a1a8 65592d85 0711cac5 fceddee1 fa494297
  525fffc0 90da8a4c e696e44e 0646c661 48b3602a 960d7a3a 52dae14a 5f983603
  e1f33e40 a6ce04f5 9a812894 b0fe0403 f8d7e05e aea79603 2dcd56cc 01261b3e
  93bff98f df422fb1 2066bfa4 2ff5d2a4 36b3b1db edaebf16 973b2bd7 248e4dd2
  071a978c 6e81f073 0c4cd57b db6d9f40 69dc2149 e755fb0f 590f2da8 b620efe6
  da6e8fa5 411a841f e72bb8ea cf4bdb79 f4e57ff3 a940ce3b 4a2c7052 56c1d17b
  af8fe2e2 e58718c6 ed1da0f0 1c6f36eb 79eb1aeb f098b5c4 79e07658 a52d8c7a
  51ceabfb f8ade096 7217cf2d 3728077e 89441d89 9bf5f875 c8d2db39 c858bb7a
  7d020301 0001
```

次に、ローカル CA CRL を表示する例を示します。

```
ciscoasa(config)# show crypto ca server crl
Certificate Revocation List:
    Issuer: cn=xx5520-1-3-2007-1
    This Update: 13:32:53 UTC Jan 4 2010
    Next Update: 13:32:53 UTC Feb 3 2010
    Number of CRL entries: 2
    CRL size: 270 bytes
Revoked Certificates:
    Serial Number: 0x6f
    Revocation Date: 12:30:01 UTC Jan 4 2010
    Serial Number: 0x47
    Revocation Date: 13:32:48 UTC Jan 4 2010
```

次に、1 人の保留中のユーザを表示する例を示します。

```
ciscoasa(config)# show crypto ca server user-db on-hold
username: wilma101
email:    <None>
dn:       <None>
allowed:  <not allowed>
notified: 0
ciscoasa(config)#
```

次に、**show running-config** コマンドの出力例を示します。この出力には、ローカルCA証明書マップ ルールが表示されています。

```
crypto ca certificate map 1
 issuer-name co asc
 subject-name attr ou eq Engineering
```

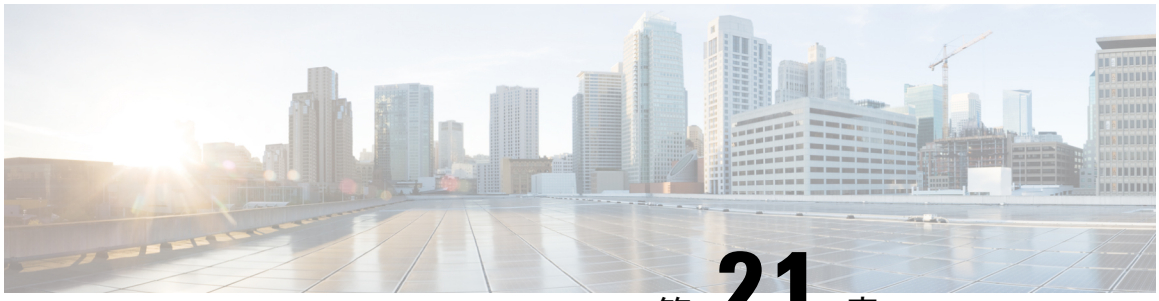
証明書管理の履歴

表 *22 :* 証明書管理の履歴

機能名	プラットフォーム リリース	説明
証明書管理	7.0(1)	デジタル証明書（CA 証明書、ID 証明書、およびコード署名者証明書など）は、認証用のデジタル ID を提供します。デジタル証明書には、名前、シリアル番号、会社、部門、またはIPアドレスなど、ユーザまたはデバイスを識別する情報が含まれます。CA は、証明書に「署名」してその認証を確認することで、デバイスまたはユーザのアイデンティティを保証する、信頼できる機関です。CA は、公開キーまたは秘密キーの暗号化を使用してセキュリティを保証する PKI コンテキストで、デジタル証明書を発行します。
証明書管理	7.2(1)	次のコマンドを導入しました。 **issuer-name** *DN-string*、**revocation-check crl none**、**revocation-check crl**、**revocation-check none**。 **crl** {**required** | **optional** | **nocheck**} コマンドが非推奨になりました。

機能名	プラットフォーム リリース	説明
証明書管理	8.0(2)	次のコマンドを導入しました。 **cdp-url**、**crypto ca server**、**crypto ca server crl issue**、**crypto ca server revoke** *cert-serial-no*、**crypto ca server unrevoke** *cert-serial-no*、**crypto ca server user-db add** *user* [**dn** *dn*] [**email** *e-mail-address*]、**crypto ca server user-db allow** {*username* | **all-unenrolled** | **all-certholders**} [**display-otp**] [**email-otp**] [**replace-otp**]、**crypto ca server user-db email-otp** {*username* | **all-unenrolled** | **all-certholders**}、**crypto ca server user-db remove** *username*、**crypto ca server user-db show-otp** {*username* | **all-certholders** | **all-unenrolled**}、**crypto ca server user-db write**、[**no**] **database path** *mount-name directory-path*、**debug crypto ca server** [*level*]、**lifetime** {**ca-certificate** | **certificate** | **crl**} *time*、**no shutdown**、**otp expiration** *timeout*、**renewal-reminder** *time*、**show crypto ca server**、**show crypto ca server cert-db** [**user** *username* | **allowed** | **enrolled** | **expired** | **on-hold**] [**serial** *certificate-serial-number*]、**show crypto ca server certificate**、**show crypto ca server crl**、**show crypto ca server user-db** [**expired** | **allowed** | **on-hold** | **enrolled**]、**show crypto key** *name of key*、**show running-config**、**shutdown**

機能名	プラットフォーム リリース	説明
SCEP プロキシ	8.4(1)	サードパーティ CA からのデバイス証明書を安全に構成できる機能を導入しました。 次のコマンドを導入しました。 **crypto ikev2 enable outside client-services port** *portnumber*、**scep-enrollment enable**、**scep-forwarding-url value** *URL*、**secondary-pre-fill-username clientless hide use-common-password** *password*、**secondary-pre-fill-username ssl-client hide use-common-password** *password*、**secondary-username-from-certificate** {**use-entire-name** | **use-script** | {*primary_attr* [*secondary-attr*]}} [**no-certificate-fallback cisco-secure-desktop machine-unique-id**]。
ローカル CA サーバ	9.12(1)	ASA の構成済み FQDN を使用する代わりに設定可能な登録用 URL の FQDN を作成するため、新しい CLI オプションが導入されました。この新しいオプションは、ccrypto ca server の smpt モードに追加されます。 ローカル CA サーバは廃止され、以降のリリースで削除されます。ASA がローカル CA サーバとして設定されている場合、デジタル証明書の発行、証明書失効リスト（CRL）の発行、および発行された証明書の安全な取り消しを行うために有効になります。この機能は古くなったため、crypto ca server コマンドは廃止されています。



第 21 章

トランスペアレントファイアウォールモードの ARP インスペクションおよび MAC アドレス テーブル

この章では、MACアドレステーブルのカスタマイズ方法、およびブリッジグループのARPインスペクションの設定方法について説明します。

ARP インスペクションと MAC アドレス テーブルについて

ブリッジ グループのインターフェイスでは、ARP インスペクションは「中間者」攻撃を防止します。他の ARP の設定をカスタマイズすることも可能です。ブリッジ グループの MAC アドレス テーブルのカスタマイズができます。これには、MAC スプーフィングに対する防御としてのスタティック ARP エントリの追加が含まれます。

ブリッジグループのトラフィックの ARP インスペクション

デフォルトでは、ブリッジグループのメンバーの間ですべてのARPパケットが許可されます。ARP パケットのフローを制御するには、ARP インスペクションをイネーブルにします。

ARPインスペクションによって、悪意のあるユーザが他のホストやルータになりすます（ARP スプーフィングと呼ばれる）のを防止できます。ARP スプーフィングが許可されていると、「中間者」攻撃を受けることがあります。たとえば、ホストが ARP 要求をゲートウェイ ルータに送信すると、ゲートウェイルータはゲートウェイ ルータのMACアドレスで応答します。ただし、攻撃者は、ルータの MAC アドレスではなく攻撃者の MAC アドレスで別の ARP 応答をホストに送信します。これで、攻撃者は、すべてのホストトラフィックを代行受信してルータに転送できるようになります。

ARP インスペクションを使用すると、正しい MAC アドレスとそれに関連付けられた IP アドレスがスタティック ARP テーブル内にある限り、攻撃者は攻撃者の MAC アドレスで ARP 応答を送信できなくなります。

ARP インスペクションをイネーブルにすると、ASAは、すべての ARP パケット内の MAC アドレス、IP アドレス、および送信元インターフェイスを ARP テーブル内のスタティック エントリと比較し、次のアクションを実行します。

- IPアドレス、MACアドレス、および送信元インターフェイスがARPエントリと一致する場合、パケットを通過させます。
- MAC アドレス、IP アドレス、またはインターフェイス間で不一致がある場合、ASAはパケットをドロップします。
- ARPパケットがスタティックARPテーブル内のどのエントリとも一致しない場合、パケットをすべてのインターフェイスに転送（フラッディング）するか、またはドロップするようにASAを設定できます。

（注） 専用の 管理 インターフェイスは、このパラメータが flood に設定されている場合でもパケットをフラッディングしません。

MAC アドレス テーブル

ブリッジ グループを使用する場合、ASA は、通常のブリッジまたはスイッチと同様に、MAC アドレスを学習して MAC アドレス テーブルを作成します。デバイスがブリッジ グループ経由でパケットを送信すると、ASA が MAC アドレスをアドレス テーブルに追加します。テーブルで MAC アドレスと発信元インターフェイスが関連付けられているため、ASAは、パケットが正しいインターフェイスからデバイスにアドレス指定されていることがわかります。ブリッジ グループ メンバー間のトラフィックには ASA セキュリティ ポリシーが適用されるため、パケットの宛先 MAC アドレスがテーブルに含まれていなくても、通常のブリッジのように、すべてのインターフェイスに元のパケットを ASA がフラッディングすることはありません。代わりに、直接接続されたデバイスまたはリモートデバイスに対して次のパケットを生成します。

- 直接接続されたデバイスへのパケット：ASA は宛先 IP アドレスに対して ARP 要求を生成し、ARP 応答を受信したインターフェイスを学習します。

- リモートデバイスへのパケット：ASA は宛先 IP アドレスへの ping を生成し、ping 応答を受信したインターフェイスを学習します。

元のパケットはドロップされます。

デフォルト設定

- ARP インスペクションをイネーブルにした場合、デフォルト設定では、一致しないパケットはフラッドします。
- ダイナミック MAC アドレス テーブルのデフォルトのタイムアウト値は 5 分です。
- デフォルトでは、各インターフェイスはトラフィックに入る MAC アドレスを自動的に学習し、ASAは対応するエントリを MAC アドレス テーブルに追加します。

ARP インスペクションと MAC アドレス テーブルのガイドライン

- ARP インスペクションは、ブリッジグループでのみサポートされます。
- MAC アドレス テーブル構成は、ブリッジグループでのみサポートされます。
- ブリッジグループは、トランスペアレント ファイアウォール モードでのみサポートされます。

ARP インスペクションとその他の ARP パラメータの設定

トランスペアレント ファイアウォール モードのブリッジ グループでは、ARP インスペクションをイネーブルにすることができます。その他の ARP パラメータは、ブリッジ グループとルーテッド モードのインターフェイスの両方で設定できます。

手順

ステップ 1 スタティック ARP エントリの追加と、他の ARP パラメータのカスタマイズ （684 ページ）に従って、スタティック ARP エントリを追加します。ARP インスペクションは ARP パケットを ARP テーブルのスタティック ARP エントリと比較するので、この機能にはスタティック ARP エントリが必要です。その他の ARP パラメータも設定できます。

ステップ 2 （トランスペアレント モードのみ）ARP インスペクションの有効化 （685 ページ）に従って ARP インスペクションを有効にします。

スタティック ARP エントリの追加と、他の ARP パラメータのカスタマイズ

ブリッジグループのデフォルトでは、ブリッジ グループ メンバー インターフェイス間の ARP パケットはすべて許可されます。ARP パケットのフローを制御するには、ARP インスペクションをイネーブルにします。ARP インスペクションは、ARP パケットを ARP テーブルのスタティック ARP エントリと比較します。

ルーテッド インターフェイスの場合、スタティック ARP エントリを入力できますが、通常はダイナミック エントリで十分です。ルーテッド インターフェイスの場合、直接接続されたホストにパケットを配送するために ARP テーブルが使用されます。送信者は IP アドレスでパケットの宛先を識別しますが、イーサネットにおける実際のパケット配信は、イーサネット MAC アドレスに依存します。ルータまたはホストは、直接接続されたネットワークでパケットを配信する必要がある場合、IP アドレスに関連付けられた MAC アドレスを要求する ARP 要求を送信し、ARP 応答に従ってパケットを MAC アドレスに配信します。ホストまたはルータには ARP テーブルが保管されるため、配信が必要なパケットごとに ARP 要求を送信する必要はありません。ARP テーブルは、ARP 応答がネットワーク上で送信されるたびにダイナミックに更新されます。一定期間使用されなかったエントリは、タイムアウトします。エントリが正しくない場合（たとえば、所定の IP アドレスの MAC アドレスが変更された場合など）、新しい情報で更新される前にこのエントリがタイムアウトする必要があります。

トランスペアレント モードの場合、管理トラフィックなどの ASA との間のトラフィックに、ASA は ARP テーブルのダイナミック ARP エントリのみを使用します。

ARP タイムアウトなどの ARP 動作を設定することもできます。

手順

ステップ 1 スタティック ARP エントリを追加します。

arp *interface_name ip_address mac_address* [**alias**]

例：

```
ciscoasa(config)# arp outside 10.1.1.1 0009.7cbe.2100
```

この例では、外部インターフェイスで、IP アドレスが 10.1.1.1、MAC アドレスが 0009.7cbe.2100 のルータからの ARP 応答が許可されます。

このマッピングでプロキシ ARP を有効にするには、ルーテッド モードで**alias**を指定します。ASA は、指定された IP アドレスの ARP 要求を受信すると、ASA MAC アドレスで応答します。このキーワードは、ARP を実行しないデバイスがある場合などに役立ちます。トランスペアレント ファイアウォール モードでは、このキーワードは無視されます。ASA はプロキシ ARP を実行しません。

ステップ 2 ダイナミック ARP エントリの ARP タイムアウトを設定します。

arp timeout *seconds*

例：

```
ciscoasa(config)# arp timeout 5000
```

このフィールドでは、ASA が ARP テーブルを再構築するまでの時間を、60 ～ 4294967 秒の範囲で設定します。デフォルトは14400秒です。ARPテーブルを再構築すると、自動的に新しいホスト情報が更新され、古いホスト情報が削除されます。ホスト情報は頻繁に変更されるため、タイムアウトを短くすることが必要になる場合があります。

ステップ 3 非接続サブネットを許可する

arp permit-nonconnected

ASA ARP キャッシュには、直接接続されたサブネットからのエントリだけがデフォルトで含まれています。ARPキャッシュをイネーブルにして、間接接続されたサブネットを含めることもできます。セキュリティリスクを認識していない場合は、この機能をイネーブルにすることは推奨しません。この機能は、ASAに対するサービス拒否（DoS）攻撃を助長する場合があります。任意のインターフェイスのユーザが大量の ARP 応答を送信して、偽エントリで ASA ARP テーブルがあふれる可能性があります。

次の機能を使用する場合は、この機能を使用する必要がある可能性があります。

- セカンデリ サブネット。
- トラフィック転送の隣接ルートのプロキシ ARP。

ARP インスペクションの有効化

この項では、ブリッジ グループ用に ARP インスペクションをイネーブルにする方法について説明します。

手順

ARP インスペクションをイネーブルにします。

arp-inspection *interface_name* **enable** [**flood** | **no-flood**]

例：

```
ciscoasa(config)# arp-inspection outside enable no-flood
```

flood キーワードは、一致しない ARP パケットをすべてのインターフェイスに転送し、**no-flood** は、一致しないパケットをドロップします。

デフォルト設定では、一致しないパケットはフラッドします。スタティック エントリにある ARP だけが ASA を通過するように制限するには、このコマンドを **no-flood** に設定します。

トランスペアレントモードのブリッジグループにおける MAC アドレス テーブルのカスタマイズ

ここでは、ブリッジグループの MAC アドレス テーブルをカスタマイズする方法について説明します。

ブリッジ グループのスタティック MAC アドレスの追加

通常、MAC アドレスは、特定の MAC アドレスからのトラフィックがインターフェイスに入ったときに、MAC アドレス テーブルに動的に追加されます。スタティック MAC アドレスは、MAC アドレス テーブルに追加できます。スタティック エントリを追加する利点の 1 つに、MAC スプーフィングに対処できることがあります。スタティック エントリと同じ MAC アドレスを持つクライアントが、そのスタティックエントリに一致しないインターフェイスにトラフィックを送信しようとした場合、ASA はトラフィックをドロップし、システム メッセージを生成します。スタティック ARP エントリを追加するときに（スタティック ARP エントリの追加と、他の ARP パラメータのカスタマイズ（684 ページ）を参照）、スタティック MAC アドレス エントリは MAC アドレス テーブルに自動的に追加されます。

MAC アドレス テーブルにスタティック MAC アドレスを追加するには、次の手順を実行します。

手順

スタティック MAC アドレス エントリを追加します。

mac-address-table static *interface_name mac_address*

例：

```
ciscoasa(config)# mac-address-table static inside 0009.7cbe.2100
```

interface_name は、発信元インターフェイスです。

MAC アドレス タイムアウトを設定する

ダイナミック MAC アドレス テーブルのデフォルトのタイムアウト値は 5 分ですが、タイムアウトは変更できます。タイムアウトを変更するには、次の手順を実行します。

手順

MAC アドレス エントリのタイムアウトを設定します。

mac-address-table aging-time *timeout_value*

例：

```
ciscoasa(config)# mac-address-table aging-time 10
```

timeout_value（分）は、5 ～ 720（12 時間）です。5 分がデフォルトです。

MAC アドレス ラーニングのディセーブル化

デフォルトで、各インターフェイスは着信トラフィックの MAC アドレスを自動的に学習し、ASA は対応するエントリを MAC アドレス テーブルに追加します。必要に応じて MAC アドレス ラーニングをディセーブルにできますが、この場合、MACアドレスをテーブルにスタティックに追加しないと、トラフィックが ASA を通過できなくなります。

MAC アドレス ラーニングをディセーブルにするには、次の手順を実行します。

手順

MAC アドレス ラーニングをディセーブルにします。

mac-learn *interface_name* **disable**

例：

```
ciscoasa(config)# mac-learn inside disable
```

このコマンドの **no** 形式を使用すると、MAC アドレス ラーニングが再度イネーブルになります。

clear configure mac-learn コマンドは、すべてのインターフェイスで MAC アドレス ラーニングを再度イネーブルにします。

ARP インスペクションと MAC アドレス テーブルのモニタリング

- **show arp-inspection**

ARP インスペクションをモニタします。すべてのインターフェイスについて、ARP インスペクションの現在の設定を表示します。

- **show mac-address-table [*interface_name*]**

  MAC アドレス テーブルをモニタします。すべての MAC アドレス テーブル（両方のインターフェイスのスタティック エントリとダイナミック エントリ）を表示できます。または、あるインターフェイスの MAC アドレス テーブルを表示できます。

  すべてのテーブルを表示する **show mac-address-table** コマンドの出力例を示します。

```
ciscoasa# show mac-address-table
interface        mac address           type         Time Left
------------------------------------------------------------------------
outside     0009.7cbe.2100       static    -
inside     0010.7cbe.6101       static    -
inside     0009.7cbe.5101       dynamic    10
```

  内部インターフェイスのテーブルを表示する **show mac-address-table** コマンドの出力例を示します。

```
ciscoasa# show mac-address-table inside
interface        mac address       type         Time Left
------------------------------------------------------------------------
inside     0010.7cbe.6101       static    -
inside     0009.7cbe.5101       dynamic    10
```

ARP インスペクションと MAC アドレス テーブルの履歴

機能名	プラットフォーム リリース	機能情報
ARP インスペクション	7.0(1)	ARP インスペクションは、すべての ARP パケットの MAC アドレス、IP アドレス、および送信元インターフェイスを、ARP テーブルのスタティック エントリと比較します。この機能は、トランスペアレント ファイアウォール モード。 **arp**、**arp-inspection**、および **show arp-inspection** コマンドが導入されました。

機能名	プラットフォーム リリース	機能情報
MAC アドレス テーブル	7.0(1)	トランスペアレント モード。 **mac-address-table static**、**mac-address-table aging-time**、**mac-learn disable**、および **show mac-address-table** コマンドが導入されました。
間接接続されたサブネットの ARP キャッシュの追加	8.4(5)/9.1(2)	ASA ARP キャッシュには、直接接続されたサブネットからのエントリだけがデフォルトで含まれています。また、ARP キャッシュに間接接続されたサブネットを含めることができるようになりました。セキュリティ リスクを認識していない場合は、この機能をイネーブルにすることは推奨しません。この機能は、ASA に対するサービス拒否（DoS）攻撃を助長する場合があります。任意のインターフェイスのユーザが大量の ARP 応答を送信して、偽エントリで ASA ARP テーブルがあふれる可能性があります。 次の機能を使用する場合は、この機能を使用する必要がある可能性があります。 • セカンデリ サブネット。 • トラフィック転送の隣接ルートのプロキシ ARP。 **arp permit-nonconnected** コマンドが導入されました。

第 V 部

IP ルーティング

第 22 章

ルーティングの概要

この章では、ASA 内でのルーティングの動作について説明します。

パス判別

ルーティング プロトコルでは、メトリックを使用して、パケットの移動に最適なパスを評価します。メトリックは、宛先への最適なパスを決定するためにルーティング アルゴリズムが使用する、パスの帯域幅などの測定基準です。パスの決定プロセスを支援するために、ルーティング アルゴリズムは、ルート情報が格納されるルーティング テーブルを初期化して保持します。ルート情報は、使用するルーティング アルゴリズムによって異なります。

ルーティング アルゴリズムにより、さまざまな情報がルーティング テーブルに入力されます。宛先またはネクスト ホップの関連付けにより、最終的な宛先に達するまで、「ネクスト ホップ」を表す特定のルータにパケットを送信することによって特定の宛先に最適に到達できることがルータに示されます。ルータは、着信パケットを受信すると宛先アドレスを確認し、このアドレスとネクスト ホップとを関連付けようとします。

ルーティング テーブルには、パスの妥当性に関するデータなど、他の情報を格納することもできます。ルータは、メトリックを比較して最適なルートを決定します。これらのメトリックは、使用しているルーティング アルゴリズムの設計によって異なります。

ルータは互いに通信し、さまざまなメッセージの送信によりそのルーティング テーブルを保持しています。ルーティング アップデート メッセージはそのようなメッセージの 1 つで、通常はルーティング テーブル全体か、その一部で構成されています。ルーティング アップデートを他のすべてのルータから分析することで、ルータはネットワーク トポロジの詳細な全体像を構築できます。ルータ間で送信されるメッセージのもう 1 つの例であるリンク ステート アドバ

タイズメントは、他のルータに送信元のリンクのステートを通知します。リンク情報も、ネットワークの宛先に対する最適なルートをルータが決定できるように、ネットワーク トポロジの全体像の構築に使用できます。

（注） 非対称ルーティングがサポートされるのは、マルチ コンテキスト モードでのアクティブ/アクティブ フェールオーバーに対してのみです。

サポートされるルート タイプ

ルータが使用できるルート タイプには、さまざまなものがあります。ASAでは、次のルート タイプが使用されます。

- スタティックとダイナミックの比較
- シングルパスとマルチパスの比較
- フラットと階層型の比較
- リンクステートと距離ベクトル型の比較

スタティックとダイナミックの比較

スタティック ルーティング アルゴリズムは、実はネットワーク管理者が確立したテーブル マップです。このようなマッピングは、ネットワーク管理者が変更するまでは変化しません。スタティック ルートを使用するアルゴリズムは設計が容易であり、ネットワーク トラフィックが比較的予想可能で、ネットワーク設計が比較的単純な環境で正しく動作します。

スタティック ルーティング システムはネットワークの変更に対応できないため、一般に、変化を続ける大規模なネットワークには不向きであると考えられています。主なルーティング アルゴリズムのほとんどはダイナミック ルーティング アルゴリズムであり、受信したルーティング アップデート メッセージを分析することで、変化するネットワーク環境に適合します。メッセージがネットワークが変化したことを示している場合は、ルーティング ソフトウェアはルートを再計算し、新しいルーティング アップデート メッセージを送信します。これらのメッセージはネットワーク全体に送信されるため、ルータはそのアルゴリズムを再度実行し、それに従ってルーティング テーブルを変更します。

ダイナミック ルーティング アルゴリズムは、必要に応じてスタティック ルートで補足できます。たとえば、ラスト リゾート ルータ（ルーティングできないすべてのパケットが送信されるルータのデフォルトルート）を、ルーティングできないすべてのパケットのリポジトリとして機能するように指定し、すべてのメッセージを少なくとも何らかの方法で確実に処理することができます。

シングルパスとマルチパスの比較

一部の高度なルーティング プロトコルは、同じ宛先に対する複数のパスをサポートしています。シングルパス アルゴリズムとは異なり、これらのマルチパス アルゴリズムでは、複数の回線でトラフィックを多重化できます。マルチパス アルゴリズムの利点は、スループットと信頼性が大きく向上することであり、これは一般に「ロードシェアリング」と呼ばれています。

フラットと階層型の比較

ルーティング アルゴリズムには、フラットなスペースで動作するものと、ルーティング階層を使用するものがあります。フラット ルーティング システムでは、ルータは他のすべてのルータのピアになります。階層型ルーティング システムでは、一部のルータが実質的なルーティング バックボーンを形成します。バックボーン以外のルータからのパケットはバックボーン ルータに移動し、宛先の一般エリアに達するまでバックボーンを通じて送信されます。この時点で、パケットは、最後のバックボーン ルータから、1 つ以上のバックボーン以外のルータを通じて最終的な宛先に移動します。

多くの場合、ルーティング システムは、ドメイン、自律システム、またはエリアと呼ばれるノードの論理グループを指定します。階層型のシステムでは、ドメイン内の一部のルータは他のドメインのルータと通信できますが、他のルータはそのドメイン内のルータ以外とは通信できません。非常に大規模なネットワークでは、他の階層レベルが存在することがあり、最も高い階層レベルのルータがルーティング バックボーンを形成します。

階層型ルーティングの第一の利点は、ほとんどの企業の組織に類似しているため、そのトラフィック パターンもサポートするという点です。ほとんどのネットワーク通信は、小さい企業グループ（ドメイン）内で発生します。ドメイン内ルータは、そのドメイン内の他のルータだけを認識していれば済むため、そのルーティング アルゴリズムを簡素化できます。また、使用しているルーティング アルゴリズムに応じて、ルーティング アップデート トラフィックを減少させることができます。

リンクステートと距離ベクトル型の比較

リンクステート アルゴリズム（最短パス優先アルゴリズムとも呼ばれる）は、インターネットワークのすべてのノードにルーティング情報をフラッドします。ただし、各ルータは、それ自体のリンクのステートを記述するルーティング テーブルの一部だけを送信します。リンクステート アルゴリズムでは、各ルータはネットワークの全体像をそのルーティング テーブルに構築します。距離ベクトル型アルゴリズム（Bellman-Ford アルゴリズムとも呼ばれる）では、各ルータが、そのネイバーだけに対してそのルーティング テーブル全体または一部を送信するように要求されます。つまり、リンクステート アルゴリズムは小規模なアップデートを全体に送信しますが、距離ベクトル型アルゴリズムは、大規模なアップデートを隣接ルータだけに送信します。距離ベクトル型アルゴリズムは、そのネイバーだけを認識します。通常、リンクステート アルゴリズムは OSPF ルーティング プロトコルとともに使用されます。

ルーティングにサポートされているインターネットプロトコル

ASA は、ルーティングに対してさまざまなインターネットプロトコルをサポートしています。この項では、各プロトコルについて簡単に説明します。

- Enhanced Interior Gateway Routing Protocol（EIGRP）

  EIGRP は、IGRP ルータとの互換性とシームレスな相互運用性を提供するシスコ独自のプロトコルです。自動再配布メカニズムにより、IGRP ルートを Enhanced IGRP に、または Enhanced IGRP からインポートできるため、Enhanced IGRP を既存の IGRP ネットワークに徐々に追加できます。

- Open Shortest Path First（OSPF）

  OSPF は、インターネット プロトコル（IP）ネットワーク向けに、インターネット技術特別調査委員会（IETF）の Interior Gateway Protocol（IGP）作業部会によって開発されたルーティング プロトコルです。OSPF は、リンクステート アルゴリズムを使用して、すべての既知の宛先までの最短パスを構築および計算します。OSPF エリア内の各ルータには、ルータが使用可能なインターフェイスと到達可能なネイバーそれぞれのリストである同一のリンクステート データベースが置かれています。

- ルーティング情報プロトコル（RIP）

  RIP は、ホップ カウントをメトリックとして使用するディスタンスベクトル プロトコルです。RIP は、グローバルなインターネットでトラフィックのルーティングに広く使用されている Interior Gateway Protocol（IGP）です。つまり、1 つの自律システム内部でルーティングを実行します。

- Border Gateway Protocol（BGP）

  BGP は自律システム間のルーティング プロトコルです。BGP は、インターネットのルーティング情報を交換するために、インターネット サービス プロバイダー（ISP）間で使用されるプロトコルです。カスタマーは ISP に接続し、ISP は BGP を使用してカスタマーおよび ISP ルートを交換します。自律システム（AS）間で BGP を使用する場合、このプロトコルは外部 BGP（EBGP）と呼ばれます。サービス プロバイダーが BGP を使用して AS 内でルートを交換する場合、このプロトコルは内部 BGP（IBGP）と呼ばれます。

ルーティング テーブル

ここでは、ルーティング テーブルの仕組みについて説明します。

ルーティング テーブルへの入力方法

ASAのルーティング テーブルには、スタティックに定義されたルート、直接接続されているルート、およびダイナミック ルーティング プロトコルで検出されたルートを入力できます。ASAは、ルーティング テーブルに含まれるスタティック ルートと接続されているルートに加えて、複数のルーティングプロトコルを実行できるため、同じルートが複数の方法で検出または入力される可能性があります。同じ宛先への2つのルートがルーティング テーブルに追加されると、ルーティング テーブルに残るルートは次のように決定されます。

- 2つのルートのネットワーク プレフィックス長（ネットワーク マスク）が異なる場合は、どちらのルートも固有と見なされ、ルーティングテーブルに入力されます。入力された後は、パケット転送ロジックが 2 つのうちどちらを使用するかを決定します。

  たとえば、RIP プロセスと OSPF プロセスが次のルートを検出したとします。

  - RIP：192.168.32.0/24
  - OSPF：192.168.32.0/19

  OSPF ルートのアドミニストレーティブ ディスタンスの方が適切であるにもかかわらず、これらのルートのプレフィックス長（サブネットマスク）はそれぞれ異なるため、両方のルートがルーティング テーブルにインストールされます。これらは異なる宛先と見なされ、パケット転送ロジックが使用するルートを決定します。

- ASAが、1 つのルーティング プロトコル（RIP など）から同じ宛先に複数のパスがあることを検知すると、（ルーティングプロトコルが判定した）メトリックがよい方のルートがルーティング テーブルに入力されます。

  メトリックは特定のルートに関連付けられた値で、ルートを最も優先されるものから順にランク付けします。メトリックスの判定に使用されるパラメータは、ルーティングプロトコルによって異なります。メトリックが最も小さいパスは最適パスとして選択され、ルーティングテーブルにインストールされます。同じ宛先への複数のパスのメトリックが等しい場合は、これらの等コスト パスに対してロード バランシングが行われます。

- ASA が、ある宛先へのルーティング プロトコルが複数あることを検知すると、ルートのアドミニストレーティブ ディスタンスが比較され、アドミニストレーティブ ディスタンスが最も小さいルートがルーティング テーブルに入力されます。

ルートのアドミニストレーティブ ディスタンス

ルーティング プロトコルによって検出されるルート、またはルーティング プロトコルに再配布されるルートのアドミニストレーティブ ディスタンスは変更できます。2 つの異なるルーティングプロトコルからの2つのルートのアドミニストレーティブディスタンスが同じ場合、デフォルトのアドミニストレーティブ ディスタンスが小さい方のルートがルーティング テーブルに入力されます。EIGRP ルートと OSPF ルートの場合、EIGRP ルートと OSPF ルートのアドミニストレーティブ ディスタンスが同じであれば、デフォルトで EIGRP ルートが選択されます。

アドミニストレーティブディスタンスは、2つの異なるルーティングプロトコルから同じ宛先に複数の異なるルートがある場合に、ASAが最適なパスの選択に使用するルートパラメータです。ルーティングプロトコルには、他のプロトコルとは異なるアルゴリズムに基づくメトリックがあるため、異なるルーティングプロトコルによって生成された、同じ宛先への2つのルートについて常に最適パスを判定できるわけではありません。

各ルーティング プロトコルには、アドミニストレーティブ ディスタンス値を使用して優先順位が付けられています。次の表に、ASAがサポートするルーティングプロトコルのデフォルトのアドミニストレーティブ ディスタンス値を示します。

表 *23*：サポートされるルーティング プロトコルのデフォルトのアドミニストレーティブ ディスタンス

ルートの送信元	デフォルトのアドミニストレーティブ ディスタンス
接続されているインターフェイス	0
スタティック ルート	1
EIGRP サマリー ルート	5
外部 BGP	20
内部 EIGRP	90
OSPF	110
RIP	120
EIGRP 外部ルート	170
内部およびローカル BGP	200
不明（Unknown）	255

アドミニストレーティブ ディスタンス値が小さいほど、プロトコルの優先順位が高くなります。たとえば、ASAが OSPF ルーティング プロセス（デフォルトのアドミニストレーティブ ディスタンスが 110）と RIP ルーティング プロセス（デフォルトのアドミニストレーティブ ディスタンスが 120）の両方から特定のネットワークへのルートを受信すると、OSPFルーティングプロセスの方が優先度が高いため、ASAはOSPFルートを選択します。この場合、ルータは OSPF バージョンのルートをルーティング テーブルに追加します。

この例では、OSPF 導出ルートの送信元が（電源遮断などで）失われると、ASAは、OSPF 導出ルートが再度現れるまで、RIP 導出ルートを使用します。

アドミニストレーティブ ディスタンスはローカルの設定値です。たとえば、OSPF を通じて取得したルートのアドミニストレーティブディスタンスを変更する場合、その変更は、コマンドが入力された ASA のルーティング テーブルにだけ影響します。アドミニストレーティブ ディスタンスがルーティング アップデートでアドバタイズされることはありません。

アドミニストレーティブ ディスタンスは、ルーティング プロセスに影響を与えません。ルーティング プロセスは、ルーティング プロセスで検出されたか、またはルーティング プロセスに再配布されたルートだけをアドバタイズします。たとえば、RIP ルーティングプロセスは、のルーティングテーブルで OSPF ルーティングプロセスによって検出されたルートが使用されていても、RIP ルートをアドバタイズします。

ダイナミック ルートとフローティング スタティック ルートのバックアップ

ルートを最初にルーティングテーブルにインストールしようとしたとき、他のルートがインストールされてしまい、インストールできなかった場合に、そのルートはバックアップルートとして登録されます。ルーティングテーブルにインストールされたルートに障害が発生すると、ルーティング テーブル メンテナンス プロセスが、登録されたバックアップ ルートを持つ各ルーティングプロトコルプロセスを呼び出し、ルーティングテーブルにルートを再インストールするように要求します。障害が発生したルートに対して、登録されたバックアップルートを持つプロトコルが複数ある場合、アドミニストレーティブディスタンスに基づいて優先順位の高いルートが選択されます。

このプロセスのため、ダイナミック ルーティング プロトコルによって検出されたルートに障害が発生したときにルーティング テーブルにインストールされるフローティング スタティック ルートを作成できます。フローティング スタティック ルートとは、単に、ASAで動作しているダイナミック ルーティング プロトコルよりも大きなアドミニストレーティブ ディスタンスが設定されているスタティック ルートです。ダイナミック ルーティング プロセスで検出された対応するルートに障害が発生すると、このスタティック ルートがルーティング テーブルにインストールされます。

転送の決定方法

転送は次のように決定されます。

- 宛先が、ルーティング テーブル内のエントリと一致しない場合、パケットはデフォルトルートに指定されているインターフェイスを通して転送されます。デフォルトルートが設定されていない場合、パケットは破棄されます。
- 宛先が、ルーティングテーブル内の1つのエントリと一致した場合、パケットはそのルートに関連付けられているインターフェイスを通して転送されます。
- 宛先が、ルーティング テーブル内の複数のエントリと一致する場合、パケットはネットワーク プレフィックス長がより長いルートに関連付けられているインターフェイスから転送されます。

たとえば、192.168.32.1 宛てのパケットが、ルーティング テーブルの次のルートを使用してインターフェイスに到着したとします。

- 192.168.32.0/24 のゲートウェイ 10.1.1.2
- 192.168.32.0/19 のゲートウェイ 10.1.1.3

この場合、192.168.32.1 は 192.168.32.0/24 ネットワークに含まれるため、192.168.32.1 宛てのパケットは 10.1.1.2 宛てに送信されます。このアドレスはまた、ルーティング テーブルの他のルートにも含まれますが、ルーティング テーブル内では 192.168.32.0/24 の方が長いプレフィックスを持ちます（24 ビットと 19 ビット）。パケットを転送する場合、プレフィックスが長い方が常に短いものより優先されます。

（注） ルートの変更が原因で新しい同様の接続が異なる動作を引き起こしたとしても、既存の接続は設定済みのインターフェイスを使用し続けます。

ダイナミック ルーティングと フェールオーバー

アクティブなユニットでルーティング テーブルが変更されると、スタンバイ ユニットでダイナミック ルートが同期されます。これは、アクティブ ユニットのすべての追加、削除、または変更がただちにスタンバイ ユニットに伝播されることを意味します。スタンバイ ユニットがアクティブ/スタンバイの待受中 フェールオーバー ペアでアクティブになると、ルートはフェールオーバー バルク同期および連続複製プロセスの一部として同期されるため、そのユニットには以前のアクティブ ユニットと同じルーティング テーブルがすでに作成されています。

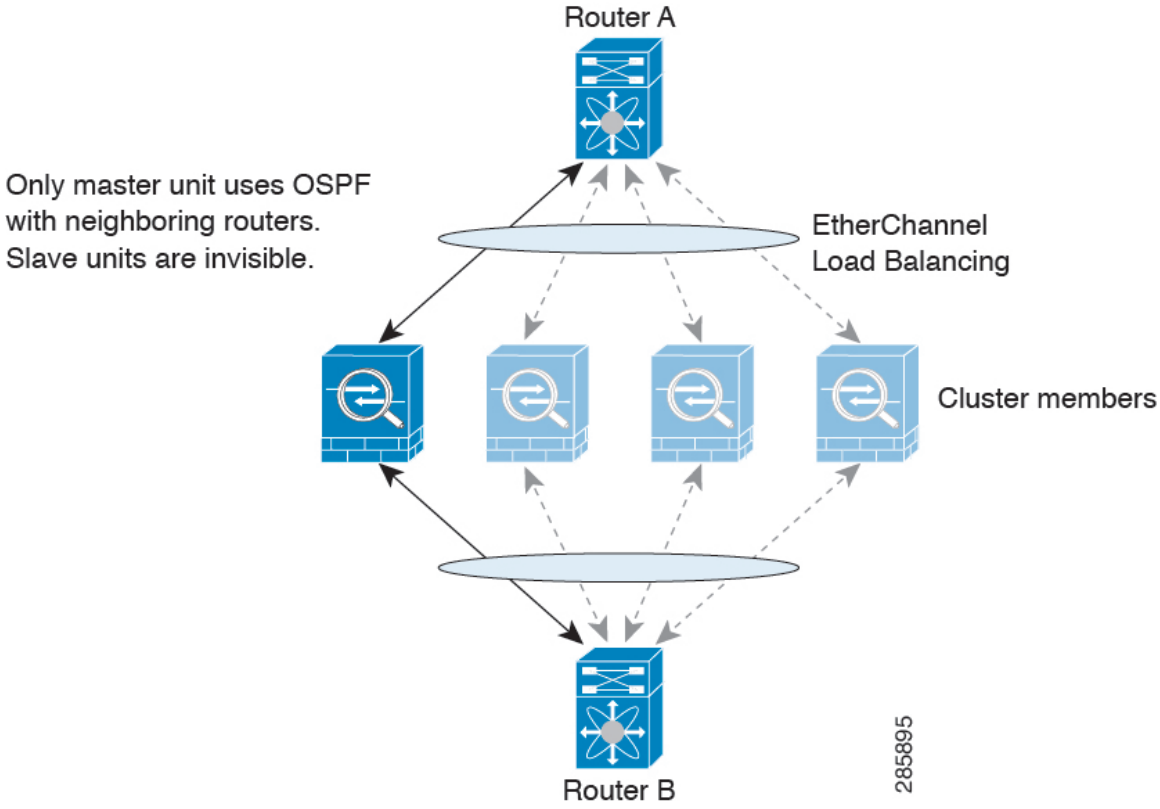
ダイナミック ルーティングおよびクラスタリング

ここでは、クラスタリングでダイナミック ルーティングを使用する方法について説明します。

スパンド EtherChannel モードでのダイナミック ルーティング

スパンド EtherChannel モード：ルーティング プロセスはマスター ユニット上だけで実行されます。ルートはマスターユニットを介して学習され、スレーブに複製されます。ルーティング パケットがスレーブに到着した場合は、マスター ユニットにリダイレクトされます。

図 *52* : スパンド *EtherChannel* モードでのダイナミック ルーティング



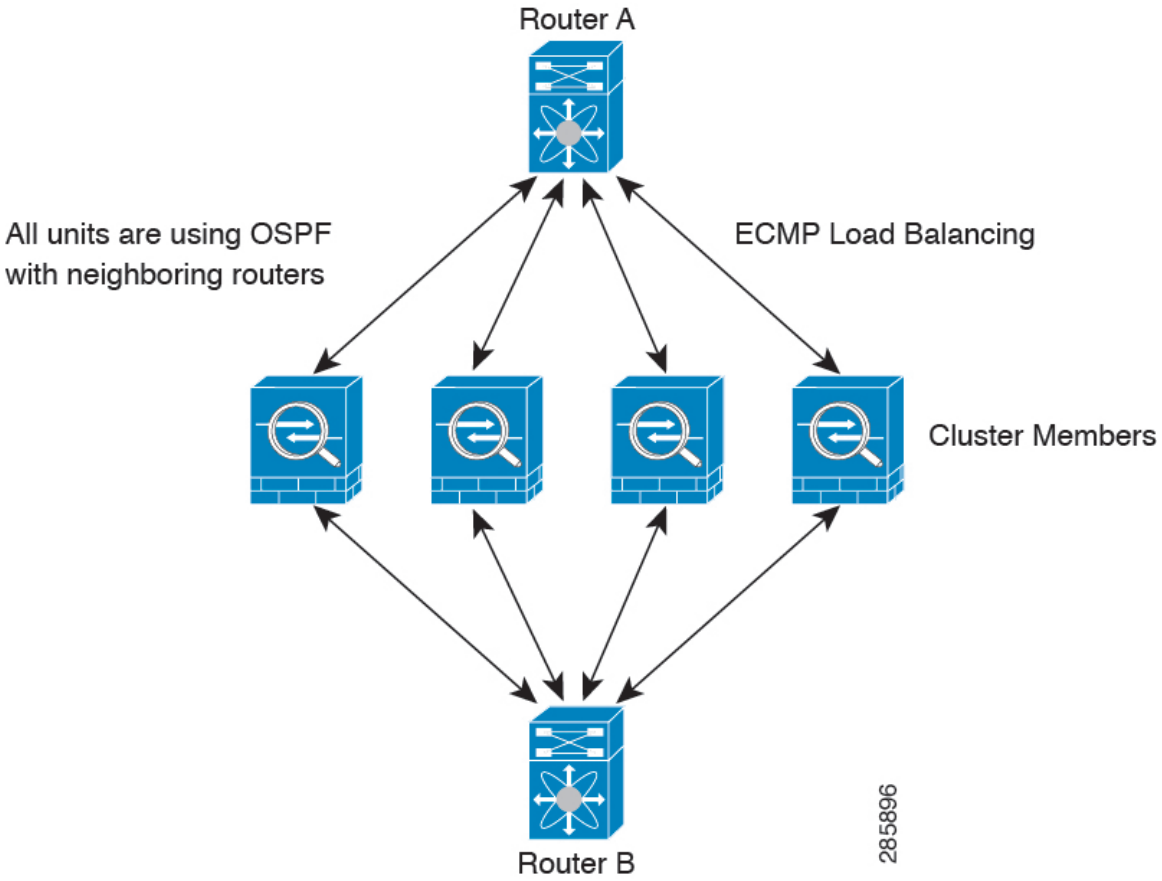
スレーブ メンバがマスター ユニットからルートを学習した後は、各ユニットが個別に転送に関する判断を行います。

OSPF LSA データベースは、マスター ユニットからスレーブ ユニットに同期されません。マスターユニットのスイッチオーバーが発生した場合は、隣接ルータが再起動を検出します。スイッチオーバーは透過的ではありません。OSPF プロセスが IP アドレスの 1 つをルータ ID として選択します必須ではありませんが、スタティック ルータ ID を割り当てることができます。これで、同じルータ ID がクラスタ全体で使用されるようになります。割り込みを解決するには、OSPF ノンストップ フォワーディング機能を参照してください。

個別インターフェイス モードでのダイナミック ルーティング

個別インターフェイス モードでは、各ユニットがスタンドアロン ルータとしてルーティング プロトコルを実行します。ルートの学習は、各ユニットが個別に行います。

図 *53 :* 個別インターフェイス モードでのダイナミック ルーティング



上の図では、ルータ A はルータ B への等コスト パスが 4 本あることを学習します。パスはそれぞれ 1 つの ASA を通過します。ECMP を使用して、4 パス間でトラフィックのロード バランシングを行います。各 ASA は、外部ルータと通信するときに、それぞれ異なるルータ ID を選択します。

管理者は、各ユニットが別のルータ ID を使用できるように、ルータ ID のクラスタ プールを設定する必要があります。

EIGRP は、個別のインターフェイス モードのクラスタ ピアとのネイバー関係を形成しません。

（注） 冗長性の目的で、クラスタに同じルータへの複数の隣接関係がある場合、非対称ルーティングは許容できないトラフィック損失の原因となる可能性があります。非対称ルーティングを避けるためには、同じトラフィック ゾーンにこれらすべての ASA インターフェイスをまとめます。トラフィック ゾーンの設定 （573 ページ）を参照してください。

マルチ コンテキスト モードのダイナミック ルーティング

マルチ コンテキスト モードでは、各コンテキストで個別のルーティング テーブルおよびルーティング プロトコル データベースが維持されます。これにより、各コンテキストの OSPFv2 およびEIGRP を個別に設定することができます。EIGRP をあるコンテキストで設定し、OSPFv2 を同じまたは異なるコンテキストで設定できます。混合コンテキスト モードでは、ルーテッド モードのコンテキストの任意のダイナミック ルーティング プロトコルをイネーブルにできます。RIP および OSPFv3 は、マルチ コンテキスト モードではサポートされていません。

次の表に、EIGRP、OSPFv2、OSPFv2 および EIGRP プロセスへのルートの配布に使用されるルート マップ、およびマルチ コンテキスト モードで使用されている場合にエリアを出入りするルーティング アップデートをフィルタリングするためにOSPFv2 で使用されるプレフィックス リストの属性を示します。

EIGRP	OSPFv2	ルートマップ とプレフィックスのリスト
コンテキストごとに 1 つのインスタンスがサポートされます。	コンテキストごとに 2 つのインスタンスがサポートされます。	該当なし
システム コンテキストでディセーブルになっています。		該当なし
2つのコンテキストが同じまたは異なる自律システム番号を使用できます。	2つのコンテキストが同じまたは異なるエリア ID を使用できます。	該当なし
2つのコンテキストの共有インターフェイスでは、複数の EIGRP のインスタンスを実行できます。	2つのコンテキストの共有インターフェイスでは、複数の OSPF のインスタンスを実行できます。	該当なし
共有インターフェイス間の EIGRP インスタンスの相互作用がサポートされます。	共有インターフェイス間の OSPFv2 インスタンスの相互作用がサポートされます。	該当なし
シングルモードで使用可能なすべてのCLI はマルチ コンテキスト モードでも使用できます。		
各 CLI は使用されているコンテキストでだけ機能します。		

ルートのリソース管理

routes というリソース クラスは、コンテキストに存在できるルーティング テーブル エントリの最大数を指定します。これは、別のコンテキストの使用可能なルーティング テーブル エントリに影響を与える 1 つのコンテキストの問題を解決し、コンテキストあたりの最大ルート エントリのより詳細な制御を提供します。

明確なシステム制限がないため、このリソース制限には絶対値のみを指定できます。割合制限は使用できません。また、コンテキストあたりの上限および下限がないため、デフォルト クラスは変更されません。コンテキストのスタティックまたはダイナミック ルーティング プロトコル（接続、スタティック、OSPF、EIGRP、および RIP）のいずれかに新しいルートを追加し、そのコンテキストのリソース制限を超えた場合、ルートの追加は失敗し、syslog メッセージが生成されます。

等コスト マルチパス（ECMP）ルーティング

ASA は、等コスト マルチパス（ECMP）ルーティングをサポートしています。

インターフェイスごとに最大 8 の等コストのスタティック ルートタまたはダイナミック ルートを設定できます。たとえば、次のように異なるゲートウェイを指定する外部インターフェイスで複数のデフォルト ルートを設定できます。

```
route outside 0 0 10.1.1.2
route outside 0 0 10.1.1.3
route outside 0 0 10.1.1.4
```

この場合、トラフィックは、10.1.1.2、10.1.1.3 と 10.1.1.4 間の外部インターフェイスでロードバランスされます。トラフィックは、送信元 IP アドレスおよび宛先 IP アドレス、着信トラフィック、プロトコル、送信元ポートおよび宛先ポートをハッシュするアルゴリズムに基づいて、指定したゲートウェイ間に分配されます。

ECMP は複数のインターフェイス間ではサポートされないため、異なるインターフェイスで同じ宛先へのルートを定義することはできません。上記のルートのいずれかを設定すると、次のルートは拒否されます。

```
route outside2 0 0 10.2.1.1
```

ゾーンがある場合は、各ゾーン内の最大 8 つのインターフェイス間に最大 8 つの等コストのスタティック ルートまたはダイナミック ルートを設定できます。たとえば、次のようにゾーン内の 3 つのインターフェイ間に複数のデフォルト ルートを設定できます。

```
route outside1 0 0 10.1.1.2
route outside2 0 0 10.2.1.2
route outside3 0 0 10.3.1.2
```

同様に、ダイナミック ルーティング プロトコルは、自動的に等コストルートを設定できます。ASAでは、より堅牢なロード バランシング メカニズムを使用してインターフェイス間でトラフィックをロード バランスします。

ルートが紛失した場合、 デバイスはフローをシームレスに別のルートに移動させます。

プロキシ ARP 要求のディセーブル化

あるホストから同じイーサネット ネットワーク上の別のデバイスに IP トラフィックを送信する場合、そのホストは送信先のデバイスの MAC アドレスを知る必要があります。ARP は、IP アドレスを MAC アドレスに解決するレイヤ 2 プロトコルです。ホストは IP アドレスの所有者

を尋ねる ARP 要求を送信します。その IP アドレスを所有するデバイスは、自分が所有者であることを自分の MAC アドレスで返答します。

プロキシ ARP は、デバイスが ARP 要求に対してその IP アドレスを所有しているかどうかに関係なく自分の MAC アドレスで応答するときに使用されます。NAT を設定し、ASA インターフェイスと同じネットワーク上のマッピング アドレスを指定する場合、ASA でプロキシ ARP が使用されます。トラフィックがホストに到達できる唯一の方法は、ASA でプロキシ ARP が使用されている場合、MAC アドレスが宛先マッピング アドレスに割り当てられていると主張することです。

まれに、NAT アドレスに対してプロキシ ARP をディセーブルにすることが必要になります。

既存のネットワークと重なる VPN クライアント アドレス プールがある場合、ASA はデフォルトで、すべてのインターフェイス上でプロキシ ARP 要求を送信します。同じレイヤ 2 ドメイン上にもう 1 つインターフェイスがあると、そのインターフェイスは ARP 要求を検出し、自分の MAC アドレスで応答します。その結果、内部ホストへの VPN クライアントのリターン トラフィックは、その誤ったインターフェイスに送信され、破棄されます。この場合、プロキシ ARP 要求をそれらが不要なインターフェイスでディセーブルにする必要があります。

手順

プロキシ ARP 要求をディセーブルにします。

sysopt noproxyarp *interface*

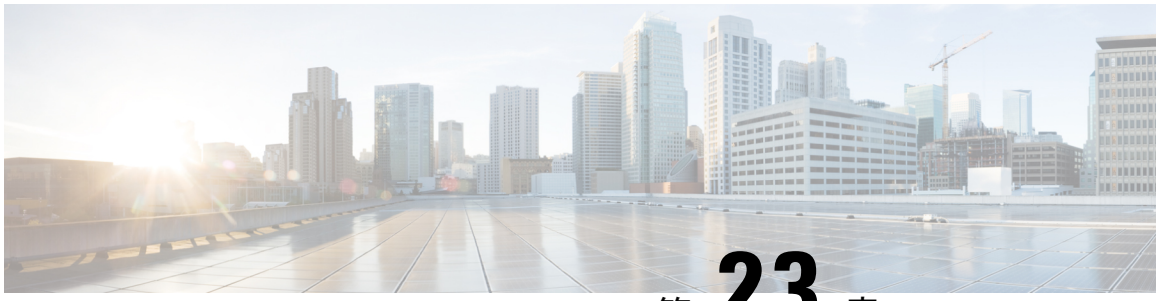
例：

```
ciscoasa(config)# sysopt noproxyarp exampleinterface
```

ルーティング テーブルの表示

show route コマンドを使用してルーティング テーブル内のエントリを表示します。

```
ciscoasa# show route

Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is 10.86.194.1 to network 0.0.0.0

S    10.1.1.0 255.255.255.0 [3/0] via 10.86.194.1, outside
C    10.86.194.0 255.255.254.0 is directly connected, outside
S*   0.0.0.0 0.0.0.0 [1/0] via 10.86.194.1, outside
```



第 23 章

スタティック ルートとデフォルト ルート

この章では、Cisco ASA でスタティック ルートとデフォルト ルートを設定する方法について説明します。

スタティック ルートとデフォルト ルートについて

トラフィックを接続されていないホストやネットワークにルーティングするには、スタティック ルーティングまたはダイナミック ルーティングを使用して、ホストやネットワークへのルートを定義する必要があります。通常は、少なくとも 1 つのスタティック ルート、つまり、他の方法でデフォルトのネットワーク ゲートウェイにルーティングされていない、すべてのトラフィック用のデフォルト ルート（通常、ネクストホップ ルータ）を設定する必要があります。

デフォルト ルート

最も単純なオプションは、すべてのトラフィックをアップストリーム ルータに送信するようにデフォルト スタティック ルートを設定して、トラフィックのルーティングをルータに任せることです。デフォルト ルートは、既知のルートもスタティック ルートも指定されていない IP パケットすべてを、ASA が送信するゲートウェイの IP アドレスを特定するルートです。デフォルト スタティック ルートとは、つまり宛先の IP アドレスとして 0.0.0.0/0（IPv4）または ::/0（IPv6）が指定されたスタティック ルートのことです。

デフォルト ルートを常に定義する必要があります。

スタティック ルート

次の場合は、スタティック ルートを使用します。

- ネットワークがサポート対象外のルータ ディスカバリ プロトコルを使用している。
- ネットワークが小規模でスタティック ルートを容易に管理できる。
- ルーティング プロトコルが関係するトラフィックまたは CPU のオーバーヘッドをなくす必要がある。
- 場合によっては、デフォルト ルートだけでは不十分である。デフォルトのゲートウェイでは宛先ネットワークに到達できない場合があるため、スタティック ルートをさらに詳しく設定する必要があります。たとえば、デフォルトのゲートウェイが外部の場合、デフォルト ルートは、ASA に直接接続されていない内部ネットワークにはまったくトラフィックを転送できません。
- ダイナミック ルーティング プロトコルをサポートしていない機能を使用している。

不要なトラフィックを「ブラックホール化」するためのnull0インターフェイスへのルート

アクセス ルールを使用すると、ヘッダーに含まれている情報に基づいてパケットをフィルタ処理することができます。null0 インターフェイスへのスタティック ルートは、アクセス ルールを補完するソリューションです。null0 ルートを使用して、不要なトラフィックや望ましくないトラフィックを「ブラック ホール」に転送できるため、トラフィックがドロップされます。

スタティック null0 ルートには、望ましいパフォーマンス プロファイルがあります。また、スタティック null0 ルートを使用して、ルーティング ループ回避することもできます。BGP では、リモート トリガ型ブラック ホール ルーティングのためにスタティック null0 ルートを活用できます。

ルートのプライオリティ

- 特定の宛先が特定されたルートはデフォルト ルートより優先されます。
- 宛先が同じルートが複数存在する場合（スタティックまたはダイナミック）、ルートのアドミニストレーティブ ディスタンスによってプライオリティが決まります。スタティック ルートは 1 に設定されるため、通常、それらが最もプライオリティの高いルートです。
- 宛先かつアドミニストレーティブ ディスタンスが同じスタティック ルートが複数存在する場合は、等コスト マルチパス（ECMP）ルーティング （704 ページ）を参照してください。
- [トンネル化（Tunneled）] オプションを使用してトンネルから出力されるトラフィックの場合、このルートが他の設定済みルートまたは学習されたデフォルト ルートをすべてオーバーライドします。

トランスペアレント ファイアウォール モード ルート

ブリッジ グループ メンバー インターフェイスを通じて直接には接続されていないネットワークに向かう ASA で発信されるトラフィックの場合、ASA がどのブリッジ グループ メンバー インターフェイスからトラフィックを送信するかを認識するように、デフォルト ルートまたはスタティック ルートを設定する必要があります。ASA で発信されるトラフィックは、syslog サーバまたはSNMP サーバへの通信も含むことがあります。1 つのデフォルト ルートで到達できないサーバがある場合、スタティック ルートを設定する必要があります。トランスペアレント モードの場合、ゲートウェイ インターフェイスに BVI を指定できません。メンバー インターフェイスのみが使用できます。詳細については、「MAC アドレスとルート ルックアップ（179 ページ）」を参照してください。

スタティック ルート トラッキング

スタティック ルートの問題の 1 つは、ルートがアップ状態なのかダウン状態なのかを判定する固有のメカニズムがないことです。スタティック ルートは、ネクスト ホップ ゲートウェイが使用できなくなった場合でも、ルーティング テーブルに保持されています。スタティック ルートは、ASA 上の関連付けられたインターフェイスがダウンした場合に限りルーティング テーブルから削除されます。

スタティック ルート トラッキング機能には、スタティック ルートの使用可能状況を追跡し、プライマリ ルートがダウンした場合のバックアップ ルートをインストールするための方式が用意されています。たとえば、ISP ゲートウェイへのデフォルト ルートを定義し、かつ、プライマリ ISP が使用できなくなった場合に備えて、セカンダリ ISP へのバックアップ デフォルト ルートを定義できます。

ASA では、ASA が ICMP エコー要求を使用してモニタする宛先ネットワーク上でモニタリング対象スタティック ルートを関連付けることでスタティック ルート トラッキングを実装します。指定された時間内にエコー応答がない場合は、そのホストはダウンしていると見なされ、関連付けられたルートはルーティング テーブルから削除されます。削除されたルートに代わって、メトリックが高い追跡対象外のバックアップ ルートが使用されます。

モニタリング対象の選択時には、その対象が ICMP エコー要求に応答できることを確認してください。対象には任意のネットワーク オブジェクトを選択できますが、次のものを使用することを検討する必要があります。

- ISP ゲートウェイ アドレス（デュアル ISP サポート用）
- ネクストホップ ゲートウェイ アドレス（ゲートウェイの使用可能状況に懸念がある場合）
- ASA が通信を行う必要のある対象ネットワーク上のサーバ（syslog サーバなど）
- 宛先ネットワーク上の永続的なネットワーク オブジェクト

（注） 夜間にシャットダウンする PC は適しません。

スタティック ルート トラッキングは、スタティックに定義されたルートや、DHCP または PPPoE を通じて取得したデフォルト ルートに対して設定することができます。設定済みのルート トラッキングでは、複数のインターフェイス上の PPPoE クライアントだけをイネーブルにすることができます。

スタティック ルートとデフォルト ルートのガイドライン

ファイアウォール モードとブリッジグループ

- トランスペアレント モードでは、スタティック ルートをブリッジグループ メンバー インターフェイスをゲートウェイとして使用する必要があります。BVI を指定することはできません。
- スタティック ルート トラッキングは、ブリッジグループ メンバー インターフェイス

IPv6

- IPv6 では、スタティック ルート トラッキングはサポートされません。

クラスタ

クラスタリングでは、スタティック ルート モニタリングはプライマリ ユニットでのみサポートされます。

デフォルト ルートおよびスタティック ルートの設定

少なくとも 1 つのデフォルト ルートを設定する必要があります。また、スタティック ルートの設定が必要になる場合があります。このセクションでは、デフォルト ルートの設定、スタティック ルートの設定、スタティック ルートの追跡を行います。

デフォルト ルートの設定

デフォルト ルートは、宛先 IP アドレスが 0.0.0.0/0 のスタティック ルートです。この手順に従って手動で設定するか、DHCP サーバや他のルーティング プロトコルから取得するかに関わらず、デフォルト ルートは必ず設定する必要があります。

始める前に

[Tunneled] オプションについては、次のガイドラインを参照してください。

- トンネル ルートの出力インターフェイスで、ユニキャスト RPF（**ip verify reverse-path** コマンド）を有効にしないでください。この設定を行うと、セッションでエラーが発生します。

- トンネル ルートの出力インターフェイスで、TCP 代行受信をイネーブルにしないでください。この設定を行うと、セッションでエラーが発生します。
- これらのインスペクション エンジンはトンネル ルートを無視するため、トンネル ルートで VoIP インスペクション エンジン（CTIQBE、H.323、GTP、MGCP、RTSP、SIP、SKINNY）、DNS インスペクション エンジン、または DCE RPC インスペクション エンジンを使用しないでください。
- tunneled オプションで複数のデフォルト ルートを定義することはできません。
- トンネル トラフィックの ECMP はサポートされません。

手順

デフォルト ルートを追加します。

IPv4：

route*if_name* **0.0.0.0 0.0.0.0** *gateway_ip* [**distance**] [**tunneled**]

IPv6：

ipv6 route *if_name* **::/0** *gateway_ip* [**distance**] [**tunneled**]

例：

```
ciscoasa(config)# route outside 0.0.0.0 0.0.0.0 192.168.2.4
ciscoasa(config)# route inside 0.0.0.0 0.0.0.0 10.1.2.3 tunneled
ciscoasa(config)# ipv6 route inside ::/0 3FFE:1100:0:CC00::1
```

if_name は、特定のトラフィックの送信を行うインターフェイスです。トランスペアレント モードの場合は、ブリッジ グループのメンバー インターフェイスの名前を指定します。

distance 引数は、ルートのアドミニストレーティブ ディスタンス（1 ～ 254）です。値を指定しない場合、デフォルトは **1** です。アドミニストレーティブ ディスタンスは、複数のルーティング プロトコル間でルートを比較するのに使用されるパラメータです。スタティック ルートのデフォルトのアドミニストレーティブ ディスタンスは 1 で、ダイナミック ルーティング プロトコルで検出されるルートより優先されますが、直接には接続されていないルートです。OSPF で検出されるルートのデフォルトのアドミニストレーティブ ディスタンスは 110 です。スタティック ルートとダイナミック ルートのアドミニストレーティブ ディスタンスが同じ場合、スタティック ルートが優先されます。接続されているルートは常に、スタティック ルートおよびダイナミックに検出されたルートのどちらよりも優先されます。

（注） 異なるメトリックを持つ個別のインターフェイス上で 2 つのデフォルト ルートが設定されている場合は、大きい方のメトリックを持つインターフェイスから ASA への接続の確立には失敗しますが、小さい方のメトリックを持つインターフェイスから ASA への接続は予期したとおりに成功します。

VPN トラフィックに非 VPN トラフィックとは別のデフォルト ルートを使用する必要がある場合は、**tunneled** キーワードを使用して VPN トラフィック用の別個のデフォルト ルートを定義

できます。その場合、たとえば VPN 接続からの着信トラフィックは内部ネットワークに転送する一方、内部ネットワークからのトラフィックは外部に転送するといった設定を簡単に行うことができます。tunneled オプションを使用してデフォルト ルートを作成すると、ASA に着信するトンネルからのすべてのトラフィックは、学習したルートまたはスタティック ルートを使用してルーティングできない場合、このルートに送信されます。

ヒント　宛先ネットワーク アドレスおよびマスクとして、**0.0.0.0 0.0.0.0** の代わりに **0 0** と入力できます。たとえば、**routeoutside 0 0 192.168.2.4** のように入力します。

スタティック ルートの設定

スタティック ルートは、特定の宛先ネットワークのトラフィックの送信先を定義します。

手順

スタティック ルートを追加します。

IPv4：

route *if_name dest_ip mask gateway_ip* [**distance**]

IPv6：

ipv6 route *if_name dest_ipv6_prefix*/*prefix_length gateway_ip* [**distance**]

例：

```
ciscoasa(config)# route outside 10.10.10.0 255.255.255.0 192.168.1.1
ciscoasa(config)# ipv6 route outside 2001:DB8:1::0/32 2001:DB8:0:CC00::1
```

if_name は、特定のトラフィックの送信を行うインターフェイスです。不要なトラフィックを「ブラック ホール化」するには、**null0** インターフェイスを入力します。トランスペアレント モードの場合は、ブリッジ グループのメンバー インターフェイスの名前を指定します。

dest_ip 引数と *mask* または *dest_ipv6_prefix*/*prefix_length* 引数は宛先ネットワークの IP アドレスであり、*gateway_ip* 引数はネクスト ホップ ルータのアドレスです。スタティック ルートに指定するアドレスは、ASA に到達して NAT を実行する前のパケットにあるアドレスです。

distance 引数は、ルートのアドミニストレーティブ ディスタンスです。値を指定しない場合、デフォルトは **1** です。アドミニストレーティブ ディスタンスは、複数のルーティング プロトコル間でルートを比較するのに使用されるパラメータです。スタティック ルートのデフォルトのアドミニストレーティブ ディスタンスは 1 で、ダイナミック ルーティング プロトコルで検出されるルートより優先されますが、直接には接続されていないルートです。OSPF で検出されるルートのデフォルトのアドミニストレーティブ ディスタンスは 110 です。スタティック ルートとダイナミック ルートのアドミニストレーティブ ディスタンスが同じ場合、スタティッ

ク ルートが優先されます。接続されているルートは常に、スタティック ルートおよびダイナミックに検出されたルートのどちらよりも優先されます。

例

次に、同じゲートウェイに移動する 3 つのネットワークと、別のゲートウェイに移動するもう 1 つのネットワークの例を示します。

```
route outside 10.10.10.0 255.255.255.0 192.168.1.1
route outside 10.10.20.0 255.255.255.0 192.168.1.1
route outside 10.10.30.0 255.255.255.0 192.168.1.1
route inside 10.10.40.0 255.255.255.0 10.1.1.1
```

スタティック ルート トラッキングの設定

スタティック ルート トラッキングを設定するには、次の手順を実行します。

手順

ステップ 1 モニタリング プロセスを次のように定義します。

sla monitor sla_id

例：

```
ciscoasa(config)# sla monitor 5
ciscoasa(config-sla-monitor)#
```

ステップ 2 モニタリング プロトコル、追跡対象ネットワークのターゲット ホスト、ネットワークに到達するときに経由するネットワークを指定します。

type echo protocol ipicmpechotarget_ip **interface** if_name

例：

```
ciscoasa(config-sla-monitor)# type echo protocol ipicmpecho 172.29.139.134
ciscoasa(config-sla-monitor-echo)#
```

target_ip 引数は、トラッキング プロセスによって使用可能かどうかをモニタされるネットワーク オブジェクトの IP アドレスです。このオブジェクトが使用可能な場合、トラッキング プロセス ルートがルーティング テーブルにインストールされます。このオブジェクトが使用できない場合、トラッキング プロセスがルートを削除し、代わりにバックアップ ルートが使用されます。

ステップ 3 （オプション）モニタリング オプションを設定します。**frequency**、**num-packets**、**request-data-size**、**threshold**、**timeout**、**tos** の各コマンドについては、コマンド リファレンスを参照してください。

ステップ 4 モニタリング プロセスのスケジュールを設定します。

sla monitor schedule sla_id [**life** {**forever** | seconds}] [**start-time** {hh:mm [:ss] [month day | day month] | **pending** | **now** | **after** hh:mm:ss}] [**ageout** seconds] [**recurring**]

例：

```
ciscoasa(config)# sla monitor schedule 5 life forever start-time now
```

通常、モニタリング スケジュールには **sla monitor schedule** *sla_id* **life forever start-time now** コマンドを使用し、モニタリング コンフィギュレーションでテスト頻度を決定できるようにします。

ただし、このモニタリング プロセスを将来開始するようにしたり、指定した時刻だけに実行されるようにスケジュールを設定したりできます。

ステップ 5 追跡するスタティック ルートを SLA モニタリング プロセスに関連付けます。

track track_id **rtr** sla_id **reachability**

例：

```
ciscoasa(config)# track 6 rtr 5 reachability
```

track_id 引数は、このコマンドで割り当てるトラッキング番号です。*sla_id* 引数は SLA プロセスの ID 番号です。

ステップ 6 次のルート タイプのいずれかを追跡します。

- スタティック ルート：

  route if_name dest_ip mask gateway_ip [distance] **track** track_id

  例：

  ```
  ciscoasa(config)# route outside 10.10.10.0 255.255.255.0 192.168.1.1 track 6
  ```

  tunneled オプションは使用できません。

- DHCP から取得したデフォルト ルート：

  ```
  interface interface_id
    dhcp client route track track_id
    ip address dhcp setroute
  ```

- PPPoE から取得したデフォルト ルート：

  ```
  interface interface_id
    pppoe client route track track_id
  ```

```
ip address pppoe setroute
```

ステップ 7 追跡対象外のバックアップ ルートを作成します。

バックアップ ルートは、追跡されたルートと同じ宛先へのスタティック ルートですが、異なるインターフェイスまたはゲートウェイを経由します。このルートは、追跡されたルートより長いアドミニストレーティブ ディスタンス（メトリック）に割り当てる必要があります。

スタティックルートまたはデフォルトルートのモニタリング

- **show route**

  ルーティング テーブルを表示します。

スタティック ルートまたはデフォルト ルートの例

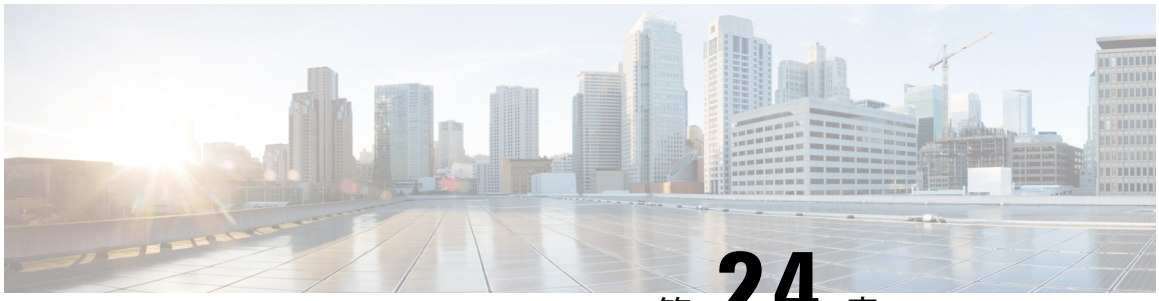
次の例は、スタティック ルートの作成方法を示します。スタティック ルートは、宛先が 10.1.1.0/24 のトラフィックすべてを内部インターフェイスに接続されているルータ（10.1.2.45）に送信します。また、dmz インターフェイスで 3 つの異なるゲートウェイにトラフィックを誘導する 3 つの等コスト スタティック ルートを定義し、トンネル トラフィックのデフォルト ルートと通常のトラフィックのデフォルト ルートを追加します。

```
route inside 10.1.1.0 255.255.255.0 10.1.2.45
route dmz 10.10.10.0 255.255.255.0 192.168.2.1
route dmz 10.10.10.0 255.255.255.0 192.168.2.2
route dmz 10.10.10.0 255.255.255.0 192.168.2.3
route outside 0 0 209.165.201.1
route inside 0 0 10.1.2.45 tunneled
```

スタティック ルートおよびデフォルト ルートの履歴

表 *24*：スタティック ルートおよびデフォルト ルートの機能履歴

機能名	プラットフォーム リリース	機能情報
スタティック ルート トラッキング	7.2(1)	スタティック ルート トラッキング機能には、スタティック ルートの使用可能状況を追跡し、プライマリ ルートがダウンした場合のバックアップ ルートをインストールするための方式が用意されています。 **clear configure sla**、**frequency, num-packets**、**request-data-size**、**show sla monitor**、**show running-config sla**、**sla monitor**、**sla monitor schedule, threshold**、**timeout**、**tos**、**track rtr** の各コマンドが導入されました。
トラフィックを「ブラック ホール化」するためのスタティック null0 ルート	9.2(1)	トラフィックを null0 インターフェイスへ送信すると、指定したネットワーク宛のパケットはドロップします。この機能は、BGP の Remotely Triggered Black Hole (RTBH) の設定に役立ちます。 **route** コマンドが変更されました。



第 24 章

Policy Based Routing：ポリシー ベース ルーティング

この章では、ポリシーベース ルーティング（PBR）をサポートするように Cisco ASA を設定する方法について説明します。この項では、ポリシーベース ルーティング、PBR のガイドライン PBR の設定について説明します。

ポリシーベース ルーティングについて

従来のルーティングは宛先ベースであり、パケットは宛先 IP アドレスに基づいてルーティングされます。ただし、宛先ベースのルーティング システムでは特定トラフィックのルーティングを変更することが困難です。ポリシーベース ルーティング（PBR）では、宛先ネットワークではなく条件に基づいてルーティングを定義できます。PBR では、送信元アドレス、送信元ポート、宛先アドレス、宛先ポート、プロトコル、またはこれらの組み合わせに基づいてトラフィックをルーティングできます。

ポリシーベース ルーティング：

- 区別したトラフィックに Quality of Service（QoS）を提供できます。
- 低帯域幅、低コストの永続パスと、高帯域幅、高コストのスイッチドパスに、インタラクティブ トラフィックとバッチ トラフィックを分散できます。
- インターネット サービス プロバイダーやその他の組織が、さまざまなユーザ セットから発信されるトラフィックを、適切に定義されたインターネット接続を経由してルーティングできます。

ポリシーベース ルーティングには、ネットワーク エッジでトラフィックを分類およびマークし、ネットワーク全体で PBR を使用してマークしたトラフィックを特定のパスに沿ってルー

ティングすることで、QoS を実装する機能があります。これにより、宛先が同じ場合でも、異なる送信元から送信されるパケットを別のネットワークにルーティングすることができます。これは、複数のプライベート ネットワークを相互接続する場合に役立ちます。

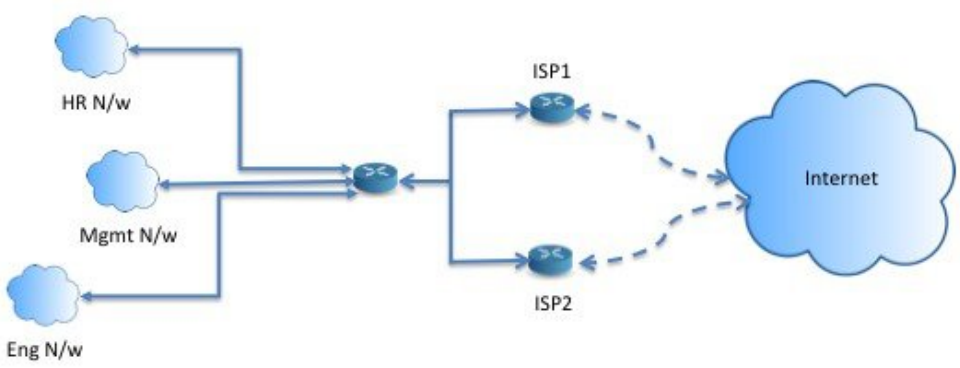
ポリシーベース ルーティングを使用する理由

ロケーション間に 2 つのリンクが導入されている企業を例に説明します。1 つのリンクは高帯域幅、低遅延、高コストのリンクであり、もう 1 つのリンクは低帯域幅、高遅延、低コストのリンクです。従来のルーティング プロトコルを使用する場合、高帯域幅リンクで、リンクの（EIGRP または OSPF を使用した）帯域幅/遅延の特性により実現するメトリックの節約に基づいて、ほぼすべてのトラフィックが送信されます。PBR では、優先度の高いトラフィックを高帯域幅/低遅延リンク経由でルーティングし、その他のすべてのトラフィックを低帯域幅/高遅延リンクで送信します。

ポリシーベース ルーティングの用途のいくつかを以下に示します。

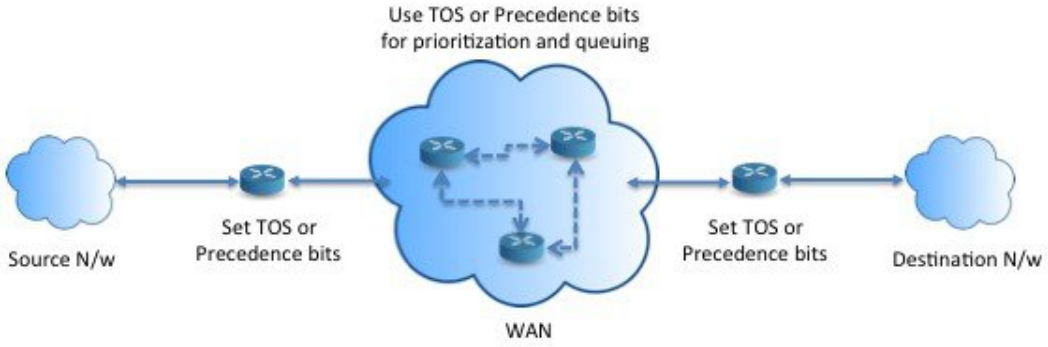
同等アクセスおよび送信元依存ルーティング

このトポロジでは、HR ネットワークと管理ネットワークからのトラフィックは ISP1 を経由するように設定し、エンジニアリング ネットワークからのトラフィックは ISP2 を経由するように設定できます。したがって、ここに示すように、ネットワーク管理者は、ポリシーベース ルーティングを使用して同等アクセスおよび送信元依存ルーティングを実現できます。



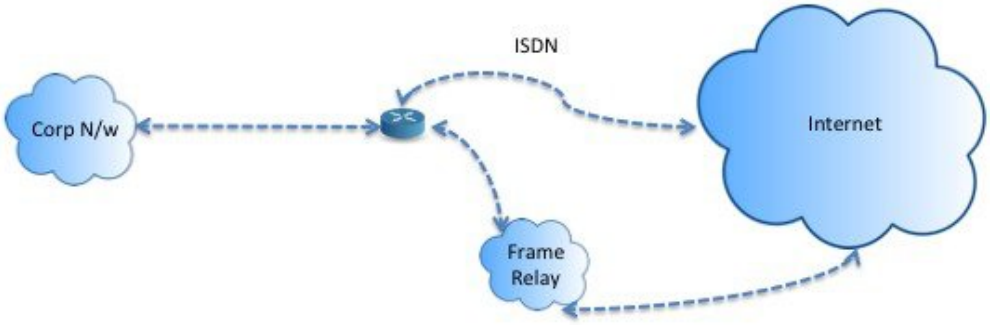
QoS

ネットワーク管理者は、ポリシーベース ルーティングでパケットにタグを付けることにより、ネットワーク トラフィックをネットワーク境界でさまざまなサービス クラスのために分類し、プライオリティ、カスタム、または重み付け均等化のキューイングを使用してそれらのサービス クラスをネットワークのコアに実装できます（下の図を参照）。この設定では、バックボーン ネットワークのコアの各 WAN インターフェイスでトラフィックを明示的に分類する必要がなくなるため、ネットワーク パフォーマンスが向上します。



コスト節約

組織は、特定のアクティビティに関連付けられている一括トラフィックを転送して、帯域幅が高い高コストリンクの使用を短時間にし、さらにここに示すようにトポロジを定義することで帯域幅が低い低コスト リンク上の基本的な接続を継続できます。



ロード シェアリング

ECMP ロード バランシングによって提供されるダイナミックなロード シェアリング機能に加え、ネットワーク管理者は、トラフィックの特性に基づいて複数のパス間にトラフィックを分散するためのポリシーを実装できます。

たとえば、同等アクセスおよび送信元依存ルーティングのシナリオに示すトポロジでは、管理者は、ISP1 を経由する HR netto からのトラフィックと ISP2 を経由するエンジニアリング ネットワークからのトラフィックをロード シェアするようにポリシーベース ルーティングを設定できます。

PBR の実装

ASA は、ACL を使用してトラフィックを照合してから、トラフィックのルーティング アクションを実行します。具体的には、照合のために ACL を指定するルート マップを設定し、次にそのトラフィックに対して 1 つ以上のアクションを指定します。最後に、すべての着信トラフィックに PBR を適用するインターフェイスにルート マップを関連付けます。

ポリシーベース ルーティングのガイドライン

ファイアウォール モード

ルーテッド ファイアウォール モードでだけサポートされています。トランスペアレント ファイアウォール モードはサポートされません。

フロー別のルーティング

ASA はフロー別にルーティングを実行するため、ポリシー ルーティングは最初のパケットに適用され、その結果決定したルーティングが、そのパケットに対して作成されたフローに格納されます。同一接続に属する後続のパケットはすべてこのフローと照合され、適切にルーティングされます。

出力ルート ルックアップに適用されない PBR ポリシー

ポリシーベース ルーティングは入力専用機能です。つまり、この機能は新しい着信接続の最初のパケットだけに適用され、この時点で接続のフォワード レグの出力インターフェイスが選択されます。着信パケットが既存の接続に属している場合、または NAT が適用されない場合には、PBR がトリガーされないことに注意してください。

クラスタ

- クラスタリングがサポートされています。
- クラスタのシナリオでは、スタティック ルートまたはダイナミック ルートがない場合、ip-verify-reverse パスを有効にした非対称トラフィックはドロップされる可能性があります。したがって、ip-verify-reverse パスを無効にすることが推奨されます。

その他のガイドライン

ルート マップ関連の既存のすべての設定の制限事項が引き続き適用されます。

ポリシーベース ルーティングの設定

ルート マップは、1 つ以上のルート マップ文で構成されます。文ごとに、シーケンス番号と permit 句または deny 句が付加されます。各ルート マップ文には、match コマンドと set コマンドが含まれています。match コマンドは、パケット データに適用される一致基準を示します。set コマンドは、パケットに対して実行されるアクションを示します。

- 複数のネクストホップまたはインターフェイスを set アクションとして設定すると、使用できる有効なオプションが見つかるまですべてのオプションが順に評価されます。設定された複数のオプション間のロード バランシングは実行されません。
- verify-availability オプションは、マルチ コンテキスト モードではサポートされません。

手順

ステップ 1 スタンドアロンまたは拡張アクセス リストを定義します。

access-list *name* **standard** {**permit** | **deny**} {**any4** | **host** *ip_address* | *ip_address mask*}

access-list *name* **extended** {**permit** | **deny**} *protocol source_and_destination_arguments*

例：

```
ciscoasa(config)# access-list testacl extended permit ip
10.1.1.0 255.255.255.0 10.2.2.0 255.255.255.0
```

標準 ACL を使用する場合、照合は宛先アドレスに対してのみ行われます。拡張 ACL を使用する場合、送信元、宛先、またはその両方に対して照合を行えます。

IPv6 ACL はサポートされません。

ステップ 2 ルート マップ エントリを作成します。

route-map *name* {**permit** | **deny**} [*sequence_number*]

例：

```
ciscoasa(config)# route-map testmap permit 12
```

ルート マップのエントリは順番に読み取られます。この順序は、*sequence_number* 引数を使用して指定できます。この引数で指定しなければ、ルートマップエントリを追加した順序が ASA で使用されます。

ACL には、固有の permit および deny 文も含まれます。ルート マップと ACL が permit/permit で一致する場合、ポリシーベース ルーティング処理が続行されます。permit/deny で一致する場合、このルート マップでの処理が終了し、別のルート マップがチェックされます。それでも結果が permit/deny であれば、通常のルーティング テーブルが使用されます。deny/deny で一致する場合、ポリシーベース ルーティング処理が続行されます。

（注） permit または deny アクションとシーケンス番号なしでルートマップを設定した場合、このマップはデフォルトでアクションが permit で、シーケンス番号が 10 であると見なされます。

ステップ 3 アクセス リストを使用して適用される一致基準を定義します。

match ip address *access-list_name* [*access-list_name...*]

例：

```
ciscoasa(config-route-map)# match ip address testacl
```

ステップ 4 1 つ以上の set アクションを設定します。

- ネクストホップ アドレスを設定します。

set ip next-hop *ip_address*

複数のネクストホップ IP アドレスを設定できます。その場合、ルーティングできる有効なネクスト ホップ IP アドレスが見つかるまで、それらのアドレスが指定された順で評価されます。設定済みのネクストホップは、直接接続する必要があります。そうでなければ、set アクションが適用されません。

- デフォルトのネクストホップ アドレスを設定します。

  set ip default next-hop *ip_address*

  一致するトラフィックに対する通常のルート ルックアップが失敗すると、ASA はここで指定されたネクスト ホップ IP アドレスを使用してトラフィックを転送します。

- 再帰ネクスト ホップ IPv4 アドレスを設定します。

  set ip next-hop recursive *ip_address*

  set ip next-hop と **set ip default next-hop** はどちらも、ネクストホップが直接接続されたサブネット上に存在している必要があります。**set ip next-hop recursive** では、ネクストホップ アドレスが直接接続されている必要はありません。代わりにネクストホップ アドレスで再帰ルックアップが実行され、一致するトラフィックは、ルータで使用されているルーティング パスに従って、そのルート エントリで使用されているネクストホップに転送されます。

- ルート マップの次の IPv4 ホップが使用できるかどうかを確認します。

  set ip next-hop verify-availability *next-hop-address sequence_number* **track** *object*

  ネクスト ホップの到達可能性を確認するには、SLA モニタ追跡オブジェクトを設定できます。複数のネクストホップの可用性を確認するために、複数の **set ip next-hop verify-availability** コマンドを異なるシーケンス番号と異なるトラッキング オブジェクトで設定できます。

- パケットの出力インターフェイスを設定します。

  set interface *interface_name*

  または

  set interface null0

  このコマンドにより、一致するトラフィックを転送するために使用するインターフェイスが設定されます。複数のインターフェイスを設定できます。その場合、有効なインターフェイスが見つかるまで、それらのインターフェイスが指定された順で評価されます。**null0** を指定すると、ルートマップと一致するすべてのトラフィックがドロップされます。指定されたインターフェイス（静的または動的のいずれか）経由でルーティングできる宛先のルートが存在している必要があります。

- デフォルトのインターフェイスを null0 に設定します。

  set default interface null0

  通常のルート ルックアップが失敗すると、ASA はトラフィックを null0 に転送し、トラフィックがドロップされます。

- IP ヘッダーに Don't Fragment（DF）ビット値を設定します。

  set ip df {0|1}

- パケットに Differentiated Services Code Point（DSCP）または IP プレシデンスの値を設定することによって、IP トラフィックを分類します。

  set ip dscp *new_dscp*

（注） 複数の set アクションが設定されている場合、ASA は、これらを次の順序で評価します。 **set ip next-hop verify-availability; set ip next-hop**; **set ip next-hop recursive**; **set interface;set ip default next-hop**; **set default interface**

ステップ 5 インターフェイスを設定して、インターフェイス コンフィギュレーション モードを開始します。

interface *interface_id*

例：

```
ciscoasa(config)# interface GigabitEthernet0/0
```

ステップ 6 ポリシーベース ルーティングを through-the-box トラフィック用に設定します。

policy-route route-map *route-map_name*

例：

```
ciscoasa(config-if)# policy-route route-map testmap
```

既存のポリシーベース ルーティング マップを削除するには、単にこのコマンドの **no** 形式を入力します。

例：

```
ciscoasa(config-if)# no policy-route route-map testmap
```

ポリシーベース ルーティングの例

以下のセクションでは、ルートマップの設定、ポリシーベース ルーティング（PBR）の例と、PBR の具体的な動作例を示します。

ルート マップ コンフィギュレーションの例

次の例では、アクションとシーケンスが指定されないため、暗黙的に permit のアクションと 10 のシーケンス番号が想定されます。

```
ciscoasa(config)# route-map testmap
```

次の例では、match 基準が指定されないため、暗黙的に match は「any」と見なされます。

```
ciscoasa(config)# route-map testmap permit 10
ciscoasa(config-route-map)# set ip next-hop 1.1.1.10
```

この例では、<acl> と一致するすべてのトラフィックが、ポリシー ルーティングされ、外部インターフェイス経由で転送されます。

```
ciscoasa(config)# route-map testmap permit 10
ciscoasa(config-route-map)# match ip address <acl>
ciscoasa(config-route-map)# set interface outside
```

次の例では、インターフェイスまたはネクストホップのアクションが設定されていないため、<acl>に一致するすべてのトラフィックのdfbitおよびdscpフィールドがコンフィギュレーションに従って変更され、通常のルーティングを使用して転送されます。

```
ciscoasa(config)# route-map testmap permit 10
ciscoasa(config-route-map)# match ip address <acl>
set ip df 1
set ip precedence af11
```

次の例では、<acl_1> に一致するすべてのトラフィックがネクストホップ 1.1.1.10 を使用して転送され、<acl_2> に一致するすべてのトラフィックがネクストホップ 2.1.1.10 を使用して転送され、残りのトラフィックはドロップされます。「match」基準がない場合、暗黙的にmatchは「any」と見なされます。

```
ciscoasa(config)# route-map testmap permit 10
ciscoasa(config-route-map)# match ip address <acl_1>
ciscoasa(config-route-map)# set ip next-hop 1.1.1.10

ciscoasa(config)# route-map testmap permit 20
ciscoasa(config-route-map)# match ip address <acl_2>

ciscoasa(config-route-map)# set ip next-hop 2.1.1.10
ciscoasa(config)# route-map testmap permit 30
ciscoasa(config-route-map)# set interface Null0
```

次の例では、ルートマップの評価は、（i）route-mapアクションpermitとaclアクションpermitが set アクションを適用する、（ii）route-map アクション deny と acl アクション permit が通常のルート ルックアップにスキップする、（iii）permit/deny の route-map アクションと acl アクション deny が次の route-map エントリを続行するといったものになります。次の route-map エントリを使用できない場合は、通常のルート ルックアップにフォールバックします。

```
ciscoasa(config)# route-map testmap permit 10
ciscoasa(config-route-map)# match ip address permit_acl_1 deny_acl_2
ciscoasa(config-route-map)# set ip next-hop 1.1.1.10

ciscoasa(config)# route-map testmap deny 20
```

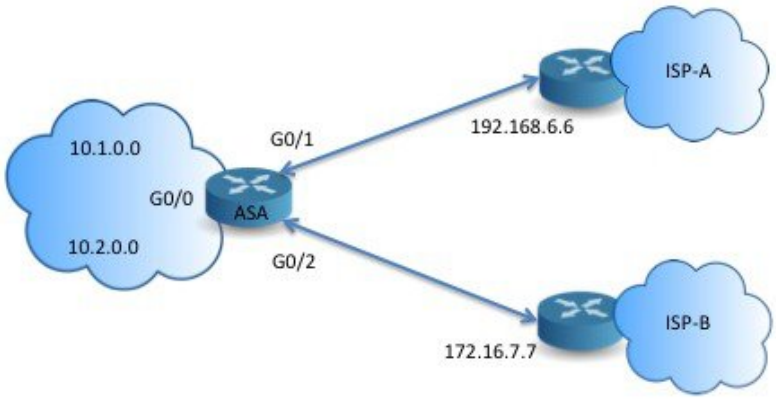
```
ciscoasa(config-route-map)# match ip address permit_acl_3 deny_acl_4
ciscoasa(config-route-map)# set ip next-hop 2.1.1.10

ciscoasa(config)# route-map testmap permit 30
ciscoasa(config-route-map)# match ip address deny_acl_5
ciscoasa(config-route-map)# set interface outside
```

次の例では、複数の set アクションを設定すると、それらのアクションが上記の順序で評価されます。setアクションのすべてのオプションが評価され、それらを適用できない場合にのみ、次の set アクションが考慮されます。この順序設定により、すぐに使用可能な最短のネクストホップが最初に試行され、その後、次のすぐに使用可能な最短のネクストホップが試行される、といったようになります。

```
ciscoasa(config)# route-map testmap permit 10
ciscoasa(config-route-map)# match ip address acl_1
ciscoasa(config-route-map)# set ip next-hop verify-availability 1.1.1.10 1 track 1
ciscoasa(config-route-map)# set ip next-hop verify-availability 1.1.1.11 2 track 2
ciscoasa(config-route-map)# set ip next-hop verify-availability 1.1.1.12 3 track 3
ciscoasa(config-route-map)# set ip next-hop 2.1.1.10 2.1.1.11 2.1.1.12
ciscoasa(config-route-map)# set ip next-hop recursive 3.1.1.10
ciscoasa(config-route-map)# set interface outside-1 outside-2
ciscoasa(config-route-map)# set ip default next-hop 4.1.1.10 4.1.1.11
ciscoasa(config-route-map)# set default interface Null0
```

PBR の設定例

ここでは、次のシナリオ用に PBR を設定するために必要な設定の完全なセットについて説明します。



まず、インターフェイスを設定する必要があります。

```
ciscoasa(config)# interface GigabitEthernet0/0
ciscoasa(config-if)# no shutdown
ciscoasa(config-if)# nameif inside
ciscoasa(config-if)# ip address 10.1.1.1 255.255.255.0

ciscoasa(config)# interface GigabitEthernet0/1
ciscoasa(config-if)# no shutdown
ciscoasa(config-if)# nameif outside-1
```

```
ciscoasa(config-if)# ip address 192.168.6.5 255.255.255.0

ciscoasa(config)# interface GigabitEthernet0/2
ciscoasa(config-if)# no shutdown
ciscoasa(config-if)# nameif outside-2
ciscoasa(config-if)# ip address 172.16.7.6 255.255.255.0
```

次に、トラフィックを照合するためのアクセスリストを設定する必要があります。

```
ciscoasa(config)# access-list acl-1 permit ip 10.1.0.0 255.255.0.0
ciscoasa(config)# access-list acl-2 permit ip 10.2.0.0 255.255.0.0
```

必要なsetアクションとともに、一致基準として上記のアクセスリストを指定することで、ルート マップを設定する必要があります。

```
ciscoasa(config)# route-map equal-access permit 10
ciscoasa(config-route-map)# match ip address acl-1
ciscoasa(config-route-map)# set ip next-hop 192.168.6.6

ciscoasa(config)# route-map equal-access permit 20
ciscoasa(config-route-map)# match ip address acl-2
ciscoasa(config-route-map)# set ip next-hop 172.16.7.7

ciscoasa(config)# route-map equal-access permit 30
ciscoasa(config-route-map)# set ip interface Null0
```

ここで、このルート マップをインターフェイスに接続する必要があります。

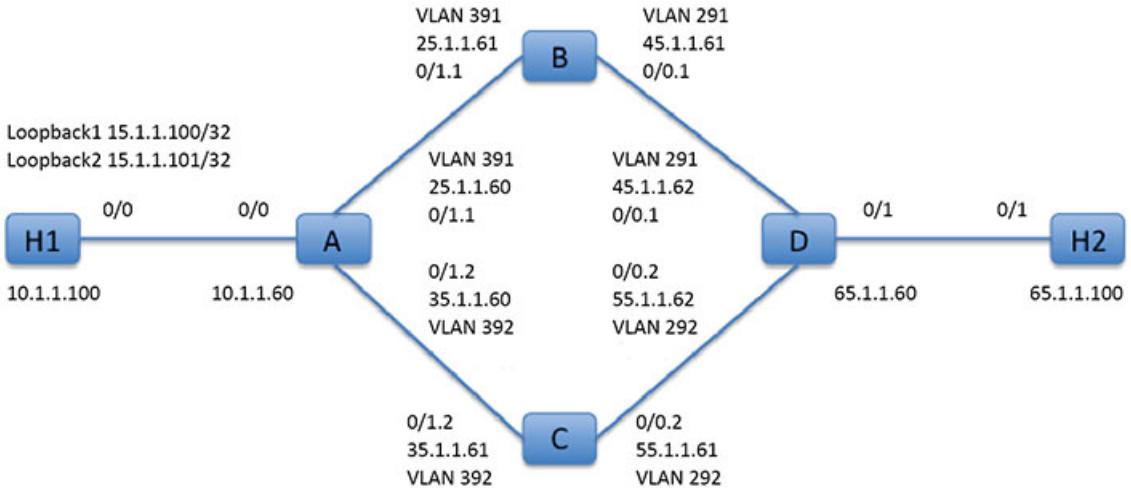
```
ciscoasa(config)# interface GigabitEthernet0/0
ciscoasa(config-if)# policy-route route-map equal-access
```

ポリシー ルーティング設定を表示するには：

```
ciscoasa(config)# show policy-route
Interface                  Route map
GigabitEthernet0/0   equal-access
```

アクションでのポリシーベース ルーティング

このテスト設定を使用して、異なる一致基準およびsetアクションでポリシーベース ルーティングが設定され、それらがどのように評価および適用されるのかを確認します。



まず、セットアップに関係するすべてのデバイスの基本設定から始めます。ここで、A、B、C、および D は ASA デバイスを表し、H1 および H2 は IOS ルータを表します。

ASA-A：

```
ciscoasa(config)# interface GigabitEthernet0/0
ciscoasa(config-if)# nameif inside
ciscoasa(config-if)# security-level 100
ciscoasa(config-if)# ip address 10.1.1.60 255.255.255.0
ciscoasa(config)# interface GigabitEthernet0/1
ciscoasa(config-if)# no shut

ciscoasa(config)# interface GigabitEthernet0/1.1
ciscoasa(config-if)# vlan 391
ciscoasa(config-if)# nameif outside
ciscoasa(config-if)# security-level 0
ciscoasa(config-if)# ip address 25.1.1.60 255.255.255.0

ciscoasa(config)# interface GigabitEthernet0/1.2
ciscoasa(config-if)# vlan 392
ciscoasa(config-if)# nameif dmz
ciscoasa(config-if)# security-level 50
ciscoasa(config-if)# ip address 35.1.1.60 255.255.255.0
```

ASA-B：

```
ciscoasa(config)# interface GigabitEthernet0/0
ciscoasa(config-if)# no shut

ciscoasa(config)# interface GigabitEthernet0/0.1
ciscoasa(config-if)# vlan 291
ciscoasa(config-if)# nameif outside
ciscoasa(config-if)# security-level 0
ciscoasa(config-if)# ip address 45.1.1.61 255.255.255.0

ciscoasa(config)# interface GigabitEthernet0/1
```

```
ciscoasa(config-if)# no shut

ciscoasa(config)# interface GigabitEthernet0/1.1
ciscoasa(config-if)# vlan 391
ciscoasa(config-if)# nameif inside
ciscoasa(config-if)# security-level 100
ciscoasa(config-if)# ip address 25.1.1.61 255.255.255.0
```

ASA-C：

```
ciscoasa(config)# interface GigabitEthernet0/0
ciscoasa(config-if)# no shut

ciscoasa(config)# interface GigabitEthernet0/0.2
ciscoasa(config-if)# vlan 292
ciscoasa(config-if)# nameif outside
ciscoasa(config-if)# security-level 0
ciscoasa(config-if)# ip address 55.1.1.61 255.255.255.0

ciscoasa(config)# interface GigabitEthernet0/1
ciscoasa(config-if)# no shut

ciscoasa(config)# interface GigabitEthernet0/1.2
ciscoasa(config-if)# vlan 392
ciscoasa(config-if)# nameif inside
ciscoasa(config-if)# security-level 0
ciscoasa(config-if)# ip address 35.1.1.61 255.255.255.0
```

ASA-D：

```
ciscoasa(config)# interface GigabitEthernet0/0
ciscoasa(config-if)# no shut

ciscoasa(config) #interface GigabitEthernet0/0.1
ciscoasa(config-if)# vlan 291
ciscoasa(config-if)# nameif inside-1
ciscoasa(config-if)# security-level 100
ciscoasa(config-if)# ip address 45.1.1.62 255.255.255.0

ciscoasa(config)# interface GigabitEthernet0/0.2
ciscoasa(config-if)# vlan 292
ciscoasa(config-if)# nameif inside-2
ciscoasa(config-if)# security-level 100
ciscoasa(config-if)# ip address 55.1.1.62 255.255.255.0

ciscoasa(config)# interface GigabitEthernet0/1
ciscoasa(config-if)# nameif outside
ciscoasa(config-if)# security-level 0
ciscoasa(config-if)# ip address 65.1.1.60 255.255.255.0
```

H1：

```
ciscoasa(config)# interface Loopback1
ciscoasa(config-if)# ip address 15.1.1.100 255.255.255.255

ciscoasa(config-if)# interface Loopback2
ciscoasa(config-if)# ip address 15.1.1.101 255.255.255.255
```

```
ciscoasa(config)# ip route 0.0.0.0 0.0.0.0 10.1.1.60
```

H2：

```
ciscoasa(config)# interface GigabitEthernet0/1
ciscoasa(config-if)# ip address 65.1.1.100 255.255.255.0

ciscoasa(config-if)# ip route 15.1.1.0 255.255.255.0 65.1.1.60
```

H1 から送信されるトラフィックをルーティングするように ASA-A で PBR を設定します。

ASA-A：

```
ciscoasa(config-if)# access-list pbracl_1 extended permit ip host 15.1.1.100 any

ciscoasa(config-if)# route-map testmap permit 10
ciscoasa(config-if)# match ip address pbracl_1
ciscoasa(config-if)# set ip next-hop 25.1.1.61

ciscoasa(config)# interface GigabitEthernet0/0
ciscoasa(config-if)# policy-route route-map testmap

ciscoasa(config-if)# debug policy-route
```

H1： ping 65.1.1.100 repeat 1 source loopback1

```
pbr: policy based route lookup called for 15.1.1.100/44397 to 65.1.1.100/0 proto 1
sub_proto 8 received on interface inside
pbr: First matching rule from ACL(2)
pbr: route map testmap, sequence 10, permit; proceed with policy routing
pbr: evaluating next-hop 25.1.1.61
pbr: policy based routing applied; egress_ifc = outside : next_hop = 25.1.1.61
```

パケットは、ルートマップのネクストホップアドレスを使用して想定どおりに転送されます。

ネクストホップを設定した場合、入力ルートテーブルで検索して設定したネクストホップに接続されたルートを特定し、対応するインターフェイスを使用します。この例の入力ルートテーブルを次に示します（一致するルート エントリが強調表示されています）。

```
in   255.255.255.255 255.255.255.255 identity
in   10.1.1.60       255.255.255.255 identity
in   25.1.1.60       255.255.255.255 identity
in   35.1.1.60       255.255.255.255 identity
in   10.127.46.17    255.255.255.255 identity
in   10.1.1.0        255.255.255.0   inside
in   25.1.1.0        255.255.255.0   outside
in   35.1.1.0        255.255.255.0   dmz
```

次に、ASA-A の dmz インターフェイスからの H1 loopback2 から送信されるパケットをルーティングするように ASA-A を設定します。

```
ciscoasa(config)# access-list pbracl_2 extended permit ip host 15.1.1.101 any

ciscoasa(config)# route-map testmap permit 20
ciscoasa(config-route-map)# match ip address pbracl
```

```
ciscoasa(config-route-map)# set ip next-hop 35.1.1.61

ciscoasa(config)# show run route-map
!
route-map testmap permit 10
  match ip address pbracl_1
  set ip next-hop 25.1.1.61
!
route-map testmap permit 20
  match ip address pbracl_2
  set ip next-hop 35.1.1.61
!
```

H1：ping 65.1.1.100 repeat 1 source loopback2

デバッグを示します。

```
pbr: policy based route lookup called for 15.1.1.101/1234 to 65.1.1.100/1234 proto 6
sub_proto 0 received on interface inside
pbr: First matching rule from ACL(3)
pbr: route map testmap, sequence 20, permit; proceed with policy routing
pbr: evaluating next-hop 35.1.1.61
pbr: policy based routing applied; egress_ifc = dmz : next_hop = 35.1.1.61
```

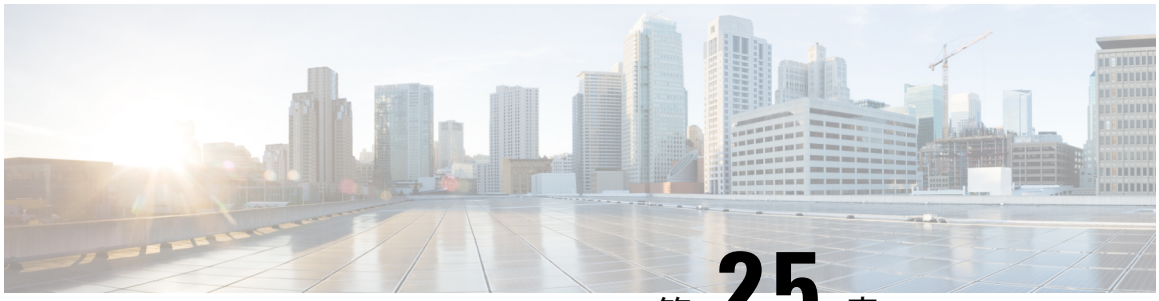
さらに、入力ルート テーブルから選択されたルートのエントリをここに示します。

```
in   255.255.255.255 255.255.255.255 identity
 in   10.1.1.60       255.255.255.255 identity
 in   25.1.1.60       255.255.255.255 identity
 in   35.1.1.60       255.255.255.255 identity
 in   10.127.46.17    255.255.255.255 identity
 in   10.1.1.0        255.255.255.0   inside
 in   25.1.1.0        255.255.255.0   outside
 in   35.1.1.0        255.255.255.0   dmz
```

ポリシーベース ルーティングの履歴

表 *25 :* ルート マップの履歴

機能名	プラットフォーム リリース	機能情報
ポリシーベース ルーティング	9.4(1)	ポリシーベースルーティング（PBR）は、ACL を使用して指定された QoS でトラフィックが特定のパスを経由するために使用するメカニズムです。ACL では、パケットのレイヤ 3 およびレイヤ4 ヘッダーの内容に基づいてトラフィックを分類できます。このソリューションにより、管理者は区別されたトラフィックに QoS を提供し、低帯域幅、低コストの永続パス、高帯域幅、高コストのスイッチドパスの間でインタラクティブ トラフィックとバッチ トラフィックを分散でき、インターネット サービス プロバイダーとその他の組織は明確に定義されたインターネット接続を介して一連のさまざまなユーザから送信されるトラフィックをルーティングできます。 **set ip next-hop verify-availability**、**set ip next-hop**、**set ip next-hop recursive**、**set interface**、**set ip default next-hop**、**set default interface**、**set ip df**、**set ip dscp**、**policy-route route-map**、**show policy-route**、**debug policy-route** の各コマンドが導入されました。



第 25 章

ルート マップ

この章では、Cisco ASA にルート マップを設定およびカスタマイズする方法について説明します。

ルート マップについて

ルート マップは、ルートを OSPF、RIP、EIGRP、または BGP ルーティング プロセスに再配布するときに使用します。また、デフォルト ルートを OSPF ルーティング プロセスに生成するときにも使用します。ルート マップは、指定されたルーティング プロトコルのどのルートを対象ルーティング プロセスに再配布できるのかを定義します。

ルート マップは、広く知られた ACL と共通の機能を数多く持っています。両方に共通する主な特性は次のとおりです。

- いずれも、それぞれが許可または拒否の結果を持つ個々の文を一定の順序で並べたものです。ACL またはルートマップの評価は、事前に定義された順序でのリストのスキャンと、一致する各文の基準の評価で構成されています。リストのスキャンは、文の一致が初めて見つかり、その文に関連付けられたアクションが実行されると中断します。
- これらは一般的なメカニズムです。基準一致と一致解釈は、適用方法とこれらを使用する機能によって決定します。異なる機能に適用される同じルートマップの解釈が異なることがあります。

次のように、ルート マップと ACL には違いがいくつかあります。

- ルート マップは ACL よりも柔軟性が高く、ACL が確認できない基準に基づいてルートを確認できます。たとえば、ルートマップはルートのタイプが内部であるかどうかを確認できます。

- 設計規則により、各 ACL は暗黙の deny 文で終了します。一致試行の間にルートマップの終わりに達した場合は、そのルートマップの特定のアプリケーションによって結果が異なります。再配布に適用されるルートマップの動作はACLと同じです。ルートがルートマップのどの句とも一致しない場合は、ルートマップの最後に deny 文が含まれている場合と同様に、ルートの再配布が拒否されます。

permit 句と deny 句

ルート マップでは permit 句と deny 句を使用できます。deny 句は、ルートの照合の再配布を拒否します。ルートマップでは、一致基準として ACL を使用できます。ACL には permit 句と deny 句もあるため、パケットが ACL と一致した場合に次のルールが適用されます。

- ACL permit + route map permit：ルートは再配布されます。
- ACL permit + route map deny：ルートは再配布されません。
- ACL deny + route map permit or deny：ルート マップの句は一致せず、次のルート マップ句が評価されます。

match 句と set 句の値

各ルート マップ句には、次の 2 種類の値があります。

- match 値は、この句が適用されるルートを選択します。
- set 値は、ターゲット プロトコルに再配布される情報を変更します。

再配布される各ルートについて、ルータは最初にルートマップの句の一致基準を評価します。一致基準が満たされると、そのルートは、permit 句または deny 句に従って再配布または拒否され、そのルートの一部の属性が、set コマンドによって設定された値で変更されます。一致基準が満たされないと、この句はルートに適用されず、ソフトウェアはルートマップの次の句でルートを評価します。ルートマップのスキャンは、ルートと一致する句が見つかるまで、もしくはルートマップの最後に到達するまで続行します。

次のいずれかの条件が満たされる場合は、各句の match 値または set 値を省略したり、何回か繰り返したりできます。

- 複数の match エントリが句に含まれる場合に、特定のルートが句に一致するためには、そのルートですべての照合に成功しなければなりません（つまり、複数の match コマンドでは論理 AND アルゴリズムが適用される）。
- match エントリが 1 つのエントリの複数のオブジェクトを指している場合は、そのいずれかが一致していなければなりません（論理 OR アルゴリズムが適用される）。
- match エントリがない場合は、すべてのルートが句に一致します。
- ルート マップの permit 句に set エントリが存在しない場合、ルートは、その現在の属性を変更されずに再配布されます。

（注） ルート マップの deny 句では set エントリを設定しないでください。deny 句を指定するとルートの再配布が禁止され、情報が何も変更されないからです。

match エントリまたは set エントリがないルート マップ句はアクションを実行します。空の permit 句を使用すると、変更を加えずに残りのルートの再配布が可能になります。空の deny 句では、他のルートの再配布はできません。これは、ルートマップがすべてスキャンされたときに、明示的な一致が見つからなかったときのデフォルト アクションです。

ルート マップのガイドライン

ファイアウォール モード

ルーテッド ファイアウォール モードでだけサポートされています。トランスペアレント ファイアウォール モードはサポートされません。

その他のガイドライン

ルート マップは、ユーザ、ユーザ グループ、または完全修飾ドメイン名のオブジェクトを含む ACL をサポートしていません。

ルート マップの定義

ルート マップを定義する必要があるのは、指定したルーティング プロトコルからのどのルートを対象ルーティング プロセスに再配布できるのかを指定するときです。

手順

ルート マップのエントリを作成します。

route-map *name* {**permit** | **deny**} [*sequence_number*]

例：

```
ciscoasa(config)# route-map name {permit} [12]
```

ルート マップのエントリは順番に読み取られます。この順序は、*sequence_number* 引数を使用して指定できます。この引数で指定しなければ、ルートマップエントリを追加した順序が ASA で使用されます。

ルート マップのカスタマイズ

ここでは、ルート マップをカスタマイズする方法について説明します。

特定の宛先アドレスに一致するルートの定義

手順

ステップ 1 ルート マップのエントリを作成します。

route-map *name* {**permit** | **deny**} [*sequence_number*]

例：

```
ciscoasa(config)# route-map name {permit} [12]
```

ルート マップのエントリは順番に読み取られます。この順序は、*sequence_number* オプションを使用して指定できます。この引数で指定しなければ、ルート マップ エントリを追加した順序が ASA で使用されます。

ステップ 2 標準 ACL またはプレフィックス リストに一致する宛先ネットワークを持つ任意のルートを照合します。

match ip address *acl_id* [*acl_id*] [...] [prefix-list]

例：

```
ciscoasa(config-route-map)# match ip address acl1
```

複数の ACL を指定する場合、ルートは任意の ACL を照合できます。

ステップ 3 指定したメトリックを持つ任意のルートを照合します。

match metric *metric_value*

例：

```
ciscoasa(config-route-map)# match metric 200
```

metric_value には、0 ～ 4294967295 の範囲が指定できます。

ステップ 4 標準 ACL と一致するネクスト ホップ ルータ アドレスを持つ任意のルートを照合します。

match ip next-hop *acl_id* [*acl_id*] [...]

例：

```
ciscoasa(config-route-map)# match ip next-hop acl2
```

複数の ACL を指定する場合、ルートは任意の ACL を照合できます。

ステップ 5 指定されたネクスト ホップ インターフェイスを持つ任意のルートを照合します。

match interface *if_name*

例：

```
ciscoasa(config-route-map)# match interface if_name
```

2 つ以上のインターフェイスを指定する場合、ルートはいずれかのインターフェイスと一致します。

ステップ 6 標準の ACL と一致するルータによってアドバタイズされた任意のルートを照合します。

match ip route-source *acl_id* [*acl_id*] [...]

例：

```
ciscoasa(config-route-map)# match ip route-source acl_id [acl_id] [...]
```

複数の ACL を指定する場合、ルートは任意の ACL を照合できます。

ステップ 7 ルート タイプを照合します。

match route-type {**internal** | **external** [**type-1** | **type-2**]}

ルート アクションのメトリック値の設定

ルートが **match** コマンドで一致する場合は、次の **set** コマンドによって、ルートを再配布する前にルートで実行するアクションが決まります。

ルート アクションのメトリック値を設定するには、次の手順を実行します。

手順

ステップ 1 ルート マップのエントリを作成します。

route-map *name* {**permit** | **deny**} [*sequence_number*]

例：

```
ciscoasa(config)# route-map name {permit} [12]
```

ルート マップのエントリは順番に読み取られます。この順序は、*sequence_number* 引数を使用して指定できます。この引数で指定しなければ、ルートマップエントリを追加した順序が ASA で使用されます。

ステップ 2 ルート マップのメトリック値を設定します。

set metric *metric_value*

例：

```
ciscoasa(config-route-map)# set metric 200
```

metric_value の引数は、0～294967295 の範囲で指定できます。

ステップ 3 ルート マップのメトリック タイプを設定します。

set metric-type {**type-1** | **type-2**}

例：

```
ciscoasa(config-route-map)# set metric-type type-2
```

metric-type 引数には type-1 と type-2 があります。

ルート マップの例

次の例は、ホップ カウント 1 でルートを OSPF に再配布する方法を示しています。

ASA は、これらのルートをメトリック 5、メトリック タイプ 1 で外部 LSA として再配布します。

```
ciscoasa(config)# route-map 1-to-2 permit
ciscoasa(config-route-map)# match metric 1
ciscoasa(config-route-map)# set metric 5
ciscoasa(config-route-map)# set metric-type type-1
```

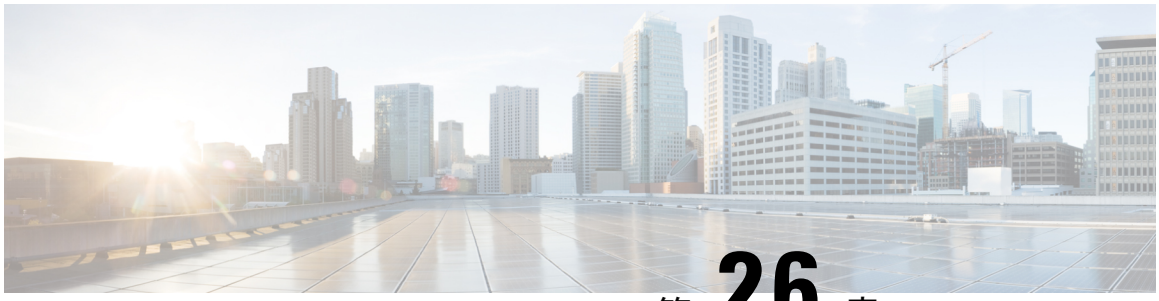
次に、メトリック値が設定された EIGRP プロセス 1 に 10.1.1.0 のスタティック ルートを再配布する例を示します。

```
ciscoasa(config)# route outside 10.1.1.0 255.255.255.0 192.168.1.1
ciscoasa(config-route-map)# access-list mymap2 line 1 permit 10.1.1.0 255.255.255.0
ciscoasa(config-route-map)# route-map mymap2 permit 10
ciscoasa(config-route-map)# match ip address mymap2
ciscoasa(config-route-map)# router eigrp 1
ciscoasa(config-router)# redistribute static metric 250 250 1 1 1 route-map mymap2
```

ルート マップの履歴

表 *26 :* ルート マップの機能履歴

機能名	プラットフォーム リリース	機能情報
ルート マップ	7.0(1)	この機能が導入されました。 **route-map** コマンドが導入されました。
スタティックおよびダイナミック ルート マップのサポートの強化	8.0(2)	ダイナミックおよびスタティック ルート マップのサポートが強化されました。
ダイナミック ルーティング プロトコル（EIGRP、OSPF、RIP）のステートフル フェールオーバーと一般的なルーティング関連動作のデバッグのサポート	8.4(1)	**debug route**、および **show debug route** コマンドが導入されました。 **show route** コマンドが変更されました。
マルチ コンテキスト モードのダイナミック ルーティング	9.0(1)	ルート マップは、マルチ コンテキスト モードでサポートされます。
BGP のサポート	9.2(1)	この機能が導入されました。 **router bgp** コマンドが導入されました。
プレフィックス ルールの IPv6 サポート	9.3.2	この機能が導入されました。



第 26 章

BGP

この章では、Border Gateway Protocol（BGP）を使用してデータのルーティング、認証の実行、ルーティング情報の再配布を行うように Cisco ASA を設定する方法について説明します。

BGPについて

BGP は相互および内部の自律システムのルーティング プロトコルです。自律システムとは、共通の管理下にあり、共通のルーティング ポリシーを使用するネットワークまたはネットワーク グループです。BGP は、インターネットのルーティング情報を交換するために、インターネット サービス プロバイダー（ISP）間で使用されるプロトコルです。

BGP を使用する状況

大学や企業などの顧客ネットワークでは、そのネットワーク内でルーティング情報を交換するために OSPF などの内部ゲートウェイ プロトコル（IGP）を通常使用しています。カスタマーは ISP に接続し、ISP は BGP を使用してカスタマーおよび ISP ルートを交換します。自律システム（AS）間で BGP を使用する場合、このプロトコルは外部 BGP（EBGP）と呼ばれます。サービス プロバイダーが BGP を使用して AS 内でルートを交換する場合、このプロトコルは内部 BGP（IBGP）と呼ばれます。

BGP は、IPv6 ネットワーク上で IPv6 プレフィックスのルーティング情報を伝送するために使用することができます。

（注） BGPv6 デバイスがクラスタに参加すると、ロギング レベル 7 が有効の場合、ソフト トレースバックを生成します。

ルーティング テーブルの変更

BGP ネイバーは、ネイバー間で最初に TCP 接続を確立する際に、完全なルーティング情報を交換します。ルーティングテーブルで変更が検出された場合、BGPルータはネイバーに対し、変更されたルートのみを送信します。BGP ルータは、定期的にルーティング アップデートを送信しません。また BGP ルーティング アップデートは、宛先ネットワークに対する最適パスのアドバタイズのみを行います。

BGPにより学習されたルートには、特定の宛先に対して複数のパスが存在する場合、宛先に対する最適なルートを決定するために使用されるプロパティが設定されています。これらのプロパティは BGP 属性と呼ばれ、ルート選択プロセスで使用されます。

- Weight：これは、シスコ定義の属性で、ルータに対してローカルです。Weight属性は、隣接ルータにアドバタイズされません。ルータが同じ宛先への複数のルートがあることを学習すると、Weight が最も大きいルートが優先されます。
- Local preference：Local preference 属性は、ローカル AS からの出力点を選択するために使用されます。Weight 属性とは異なり、Local preference 属性は、ローカル AS 全体に伝搬されます。AS からの出力点が複数ある場合は、Local preference 属性が最も高い出力点が特定のルートの出力点として使用されます。
- Multi-exit discriminator：メトリック属性である Multi-exit discriminator（MED）は、メトリックをアドバタイズしている AS への優先ルートに関して、外部 AS への提案として使用されます。これが提案と呼ばれるのは、MEDを受信している外部ASがルート選択の際に他の BGP 属性も使用している可能性があるためです。MED メトリックが小さい方のルートが優先されます。
- Origin：Origin 属性は、BGP が特定のルートについてどのように学習したかを示します。Origin 属性は、次の 3 つの値のいずれかに設定することができ、ルート選択に使用されます。
  - IGP：ルートは発信側 AS の内部にあります。この値は、ネットワーク ルータ コンフィギュレーション コマンドを使用して BGP にルートを挿入する場合に設定されます。
  - EGP：ルートは Exterior Border Gateway Protocol（EBGP）を使用して学習されます。
  - Incomplete：ルートの送信元が不明であるか、他の方法で学習されています。Incomplete の Origin は、ルートが BGP に再配布されるときに発生します。
- AS_path：ルートアドバタイズメントが自律システムを通過すると、ルートアドバタイズメントが通過した AS 番号が AS 番号の順序付きリストに追加されます。AS_path リストが最も短いルートのみ、IP ルーティング テーブルにインストールされます。
- Next hop：EBGP の Next-hop 属性は、アドバタイズしているルータに到達するために使用される IP アドレスです。EBGP ピアの場合、ネクスト ホップ アドレスは、ピア間の接続の IP アドレスです。IBGP の場合、EBGP のネクスト ホップ アドレスがローカル AS に伝送されます。

- Community：Community 属性は、ルーティングの決定（承認、優先度、再配布など）を適用できる宛先をグループ化する方法、つまりコミュニティを提供します。ルート マップは、Community 属性を設定するために使用されます。事前定義済みの Community 属性は次のとおりです。
  - no-export：EBGP ピアにこのルートをアドバタイズしません。
  - no-advertise：このルートをどのピアにもアドバタイズしない。
  - internet：インターネット コミュニティにこのルートをアドバタイズします。ネットワーク内のすべてのルートがこのコミュニティに属します。

BGP パスの選択

BGP は、異なる送信元から同じルートの複数のアドバタイズメントを受信する場合があります。BGP は最適なパスとして 1 つのパスだけを選択します。このパスを選択すると、BGP は IP ルーティング テーブルに選択したパスを格納し、そのネイバーにパスを伝搬します。BGP は次の基準を使用して（示されている順序で）、宛先へのパスを選択します。

- パスで指定されているネクストホップが到達不能な場合、このアップデートは削除されます。
- Weight が最大のパスが優先されます。
- Weight が同じである場合、Local preference が最大のパスが優先されます。
- Local preference が同じである場合、このルータで動作している BGP により発信されたパスが優先されます。
- ルートが発信されていない場合、AS_path が最短のルートが優先されます。
- すべてのパスの AS_path の長さが同じである場合、Origin タイプが最下位のパス（IGP は EGP よりも低く、EGP は Incomplete よりも低い）が優先されます。
- Origin コードが同じである場合、最も小さい MED 属性を持つパスが優先されます。
- パスの MED が同じである場合、内部パスより外部パスが優先されます。
- それでもパスが同じである場合、最も近い IGP ネイバーを経由するパスが優先されます。
- BGP マルチパス （744 ページ） のルーティング テーブルで、複数のパスのインストールが必要かどうかを判断します。
- 両方のパスが外部の場合、最初に受信したパス（最も古いパス）が優先されます。
- BGP ルータ ID で指定された、IP アドレスが最も小さいパスが優先されます。
- 送信元またはルータ ID が複数のパスで同じである場合、クラスタ リストの長さが最小のパスが優先されます。
- 最も小さいネイバー アドレスから発信されたパスが優先されます。

BGP マルチパス

BGP マルチパスでは、同一の宛先プレフィックスへの複数の等コスト BGP パスを IP ルーティング テーブルに組み込むことができます。その場合、宛先プレフィックスへのトラフィックは、組み込まれたすべてのパス間で共有されます。

これらのパスは、負荷共有のためのベスト パスと共にテーブルに組み込まれます。BGP マルチパスは、ベストパスの選択には影響しません。たとえば、ルータは引き続き、アルゴリズムに従っていずれかのパスをベスト パスとして指定し、このベスト パスをルータの BGP ピアにアドバタイズします。

同一宛先へのパスをマルチパスの候補にするには、これらのパスの次の特性がベストパスと同等である必要があります。

- 重量
- ローカル プリファレンス
- AS-PATH の長さ
- オリジン コード
- Multi Exit Discriminator（MED）
- 次のいずれかです。
  - ネイバー AS またはサブ AS（BGP マルチパスの追加前）
  - AS-PATH（BGP マルチパスの追加後）

一部の BGP マルチパス機能では、マルチパス候補に要件が追加されます。

- パスは外部ネイバーまたは連合外部ネイバー（eBGP）から学習される必要があります。
- BGP ネクスト ホップへの IGP メトリックは、ベストパス IGP メトリックと同等である必要があります。

内部 BGP（iBGP）マルチパス候補の追加要件を次に示します。

- 内部ネイバー（iBGP）からパスが学習される必要があります。
- ルータが不等コスト iBGP マルチ パス用に設定されていない限り、BGP ネクストホップへの IGP メトリックは、ベスト パス IGP メトリックと同等です。

BGP はマルチパス候補から最近受信したパスのうち、最大 *n* 本のパスを IP ルーティング テーブルに挿入します。この *n* は、BGP マルチパスの設定時に指定した、ルーティング テーブルに組み込まれるルートの数です。マルチパスが無効な場合のデフォルト値は 1 です。

不等コスト ロード バランシングの場合、BGP リンク帯域幅も使用できます。

（注） 内部ピアへの転送前に、eBGP マルチパスで選択されたベストパスに対し、同等の next-hop-self が実行されます。

BGP のガイドライン

コンテキスト モードのガイドライン

シングル コンテキスト モードとマルチ コンテキスト モードでサポートされています。

ファイアウォール モードのガイドライン

トランスペアレント ファイアウォール モードはサポートされません。BGP は、ルーテッドモードでのみサポートされています。

IPv6 のガイドライン

IPv6 をサポートします。グレースフル リスタートは、IPv6 アドレス ファミリではサポートされません。

BGP を設定する

ここでは、システムで BGP プロセスをイネーブルにして設定する方法について説明します。

手順

ステップ 1 BGP の有効化 （745 ページ）。
ステップ 2 BGP ルーティング プロセスの最適なパスの定義 （747 ページ）。
ステップ 3 ポリシー リストの設定 （748 ページ）。
ステップ 4 AS パス フィルタの設定 （749 ページ）。
ステップ 5 コミュニティ ルールの設定 （750 ページ）。
ステップ 6 IPv4 アドレス ファミリの設定 （751 ページ）。
ステップ 7 IPv6 アドレス ファミリの設定 （765 ページ）。

BGP の有効化

ここでは、BGP の有効化、BGP ルーティング プロセスの確立、一般的な BGP パラメータの設定に必要な手順について説明します。

手順

ステップ 1 BGP ルーティング プロセスをイネーブルにし、ASA をルータ コンフィギュレーション モードにします。

router bgp autonomous-num

例：

```
ciscoasa(config)# router bgp 2
```

autonomous-num の有効値は 1 ～ 4294967295 および 1.0 ～ XX.YY です。

ステップ 2 指定値を超えている AS パス セグメントを含むルートを破棄します。

bgp maxas-limit number

例：

```
ciscoasa(config-router)# bgp maxas-limit 15
```

number 引数には、自律システム セグメントの最大許容数を指定します。有効値は 1 ～ 254 です。

ステップ 3 BGP ネイバーのリセットをログに記録します。

bgp log-neighbor-changes

ステップ 4 BGP で各 BGP セッションの最適な TCP パス MTU を自動検出できるようにします。

bgp transport path-mtu-discovery

ステップ 5 BGP が、ピアに到達するために使用されているリンクがダウンした場合に、ホールドダウン タイマーが期限切れになるのを待たずに、直接隣接するいずれかのピアの外部 BGP セッションを終了できるようにします。

bgp fast-external-fallover

ステップ 6 BGP ルーティング プロセスで、自律システム（AS）番号を着信ルートの AS_path 属性の 1 つ目の AS パス セグメントとしてリストしていない外部 BGP（eBGP）ピアから受信したアップデートを破棄できるようにします。

bgp enforce-first-as

ステップ 7 デフォルトの表示を変更し、BGP 4 バイト自律システム番号の正規表現一致形式を、asplain（10 進数の値）からドット付き表記にします。

bgp asnotation dot

ステップ 8 BGP ネットワーク タイマーを調整します。

timers bgp keepalive holdtime [min-holdtime]

例：

```
ciscoasa(config-router)# timers bgp 80 120
```

- keepalive：ASA がキープアライブ メッセージをピアに送信する頻度（秒）。デフォルト値は 60 秒です。
- holdtime：キープアライブ メッセージを受信できない状態が継続して、ピアがデッドであると ASA が宣言するまでの時間（秒）。デフォルト値は 180 秒です。
- （オプション）min-holdtime：ネイバーからキープアライブ メッセージを受信できない状態が継続して、ネイバーがデッドであると ASA が宣言するまでの時間（秒）。

ステップ 9 BGP グレースフル リスタート機能をイネーブルにします。

bgp graceful-restart [restart-time seconds|stalepath-time seconds][all]

例：

```
ciscoasa(config-router)# bgp graceful-restart restart-time 200
```

- restart-time：リスタート イベントが発生した後、グレースフル リスタート対応ネイバーが通常の動作に戻るまで ASA が待機する最大時間（秒）。デフォルトは 120 秒です。有効な値は 1 ～ 3600 秒です。
- stalepath-time：リスタートしているピアの古いパスを ASA が保持する最大時間（秒）。すべての古いパスは、このタイマーが期限切れになった後に削除されます。デフォルト値は 360 秒です。有効な値は 1 ～ 3600 秒です。

BGP ルーティング プロセスの最適なパスの定義

ここでは、BGP の最適なパスを設定するために必要な手順について説明します。最適なパスの詳細については、BGP パスの選択 （743 ページ）を参照してください。

手順

ステップ 1 BGP ルーティング プロセスをイネーブルにし、ASA をルータ コンフィギュレーション モードにします。

router bgp autonomous-num

例：

```
ciscoasa(config)# router bgp 2
```

ステップ 2 デフォルトの Local preference 値を変更します。

bgp default local-preference number

例：

```
ciscoasa(config-router)# bgp default local-preference 500
```

number 引数は、0 ～ 4294967295 の値です。値が大きいほど、優先度が高いことを示します。

デフォルト値は 100 です。

ステップ 3 さまざまな自律システムのネイバーから学習したパス間での Multi-exit discriminator（MED）比較をイネーブルにします。

bgp always-compare-med

ステップ 4 最適なパスの選択プロセス中に外部 BGP（eBGP）ピアから受信した類似ルートを比較し、最適なパスをルータ ID が最も小さいルートに切り替えます。

bgp bestpath compare-routerid

ステップ 5 隣接 AS からアドバタイズされた最適な MED パスを選択します。

bgp deterministic-med

ステップ 6 MED 属性が欠落しているパスを最も優先度の低いパスとして設定します。

bgp bestpath med missing-as-worst

ポリシー リストの設定

ルート マップ内でポリシー リストが参照されると、ポリシー リスト内の match 文すべてが評価され、処理されます。1 つのルート マップに 2 つ以上のポリシー リストを設定できる。ポリシー リストは、同じルート マップ内にあるがポリシー リストの外で設定されている他の既存の match および set 文とも共存できます。ここでは、ポリシー リストを設定するために必要な手順について説明します。

手順

ステップ 1 ポリシー マップ コンフィギュレーション モードをイネーブルにし、BGP ポリシー リストを作成できるようにします。

policy-list policy_list_name {permit | deny}

例：

```
ciscoasa(config)# policy-list Example-policy-list1 permit
```

permit キーワードを指定すると、条件が一致した場合にアクセスが許可されます。

deny キーワードを指定すると、条件が一致した場合にアクセスが拒否されます。

ステップ 2 指定したいずれかのインターフェイスの外部にネクスト ホップを持つルートを配布します。

match interface [...interface_name]

例：

```
ciscoasa(config-policy-list)# match interface outside
```

ステップ 3 宛先アドレス、ネクスト ホップ ルータ アドレス、ルータ/アクセス サーバ ソースのいずれかまたはすべてを一致させてルートを再配布します。

match ip {address | next-hop | route-source}

ステップ 4 BGP 自律システム パスを一致させます。

match as-path

ステップ 5 BGP コミュニティを一致させます。

match community {community-list_name | exact-match}

例：

```
ciscoasa(config-policy-list)# match community ExampleCommunity1
```

- community-list_name：1 つ以上のコミュニティ リスト。
- exact-match：完全に一致する必要があることを示します。指定されたすべてのコミュニティのみが存在する必要があります。

ステップ 6 指定したメトリックを持つルートを再配布します。

match metric

ステップ 7 指定されたタグと一致するルーティング テーブルのルートを再配布します。

match tag

AS パス フィルタの設定

AS パス フィルタで、アクセス リストを使用してルーティング アップデート メッセージをフィルタリングし、アップデート メッセージ内の個々のプレフィックスを確認できます。アップデート メッセージ内のプレフィックスがフィルタ基準に一致すると、フィルタ エントリで実行するように設定されているアクションに応じて、個々のプレフィックスは除外されるか受け入れられます。ここでは、AS パス フィルタを設定するために必要な手順について説明します。

（注） AS パス アクセス リストは、通常のファイアウォール ACL とは異なります。

手順

グローバル コンフィギュレーション モードで正規表現を使用して自律システム パス フィルタを設定します。

as-path access-list acl-number {permit|deny} regexp

例：

```
ciscoasa(config)# as-path access-list 35 permit testaspath
```

- *acl-number*：AS パス アクセスリストの番号。有効な値は、1 ～ 500 です。
- regexp：AS パス フィルタを定義する正規表現。自律システム番号は 1 ～ 65535 の範囲で表します。

コミュニティ ルールの設定

コミュニティは、共通するいくつかの属性を共有する宛先のグループです。コミュニティ リストを使用すると、ルート マップの match 句で使用されるコミュニティ グループを作成できます。アクセス リストと同様に、一連のコミュニティ リストを作成できます。ステートメントは一致が見つかるまでチェックされ、1 つのステートメントが満たされると、テストは終了します。ここでは、コミュニティ ルールを設定するために必要な手順について説明します。

手順

BGP コミュニティ リストを作成または設定して、そのリストへのアクセスを制御します。

community-list {standard| community list-name {deny|permit} [community-number] [AA:NN] [internet] [no-advertise][no-export]}| {expanded|expanded list-name {deny| permit}regexp}

例：

```
ciscoasa(config)# community-list standard excomm1 permit 100 internet no-advertise
no-export
```

- standard：1 ～ 99 の数字を使用して標準のコミュニティ リストを設定し、1 つ以上の許可または拒否コミュニティ グループを識別します。
- （オプション）community-number：1 ～ 4294967200 の 32 ビットの数値で表わされたコミュニティ。1 つのコミュニティ、または複数のコミュニティをそれぞれスペースで区切って入力できます。
- AA:NN：4 バイトの新コミュニティ形式で入力された自律システム番号およびネットワーク番号。この値は、コロンで区切られた 2 バイトの数 2 つで設定されます。2 バイトの数

ごとに 1 ～ 65535 の数を入力できます。1 つのコミュニティ、または複数のコミュニティをそれぞれスペースで区切って入力できます。

- （オプション）internet：インターネット コミュニティを指定します。このコミュニティのルートは、すべてのピア（内部および外部）にアドバタイズされます。
- （オプション）no-advertise：no-advertise コミュニティを指定します。このコミュニティのあるルートはピア（内部または外部）にはアドバタイズされません。
- （オプション）no-export：no-export コミュニティを指定します。このコミュニティのあるルートは、同じ自律システム内のピアへのみ、または連合内の他のサブ自律システムへのみアドバタイズされます。これらのルートは外部ピアにはアドバタイズされません。
- （オプション）expanded：100 ～ 500 の拡張コミュニティ リスト番号を設定し、1 つ以上の許可または拒否コミュニティ グループを識別します。
- regexp：AS パス フィルタを定義する正規表現。自律システム番号は 1 ～ 65535 の範囲で表します。

（注） 正規表現を使用できるのは拡張コミュニティ リストだけです。

IPv4 アドレス ファミリの設定

BGP の IPv4 設定は、BGP 設定セットアップ内の IPv4 ファミリ オプションから指定できます。IPv4 ファミリ セクションには、一般設定、集約アドレスの設定、フィルタリング設定、ネイバー 設定のサブセクションが含まれます。これらの各サブセクションを使用して、IPv4 ファミリに固有のパラメータをカスタマイズすることができます。

IPv4 ファミリの一般設定

ここでは、一般的な IPv4 の設定に必要な手順を説明します。

手順

ステップ 1 BGP ルーティング プロセスをイネーブルにし、ルータをルータ コンフィギュレーション モードにします。

router bgp autonomous-num

例：

```
ciscoasa(config)# router bgp 2
```

ステップ 2 アドレス ファミリ コンフィギュレーション モードを開始し、標準 IPv4 アドレス プレフィックスを使用するルーティング セッションを設定します。

address-family ipv4 [unicast]

キーワード unicast では、IPv4 ユニキャスト アドレス プレフィックスを指定します。これは、指定されていない場合でもデフォルト値になります。

ステップ 3 （オプション）ローカル BGP ルーティング プロセスの固定ルータ ID を設定します。

bgp router-id A.B.C.D

例：

```
ciscoasa(config-router-af)# bgp router-id 10.86.118.3
```

引数 A.B.C.D には、ルータ ID を IP アドレス形式で指定します。ルータ ID を指定しない場合、自動的に割り当てられます。

ステップ 4 （オプション）個別インターフェイス（L3）モードで IP アドレスのクラスタ プールを設定します。

bgp router-id cluster-pool

例：

```
ciscoasa(config-router-af)# bgp router-id cp
```

（注） L3 クラスタでは、BGP ネイバーをクラスタ プールの IP アドレスの 1 つとして定義できません。

ステップ 5 BGP ルートのアドミニストレーティブ ディスタンスを設定します。

distance bgp external-distance internal-distance local-distance

例：

```
ciscoasa(config-router-af)# distance bgp 80 180 180
```

- external-distance：外部 BGP ルートのアドミニストレーティブ ディスタンス。ルートは、外部自律システムから学習された場合は外部になります。この引数の値の範囲は 1 ～ 255 です。
- internal-distance：内部 BGP ルートのアドミニストレーティブ ディスタンス。ルートは、ローカル自律システムのピアから学習された場合は内部です。この引数の値の範囲は 1 ～ 255 です。
- local-distance：ローカル BGP ルートのアドミニストレーティブ ディスタンス。ローカル ルートは、別のプロセスから再配布されているルータまたはネットワークの、多くの場合バック ドアとして、ネットワーク ルータ コンフィギュレーション コマンドによりリストされるネットワークです。この引数の値の範囲は 1 ～ 255 です。

ステップ 6 BGP で学習されたルートを使用して IP ルーティング テーブルが更新されたときに、メトリックおよびタグ値を変更します。

table-map {WORD|route-map_name}

例：

```
ciscoasa(config-router-af)# table-map example1
```

引数 route-map_name には route-map コマンドのルート マップ名を指定します。

ステップ 7 BGP ルーティング プロセスを設定し、デフォルト ルート（ネットワーク 0.0.0.0）を配布します。

default-information originate

ステップ 8 ネットワーク レベルのルートへのサブネット ルートの自動集約を設定します。

auto-summary

ステップ 9 ルーティング情報ベース（RIB）にインストールされていないルートのアドバタイズメントを抑制します。

bgp suppress-inactive

ステップ 10 BGP と Interior Gateway Protocol（IGP）システム間で同期します。

同期

ステップ 11 OSPF などの IGP への iBGP の再配布を設定します。

bgp redistribute-internal

ステップ 12 ネクスト ホップの検証用に BGP ルータのスキャン間隔を設定します。

bgp scan-time scanner-interval

例：

```
ciscoasa(config-router-af)# bgp scan-time 15
```

引数 scanner-interval には BGP ルーティング情報のスキャン間隔を指定します。有効な値は 5 ～ 60 秒です。デフォルトは 60 秒です。

ステップ 13 BGP ネクスト ホップ アドレス トラッキングを設定します。

bgp nexthop trigger {delay seconds|enable}

例：

```
ciscoasa(config-router-af)# bgp nexthop trigger delay 15
```

- trigger：BGP ネクスト ホップ アドレス トレッキングの使用を指定します。ネクスト ホップ トラッキングの遅延を変更するには、このキーワードを delay キーワードとともに使用します。ネクスト ホップ アドレス トラッキングを有効にするには、このキーワードを enable キーワードとともに使用します。

- delay：ルーティング テーブルにインストールされている更新済みのネクスト ホップ ルートのチェック間の遅延間隔を変更します。
- seconds：遅延を秒数で指定します。指定できる値の範囲は 0 ～ 100 です。デフォルトは 5 です。
- enable：BGP ネクスト ホップ アドレス トラッキングをすぐに有効化します。

ステップ 14 ルーティング テーブルにインストールできる並列 iBGP ルートの最大数を制御します。

maximum-paths {number_of_paths|ibgp number_of_paths}

例：

```
ciscoasa(config-router-af)# maximum-paths ibgp 2
```

（注） ibgp キーワードを使用しない場合、number_of_paths 引数は、並列 EBGP ルートの最大数を制御します。

number_of_paths 引数には、ルーティング テーブルにインストールするルートの数を指定します。有効な値は、1 ～ 8 です。

IPv4 ファミリ集約アドレスの設定

ここでは、特定のルートの 1 つのルートへの集約を定義するために必要な手順について説明します。

手順

ステップ 1 BGP ルーティング プロセスをイネーブルにし、ASA をルータ コンフィギュレーション モードにします。

router bgp autonomous-num

例：

```
ciscoasa(config)# router bgp 2
```

ステップ 2 アドレス ファミリ コンフィギュレーション モードを開始し、標準 IPv4 アドレス プレフィックスを使用するルーティング セッションを設定します。

address-family ipv4 [unicast]

キーワード unicast では、IPv4 ユニキャスト アドレス プレフィックスを指定します。これは、指定されていない場合でもデフォルト値になります。

ステップ 3 BGP データベースで集約エントリを作成します。

aggregate-address address mask [as-set][summary-only][suppress-map map-name][advertise-map map-name][attribute-map map-name]

例：

```
ciscoasa(config-router-af) aggregate-address 10.86.118.0 255.255.255.0 as-set summary-only
 suppress-map example1 advertise-map example1 attribute-map example1
```

- address：集約アドレス。
- mask：集約マスク。
- map-name：ルート マップ。
- （オプション）as-set：自律システムの設定パス情報を生成します。
- （オプション）summary-only：アップデートから固有性の強いルートをすべてフィルタリングします。
- （オプション）Suppress-map map-name：抑制するルートを選択するために使用するルートマップの名前を指定します。
- （オプション）Advertise-map map-name：AS_SET 発信コミュニティを作成するためのルートを選択するために使用するルート マップの名前を指定します。
- （オプション）Attribute-map map-name：集約ルートの属性を設定するために使用するルート マップの名前を指定します。

IPv4 ファミリのフィルタリング設定

ここでは、着信 BGP アップデートで受信したルートまたはネットワークをフィルタリングするために必要な手順について説明します。

手順

ステップ 1 BGPP ルーティング プロセスを有効にし、ルータ コンフィギュレーション モードを開始します。

router bgp *autonomous-num*

例：

```
ciscoasa(config)# router bgp 2
```

ステップ 2 アドレス ファミリ コンフィギュレーション モードを開始し、標準 IPv4 アドレス プレフィックスを使用するルーティング セッションを設定します。

address-family ipv4 [**unicast**]

キーワード unicast では、IPv4 ユニキャスト アドレス プレフィックスを指定します。これは、指定されていない場合でもデフォルト値になります。

ステップ 3 着信 BGP アップデートで受信したルータまたはネットワーク、あるいは発信 BGP アップデートでアドバタイズされたルータまたはネットワークをフィルタリングします。

distribute-list *acl-number* {**in** | **out**} [*protocol process-number* | **connected** | **static**]

引数 *acl-number* には、IP アクセス リストの番号を指定します。アクセス リストは、ルーティング アップデートで受信されるネットワークと抑制されるネットワークを定義します。

キーワード **in** はフィルタを着信 BGP アップデートに適用する必要があることを指定し、**out** はフィルタを発信 BGP アップデートに適用する必要があることを指定します。

アウトバウンド フィルタの場合、必要に応じて、配布リストに適用するプロトコル（**bgp**、**eigrp**、**ospf**、または **rip**）をプロセス番号付き（RIP を除く）で指定できます。ピアおよびネットワークが **connected** または **static** ルート経由で学習されたかどうかでフィルタすることもできます。

例：

```
ciscoasa(config-router-af)# distribute-list ExampleAcl in bgp 2
```

IPv4 ファミリの BGP ネイバーの設定

ここでは、BGP ネイバーおよびネイバー設定を定義するために必要な手順について説明します。

手順

ステップ 1 BGP ルーティング プロセスをイネーブルにし、ルータをルータ コンフィギュレーション モードにします。

router bgp autonomous-num

例：

```
ciscoasa(config)# router bgp 2
```

ステップ 2 アドレス ファミリ コンフィギュレーション モードを開始し、標準 IPv4 アドレス プレフィックスを使用するルーティング セッションを設定します。

address-family ipv4 [unicast]

キーワード unicast では、IPv4 ユニキャスト アドレス プレフィックスを指定します。これは、指定されていない場合でもデフォルト値になります。

ステップ 3 エントリを BGP ネイバー テーブルに追加します。

neighbor ip-address remote-as autonomous-number

例：

```
ciscoasa(config-router-af)# neighbor 10.86.118.12 remote-as 3
```

ステップ 4 （オプション）ネイバーまたはピア グループをディセーブルにします。

neighbor ip-address shutdown

例：

```
ciscoasa(config-router-af)# neighbor 10.86.118.12 shutdown 3
```

ステップ 5 BGP ネイバーと情報を交換します。

neighbor ip-address activate

例：

```
ciscoasa(config-router-af)# neighbor 10.86.118.12 activate
```

ステップ 6 BGP ネイバーの Border Gateway Protocol（BGP）グレースフル リスタート機能をイネーブルまたはディセーブルにします。

neighbor ip-address ha-mode graceful-restart [disable]

例：

```
ciscoasa(config-router-af)# neighbor 10.86.118.12 ha-mode graceful-restart
```

（オプション）disable キーワードを指定すると、ネイバーの BGP グレースフル リスタート機能が無効化されます。

ステップ 7 アクセス リストで指定された BGP ネイバー情報を配布します。

neighbor {ip-address} distribute-list {access-list-name}{in|out}

例：

```
ciscoasa(config-router-af)# neighbor 10.86.118.12 distribute-list ExampleAcl in
```

- access-list-number：標準アクセス リストまたは拡張アクセス リストの番号。標準アクセス リストの番号の範囲は 1 ～ 99 です。拡張アクセス リストの番号の範囲は 100 ～ 199 です。
- expanded-list-number：拡張アクセス リストの番号。拡張アクセス リストの範囲は 1300 ～ 2699 です。
- access-list-name：標準アクセス リストまたは拡張アクセス リストの名前。
- prefix-list-name：BGP プレフィックス リストの名前。
- in：アクセス リストはそのネイバーへの着信アドバタイズメントに適用されます。

- out：アクセス リストはそのネイバーへの発信アドバタイズメントに適用されます。

ステップ 8 着信ルートまたは発信ルートにルート マップを適用します。

neighbor {ip-address} route-map map-name {in|out}

例：

```
ciscoasa(config-router-af)# neighbor 10.86.118.12 route-map example1 in
```

キーワード in を指定すると、ルート マップは着信ルートに適用されます。

キーワード out を指定すると、ルート マップは発信ルートに適用されます。

ステップ 9 プレフィックス リストで指定された BGP ネイバー情報を配布します。

neighbor {ip-address} prefix-list prefix-list-name {in|out}

例：

```
ciscoasa(config-router-af)# neighbor 10.86.118.12 prefix-list NewPrefixList in
```

キーワード in は、プレフィックス リストがそのネイバーからの着信アドバタイズメントに適用されることを意味します。

キーワード out は、プレフィックス リストがそのネイバーへの発信アドバタイズメントに適用されることを意味します。

ステップ 10 フィルタ リストを設定します。

neighbor {ip-address} filter-list access-list-number {in|out}

例：

```
ciscoasa(config-router-af)# neighbor 10.86.118.12 filter-list 5 in
```

- access-list-name：自律システム パスのアクセス リストの番号を指定します。ip as-path access-list コマンドを使用して、このアクセス リストを定義します。
- in：アクセス リストはそのネイバーからの着信アドバタイズメントに適用されます。
- out：アクセス リストはそのネイバーへの発信アドバタイズメントに適用されます。

ステップ 11 ネイバーから受信できるプレフィックスの数を制御します。

neighbor {ip-address} maximum-prefix maximum [threshold][restart restart interval][warning-only]

例：

```
ciscoasa(config-router-af)# neighbor 10.86.118.12 maximum-prefix 7 75 restart 12
```

- maximum：このネイバーからの許可される最大プレフィックス数。

- （オプション）threshold：最大数の何パーセントになったらルータが警告メッセージの生成を開始するかを指定する整数。指定できる範囲は1～100です。デフォルト値は75（%）です。
- （オプション）restart interval：BGP ネイバーが再起動するまでの時間を指定する整数値（分）。
- （オプション）warning-only：プレフィックスの最大数を超えた場合に、ピアリングを終了する代わりに、ルータでログ メッセージを生成できます。

ステップ 12 BGP スピーカー（ローカル ルータ）にネイバーへのデフォルト ルート 0.0.0.0 の送信を許可して、このルートがデフォルト ルートとして使用されるようにします。

neighbor {ip-address} default-originate [route-map map-name]

例：

```
ciscoasa(config-router-af)# neighbor 10.86.118.12 default-originate route-map example1
```

引数 map-name はルート マップの名前です。ルート マップにより、ルート 0.0.0.0 が条件に応じて注入されます。

ステップ 13 BGP ルーティング アップデートの最小送信間隔を設定します。

neighbor {ip-address} advertisement-interval seconds

例：

```
ciscoasa(config-router-af)# neighbor 10.86.118.12 advertisement-interval 15
```

引数 seconds は時間（秒）です。0 ～ 600 の範囲の値を指定できます。

ステップ 14 設定されているルート マップと一致する BGP テーブル内のルートをアドバタイズします。

neighbor {ip-address} advertise-map map-name {exist-map map-name |non-exist-map map-name}[check-all-paths]

例：

```
ciscoasa(config-router-af)# neighbor 10.2.1.1 advertise-map MAP1 exist-map MAP2
```

- advertise-map map name：exist-map または non-exist-map の条件に一致した場合にアドバタイズされるルート マップの名前。
- exist-map map name：advertise-map のルートがアドバタイズされるかどうかを判断するために BGP テーブル内のルートと比較される exist-map の名前。
- non-exist-map map name：advertise-map のルートがアドバタイズされるかどうかを判断するために BGP テーブル内のルートと比較される non-exist-map の名前。
- （オプション）check all paths：BGP テーブル内のプレフィックスを持つ exist-map によるすべてのパスのチェックを有効化します。

ステップ 15 プライベート自律システム番号を発信ルーティング アップデートから削除します。

neighbor {ip-address} remove-private-as

例：

```
ciscoasa(config-router-af)# neighbor 10.86.118.12 remove-private-as
```

ステップ 16 特定の BGP ピアまたは BGP ピア グループのタイマーを設定します。

neighbor {ip-address} timers keepalive holdtime min holdtime

例：

```
ciscoasa(config-router-af)# neighbor 10.86.118.12 timers 15 20 12
```

- keepalive：ASA がキープアライブ メッセージをピアに送信する頻度（秒）。デフォルトは 60 秒です。有効値は、0 ～ 65535 です。
- holdtime：キープアライブ メッセージを受信できない状態が継続して、ピアがデッドであると ASA が宣言するまでの時間（秒）。デフォルト値は 180 秒です。
- min holdtime：キープアライブ メッセージを受信できない状態が継続して、ピアがデッドであると ASA が宣言するまでの最小時間（秒）。

ステップ 17 2 つの BGP ピア間の TCP 接続で Message Digest 5（MD5）認証をイネーブルにします。

neighbor {ip-address} password string

例：

```
ciscoasa(config-router-af)# neighbor 10.86.118.12 password test
```

引数 string は大文字と小文字を区別するパスワードで、service password-encryption コマンドが有効化されている場合は最大 25 文字、service password-encryption コマンドが有効化されていない場合は最大 81 文字を指定できます。この文字列には、スペースも含め、あらゆる英数字を使用できます。

（注） 最初の文字を数値にはできません。数字-スペース-任意の文字の形式でパスワードを指定することはできません。数字の後にスペースを使用すると、認証に失敗する原因となることがあります。

ステップ 18 BGP ネイバーに送信する Community 属性を指定します。

neighbor {ip-address} send-community[both|standard|extended]

例：

```
ciscoasa(config-router-af)# neighbor 10.86.118.12 send-community
```

- （オプション）both キーワード：標準コミュニティと拡張コミュニティの両方が送信されます。

- （オプション）standard キーワード：標準コミュニティのみ送信されます。
- （オプション）extended キーワード：拡張コミュニティのみ送信されます。

ステップ 19 ルータを BGP スピーキング ネイバーまたはピア グループのネクスト ホップとして設定します。

neighbor {ip-address}next-hop-self

例：

```
ciscoasa(config-router-af)# neighbor 10.86.118.12 next-hop-self
```

ステップ 20 直接接続されていないネットワーク上の外部ピアからの BGP 接続を受け入れ、またそのピアへの BGP 接続を試みます。

neighbor {ip-address} ebgp-multihop [ttl]

例：

```
ciscoasa(config-router-af)# neighbor 10.86.118.12 ebgp-multihop 5
```

引数 ttl には、1 ～ 255 ホップの範囲の存続可能時間を指定します。

ステップ 21 ループバック インターフェイスを使用するシングル ホップ ピアと eBGP ピアリング セッションを確立するための接続確認をディセーブルにします。

neighbor {ip-address} disable-connected-check

例：

```
ciscoasa(config-router-af)# neighbor 10.86.118.12 disable-connected-check
```

ステップ 22 BGP ピアリング セッションを保護し、2 つの外部 BGP （eBGP）ピアを区切るホップの最大数を設定します。

neighbor ip-addressttl-security hops hop-count

例：

```
ciscoasa(config-router-af)# neighbor 10.86.118.12 ttl-security hops 15
```

引数 hop-count は、eBGP ピアを区切るホップの数です。TTL 値は、設定された hop-count 引数に基づいてルータにより計算されます。有効値は 1 ～ 254 です。

ステップ 23 ネイバー接続に重みを割り当てます。

neighbor {ip-address} weight number

例：

```
ciscoasa(config-router-af)# neighbor 10.86.118.12 weight 30
```

引数 number は、ネイバー接続に割り当てる重みです。有効値は、0 ～ 65535 です。

ステップ 24 特定の BGP バージョンだけを受け入れるように ASA を設定します。

neighbor {ip-address} version number

例：

```
ciscoasa(config-router-af)# neighbor 10.86.118.12 version 4
```

引数 number には、BGP バージョン番号を指定します。バージョンを 2 に設定すると、指定されたネイバーとの間でバージョン 2 だけが使用されます。デフォルトでは、バージョン 4 が使用され、要求された場合は動的にネゴシエートしてバージョン 2 に下がります。

ステップ 25 BGP セッションの TCP トランスポート セッション オプションをイネーブルにします。

neighbor {ip-address} transport {connection-mode{active|passive}| path-mtu-discovery[disable]}

例：

```
ciscoasa(config-router-af)# neighbor 10.86.118.12 transport path-mtu-discovery
```

- connection-mode：接続のタイプ（active または passive）。
- path-mtu-discovery：TCP トランスポート パスの最大伝送ユニット（MTU）ディスカバリを有効にします。TCP パス MTU ディスカバリは、デフォルトではイネーブルです。
- （オプション）disable：TCP パス MTU ディスカバリを無効にします。

ステップ 26 External Border Gateway Protocol（eBGP）ネイバーから受信したルートの AS_path 属性をカスタマイズします。

neighbor {ip-address} local-as [autonomous-system-number[no-prepend]]

例：

```
ciscoasa(config-router-af)# neighbor 10.86.118.12 local-as 5 no-prepend replace-as
```

- （オプション）autonomous-system-number：AS_path 属性の前に追加する自律システムの番号。この引数の値の範囲は、1 ～ 4294967295 または 1.0 ～ XX.YY の有効な任意の自律システム番号です。
- （オプション）no-prepend：eBGP ネイバーから受信したルートの前にローカル自律システム番号を追加しません。

IPv4 ネットワークの設定

ここでは、BGP ルーティング プロセスによってアドバタイズされるネットワークを定義するために必要な手順について説明します。

手順

ステップ 1 BGP ルーティング プロセスをイネーブルにし、ASA をルータ コンフィギュレーション モードにします。

router bgp autonomous-num

例：

```
ciscoasa(config)# router bgp 2
```

ステップ 2 アドレス ファミリ コンフィギュレーション モードを開始し、標準 IPv4 アドレス プレフィックスを使用するルーティング セッションを設定します。

address-family ipv4 [unicast]

キーワード unicast では、IPv4 ユニキャスト アドレス プレフィックスを指定します。これは、指定されていない場合でもデフォルト値になります。

ステップ 3 BGP ルーティング プロセスによってアドバタイズされるネットワークを指定します。

network {network-number [mask network-mask]}[route-map map-tag]

例：

```
ciscoasa(config-router-af)# network 10.86.118.13 mask 255.255.255.255 route-map example1
```

- network-number：BGP がアドバタイズするネットワーク。
- （オプション）network-mask：マスク アドレスを持つネットワーク マスクまたはサブネットワーク マスク。
- （オプション）map-tag：設定されているルート マップの ID。ルート マップは、アドバタイズされるネットワークをフィルタリングするために調べる必要があります。この値を指定しない場合、すべてのネットワークがアドバタイズされます。

IPv4 再配布の設定

ここでは、別のルーティング ドメインから BGP にルートを再配布する条件を定義するために必要な手順について説明します。

手順

ステップ 1 BGP ルーティング プロセスをイネーブルにし、ASA をルータ コンフィギュレーション モードにします。

router bgp autonomous-num

例：

```
ciscoasa(config)# router bgp 2
```

ステップ 2 アドレス ファミリ コンフィギュレーション モードを開始し、標準 IPv4 アドレス プレフィックスを使用するルーティング セッションを設定します。

address-family ipv4 [unicast]

例：

```
ciscoasa(config-router)# address-family ipv4[unicast]
```

キーワード unicast では、IPv4 ユニキャスト アドレス プレフィックスを指定します。これは、指定されていない場合でもデフォルト値になります。

ステップ 3 別のルーティング ドメインから BGP 自律システムにルートを再配布します。

redistribute protocol [process-id] [metric] [route-map [map-tag]]

例：

```
ciscoasa(config-router-af)# redistribute ospf 2 route-map example1 match external
```

- protocol：ルートの再配布元となるソース プロトコル。Connected、EIGRP、OSPF、RIP または Static のいずれかを指定できます。
- （オプション）process-id：特定のルーティング プロセスの名前。
- （オプション）metric：再配布されるルートのメトリック。
- （オプション）map-tag：設定されているルート マップの ID。

（注） ルートマップは、再配布されるネットワークをフィルタリングするために調べる必要があります。この値を指定しない場合、すべてのネットワークが再配布されます。

IPv4 ルート注入の設定

ここでは、条件に応じて BGP ルーティング テーブルに注入されるルートを定義するために必要な手順について説明します。

手順

ステップ 1 BGP ルーティング プロセスをイネーブルにし、ASA をルータ コンフィギュレーション モードにします。

router bgp autonomous-num

例：

```
ciscoasa(config)# router bgp 2
```

ステップ 2 アドレス ファミリ コンフィギュレーション モードを開始し、標準 IPv4 アドレス プレフィックスを使用するルーティング セッションを設定します。

address-family ipv4 [unicast]

例：

```
ciscoasa(config-router)# address-family ipv4[unicast]
```

キーワード unicast では、IPv4 ユニキャスト アドレス プレフィックスを指定します。これは、指定されていない場合でもデフォルト値になります。

ステップ 3 BGP ルーティング テーブルに固有性の強いルートを注入するよう条件付きルート注入を設定します。

bgp inject-map inject-map exist-map exist-map [copy-attributes]

例：

```
ciscoasa(config-router-af)# bgp inject-map example1 exist-map example2 copy-attributes
```

- inject-map：ローカル BGP ルーティング テーブルに注入するプレフィックスを指定するルート マップの名前。
- exist-map：BGP スピーカーが追跡するプレフィックスを含むルート マップの名前。
- （オプション）copy-attributes：集約ルートの属性を継承するよう注入されたルートを設定します。

IPv6 アドレス ファミリの設定

BGP の IPv6 設定は、BGP 設定セットアップ内の IPv6 ファミリ オプションから指定できます。IPv6 ファミリ セクションには、一般設定、集約アドレスの設定、ネイバー設定のサブセクションが含まれます。これらの各サブセクションを使用して、IPv6 ファミリに固有のパラメータをカスタマイズすることができます。

ここでは、BGP IPv6 ファミリの設定をカスタマイズする方法について説明します。

IPv6 ファミリの一般設定

ここでは、一般的な IPv6 の設定に必要な手順を説明します。

手順

ステップ 1 BGP ルーティング プロセスをイネーブルにし、ルータをルータ コンフィギュレーション モードにします。

router bgp autonomous-num

例：

```
ciscoasa(config)# router bgp 2
```

ステップ 2 アドレス ファミリ コンフィギュレーション モードを開始し、標準 IPv6 アドレス プレフィックスを使用するルーティング セッションを設定します。

address-family ipv6 [unicast]

ステップ 3 BGP ルートのアドミニストレーティブ ディスタンスを設定します。

distance bgp external-distance internal-distance local-distance

例：

```
ciscoasa(config-router-af)# distance bgp 80 180 180
```

- external-distance：外部 BGP ルートのアドミニストレーティブ ディスタンス。ルートは、外部自律システムから学習された場合は外部になります。この引数の値の範囲は 1 ～ 255 です。
- internal-distance：内部 BGP ルートのアドミニストレーティブ ディスタンス。ルートは、ローカル自律システムのピアから学習された場合は内部です。この引数の値の範囲は 1 ～ 255 です。
- local-distance：ローカル BGP ルートのアドミニストレーティブ ディスタンス。ローカル ルートは、別のプロセスから再配布されているルータまたはネットワークの、多くの場合バック ドアとして、ネットワーク ルータ コンフィギュレーション コマンドによりリストされるネットワークです。この引数の値の範囲は 1 ～ 255 です。

ステップ 4 （オプション）デフォルト ルート（ネットワーク 0.0.0.0）を配布するように BGP ルーティング プロセスを設定します。

default-information originate

ステップ 5 （オプション）ルーティング情報ベース（RIB）にインストールされていないルートのアドバタイズメントを抑制します。

bgp suppress-inactive

ステップ 6 BGP と Interior Gateway Protocol（IGP）システム間で同期します。

同期

ステップ 7 OSPF などの IGP への iBGP の再配布を設定します。

bgp redistribute-internal

ステップ 8 ネクスト ホップの検証用に BGP ルータのスキャン間隔を設定します。

bgp scan-time scanner-interval

例：

```
ciscoasa(config-router-af)# bgp scan-time 15
```

scanner-interval 引数の有効な値は 5 ～ 60 秒です。デフォルトは 60 秒です。

ステップ 9 ルーティング テーブルにインストールできる並列 iBGP ルートの最大数を制御します。

maximum-paths {number_of_paths|ibgp number_of_paths}

例：

```
ciscoasa(config-router-af)# maximum-paths ibgp 2
```

number_of_paths 引数の有効な値は 1 ～ 8 です。

ibgp キーワードを使用しない場合、number_of_paths 引数は、並列 EBGP ルートの最大数を制御します。

IPv6 ファミリ集約アドレスの設定

ここでは、特定のルートの 1 つのルートへの集約を定義するために必要な手順について説明します。

手順

ステップ 1 BGP ルーティング プロセスをイネーブルにし、ASA をルータ コンフィギュレーション モードにします。

router bgp autonomous-num

例：

```
ciscoasa(config)# router bgp 2
```

ステップ 2 アドレス ファミリ コンフィギュレーション モードを開始し、標準 IPv6 アドレス プレフィックスを使用するルーティング セッションを設定します。

address-family ipv6 unicast

ステップ 3 BGP データベースで集約エントリを作成します。

aggregate-address ipv6-address/cidr [as-set][summary-only][suppress-map map-name][advertise-map ipv6-map-name][attribute-map map-name]

例：

```
ciscoasa(config-router-af) aggregate-address 2000::1/8 summary-only
```

- address：集約 IPv6 アドレス。
- （オプション）as-set：自律システムの設定パス情報を生成します。
- （オプション）summary-only：アップデートから固有性の強いルートをすべてフィルタリングします。
- （オプション）suppress-map map-name：抑制するルートを選択するために使用するルートマップの名前を指定します。
- （オプション）advertise-map map-name：AS_SET 発信コミュニティを作成するためのルートを選択するために使用するルート マップの名前を指定します。
- （オプション）attribute-map map-name：集約ルートの属性を設定するために使用するルート マップの名前を指定します。

ステップ 4 BGP ルートが集約される間隔を設定します。

bgp aggregate-timer seconds

例：

```
ciscoasa(config-router-af)bgp aggregate-timer 20
```

IPv6 ファミリの BGP ネイバーの設定

ここでは、BGP ネイバーおよびネイバー設定を定義するために必要な手順について説明します。

手順

ステップ 1 BGP ルーティング プロセスをイネーブルにし、ルータをルータ コンフィギュレーション モードにします。

router bgp autonomous-num

例：

```
ciscoasa(config)# router bgp 2
```

ステップ 2 アドレス ファミリ コンフィギュレーション モードを開始し、標準 IPv6 アドレス プレフィックスを使用するルーティング セッションを設定します。

address-family ipv6 [unicast]

ステップ 3 エントリを BGP ネイバー テーブルに追加します。

neighbor ipv6-address remote-as autonomous-number

例：

```
ciscoasa(config-router-af)# neighbor 2000::1/8 remote-as 3
```

引数 ipv6-address には、指定したネットワークに到達するために使用できるネクスト ホップの IPv6 アドレスを指定します。ネクスト ホップの IPv6 アドレスは直接接続しないようにする必要があります。直接接続されたネクスト ホップの IPv6 アドレスを検出するために再帰が実行されるためです。インターフェイス タイプおよびインターフェイス番号を指定すると、パケットの出力先のネクスト ホップの IPv6 アドレスを指定できます（オプション）。リンクローカル アドレスをネクストホップとして使用する場合は、インターフェイス タイプおよびインターフェイス番号を指定する必要があります（また、リンクローカル ネクスト ホップが隣接デバイスである必要があります）。

（注） この引数は、RFC 2373 に記述されている形式にする必要があります。コロン区切りの 16 ビット値を使用して、アドレスを 16 進数で指定します。

ステップ 4 （オプション）ネイバーまたはピア グループをディセーブルにします。

neighbor ipv6-address shutdown

例：

```
ciscoasa(config-router-af)# neighbor 2000::1/8 shutdown 3
```

ステップ 5 BGP ネイバーと情報を交換します。

neighbor ipv6-address activate

例：

```
ciscoasa(config-router-af)# neighbor 2000::1/8 activate
```

ステップ 6 着信ルートまたは発信ルートにルート マップを適用します。

neighbor {ipv6-address} route-map map-name {in|out}

例：

```
ciscoasa(config-router-af)# neighbor 2000::1 route-map example1 in
```

キーワード in を指定すると、ルート マップは着信ルートに適用されます。

キーワード out を指定すると、ルート マップは発信ルートに適用されます。

ステップ 7 プレフィックス リストで指定された BGP ネイバー情報を配布します。

neighbor {ipv6-address} prefix-list prefix-list-name {in|out}

例：

```
ciscoasa(config-router-af)# neighbor 2000::1 prefix-list NewPrefixList in
```

キーワード in は、プレフィックス リストがそのネイバーからの着信アドバタイズメントに適用されることを意味します。

キーワード out は、プレフィックス リストがそのネイバーへの発信アドバタイズメントに適用されることを意味します。

ステップ 8 フィルタ リストを設定します。

neighbor {ipv6-address} filter-list access-list-name {in|out}

例：

```
ciscoasa(config-router-af)# neighbor 2000::1 filter-list 5 in
```

- access-list-name：自律システム パスのアクセス リストの番号を指定します。ip as-path access-list コマンドを使用して、このアクセス リストを定義します。
- in：アクセス リストはそのネイバーからの着信アドバタイズメントに適用されます。
- out：アクセス リストはそのネイバーへの発信アドバタイズメントに適用されます。

ステップ 9 ネイバーから受信できるプレフィックスの数を制御します。

neighbor {ipv6-address} maximum-prefix maximum [threshold][restart restart interval][warning-only]

例：

```
ciscoasa(config-router-af)# neighbor 2000::1 maximum-prefix 7 75 restart 12
```

- maximum：このネイバーからの許可される最大プレフィックス数。
- （オプション）threshold：最大数の何パーセントになったらルータが警告メッセージの生成を開始するかを指定する整数。指定できる範囲は 1 ～ 100 です。デフォルト値は 75（%）です。
- （オプション）restart interval：BGP ネイバーが再起動するまでの時間を指定する整数値（分）。
- （オプション）warning-only：プレフィックスの最大数を超えた場合に、ピアリングを終了する代わりに、ルータでログ メッセージを生成できます。

ステップ 10 BGP スピーカー（ローカル ルータ）にネイバーへのデフォルト ルート 0.0.0.0 の送信を許可して、このルートがデフォルト ルートとして使用されるようにします。

neighbor {ipv6-address} default-originate [route-map map-name]

例：

```
ciscoasa(config-router-af)# neighbor 2000::1 default-originate route-map example1
```

引数 map-name はルート マップの名前です。ルート マップにより、ルート 0.0.0.0 が条件に応じて注入されます。

ステップ 11 BGP ルーティング アップデートの最小送信間隔を設定します。

neighbor {ipv6-address} advertisement-interval seconds

例：

```
ciscoasa(config-router-af)# neighbor 2000::1 advertisement-interval 15
```

引数 seconds は時間（秒）です。0 ～ 600 の範囲の値を指定できます。

ステップ 12 プライベート自律システム番号を発信ルーティング アップデートから削除します。

neighbor {ipv6-address} remove-private-as

例：

```
ciscoasa(config-router-af)# neighbor 2000::1 remove-private-as
```

ステップ 13 設定されているルート マップと一致する BGP テーブル内のルートをアドバタイズします。

neighbor {ipv6-address} advertise-map map-name {exist-map map-name |non-exist-map map-name}[check-all-paths]

例：

```
ciscoasa(config-router-af)# neighbor 2000::1 advertise-map MAP1 exist-map MAP2
```

- advertise-map map name：exist-map または non-exist-map の条件に一致した場合にアドバタイズされるルート マップの名前。
- exist-map map name：advertise-map のルートがアドバタイズされるかどうかを判断するために BGP テーブル内のルートと比較される exist-map の名前。
- non-exist-map map name：advertise-map のルートがアドバタイズされるかどうかを判断するために BGP テーブル内のルートと比較される non-exist-map の名前。
- （オプション）check all paths：BGP テーブル内のプレフィックスを持つ exist-map によるすべてのパスのチェックを有効化します。

ステップ 14 特定の BGP ピアまたは BGP ピア グループのタイマーを設定します。

neighbor {ipv6-address} timers keepalive holdtime min holdtime

例：

```
ciscoasa(config-router-af)# neighbor 2000::1 timers 15 20 12
```

- keepalive：ASA がキープアライブ メッセージをピアに送信する頻度（秒）。デフォルトは 60 秒です。有効値は、0 ～ 65535 です。

- holdtime：キープアライブ メッセージを受信できない状態が継続して、ピアがデッドであると ASA が宣言するまでの時間（秒）。デフォルト値は 180 秒です。
- min holdtime：キープアライブ メッセージを受信できない状態が継続して、ピアがデッドであると ASA が宣言するまでの最小時間（秒）。

ステップ 15 2 つの BGP ピア間の TCP 接続で Message Digest 5（MD5）認証をイネーブルにします。

neighbor {ipv6-address} password string

例：

```
ciscoasa(config-router-af)# neighbor 2000::1 password test
```

引数 string は大文字と小文字を区別するパスワードで、service password-encryption コマンドが有効化されている場合は最大 25 文字、service password-encryption コマンドが有効化されていない場合は最大 81 文字を指定できます。この文字列には、スペースも含め、あらゆる英数字を使用できます。

（注） 最初の文字を数値にはできません。数字-スペース-任意の文字の形式でパスワードを指定することはできません。数字の後にスペースを使用すると、認証に失敗する原因となることがあります。

ステップ 16 BGP ネイバーに送信する Community 属性を指定します。

neighbor {ipv6-address} send-community [standard]

例：

```
ciscoasa(config-router-af)# neighbor 2000::1 send-community
```

（オプション）standard キーワード：標準コミュニティのみ送信されます。

ステップ 17 ルータを BGP スピーキング ネイバーまたはピア グループのネクスト ホップとして設定します。

neighbor {ipv6-address}next-hop-self

例：

```
ciscoasa(config-router-af)# neighbor 2000::1 next-hop-self
```

ステップ 18 直接接続されていないネットワーク上の外部ピアからの BGP 接続を受け入れ、またそのピアへの BGP 接続を試みます。

neighbor {ipv6-address} ebgp-multihop [ttl]

例：

```
ciscoasa(config-router-af)# neighbor 2000::1 ebgp-multihop 5
```

引数 ttl には、1 ～ 255 ホップの範囲の存続可能時間を指定します。

ステップ 19 ループバック インターフェイスを使用するシングル ホップ ピアと eBGP ピアリング セッションを確立するための接続確認をディセーブルにします。

neighbor {ipv6-address} disable-connected-check

例：

```
ciscoasa(config-router-af)# neighbor 2000::1 disable-connected-check
```

ステップ 20 BGP ピアリング セッションを保護し、2 つの外部 BGP （eBGP）ピアを区切るホップの最大数を設定します。

neighbor {ipv6-address} ttl-security hops hop-count

例：

```
ciscoasa(config-router-af)# neighbor 10.86.118.12 ttl-security hops 15
```

引数 hop-count は、eBGP ピアを区切るホップの数です。TTL 値は、設定された hop-count 引数に基づいてルータにより計算されます。有効値は 1 ～ 254 です。

ステップ 21 ネイバー接続に重みを割り当てます。

neighbor {ipv6-address} weight number

例：

```
ciscoasa(config-router-af)# neighbor 2000::1 weight 30
```

引数 number は、ネイバー接続に割り当てる重みです。有効値は、0 ～ 65535 です。

ステップ 22 特定の BGP バージョンだけを受け入れるように ASA を設定します。

neighbor {ipv6-address} version number

例：

```
ciscoasa(config-router-af)# neighbor 2000::1 version 4
```

引数 number には、BGP バージョン番号を指定します。デフォルトはバージョン 4 です。現在は、BGP バージョン 4 のみがサポートされます。

ステップ 23 BGP セッションの TCP トランスポート セッション オプションをイネーブルにします。

neighbor {ipv6-address} transport {connection-mode{active|passive}| path-mtu-discovery[disable]}

例：

```
ciscoasa(config-router-af)# neighbor 2000::1 transport connection-mode active
```

- connection-mode：接続のタイプ（active または passive）。

- path-mtu-discovery：TCP トランスポート パスの最大伝送ユニット（MTU）ディスカバリを有効にします。TCP パス MTU ディスカバリは、デフォルトではイネーブルです。
- （オプション）disable：TCP パス MTU ディスカバリを無効にします。

ステップ 24 External Border Gateway Protocol（eBGP）ネイバーから受信したルートの AS_path 属性をカスタマイズします。

neighbor {ipv6-address} local-as [autonomous-system-number[no-prepend]]

例：

```
ciscoasa(config-router-af)# neighbor 10.86.118.12 local-as 5 no-prepend replace-as
```

- （オプション）autonomous-system-number：AS_path 属性の前に追加する自律システムの番号。この引数の値の範囲は、1 ～ 4294967295 または 1.0 ～ XX.YY の有効な任意の自律システム番号です。
- （オプション）no-prepend：eBGP ネイバーから受信したルートの前にローカル自律システム番号を追加しません。

注意 BGP は、ネットワーク到着可能性情報を維持し、ルーティング ループを防ぐために、ルートが通過する各 BGP ネットワークから自律システム番号をプリペンドします。このコマンドは、自律システムの移行のためだけに設定する必要があり、遷移が完了した後設定解除する必要があります。この手順は、経験豊富なネットワーク オペレータだけが行うべきものです。不適切な設定によってルーティング ループが作成される可能性があります。

IPv6 ネットワークの設定

ここでは、BGP ルーティング プロセスによってアドバタイズされるネットワークを定義するために必要な手順について説明します。

手順

ステップ 1 BGP ルーティング プロセスをイネーブルにし、ASA をルータ コンフィギュレーション モードにします。

router bgp *autonomous-num*

例：

```
ciscoasa(config)# router bgp 2
```

ステップ 2 アドレス ファミリ コンフィギュレーション モードを開始し、標準 IPv6 アドレス プレフィックスを使用するルーティング セッションを設定します。

address-family ipv6 [unicast]

ステップ 3 BGP ルーティング プロセスによってアドバタイズされるネットワークを指定します。

network *ipv6_prefix*/*prefix_length* [**route-map** *route_map_name*]

例：

```
ciscoasa(config-router-af)# network 2001:1/64 route-map test_route_map
```

- *ipv6 network*/*prefix_length*：BGP がアドバタイズするネットワーク。
- （オプション）**route-map** *name*：設定されているルート マップの ID。ルート マップは、アドバタイズされるネットワークをフィルタリングするために調べる必要があります。この値を指定しない場合、すべてのネットワークがアドバタイズされます。

IPv6 再配布の設定

ここでは、別のルーティング ドメインから BGP にルートを再配布する条件を定義するために必要な手順について説明します。

手順

ステップ 1 BGP ルーティング プロセスをイネーブルにし、ASA をルータ コンフィギュレーション モードにします。

router bgp autonomous-num

例：

```
ciscoasa(config)# router bgp 2
```

ステップ 2 アドレス ファミリ コンフィギュレーション モードを開始し、標準 IPv6 アドレス プレフィックスを使用するルーティング セッションを設定します。

address-family ipv6 [unicast]

例：

```
ciscoasa(config-router)# address-family ipv6[unicast]
```

ステップ 3 別のルーティング ドメインから BGP 自律システムにルートを再配布します。

```
redistribute protocol [process-id][autonomous-num][metric metric value][match{internal|
 external1|external2|NSSA external 1|NSSA external 2}][route-map [map-tag]][subnets]
```

例：

```
ciscoasa(config-router-af)# redistribute ospf 2 route-map example1 match external
```

- protocol：ルートの再配布元となるソース プロトコル。Connected、EIGRP、OSPF、RIP または Static のいずれかを指定できます。
- （オプション）process-id：OSPF プロトコルの場合は、ルートの再配布元となる適切な OSPF プロセス ID です。この値により、ルーティング プロセスを識別します。この値は 0 以外の 10 進数で指定します。

  （注） この値は、その他のプロトコルでは自動入力されます。

- （オプション）metric metric value：同じルータ上で 1 つの OSPF プロセスから別の OSPF プロセスに再配布する場合、メトリック値を指定しないと、メトリックは 1 つのプロセスから他のプロセスへ存続します。他のプロセスを OSPF プロセスに再配布するときに、メトリック値を指定しない場合、デフォルトのメトリックは 20 です。デフォルト値は 0 です
- （オプション）match internal | external1 | external2 | NSSA external 1 | NSSA external 2：OSPF ルートが他のルーティング ドメインに再配布される条件を表します。次のいずれかを指定できます。
  - internal：特定の自律システムの内部にあるルート。
  - external 1：自律システムの外部だが、BGP に OSPF タイプ 1 外部ルートとしてインポートされるルート。
  - external 2：自律システムの外部だが、BGP に OSPF タイプ 2 外部ルートとしてインポートされるルート。
  - NSSA external 1：自律システムの外部だが、BGP に OSPF NSSA タイプ 1 外部ルートとしてインポートされるルート。
  - NSSA external 2：自律システムの外部だが、BGP に OSPF NSSA タイプ 2 外部ルートとしてインポートされるルート。
- （オプション）map-tag：設定されているルート マップの ID。

（注） ルートマップは、再配布されるネットワークをフィルタリングするために調べる必要があります。この値を指定しない場合、すべてのネットワークが再配布されます。

IPv6 ルート注入の設定

ここでは、条件に応じて BGP ルーティング テーブルに注入されるルートを定義するために必要な手順について説明します。

手順

ステップ 1 BGP ルーティング プロセスをイネーブルにし、ASA をルータ コンフィギュレーション モードにします。

router bgp autonomous-num

例：

```
ciscoasa(config)# router bgp 2
```

ステップ 2 アドレス ファミリ コンフィギュレーション モードを開始し、標準 IPv6 アドレス プレフィックスを使用するルーティング セッションを設定します。

address-family ipv6 [unicast]

例：

```
ciscoasa(config-router)# address-family ipv6 [unicast]
```

ステップ 3 BGP ルーティング テーブルに固有性の強いルートを注入するよう条件付きルート注入を設定します。

bgp inject-map inject-map exist-map exist-map [copy-attributes]

例：

```
ciscoasa(config-router-af)# bgp inject-map example1 exist-map example2 copy-attributes
```

- inject-map：ローカル BGP ルーティング テーブルに注入するプレフィックスを指定するルート マップの名前。
- exist-map：BGP スピーカーが追跡するプレフィックスを含むルート マップの名前。
- （オプション）copy-attributes：集約ルートの属性を継承するよう注入されたルートを設定します。

BGP のモニタリング

次のコマンドを使用して、BGP ルーティング プロセスをモニタできます。コマンド出力の例と説明については、コマンドリファレンスを参照してください。また、ネイバー変更メッセージとネイバー警告メッセージのロギングをディセーブルにできます。

さまざまなBGPルーティング統計情報をモニタするには、次のコマンドの1つを入力します。

- **show bgp** [ip-address [mask [longer-prefixes [injected] | shorter-prefixes [length]]]| prefix-list name | route-map name]

BGP ルーティング テーブル内のエントリを表示します。

- **show bgp** cidr-only

  ナチュラル ネットワーク マスク以外を使用するルート（つまり、クラスレス ドメイン間ルーティング（CIDR））を表示します。

- **show bgp community community-number [exact-match][no-advertise][no-export]**

  指定された BGP コミュニティに属するルートを表示します。

- **show bgp community-list community-list-name [exact-match]**

  BGP コミュニティ リストによって許可されたルートを表示します。

- **show bgp filter-list** *access-list-number*

  指定されたフィルタ リストと一致するルートを表示します。

- **show bgp injected-paths**

  BGP ルーティング テーブルに注入されたすべてのパスを表示します。

- **show bgp ipv4 unicast**

  ユニキャスト セッションの IPv4 BGP ルーティング テーブルのエントリを表示します。

- show bgp ipv6 unicast

  IPv6 の Border Gateway Protocol（BGP）ルーティング テーブルのエントリを表示します。

- show bgp ipv6 community

  指定された IPv6 Border Gateway Protocol（BGP）コミュニティに属するルートを表示します。

- show bgp ipv6 community-list

  IPv6 Border Gateway Protocol（BGP）コミュニティ リストによって許可されたルートを表示します。

- show bgp ipv6 filter-list

  指定された IPv6 フィルタ リストと一致するルートを表示します。

- show bgp ipv6 inconsistent-as

  整合性のない発信自律システムを使用している IPv6 Border Gateway Protocol（BGP）ルートを表示します。

- show bgp ipv6 neighbors

  ネイバーへの IPv6 Border Gateway Protocol（BGP）接続に関する情報を表示します。

- show bgp ipv6 paths

  データベース内のすべての IPv6 Border Gateway Protocol（BGP）パスを表示します。

- show bgp ipv6 prefix-list

  プレフィックス リストに一致するルートを表示します。

- show bgp ipv6 quote-regexp

  自律システム パスの正規表現と一致する IPv6 Border Gateway Protocol（BGP）ルートを引用符で囲まれた文字列として表示します。

- show bgp ipv6 regexp

  自律システム パスの正規表現と一致する IPv6 Border Gateway Protocol（BGP）ルートを表示します。

- show bgp ipv6 route-map

  ルーティング テーブルにインストールできなかった IPv6 Border Gateway Protocol（BGP）ルートを表示します。

- show bgp ipv6 summary

  すべての IPv6 Border Gateway Protocol（BGP）接続のステータスを表示します。

- show bgp neighbors ip_address

  ネイバーに対する BGP 接続と TCP 接続に関する情報を表示します。

- show bgp paths [LINE]

  データベース内のすべての BGP パスを表示します。

- show bgp pending-prefixes

  削除が保留されているプレフィックスを表示します。

- show bgp prefix-list prefix_list_name [WORD]

  指定のプレフィックス リストに一致するルートを表示します。

- show bgp regexp regexp

  自律システム パスの正規表現と一致するルートを表示します。

- show bgp replication [index-group | ip-address]

  BGP アップデート グループのアップデートのレプリケーション統計情報を表示します。

- show bgp rib-failure

  ルーティング情報ベース（RIB）テーブルにインストールできなかったBGPルートを表示します。

- show bgp route-map map-name

  指定されたルート マップに基づいて、BGP ルーティング テーブルのエントリを表示します。

- show bgp summary

  すべての BGP 接続のステータスを表示します。

- show bgp system-config

  マルチ コンテキスト モードでシステム コンテキスト固有の BGP 設定を表示します。

このコマンドは、マルチ コンテキスト モードのすべてのユーザ コンテキストで使用できます。

- show bgp update-group

  BGP アップデート グループに関する情報を表示します。

（注） BGP ログ メッセージを無効にするには、ルータ コンフィギュレーション モードで **no bgp log-neighbor-changes** コマンドを入力します。これにより、ネイバー変更メッセージのロギングが無効になります。BGP ルーティング プロセスのルータ コンフィギュレーション モードでこのコマンドを入力します。デフォルトでは、ネイバー変更はログに記録されます。

BGP の例

次の例に、さまざまなオプションのプロセスを使用して BGPv4 をイネーブルにし、設定する方法を示します。

1. ルーティング プロトコル間のルートの再配布に対する条件を定義します。または、ポリシー ルーティングをイネーブルにします。

```
ciscoasa(config)# route-map mymap2 permit 10
```

2. 指定されたアクセス リストのいずれかによって渡されるルート アドレスまたは一致パケットを持つルートを再配布します。

```
ciscoasa(config-route-map)# match ip address acl_dmz1 acl_dmz2
```

3. ポリシー ルーティング用のルート マップの match 節を通過したパケットの送出先を指定します。

```
ciscoasa(config-route-map)# set ip next-hop peer address
```

4. グローバル コンフィギュレーション モードで BGP ルーティング プロセスをイネーブルにします。

```
ciscoasa(config)# router bgp 2
```

5. アドレス ファミリ コンフィギュレーション モードでローカル Border Gateway Protocol（BGP）ルーティング プロセスの固定ルータ ID を設定します。

```
ciscoasa(config)# address-family ipv4
ciscoasa(config-router-af)# bgp router-id 19.168.254.254
```

6. エントリを BGP ネイバー テーブルに追加します。

```
ciscoasa(config-router-af)# neighbor 10.108.0.0 remote-as 65
```

7. 着信ルートまたは発信ルートにルート マップを適用します。

```
ciscoasa(config-router-af)# neighbor 10.108.0.0 route-map mymap2 in
```

次の例に、さまざまなオプションのプロセスを使用して BGPv6 を有効にし、設定する方法を示します。

1. ルーティング プロトコル間のルートの再配布に対する条件を定義します。または、ポリシー ルーティングをイネーブルにします。

```
ciscoasa(config)# route-map mymap1 permit 10
```

2. 指定されたアクセス リストのいずれかによって渡されるルート アドレスまたは一致パケットを持つルートを再配布します。

```
ciscoasa(config-route-map)# match ipv6 address acl_dmz1 acl_dmz2
```

3. ポリシー ルーティング用のルート マップの match 節を通過したパケットの送出先を指定します。

```
ciscoasa(config-route-map)# set ipv6 next-hop peer address
```

4. グローバル コンフィギュレーション モードで BGP ルーティング プロセスをイネーブルにします。

```
ciscoasa(config)# router bgp 2
```

5. アドレス ファミリ コンフィギュレーション モードでローカル Border Gateway Protocol（BGP）ルーティング プロセスの固定ルータ ID を設定します。

```
ciscoasa(config)# address-family ipv4
ciscoasa(config-router-af)# bgp router-id 19.168.254.254
```

6. アドレス ファミリ コンフィギュレーション モードを開始し、標準 IPv6 アドレス プレフィックスを使用するルーティング セッションを設定します。

```
address-family ipv6 [unicast]
```

7. エントリを BGP ネイバー テーブルに追加します。

```
ciscoasa(config-router-af)# neighbor 2001:DB8:0:CC00::1 remote-as 64600
```

8. 着信ルートまたは発信ルートにルート マップを適用します。

```
ciscoasa(config-router-af)# neighbor 2001:DB8:0:CC00::1 route-map mymap1 in
```

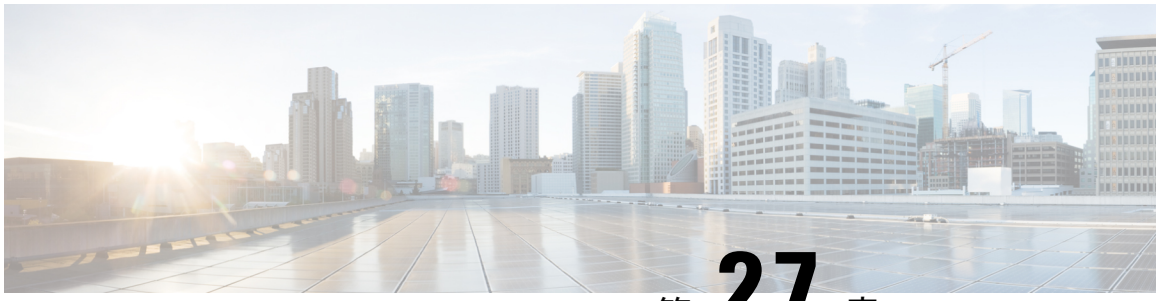
BGP の履歴

表 *27 : BGP* の各機能の履歴

機能名	プラットフォーム リリース	機能情報
BGP のサポート	9.2(1)	

機能名	プラットフォーム リリース	機能情報
		Border Gateway Protocol を使用した、データのルーティング、認証の実行、およびルーティング情報の再配布とモニタについて、サポートが追加されました。 次のコマンドが導入されました。**router bgp**、**bgp maxas-limitbgp maxas-limit**、**bgp log-neighbor-changes**、**bgp transport path-mtu-discovery**、**bgp fast-external-fallover**、**bgp enforce-first-as**、**bgp asnotation dot**、**timers bgp**、**bgp default local-preference**、**bgp always-compare-med**、**bgp bestpath compare-routerid**、**bgp deterministic-med**、**bgp bestpath med missing-as-worst**、**policy-list**、**match as-path**、**match community**、**match metric**、**match tag**、**as-path access-list**、**community-list**、**address-family ipv4**、**bgp router-id**、**distance bgp**、**table-map**、**bgp suppress-inactive**、**bgp redistribute-internal**、**bgp scan-time**、**bgp nexthop**、**aggregate-address**、**neighbor**、**bgp inject-map**、**show bgp**、**show bgp cidr-only**、**show bgp all community**、**show bgp all neighbors**、**show bgp community**、**show bgp community-list**、**show bgp filter-list**、**show bgp injected-paths**、**show bgp ipv4 unicast**、**show bgp neighbors**、**show bgp paths**、**show bgp pending-prefixes**、**show bgp prefix-list**、**show bgp regexp**、**show bgp replication**、**show bgp rib-failure**、 **show bgp route-map**、**show bgp summary**、**show bgp system-config**、**show bgp update-group**、**clear route network**、**maximum-path**、 **network**。 次のコマンドが変更されました。**show route**、**show route summary**、**show running-config router**、**clear config**

機能名	プラットフォーム リリース	機能情報
		router、**clear route all**、**timers lsa arrival**、**timers pacing**、**timers throttle**、**redistribute bgp**。
ASA クラスタリングに対する BGP のサポート	9.3(1)	L2 および L3 クラスタリングのサポートが追加されました。 次のコマンドが導入されました。bgp router-id clusterpool
ノンストップ フォワーディングに対する BGP のサポート	9.3(1)	ノンストップ フォワーディングのサポートが追加されました。 次のコマンドが導入されました。bgp graceful-restart、neighbor ha-mode graceful-restart
アドバタイズされたマップに対する BGP のサポート	9.3(1)	アドバタイズされたマップに対する BGPv4 のサポートが追加されました。 次のコマンドが導入されました。neighbor advertise-map
IPv6 に対する BGP のサポート	9.3(2)	IPv6 のサポートが追加されました。 次のコマンドが導入されました。address-family ipv6、ipv6 prefix-list、ipv6 prefix-list description、ipv6 prefix-list sequence-number、match ipv6 next-hop、match ipv6 route-source、match ipv6-address prefix-list、set ipv6-address prefix-list、set ipv6 next-hop、set ipv6 next-hop peer-address 次のコマンドが変更されました。bgp router-id



第 27 章

OSPF

この章では、Open Shortest Path First（OSPF）ルーティング プロトコルを使用してデータをルーティングし、認証を実行し、ルーティング情報を再配布するように Cisco ASA を設定する方法について説明します。

OSPF の概要

OSPF は、パスの選択に距離ベクトル型ではなくリンク ステートを使用する Interior Gateway Routing Protocol（IGRP）です。OSPF は、ルーティング テーブル アップデートではなく、リンクステート アドバタイズメントを伝搬します。ルーティング テーブル全体ではなく LSA だけが交換されるため、OSPF ネットワークは RIP ネットワークよりも迅速に収束します。

OSPF は、リンクステート アルゴリズムを使用して、すべての既知の宛先までの最短パスを構築および計算します。OSPF エリア内の各ルータには、ルータが使用可能なインターフェイスと到達可能なネイバーそれぞれのリストである同一のリンクステート データベースが置かれています。

RIP に比べると OSPF は次の点で有利です。

- OSPF のリンクステート データベースのアップデート送信は RIP ほど頻繁ではありません。また、古くなった情報がタイムアウトしたときに、リンクステート データベースは徐々にアップデートされるのではなく、瞬時にアップデートされます。
- ルーティング決定はコストに基づいて行われます。これは、特定のインターフェイスを介してパケットを送信するためにオーバーヘッドが必要であることを示しています。ASA は、インターフェイスのコストをリンク帯域幅に基づいて計算し、宛先までのホップ数は使用しません。コストは優先パスを指定するために設定できます。

最短パス優先アルゴリズムの欠点は、CPU サイクルとメモリが大量に必要になることです。

ASA は、OSPF プロトコルの 2 つのプロセスを異なるセットのインターフェイス上で同時に実行できます。同じ IP アドレスを使用する複数のインターフェイス（NAT ではこのようなインターフェイスは共存可能ですが、OSPF ではアドレスの重複は許しません）があるときに、2 つのプロセスを実行する場合があります。あるいは、一方のプロセスを内部で実行しながら別のプロセスを外部で実行し、ルートのサブセットをこの2つのプロセス間で再配布する場合もあります。同様に、プライベート アドレスをパブリック アドレスから分離する必要がある場合もあります。

OSPF ルーティング プロセスには、別の OSPF ルーティング プロセスや RIP ルーティング プロセスから、またはOSPF対応インターフェイスに設定されているスタティック ルートおよび接続されているルートから、ルートを再配布できます。

ASAでは、次の OSPF の機能がサポートされています。

- エリア内ルート、エリア間ルート、および外部ルート（タイプ I とタイプ II）。
- 仮想リンク。
- LSA フラッディング。
- OSPF パケットの認証（パスワード認証と MD5 認証の両方）
- ASA の指定ルータまたは指定バックアップ ルータとしての設定。ASAは、ABR として設定することもできます。
- スタブ エリアと not so stubby エリア。
- エリア境界ルータのタイプ 3 LSA フィルタリング

OSPF は、MD5 とクリア テキスト ネイバー認証をサポートしています。OSPF と他のプロトコル（RIP など）の間のルート再配布は、攻撃者によるルーティング情報の悪用に使用される可能性があるため、できる限りすべてのルーティング プロトコルで認証を使用する必要があります。

NAT が使用されている場合、OSPF がパブリック エリアおよびプライベート エリアで動作している場合、またアドレス フィルタリングが必要な場合は、2 つの OSPF プロセス（1 つはパブリック エリア用、1 つはプライベート エリア用）を実行する必要があります。

複数のエリアにインターフェイスを持つルータは、エリア境界ルータ（ABR）と呼ばれます。ゲートウェイとして動作し、OSPF を使用しているルータと他のルーティング プロトコルを使

用しているルータの間でトラフィックを再配布するルータは、自律システム境界ルータ（ASBR）と呼ばれます。

ABR は LSA を使用して、使用可能なルータに関する情報を他の OSPF ルータに送信します。ABR タイプ 3 LSA フィルタリングを使用して、ABR として機能する ASA で、プライベート エリアとパブリック エリアを分けることができます。タイプ 3 LSA（エリア間ルート）は、プライベート ネットワークをアドバタイズしなくても NAT と OSPF を一緒に使用できるように、1 つのエリアから他のエリアにフィルタリングできます。

（注） フィルタリングできるのはタイプ 3 LSA だけです。プライベート ネットワーク内の ASBR として設定されている ASA は、プライベート ネットワークを記述するタイプ 5 LSA を送信しますが、これは AS 全体（パブリック エリアも含む）にフラッディングされます。

NAT が採用されているが、OSPF がパブリック エリアだけで実行されている場合は、パブリック ネットワークへのルートを、デフォルトまたはタイプ 5 AS 外部 LSA としてプライベート ネットワーク内で再配布できます。ただし、ASAにより保護されているプライベート ネットワークにはスタティック ルートを設定する必要があります。また、同一のASA インターフェイス上で、パブリック ネットワークとプライベート ネットワークを混在させることはできません。

ASAでは、2 つの OSPF ルーティング プロセス（1 つの RIP ルーティング プロセスと 1 つの EIGRP ルーティング プロセス）を同時に実行できます。

fast hello パケットに対する OSPF のサポート

fast hello パケットに対する OSPF のサポートには、1 秒未満のインターバルで hello パケットの送信を設定する方法が用意されています。このような設定により、Open Shortest Path First（OSPF）ネットワークでの統合がより迅速になります。

fast hello パケットに対する OSPF のサポートの前提条件

OSPF がネットワークですでに設定されているか、fast hello パケットに対する OSPF のサポートと同時に設定される必要があります。

fast hello パケットに対する OSPF のサポートについて

次に、fast hello パケットに関する OSPF のサポートと、OSPF fast hello パケットの利点について説明します。

OSPF Hello インターバルおよび dead 間隔

OSPF helloパケットとは、OSPFプロセスがネイバーとの接続を維持するためにOSPFネイバーに送信するパケットです。helloパケットは、設定可能なインターバル（秒単位）で送信されます。デフォルトのインターバルは、イーサネット リンクの場合 10 秒、ブロードキャスト以外のリンクの場合 30 秒です。helloパケットには、デッド インターバル中に受信したすべてのネイバーのリストが含まれます。デッドインターバルも設定可能なインターバル（秒単位）で送

信されます。デフォルトはhelloインターバルの値の4倍です。helloインターバルの値は、ネットワーク内ですべて同一にする必要があります。デッドインターバルの値も、ネットワーク内ですべて同一にする必要があります。

この2つのインターバルは、リンクが動作していることを示すことにより、接続を維持するために連携して機能します。ルータがデッド インターバル内にネイバーから hello パケットを受信しない場合、ルータはこのネイバーがダウンしていると判定します。

OSPF fast hello パケット

OSPF fast hello パケットとは、1 秒よりも短いインターバルで送信される hello パケットのことです。fast helloパケットを理解するには、OSPF helloパケットインターバルとデッドインターバルとの関係についてあらかじめ理解しておく必要があります。OSPF Helloインターバルおよび dead 間隔 （789 ページ）を参照してください。

OSPF fast hello パケットは、ospf dead-interval コマンドで設定されます。デッド インターバルは 1 秒に設定され、hello-multiplier の値は、その 1 秒間に送信する hello パケット数に設定されるため、1 秒未満の「fast」hello パケットになります。

インターフェイスでfast helloパケットが設定されている場合、このインターフェイスから送出される hello パケットでアドバタイズされる hello 間隔は 0 に設定されます。このインターフェイス経由で受信した hello パケットの hello 間隔は無視されます。

デッド インターバルは、1 つのセグメント上で一貫している必要があり、1 秒に設定するか（fast helloパケットの場合）、他の任意の値を設定します。デッドインターバル内に少なくとも 1 つの hello パケットが送信される限り、hello multiplier がセグメント全体で同じである必要はありません。

OSPF fast hello パケットの利点

OSPF fast helloパケット機能を利用すると、ネットワークがこの機能を使用しない場合よりも、短い時間で統合されます。この機能によって、失われたネイバーを1秒以内に検出できるようになります。この機能は、ネイバーの損失が Open System Interconnection（OSI）物理層またはデータ リンク層で検出されないことがあっても、特に LAN セグメントで有効です。

OSPFv2 および OSPFv3 間の実装の差異

OSPFv3 には、OSPFv2 との下位互換性はありません。OSPF を使用して、IPv4 および IPv6 トラフィックの両方をルーティングするには、OSPFv2 および OSPFv3 の両方を同時に実行する必要があります。これらは互いに共存しますが、相互に連携していません。

OSPFv3 では、次の追加機能が提供されます。

- リンクごとのプロトコル処理。
- アドレッシング セマンティックの削除。
- フラッディング スコープの追加。
- リンクごとの複数インスタンスのサポート。

- ネイバー探索およびその他の機能に対する IPv6 リンクローカル アドレスの使用。
- プレフィックスおよびプレフィックス長として表される LSA。
- 2 つの LSA タイプの追加。
- 未知の LSA タイプの処理。
- RFC-4552 で指定されている OSPFv3 ルーティング プロトコル トラフィックの IPsec ESP 標準を使用する認証サポート。

OSPF のガイドライン

コンテキスト モードのガイドライン

OSPFv2 は、シングル コンテキスト モードとマルチ コンテキスト モードをサポートしています。

- デフォルトでは、共有インターフェイス間でのマルチキャスト トラフィックのコンテキスト間交換がサポートされていないため、OSPFv2 インスタンスは共有インターフェイス間で相互に隣接関係を形成できません。ただし、OSPFv2 プロセスの OSPFv2 プロセス設定で静的ネイバー設定を使用すると、共有インターフェイスでの OSPFv2 ネイバーシップを形成できます。
- 個別のインターフェイスでのコンテキスト間 OSPFv2 がサポートされています。

OSPFv3 は、シングル モードのみをサポートしています。

ファイアウォール モードのガイドライン

OSPF は、ルーテッド ファイアウォール モードのみをサポートしています。OSPF は、トランスペアレント ファイアウォール モードをサポートしません。

フェールオーバー ガイドライン

OSPFv2 および OSPFv3 は、ステートフル フェールオーバー をサポートしています。

IPv6 のガイドライン

- OSPFv2 は IPv6 をサポートしません。
- OSPFv3 は IPv6 をサポートしています。
- OSPFv3 は、IPv6 を使用して認証を行います。
- ASA は、OSPFv3 ルートが最適なルートの場合、IPv6 RIB にこのルートをインストールします。
- OSPFv3 パケットは、**capture** コマンドの IPv6 ACL を使用してフィルタリングで除外できます。

クラスタリングのガイドライン

- OSPFv3 暗号化はサポートされていません。クラスタリング環境で OSPFv3 暗号化を設定しようとすると、エラー メッセージが表示されます。
- スパンド インターフェイス モードでは、ダイナミック ルーティングは管理専用インターフェイスではサポートされません。
- 個別インターフェイス モードで、OSPFv2 または OSPFv3 ネイバーとしてマスター ユニットおよびスレーブ ユニットが確立されていることを確認します。
- 個別インターフェイス モードでは、OSPFv2 との隣接関係は、マスターユニットの共有インターフェイスの 2 つのコンテキスト間でのみ確立できます。スタティック ネイバーの設定は、ポイントツーポイン リンクでのみサポートされます。したがって、インターフェイスで許可されるのは 1 つのネイバー ステートメントだけです。
- クラスタでマスター ロールの変更が発生した場合、次の挙動が発生します。
  - スパンド インターフェイス モードでは、ルータ プロセスはマスター ユニットでのみアクティブになり、スレーブ ユニットでは停止状態になります。コンフィギュレーションがマスターユニットと同期されているため、各クラスタ ユニットには同じルータ ID があります。その結果、隣接ルータはロール変更時のクラスタのルータ ID の変更を認識しません。
  - 個別インターフェイス モードでは、ルータ プロセスはすべての個別のクラスタ ユニットでアクティブになります。各クラスタ ユニットは設定されたクラスタ プールから独自の個別のルータ ID を選択します。クラスタでマスターシップ ロールが変更されても、ルーティング トポロジは変更されません。

マルチプロトコル ラベル スイッチング（MPLS）と OSPF のガイドライン

MPLS 設定ルータから送信されるリンク ステート（LS）アップデート パケットに、Opaque Type-10 リンクステート アドバタイズメント（LSA）が含まれており、この LSA に MPLS ヘッダーが含まれている場合、認証は失敗し、アプライアンスはアップデート パケットを確認せずにサイレントにドロップします。ピア ルータは確認応答を受信していないため、最終的にネイバー関係を終了します。

ネイバー関係の安定を維持するため、ASA の Opaque 機能を無効にします。

```
router ospf process_ID_number
no nsf ietf helper
no capability opaque
```

その他のガイドライン

- OSPFv2 および OSPFv3 は 1 つのインターフェイス上での複数インスタンスをサポートしています。
- OSPFv3 は、非クラスタ環境での ESP ヘッダーを介した暗号化をサポートしています。
- OSPFv3 は非ペイロード暗号化をサポートします。

- OSPFv2 は RFC 4811、4812 および 3623 でそれぞれ定義されている、Cisco NSF グレースフル リスタートおよびIETF NSF グレースフル リスタート メカニズムをサポートします。
- OSPFv3 は RFC 5187 で定義されているグレースフル リスタート メカニズムをサポートします。
- 配布可能なエリア内（タイプ 1）ルートの数は限られています。これらのルートでは、1 つのタイプ 1 LSA にすべてのプレフィックスが含まれています。システムではパケット サイズが 35 KB に制限されているため、3000 ルートの場合、パケットがこの制限を超過します。2900 本のタイプ 1 ルートが、サポートされる最大数であると考えてください。

OSPFv2 の設定

ここでは、ASA で OSPFv2 プロセスを有効化する方法について説明します。

OSPFv2 をイネーブルにした後、ルート マップを定義する必要があります。詳細については、ルート マップの定義（735 ページ）を参照してください。その後、デフォルト ルートを生成します。詳細については、スタティック ルートの設定（712 ページ）を参照してください。

OSPFv2 プロセスのルート マップを定義した後で、ニーズに合わせてカスタマイズできます。ASA 上で OSPFv2 プロセスをカスタマイズする方法については、OSPFv2 のカスタマイズ（796 ページ）を参照してください。

OSPFv2 をイネーブルにするには、OSPFv2 ルーティング プロセスを作成し、このルーティング プロセスに関連付ける IP アドレスの範囲を指定し、さらにその IP アドレスの範囲にエリア ID を割り当てる必要があります。

最大 2 つの OSPFv2 プロセス インスタンスをイネーブルにできます。各 OSPFv2 プロセスには、独自のエリアとネットワークが関連付けられます。

OSPFv2 をイネーブルにするには、次の手順を実行します。

手順

ステップ 1 OSPF ルーティング プロセスを作成します。

router ospf *process_id*

例：

```
ciscoasa(config)# router ospf 2
```

process_id 引数は、このルーティング プロセス内部で使用される識別子です。任意の正の整数が使用できます。この ID は内部専用のため、他のどのデバイス上の ID とも照合する必要はありません。最大 2 つのプロセスが使用できます。

ASA 上で OSPF プロセスが 1 つしか有効化されていないと、そのプロセスがデフォルトで選択されます。既存のエリアを編集する場合、OSPF プロセス ID を変更できません。

ステップ 2 OSPF を実行する IP アドレスを定義し、そのインターフェイスのエリア ID を定義します。

network *ip_address mask* **area** *area_id*

例：

```
ciscoasa(config)# router ospf 2
ciscoasa(config-rtr)# network 10.0.0.0 255.0.0.0 area 0
```

新しいエリアを追加する場合、そのエリア ID を入力します。このエリア ID には、10 進数か IP アドレスを指定できます。有効な 10 進値の範囲は、0 ～ 4294967295 です。既存のエリアを編集する場合、エリア ID は変更できません。

OSPFv2 ルータ ID の設定

OSPF ルータ ID は、OSPF データベース内の特定のデバイスを識別するために使用されます。OSPF システム内の 2 台のルータが同じルータ ID を持つことはできません。

ルータ ID が OSPF ルーティング プロセスで手動で設定されていない場合、ルータは論理インターフェイス（ループバック インターフェイス）の最も高い IP アドレスまたはアクティブ インターフェイスの最も高い IP アドレスから決定されたルータ ID を自動的に設定します。ルータ ID を設定すると、ルータに障害が発生するか、または OSPF プロセスがクリアされ、ネイバー関係が再確立されるまで、ネイバーは自動的に更新されません。

OSPF ルータ ID の手動設定

ここでは、ASA の OSPFv2 プロセスで router-id を手動で設定する方法について説明します。

手順

ステップ 1 固定ルータ ID を使用するには、**router-id** コマンドを使用します。

router-id *ip-address*

例：

```
ciscoasa(config-router)# router-id 193.168.3.3
```

ステップ 2 以前の OSPF ルータ ID の動作に戻すには、**no router-id** コマンドを使用します。

no router-id *ip-address*

例：

```
ciscoasa(config-router)# no router-id 193.168.3.3
```

移行中のルータ ID の挙動

ある ASA、たとえば ASA 1 から別の ASA、たとえば ASA 2 に OSPF 設定を移行すると、次のルータ ID 選択動作が見られます。

1. すべてのインターフェイスがシャットダウン モードの場合、ASA 2 は OSPF router-id に IP アドレスを使用しません。すべてのインターフェイスが「admin down」ステートまたはシャットダウン モードの場合に考えられる router-id の設定は次のとおりです。
   - ASA 2 に以前設定された router-id がない場合は、次のメッセージが表示されます。

     ```
     %OSPF: Router process 1 is not running, please configure a router-id
     ```

     最初のインターフェイスが起動すると、ASA 2 はこのインターフェイスの IP アドレスをルータ ID として取得します。
   - ASA 2 に router-id が以前設定されていて、「no router-id」コマンドが発行されたときにすべてのインターフェイスが「admin down」ステートになっていた場合、ASA 2 は古いルータ ID を使用します。ASA 2 は、「clear ospf process」コマンドが発行されるまで、起動されたインターフェイスの IP アドレスが変更されても、古いルータ ID を使用します。
2. ASA 2 に router-id が以前設定されていて、「no router-id」コマンドが発行されたときに少なくとも 1 つのインターフェイスが「admin down」ステートまたはシャットダウン モードになっていない場合、ASA 2 は新しいルータ ID を使用します。インターフェイスが「down/down」ステートの場合でも、ASA 2 はインターフェイスの IP アドレスから新しいルータ ID を使用します。

OSPF fast hello パケットの設定

ここでは、OSPF fast hello パケットを設定する方法について説明します。

手順

ステップ 1 インターフェイスを設定します。

interface *port-channel number*

例：

```
ciscoasa(config)# interface port-channel 10
```

number 引数は、ポートチャネル インターフェイスの番号を示します。

ステップ 2 少なくとも 1 個の hello パケットの受信が必要なインターバルを設定します。受信されなければ、ネイバーがダウンしていると判断されます。

ospf dead-interval minimal hello-multiplier *no.of times*

例：

```
ciscoasa(config-if)# ospf dead-interval minimal hell0-multiplier 5
ciscoasa
```

no.of times 引数は、毎秒送信される hello パケットの数を示します。有効な値は、3 ～ 20 です。

ここでは、minimal キーワードおよび hello-multiplier キーワードと値を指定することにより、fast hello パケットに対する OSPF のサポートがイネーブルになっています。multiplier キーワードが 5 に設定されているため、hello パケットが毎秒 5 回送信されます。

OSPFv2 のカスタマイズ

ここでは、OSPFv2 プロセスをカスタマイズする方法について説明します。

OSPFv2 へのルートの再配布

ASA は、OSPFv2 ルーティング プロセス間のルート再配布を制御できます。

（注） 指定されたルーティング プロトコルから、ターゲット ルーティング プロセスに再配布できるルートを定義することでルートを再配布する場合は、デフォルト ルートを最初に生成する必要があります。スタティック ルートの設定（712 ページ）を参照し、その後にルート マップの定義（735 ページ）に従ってルート マップを定義します。

スタティック ルート、接続されているルート、RIP ルート、または OSPFv2 ルートを OSPFv2 プロセスに再配布するには、次の手順を実行します。

手順

ステップ 1 OSPF ルーティング プロセスを作成します。

router ospf *process_id*

例：

```
ciscoasa(config)# router ospf 2
```

process_id 引数は、このルーティング プロセス内部で使用される識別子です。任意の正の整数が使用できます。この ID は内部専用のため、他のどのデバイス上の ID とも照合する必要はありません。最大 2 つのプロセスが使用できます。

ステップ 2 接続済みルートを OSPF ルーティング プロセスに再配布します。

redistribute connected [[**metric** *metric-value*] [**metric-type** {**type-1** | **type-2**}] [**tag** *tag_value*] [**subnets**] [**route-map** *map_name*]

例：

```
ciscoasa(config)# redistribute connected 5 type-1 route-map-practice
```

ステップ 3 スタティック ルートを OSPF ルーティング プロセスに再配布します。

redistribute static [**metric** *metric-value*] [**metric-type** {**type-1** | **type-2**}] [**tag** *tag_value*] [**subnets**] [**route-map** *map_name*

例：

```
ciscoasa(config)# redistribute static 5 type-1 route-map-practice
```

ステップ 4 ルートを OSPF ルーティング プロセスから別の OSPF ルーティング プロセスに再配布します。

redistribute ospf pid [**match {internal** | **external** [**1** | **2]** | **nssa-external** [**1** | **2**]}] [**metric** *metric-value*] [**metric-type** {**type-1** | **type-2**}] [**tag** *tag_value*] [**subnets**] [**route-map** *map_name*]

例：

```
ciscoasa(config)# route-map 1-to-2 permit
ciscoasa(config-route-map)# match metric 1
ciscoasa(config-route-map)# set metric 5
ciscoasa(config-route-map)# set metric-type type-1
ciscoasa(config-route-map)# router ospf 2
ciscoasa(config-rtr)# redistribute ospf 1 route-map 1-to-2
```

このコマンドの **match** オプションを使用して、ルート プロパティを照合および設定したり、ルート マップを使用したりできます。**subnets** オプションは、**route-map** コマンドで使用する場合と同じではありません。ルート マップと **redistribute** コマンドの **match** オプションの両方を使用する場合、これらは一致している必要があります。

この例では、ルートをメトリック 1 に照合することによる、OSPF プロセス 1 から OSPF プロセス 2 へのルートの再配布を示しています。ASA は、これらのルートをメトリック 5、メトリック タイプ 1 で外部 LSA として再配布します。

ステップ 5 ルートを RIP ルーティング プロセスから OSPF ルーティング プロセスに再配布します。

redistribute rip [**metric** *metric-value*] [**metric-type** {**type-1** | **type-2**}] [**tag** *tag_value*] [**subnets**] [**route-map** *map_name*]

例：

```
ciscoasa(config)# redistribute rip 5
ciscoasa(config-route-map)# match metric 1
```

```
ciscoasa(config-route-map)# set metric 5
ciscoasa(config-route-map)# set metric-type type-1
ciscoasa(config-rtr)# redistribute ospf 1 route-map 1-to-2
```

ステップ 6 ルートを EIGRP ルーティング プロセスから OSPF ルーティング プロセスに再配布します。

redistribute eigrp as-num [**metric** *metric-value*] [**metric-type** {**type-1** | **type-2**}] [**tag** *tag_value*] [**subnets**] [**route-map** *map_name*]

例：

```
ciscoasa(config)# redistribute eigrp 2
ciscoasa(config-route-map)# match metric 1
ciscoasa(config-route-map)# set metric 5
ciscoasa(config-route-map)# set metric-type type-1
ciscoasa(config-rtr)# redistribute ospf 1 route-map 1-to-2
```

OSPFv2 にルートを再配布する場合のルート集約の設定

他のプロトコルからのルートを OSPF に再配布する場合、各ルートは外部 LSA で個別にアドバタイズされます。その一方で、指定したネットワーク アドレスとマスクに含まれる再配布ルートすべてに対して 1 つのルートをアドバタイズするように ASA を設定することができます。この設定によって OSPF リンクステート データベースのサイズが小さくなります。

指定した IP アドレス マスク ペアと一致するルートは廃止できます。ルート マップで再配布を制御するために、タグ値を一致値として使用できます。

ルート サマリー アドレスの追加

ネットワーク アドレスとマスクに含まれる再配布ルートすべてに対して 1 つのサマリー ルートをアドバタイズするようにソフトウェアを設定するには、次の手順を実行します。

手順

ステップ 1 OSPF ルーティング プロセスを作成します。

router ospf *process_id*

例：

```
ciscoasa(config)# router ospf 1
```

process_id 引数は、このルーティング プロセス内部で使用される識別子です。任意の正の整数が使用できます。この ID は内部専用のため、他のどのデバイス上の ID とも照合する必要はありません。最大 2 つのプロセスが使用できます。

ステップ 2 サマリー アドレスを設定します。

summary-address *ip_address mask* [**not-advertise**] [tag *tag*]

例：

```
ciscoasa(config)# router ospf 1
ciscoasa(config-rtr)# summary-address 10.1.0.0 255.255.0.0
```

この例のサマリー アドレスの 10.1.0.0 には、10.1.1.0、10.1.2.0、10.1.3.0 などのアドレスが含まれます。外部のリンクステート アドバタイズメントでは、アドレス 10.1.0.0 だけがアドバタイズされます。

OSPFv2 エリア間のルート集約の設定

ルート集約は、アドバタイズされるアドレスを統合することです。この機能を実行すると、1 つのサマリー ルートがエリア境界ルータを通して他のエリアにアドバタイズされます。OSPF のエリア境界ルータは、ネットワークをある 1 つのエリアから別のエリアへとアドバタイズしていきます。あるエリアにおいて連続する複数のネットワーク番号が割り当てられている場合、指定された範囲に含まれるエリア内の個別のネットワークをすべて含むサマリー ルートをアドバタイズするようにエリア境界ルータを設定することができます。

ルート集約のアドレス範囲を定義するには、次の手順を実行します。

手順

ステップ 1 OSPF ルーティング プロセスを作成して、この OSPF プロセスのルータ コンフィギュレーション モードを開始します。

router ospf *process_id*

例：

```
ciscoasa(config)# router ospf 1
```

process_id 引数は、このルーティング プロセス内部で使用される識別子です。任意の正の整数が使用できます。この ID は内部専用のため、他のどのデバイス上の ID とも照合する必要はありません。最大 2 つのプロセスが使用できます。

ステップ 2 アドレス範囲を設定します。

area *area-id* range *ip-address mask* [**advertise** | **not-advertise**]

例：

```
ciscoasa(config-rtr)# area 17 range 12.1.0.0 255.255.0.0
```

この例では、アドレス範囲は OSPF エリア間で設定されます。

OSPFv2 インターフェイス パラメータの設定

必要に応じて一部のインターフェイス固有の OSPFv2 パラメータを変更できます。これらのパラメータを必ずしも変更する必要はありませんが、**ospf hello-interval**、**ospf dead-interval**、**ospf authentication-key** の各インターフェイス パラメータは、接続されているネットワーク内のすべてのルータで一致している必要があります。これらのパラメータを設定する場合は、ネットワーク上のすべてのルータで、コンフィギュレーションの値が矛盾していないことを確認してください。

OSPFv2 インターフェイス パラメータを設定するには、次の手順を実行します。

手順

ステップ 1 OSPF ルーティング プロセスを作成します。

router ospf*process-id*

例：

```
ciscoasa(config)# router ospf 2
```

process_id 引数は、このルーティング プロセス内部で使用される識別子で、任意の正の整数を使用できます。この ID は内部専用のため、他のどのデバイス上の ID とも照合する必要はありません。最大 2 つのプロセスが使用できます。

ステップ 2 OSPF を実行する IP アドレスを定義し、そのインターフェイスのエリア ID を定義します。

network*ip-address mask***area***area-id*

例：

```
ciscoasa(config)# router ospf 2
ciscoasa(config-rtr)# network 10.0.0.0 255.0.0.0 area 0
```

ステップ 3 インターフェイス コンフィギュレーション モードを開始します。

interface *interface-name*

例：

```
ciscoasa(config)# interface my_interface
```

ステップ 4 インターフェイスの認証タイプを指定します。

ospf authentication [**message-digest** | **null**]

例：

```
ciscoasa(config-interface)# ospf authentication message-digest
```

ステップ 5 OSPF 簡易パスワード認証を使用しているネットワーク セグメント上で近接する OSPF ルータが使用するパスワードを割り当てます。

ospf authentication-key*key*

例：

```
ciscoasa(config-interface)# ospf authentication-key cisco
```

key 引数には、最大 8 バイトの連続する文字列が指定できます。

このコマンドで作成するパスワードはキーとして使用され、このキーは ASA のソフトウェアによるルーティング プロトコル パケットの発信時に OSPF ヘッダーに直接挿入されます。各ネットワークにはインターフェイスごとに個別のパスワードを割り当てることができます。OSPF 情報を交換するには、同じネットワーク上のすべての隣接ルータが同じパスワードを持っている必要があります。

ステップ 6 OSPF インターフェイスでパケットを送信するコストを明示的に指定します。

ospf cost*cost*

例：

```
ciscoasa(config-interface)# ospf cost 20
```

cost は、1 ～ 65535 の整数です。

この例では、cost は 20 に設定されています。

ステップ 7 デバイスが hello パケットを受信していないためネイバー OSPF ルータがダウンしていることを宣言するまでデバイスが待機する秒数を設定します。

ospf dead-interval*seconds*

例：

```
ciscoasa(config-interface)# ospf dead-interval 40
```

この値はネットワーク上のすべてのノードで同じにする必要があります。

ステップ 8 ASA が OSPF インターフェイスから hello パケットを送信する時間間隔を指定します。

ospf hello-interval*seconds*

例：

```
ciscoasa(config-interface)# ospf hello-interval 10
```

この値はネットワーク上のすべてのノードで同じにする必要があります。

ステップ 9 OSPF Message Digest 5（MD5）認証を有効にします。

ospf message-digest-key*key-id***md5***key*

例：

```
ciscoasa(config-interface)# ospf message-digest-key 1 md5 cisco
```

次の引数を設定できます。

key-id：1 ～ 255 の範囲の識別子。

key：最大 16 バイトの英数字パスワード

通常は、インターフェイスあたり 1 つのキーを使用して、パケット送信時に認証情報を生成するとともに着信パケットを認証します。隣接ルータの同一キー識別子は、キー値を同一にする必要があります。

1 インターフェイスで 2 つ以上のキーを保持しないことをお勧めします。新しいキーを追加したらその都度古いキーを削除して、ローカルシステムが古いキー情報を持つ悪意のあるシステムと通信を続けることのないようにしてください。古いキーを削除すると、ロールオーバー中のオーバーヘッドを減らすことにもなります。

ステップ 10 ネットワークに対して、OSPF で指定されたルータを判別するときに役立つプライオリティを設定します。

ospf priority *number-value*

例：

```
ciscoasa(config-interface)# ospf priority 20
```

number_value 引数の範囲は 0 ～ 255 です。

ステップ 11 OSPF インターフェイスに属する隣接ルータに LSA を再送信する間隔を秒単位で指定します。

ospf retransmit-interval *number-value*

例：

```
ciscoasa(config-interface)# ospf retransmit-interval seconds
```

seconds の値は、接続されているネットワーク上の任意の 2 ルータ間で予想されるラウンドトリップ遅延よりも長い秒数でなければなりません。範囲は 1 ～ 8192 秒です。デフォルト値は 5 秒です。

ステップ 12 OSPF インターフェイスでリンクステートアップデートパケットを送信するために必要な予想時間を秒単位で設定します。

ospf transmit-delay*seconds*

例：

```
ciscoasa(config-interface)# ospf transmit-delay 5
```

seconds の値は、1 ～ 8192 秒です。デフォルト値は 1 秒です。

ステップ 13 1 秒間に送信される hello パケットの数を設定します。

ospf dead-interval minimal hello-interval multiplier整数

例：

```
ciscoasa(config-if)# ospf dead-interval minimal hello-multiplier 6
```

有効な値は 3 ～ 20 の整数です。

ステップ 14 インターフェイスをポイントツーポイントの非ブロードキャスト ネットワークとして指定します。

ospf network point-to-point non-broadcast

例：

```
ciscoasa(config-interface)# ospf network point-to-point non-broadcast
```

インターフェイスをポイントツーポイントの非ブロードキャストとして指定するには、手動で OSPF ネイバーを定義する必要があります。ダイナミック ネイバー探索はできません。詳細については、「スタティック OSPFv2 ネイバーの定義 （807 ページ）」を参照してください。さらに、そのインターフェイスに定義できる OSPF ネイバーは 1 つだけです。

OSPFv2 エリア パラメータの設定

複数の OSPF エリア パラメータを設定できます。これらのエリア パラメータ（後述のタスク リストに表示）には、認証の設定、スタブ エリアの定義、デフォルト サマリー ルートへの特定のコストの割り当てがあります。認証では、エリアへの不正アクセスに対してパスワード ベースで保護します。

スタブ エリアは、外部ルートの情報が送信されないエリアです。その代わりに、ABR で生成されるデフォルトの外部ルートがあり、このルートは自律システムの外部の宛先としてスタブ エリアに送信されます。OSPF スタブ エリアのサポートを活用するには、デフォルトのルーティングをスタブ エリアで使用する必要があります。スタブ エリアに送信される LSA の数をさらに減らすには、ABR で実行する **area stub** コマンドの **no-summary** キーワードを使用して、スタブ エリアにサマリー リンク アドバタイズメント（LSA タイプ 3）が送信されないようにします。

手順

ステップ 1 OSPF ルーティング プロセスを作成します。

router ospf *process_id*

例：

```
ciscoasa(config)# router ospf 2
```

process_id 引数は、このルーティング プロセス内部で使用される識別子です。任意の正の整数が使用できます。この ID は内部専用のため、他のどのデバイス上の ID とも照合する必要はありません。最大 2 つのプロセスが使用できます。

ステップ 2 OSPF エリアの認証を有効にします。

area *area-id* authentication

例：

```
ciscoasa(config-rtr)# area 0 authentication
```

ステップ 3 OSPF エリアの MD5 認証を有効にします。

area *area-id* authentication message-digest

例：

```
ciscoasa(config-rtr)# area 0 authentication message-digest
```

OSPFv2 フィルタ ルールの設定

OSPF アップデートで受信または送信されるルートまたはネットワークをフィルタリングするには、次の手順を実行します。

手順

ステップ 1 OSPF ルーティング プロセスを有効にし、ルータ コンフィギュレーション モードを開始します。

router ospf *process_id*

例：

```
ciscoasa(config)# router ospf 2
```

ステップ 2 着信 OSPF アップデートで受信したルートまたはネットワーク、あるいは発信 OSPF アップデートでアドバタイズされたルートまたはネットワークをフィルタリングします。

distribute-list *acl-number* **in** [**interface** *ifname*]

distribute-list *acl-number* **out** [*protocol process-number* | **connected** | **static**]

引数 *acl-number* には、IP アクセス リストの番号を指定します。アクセス リストは、ルーティング アップデートで受信されるネットワークと抑制されるネットワークを定義します。

着信アップデートにフィルタを適用するには、**in** を指定します。オプションで、インターフェイスを指定して、そのインターフェイスが受信するアップデートにフィルタを制限することができます。

発信アップデートにフィルタを適用するには、**out** を指定します。必要に応じて、配布リストに適用するプロトコル（**bgp**、**eigrp**、**ospf**、または **rip**）をプロセス番号付き（RIP を除く）で指定できます。ピアおよびネットワークが **connected** または **static** ルート経由で学習されたかどうかでフィルタすることもできます。

例：

```
ciscoasa(config-rtr)# distribute-list ExampleAcl in interface inside
```

OSPFv2 NSSA の設定

NSSA の OSPFv2 への実装は、OSPFv2 のスタブ エリアに似ています。NSSA は、タイプ 5 の外部 LSA をコアからエリアにフラッディングすることはありませんが、自律システムの外部ルートをある限られた方法でエリア内にインポートできます。

NSSA は、再配布によって、タイプ 7 の自律システムの外部ルートを NSSA エリア内部にインポートします。これらのタイプ 7 の LSA は、NSSA の ABR によってタイプ 5 の LSA に変換され、ルーティング ドメイン全体にフラッディングされます。変換中は集約とフィルタリングがサポートされます。

OSPFv2 を使用する中央サイトから異なるルーティング プロトコルを使用するリモート サイトに接続しなければならない ISP またはネットワーク管理者は、NSSA を使用することによって管理を簡略化できます。

NSSA が実装される前は、企業サイトの境界ルータとリモート ルータ間の接続では、OSPFv2 スタブ エリアとしては実行されませんでした。これは、リモート サイト向けのルートは、スタブ エリアに再配布することができず、2 種類のルーティング プロトコルを維持する必要があったためです。RIP のようなシンプルなプロトコルを実行して再配布を処理する方法が一般的でした。NSSA が実装されたことで、企業ルータとリモート ルータ間のエリアを NSSA として定義することにより、NSSA で OSPFv2 を拡張してリモート接続をカバーできます。

この機能を使用する前に、次のガイドラインを参考にしてください。

- 外部の宛先に到達するために使用可能なタイプ7のデフォルトルートを設定できます。設定すると、NSSA または NSSA エリア境界ルータまでのタイプ 7 のデフォルトがルータによって生成されます。
- 同じエリア内のすべてのルータは、エリアが NSSA であることを認識する必要があります。そうでない場合、ルータは互いに通信できません。

手順

ステップ 1 OSPF ルーティング プロセスを作成します。

router ospf *process_id*

例：

```
ciscoasa(config)# router ospf 2
```

process_id 引数は、このルーティング プロセス内部で使用される識別子です。任意の正の整数が使用できます。この ID は内部専用のため、他のどのデバイス上の ID とも照合する必要はありません。最大 2 つのプロセスが使用できます。

ステップ 2 NSSA エリアを定義します。

area *area-id* nssa [**no-redistribution**] [**default-information-originate**]

例：

```
ciscoasa(config-rtr)# area 0 nssa
```

ステップ 3 サマリー アドレスを設定します。これは、ルーティング テーブルのサイズを小さくするために役立ちます。

summary-address *ip_address mask* [**not-advertise**] [tag *tag*]

例：

```
ciscoasa(config-rtr)# summary-address 10.1.0.0 255.255.0.0
```

OSPF でこのコマンドを使用すると、このアドレスでカバーされる再配布ルートすべての集約として、1 つの外部ルートが OSPF ASBR からアドバタイズされます。

この例のサマリー アドレスの 10.1.0.0 には、10.1.1.0、10.1.2.0、10.1.3.0 などのアドレスが含まれます。外部のリンクステート アドバタイズメントでは、アドレス 10.1.0.0 だけがアドバタイズされます。

（注） OSPF は summary-address 0.0.0.0 0.0.0.0 をサポートしません。

クラスタリングの IP アドレス プールの設定（OSPFv2 および OSPFv3）

個別インターフェイス クラスタリングを使用する場合は、ルータ ID のクラスタ プールの IPv4 アドレスの範囲を割り当てることができます。

OSPFv2 および OSPFv3 の個別インターフェイス クラスタリングのルータ ID のクラスタ プールの IPv4 アドレスの範囲を割り当てるには、次のコマンドを入力します。

手順

個別インターフェイス クラスタリングのルータ ID のクラスタ プールを指定します。

router-id cluster-pool hostname | A.B.C.D ip_pool

例：

```
hostname(config)# ip local pool rpool 1.1.1.1-1.1.1.4
hostname(config)# router ospf 1
hostname(config-rtr)# router-id cluster-pool rpool
hostname(config-rtr)# network 17.5.0.0 255.255.0.0 area 1
hostname(config-rtr)# log-adj-changes
```

cluster-pool キーワードは、個別インターフェイス クラスタリングが設定されている場合に、IP アドレス プールのコンフィギュレーションをイネーブルにします。**hostname**|**A.B.C.D.** キーワードは、この OSPF プロセスの OSPF ルータ ID を指定します。*ip_pool* 引数には、IP アドレス プールの名前を指定します。

（注） クラスタリングを使用している場合は、ルータ ID の IP アドレス プールを指定する必要はありません。IP アドレス プールを設定しない場合、ASA は自動的に生成されたルータ ID を使用します。

スタティック OSPFv2 ネイバーの定義

ポイントツーポイントの非ブロードキャスト ネットワークを介して OSPFv2 ルートをアドバタイズするには、スタティック OSPFv2 ネイバーを定義する必要があります。この機能により、OSPFv2 アドバタイズメントを GRE トンネルにカプセル化しなくても、既存の VPN 接続でブロードキャストすることができます。

開始する前に、OSPFv2 ネイバーに対するスタティック ルートを作成する必要があります。スタティック ルートの作成方法の詳細については、スタティック ルートの設定（712 ページ）を参照してください。

手順

ステップ 1 OSPFv2 ルーティング プロセスを作成します。

router ospf *process_id*

例：

```
ciscoasa(config)# router ospf 2
```

process_id 引数は、このルーティング プロセス内部で使用される識別子です。任意の正の整数が使用できます。この ID は内部専用のため、他のどのデバイス上の ID とも照合する必要はありません。最大 2 つのプロセスが使用できます。

ステップ 2 OSPFv2 ネイバーフッドを定義します。

neighbor *addr* [**interface** if_name]

例：

```
ciscoasa(config-rtr)# neighbor 255.255.0.0 [interface my_interface]
```

addr 引数には OSPFv2 ネイバーの IP アドレスを指定します。*if_name* 引数は、ネイバーとの通信に使用するインターフェイスです。OSPFv2 ネイバーが直接接続されているインターフェイスのいずれとも同じネットワーク上にない場合、interface を指定する必要があります。

ルート計算タイマーの設定

OSPFv2 によるトポロジ変更受信と最短パス優先（SPF）計算開始との間の遅延時間が設定できます。最初に SPF を計算してから次に計算するまでの保持時間も設定できます。

手順

ステップ 1 OSPFv2 ルーティング プロセスを作成します。

router ospf *process_id*

例：

```
ciscoasa(config)# router ospf 2
```

process_id 引数は、このルーティング プロセス内部で使用される識別子です。任意の正の整数が使用できます。この ID は内部専用のため、他のどのデバイス上の ID とも照合する必要はありません。最大 2 つのプロセスが使用できます。

ステップ 2 ルート計算時間を設定します。

timers throttle spf *spf-start spf-hold spf-maximum*

例：

```
ciscoasa(config-router)# timers throttle spf 500 500 600
```

spf-start 引数は、OSPF によるトポロジ変更受信と SPF 計算開始との間の遅延時間（ミリ秒）です。0 ～ 600000 の整数に設定できます。

spf-hold 引数は、2 回の連続する SPF 計算間の最小時間（ミリ秒）です。0 ～ 600000 の整数に設定できます。

spf-maximum 引数は、2 回の連続する SPF 計算間の最大時間（ミリ秒）です。0 ～ 600000 の整数に設定できます。

ネイバーの起動と停止のロギング

デフォルトでは、OSPFv2 ネイバーがアップ状態またはダウン状態になったときに、syslog メッセージが生成されます。

アップ状態またはダウン状態になった OSPFv2 ネイバーについて、**debug ospf adjacency** コマンドを実行せずに確認する必要がある場合に、**log-adj-changes** コマンドを設定します。**log-adj-changes** コマンドでは、少ない出力によってピアの関係が高いレベルで表示されます。それぞれの状態変化メッセージを確認するには、**log-adj-changes detail** コマンドを設定します。

手順

ステップ 1 OSPFv2 ルーティング プロセスを作成します。

router ospf *process_id*

例：

```
ciscoasa(config)# router ospf 2
```

process_id 引数は、このルーティング プロセス内部で使用される識別子です。任意の正の整数が使用できます。この ID は内部専用のため、他のどのデバイス上の ID とも照合する必要はありません。最大 2 つのプロセスが使用できます。

ステップ 2 アップ状態またはダウン状態になったネイバーに対するロギングを設定します。

log-adj-changes [**detail**]

OSPFv3 の設定

ここでは、OSPFv3 ルーティング プロセスの設定に関連するタスクについて説明します。

OSPFv3 の有効化

OSPFv3 をイネーブルにするには、OSPFv3 ルーティング プロセスを作成し、OSPFv3 用のエリアを作成して、OSPFv3 のインターフェイスをイネーブルにする必要があります。その後、ターゲットの OSPFv3 ルーティング プロセスにルートを再配布する必要があります。

手順

ステップ 1 OSPFv3 ルーティング プロセスを作成します。

ipv6 router ospf *process-id*

例：

```
ciscoasa(config)# ipv6 router ospf 10
```

process-id 引数は、このルーティング プロセス内部で使用されるタグです。任意の正の整数が使用できます。このタグは内部専用のため、他のどのデバイス上のタグとも照合する必要はありません。最大 2 つのプロセスが使用できます。

ステップ 2 インターフェイスをイネーブルにします。

interface *interface_name*

例：

```
ciscoasa(config)# interface Gigabitethernet0/0
```

ステップ 3 特定のプロセス ID を持つ OSPFv3 ルーティング プロセスおよび指定したエリア ID を持つ OSPFv3 のエリアを作成します。

ipv6 ospf *process-id* **area** *area_id*

例：

```
ciscoasa(config)# ipv6 ospf 200 area 100
```

OSPFv3 インターフェイス パラメータの設定

必要に応じて特定のインターフェイス固有の OSPFv3 パラメータを変更できます。これらのパラメータを必ずしも変更する必要はありませんが、hello interval と dead interval というインターフェイスパラメータは、接続されているネットワーク内のすべてのルータで一致している必要があります。これらのパラメータを設定する場合は、ネットワーク上のすべてのルータで、コンフィギュレーションの値が矛盾していないことを確認してください。

手順

ステップ 1 OSPFv3 のルーティング プロセスをイネーブルにします。

ipv6 router ospf *process-id*

例：

```
ciscoasa(config-if)# ipv6 router ospf 10
```

process-id 引数は、このルーティング プロセス内部で使用されるタグです。任意の正の整数が使用できます。このタグは内部専用のため、他のどのデバイス上のタグとも照合する必要はありません。最大 2 つのプロセスが使用できます。

ステップ 2 OSPFv3 エリアを作成します。

ipv6 ospf **area** [*area-num*] [**instance**]

例：

```
ciscoasa(config-if)# interface GigabitEthernet3/2.200
 vlan 200
 nameif outside
 security-level 100
 ip address 10.20.200.30 255.255.255.0 standby 10.20.200.31
 ipv6 address 3001::1/64 standby 3001::8
 ipv6 address 6001::1/64 standby 6001::8
 ipv6 enable
 ospf priority 255
 ipv6 ospf cost 100
 ipv6 ospf 100 area 10 instance 200
```

area-num 引数は、認証がイネーブルになるエリアであり、10 進数値または IP アドレスを指定できます。**instance** キーワードは、インターフェイスに割り当てられるエリア インスタンス ID を指定します。インターフェイスは、OSPFv3 エリアを 1 つだけ保有できます。複数のインターフェイスで同じエリアを使用でき、各インターフェイスは異なるエリア インスタンス ID を使用できます。

ステップ 3 インターフェイス上でパケットを送信するコストを指定します。

ipv6 ospf cost *interface-cost*

例：

```
ciscoasa(config-if)# interface GigabitEthernet3/2.200
 vlan 200
 nameif outside
 security-level 100
 ip address 10.20.200.30 255.255.255.0 standby 10.20.200.31
 ipv6 address 3001::1/64 standby 3001::8
 ipv6 address 6001::1/64 standby 6001::8
 ipv6 enable
 ospf priority 255
 ipv6 ospf cost 100
```

```
 ipv6 ospf 100 area 10 instance 200
```

interface-cost 引数は、リンクステート メトリックとして表される符号なし整数値を指定します。値の範囲は、1 ～ 65535 です。デフォルトのコストは帯域幅に基づきます。

ステップ 4 OSPFv3 インターフェイスへの発信 LSA をフィルタリングします。

ipv6 ospf database-filter all out

例：

```
ciscoasa(config-if)# interface GigabitEthernet3/2.200
 vlan 200
 nameif outside
 security-level 100
 ip address 10.20.200.30 255.255.255.0 standby 10.20.200.31
 ipv6 address 3001::1/64 standby 3001::8
 ipv6 address 6001::1/64 standby 6001::8
 ipv6 enable
 ospf priority 255
 ipv6 ospf cost 100
 ipv6 ospf 100 area 10 instance 200
ipv6 ospf database-filter all out
```

デフォルトでは、すべての発信 LSA がインターフェイスにフラッディングされます。

ステップ 5 秒単位で設定する期間内に hello パケットが確認されないと、当該ルータがダウンしていることがネイバーによって示されます。

ipv6 ospf dead-interval *seconds*

例：

```
ciscoasa(config-if)# interface GigabitEthernet3/2.200
 vlan 200
 nameif outside
 security-level 100
 ip address 10.20.200.30 255.255.255.0 standby 10.20.200.31
 ipv6 address 3001::1/64 standby 3001::8
 ipv6 address 6001::1/64 standby 6001::8
 ipv6 enable
 ospf priority 255
 ipv6 ospf cost 100
 ipv6 ospf 100 area 10 instance 200
ipv6 ospf dead-interval 60
```

この値はネットワーク上のすべてのノードで同じにする必要があります。値の範囲は、1 ～ 65535 です。デフォルト値は、**ipv6 ospf hello-interval** コマンドで設定された間隔の 4 倍です。

ステップ 6 インターフェイスに暗号化タイプを指定します。

ipv6 ospf encryption {**ipsec spi** *spi* **esp** *encryption-algorithm* [[*key-encryption-type*] *key*] *authentication-algorithm* [[*key-encryption-type*] *key* | **null**}

例：

```
ciscoasa(config-if)# interface GigabitEthernet3/2.200
 vlan 200
```

```
 nameif outside
 security-level 100
 ip address 10.20.200.30 255.255.255.0 standby 10.20.200.31
 ipv6 address 3001::1/64 standby 3001::8
 ipv6 address 6001::1/64 standby 6001::8
 ipv6 enable
 ospf priority 255
 ipv6 ospf cost 100
 ipv6 ospf 100 area 10 instance 200
ipv6 ospf encryption ipsec spi 1001 esp null sha1 123456789A123456789B123456789C123456789D
```

ipsec キーワードは、IP セキュリティ プロトコルを指定します。**spi** *spi* キーワード引数のペアは、セキュリティ ポリシー インデックスを指定します。値の範囲は 256 ～ 42949667295 である必要があり、10 進数で入力する必要があります。

esp キーワードは、カプセル化セキュリティ ペイロードを指定します。*encryption-algorithm* 引数は、ESP で使用される暗号化アルゴリズムを指定します。有効な値は次のとおりです。

- aes-cdc：AES-CDC 暗号化をイネーブルにします。
- 3des：トリプル DES 暗号化をイネーブルにします。
- des：DES 暗号化をイネーブルにします。
- null：暗号化なしの ESP を指定します。

key-encryption-type 引数に、次の 2 つのうちいずれかの値を指定します。

- 0：キーは暗号化されません。
- 7：キーは暗号化されます。

key 引数は、メッセージ ダイジェストの計算で使用される番号を指定します。この番号の長さは 32 桁の 16 進数（16 バイト）です。キーのサイズは、使用される暗号化アルゴリズムによって異なります。AES-CDC など、一部のアルゴリズムでは、キーのサイズを選択することができます。*authentication-algorithm* 引数は、使用される次のいずれかの暗号化認証アルゴリズムを指定します。

- md5：Message Digest 5（MD5）をイネーブルにします。
- sha1：SHA-1 をイネーブルにします。

null キーワードはエリアの暗号化より優先されます。

インターフェイスで OSPFv3 暗号化が有効化されており、ネイバーが異なるエリア（たとえば、エリア 0）にあり、ASA がそのエリアとの隣接関係を形成する場合は、ASA のエリアを変更する必要があります。ASA のエリアを 0 に変更すると、OSPFv3 の隣接関係が確立される前に 2 分の遅延が発生します。

ステップ 7 インターフェイスに LSA のフラッディング削減を指定します。

ipv6 ospf flood-reduction

例：

```
ciscoasa(config-if)# interface GigabitEthernet3/2.200
 vlan 200
 nameif outside
 security-level 100
 ip address 10.20.200.30 255.255.255.0 standby 10.20.200.31
 ipv6 address 3001::1/64 standby 3001::8
 ipv6 address 6001::1/64 standby 6001::8
 ipv6 enable
 ospf priority 255
 ipv6 ospf cost 100
 ipv6 ospf 100 area 10 instance 200
ipv6 ospf flood reduction
```

ステップ 8 インターフェイス上で送信される hello パケット間の間隔（秒数）を指定します。

ipv6 ospf hello-interval *seconds*

例：

```
ciscoasa(config-if)# interface GigabitEthernet3/2.200
 vlan 200
 nameif outside
 security-level 100
 ip address 10.20.200.30 255.255.255.0 standby 10.20.200.31
 ipv6 address 3001::1/64 standby 3001::8
 ipv6 address 6001::1/64 standby 6001::8
 ipv6 enable
 ospf priority 255
 ipv6 ospf cost 100
 ipv6 ospf 100 area 10 instance 200
ipv6 ospf hello-interval 15
```

この値は特定のネットワーク上のすべてのノードで同じにする必要があります。値の範囲は、1 ～ 65535 です。デフォルトの間隔は、イーサネット インターフェイスで 10 秒、非ブロードキャスト インターフェイスで 30 秒です。

ステップ 9 DBD パケットを受信した場合の OSPF MTU 不一致検出をディセーブルにします。

ipv6 ospf mtu-ignore

例：

```
ciscoasa(config-if)# interface GigabitEthernet3/2.200
 vlan 200
 nameif outside
 security-level 100
 ip address 10.20.200.30 255.255.255.0 standby 10.20.200.31
 ipv6 address 3001::1/64 standby 3001::8
 ipv6 address 6001::1/64 standby 6001::8
 ipv6 enable
 ospf priority 255
 ipv6 ospf cost 100
 ipv6 ospf 100 area 10 instance 200
ipv6 ospf mtu-ignore
```

OSPF MTU 不一致検出は、デフォルトでイネーブルになっています。

ステップ 10 ネットワーク タイプに依存するデフォルト以外のタイプに OSPF ネットワーク タイプを設定します。

ipv6 ospf network {**broadcast** | **point-to-point non-broadcast**}

例：

```
ciscoasa(config-if)# interface GigabitEthernet3/2.200
 vlan 200
 nameif outside
 security-level 100
 ip address 10.20.200.30 255.255.255.0 standby 10.20.200.31
 ipv6 address 3001::1/64 standby 3001::8
 ipv6 address 6001::1/64 standby 6001::8
 ipv6 enable
 ospf priority 255
 ipv6 ospf cost 100
 ipv6 ospf 100 area 10 instance 200
ipv6 ospf network point-to-point non-broadcast
```

point-to-point non-broadcast キーワードは、ネットワーク タイプをポイントツーポイント、非ブロードキャストに設定します。**broadcast** キーワードは、ネットワーク タイプをブロードキャストに設定します。

ステップ 11 ルータ プライオリティを設定します。これは、ネットワークにおける指定ルータの特定に役立ちます。

ipv6 ospf priority *number-value*

例：

```
ciscoasa(config-if)# interface GigabitEthernet3/2.200
 vlan 200
 nameif outside
 security-level 100
 ip address 10.20.200.30 255.255.255.0 standby 10.20.200.31
 ipv6 address 3001::1/64 standby 3001::8
 ipv6 address 6001::1/64 standby 6001::8
 ipv6 enable
 ospf priority 255
 ipv6 ospf cost 100
 ipv6 ospf 100 area 10 instance 200
ipv6 ospf priority 4
```

有効値の範囲は 0 ～ 255 です。

ステップ 12 非ブロードキャスト ネットワークへの OSPFv3 ルータの相互接続を設定します。

ipv6 ospf neighbor *ipv6-address* [**priority** *number*] [**poll-interval** *seconds*] [**cost** *number*] [**database-filter all out**]

例：

```
ciscoasa(config-if)# interface GigabitEthernet3/2.200
 vlan 200
 nameif outside
 security-level 100
 ip address 10.20.200.30 255.255.255.0 standby 10.20.200.31
```

```
 ipv6 address 3001::1/64 standby 3001::8
 ipv6 address 6001::1/64 standby 6001::8
 ipv6 enable
 ospf priority 255
 ipv6 ospf cost 100
 ipv6 ospf 100 area 10 instance 200
ipv6 ospf neighbor FE80::A8BB:CCFF:FE00:C01
```

ステップ 13 インターフェイスに属する隣接関係の LSA 再送信間の時間を秒単位で指定します。

ipv6 ospf retransmit-interval *seconds*

例：

```
ciscoasa(config-if)# interface GigabitEthernet3/2.200
 vlan 200
 nameif outside
 security-level 100
 ip address 10.20.200.30 255.255.255.0 standby 10.20.200.31
 ipv6 address 3001::1/64 standby 3001::8
 ipv6 address 6001::1/64 standby 6001::8
 ipv6 enable
 ospf priority 255
 ipv6 ospf cost 100
 ipv6 ospf 100 area 10 instance 200
ipv6 ospf retransmit-interval 8
```

接続ネットワーク上の任意の2台のルータ間で想定される往復遅延より大きな値にする必要があります。有効値の範囲は、1 ～ 65535 秒です。デフォルトは 5 秒です。

ステップ 14 インターフェイス上でリンクステート更新パケットを送信する時間を秒単位で設定します。

ipv6 ospf transmit-delay *seconds*

例：

```
ciscoasa(config-if)# interface GigabitEthernet3/2.200
 vlan 200
 nameif outside
 security-level 100
 ip address 10.20.200.30 255.255.255.0 standby 10.20.200.31
 ipv6 address 3001::1/64 standby 3001::8
 ipv6 address 6001::1/64 standby 6001::8
 ipv6 enable
 ospf priority 255
 ipv6 ospf cost 100
 ipv6 ospf 100 area 10 instance 200
ipv6 ospf retransmit-delay 3
```

有効値の範囲は、1 ～ 65535 秒です。デフォルト値は 1 秒です。

OSPFv3 ルータ パラメータの設定

手順

ステップ 1 OSPFv3 のルーティング プロセスをイネーブルにします。

ipv6 router ospf *process-id*

例：

```
ciscoasa(config)# ipv6 router ospf 10
```

process-id 引数は、このルーティング プロセス内部で使用される識別子です。ローカルに割り当てられ、1 ～ 65535 の任意の正の整数を指定できます。この ID は内部管理専用のため、他のどのデバイス上の ID とも照合する必要はありません。最大 2 つのプロセスが使用できます。

ステップ 2 OSPFv3 エリア パラメータを設定します。

area

例：

```
ciscoasa(config-rtr)# area 10
```

サポートされているパラメータには、0 ～ 4294967295 の 10 進数値のエリア ID、**A.B.C.D** の IP アドレス形式のエリア ID などがあります。

ステップ 3 コマンドをデフォルト値に設定します。

デフォルト

例：

```
ciscoasa(config-rtr)# default originate
```

originate パラメータはデフォルト ルートを配布します。

ステップ 4 デフォルト情報の配布を制御します。

default-information

ステップ 5 ルート タイプに基づいて、OSPFv3 ルート アドミニストレーティブ ディスタンスを定義します。

distance

例：

```
ciscoasa(config-rtr)# distance 200
```

サポートされるパラメータには、1～254の値のアドミニストレーティブディスタンス、OSPFv3ディスタンスの **ospf** などがあります。

ステップ 6 ルータがタイプ 6 Multicast OSPF（MOSPF）パケットのリンクステート アドバタイズメント（LSA）を受信した場合に、**lsa** パラメータが指定されている syslog メッセージの送信を抑止します。

ignore

例：

```
ciscoasa(config-rtr)# ignore lsa
```

ステップ 7 OSPFv3 ネイバーが起動または停止したときに、ルータが syslog メッセージを送信するように設定します。

log-adjacency-changes

例：

```
ciscoasa(config-rtr)# log-adjacency-changes detail
```

detail パラメータによって、すべての状態変更がログに記録されます。

ステップ 8 インターフェイスでのルーティング アップデートの送受信を抑止します。

passive-interface [*interface_name*]

例：

```
ciscoasa(config-rtr)# passive-interface inside
```

interface_name 引数は、OSPFv3 プロセスが実行されているインターフェイスの名前を指定します。

ステップ 9 あるルーティング ドメインから別のルーティング ドメインへのルートの再配布を設定します。

redistribute {**connected** | **ospf** | **static**}

それぞれの説明は次のとおりです。

- **connected**：接続ルートを指定します。
- **ospf**：OSPFv3 ルートを指定します。
- **static**：スタティック ルートを指定します。

例：

```
ciscoasa(config-rtr)# redistribute ospf
```

ステップ 10 指定したプロセスの固定ルータ ID を作成します。

router-id {*A.B.C.D* | **cluster-pool** | **static**}

それぞれの説明は次のとおりです。

A.B.C.D：IP アドレス形式の OSPF ルータ ID を指定します。

cluster-pool：個別インターフェイス クラスタリングが設定されている場合に、IP アドレス プールを設定します。クラスタリングで使用される IP アドレス プールの詳細については、クラスタリングの IP アドレス プールの設定（OSPFv2 および OSPFv3）（807 ページ）を参照してください。

例：

```
ciscoasa(config-rtr)# router-id 10.1.1.1
```

ステップ 11 0 ～ 128 の有効な値で IPv6 アドレス サマリーを設定します。

summary-prefix *X:X:X:X::X/*

例：

```
ciscoasa(config-if)# ipv6 router ospf 1
ciscoasa(config-router)# router-id 192.168.3.3
ciscoasa(config-router)# summary-prefix FECO::/24
ciscoasa(config-router)# redistribute static
```

X:X:X:X::X/ パラメータは、IPv6 プレフィックスを指定します。

ステップ 12 ルーティング タイマーを調整します。

timers

ルーティング タイマー パラメータは次のとおりです。

- **lsa**：OSPFv3 LSA タイマーを指定します。
- **nsf**：OSPFv3 NSF 待機タイマーを指定します。
- **pacing**：OSPFv3 ペーシング タイマーを指定します。
- **throttle**：OSPFv3 スロットル タイマーを指定します。

例：

```
ciscoasa(config)# ipv6 router ospf 10
ciscoasa(config-rtr)# timers throttle spf 6000 12000 14000
```

OSPFv3 エリア パラメータの設定

手順

ステップ 1 OSPFv3 のルーティング プロセスをイネーブルにします。

ipv6 router ospf *process-id*

例：

```
ciscoasa(config)# ipv6 router ospf 1
```

process-id 引数は、このルーティング プロセス内部で使用される識別子です。ローカルに割り当てられ、1 ～ 65535 の任意の正の整数を指定できます。

この ID は内部管理専用のため、他のどのデバイス上の ID とも照合する必要はありません。最大 2 つのプロセスが使用できます。

ステップ 2 NSSA エリアまたはスタブ エリアのサマリー デフォルト コストを設定します。

area *area-id* **default-cost** *cost*

例：

```
ciscoasa(config-rtr)# area 1 default-cost nssa
```

ステップ 3 アドレスおよび境界ルータ専用のマスクと一致するルートを集約します。

area *area-id* **range** *ipv6-prefix*/ *prefix-length* [**advertise** | **not advertise**] [**cost** *cost*]

例：

```
ciscoasa(config-rtr)# area 1 range FE01:1::1/64
```

- *area-id* 引数は、ルートが集約されているエリアを識別します。値には、10 進数または IPv6 プレフィックスを指定できます。
- *ipv6-prefix* 引数は、IPv6 プレフィックスを指定します。*prefix-length* 引数は、プレフィックス長を指定します。
- **advertise** キーワードは、アドレス範囲ステータスをアドバタイズに設定し、Type 3 サマリー LSA を生成します。
- **not-advertise** キーワードはアドレス範囲ステータスを DoNotAdvertise に設定します。
- Type 3 サマリー LSA は抑制され、コンポーネント ネットワークは他のネットワークから隠された状態のままです。
- **cost** *cost* キーワード引数のペアは、宛先への最短パスを決定するために OSPF SPF 計算で使用されるサマリー ルートのメトリックまたはコストを指定します。

- 有効値の範囲は 0 ～ 16777215 です。

ステップ 4 NSSA エリアを指定します。

area *area-id* **nssa**

例：

```
ciscoasa(config-rtr)# area 1 nssa
```

ステップ 5 スタブ エリアを指定します。

area *area-id* **stub**

例：

```
ciscoasa(config-rtr)# area 1 stub
```

ステップ 6 仮想リンクとそのパラメータを定義します。

area *area-id* **virtual-link** *router-id* [**hello-interval** *seconds*] [**retransmit-interval** *seconds*] [**transmit-delay** *seconds*] [**dead-interval** *seconds*] [**ttl-security hops** *hop-count*]

例：

```
ciscoasa(config-rtr)# area 1 virtual-link 192.168.255.1 hello-interval 5
```

- *area-id* 引数は、ルートが集約されているエリアを識別します。**virtual link** キーワードは、仮想リンク ネイバーの作成を指定します。
- *router-id* 引数は、仮想リンク ネイバーに関連付けられたルータ ID を指定します。
- ルータ ID を表示するには、**show ospf** コマンドまたは **show ipv6 ospf** コマンドを入力します。デフォルト値はありません。
- **hello-interval** キーワードは、インターフェイス上で送信される hello パケット間の時間を秒単位で指定します。hello 間隔は、hello パケットでアドバタイズされる符号なし整数です。この値は、共通のネットワークに接続されているすべてのルータおよびアクセス サーバで同じであることが必要です。有効値の範囲は 1 ～ 8192 です。デフォルトは 10 です。
- **retransmit-interval** *seconds* キーワード引数のペアは、インターフェイスに属する隣接関係の LSA 再送信間の時間を秒単位で指定します。再送信間隔は、接続されているネットワーク上の任意の 2 台のルータ間の予想されるラウンドトリップ遅延です。この値は、予想されるラウンドトリップ遅延より大きくなり、1 ～ 8192 の範囲で指定できます。デフォルトは 5 分です。
- **transmit-delay** *seconds* キーワード引数のペアは、インターフェイス上でリンクステート更新パケットを送信するために必要とされる時間を秒単位で設定します。ゼロよりも大きい整数値を指定します。アップデート パケット内の LSA 自体の経過時間は、転送前にこの値の分だけ増分されます。値の範囲は 1 ～ 8192 です。デフォルトは 1 です。

- **dead-interval seconds** キーワード引数のペアは、ルータがダウンしていることをネイバーが示す前に hello パケットを非表示にする時間を秒単位で指定します。デッド間隔は符号なし整数です。デフォルトは hello 間隔の 4 倍または 40 秒です。この値は、共通のネットワークに接続されているすべてのルータおよびアクセス サーバで同じであることが必要です。有効値の範囲は 1 ～ 8192 です。
- **ttl-security hops** キーワードは仮想リンクの存続可能時間（TTL）セキュリティを設定します。*hop-count* 引数の値は 1 ～ 254 の範囲で指定できます。

OSPFv3 受動インターフェイスの設定

手順

ステップ 1 OSPFv3 のルーティング プロセスをイネーブルにします。

ipv6 router ospf *process_id*

例：

```
ciscoasa(config-if)# ipv6 router ospf 1
```

process_id 引数は、このルーティング プロセス内部で使用される識別子です。ローカルに割り当てられ、1 ～ 65535 の任意の正の整数を指定できます。この ID は内部管理専用のため、他のどのデバイス上の ID とも照合する必要はありません。最大 2 つのプロセスが使用できます。

ステップ 2 インターフェイスでのルーティング アップデートの送受信を抑止します。

passive-interface [*interface_name*]

例：

```
ciscoasa(config-rtr)# passive-interface inside
```

interface_name 引数は、OSPFv3 プロセスが実行されているインターフェイスの名前を指定します。*no interface_name* 引数を指定すると、OSPFv3 プロセス *process_id* のすべてのインターフェイスがパッシブとなります。

OSPFv3 アドミニストレーティブ ディスタンスの設定

手順

ステップ 1 OSPFv3 のルーティング プロセスをイネーブルにします。

ipv6 router ospf *process_id*

例：

```
ciscoasa(config-if)# ipv6 router ospf 1
```

process_id 引数は、このルーティング プロセス内部で使用される識別子です。ローカルに割り当てられ、1 ～ 65535 の任意の正の整数を指定できます。この ID は内部管理専用のため、他のどのデバイス上の ID とも照合する必要はありません。最大 2 つのプロセスが使用できます。

ステップ 2 OSPFv3 ルートのアドミニストレーティブ ディスタンスを設定します。

distance [**ospf** {**external** | **inter-area** | **intra-area**}] *distance*

例：

```
ciscoasa(config-rtr)# distance ospf external 200
```

ospf キーワードは、OSPFv3 ルートを指定します。**external** キーワードは、OSPFv3 の外部タイプ 5 およびタイプ 7 ルートを指定します。**inter-area** キーワードは、OSPVv3 のエリア間ルートを指定します。**intra-area** キーワードは、OSPFv3 のエリア内ルートを指定します。*distance* 引数は、10 ～ 254 の整数であるアドミニストレーティブ ディスタンスを指定します。

OSPFv3 タイマーの設定

OSPFv3 の LSA 到着タイマー、LSA ペーシング タイマー、およびスロットリング タイマーを設定できます。

手順

ステップ 1 OSPFv3 のルーティング プロセスをイネーブルにします。

ipv6 router ospf *process-id*

例：

```
ciscoasa(config-if)# ipv6 router ospf 1
```

process-id 引数は、このルーティング プロセス内部で使用される識別子です。ローカルに割り当てられ、1 ～ 65535 の任意の正の整数を指定できます。この ID は内部管理専用のため、他のどのデバイス上の ID とも照合する必要はありません。最大 2 つのプロセスが使用できます。

ステップ 2 ASAが OSPF ネイバーから同一の LSA を受け入れる最小間隔を設定します。

timers lsa arrival *milliseconds*

例：

```
ciscoasa(config-rtr)# timers lsa arrival 2000
```

milliseconds 引数は、ネイバーから到着する同じ LSA の受け入れの間で経過する最小遅延をミリ秒単位で指定します。有効な範囲は 0 ～ 6,000,000 ミリ秒です。デフォルトは 1000 ミリ秒です。

ステップ 3 LSA フラッド パケット ペーシングを設定します。

timers pacing flood *milliseconds*

例：

```
ciscoasa(config-rtr)# timers lsa flood 20
```

milliseconds 引数は、フラッディング キュー内の LSA が更新と更新の間にペーシングされる時間（ミリ秒）を指定します。設定できる範囲は 5 ～ 100 ミリ秒です。デフォルト値は 33 ミリ秒です。

ステップ 4 OSPFv3 LSA を収集してグループ化し、リフレッシュ、チェックサム、またはエージングを行う間隔を変更します。

timers pacing lsa-group *seconds*

例：

```
ciscoasa(config-rtr)# timers pacing lsa-group 300
```

seconds 引数は、LSA がグループ化、リフレッシュ、チェックサム計算、またはエージングされる間隔を秒単位で指定します。有効な範囲は 10 ～ 1800 秒です。デフォルト値は 240 秒です。

ステップ 5 LSA 再送信パケット ペーシングを設定します。

timers pacing retransmission *milliseconds*

例：

```
ciscoasa(config-rtr)# timers pacing retransmission 100
```

milliseconds 引数は、再送信キュー内の LSA がペーシングされる時間（ミリ秒）を指定します。設定できる範囲は 5 ～ 200 ミリ秒です。デフォルト値は 66 ミリ秒です。

ステップ 6 OSPFv3 LSA スロットリングを設定します。

timers throttle lsa *milliseconds1 milliseconds2 milliseconds3*

例：

```
ciscoasa(config-rtr)# timers throttle lsa 500 6000 8000
```

- *milliseconds1* 引数は、LSA の最初のオカレンスを生成する遅延をミリ秒単位で指定します。*milliseconds2* 引数は、同じ LSA を送信する最大遅延をミリ秒単位で指定します。*milliseconds3* 引数は、同じ LSA を送信する最小遅延をミリ秒単位で指定します。
- LSA スロットリングでは、最小時間または最大時間が最初のオカレンスの値よりも小さい場合、OSPFv3 が自動的に最初のオカレンス値に修正します。同様に、指定された最遅延が最小遅延よりも小さい場合、OSPFv3 が自動的に最小遅延値に修正します。
- *milliseconds1* の場合、デフォルト値は 0 ミリ秒です。
- *milliseconds2* および *milliseconds3* の場合、デフォルト値は 5000 ミリ秒です。

ステップ 7 OSPFv3 SPF スロットリングを設定します。

timers throttle spf *milliseconds1 milliseconds2 milliseconds3*

例：

```
ciscoasa(config-rtr)# timers throttle spf 5000 12000 16000
```

- *milliseconds1* 引数は、SPF 計算の変更を受信する遅延をミリ秒単位で指定します。*milliseconds2* 引数は、最初と 2 番目の SPF 計算の間の遅延をミリ秒単位で指定します。*milliseconds3* 引数は、SPF 計算の最大待機時間をミリ秒単位で指定します。
- SPF スロットリングでは、*milliseconds2* または *milliseconds3* が *milliseconds1* よりも小さい場合、OSPFv3 が自動的に *milliseconds1* の値に修正します。同様に、*milliseconds3* が *milliseconds2* より小さい場合、OSPFv3 が自動的に *milliseconds2* の値に修正します。
- *milliseconds1* の場合、SPF スロットリングのデフォルト値は 5000 ミリ秒です。
- *milliseconds2* および *milliseconds3* の場合、SPF スロットリングのデフォルト値は 10000 ミリ秒です。

スタティック OSPFv3 ネイバーの定義

ポイントツーポイントの非ブロードキャストネットワークを介して OSPFv3 ルートをアドバタイズするには、スタティック OSPF ネイバーを定義する必要があります。この機能により、OSPFv3 アドバタイズメントを GRE トンネルにカプセル化しなくても、既存の VPN 接続でブロードキャストすることができます。

開始する前に、OSPFv3 ネイバーに対するスタティック ルートを作成する必要があります。スタティック ルートの作成方法の詳細については、スタティック ルートの設定（712ページ）を参照してください。

手順

ステップ 1 OSPFv3 ルーティング プロセスをイネーブルにし、IPv6 ルータ コンフィギュレーション モードを開始します。

ipv6 router ospf *process-id*

例：

```
ciscoasa(config)# ipv6 router ospf 1
```

process-id 引数は、このルーティング プロセス内部で使用される識別子です。ローカルに割り当てられ、1 ～ 65535 の任意の正の整数を指定できます。この ID は内部管理専用のため、他のどのデバイス上の ID とも照合する必要はありません。最大 2 つのプロセスが使用できます。

ステップ 2 非ブロードキャスト ネットワークへの OSPFv3 ルータの相互接続を設定します。

ipv6 ospf neighbor *ipv6-address* [**priority** *number*] [**poll-interval** *seconds*] [**cost** *number*] [**database-filter all out**]

例：

```
ciscoasa(config-if)# interface ethernet0/0 ipv6 ospf neighbor FE80::A8BB:CCFF:FE00:C01
```

OSPFv3 デフォルト パラメータのリセット

OSPFv3 パラメータをデフォルト値に戻すには、次の手順を実行します。

手順

ステップ 1 OSPFv3 のルーティング プロセスをイネーブルにします。

ipv6 router ospf *process-id*

例：

```
ciscoasa(config-if)# ipv6 router ospf 1
```

process_id 引数は、このルーティング プロセス内部で使用される識別子です。ローカルに割り当てられ、1 ～ 65535 の任意の正の整数を指定できます。この ID は内部管理専用のため、他のどのデバイス上の ID とも照合する必要はありません。最大 2 つのプロセスが使用できます。

ステップ 2 オプションのパラメータをデフォルト値に戻します。

default [**area** | **auto-cost** | **default-information** | **default-metric** | **discard-route** | **discard-route** | **distance** | **distribute-list** | **ignore** | **log-adjacency-changes** | **maximum-paths** | **passive-interface** | **redistribute** | **router-id** | **summary-prefix** | **timers**]

例：

```
ciscoasa(config-rtr)# default metric 5
```

- **area** キーワードは、OSPFv3 エリア パラメータを指定します。**auto-cost** キーワードは、帯域幅に従って OSPFv3 インターフェイス コストを指定します。
- **default-information** キーワードはデフォルト情報を配布します。**default-metric** キーワードは、再配布ルートのメトリックを指定します。
- **discard-route** キーワードは、廃棄ルートのインストールをイネーブルまたはディセーブルにします。**distance** キーワードはアドミニストレーティブ ディスタンスを指定します。
- **distribute-list** キーワードは、ルーティング アップデートのネットワークをフィルタリングします。
- **Ignore** キーワードは、特定のイベントを無視します。**log-adjacency-changes** キーワードは、隣接状態の変更をログに記録します。
- **maximum-paths** キーワードは、複数のパスを介して複数のパケットを転送します。
- **passive-interface** キーワードは、インターフェイス上のルーティング アップデートを抑止します。
- **redistribute** キーワードは、別のルーティング プロトコルからの IPv6 プレフィックスを再配布します。
- **router-id** キーワードは、指定されたルーティング プロセスのルータ ID を指定します。
- **summary-prefix** キーワードは、IPv6 サマリー プレフィックスを指定します。
- **timers** キーワードは、OSPFv3 タイマーを指定します。

Syslog メッセージの送信

OSPFv3 ネイバーが起動または停止したときに、ルータが syslog メッセージを送信するように設定します。

手順

ステップ 1 OSPFv3 のルーティング プロセスをイネーブルにします。

ipv6 router ospf *process-id*

例：

```
ciscoasa(config-if)# ipv6 router ospf 1
```

process-id 引数は、このルーティング プロセス内部で使用される識別子です。ローカルに割り当てられ、1 ～ 65535 の任意の正の整数を指定できます。この ID は内部管理専用のため、他のどのデバイス上の ID とも照合する必要はありません。最大 2 つのプロセスが使用できます。

ステップ 2 OSPFv3 ネイバーが起動または停止したときに、ルータが syslog メッセージを送信するように設定します。

log-adjacency-changes [**detail**]

例：

```
ciscoasa(config-rtr)# log-adjacency-changes detail
```

detail キーワードは、OSPFv3 ネイバーが起動または停止したときだけではなく、各状態の syslog メッセージを送信します。

Syslog メッセージの抑止

ルータがサポートされていない LSA タイプ 6 Multicast OSPF（MOSPF）パケットを受信した場合の syslog メッセージの送信を抑止するには、次の手順を実行します。

手順

ステップ 1 OSPFv2 のルーティング プロセスをイネーブルにします。

router ospf *process_id*

例：

```
ciscoasa(config-if)# router ospf 1
```

process_id 引数は、このルーティング プロセス内部で使用される識別子です。ローカルに割り当てられ、1 ～ 65535 の任意の正の整数を指定できます。この ID は内部管理専用のため、他のどのデバイス上の ID とも照合する必要はありません。最大 2 つのプロセスが使用できます。

ステップ 2 ルータが、サポートされていない LSA タイプ 6 MOSPF パケットを受信した場合の syslog メッセージの送信を抑止します。

ignore lsa mospf

例：

```
ciscoasa(config-rtr)# ignore lsa mospf
```

集約ルート コストの計算

手順

RFC 1583 に従ってサマリー ルート コストの計算に使用される方式に復元します。

compatible rfc1583

例：

```
ciscoasa (config-rtr)# compatible rfc1583
```

OSPFv3 ルーティング ドメインへのデフォルトの外部ルートの生成

手順

ステップ 1 OSPFv3 のルーティング プロセスをイネーブルにします。

ipv6 router ospf *process-id*

例：

```
ciscoasa(config-if)# ipv6 router ospf 1
```

process-id 引数は、このルーティング プロセス内部で使用される識別子です。ローカルに割り当てられ、1 ～ 65535 の任意の正の整数を指定できます。この ID は内部管理専用のため、他のどのデバイス上の ID とも照合する必要はありません。最大 2 つのプロセスが使用できます。

ステップ 2 OSPFv3 ルーティング ドメインへのデフォルトの外部ルートを生成します。

default-information originate [**always**] **metric** *metric-value* [**metric-type** *type-value*] [**route-map** *map-name*]

例：

```
ciscoasa(config-rtr)# default-information originate always metric 3 metric-type 2
```

- **always** キーワードは、デフォルト ルートがあるかどうかにかかわらず、デフォルト ルートをアドバタイズします。

- **metric** *metric-value* キーワード引数のペアは、デフォルト ルートの生成に使用するメトリックを指定します。
- **default-metric** コマンドを使用して値を指定しない場合、デフォルト値は 10 です。有効なメトリック値の範囲は、0 ～ 16777214 です。
- **metric-type** *type-value* キーワード引数のペアは、OSPFv3 ルーティング ドメインにアドバタイズされるデフォルト ルートに関連付けられる外部リンク タイプを指定します。有効な値は次のいずれかになります。
  - 1：タイプ 1 外部ルート
  - 2：タイプ 2 外部ルート

  デフォルトはタイプ 2 外部ルートです。
- **route-map** *map-name* キーワード引数のペアは、ルート マップが一致している場合にデフォルト ルートを生成するルーティング プロセスを指定します。

IPv6 サマリー プレフィックスの設定

手順

ステップ 1 OSPFv3 のルーティング プロセスをイネーブルにします。

ipv6 router ospf *process-id*

例：

```
ciscoasa(config-if)# ipv6 router ospf 1
```

process_id 引数は、このルーティング プロセス内部で使用される識別子です。ローカルに割り当てられ、1 ～ 65535 の任意の正の整数を指定できます。この ID は内部管理専用のため、他のどのデバイス上の ID とも照合する必要はありません。最大 2 つのプロセスが使用できます。

ステップ 2 IPv6 サマリー プレフィックスを設定します。

summary-prefix *prefix* [**not-advertise** | **tag** *tag-value*]

例：

```
ciscoasa(config-if)# ipv6 router ospf 1
ciscoasa(config-rtr)# router-id 192.168.3.3
ciscoasa(config-rtr)# summary-prefix FECO::/24
ciscoasa(config-rtr)# redistribute static
```

prefix 引数は、宛先の IPv6 ルート プレフィックスです。**not-advertise** キーワードは、指定したプレフィックスとマスク ペアと一致するルートを抑止します。このキーワードは OSPFv3 だけ

に適用されます。**tag** *tag-value* キーワード引数のペアは、ルート マップで再配布を制御するために一致値として使用できるタグ値を指定します。このキーワードはOSPFv3 だけに適用されます。

IPv6 ルートの再配布

手順

ステップ 1 OSPFv3 のルーティング プロセスをイネーブルにします。

ipv6 router ospf *process-id*

例：

```
ciscoasa(config-if)# ipv6 router ospf 1
```

process-id 引数は、このルーティング プロセス内部で使用される識別子です。ローカルに割り当てられ、1 ～ 65535 の任意の正の整数を指定できます。この ID は内部管理専用のため、他のどのデバイス上の ID とも照合する必要はありません。最大 2 つのプロセスが使用できます。

ステップ 2 ある OSPFv3 プロセスから別の OSPFv3 プロセスに IPv6 ルートを再配布します。

redistribute *source-protocol* [*process-id*] [**include-connected** {[**level-1** | **level-2**}] [*as-number*] [**metric** [*metric-value* | **transparent**}] **[metric-type** *type-value*] [**match** {**external** [**1**|**2**] | **internal** | **nssa-external** [**1**|**2**]}] [**tag** *tag-value*] [**route-map** *map-tag*]

例：

```
ciscoasa(config-rtr)# redistribute connected 5 type-1
```

- *source-protocol* 引数は、ルートの再配布元となるソース プロトコルを指定します。これは、スタティック、接続済み、または OSPFv3 にすることができます。
- *process-id* 引数は、OSPFv3 ルーティング プロセスがイネーブルになったときに管理目的で割り当てられる番号です。
- **include-connected** キーワードは、ソース プロトコルから学習したルートと、ソース プロトコルが動作しているインターフェイス上の接続先プレフィックスを、ターゲット プロトコルが再配布できるようにします。
- **level-1** キーワードは、Intermediate System-to-Intermediate System（IS-IS）用に、レベル 1 ルートが他の IP ルーティング プロトコルに個別に再配布されることを指定します。
- **level-1-2** キーワードは、IS-IS 用に、レベル 1 とレベル 2 の両方のルートが他の IP ルーティング プロトコルに再配布されることを指定します。

- **level-2** キーワードは、IS-IS 用に、レベル 2 ルートが他の IP ルーティング プロトコルに個別に再配布されることを指定します。
- **metric** *metric-value* キーワード引数のペアでは、ある OSPFv3 プロセスのルートを同じルータ上の別の OSPFv3 プロセスに再配布する場合、メトリック値を指定しないと、メトリックは 1 つのプロセスから他のプロセスへ存続します。他のプロセスを OSPFv3 プロセスに再配布するときに、メトリック値を指定しない場合、デフォルトのメトリックは 20 です。
- **metric transparent** キーワードにより、RIP は RIP メトリックとして再配布ルートのルーティング テーブル メトリックを使用します。
- **metric-type** *type-value* キーワード引数のペアは、OSPFv3 ルーティング ドメインにアドバタイズされるデフォルト ルートに関連付けられる外部リンク タイプを指定します。有効な値は、タイプ 1 外部ルートの場合は 1、タイプ 2 外部ルートの場合は 2 です。**metric-type** キーワードに値が指定されていない場合、ASA は、タイプ 2 外部ルートを受け入れます。IS-IS の場合、リンク タイプは、63 未満の IS-IS メトリックの場合は内部、64 を超えて 128 未満の IS-IS メトリックの場合は外部となります。デフォルトは、内部です。
- **match** キーワードは、他のルーティング ドメインにルートを再配布し、次のいずれかのオプションとともに使用されます。自律システムの外部であり、タイプ 1 またはタイプ 2 の外部ルートとして OSPFv3 にインポートされるルートの場合は **external** [**1**|**2**]、特定の自律システムの内部にあるルートの場合は **internal**、自律システムの外部であり、タイプ 1 またはタイプ 2 の外部ルートとして IPv6 の NSSA で OSPFv3 にインポートされるルートの場合は **nssa-external** [**1**|**2**]。
- **tag** *tag-value* キーワード引数のペアは、ASBR 間で情報を通信するために使用できる、各外部ルートに付加される 32 ビットの 10 進数値を指定します。何も指定しない場合、BGP および EGP からのルートにはリモート自律システムの番号が使用されます。その他のプロトコルについては、ゼロが使用されます。有効値の範囲は、0 ～ 4294967295 です。
- **route-map** キーワードは、送信元ルーティング プロトコルから現在のルーティング プロトコルへのルートのインポートのフィルタリングをチェックするルート マップを指定します。このキーワードを指定しない場合、すべてのルートが再配布されます。このキーワードを指定し、ルート マップ タグが表示されていない場合、ルートはインポートされません。*map-tag* 引数は、設定されたルート マップを識別します。

グレースフル リスタートの設定

ASA では、既知の障害状況が発生することがあります。これにより、スイッチング プラットフォーム全体でパケット転送に影響を与えることがあってはなりません。Non-Stop Forwarding（NSF）機能では、ルーティング プロトコル情報を復元している間に、既知のルートへのデータ転送が続行されます。この機能は、コンポーネントに障害がある場合（フェールオーバー（HA）モードで処理を引き継ぐスタンバイ ユニットが存在するアクティブ ユニットがクラッシュした場合や、クラスタ モードで新しいマスターとして選択されたスレーブ ユニットが存

在するマスターユニットがクラッシュした場合など）、またはスケジュールされたヒットレスソフトウェア アップグレードがある場合に役立ちます。

グレースフル リスタートは、OSPFv2 と OSPFv3 の両方でサポートされています。NSF Cisco（RFC 4811 および RFC 4812）または NSF IETF（RFC 3623）のいずれかを使用して、OSPFv2 上でグレースフル リスタートを設定できます。graceful-restart（RFC 5187）を使用して、OSPFv3 上でグレースフル リスタートを設定できます。

NSF グレースフル リスタート機能の設定には、機能の設定と NSF 対応または NSF 認識としてのデバイスの設定という 2 つのステップが伴います。NSF 対応デバイスは、ネイバーに対して独自のリスタート アクティビティを示すことができ、NSF 認識デバイスはネイバーのリスタートをサポートすることができます。

デバイスは、いくつかの条件に応じて、NSF 対応または NSF 認識として設定できます。

- デバイスは、現在のデバイスのモードに関係なく、NSF 認識デバイスとして設定できます。
- デバイスを NSF 対応として設定するには、デバイスはフェールオーバーまたはスパンド EtherChannel（L2）クラスタ モードのいずれかである必要があります。
- デバイスを NSF 認識または NSF 対応にするには、必要に応じて opaque リンク ステート アドバタイズメント（LSA）/リンク ローカル シグナリング（LLS）ブロックの機能を使って設定する必要があります。

（注） OSPFv2 用に fast hello が設定されている場合、アクティブ ユニットのリロードが発生し、スタンバイ ユニットがアクティブになっても、グレースフル リスタートは発生しません。これは、ロール変更にかかる時間は、設定されているデッド インターバルよりも大きいためです。

機能の設定

Cisco NSF グレースフル リスタート メカニズムは、リスタート アクティビティを示すために、Hello パケットで RS ビットが設定された LLS ブロックを送信するため、LLS 機能に依存しています。IETF NSF メカニズムは、リスタート アクティビティを示すために、タイプ 9 の opaque LSA を送信するため、opaque LSA 機能に依存しています。機能を設定するには、次のコマンドを入力します。

手順

ステップ 1 OSPF ルーティング プロセスを作成し、再配布する OSPF プロセスのルータ コンフィギュレーション モードに入ります。

router ospf *process_id*

例：

```
ciscoasa(config)# router ospf 2
```

process_id 引数は、このルーティング プロセス内部で使用される識別子です。任意の正の整数を使用できます。この ID は内部専用のため、他のどのデバイス上の ID とも照合する必要はありません。最大 2 つのプロセスが使用できます。

ステップ 2 LLS データ ブロックまたは opaque LSA の使用をイネーブルにして、NSF をイネーブルにします。

capability {lls|opaque}

lls キーワードは、Cisco NSF グレースフル リスタート メカニズムに対して、LLS 機能をイネーブルにするために使用されます。

opaque キーワードは、IETF NSF グレースフル リスタート メカニズムに対して、opaque LSA 機能をイネーブルにするために使用されます。

OSPFv2 のグレースフル リスタートの設定

OSPFv2、Cisco NSF および IETF NSF には、2 つのグレースフル リスタート メカニズムがあります。OSPF インスタンスに対しては、これらのグレースフル リスタート メカニズムのうち一度に設定できるのは 1 つだけです。NSF 認識デバイスは、Cisco NSF ヘルパーと IETF NSF ヘルパーの両方として設定できますが、NSF 対応デバイスは OSPF インスタンスに対して、Cisco NSF または IETF NSF モードのいずれかとして設定できます。

OSPFv2 の Cisco NSF グレースフル リスタートの設定

NSF 対応または NSF 認識デバイスに対して、OSPFv2 の Cisco NSF グレースフル リスタートを設定します。

手順

ステップ 1 NSF 対応デバイスで Cisco NSF をイネーブルにします。

nsf cisco [enforce global]

例：

```
ciscoasa(config-router)# nsf cisco
```

enforce global キーワードは、非 NSF 認識ネイバー デバイスが検出されると、NSF リスタートをキャンセルします。

ステップ 2 NSF 認識デバイスで、Cisco NSF ヘルパー モードをイネーブルにします。

capability {lls|opaque}

例：

```
ciscoasa(config-router)# capability lls
```

このコマンドは、デフォルトでイネーブルになっています。このコマンドの no 形式を使用すると、ディセーブルになります。

OSPFv2 の IETF NSF グレースフル リスタートの設定

NSF 対応または NSF 認識デバイスに対して、OSPFv2 の IETF NSF グレースフル リスタートを設定します。

手順

ステップ 1 NSF 対応デバイスで IETF NSF を有効にします。

nsf ietf [restart interval seconds]

例：

```
ciscoasa(config-router)# nsf ietf restart interval 80
```

restart interval seconds は、グレースフル リスタート間隔の長さを秒単位で指定します。有効な値は 1 ～ 1800 秒です。デフォルト値は 120 秒です。

隣接関係（アジャセンシー）が有効になるまでにかかる時間よりも再起動間隔が小さい値に設定されている場合、グレースフル リスタートは終了することがあります。たとえば、30 秒以下の再起動間隔はサポートされていません。

ステップ 2 NSF 認識デバイスで、IETF NSF ヘルパー モードをイネーブルにします。

nsf ietf helper [strict-lsa-checking]

例：

```
ciscoasa(config-router)# nsf ietf helper
```

strict-LSA-checking キーワードは、再起動ルータにフラッディングされる可能性がある LSA への変更があることが検出された場合、またはグレースフル リスタート プロセスが開始されたときに再起動ルータの再送リスト内に変更された LSA があると検出された場合、ヘルパー ルータはルータの再起動プロセスを終了させることを示します。

このコマンドは、デフォルトでイネーブルになっています。このコマンドの no 形式を使用すると、ディセーブルになります。

OSPFv3 のグレースフル リスタートの設定

OSPFv3 の NSF グレースフル リスタート機能を設定するには、2 つのステップを伴います。NSF 対応としてのデバイスの設定と、NSF 認識としてのデバイスの設定です。

手順

ステップ 1 明示的な IPv6 アドレスが設定されていないインターフェイスにおける IPv6 処理をイネーブルにします。

interface physical_interface ipv6 enable

例：

```
ciscoasa(config)# interface ethernet 0/0
ciscoasa(config-if)# ipv6 enable
```

physical_interface 引数は、OSPFv3 NSF に参加するインターフェイスを識別します。

ステップ 2 NSF 対応デバイスで OSPFv3 のグレースフル リスタートをイネーブルにします。

graceful-restart [restart interval seconds]

例：

```
ciscoasa(config-router)# graceful-restart restart interval 80
```

restart interval seconds は、グレースフル リスタート間隔の長さを秒単位で指定します。有効な値は 1 ～ 1800 秒です。デフォルト値は 120 秒です。

隣接関係（アジャセンシー）が有効になるまでにかかる時間よりもリスタート間隔が小さい値に設定されている場合、グレースフル リスタートは終了することがあります。たとえば 30 秒以下の再起動間隔は、サポートされていません。

ステップ 3 NSF 認識デバイスで OSPFv3 のグレースフル リスタートをイネーブルにします。

graceful-restart helper [strict-lsa-checking]

例：

```
ciscoasa(config-router)# graceful-restart helper strict-lsa-checking
```

strict-LSA-checking キーワードは、再起動ルータにフラッディングされる可能性がある LSA への変更があることが検出された場合、またはグレースフル リスタート プロセスが開始されたときに再起動ルータの再送リスト内に変更された LSA があると検出された場合、ヘルパールータはルータの再起動プロセスを終了させることを示します。

グレースフル リスタート ヘルパー モードは、デフォルトでイネーブルになっています。

OSPFv2 設定の削除

OSPFv2 設定を削除します。

手順

イネーブルにした OSPFv2 設定全体を削除します。

clear configure router ospf *pid*

例：

```
ciscoasa(config)# clear configure router ospf 1000
```

設定をクリアした後、**router ospf** コマンドを使用して OSPF を再設定する必要があります。

OSPFv3 設定の削除

OSPFv3 設定を削除します。

手順

イネーブルにした OSPFv3 設定全体を削除します。

clear configure ipv6 router ospf *process-id*

例：

```
ciscoasa(config)# clear configure ipv6 router ospf 1000
```

設定をクリアした後、**ipv6 router ospf** コマンドを使用して OSPFv3 を再設定する必要があります。

OSPFv2 の例

次の例に、さまざまなオプションのプロセスを使用して OSPFv2 をイネーブルにし、設定する方法を示します。

1. OSPFv2 をイネーブルにするには、次のコマンドを入力します。

```
ciscoasa(config)# router ospf 2
```

```
ciscoasa(config-rtr)# network 10.0.0.0 255.0.0.0 area 0
```

2. （オプション）1 つの OSPFv2 プロセスから別の OSPFv2 プロセスにルートを再配布するには、次のコマンドを入力します。

```
ciscoasa(config)# route-map 1-to-2 permit
ciscoasa(config-route-map)# match metric 1
ciscoasa(config-route-map)# set metric 5
ciscoasa(config-route-map)# set metric-type type-1
ciscoasa(config-route-map)# router ospf 2
ciscoasa(config-rtr)# redistribute ospf 1 route-map 1-to-2
```

3. （オプション）OSPFv2 インターフェイス パラメータを設定するには、次のコマンドを入力します。

```
ciscoasa(config)# router ospf 2
ciscoasa(config-rtr)# network 10.0.0.0 255.0.0.0 area 0
ciscoasa(config-rtr)# interface inside
ciscoasa(config-interface)# ospf cost 20
ciscoasa(config-interface)# ospf retransmit-interval 15
ciscoasa(config-interface)# ospf transmit-delay 10
ciscoasa(config-interface)# ospf priority 20
ciscoasa(config-interface)# ospf hello-interval 10
ciscoasa(config-interface)# ospf dead-interval 40
ciscoasa(config-interface)# ospf authentication-key cisco
ciscoasa(config-interface)# ospf message-digest-key 1 md5 cisco
ciscoasa(config-interface)# ospf authentication message-digest
```

4. （オプション）OSPFv2 エリア パラメータを設定するには、次のコマンドを入力します。

```
ciscoasa(config)# router ospf 2
ciscoasa(config-rtr)# area 0 authentication
ciscoasa(config-rtr)# area 0 authentication message-digest
ciscoasa(config-rtr)# area 17 stub
ciscoasa(config-rtr)# area 17 default-cost 20
```

5. （オプション）ルート計算タイマーを設定し、ログにネイバーのアップおよびダウンのメッセージを表示するには、次のコマンドを入力します。

```
ciscoasa(config-rtr)# timers spf 10 120
ciscoasa(config-rtr)# log-adj-changes [detail]
```

6. （オプション）現在の OSPFv2 の設定を表示するには、**show ospf** コマンドを入力します。

次に、 **show ospf** コマンドの出力例を示します。

```
ciscoasa(config)# show ospf

Routing Process “ospf 2” with ID 10.1.89.2 and Domain ID 0.0.0.2
Supports only single TOS(TOS0) routes
Supports opaque LSA
SPF schedule delay 5 secs, Hold time between two SPFs 10 secs
Minimum LSA interval 5 secs. Minimum LSA arrival 1 secs
```

```
Number of external LSA 5. Checksum Sum 0x 26da6
Number of opaque AS LSA 0. Checksum Sum 0x     0
Number of DCbitless external and opaque AS LSA 0
Number of DoNotAge external and opaque AS LSA 0
Number of areas in this router is 1. 1 normal 0 stub 0 nssa
External flood list length 0
    Area BACKBONE(0)
        Number of interfaces in this area is 1
        Area has no authentication
        SPF algorithm executed 2 times
        Area ranges are
        Number of LSA 5. Checksum Sum 0x 209a3
        Number of opaque link LSA 0. Checksum Sum 0x     0
        Number of DCbitless LSA 0
        Number of indication LSA 0
        Number of DoNotAge LSA 0
        Flood list length 0
```

7. OSPFv2 設定をクリアするには、次のコマンドを入力します。

```
ciscoasa(config)# clear configure router ospf pid
```

OSPFv3 の例

次に、インターフェイス レベルで OSPFv3 をイネーブルにして設定する例を示します。

```
ciscoasa (config)# interface GigabitEthernet3/1
ciscoasa (config-if)# ipv6 enable
ciscoasa (config-if)# ipv6 ospf 1 area 1
```

次に、**show running-config ipv6** コマンドの出力例を示します。

```
ciscoasa (config)# show running-config ipv6
ipv6 router ospf 1
 log-adjacency-changes
```

次に、**show running-config interface** コマンドの出力例を示します。

```
ciscoasa (config-if)# show running-config interface GigabitEthernet3/1
interface GigabitEthernet3/1
 nameif fda
 security-level 100
 ip address 1.1.11.1 255.255.255.0 standby 1.1.11.2
 ipv6 address 9098::10/64 standby 9098::11
 ipv6 enable
 ipv6 ospf 1 area 1
```

次に、OSPFv3 専用インターフェイスを設定する例を示します。

```
ciscoasa (config)# interface GigabitEthernet3/1
ciscoasa (config-if)# nameif fda
ciscoasa (config-if)# security-level 100
ciscoasa (config-if)# ip address 10.1.11.1 255.255.255.0 standby 10.1.11.2
```

```
ciscoasa (config-if)# ipv6 address 9098::10/64 standby 9098::11
ciscoasa (config-if)# ipv6 enable
ciscoasa (config-if)# ipv6 ospf cost 900
ciscoasa (config-if)# ipv6 ospf hello-interval 20
ciscoasa (config-if)# ipv6 ospf network broadcast
ciscoasa (config-if)# ipv6 ospf database-filter all out
ciscoasa (config-if)# ipv6 ospf flood-reduction
ciscoasa (config-if)# ipv6 ospf mtu-ignore
ciscoasa (config-if)# ipv6 ospf 1 area 1 instance 100
ciscoasa (config-if)# ipv6 ospf encryption ipsec spi 890 esp null md5
123456789012345678901234567890 12

ciscoasa (config)# ipv6 router ospf 1
ciscoasa (config)# area 1 nssa
ciscoasa (config)# distance ospf intra-area 190 inter-area 100 external 100
ciscoasa (config)# timers lsa arrival 900
ciscoasa (config)# timers pacing flood 100
ciscoasa (config)# timers throttle lsa 900 900 900
ciscoasa (config)# passive-interface fda
ciscoasa (config)# log-adjacency-changes
ciscoasa (config)# redistribute connected metric 100 metric-type 1 tag 700
```

OSPFv3 仮想リンクを設定する方法の例については、次の URL を参照してください:

http://www.cisco.com/en/US/tech/tk365/technologies_configuration_example09186a0080b8fd06.shtml

OSPF のモニタリング

IP ルーティング テーブルの内容、キャッシュの内容、およびデータベースの内容など、特定の統計情報を表示できます。提供される情報は、リソースの使用状況を判定してネットワークの問題を解決するために使用することもできます。また、ノードの到達可能性情報を表示して、デバイス パケットがネットワークを通過するときにとるルーティング パスを見つけることもできます。

さまざまな OSPFv2 ルーティング統計情報をモニタまたは表示するには、次のいずれかのコマンドを入力します。

コマンド	目的
show ospf [*process-id* [*area-id*]]	OSPFv2 ルーティング プロセスに関する一般情報を表示します。
show ospf border-routers	ABR および ASBR までの内部 OSPFv2 ルーティング テーブル エントリを表示します。
show ospf [*process-id* [*area-id*]] database	特定のルータの OSPFv2 データベースに関係する情報のリストを表示します。

コマンド	目的
show ospf flood-list *if-name*	（OSPFv2 パケット ペーシングの観察のため）インターフェイスへのフラッディングを待機している LSA のリストを表示します。 OSPFv2 アップデート パケットは、自動的にペーシングされるため、各パケットの送信間隔が 33 ミリ秒未満になることはありません。ペーシングを行わないと、リンクが低速の状態でアップデート パケットの一部が失われたり、ネイバーがアップデートを十分すばやく受信できなくなったり、あるいは、ルータがバッファ スペースを使い切ってしまったりすることがあります。たとえば、ペーシングを行わないと、次のいずれかのトポロジが存在する場合にパケットがドロップされる可能性があります。 • 高速ルータがポイントツーポイント リンクを介して低速のルータと接続している。 • フラッディング中に、複数のネイバーから 1 つのルータに同時にアップデートが送信される。 ペーシングは、再送信間でも、送信効率を高めて再送信パケットの損失を最小にするために利用されます。インターフェイスからの送信を待機している LSA を表示することもできます。ペーシングの利点は、OSPFv2 アップデートおよび再送信パケットの送信の効率をよくすることです。 この機能を設定するタスクはありません。自動的に行われます。
show ospf interface [*if_name*]	OSPFv2-related インターフェイスの情報を表示します。
show ospf neighbor [*interface-name*] [*neighbor-id*] [**detail**]	OSPFv2 ネイバー情報をインターフェイスごとに表示します。
show ospf request-list *neighbor if_name*	ルータで要求されるすべての LSA のリストを表示します。
show ospf retransmission-list *neighbor if_name*	再送信を待機しているすべての LSA のリストを表示します。

コマンド	目的
show ospf [*process-id*] summary-address	OSPFv2 プロセスで設定されているサマリー アドレスのすべての再配布情報のリストを表示します。
show ospf [*process-id*] **traffic**	特定の OSPFv2 インスタンスで送信または受信されたパケットのさまざまなタイプのリストを表示します。
show ospf [*process-id*] virtual-links	OSPFv2-related 仮想リンク情報を表示します。
show route cluster	クラスタリングの追加 OSPFv2 ルートの同期情報を表示します。

さまざまな OSPFv3 ルーティング統計情報をモニタまたは表示するには、次のいずれかのコマンドを入力します。

コマンド	目的
show ipv6 ospf [*process-id* [*area-id*]]	OSPFv3 ルーティング プロセスに関する一般的な情報を表示します。
show ipv6 ospf [*process-id*] **border-routers**	ABR および ASBR までの内部 OSPFv3 ルーティング テーブル エントリを表示します。
show ipv6 ospf [*process-id* [*area-id*]] database [**external** | **inter-area prefix** | **inter-area-router** | **network** | **nssa-external** | **router** | **area** | **as** | **ref-lsa** | [*destination-router-id*] [**prefix** *ipv6-prefix*] [*link-state-id*]] [**link** [**interface** *interface-name*] [**adv-router** *router-id*] | **self-originate**] [**internal**] [**database-summary**]	特定のルータの OSPFv3 データベースに関する情報のリストを表示します。
show ipv6 ospf [*process-id* [*area-id*]] **events**	OSPFv3 イベント情報を表示します。

コマンド	目的
show ipv6 ospf [*process-id*] [*area-id*] flood-list *interface-type interface-number*	（OSPFv3 パケット ペーシングの観察のため）インターフェイスへのフラッディングを待機している LSA のリストを表示します。 OSPFv3 アップデート パケットは、自動的にペーシングされるため、各パケットの送信間隔が 33 ミリ秒未満になることはありません。ペーシングを行わないと、リンクが低速の状態でアップデート パケットの一部が失われたり、ネイバーがアップデートを十分すばやく受信できなくなったり、あるいは、ルータがバッファ スペースを使い切ってしまったりすることがあります。たとえば、ペーシングを行わないと、次のいずれかのトポロジが存在する場合にパケットがドロップされる可能性があります。 • 高速ルータがポイントツーポイント リンクを介して低速のルータと接続している。 • フラッディング中に、複数のネイバーから 1 つのルータに同時にアップデートが送信される。 ペーシングは、再送信間でも、送信効率を高めて再送信パケットの損失を最小にするために利用されます。インターフェイスからの送信を待機している LSA を表示することもできます。ペーシングの利点は、OSPFv3 アップデートおよび再送信パケットの送信の効率をよくすることです。 この機能を設定するタスクはありません。自動的に行われます。
show ipv6 ospf [*process-id*] [*area-id*] **interface** [*type number*] [**brief**]	OSPFv3 関連のインターフェイス情報を表示します。
show ipv6 ospf neighbor [*process-id*] [*area-id*] [*interface-type interface-number*] [*neighbor-id*] [**detail**]	OSPFv3 ネイバー情報をインターフェイスごとに表示します。
show ipv6 ospf [*process-id*] [*area-id*] **request-list** [*neighbor*] [*interface*] [*interface-neighbor*]	ルータで要求されるすべての LSA のリストを表示します。
show ipv6 ospf [*process-id*] [*area-id*] retransmission-list [*neighbor*] [*interface*] [*interface-neighbor*]	再送信を待機しているすべての LSA のリストを表示します。
show ipv6 ospf statistic [*process-id*] [**detail**]	さまざまな OSPFv3 統計情報を表示します。
show ipv6 ospf [*process-id*] summary-prefix	OSPFv3 プロセスで設定されているサマリー アドレスのすべての再配布情報のリストを表示します。
show ipv6 ospf [*process-id*] **timers** [**lsa-group** | **rate-limit**]	OSPFv3 タイマー情報を表示します。

コマンド	目的
show ipv6 ospf [*process-id*] **traffic** [*interface_name*]	OSPFv3 トラフィック関連の統計情報を表示します。
show ipv6 ospf virtual-links	OSPFv3-related 仮想リンク情報を表示します。
show ipv6 route cluster [**failover**] [**cluster**] [**interface**] [**ospf**] [**summary**]	クラスタ内の IPv6 ルーティング テーブルのシーケンス番号、IPv6 再コンバージェンス タイマーのステータス、および IPv6 ルーティング エントリのシーケンス番号を表示します。

OSPF の履歴

表 *28 : OSPF* の機能履歴

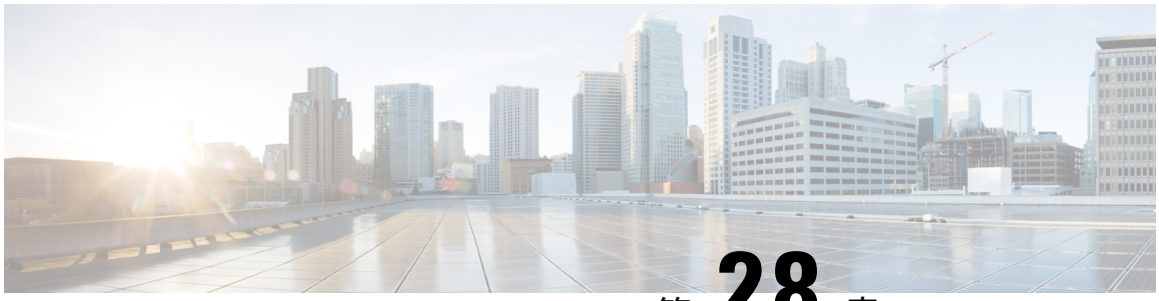
機能名	プラットフォーム リリース	機能情報
OSPF サポート	7.0(1)	Open Shortest Path First（OSPF）ルーティング プロトコルを使用した、データのルーティング、認証、およびルーティング情報の再配布とモニタについて、サポートが追加されました。 **route ospf** コマンドが導入されました。
マルチ コンテキスト モードのダイナミック ルーティング	9.0(1)	OSPFv2 ルーティングは、マルチ コンテキスト モードでサポートされます。
クラスタ	9.0(1)	OSPFv2 および OSPFv3 の場合、バルク同期、ルートの同期およびスパンド EtherChannel ロード バランシングは、クラスタリング環境でサポートされます。 **show route cluster**、**show ipv6 route cluster**、**debug route cluster**、**router-id cluster-pool** の各コマンドが導入または変更されました。

機能名	プラットフォーム リリース	機能情報
IPv6 の OSPFv3 サポート	9.0(1)	

機能名	プラットフォーム リリース	機能情報
		OSPFv3 ルーティングが IPv6 に対してサポートされます。 **ipv6 ospf、ipv6 ospf area、ipv6 ospf cost、ipv6 ospf database-filter all out、ipv6 ospf dead-interval、ipv6 ospf encryption、ipv6 ospf hello-interval、ipv6 ospf mtu-ignore、ipv6 ospf neighbor、ipv6 ospf network、ipv6 ospf flood-reduction、ipv6 ospf priority、ipv6 ospf retransmit-interval、ipv6 ospf transmit-delay、ipv6 router ospf、ipv6 router ospf area、ipv6 router ospf default、ipv6 router ospf default-information、ipv6 router ospf distance、ipv6 router ospf exit、ipv6 router ospf ignore、ipv6 router ospf log-adjacency-changes、ipv6 router ospf no、ipv6 router ospf passive-interface、ipv6 router ospf redistribute、ipv6 router ospf router-id、ipv6 router ospf summary-prefix、ipv6 router ospf timers、area encryption、area range、area stub、area nssa、area virtual-link、default、default-information originate、distance、ignore lsa mospf、log-adjacency-changes、redistribute、router-id、summary-prefix、timers lsa arrival、timers pacing flood、timers pacing lsa-group、timers pacing retransmission、timers throttle、show ipv6 ospf、show ipv6 ospf border-routers、show ipv6 ospf database、show ipv6 ospf events、show ipv6 ospf flood-list、show ipv6 ospf graceful-restart、show ipv6 ospf interface、show ipv6 ospf neighbor、show ipv6 ospf request-list、show ipv6 ospf retransmission-list、show ipv6 ospf statistic、show ipv6 ospf summary-prefix、show ipv6 ospf timers、show ipv6 ospf traffic、show**

機能名	プラットフォーム リリース	機能情報
		ipv6 ospf virtual-links、**show ospf**、**show running-config ipv6 router**、**clear ipv6 ospf**、**clear configure ipv6 router**、**debug ospfv3**、**ipv6 ospf neighbor** の各コマンドが導入または変更されました。
Fast Hello に対する OSPF サポート	9.2(1)	OSPF は、Fast Hello パケット機能をサポートしているため、OSPF ネットワークでのコンバージェンスが高速なコンフィギュレーションになります。 次のコマンドが変更されました。**ospf dead-interval**
タイマー	9.2(1)	新しい OSPF タイマーを追加し、古いタイマーを廃止しました。 次のコマンドが導入されました。timers lsa arrival、timers pacing、timers throttle 次のコマンドが削除されました。Timers spf、timers lsa-grouping-pacing
アクセスリストを使用したルートフィルタリング	9.2(1)	ACL を使用したルート フィルタリングがサポートされるようになりました。 次のコマンドが導入されました。distribute-list
OSPF モニタリングの強化	9.2(1)	OSPF モニタリングの詳細情報が追加されました。 次のコマンドが変更されました。show ospf events、show ospf rib、show ospf statistics、show ospf border-routers [detail]、show ospf interface brief
OSPF 再配布 BGP	9.2(1)	OSPF 再配布機能が追加されました。 次のコマンドが追加されました。redistribute bgp

機能名	プラットフォーム リリース	機能情報
ノンストップ フォワーディング（NSF）に対する OSPF のサポート	9.3(1)	NSF に対する OSPFv2 および OSPFv3 のサポートが追加されました。 次のコマンドが追加されました。capability、nsf cisco、nsf cisco helper、nsf ietf、nsf ietf helper、nsf ietf helper strict-lsa-checking、graceful-restart、graceful-restart helper、graceful-restart helper strict-lsa-checking
		NSF 待機タイマーが追加されました。 NSF 再起動間隔のタイマーを設定するための新しいコマンドが追加されました。このコマンドが導入され、待機間隔がルータの dead 間隔よりも長くならないようになりました。 次のコマンドが導入されました。 **timers nsf wait <seconds>**



第 28 章

EIGRP

この章では、Enhanced Interior Gateway Routing Protocol（EIGRP）を使用してデータをルーティングし、認証を実行し、ルーティング情報を再配布するように Cisco ASA を設定する方法について説明します。

EIGRP について

EIGRP は、シスコが開発した、IGRP の拡張バージョンです。IGRP や RIP と異なり、EIGRP が定期的にルート アップデートを送信することはありません。EIGRP アップデートは、ネットワーク トポロジが変更された場合にだけ送信されます。EIGRP を他のルーティング プロトコルと区別する主な機能には、迅速なコンバージェンス、可変長サブネット マスクのサポート、部分的アップデートのサポート、複数のネットワーク レイヤ プロトコルのサポートなどがあります。

EIGRP を実行するルータでは、すべてのネイバー ルーティング テーブルが格納されているため、代替ルートに迅速に適応できます。適切なルートが存在しない場合、EIGRP はそのネイバーにクエリーを送信して代替のルートを検出します。これらのクエリーは、代替ルートが検出されるまで伝搬します。EIGRP では可変長サブネット マスクがサポートされているため、ルートはネットワーク番号の境界で自動的に集約されます。さらに、任意のインターフェイスの任意のビット境界で集約を行うように EIGRP を設定することもできます。EIGRP は定期的なアップデートを行いません。その代わり、ルートのメトリックが変更されたときだけ、部分的なアップデートを送信します。部分的アップデートの伝搬では、境界が自動的に設定されるため、その情報を必要とするルータだけがアップデートされます。これらの 2 つの機能により、EIGRP の帯域幅消費量は IGRP に比べて大幅に減少します。

ネイバー探索は、ASA が直接接続されているネットワーク上にある他のルータをダイナミックに把握するために使用するプロセスです。EIGRP ルータは、マルチキャスト hello パケットを送信して、ネットワーク上に自分が存在していることを通知します。ASA は、新しいネイバーから hello パケットを受信すると、トポロジ テーブルに初期化ビットを設定してそのネイバーに送信します。ネイバーは、初期化ビットが設定されたトポロジアップデートを受信すると、自分のトポロジ テーブルを ASA に返送します。

hello パケットはマルチキャスト メッセージとして送信されます。hello メッセージへの応答は想定されていません。ただし、スタティックに定義されたネイバーの場合は例外です。**neighbor** コマンドを使用して（または ASDM で [Hello Interval] を設定して）ネイバーを設定すると、そのネイバーへ送信される hello メッセージはユニキャスト メッセージとして送信されます。ルーティング アップデートと確認応答が、ユニキャスト メッセージとして送信されます。

このネイバー関係が確立した後は、ネットワーク トポロジが変更された場合にだけ、ルーティング アップデートが交換されます。ネイバー関係は、hello パケットによって維持されます。ネイバーから受信した各 hello パケットには、保持時間が含まれています。ASA は、この時間内にそのネイバーから hello パケットを受信すると想定できます。ASA が保持時間内にそのネイバーからアドバタイズされた hello パケットを受信しない場合、ASA はそのネイバーを使用不能と見なします。

EIGRP プロトコルは、ネイバーの検出、ネイバーの回復、Reliable Transport Protocol（RTP）、およびルート計算に重要な DUAL を含む、4 の主要なアルゴリズム テクノロジーと 4 つの主要なテクノロジーを使用します。DUAL は、最小コストのルートだけでなく、宛先へのすべてのルートをトポロジ テーブルに保存します。最小コストのルートはルーティング テーブルに挿入されます。その他のルートは、トポロジテーブルに残ります。メインのルートに障害が発生したら、フィジブルサクセサから別のルートが選択されます。サクセサとは、宛先への最小コスト パスを持ち、パケット転送に使用される隣接ルータです。フィジビリティ計算によって、パスがルーティング ループを形成しないことが保証されます。

フィジブル サクセサがトポロジ テーブル内にない場合、必ずルート計算が発生します。ルートの再計算中、DUAL は EIGRP ネイバーにルートを求めるクエリーを送信して、次に EIGRP ネイバーがそのネイバーにクエリーを送信します。ルートのフィジブル サクセサがないルータは、到達不能メッセージを返します。

ルートの再計算中、DUAL は、ルートをアクティブとマークします。デフォルトでは、ASA は、ネイバーから応答が返ってくるのを 3 分間待ちます。ASA がネイバーから応答を受信しないと、そのルートは stuck-in-active とマークされます。トポロジ テーブル内のルートのうち、応答しないネイバーをフィジブル サクセサとして指しているものはすべて削除されます。

（注） EIGRP ネイバー関係では、GRE トンネルを使用しない IPsec トンネルの通過はサポートされていません。

EIGRP のガイドライン

ファイアウォール モードのガイドライン

ルーテッド ファイアウォール モードでだけサポートされています。トランスペアレント ファイアウォール モードはサポートされません。

クラスタのガイドライン

EIGRPは、個別のインターフェイス モードのクラスタ ピアとのネイバー関係を形成しません。

IPv6 のガイドライン

IPv6 はサポートされません。

コンテキストのガイドライン

- デフォルトでは、共有インターフェイス間でのマルチキャスト トラフィックのコンテキスト間交換がサポートされていないため、EIGRPインスタンスは共有インターフェイス間で相互に隣接関係を形成できません。ただし、EIGRP プロセスの EIGRP プロセス設定で静的ネイバー設定を使用すると、共有インターフェイスでの EIGRP ネイバーシップを形成できます。
- 個別のインターフェイスでのコンテキスト間 EIGRP がサポートされています。

その他のガイドライン

- 最大 1 つの EIGRP プロセスがサポートされます。
- 設定の変更が適用されるたびに、EIGRP隣接関係のフラップが発生し、特に配布リスト、オフセットリスト、および集約への変更のネイバーからの（送信または受信された）ルーティング情報が変更されます。ルータが同期されると、EIGRPはネイバー間の隣接関係を再確立します。隣接関係が壊れて再確立されると、ネイバー間で学習されたすべてのルートが消去され、新しい配布リストを使用して、ネイバー間の同期がすべて新しく実行されます。

EIGRP の設定

この項では、システムでEIGRPプロセスをイネーブルにする方法について説明します。EIGRPをイネーブルにした後に、システムで EIGRP プロセスをカスタマイズする方法については、次の項を参照してください。

EIGRP のイネーブル化

ASA でイネーブルにすることができる EIGRP ルーティング プロセスは 1 つだけです。

手順

ステップ 1 EIGRP ルーティング プロセスを作成して、この EIGRP プロセスのルータ コンフィギュレーション モードを開始します。

router eigrp as-num

例：

```
ciscoasa(config)# router eigrp 2
```

as-num 引数には、EIGRP ルーティング プロセスの自律システム番号を指定します。

ステップ 2 EIGRP ルーティングに参加するインターフェイスとネットワークを設定します。

network ip-addr [mask]

例：

```
ciscoasa(config)# router eigrp 2
ciscoasa(config-router)# network 10.0.0.0 255.0.0.0
```

このコマンドで、1 つ以上の **network** 文を設定できます。

直接接続されるネットワークとスタティック ネットワークが定義済みネットワークに含まれていれば、それらが ASA によってアドバタイズされます。さらに、定義されたネットワークに含まれる IP アドレスを持つインターフェイスだけが、EIGRP ルーティング プロセスに参加します。

アドバタイズするネットワークに接続されているインターフェイスを EIGRP ルーティングに参加させない場合は、EIGRP のインターフェイスの設定（855 ページ）を参照してください。

EIGRP スタブ ルーティングのイネーブル化

ASA を EIGRP スタブ ルータとしてイネーブル化し、設定することができます。スタブ ルーティングを使用すると、ASA で必要となるメモリおよび処理要件を減らすことができます。ASA をスタブ ルータとして設定すると、ローカル以外のトラフィックがすべて配布ルータに転送されるようになり、完全な EIGRP ルーティング テーブルを維持する必要がなくなります。一般に、配布ルータからスタブ ルートに送信する必要があるのは、デフォルト ルートだけです。

スタブ ルータから配布ルータには、指定されたルートだけが伝搬されます。スタブ ルータである ASA は、サマリー、接続されているルート、再配布されたスタティック ルート、外部ルー

ト、および内部ルートに対するクエリーすべてに、応答として「inaccessible」というメッセージを返します。ASA がスタブとして設定されているときは、自身のスタブ ルータとしてのステータスを報告するために、特殊なピア情報パケットをすべての隣接ルータに送信します。スタブ ステータスの情報を伝えるパケットを受信したネイバーはすべて、スタブ ルータにルートのクエリーを送信しなくなり、スタブ ピアを持つルータはそのピアのクエリーを送信しなくなります。スタブルータが正しいアップデートをすべてのピアに送信するには、配布ルータが必要です。

手順

ステップ 1 EIGRP ルーティング プロセスを作成して、この EIGRP プロセスのルータ コンフィギュレーション モードを開始します。

router eigrp as-num

例：

```
ciscoasa(config)# router eigrp 2
```

as-num 引数には、EIGRP ルーティング プロセスの自律システム番号を指定します。

ステップ 2 EIGRP ルーティングに参加するインターフェイスとネットワークを設定します。

network ip-addr [mask]

例：

```
ciscoasa(config)# router eigrp 2
ciscoasa(config-router)# network 10.0.0.0 255.0.0.0
```

このコマンドで、1 つ以上の **network** 文を設定できます。

直接接続されるネットワークとスタティック ネットワークが定義済みネットワークに含まれていれば、それらが ASA によってアドバタイズされます。さらに、定義されたネットワークに含まれる IP アドレスを持つインターフェイスだけが、EIGRP ルーティング プロセスに参加します。

アドバタイズするネットワークに接続されているインターフェイスを EIGRP ルーティングに参加させない場合は、パッシブ インターフェイスの設定（857 ページ）の項を参照してください。

ステップ 3 スタブ ルーティング プロセスを設定します。

eigrp stub {**receive-only** |[**connected**] [**redistributed**] [**static**] [**summary**]}

例：

```
ciscoasa(config)# router eigrp 2
ciscoasa(config-router)# network 10.0.0.0 255.0.0.0
ciscoasa(config-router)# eigrp stub {receive-only | [connected] [redistributed] [static]
 [summary]}
```

スタブ ルーティング プロセスから配布ルータにアドバタイズされるネットワークを指定する必要があります。スタティック ルートおよび接続されているネットワークが、自動的にスタブ ルーティング プロセスに再配布されることはありません。

（注） スタブ ルーティング プロセスでは、完全なトポロジ テーブルは維持されません。スタブ ルーティングには、ルーティングの決定を行うために、少なくとも配布ルータへのデフォルト ルートが必要です。

EIGRP のカスタマイズ

ここでは、EIGRP ルーティングをカスタマイズする方法について説明します。

EIGRP ルーティング プロセスのネットワークの定義

[Network] テーブルでは、EIGRP ルーティング プロセスで使用されるネットワークを指定できます。EIGRP ルーティングに参加するインターフェイスは、これらのネットワーク エントリで定義されるアドレスの範囲内に存在する必要があります。アドバタイズされる直接接続およびスタティックのネットワークも、これらのネットワーク エントリの範囲内である必要があります。

[Network] テーブルには、EIGRP ルーティング プロセス用に設定されているネットワークが表示されます。このテーブルの各行には、指定した EIGRP ルーティング プロセス用に設定されているネットワーク アドレスおよび関連するマスクが表示されます。

手順

ステップ 1 EIGRP ルーティング プロセスを作成して、この EIGRP プロセスのルータ コンフィギュレーション モードを開始します。

router eigrp as-num

例：

```
ciscoasa(config)# router eigrp 2
```

as-num 引数には、EIGRP ルーティング プロセスの自律システム番号を指定します。

ステップ 2 EIGRP ルーティングに参加するインターフェイスとネットワークを設定します。

network ip-addr [mask]

例：

```
ciscoasa(config)# router eigrp 2
ciscoasa(config-router)# network 10.0.0.0 255.0.0.0
```

このコマンドで、1 つ以上の **network** 文を設定できます。

直接接続されるネットワークとスタティック ネットワークが定義済みネットワークに含まれていれば、それらが ASA によってアドバタイズされます。さらに、定義されたネットワークに含まれる IP アドレスを持つインターフェイスだけが、EIGRP ルーティング プロセスに参加します。

アドバタイズするネットワークに接続されているインターフェイスを EIGRP ルーティングに参加させない場合は、パッシブ インターフェイスの設定（857 ページ）を参照してください。

EIGRP のインターフェイスの設定

アドバタイズするネットワークに接続されているインターフェイスを EIGRP ルーティングに参加させない場合は、インターフェイスが接続されているネットワークが対象に含まれるように **network** コマンドを設定し、**passive-interface** コマンドを使用して、そのインターフェイスが EIGRP アップデートを送受信しないようにします。

手順

ステップ 1 EIGRP ルーティング プロセスを作成して、この EIGRP プロセスのルータ コンフィギュレーション モードを開始します。

router eigrp as-num

例：

```
ciscoasa(config)# router eigrp 2
```

as-num 引数には、EIGRP ルーティング プロセスの自律システム番号を指定します。

ステップ 2 EIGRP ルーティングに参加するインターフェイスとネットワークを設定します。

network ip-addr [mask]

例：

```
ciscoasa(config)# router eigrp 2
ciscoasa(config-router)# network 10.0.0.0 255.0.0.0
```

このコマンドで、1 つ以上の network 文を設定できます。

直接接続されるネットワークとスタティック ネットワークが定義済みネットワークに含まれていれば、それらが ASA によってアドバタイズされます。さらに、定義されたネットワークに含まれる IP アドレスを持つインターフェイスだけが、EIGRP ルーティング プロセスに参加します。

アドバタイズするネットワークに接続されているインターフェイスを EIGRP ルーティングに参加させない場合は、EIGRP ルーティング プロセスのネットワークの定義 （854 ページ）を参照してください。

ステップ 3 候補となるデフォルト ルート情報の送受信を制御します。

no default-information {**in** | **out** | **WORD**}

例：

```
ciscoasa(config)# router eigrp 2
ciscoasa(config-router)# network 10.0.0.0 255.0.0.0
ciscoasa(config-router)# no default-information {in | out | WORD}
```

no default-information in コマンドを入力すると、候補のデフォルト ルート ビットが受信ルート上でブロックされます。

no default-information out コマンドを入力すると、アドバタイズされるルートのデフォルト ルート ビット設定がディセーブルになります。

詳細については、EIGRP でのデフォルト情報の設定 （867 ページ）を参照してください。

ステップ 4 EIGRP パケットの MD5 認証をイネーブルにします。

authentication mode eigrp as-num **md5**

例：

```
ciscoasa(config)# authentication mode eigrp 2 md5
```

as-num 引数は、ASA に設定されている EIGRP ルーティング プロセスの自律システム番号です。EIGRP がイネーブルになっていないか、または誤った番号を入力した場合には、ASA が次のエラー メッセージを返します。

```
% Asystem(100) specified does not exist
```

詳細については、インターフェイスでの EIGRP 認証のイネーブル化 （860 ページ）を参照してください。

ステップ 5 遅延値を設定します。

delay *value*

例：

```
ciscoasa(config-if)# delay 200
```

value 引数は 10 マイクロ秒単位で入力します。2000 マイクロ秒の遅延を設定するには、*value* に 200 を入力します。

インターフェイスに割り当てられている遅延値を表示するには、**show interface** コマンドを使用します。

詳細については、インターフェイス遅延値の変更 （859 ページ）を参照してください。

ステップ 6 hello 間隔を変更します。

hello-interval eigrp as-num seconds

例：

```
ciscoasa(config)# hello-interval eigrp 2 60
```

詳細については、EIGRP Hello 間隔と保持時間のカスタマイズ （865 ページ）を参照してください。

ステップ 7 保持時間を変更します。

hold-time eigrp as-num seconds

例：

```
ciscoasa(config)# hold-time eigrp 2 60
```

詳細については、EIGRP Hello 間隔と保持時間のカスタマイズ （865 ページ）を参照してください。

パッシブ インターフェイスの設定

1 つ以上のインターフェイスを受動インターフェイスとして設定できます。EIGRP の場合、受動インターフェイスではルーティング アップデートが送受信されません。

手順

ステップ 1 EIGRP ルーティング プロセスを作成して、この EIGRP プロセスのルータ コンフィギュレーション モードを開始します。

router eigrp as-num

例：

```
ciscoasa(config)# router eigrp 2
```

as-num 引数には、EIGRP ルーティング プロセスの自律システム番号を指定します。

ステップ 2 EIGRP ルーティングに参加するインターフェイスとネットワークを設定します。このコマンドで、1 つ以上の **network** 文を設定できます。

network ip-addr [mask]

例：

```
ciscoasa(config)# router eigrp 2
```

```
ciscoasa(config-router)# network 10.0.0.0 255.0.0.0
```

直接接続されるネットワークとスタティック ネットワークが定義済みネットワークに含まれていれば、それらが ASA によってアドバタイズされます。さらに、定義されたネットワークに含まれる IP アドレスを持つインターフェイスだけが、EIGRP ルーティング プロセスに参加します。

アドバタイズするネットワークに接続されているインターフェイスを EIGRP ルーティングに参加させない場合は、EIGRP ルーティング プロセスのネットワークの定義（854 ページ）を参照してください。

ステップ 3 インターフェイスが EIGRP ルーティング メッセージを送受信しないようにします。

passive-interface {**default** | if-name}

例：

```
ciscoasa(config)# router eigrp 2
ciscoasa(config-router)# network 10.0.0.0 255.0.0.0
ciscoasa(config-router)# passive-interface {default}
```

default キーワードを使用すると、すべてのインターフェイスで EIGRP ルーティング アップデートが無効になります。**nameif** コマンドで定義したインターフェイス名を指定すると、指定したインターフェイスで EIGRP ルーティング アップデートが無効になります。EIGRP ルータ コンフィギュレーション内で、複数の **passive-interface** コマンドを使用できます。

インターフェイスでのサマリー集約アドレスの設定

サマリー アドレスはインターフェイスごとに設定できます。ネットワーク番号の境界以外でサマリー アドレスを作成する場合、または自動ルート集約がディセーブルになった ASA でサマリー アドレスを使用する場合は、手動でサマリー アドレスを定義する必要があります。ルーティング テーブルに他にも個別のルートがある場合、EIGRP は、他の個別ルートすべての中で最小のメトリックと等しいメトリックで、サマリー アドレスをインターフェイスからアドバタイズします。

手順

ステップ 1 EIGRP で使用される遅延値を変更するインターフェイスのインターフェイス コンフィギュレーション モードに入ります。

interface phy_if

例：

```
ciscoasa(config)# interface inside
```

ステップ 2 サマリー アドレスを作成します。

summary-address eigrp *as-num address mask* [*distance*]

例：

```
ciscoasa(config-if)# summary-address eigrp 2 address mask [20]
```

デフォルトでは、定義する EIGRP サマリー アドレスのアドミニストレーティブ ディスタンスは 5 になります。この値は、**summary-address** コマンドにオプションの引数 *distance* を指定して変更できます。

インターフェイス遅延値の変更

インターフェイス遅延値は、EIGRP ディスタンス計算で使用されます。この値は、インターフェイスごとに変更できます。

手順

ステップ 1 EIGRP で使用される遅延値を変更するインターフェイスのインターフェイス コンフィギュレーション モードに入ります。

interface phy_if

例：

```
ciscoasa(config)# interface inside
```

ステップ 2 遅延値を設定します。

delay *value*

例：

```
ciscoasa(config-if)# delay 200
```

value 引数は 10 マイクロ秒単位で入力します。2000 マイクロ秒の遅延を設定するには、*value* に 200 を入力します。

（注） インターフェイスに割り当てられている遅延値を表示するには、**show interface** コマンドを使用します。

インターフェイスでの EIGRP 認証のイネーブル化

EIGRP ルート認証では、EIGRP ルーティング プロトコルからのルーティング アップデートに対する MD5 認証を提供します。MD5 キーを使用したダイジェストが各 EIGRP パケットに含まれており、承認されていない送信元からの不正なルーティング メッセージや虚偽のルーティング メッセージが取り込まれないように阻止します。

EIGRP ルート認証は、インターフェイスごとに設定します。EIGRP メッセージ認証対象として設定されたインターフェイス上にあるすべての EIGRP ネイバーには、隣接関係を確立できるように同じ認証モードとキーを設定する必要があります。

（注） EIGRP ルート認証をイネーブルにするには、事前に EIGRP をイネーブルにする必要があります。

手順

ステップ 1 EIGRP ルーティング プロセスを作成して、この EIGRP プロセスのルータ コンフィギュレーション モードを開始します。

router eigrp *as-num*

例：

```
ciscoasa(config)# router eigrp 2
```

as-num 引数は、EIGRP ルーティング プロセスの自律システム番号です。

ステップ 2 EIGRP ルーティングに参加するインターフェイスとネットワークを設定します。

network *ip-addr* [*mask*]

例：

```
ciscoasa(config)# router eigrp 2
ciscoasa(config-router)# network 10.0.0.0 255.0.0.0
```

- このコマンドで、1 つ以上の network 文を設定できます。
- 直接接続されるネットワークとスタティック ネットワークが定義済みネットワークに含まれていれば、それらが ASA によってアドバタイズされます。さらに、定義されたネットワークに含まれる IP アドレスを持つインターフェイスだけが、EIGRP ルーティング プロセスに参加します。
- アドバタイズするネットワークに接続されているインターフェイスを EIGRP ルーティングに参加させない場合は、EIGRP の設定 （851 ページ）を参照してください。

ステップ 3 EIGRP メッセージ認証を設定するインターフェイスのインターフェイス コンフィギュレーション モードに入ります。

interface *phy_if*

例：

```
ciscoasa(config)# interface inside
```

ステップ 4 EIGRP パケットの MD5 認証をイネーブルにします。

authentication mode eigrp *as-num* md5

例：

```
ciscoasa(config)# authentication mode eigrp 2 md5
```

as-num 引数は、ASA に設定されている EIGRP ルーティング プロセスの自律システム番号です。EIGRP がイネーブルになっていないか、または誤った番号を入力した場合には、ASA が次のエラー メッセージを返します。

```
% Asystem(100) specified does not exist
```

ステップ 5 MD5 アルゴリズムで使用するキーを設定します。

authentication key eigrp *as-num key* key-id *key-id*

例：

```
ciscoasa(config)# authentication key eigrp 2 cisco key-id 200
```

- as-num 引数は、ASA に設定されている EIGRP ルーティング プロセスの自律システム番号です。EIGRP がイネーブルになっていないか、または誤った番号を入力した場合には、ASA が次のエラー メッセージを返します。

  ```
  % Asystem(100) specified does not exist%
  ```

- key 引数には、アルファベット、数字、特殊文字を含む最大 16 文字を含めることができます。key 引数では空白を使用できません。
- key-id 引数には、0 ～ 255 の範囲の数字を指定できます。

EIGRP ネイバーの定義

EIGRP hello パケットはマルチキャスト パケットとして送信されます。EIGRP ネイバーが、トンネルなど、非ブロードキャスト ネットワークを越えた場所にある場合、手動でネイバーを定

義する必要があります。手動で EIGRP ネイバーを定義すると、hello パケットはユニキャスト メッセージとしてそのネイバーに送信されます。

手順

ステップ 1 EIGRP ルーティング プロセスを作成して、この EIGRP プロセスのルータ コンフィギュレーション モードを開始します。

router eigrp as-num

例：

```
ciscoasa(config)# router eigrp 2
```

as-num 引数には、EIGRP ルーティング プロセスの自律システム番号を指定します。

ステップ 2 スタティック ネイバーを定義します。

neighbor *ip-addr* **interface** *if_name*

例：

```
ciscoasa(config)# router eigrp 2
ciscoasa(config-router)# neighbor 10.0.0.0 interface interface1
```

ip-addr 引数には、ネイバーの IP アドレスを指定します。

if-name 引数は、ネイバーを使用可能にしている **nameif** コマンドで指定したインターフェイスの名前です。1 つの EIGRP ルーティング プロセスに対して複数のネイバーを定義できます。

EIGRP へのルート再配布

RIP および OSPF で検出されたルートを、EIGRP ルーティング プロセスに再配布することができます。スタティック ルートおよび接続されているルートも、EIGRP ルーティング プロセスに再配布できます。接続されているルートが、EIGRP コンフィギュレーション内の **network** 文で指定された範囲に含まれている場合、再配布する必要はありません。

（注） RIP 限定：この手順を開始する前に、ルート マップを作成し、指定されたルーティング プロトコルのうち RIP ルーティング プロセスに再配布されるルートを詳細に定義する必要があります。

手順

ステップ 1 EIGRP ルーティング プロセスを作成して、この EIGRP プロセスのルータ コンフィギュレーション モードを開始します。

router eigrp as-num

例：

```
ciscoasa(config)# router eigrp 2
```

as-num 引数には、EIGRP ルーティング プロセスの自律システム番号を指定します。

ステップ 2 （オプション）EIGRP ルーティング プロセスに再配布するルートに適用するデフォルト メトリックを指定します。

default-metric bandwidth delay reliability loading mtu

例：

```
ciscoasa(config)# router eigrp 2
ciscoasa(config-router)# default-metric bandwidth delay reliability loading mtu
```

EIGRP ルータ コンフィギュレーション内にデフォルト メトリックを指定しない場合、各 **redistribute** コマンドにメトリック値を指定する必要があります。**redistribute** コマンドで EIGRP メトリックを指定し、EIGRP ルータ コンフィギュレーション内に **default-metric** コマンドが含まれている場合、**redistribute** コマンドのメトリックが使用されます。

ステップ 3 接続済みルートを EIGRP ルーティング プロセスに再配布します。

redistribute connected [**metric** bandwidth delay reliability loading mtu] [**route-map** map_name]

例：

```
ciscoasa(config-router): redistribute connected [metric bandwidth delay reliability
loading mtu] [route-map map_name]
```

EIGRP ルータ コンフィギュレーション内に **default-metric** コマンドが含まれていない場合、**redistribute** コマンドに EIGRP メトリック値を指定する必要があります。

ステップ 4 スタティック ルートを EIGRP ルーティング プロセスに再配布します。

redistribute static [**metric** bandwidth delay reliability loading mtu] [**route-map** map_name]

例：

```
ciscoasa(config-router): redistribute static [metric bandwidth delay
reliability loading mtu] [route-map map_name]
```

ステップ 5 ルートを OSPF ルーティング プロセスから EIGRP ルーティング プロセスに再配布します。

redistribute ospf pid [**match** {**internal** | **external** [**1** | **2**] | **nssa-external** [**1** | **2**]}] [**metric** bandwidth delay reliability loading mtu] [**route-map** map_name]

例：

```
ciscoasa(config-router): redistribute ospf pid [match {internal | external [1 | 2] |
nssa-external [1 | 2]}] [metric bandwidth delay reliability loading mtu] [route-map
map_name]
```

ステップ 6 ルートを RIP ルーティング プロセスから EIGRP ルーティング プロセスに再配布します。

redistribute rip [**metric** bandwidth delay reliability load mtu] [**route-map map_name**]

例：

```
ciscoasa(config-router): redistribute rip [metric bandwidth delay
reliability load mtu] [route-map map_name]
```

EIGRP でのネットワークのフィルタリング

（注） この手順を開始する前に、標準の ACL を作成し、その中にアドバタイズするルートを定義する必要があります。つまり、標準の ACL を作成し、その中に送信または受信したアップデートからフィルタリングするルートを定義します。

手順

ステップ 1 EIGRP ルーティング プロセスを作成して、この EIGRP プロセスのルータ コンフィギュレーション モードを開始します。

router eigrp as-num

例：

```
ciscoasa(config)# router eigrp 2
```

as-num 引数には、EIGRP ルーティング プロセスの自律システム番号を指定します。

ステップ 2 EIGRP ルーティングに参加するインターフェイスとネットワークを設定します。

ciscoasa(config-router)# **network** ip-addr [mask]

例：

```
ciscoasa(config)# router eigrp 2
ciscoasa(config-router)# network 10.0.0.0 255.0.0.0
```

このコマンドで、1 つ以上の network 文を設定できます。

直接接続されるネットワークとスタティック ネットワークが定義済みネットワークに含まれていれば、それらが ASA によってアドバタイズされます。さらに、定義されたネットワークに含まれる IP アドレスを持つインターフェイスだけが、EIGRP ルーティング プロセスに参加します。

アドバタイズするネットワークに接続されているインターフェイスを EIGRP ルーティングに参加させない場合は、EIGRP のインターフェイスの設定（855 ページ）を参照してください。

ステップ 3 EIGRP ルーティング アップデートで送信するネットワークをフィルタリングします。

distribute-list acl **out** [**connected** | **ospf** | **rip** | **static** | **interface** if_name]

例：

```
ciscoasa(config)# router eigrp 2
ciscoasa(config-router)# network 10.0.0.0 255.0.0.0
ciscoasa(config-router): distribute-list acl out [connected]
```

インターフェイスを指定して、そのインターフェイスが送信するアップデートだけにフィルタを適用することができます。

EIGRP ルータ コンフィギュレーション内に、複数の **distribute-list** コマンドを入力できます。

ステップ 4 EIGRP ルーティング アップデートで受信するネットワークをフィルタリングします。

distribute-list acl **in** [**interface** if_name]

例：

```
ciscoasa(config)# router eigrp 2
ciscoasa(config-router)# network 10.0.0.0 255.0.0.0
ciscoasa(config-router): distribute-list acl in [interface interface1]
```

インターフェイスを指定して、そのインターフェイスが受信するアップデートだけにフィルタを適用することができます。

EIGRP Hello 間隔と保持時間のカスタマイズ

ASA は、ネイバーを検出する目的、およびネイバーが到達不能または動作不能になったことを把握する目的で、定期的に hello パケットを送信します。デフォルトでは、hello パケットは 5 秒間隔で送信されます。

hello パケットは、ASA の保持時間をアドバタイズします。保持時間によって、EIGRP ネイバーに、ASA を到達可能と見なす時間の長さを知らせます。アドバタイズされた保持時間内にネイバーが hello パケットを受信しなかった場合、ASA は到達不能と見なされます。デフォルトでは、アドバタイズされる保持時間は 15 秒です（hello 間隔の 3 倍）。

hello間隔とアドバタイズされる保持時間のいずれも、インターフェイスごとに設定します。保持時間は hello 間隔の 3 倍以上に設定することをお勧めします。

手順

ステップ 1 hello間隔またはアドバタイズされる保持時間を設定するインターフェイスのインターフェイス コンフィギュレーション モードに入ります。

interface phy_if

例：

```
ciscoasa(config)# interface inside
```

ステップ 2 hello 間隔を変更します。

hello-interval eigrp as-num seconds

例：

```
ciscoasa(config)# hello-interval eigrp 2 60
```

ステップ 3 保持時間を変更します。

hold-time eigrp as-num seconds

例：

```
ciscoasa(config)# hold-time eigrp 2 60
```

自動ルート集約の無効化

自動ルート集約は、デフォルトでイネーブルになっています。EIGRP ルーティング プロセスは、ネットワーク番号の境界で集約を行います。このことは、不連続ネットワークがある場合にルーティングの問題の原因となることがあります。

たとえば、ネットワーク 192.168.1.0、192.168.2.0、192.168.3.0 が接続されているルータがあり、それらのネットワークがすべて EIGRP に参加しているとすると、EIGRP ルーティング プロセスはそれらのルートに対しサマリー アドレス 192.168.0.0 を作成します。さらにネットワーク 192.168.10.0 と 192.168.11.0 が接続されているルータがこのネットワークに追加され、それらのネットワークが EIGRP に参加すると、これらもまた 192.168.0.0 として集約されます。トラフィックが誤った場所にルーティングされる可能性をなくすために、競合するサマリーアドレスを作成するルータでの自動ルート集約をディセーブルにする必要があります。

手順

ステップ 1 EIGRP ルーティング プロセスを作成して、この EIGRP プロセスのルータ コンフィギュレーション モードを開始します。

router eigrp as-num

例：

```
ciscoasa(config)# router eigrp 2
```

as-num 引数には、EIGRP ルーティング プロセスの自律システム番号を指定します。

ステップ 2 自動ルート集約をディセーブルにします。

no auto-summary

例：

```
ciscoasa(config-router)# no auto-summary
```

自動サマリー アドレスのアドミニストレーティブ ディスタンスは 5 です。

EIGRP でのデフォルト情報の設定

EIGRP アップデート内のデフォルト ルート情報の送受信を制御できます。デフォルトでは、デフォルト ルートが送信され、受け入れられます。デフォルト情報の受信を禁止するように ASA を設定すると、候補のデフォルト ルート ビットが受信ルート上でブロックされます。デフォルト情報の送信を禁止するように ASA を設定すると、アドバタイズされるルートのデフォルト ルート ビット設定が無効になります。

手順

ステップ 1 EIGRP ルーティング プロセスを作成して、この EIGRP プロセスのルータ コンフィギュレーション モードを開始します。

router eigrp as-num

例：

```
ciscoasa(config)# router eigrp 2
```

as-num 引数には、EIGRP ルーティング プロセスの自律システム番号を指定します。

ステップ 2 EIGRP ルーティングに参加するインターフェイスとネットワークを設定します。

network ip-addr [mask]

例：

```
ciscoasa(config)# router eigrp 2
ciscoasa(config-router)# network 10.0.0.0 255.0.0.0
```

このコマンドで、1 つ以上の network 文を設定できます。

直接接続されるネットワークとスタティック ネットワークが定義済みネットワークに含まれていれば、それらが ASA によってアドバタイズされます。さらに、定義されたネットワークに含まれる IP アドレスを持つインターフェイスだけが、EIGRP ルーティング プロセスに参加します。

アドバタイズするネットワークに接続されているインターフェイスを EIGRP ルーティングに参加させない場合は、EIGRP のインターフェイスの設定（855 ページ）を参照してください。

ステップ 3 候補となるデフォルト ルート情報の送受信を制御します。

no default-information {**in** | **out** | **WORD**}

例：

```
ciscoasa(config)# router eigrp 2
ciscoasa(config-router)# network 10.0.0.0 255.0.0.0
ciscoasa(config-router)# no default-information {in | out | WORD}
```

（注） **no default-information in** コマンドを入力すると、候補のデフォルト ルート ビットが受信ルート上でブロックされます。**no default-information out** コマンドを入力すると、アドバタイズされるルートのデフォルト ルート ビット設定がディセーブルになります。

EIGRP スプリット ホライズンのディセーブル化

スプリット ホライズンは、EIGRP アップデート パケットとクエリー パケットの送信を制御します。スプリット ホライズンがインターフェイスでイネーブルになると、アップデート パケットとクエリー パケットは、このインターフェイスがネクスト ホップとなる宛先には送信されません。この方法でアップデート パケットとクエリー パケットを制御すると、ルーティング ループが発生する可能性が低くなります。

デフォルトでは、スプリット ホライズンはすべてのインターフェイスでイネーブルになっています。

スプリット ホライズンは、ルート情報が、その情報の発信元となるインターフェイスからルータによってアドバタイズされないようにします。通常、特にリンクが切断された場合には、この動作によって複数のルーティング デバイス間の通信が最適化されます。ただし、非ブロードキャスト ネットワークでは、この動作が望ましくない場合があります。このような場合は、EIGRP を設定したネットワークを含め、スプリット ホライズンをディセーブルにする必要が生じることもあります。

インターフェイスでのスプリットホライズンをディセーブルにする場合、そのインターフェイス上のすべてのルータとアクセス サーバに対してディセーブルにする必要があります。

EIGRP スプリット ホライズンをディセーブルにするには、次の手順を実行します。

手順

ステップ 1 EIGRP で使用される遅延値を変更するインターフェイスのインターフェイス コンフィギュレーション モードに入ります。

interface phy_if

例：

```
ciscoasa(config)# interface phy_if
```

ステップ 2 スプリット ホライズンをディセーブルにします。

no split-horizon eigrp *as-number*

例：

```
ciscoasa(config-if)# no split-horizon eigrp 2
```

EIGRP プロセスの再始動

EIGRP プロセスを再始動したり、再配布またはカウンタをクリアしたりすることができます。

手順

EIGRP プロセスを再始動するか、再配布またはカウンタをクリアします。

clear eigrp pid {**1-65535** | **neighbors** | **topology** | **events)**}

例：

```
ciscoasa(config)# clear eigrp pid 10 neighbors
```

EIGRP のモニタリング

次のコマンドを使用して、EIGRP ルーティング プロセスをモニタできます。コマンド出力の例と説明については、コマンド リファレンスを参照してください。また、ネイバー変更メッセージとネイバー警告メッセージのロギングをディセーブルにできます。

さまざまな EIGRP ルーティング統計情報をモニタまたはディセーブル化するには、次のいずれかのコマンドを入力します。

- **router-id**

  EIGRP プロセスの router-id を表示します。

- **show eigrp** [*as-number*] **events** [{*start end*} | **type**]

  EIGRP イベント ログを表示します。

- **show eigrp** [*as-number*] **interfaces** [*if-name*] [**detail**]

  EIGRP ルーティングに参加するインターフェイスを表示します。

- **show eigrp** [as-number] **neighbors** [**detail** | **static**] [*if-name*]

  EIGRP ネイバー テーブルを表示します。

- **show eigrp** [*as-number*] **topology** [*ip-addr* [**mask**] | **active** | **all-links** | **pending** | **summary** | **zero-successors**]

  EIGRP トポロジ テーブルを表示します。

- **show eigrp** [*as-number*] **traffic**

  EIGRP トラフィックの統計情報を表示します。

- **show mfib cluster**

  転送する側のエントリおよびインターフェイスに関する MFIB 情報を表示します。

- **show route cluster**

  クラスタリングに関する追加ルートの同期の詳細を表示します。

- **no eigrp log-neighbor-changes**

  ネイバー変更メッセージのロギングをディセーブルにします。EIGRP ルーティング プロセスのルータ コンフィギュレーション モードでこのコマンドを入力します。

- **no eigrp log-neighbor-warnings**

  ネイバー警告メッセージのロギングをディセーブルにします。

EIGRP の例

次の例に、さまざまなオプションのプロセスを使用して EIGRP をイネーブルにし、設定する方法を示します。

手順

ステップ 1 EIGRP をイネーブルにするには、次のコマンドを入力します。

```
ciscoasa(config)# router eigrp 2
ciscoasa(config-router)# network 10.0.0.0 255.0.0.0
```

ステップ 2 EIGRP ルーティング メッセージの送信または受信からインターフェイスを設定するには、次のコマンドを入力します。

```
ciscoasa(config-router)# passive-interface {default}
```

ステップ 3 EIGRP ネイバーを定義するには、次のコマンドを入力します。

```
ciscoasa(config-router)# neighbor 10.0.0.0 interface interface1
```

ステップ 4 EIGRP ルーティングに参加するインターフェイスとネットワークを設定するには、次のコマンドを入力します。

```
ciscoasa(config-router)# network 10.0.0.0 255.0.0.0
```

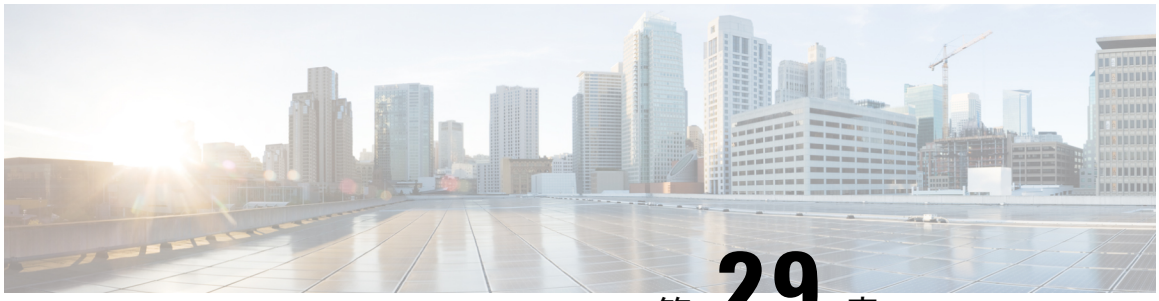
ステップ 5 EIGRP ディスタンス計算で使用されるインターフェイス遅延値を変更するには、次のコマンドを入力します。

```
ciscoasa(config-router)# exit
ciscoasa(config)# interface phy_if
ciscoasa(config-if)# delay 200
```

EIGRP の履歴

表 *29 : EIGRP* の機能の履歴

機能名	プラットフォーム リリース	機能情報
EIGRP サポート	7.0(1)	Enhanced Interior Gateway Routing Protocol（EIGRP）を使用するデータのルーティング、認証の実行、およびルーティング情報の再配布とモニタリングのサポートが追加されました。 **route eigrp** コマンドが導入されました。
マルチ コンテキスト モードのダイナミック ルーティング	9.0(1)	EIGRP ルーティングは、マルチ コンテキスト モードでサポートされます。
クラスタ	9.0(1)	EIGRP の場合、バルク同期、ルートの同期およびレイヤ 2 ロードバランシングは、クラスタリング環境でサポートされます。 **show route cluster**、**debug route cluster**、**show mfib cluster**、**debug mfib cluster** の各コマンドが導入または変更されました。
EIGRP Auto-Summary	9.2(1)	EIGRP の [Auto-Summary] フィールドはデフォルトでディセーブルになりました。



第 29 章

マルチキャスト ルーティング

この章では、マルチキャスト ルーティング プロトコルを使用するように Cisco ASA を設定する方法について説明します。

マルチキャスト ルーティングの概要

マルチキャストルーティングは、単一の情報ストリームを数千もの企業や家庭に同時に配信することでトラフィックを軽減する帯域幅節約型のテクノロジーです。マルチキャストルーティングを活用するアプリケーションには、ビデオ会議、企業通信、遠隔学習に加えて、ソフトウェア、株価、およびニュースの配信などがあります。

マルチキャスト ルーティング プロトコルでは、競合テクノロジーのネットワーク帯域幅の使用量を最小限に抑えながら、発信元や受信者の負荷を増加させずに発信元のトラフィックを複数の受信者に配信します。マルチキャスト パケットは、Protocol Independent Multicast（PIM）やサポートする他のマルチキャストプロトコルを使用したASAによりネットワークで複製されるため、複数の受信者にできる限り高い効率でデータを配信できます。

ASAは、スタブ マルチキャスト ルーティングと PIM マルチキャスト ルーティングの両方をサポートしています。ただし、1 つのASAに両方を同時に設定できません。

（注） UDP と非 UDP の両方のトランスポートがマルチキャスト ルーティングに対してサポートされます。ただし、非 UDP トランスポートでは FastPath 最適化は行われません。

スタブ マルチキャスト ルーティング

スタブ マルチキャスト ルーティングは、ダイナミック ホスト登録の機能を提供して、マルチキャスト ルーティングを容易にします。スタブ マルチキャスト ルーティングを設定すると、ASAは IGMP のプロキシ エージェントとして動作します。ASAは、マルチキャスト ルーティングに全面的に参加するのではなく、IGMP メッセージをアップストリームのマルチキャスト ルータに転送し、そのルータがマルチキャスト データの送信をセットアップします。スタブ マルチキャスト ルーティングを設定する場合は、ASA を PIM スパース モードまたは双方向モードに設定できません。IGMP スタブ マルチキャスト ルーティングに参加しているインターフェイス上で PIM を有効にする必要があります。

ASA は、PIM-SM および双方向 PIM の両方をサポートしています。PIM-SM は、基盤となるユニキャスト ルーティング情報ベースまたは別のマルチキャスト対応ルーティング情報ベースを使用するマルチキャスト ルーティング プロトコルです。このプロトコルは、マルチキャスト グループあたり 1 つのランデブー ポイント（RP）をルートにした単方向の共有ツリーを構築し、オプションでマルチキャストの発信元ごとに最短パス ツリーを作成します。

PIM マルチキャスト ルーティング

双方向 PIM は PIM-SM の変形で、マルチキャストの発信元と受信者を接続する双方向の共有ツリーを構築します。双方向ツリーは、マルチキャスト トポロジの各リンクで動作する指定フォワーダ（DF）選択プロセスを使用して構築されます。DF に支援されたマルチキャスト データは発信元からランデブー ポイント（RP）に転送されます。この結果、マルチキャスト データは発信元固有の状態を必要とせず、共有ツリーをたどって受信者に送信されます。DF の選択は RP の検出中に行われ、これによってデフォルト ルートが RP に提供されます。

（注） ASAが PIM RP の場合は、ASAの変換されていない外部アドレスを RP アドレスとして使用してください。

マルチキャスト グループの概念

マルチキャストはグループの概念に基づくものです。受信者の任意のグループは、特定のデータ ストリームを受信することに関心があります。このグループには物理的または地理的な境界がなく、インターネット上のどの場所にホストを置くこともできます。特定のグループに流れるデータの受信に関心があるホストは、IGMP を使用してグループに加入する必要があります。ホストがデータ ストリームを受信するには、グループのメンバでなければなりません。

マルチキャスト アドレス

マルチキャスト アドレスは、グループに加入し、このグループに送信されるトラフィックの受信を希望する IP ホストの任意のグループを指定します。

クラスタ

マルチキャスト ルーティングは、クラスタリングをサポートします。スパンド EtherChannel クラスタリングでは、ファースト パス転送が確立されるまでの間、プライマリ ユニットがすべてのマルチキャスト ルーティング パケットとデータ パケットを送信します。ファースト パス転送が確立されると、従属ユニットがマルチキャスト データ パケットを転送できます。すべてのデータ フローは、フル フローです。スタブ転送フローもサポートされます。スパンド EtherChannel クラスタリングでは 1 つのユニットだけがマルチキャスト パケットを受信するため、プライマリ ユニットへのリダイレクションは共通です。 個別インターフェイス クラスタリングでは、ユニットは個別に機能しません。すべてのデータとルーティング パケットはプライマリ ユニットで処理され、転送されます。従属ユニットは、送信されたすべてのパケットをドロップします。

クラスタリングの詳細については、ASA クラスタ （319 ページ）を参照してください。

マルチキャスト ルーティングのガイドライン

コンテキスト モード

シングル コンテキスト モードでサポートされています。

ファイアウォール モード

ルーテッド ファイアウォール モードでだけサポートされています。トランスペアレント ファイアウォール モードはサポートされません。

IPv6

IPv6 はサポートされません。

クラスタ

IGMP および PIM のクラスタリングでは、この機能はプライマリ ユニットでのみサポートされます。

その他のガイドライン

224.1.2.3 などのマルチキャスト ホストへのトラフィックを許可するには、インバウンド インターフェイス上のアクセス制御ルールを設定する必要があります。ただし、ルールの宛先インターフェイスを指定したり、初期接続確認の間にマルチキャストの接続に適用したりすることはできません。

マルチキャスト ルーティングの有効化

ASA でマルチキャスト ルーティングを有効にすると、デフォルトではすべてのデータ インターフェイスで IGMP と PIM が有効になりますが、5506-X ～ 5555-X モデルの管理インターフェイスでは有効になりません。IGMP は、直接接続されているサブネット上にグループのメンバが存在するかどうか学習するために使用されます。ホストは、IGMP 報告メッセージを送信することにより、マルチキャスト グループに参加します。PIM は、マルチキャスト データグラムを転送するための転送テーブルを維持するために使用されます。

5506-X ～ 5555-X モデルの管理インターフェイスでマルチキャスト ルーティングを有効にするには、管理インターフェイスでマルチキャスト境界を明示的に設定する必要があります。

（注） マルチキャスト ルーティングでは、UDP トランスポート レイヤだけがサポートされています。

以下の表に、ASA の RAM の量に基づいた特定のマルチキャスト テーブルのエントリの最大数を示します。この上限に達すると、新しいエントリは廃棄されます。

表 *30*：マルチキャスト テーブルのエントリの上限（スタティック/ダイナミック エントリの合計の上限）

Table	16 MB	128 MB	128 + MB
MFIB	1000	3000	30000
IGMP グループ	1000	3000	30000
PIM ルート	3000	7000	72000

手順

マルチキャスト ルーティングをイネーブルにします。

multicast-routing

例：

```
ciscoasa(config)# multicast-routing
```

マルチキャスト ルーティング テーブルのエントリの数は、ASA に搭載されている RAM の量によって制限されます。

マルチキャスト ルーティングのカスタマイズ

ここでは、マルチキャスト ルーティングをカスタマイズする方法について説明します。

スタブ マルチキャスト ルーティングの設定と IGMP メッセージの転送

（注） スタブ マルチキャスト ルーティングは、PIM スパース モードおよび双方向モードと同時にはサポートされません。

スタブ エリアへのゲートウェイとして動作している ASA は、PIM スパース モードまたは双方向モードに参加する必要はありません。その代わりに、そのセキュリティ アプライアンスを IGMP プロキシ エージェントとして設定すると、あるインターフェイスに接続されているホストから、別のインターフェイスのアップストリーム マルチキャスト ルータに IGMP メッセージを転送することができます。ASA を IGMP プロキシ エージェントとして設定するには、ホスト加入（join）メッセージおよびホスト脱退（leave）メッセージをスタブ エリアからアップストリーム インターフェイスに転送します。スタブ モードのマルチキャスト ルーティングに参加しているインターフェイスでも、PIM を有効にする必要があります。

手順

スタブ マルチキャスト ルーティングを設定し、IGMP メッセージを転送します。

igmp forward interface if_name

例：

```
ciscoasa(config-if)# igmp forward interface interface1
```

スタティック マルチキャスト ルートの設定

スタティック マルチキャスト ルートを設定すると、マルチキャスト トラフィックをユニキャスト トラフィックから分離できます。たとえば、送信元と宛先の間のパスでマルチキャスト ルーティングがサポートされていない場合は、その解決策として、2つのマルチキャスト デバイスの間に GRE トンネルを設定し、マルチキャスト パケットをそのトンネル経由で送信します。

PIM を使用する場合、ASA は、ユニキャスト パケットを発信元に返送するときと同じインターフェイスでパケットを受信することを想定しています。マルチキャスト ルーティングをサポートしていないルートをバイパスする場合などは、ユニキャスト パケットで 1 つのパスを使用し、マルチキャスト パケットで別の 1 つのパスを使用することもあります。

スタティック マルチキャスト ルートはアドバタイズも再配布もされません。

手順

ステップ 1 スタティック マルチキャスト ルートを設定します。

mroute src_ip src_mask {input_if_name | *rpf_neighbor*} [distance]

例：

```
ciscoasa(config)# mroute src_ip src_mask {input_if_name | rpf_neighbor} [distance]
```

ステップ 2 スタブ エリアのスタティック マルチキャスト ルートを設定します。

mroute src_ip src_mask input_if_name [**dense** output_if_name] [distance]

例：

```
ciscoasa(config)# mroute src_ip src_mask input_if_name [dense output_if_name] [distance]
```

dense*output_if_name* キーワードと引数のペアは、スタブ マルチキャスト ルーティングでのみサポートされています。

IGMP 機能の設定

IP ホストは、自身のグループ メンバーシップを直接接続されているマルチキャスト ルータに報告するために IGMP を使用します。IGMP は、マルチキャスト グループの個々のホストを特定の LAN にダイナミックに登録するために使用します。ホストは、そのローカル マルチキャスト ルータに IGMP メッセージを送信することで、グループ メンバーシップを識別します。IGMP では、ルータは IGMP メッセージを受信し、定期的にクエリーを送信して、特定のサブネットでアクティブなグループと非アクティブなグループを検出します。

ここでは、インターフェイス単位で任意の IGMP 設定を行う方法について説明します。

インターフェイスでの IGMP の有効化

IGMP は、特定のインターフェイスでディセーブルにできます。この情報は、特定のインターフェイスにマルチキャスト ホストがないことがわかっていて、ASA からそのインターフェイスにホスト クエリー メッセージを発信しないようにする場合に有用です。

手順

インターフェイスで IGMP をディセーブルにします。

no igmp

例：

```
ciscoasa(config-if)# no igmp
```

インターフェイスで IGMP を再度イネーブルにするには、**igmp** コマンドを使用します。

（注） インターフェイス コンフィギュレーションには、**no igmp** コマンドだけが表示されます。

IGMP グループ メンバーシップの設定

ASA をマルチキャスト グループのメンバとして設定できます。マルチキャスト グループに加入するように ASA を設定すると、アップストリーム ルータはそのグループのマルチキャスト ルーティング テーブル情報を維持して、このグループをアクティブにするパスを保持します。

（注） 特定のグループのマルチキャスト パケットを特定のインターフェイスに転送する必要がある場合に、ASA がそのパケットをそのグループの一部として受け付けることがないようにする方法については、スタティック加入した IGMP グループの設定（879 ページ）を参照してください。

手順

ASA をマルチキャスト グループのメンバとして設定します。

igmp join-group group-address

例：

```
ciscoasa(config-if)# igmp join-group mcast-group
```

group-address 引数はグループの IP アドレスです。

スタティック加入した IGMP グループの設定

設定によってはグループ メンバがグループ内で自分のメンバーシップを報告できない場合があります。また、ネットワーク セグメント上にグループのメンバが存在しないこともあります。しかし、それでも、そのグループのマルチキャスト トラフィックをそのネットワーク セグメントに送信することが必要になる場合があります。そのようなグループのマルチキャスト トラフィックをそのセグメントに送信するには、スタティック加入した IGMP グループを設定します。

igmp static-group コマンドを入力します。ASA は、マルチキャスト パケットを受け入れる代わりに、指定されたインターフェイスに転送します。

手順

インターフェイスのマルチキャスト グループにスタティック加入するように、ASA を設定します。

igmp static-group

例：

```
ciscoasa(config-if)# igmp static-group group-address
```

group-address 引数はグループの IP アドレスです。

マルチキャスト グループへのアクセスの制御

アクセス コントロール リストを使用して、マルチキャスト グループへのアクセスを制御できます。

手順

ステップ 1 マルチキャスト トラフィックの標準 ACL を作成します。

access-list name **standard** [**permit | deny]** ip_addr mask

例：

```
ciscoasa(config)# access-list acl1 standard permit 192.52.662.25
```

1 つの ACL に複数のエントリを作成することができます。標準 ACL または拡張 ACL を使用できます。

ip_addr mask 引数は、許可または拒否されるマルチキャスト グループの IP アドレスです。

ステップ 2 拡張 ACL を作成します。

access-list name **extended** [**permit | deny]** protocol src_ip_addr src_mask dst_ip_addr dst_mask

例：

```
ciscoasa(config)# access-list acl2 extended permit protocol
src_ip_addr src_mask dst_ip_addr dst_mask
```

dst_ip_addr 引数は、許可または拒否されるマルチキャスト グループの IP アドレスです。

ステップ 3 ACL をインターフェイスに適用します。

igmp access-group acl

例：

```
ciscoasa(config-if)# igmp access-group acl
```

acl 引数は、標準 IP ACL または拡張 IP ACL の名前です。

インターフェイスにおける IGMP 状態の数の制限

IGMP メンバーシップ報告の結果の IGMP 状態の数は、インターフェイスごとに制限することができます。設定された上限を超過したメンバーシップ報告は IGMP キャッシュに入力されず、超過した分のメンバーシップ報告のトラフィックは転送されません。

手順

インターフェイスにおける IGMP 状態の数を制限します。

igmp limit number

例：

```
ciscoasa(config-if)# igmp limit 50
```

有効値の範囲は 0 ～ 500 で、デフォルト値は 500 です。

この値を 0 に設定すると、学習したグループが追加されなくなりますが、（**igmp join-group** コマンドおよび **igmp static-group** コマンドを使用して）手動で定義したメンバーシップは引き続き許可されます。このコマンドの **no** 形式を使用すると、デフォルト値に戻ります。

マルチキャスト グループに対するクエリー メッセージの変更

ASA は、クエリー メッセージを送信して、インターフェイスに接続されているネットワークにメンバを持つマルチキャスト グループを検出します。メンバは、IGMP 報告メッセージで応答して、特定のグループに対するマルチキャスト パケットの受信を希望していることを示します。クエリー メッセージは、アドレスが 224.0.0.1 で存続可能時間値が 1 の全システム マルチキャスト グループ宛に送信されます。

これらのメッセージが定期的に送信されることにより、ASA に保存されているメンバーシップ情報はリフレッシュされます。ASA で、ローカル メンバがいなくなったマルチキャスト グループがまだインターフェイスに接続されていることがわかると、そのグループへのマルチキャスト パケットを接続されているネットワークに転送するのを停止し、そのパケットの送信元にプルーニング メッセージを戻します。

デフォルトでは、サブネット上の PIM 指定ルータがクエリー メッセージの送信を担当します。このメッセージは、デフォルトでは 125 秒間に 1 回送信されます。

クエリー応答時間を変更する場合は、IGMP クエリーでアドバタイズする最大クエリー応答時間はデフォルトで 10 秒になります。ASA がこの時間内にホスト クエリーの応答を受信しなかった場合、グループを削除します。

（注） **igmp query-timeout** および **igmp query-interval** コマンドを実行するには、IGMP バージョン 2 が必要です。

クエリー間隔、クエリー応答時間、クエリータイムアウト値を変更するには、次の手順を実行します。

手順

ステップ 1 クエリー間隔を秒単位で設定します。

igmp query-interval *seconds*

例：

```
ciscoasa(config-if)# igmp query-interval 30
```

有効値の範囲は 1～3600 で、デフォルト値は 125 です。

指定されたタイムアウト値（デフォルトは255秒）の間にインターフェイス上でクエリー メッセージが ASA によって検出されないと、ASA が指定ルータになり、クエリー メッセージの送信を開始します。

ステップ 2 クエリーのタイムアウト値を変更します。

igmp query-timeout *seconds*

例：

```
ciscoasa(config-if)# igmp query-timeout 30
```

有効値の範囲は 60～300 で、デフォルト値は 225 です。

ステップ 3 最大クエリー応答時間を変更します。

igmp query-max-response-time *seconds*

有効値の範囲は 1～25 で、デフォルト値は 10 です。

例：

```
ciscoasa(config-if)# igmp query-max-response-time 20
```

IGMP バージョンの変更

デフォルトでは、ASA は IGMP バージョン 2 を実行します。このバージョンでは **igmp query-timeout** コマンドや **igmp query-interval** コマンド などの、いくつかの追加機能を使用できます。

サブネットのマルチキャストルータはすべて、同じIGMPバージョンをサポートしている必要があります。ASA は、バージョン 1 ルータを自動的に検出してバージョン 1 に切り替えることはありません。しかし、サブネットに IGMP のバージョン 1 のホストとバージョン 2 のホストが混在しても問題はありません。IGMP バージョン 2 を実行している ASA は、IGMP バージョン 1 のホストが存在しても正常に動作します。

手順

インターフェイスで実行する IGMP のバージョンを制御します。

igmp version {**1** | **2**}

例：

```
ciscoasa(config-if)# igmp version 2
```

PIM 機能の設定

ルータは PIM を使用して、マルチキャスト ダイアグラムを転送するために使われる転送テーブルを維持します。ASAでマルチキャスト ルーティングをイネーブルにすると、PIM および IGMP がすべてのインターフェイスで自動的にイネーブルになります。

（注） PIM は、PAT ではサポートされません。PIM プロトコルはポートを使用せず、PAT はポートを使用するプロトコルに対してのみ動作します。

ここでは、任意の PIM 設定を行う方法について説明します。

インターフェイスでの PIM の有効化またはディセーブル化

PIM は、特定のインターフェイスでイネーブルまたはディセーブルにできます。

手順

ステップ 1 特定のインターフェイスで PIM をイネーブルにする、または再度イネーブルにします。

pim

例：

```
ciscoasa(config-if)# pim
```

ステップ 2 特定のインターフェイスで PIM をディセーブルにします。

no pim

例：

```
ciscoasa(config-if)# no pim
```

（注） インターフェイス コンフィギュレーションには、**no pim** コマンドだけが表示されます。

スタティック ランデブー ポイント アドレスの設定

共通の PIM スパース モードまたは双方向ドメイン内のルータはすべて、PIM RP アドレスを認識している必要があります。このアドレスは、**pim rp-address** コマンドを使用してスタティックに設定されます。

（注） ASA は、Auto-RP または PIM BSR をサポートしていません。RP アドレスを指定するには、**pim rp-address** コマンドを使用する必要があります。

複数のグループの RP として機能するように ASA を設定することができます。ACL に指定されているグループ範囲によって、PIM RP のグループ マッピングが決まります。ACL が指定されていない場合は、マルチキャスト グループ全体の範囲（224.0.0.0/4）にグループの RP が適用されます。

手順

特定のインターフェイスで PIM をイネーブルにする、または再度イネーブルにします。

pim rp-address ip_address [acl] [**bidir**]

ip_address 引数は、PIM RP となるように割り当てられたルータのユニキャスト IP アドレスです。

acl 引数は、RP とともに使用する必要があるマルチキャスト グループを定義している標準 ACL の名前または番号です。このコマンドではホスト ACL を使用しないでください。

bidir キーワードを除外すると、グループは PIM スパース モードで動作するようになります。

（注） ASA は、実際の双方向構成にかかわらず、PIM の hello メッセージを使用して双方向の機能を常時アドバタイズします。

例：

```
ciscoasa(config)# pim rp-address 10.86.75.23 [acl1] [bidir]
```

指定ルータのプライオリティの設定

DR は、PIM 登録メッセージ、PIM 加入メッセージ、およびプルーニング メッセージの RP への送信を担当します。1 つのネットワーク セグメントに複数のマルチキャスト ルータがある場合は、DR プライオリティに基づいて DR が選択されます。複数のデバイスの DR プライオリティが等しい場合、最上位の IP アドレスを持つデバイスが DR になります。

デフォルトでは、ASA の DR プライオリティは 1 です。この値を変更できます。

手順

指定ルータのプライオリティを変更します。

pim dr-priority num

例：

```
ciscoasa(config-if)# pim dr-priority 500
```

num 引数は、1 ～ 4294967294 の任意の数字にできます。

PIM 登録メッセージの設定とフィルタリング

ASA が RP として動作しているときは、特定のマルチキャスト送信元を登録できないように制限することができます。このようにすると、未許可の送信元が RP に登録されるのを回避できます。[Request Filter] ペインでは、ASA で PIM 登録メッセージが受け入れられるマルチキャスト ソースを定義できます。

手順

PIM 登録メッセージをフィルタリングするように ASA を設定します。

pim accept-register {**list** acl | **route-map** map-name}

例：

```
ciscoasa(config)# pim accept-register {list acl1 | route-map map2}
```

この例では、ASA によって PIM 登録メッセージ *acl1* とルート マップ *map2* がフィルタリングされます。

PIM メッセージ間隔の設定

ルータ クエリー メッセージは、PIM DR の選択に使用されます。PIM DR は、ルータ クエリー メッセージを送信します。デフォルトでは、ルータ クエリー メッセージは 30 秒間隔で送信されます。さらに、60 秒ごとに、ASA は PIM 加入メッセージおよびプルーニング メッセージを送信します。

手順

ステップ 1 ルータ クエリー メッセージを送信します。

pim hello-interval seconds

例：

```
ciscoasa(config-if)# pim hello-interval 60
```

seconds 引数の有効な値は 1 ～ 3600 秒です。

ステップ 2 ASA が PIM 加入メッセージまたはプルーニング メッセージを送信する時間（秒）を変更します。

pim join-prune-interval seconds

例：

```
ciscoasa(config-if)# pim join-prune-interval 60
```

seconds 引数の有効な値は 10 ～ 600 秒です。

PIM ネイバーのフィルタリング

PIM ネイバーにできるルータの定義が可能です。PIM ネイバーにできるルータをフィルタリングすると、次の制御を行うことができます。

- 許可されていないルータが PIM ネイバーにならないようにする。
- 添付されたスタブ ルータが PIM に参加できないようにする。

手順

ステップ 1 標準 ACL を使用して、PIM に参加させるルータを定義します。

access-list pim_nbr deny *router-IP_addr PIM neighbor*

例：

```
ciscoasa(config)# access-list pim_nbr deny 10.1.1.1 255.255.255.255
```

この例では、次の ACL を **pim neighbor-filter** コマンドで使用すると、10.1.1.1 ルータを PIM ネイバーとして設定できなくなります。

ステップ 2 隣接ルータをフィルタリングします。

pim neighbor-filter pim_nbr

例：

```
ciscoasa(config)# interface GigabitEthernet0/3
ciscoasa(config-if)# pim neighbor-filter pim_nbr
```

この例では、インターフェイス GigabitEthernet0/3 で 10.1.1.1 ルータを PIM ネイバーとして設定できなくなります。

双方向ネイバー フィルタの設定

ASA に PIM 双方向ネイバー フィルタが設定されている場合、[Bidirectional Neighbor Filter] ペインにそれらのフィルタが表示されます。PIM 双方向ネイバー フィルタは、DF 選定に参加できるネイバー デバイスを定義する ACL です。PIM 双方向ネイバー フィルタがインターフェイスに設定されていなければ、制限はありません。PIM 双方向ネイバー フィルタが設定されている場合は、ACL で許可されるネイバーだけが DF 選択プロセスに参加できます。

PIM 双方向ネイバー フィルタ設定が ASA に適用されると、実行コンフィギュレーションに *interface-name*_multicast という名前の ACL が表示されます。ここで、*interface-name* はマルチキャスト境界フィルタが適用されるインターフェイスの名前です。そのような名前の ACL がすでに存在していた場合は、名前に番号が追加されます（inside_multicast_1 など）。この ACL により、どのデバイスが ASA の PIM ネイバーになれるか定義されます。

双方向 PIM では、マルチキャスト ルータで保持するステート情報を減らすことができます。双方向で DF を選定するために、セグメント内のすべてのマルチキャスト ルータが双方向でイネーブルになっている必要があります。

PIM 双方向ネイバー フィルタを利用すると、スパース モード専用ネットワークから双方向ネットワークへの移行が可能になります。このフィルタで、DF 選定に参加するルータを指定する一方で、引き続きすべてのルータにスパース モード ドメインへの参加を許可できるからです。双方向にイネーブルにされたルータは、セグメントに非双方向ルータがある場合でも、それらのルータの中から DF を選定できます。非双方向ルータ上のマルチキャスト境界により、双方

向グループから PIM メッセージやデータが双方向サブセット クラウドに出入りできないようにします。

PIM 双方向ネイバー フィルタがイネーブルの場合、その ACL によって許可されるルータは、双方向に対応していると見なされます。したがって、次のことが当てはまります。

- 許可されたネイバーが双方向対応でない場合、DF 選択は実施されません。
- 拒否されたネイバーが双方向対応である場合、DF 選択は実施されません。
- 拒否されたネイバーが双方向をサポートしない場合、DF 選定が実行される可能性があります。

手順

ステップ 1 標準 ACL を使用して、PIM に参加させるルータを定義します。

access-list pim_nbr deny *router-IP_addr PIM neighbor*

例：

```
ciscoasa(config)# access-list pim_nbr deny 10.1.1.1 255.255.255.255
```

この例では、次の ACL を **pim neighbor-filter** コマンドで使用すると、10.1.1.1 ルータを PIM ネイバーとして設定できなくなります。

ステップ 2 隣接ルータをフィルタリングします。

pim bidirectional-neighbor-filter pim_nbr

例：

```
ciscoasa(config)# interface GigabitEthernet0/3
ciscoasa(config-if)# pim bidirectional neighbor-filter pim_nbr
```

この例では、10.1.1.1 ルータが、インターフェイス GigabitEthernet0/3 上で PIM 双方向ネイバーとして設定できなくなります。

マルチキャスト境界の設定

アドレス スコーピングは、同じ IP アドレスを持つ RP が含まれるドメインが相互にデータを漏出させることのないように、ドメイン境界を定義します。スコーピングは、大きなドメイン内のサブネット境界や、ドメインとインターネットの間の境界で実行されます。

インターフェイスでマルチキャスト グループ アドレスの管理スコープ境界を設定できます。IANA では、239.0.0.0 ～ 239.255.255.255 のマルチキャスト アドレス範囲が管理スコープ アドレスとして指定されています。この範囲のアドレスは、さまざまな組織で管理されるドメイン

内で再使用されます。このアドレスはグローバルではなく、ローカルで一意であると見なされます。

影響を受けるアドレスの範囲は、標準 ACL で定義します。境界が設定されると、マルチキャスト データ パケットは境界を越えて出入りできなくなります。境界を定めることで、同じマルチキャスト グループ アドレスをさまざまな管理ドメイン内で使用できます。

filter-autorp キーワードを入力することにより、管理スコープ境界で Auto-RP 検出メッセージと通知メッセージを設定、検証、フィルタリングできます。境界の ACL で拒否された Auto-RP パケットからの Auto-RP グループ範囲通知は削除されます。Auto-RP グループ範囲通知は、Auto-RP グループ範囲のすべてのアドレスが境界 ACL によって許可される場合に限り境界を通過できます。許可されないアドレスがある場合は、グループ範囲全体がフィルタリングされ、Auto-RP メッセージが転送される前に Auto-RP メッセージから削除されます。

手順

マルチキャスト境界を設定します。

multicast boundary acl [**filter-autorp**]

例：

```
ciscoasa(config-if)# multicast boundary acl1 [filter-autorp]
```

マルチキャスト ルーティングの例

次の例に、さまざまなオプションのプロセスを使用してマルチキャスト ルーティングをイネーブルにし、設定する方法を示します。

1. マルチキャスト ルーティングをイネーブルにします。

```
ciscoasa(config)# multicast-routing
```

2. スタティック マルチキャスト ルートを設定します。

```
ciscoasa(config)# mroute src_ip src_mask {input_if_name | rpf_neighbor} [distance]
ciscoasa(config)# exit
```

3. ASA をマルチキャスト グループのメンバとして設定します。

```
ciscoasa(config)# interface
ciscoasa(config-if)# igmp join-group group-address
```

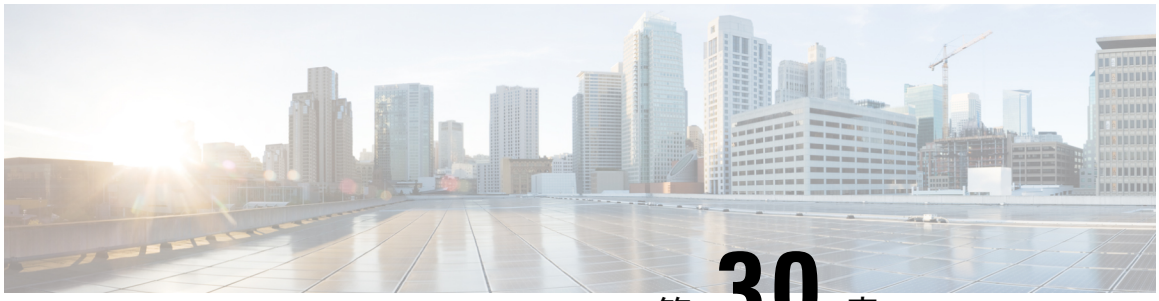
マルチキャスト ルーティングの履歴

表 *31*：マルチキャスト ルーティングの機能履歴

機能名	プラットフォーム リリース	機能情報
マルチキャスト ルーティング サポート	7.0(1)	マルチキャスト ルーティング プロトコルを使用した、データのマルチキャスト ルーティング データ、認証、およびルーティング情報の再配布とモニタリングのサポートが追加されました。 **multicast-routing** コマンドが導入されました。
クラスタリングのサポート	9.0(1)	クラスタリングのサポートが追加されました。 **debug mfib cluster**、**show mfib cluster** の各コマンドが導入されました。
Protocol Independent Multicast Source-Specific Multicast（PIM-SSM）パススルーのサポート	9.5(1)	ASA が最後のホップ ルータである場合を除いて、マルチキャスト ルーティングが有効になっているときに PIM-SSM パケットが通過できるようサポートを追加しました。これにより、さまざまな攻撃から保護すると同時に、マルチキャスト グループをより柔軟に選択できるようになりました。ホストは、明示的に要求された送信元からのトラフィックのみを受信します。 変更されたコマンドはありません。

第 VI 部

AAA サーバおよびローカル データベース



第 30 章

AAA サーバとローカル データベース

この章では、認証、認可、アカウンティング（AAA は「トリプル A」と読む）について説明します。AAA は、コンピュータ リソースへのアクセスを制御するための一連のサービスで、サービスの課金に必要な情報を提供します。これらの処理は、効果的なネットワーク管理およびセキュリティにとって重要です。

この章では、AAA 機能用にローカル データベースを設定する方法について説明します。外部 AAA サーバについては、ご使用のサーバ タイプに関する章を参照してください。

AAA とローカル データベースについて

ここでは、AAA とローカル データベースについて説明します。

認証

認証はユーザを特定する方法です。アクセスが許可されるには、ユーザは通常、有効なユーザ名と有効なパスワードが必要です。AAA サーバは、データベースに保存されている他のユーザ クレデンシャルとユーザの認証資格情報を比較します。クレデンシャルが一致する場合、ユーザはネットワークへのアクセスが許可されます。クレデンシャルが一致しない場合は、認証は失敗し、ネットワーク アクセスは拒否されます。

次の項目を認証するように、Cisco ASA を設定できます。

- ASA へのすべての管理接続（この接続には、次のセッションが含まれます）
  - Telnet
  - SSH
  - シリアル コンソール

- ASDM（HTTPS を使用）
- VPN 管理アクセス

- **enable** コマンド
- ネットワーク アクセス層
- VPN アクセス

認証

許可はポリシーを適用するプロセスです。どのようなアクティビティ、リソース、サービスに対するアクセス許可をユーザが持っているのかを判断します。ユーザが認証されると、そのユーザはさまざまなタイプのアクセスやアクティビティを認可される可能性があります。

次の項目を認可するように、ASA を設定できます。

- 管理コマンド
- ネットワーク アクセス層
- VPN アクセス

アカウンティング

アカウンティングは、アクセス時にユーザが消費したリソースを測定します。これには、システム時間またはセッション中にユーザが送受信したデータ量などが含まれます。アカウンティングは、許可制御、課金、トレンド分析、リソース使用率、キャパシティプランニングのアクティビティに使用されるセッションの統計情報と使用状況情報のログを通じて行われます。

認証、認可、アカウンティング間の相互作用

認証だけで使用することも、認可およびアカウンティングとともに使用することもできます。認可では必ず、ユーザの認証が最初に済んでいる必要があります。アカウンティングだけで使用することも、認証および認可とともに使用することもできます。

AAA Servers

AAA サーバは、アクセス制御に使用されるネットワーク サーバです。認証は、ユーザを識別します。認可は、認証されたユーザがアクセスする可能性があるリソースとサービスを決定するポリシーを実行します。アカウンティングは、課金と分析に使用される時間とデータのリソースを追跡します。

AAA Server Groups

認証、許可、またはアカウンティングに外部 AAA サーバを使用する場合は、まず AAA プロトコルあたり少なくとも 1 つの AAA サーバ グループを作成して、各グループに 1 つ以上のサーバを追加する必要があります。AAA サーバ グループは名前で識別されます。各サーバ グループは、あるサーバまたはサービスに固有です。

次の項を参照してください。

- RADIUS サーバ グループの設定 （923 ページ）
- TACACS+ サーバ グループの設定 （936 ページ）
- LDAP サーバ グループの設定 （948 ページ）

Kerberos、SDI および HTTP フォーム用のサーバ グループも設定できます。これらのグループは VPN 設定で使用されます。これらのグループのタイプについては、『VPN 構成ガイド』を参照してください。

ローカル データベースについて

ASA は、ユーザ プロファイルを取り込むことができるローカル データベースを管理します。AAA サーバの代わりにローカル データベースを使用して、ユーザ認証、認可、アカウンティングを提供することもできます。

次の機能にローカル データベースを使用できます。

- ASDM ユーザごとのアクセス
- コンソール認証
- Telnet 認証および SSH 認証
- **enable** コマンド認証

  この設定は、CLI アクセスにだけ使用され、Cisco ASDM ログインには影響しません。
- コマンド許可

  ローカル データベースを使用するコマンド許可を有効にすると、Cisco ASA では、ユーザ特権レベルを参照して、どのコマンドが使用できるかが特定されます。コマンド許可がディセーブルの場合は通常、特権レベルは参照されません。デフォルトでは、コマンドの特権レベルはすべて、0 または 15 のどちらかです。
- ネットワーク アクセス認証
- VPN クライアント認証

マルチ コンテキスト モードの場合、システム実行スペースでユーザ名を設定し、**login** コマンドを使用して CLI で個々にログインできます。ただし、システム実行スペースではローカル データベースを参照する AAA ルールは設定できません。

（注） ローカル データベースはネットワーク アクセス認可には使用できません。

フォールバック サポート

ローカル データベースは、複数の機能のフォールバック方式として動作できます。この動作は、ASA から誤ってロックアウトされないように設計されています。

ログインすると、コンフィギュレーション内で指定されている最初のサーバから、応答があるまでグループ内のサーバが順に 1 つずつアクセスされます。グループ内のすべてのサーバが使用できない場合、ローカルデータベースがフォールバック方式（管理認証および許可限定）として設定されていると、ASA はローカル データベースに接続しようとします。フォールバック方式として設定されていない場合、ASA は引き続き AAA サーバにアクセスしようとします。

フォールバック サポートを必要とするユーザについては、ローカル データベース内のユーザ名およびパスワードと、AAA サーバ上のユーザ名およびパスワードとを一致させることを推奨します。これにより、透過フォールバックがサポートされます。ユーザは、AAA サーバとローカル データベースのどちらがサービスを提供しているかが判別できないので、ローカル データベースのユーザ名およびパスワードとは異なるユーザ名およびパスワードを AAA サーバで使用することは、指定するべきユーザ名とパスワードをユーザが確信できないことを意味します。

ローカル データベースでサポートされているフォールバック機能は次のとおりです。

- コンソールおよびイネーブル パスワード認証：グループ内のサーバがすべて使用できない場合、ASA ではローカルデータベースを使用して管理アクセスを認証します。これには、イネーブル パスワード認証が含まれる場合があります。
- コマンド許可：グループ内の TACACS+ サーバがすべて使用できない場合、特権レベルに基づいてコマンドを認可するためにローカル データベースが使用されます。
- VPN 認証および認可：VPN 認証および認可は、通常この VPN サービスをサポートしている AAA サーバが使用できない場合、ASA へのリモート アクセスをイネーブルにするためにサポートされます。管理者である VPN クライアントが、ローカル データベースへのフォールバックを設定されたトンネル グループを指定する場合、AAA サーバ グループが使用できない場合でも、ローカル データベースが必要な属性で設定されていれば、VPN トンネルが確立できます。

グループ内の複数のサーバを使用したフォールバックの仕組み

サーバ グループ内に複数のサーバを設定し、サーバ グループのローカル データベースへのフォールバックをイネーブルにしている場合、ASA からの認証要求に対してグループ内のどのサーバからも応答がないと、フォールバックが発生します。次のシナリオで例証します。

サーバ 1、サーバ 2 の順で、LDAP サーバ グループに 2 台の Active Directory サーバを設定します。リモート ユーザがログインすると、ASA によってサーバ 1 に対する認証が試みられます。

サーバ 1 から認証エラー（「user not found」など）が返されると、ASA によるサーバ 2 に対する認証は試みられません。

タイムアウト期間内にサーバ 1 から応答がないと（または認証回数が、設定されている最大数を超えている場合）、ASA によってサーバ 2 に対する認証が試みられます。

グループ内のどちらのサーバからも応答がなく、ASA にローカル データベースへのフォールバックが設定されている場合、ASA によってローカル データベースに対する認証が試みられます。

ローカル データベースのガイドライン

ローカル データベースを認証または認可に使用する場合、ASA からのロックアウトを必ず防止してください。

ローカル データベースへのユーザ アカウントの追加

ユーザをローカル データベースに追加するには、次の手順を実行します。

手順

ステップ 1 ユーザ アカウントを作成します。

username *username* **password** *password* [**privilege** *priv_level*]

例：

```
ciscoasa(config)# username exampleuser1 password madmaxfuryroadrules privilege 1
```

username *username* キーワードは、3 ～ 64 文字の文字列で、スペースと疑問符を除く任意の ASCII 印刷可能文字（文字コード 32 ～ 126）で構成されます。**password** *password* キーワードは、3 ～ 32 文字の文字列で、スペースと疑問符を除く任意の ASCII 印刷可能文字（文字コード 32 ～ 126）で構成できます。**privilege** *priv_level* キーワードでは、0 ～ 15 の範囲で特権レベルを設定します。デフォルトは 2 です。この特権レベルは、コマンド認可で使用されます。

注意 コマンド認可（**aaa authorization console LOCAL** コマンド）を使用していない場合、デフォルトのレベル 2 を使用して特権 EXEC モードにアクセスできます。特権 EXEC モードへのアクセスを制限する場合、特権レベルを 0 または 1 に設定するか、**service-type** コマンドを使用します。

使用頻度の低いこれらのオプションは上記の構文には示されていません。**nopassword** キーワードを使用すると、任意のパスワードを受け入れるユーザ アカウントが作成されます。このオプションは安全ではないため推奨されません。

encrypted キーワードは、（MD5 ベースのハッシュまたは PBKDF2（Password-Based Key Derivation Function 2）ハッシュを使用して）パスワードが暗号化されていることを示します。**username** コマンドのパスワードを定義すると、ASA はセキュリティを維持するために、そのパスワードを設定に保存するときに暗号化します。**show running-config** コマンドを入力すると、**username** コマンドでは実際のパスワードは示されません。暗号化されたパスワードとそれに続けて **encrypted** キーワードが示されます。たとえば、パスワードに「test」と入力すると、**show running-config** コマンドの出力には次のように表示されます。

```
username user1 password DLaUiAX3l78qgoB5c7iVNw== encrypted
```

実際に CLI で **encrypted** キーワードを入力するのは、同じパスワードを使用して、ある設定ファイルを他の ASA で使用するためにカット アンド ペーストする場合だけです。

ステップ 2 （オプション）ユーザ名属性を設定します。

username *username* **attributes**

例：

```
ciscoasa(config)# username exampleuser1 attributes
```

username 引数は、最初の手順で作成したユーザ名です。

デフォルトでは、このコマンドで追加した VPN ユーザには属性またはグループ ポリシーが関連付けられません。**username attributes** コマンドを使用して、すべての値を明示的に設定する必要があります。詳細については、VPN 構成ガイドを参照してください。

ステップ 3 （オプション）管理認可を設定している場合は、**aaa authorization exec** コマンドを使用して、ユーザ レベルを設定します。

service-type {**admin** | **nas-prompt** | **remote-access**}

例：

```
ciscoasa(config-username)# service-type admin
```

admin キーワードは、**aaa authentication console LOCAL** コマンドによって指定されたサービスへのフル アクセスを許可します。デフォルトは **admin** キーワードです。

nas-prompt キーワードは、**aaa authentication** {**telnet** | **ssh** | **serial**} **console** コマンドを設定している場合は CLI へのアクセスを許可しますが、**aaa authentication http console** コマンドを設定している場合は ASDM へのコンフィギュレーション アクセスを拒否します。ASDM モニタリング アクセスは許可します。**aaa authentication enable console** コマンドを使用して認証を有効にしている場合、ユーザは、 **enable** コマンド（または **login** コマンド）を使用して特権 EXEC モードにアクセスできません。

remote-access キーワードは管理アクセスを拒否します。**aaa authentication console** コマンドで指定されたサービスは使用できません（**serial** キーワードを除きます。シリアル アクセスは許可されます）。

ステップ 4 （任意） ユーザ単位の ASA への SSH 接続の公開キー認証については、SSH アクセスの設定（957 ページ） を参照してください。

ステップ 5 （任意） VPN 認証にこのユーザ名を使用している場合、そのユーザに多くの VPN 属性を設定できます。詳細については、VPN 構成ガイドを参照してください。

例

次の例では、admin ユーザ アカウントに対して特権レベル 15 を割り当てます。

```
ciscoasa(config)# username admin password farscape1 privilege 15
```

次の例では、管理認可を有効にし、パスワードを指定してユーザ アカウントを作成し、ユーザ名コンフィギュレーション モードを開始して、**nas-prompt** の **service-type** を指定します。

```
ciscoasa(config)# aaa authorization exec authentication-server
ciscoasa(config)# username user1 password gOrgeOus
ciscoasa(config)# username user1 attributes
ciscoasa(config-username)# service-type nas-prompt
```

ローカル データベースのモニタリング

ローカル データベースのモニタリングについては、次のコマンドを参照してください。

- **show aaa-server**

  このコマンドは、設定されたデータベースの統計情報を表示します。AAA サーバ コンフィギュレーションをクリアするには、**clear aaa-server statistics** コマンドを入力します。

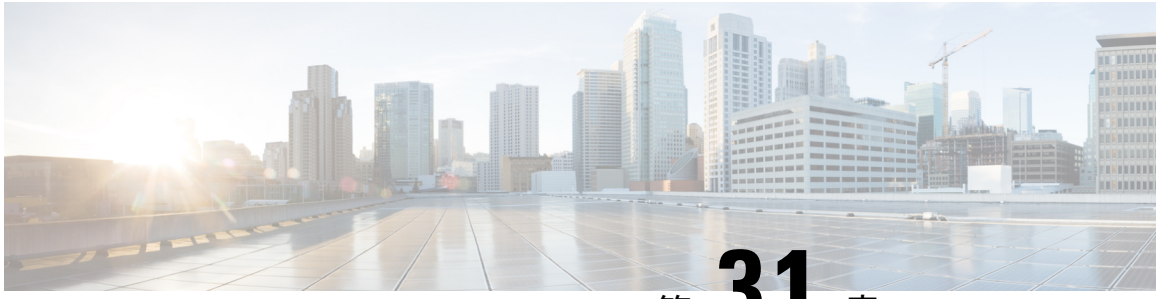
- **show running-config aaa-server**

  このコマンドは、AAA サーバの実行コンフィギュレーションを表示します。AAA サーバの統計情報をクリアするには、**clear configure aaa-server** コマンドを入力します。

ローカル データベースの履歴

表 *32 :* ローカル データベースの履歴

機能名	プラットフォーム リリース	説明
AAA のローカル データベース設定	7.0(1)	AAA 用にローカル データベースを設定する方法について説明します。 次のコマンドを導入しました。 **username**、**aaa authorization exec authentication-server**、**aaa authentication console LOCAL**、**aaa authorization exec LOCAL**、**service-type**、**aaa authentication {telnet | ssh | serial} console LOCAL**、**aaa authentication http console LOCAL**、**aaa authentication enable console LOCAL**、**show running-config aaa-server**、**show aaa-server**、**clear configure aaa-server**、**clear aaa-server statistics**。
SSH 公開キー認証のサポート	9.1(2)	ASA への SSH 接続の公開キー認証は、ユーザ単位で有効にできるようになりました。公開キー ファイル（PKF）でフォーマットされたキーまたは Base64 キーを指定できます。PKF キーは、4096 ビットまで使用できます。ASA がサポートする Base64 形式（最大 2048 ビット）では大きすぎるキーについては、PKF 形式を使用します。 次のコマンドが導入されました。**ssh authenticaion**。 *8.4(4.1)* でも使用可能。*PKF* キー形式は *9.1(2)* でのみサポートされます。



第 31 章

AAA の RADIUS サーバ

この章では、AAA 用に RADIUS サーバを設定する方法について説明します。

AAA 用の RADIUS サーバについて

Cisco ASA は AAA について、次の RFC 準拠 RADIUS サーバをサポートしています。

- Cisco Secure ACS 3.2、4.0、4.1、4.2、および 5.x
- Cisco Identity Services Engine（ISE）
- RSA 認証マネージャ 5.2、6.1 および 7.x の RSA Radius
- Microsoft

サポートされている認証方式

ASA は、RADIUS サーバでの次の認証方式をサポートします。

- PAP：すべての接続タイプの場合。
- CHAP および MS-CHAPv1：L2TP-over-IPsec 接続の場合。
- MS-CHAPv2：L2TP-over-IPsec 接続の場合。また、パスワード管理機能がイネーブルで、通常の IPsec リモート アクセス接続の場合。MS-CHAPv2 は、クライアントレス接続でも使用できます。
- 認証プロキシ モード：RADIUS から Active Directory、RADIUS から RSA/SDI、Radius からトークン サーバ、RSA/SDI から RADIUS の各接続。

（注） MS-CHAPv2 を、ASA と RADIUS サーバの間の VPN 接続で使用されるプロトコルとしてイネーブルにするには、トンネル グループ一般属性でパスワード管理をイネーブルにする必要があります。パスワード管理を有効にすると、ASA から RADIUS サーバへの MS-CHAPv2 認証要求が生成されます。詳細については、**password-management** コマンドの説明を参照してください。

二重認証を使用し、トンネル グループでパスワード管理をイネーブルにした場合は、プライマリ認証要求とセカンダリ認証要求に MS-CHAPv2 要求属性が含まれます。RADIUS サーバが MS-CHAPv2 をサポートしない場合は、**no mschapv2-capable** コマンドを使用して、そのサーバが MS-CHAPv2 以外の認証要求を送信するように設定できます。

VPN 接続のユーザ認証

ASA は、RADIUS サーバを使用して、ダイナミック ACL またはユーザごとの ACL 名を使用する VPN リモート アクセスおよびファイアウォール カットスルー プロキシ セッションのユーザ許可を実行できます。ダイナミック ACL を実装するには、これをサポートするように RADIUS サーバを設定する必要があります。ユーザを認証する場合、RADIUS サーバによってダウンロード可能 ACL、または ACL 名が ASA に送信されます。所定のサービスへのアクセスが ACL によって許可または拒否されます。認証セッションの有効期限が切れると、ASA は ACL を削除します。

ACL に加えて、ASA は、VPN リモート アクセスおよびファイアウォール カットスルー プロキシセッションの認証およびアクセス許可の設定を行うための多くの属性をサポートしています。

RADIUS 属性のサポートされるセット

ASA は次の RADIUS 属性のセットをサポートしています。

- RFC 2138 に定義されている認証属性
- RFC 2139 に定義されているアカウンティング属性
- RFC 2868 に定義されているトンネル プロトコル サポート用の RADIUS 属性
- Cisco IOS ベンダー固有属性（VSA）は、RADIUS ベンダー ID 9 で識別されます。
- RADIUS ベンダー ID 3076 によって識別される Cisco VPN 関連 VSA
- RFC 2548 に定義されている Microsoft VSA

サポートされる RADIUS 認証属性

認可では、権限または属性を使用するプロセスを参照します。認証サーバとして定義されているRADIUSサーバは、権限または属性が設定されている場合はこれらを使用します。これらの属性のベンダー ID は 3076 です。

次の表に、ユーザ認可に使用可能な、サポートされている RADIUS 属性の一覧を示します。

（注） RADIUS 属性名には、cVPN3000 プレフィックスは含まれていません。Cisco Secure ACS 4.x は、この新しい名前をサポートしますが、4.0 以前の ACS の属性名にはまだ cVPN3000 プレフィックスが含まれています。ASA は、属性名ではなく数値の属性 ID に基づいて RADIUS 属性を使用します。

次の表に示した属性はすべてダウンストリーム属性であり、RADIUS サーバから ASA に送信されます。ただし、属性番号146、150、151、および152を除きます。これらの属性番号はアップストリーム属性であり、ASA から RADIUS サーバに送信されます。RADIUS 属性 146 および 150 は、認証および認可の要求の場合に ASA から RADIUS サーバに送信されます。前述の 4 つの属性はすべて、アカウンティング開始、中間アップデート、および終了の要求の場合に ASA から RADIUS サーバに送信されます。アップストリーム RADIUS 属性 146、150、151、152 は、バージョン 8.4(3) で導入されました。

表 *33 :* サポートされる *RADIUS* 認証属性

属性名	ASA	属性番号	構文/タイプ	シングルまたはマルチ値	説明または値
Access-Hours	Y	1	文字列	シングル	時間範囲の名前（Business-hours など）
Access-List-Inbound	Y	86	文字列	シングル	ACL ID
Access-List-Outbound	Y	87	文字列	シングル	ACL ID
Address-Pools	Y	217	文字列	シングル	IP ローカルプールの名前
Allow-Network-Extension-Mode	Y	64	ブール	シングル	0 = 無効1 = 有効
Authenticated-User-Idle-Timeout	Y	50	整数	シングル	1 ～ 35791394 分

属性名	ASA	属性番号	構文/タイプ	シングルまたはマルチ値	説明または値
Authorization-DN-Field	Y	67	文字列	シングル	有効な値：UID、OU、O、CN、L、SP、C、EA、T、N、GN、SN、I、GENQ、DNQ、SER、use-entire-name
Authorization-Required		66	整数	シングル	0 = いいえ 1 = はい
Authorization-Type	Y	65	整数	シングル	0 = なし 1 = RADIUS 2 = LDAP
Banner1	Y	15	文字列	シングル	Cisco VPN リモート アクセス セッション（IPsec IKEv1、AnyConnect SSL-TLS/DTLS/IKEv2、およびクライアントレス SSL）に対して表示されるバナー文字列
Banner2	Y	36	文字列	シングル	Cisco VPN リモート アクセス セッション（IPsec IKEv1、AnyConnect SSL-TLS/DTLS/IKEv2、およびクライアントレス SSL）に対して表示されるバナー文字列。Banner2 文字列は Banner1 文字列に連結されます（設定されている場合）。
Cisco-IP-Phone-Bypass	Y	51	整数	シングル	0 = 無効1 = 有効
Cisco-LEAP-Bypass	Y	75	整数	シングル	0 = 無効1 = 有効

属性名	ASA	属性番号	構文/タイプ	シングルまたはマルチ値	説明または値
クライアントタイプ	Y	150	整数	シングル	1 = Cisco VPN Client（IKEv1） 2 = AnyConnect Client SSL VPN 3 = Clientless SSL VPN 4 = Cut-Through-Proxy 5 = L2TP/IPsec SSL VPN 6 = AnyConnect Client IPsec VPN（IKEv2）
Client-Type-Version-Limiting	Y	77	文字列	シングル	IPsec VPN のバージョン番号を示す文字列
DHCP-Network-Scope	Y	61	文字列	シングル	IP アドレス
Extended-Authentication-On-Rekey	Y	122	整数	シングル	0 = 無効1 = 有効
Framed-Interface-Id	Y	96	文字列	シングル	割り当てられた IPv6 インターフェイス ID。完全に割り当てられた IPv6 アドレスを作成するために、Framed-IPv6-Prefix と組み合わせます。例：Framed-Interface-ID=1:1:1:1 と Framed-IPv6-Prefix=2001:0db8::/64 を組み合わせると、IP アドレス 2001:0db8::1:1:1:1 が得られます。

属性名	ASA	属性番号	構文/タイプ	シングルまたはマルチ値	説明または値
Framed-IPv6-Prefix	Y	97	文字列	シングル	割り当てられた IPv6 プレフィックスと長さ。完全に割り当てられた IPv6 アドレスを作成するために、Framed-Interface-Id と組み合わせます。例：プレフィックス 2001:0db8::/64 と Framed-Interface-Id=1:1:1:1 を組み合わせると、IP アドレス 2001:0db8::1:1:1:1 が得られます。この属性を使用し、プレフィックス長 /128 の完全な IPv6 アドレスを割り当てて、Framed-Interface-Id を使用せずに IP アドレスを割り当てることができます。例：Framed-IPv6-Prefix=2001:db8::1/128。

属性名	ASA	属性番号	構文/タイプ	シングルまたはマルチ値	説明または値
Group-Policy	Y	25	文字列	シングル	リモートアクセス VPN セッションのグループ ポリシーを設定します。バージョン 8.2.x 以降では、IETF-Radius-Class の代わりにこの属性を使用します。次の形式のいずれかを使用できます。 • グループ ポリシー名 • OU=グループ ポリシー名 • OU=グループ ポリシー名;
IE-Proxy-Bypass-Local		83	整数	シングル	0 = なし 1 = ローカル
IE-Proxy-Exception-List		82	文字列	シングル	改行（\n）区切りの DNS ドメインのリスト
IE-Proxy-PAC-URL	Y	133	文字列	シングル	PAC アドレス文字列
IE-Proxy-Server		80	文字列	シングル	IP アドレス
IE-Proxy-Server-Policy		81	整数	シングル	1 = 変更なし 2 = プロキシなし 3 = 自動検出 4 = コンセントレータ設定を使用する
IKE-KeepAlive-Confidence-Interval	Y	68	整数	シングル	10 ～ 300 秒
IKE-Keepalive-Retry-Interval	Y	84	整数	シングル	2 ～ 10 秒
IKE-Keep-Alives	Y	41	ブール	シングル	0 = 無効1 = 有効

属性名	ASA	属性番号	構文/タイプ	シングルまたはマルチ値	説明または値
Intercept-DHCP-Configure-Msg	Y	62	ブール	シングル	0 = 無効1 = 有効
IPsec-Allow-Passwd-Store	Y	16	ブール	シングル	0 = 無効1 = 有効
IPsec-Authentication		13	整数	シングル	0 = なし 1 = RADIUS 2 = LDAP（認可のみ） 3 = NT ドメイン 4 = SDI 5 = 内部 6 = RADIUS での Expiry 認証 7 = Kerberos/Active Directory
IPsec-Auth-On-Rekey	Y	42	ブール	シングル	0 = 無効1 = 有効
IPsec-Backup-Server-List	Y	60	文字列	シングル	サーバ アドレス（スペース区切り）
IPsec-Backup-Servers	Y	59	文字列	シングル	1=クライアントが設定したリストを使用する 2 = クライアントリストをディセーブルにして消去する 3 = バックアップ サーバ リストを使用する
IPsec-Client-Firewall-Filter-Name		57	文字列	シングル	クライアントにファイアウォール ポリシーとして配信するフィルタの名前を指定します。
IPsec-Client-Firewall-Filter-Optional	Y	58	整数	シングル	0 = 必須 1 = オプション
IPsec-Default-Domain	Y	28	文字列	シングル	クライアントに送信するデフォルト ドメイン名を 1 つだけ指定します（1 ～ 255 文字）。

属性名	ASA	属性番号	構文/タイプ	シングルまたはマルチ値	説明または値
IPsec-IKE-Peer-ID-Check	Y	40	整数	シングル	1 = 必須 2 = ピア証明書でサポートされる場合 3 = チェックしない
IPsec-IP-Compression	Y	39	整数	シングル	0 = 無効1 = 有効
IPsec-Mode-Config	Y	31	ブール	シングル	0 = 無効1 = 有効
IPsec-Over-UDP	Y	34	ブール	シングル	0 = 無効1 = 有効
IPsec-Over-UDP-Port	Y	35	整数	シングル	4001 ～ 49151。デフォルトは 10000 です。
IPsec-Required-Client-Firewall-Capability	Y	56	整数	シングル	0 = なし 1 = リモート FW Are-You-There（AYT）で定義されているポリシー 2 = Policy pushed CPP 4 = サーバからのポリシー
IPsec-Sec-Association		12	文字列	シングル	セキュリティ アソシエーションの名前
IPsec-Split-DNS-Names	Y	29	文字列	シングル	クライアントに送信するセカンダリドメイン名のリストを指定します（1 ～ 255 文字）。
IPsec-Split-Tunneling-Policy	Y	55	整数	シングル	0 = スプリット トンネリングなし 1 = スプリット トンネリング 2 = ローカル LAN を許可

属性名	ASA	属性番号	構文/タイプ	シングルまたはマルチ値	説明または値
IPsec-Split-Tunnel-List	Y	27	文字列	シングル	スプリットトンネルの包含リストを記述したネットワークまたはACLの名前を指定します。
IPsec-Tunnel-Type	Y	30	整数	シングル	1 = LAN-to-LAN 2 = リモート アクセス
IPsec-User-Group-Lock		33	ブール	シングル	0 = 無効1 = 有効
IPv6-Address-Pools	Y	218	文字列	シングル	IP ローカル プール IPv6 の名前
IPv6-VPN-Filter	Y	219	文字列	シングル	ACL 値
L2TP-Encryption		21	整数	シングル	ビットマップ： 1 = 暗号化が必要 2 = 40 ビット 4 = 128 ビット 8 = ステートレスが必要 15 = 40/128 ビットで暗号化/ステートレスが必要
L2TP-MPPC-Compression		38	整数	シングル	0 = 無効1 = 有効
Member-Of	Y	145	文字列	シングル	カンマ区切りの文字列。例： `Engineering, Sales` ダイナミック アクセス ポリシーで使用できる管理属性。グループ ポリシーは設定されません。
MS-Client-Subnet-Mask	Y	63	ブール	シングル	IP アドレス
NAC-Default-ACL		92	文字列		ACL

属性名	ASA	属性番号	構文/タイプ	シングルまたはマルチ値	説明または値
NAC-Enable		89	整数	シングル	0 = いいえ 1 = はい
NAC-Revalidation-Timer		91	整数	シングル	300 ～ 86400 秒
NAC-Settings	Y	141	文字列	シングル	NAC ポリシーの名前
NAC-Status-Query-Timer		90	整数	シングル	30 ～ 1800 秒
Perfect-Forward-Secrecy-Enable	Y	88	ブール	シングル	0 = いいえ 1 = はい
PPTP-Encryption		20	整数	シングル	ビットマップ： 1 = 暗号化が必要 2 = 40 ビット 4 = 128 ビット 8 = ステートレスが必要 15 = 40/128 ビットで暗号化/ステートレスが必要
PPTP-MPPC-Compression		37	整数	シングル	0 = 無効1 = 有効
Primary-DNS	Y	5	文字列	シングル	IP アドレス
Primary-WINS	Y	7	文字列	シングル	IP アドレス
Privilege-Level	Y	220	整数	シングル	0 ～ 15 の整数。
Required-Client-Firewall-Vendor-Code	Y	45	整数	シングル	1 = Cisco Systems（Cisco Integrated Client を使用） 2 = Zone Labs 3 = NetworkICE 4 = Sygate 5 = Cisco Systems（Cisco Intrusion Prevention Security Agent を使用）
Required-Client-Firewall-Description	Y	47	文字列	シングル	文字列

属性名	ASA	属性番号	構文/タイプ	シングルまたはマルチ値	説明または値
Required-Client-Firewall-Product-Code	Y	46	整数	シングル	シスコ製品： 1 = Cisco Intrusion Prevention Security Agent または Cisco Integrated Client（CIC） Zone Labs 製品： 1 = Zone Alarm 2 = Zone AlarmPro 3 = Zone Labs Integrity NetworkICE 製品： 1 = BlackIce Defender/Agent Sygate 製品： 1 = Personal Firewall 2 = Personal Firewall Pro 3 = Security Agent
Required-Individual-User-Auth	Y	49	整数	シングル	0 = 無効1 = 有効
Require-HW-Client-Auth	Y	48	ブール	シングル	0 = 無効1 = 有効
Secondary-DNS	Y	6	文字列	シングル	IP アドレス
Secondary-WINS	Y	8	文字列	シングル	IP アドレス
SEP-Card-Assignment		9	整数	シングル	未使用
Session Subtype	Y	152	整数	シングル	0 = なし 1 =クライアントレス 2=クライアント 3=クライアントのみ Session Subtype が適用されるのは、Session Type（151）属性の値が 1、2、3、または 4 の場合のみです。

属性名	ASA	属性番号	構文/タイプ	シングルまたはマルチ値	説明または値
Session Type	Y	151	整数	シングル	0 = なし 1 = AnyConnect Client SSL VPN 2 = AnyConnect Client IPSec VPN（IKEv2） 3 = クライアントレス SSL VPN 4 = クライントレス電子メールプロキシ 5 = Cisco VPN Client（IKEv1） 6 = IKEv1 LAN-LAN 7 = IKEv2 LAN-LAN 8 = VPN ロードバランシング
Simultaneous-Logins	Y	2	整数	シングル	0-2147483647
Smart-Tunnel	Y	136	文字列	シングル	スマートトンネルの名前
Smart-Tunnel-Auto	Y	138	整数	シングル	0 = ディセーブル 1 = イネーブル 2 = 自動スタート
SmartTunnelAutoSignonEnable	Y	139	文字列	シングル	ドメイン名が付加された Smart Tunnel Auto Signon リストの名前
Strip-Realm	Y	135	ブール	シングル	0 = 無効1 = 有効
SVC-Ask	Y	131	文字列	シングル	0 = ディセーブル 1 = イネーブル 3 = デフォルトサービスをイネーブルにする 5 = デフォルトクライアントレスをイネーブルにする （2 と 4 は使用しない）
SVC-Ask-Timeout	Y	132	整数	シングル	5 ～ 120 秒

属性名	ASA	属性番号	構文/タイプ	シングルまたはマルチ値	説明または値
SVC-DPD-Interval-Client	Y	108	整数	シングル	0 = オフ 5 ～ 3600 秒
SVC-DPD-Interval-Gateway	Y	109	整数	シングル	0 = オフ 5 ～ 3600 秒
SVC-DTLS	Y	123	整数	シングル	0 = False 1 = True
SVC-Keepalive	Y	107	整数	シングル	0 = オフ 15 ～ 600 秒
SVC-Modules	Y	127	文字列	シングル	文字列（モジュールの名前）
SVC-MTU	Y	125	整数	シングル	MTU 値 256 ～ 1406 バイト
SVC-Profiles	Y	128	文字列	シングル	文字列（プロファイルの名前）
SVC-Rekey-Time	Y	110	整数	シングル	0 = ディセーブル 1 ～ 10080 分
Tunnel Group Name	Y	146	文字列	シングル	1 ～ 253 文字
Tunnel-Group-Lock	Y	85	文字列	シングル	トンネル グループの名前または「none」
Tunneling-Protocols	Y	11	整数	シングル	1 = PPTP 2 = L2TP 4 = IPSec (IKEv1) 8 = L2TP/IPSec 16 = WebVPN 32 = SVC 64 = IPsec (IKEv2) 8 と 4 は相互排他。0 ～ 11、16 ～ 27、32 ～ 43、48 ～ 59 は有効な値。
Use-Client-Address		17	ブール	シングル	0 = 無効1 = 有効
VLAN	Y	140	整数	シングル	0 ～ 4094
WebVPN-Access-List	Y	73	文字列	シングル	アクセス リスト名
WebVPN ACL	Y	73	文字列	シングル	デバイスの WebVPN ACL 名

属性名	ASA	属性番号	構文/タイプ	シングルまたはマルチ値	説明または値
WebVPN-ActiveX-Relay	Y	137	整数	シングル	0 = 無効 その他 = 有効
WebVPN-Apply-ACL	Y	102	整数	シングル	0 = 無効1 = 有効
WebVPN-Auto-HTTP-Signon	Y	124	文字列	シングル	予約済み
WebVPN-Citrix-Metaframe-Enable	Y	101	整数	シングル	0 = 無効1 = 有効
WebVPN-Content-Filter-Parameters	Y	69	整数	シングル	1 = Java ActiveX 2 = Java スクリプト 4 = イメージ 8 = イメージに含まれるクッキー
WebVPN-Customization	Y	113	文字列	シングル	カスタマイゼーションの名前
WebVPN-Default-Homepage	Y	76	文字列	シングル	URL（たとえば http://example.example.com）
WebVPN-Deny-Message	Y	116	文字列	シングル	有効な文字列（500 文字以内）
WebVPN-Download_Max-Size	Y	157	整数	シングル	0x7fffffff
WebVPN-File-Access-Enable	Y	94	整数	シングル	0 = 無効1 = 有効
WebVPN-File-Server-Browsing-Enable	Y	96	整数	シングル	0 = 無効1 = 有効
WebVPN-File-Server-Entry-Enable	Y	95	整数	シングル	0 = 無効1 = 有効
WebVPN-Group-based-HTTP/HTTPS-Proxy-Exceptions	Y	78	文字列	シングル	オプションのワイルドカード（*）を使用したカンマ区切りの DNS/IP（たとえば、*.cisco.com、192.168.1.*、wwwin.cisco.com）
WebVPN-Hidden-Shares	Y	126	整数	シングル	0 = なし 1 = 表示される

属性名	ASA	属性番号	構文/タイプ	シングルまたはマルチ値	説明または値
WebVPN-HomePageUseSmartTunnel	Y	228	ブール	シングル	クライアントレス ホーム ページをスマート トンネル経由で表示する場合にイネーブルにします。
WebVPN-HTML-Filter	Y	69	Bitmap	シングル	1 = Java ActiveX 2 = スクリプト 4 = イメージ 8 = クッキー
WebVPN-HTTP-Compression	Y	120	整数	シングル	0 = オフ 1 = デフレート圧縮
WebVPN-HTTP-Proxy-IP-Address	Y	74	文字列	シングル	http= または https= プレフィックス付きの、カンマ区切りの DNS/IP:ポート（例：http=10.10.10.10:80、https=11.11.11.11:443）
WebVPN-Idle-Timeout-Alert-Interval	Y	148	整数	シングル	0 ～ 30。0 = ディセーブル。
WebVPN-Keepalive-Ignore	Y	121	整数	シングル	0 ～ 900
WebVPN-Macro-Substitution	Y	223	文字列	シングル	無制限。
WebVPN-Macro-Substitution	Y	224	文字列	シングル	無制限。
WebVPN-Port-Forwarding-Enable	Y	97	整数	シングル	0 = 無効1 = 有効
WebVPN-Port-Forwarding-Exchange-Proxy-Enable	Y	98	整数	シングル	0 = 無効1 = 有効
WebVPN-Port-Forwarding-HTTP-Proxy	Y	99	整数	シングル	0 = 無効1 = 有効
WebVPN-Port-Forwarding-List	Y	72	文字列	シングル	ポート転送リスト名

属性名	ASA	属性番号	構文/タイプ	シングルまたはマルチ値	説明または値
WebVPN-Port-Forwarding-Name	Y	79	文字列	シングル	名前の文字列（例、「Corporate-Apps」）。 このテキストでクライアントレス ポータル ホーム ページのデフォルト文字列「Application Access」が置き換えられます。
WebVPN-Post-Max-Size	Y	159	整数	シングル	0x7fffffff
WebVPN-Session-Timeout-Alert-Interval	Y	149	整数	シングル	0 ～ 30。0 = ディセーブル。
WebVPN SmartCard-Removal-Disconnect	Y	225	ブール	シングル	0 = 無効1 = 有効
WebVPN-Smart-Tunnel	Y	136	文字列	シングル	スマート トンネルの名前
WebVPN-Smart-Tunnel-Auto-Sign-On	Y	139	文字列	シングル	ドメイン名が付加されたスマート トンネル自動サインオン リストの名前
WebVPN-Smart-Tunnel-Auto-Start	Y	138	整数	シングル	0 = 無効1 = 有効2 = 自動スタート

属性名	ASA	属性番号	構文/タイプ	シングルまたはマルチ値	説明または値
WebVPN-Smart-Tunnel-Policy	Y	227	文字列	シングル	「e ネットワーク名」、「i ネットワーク名」、「a」のいずれか。ここで、ネットワーク名は、スマートトンネル ネットワークのリストの名前です。e はトンネルが除外されることを示し、i はトンネルが指定されることを示し、a はすべてのトンネルを示します。
WebVPN-SSL-VPN-Client-Enable	Y	103	整数	シングル	0 = 無効1 = 有効
WebVPN-SSL-VPN-Client-Keep-Installation	Y	105	整数	シングル	0 = 無効1 = 有効
WebVPN-SSL-VPN-Client-Required	Y	104	整数	シングル	0 = 無効1 = 有効
WebVPN-SSO-Server-Name	Y	114	文字列	シングル	有効な文字列
WebVPN-Storage-Key	Y	162	文字列	シングル	
WebVPN-Storage-Objects	Y	161	文字列	シングル	
WebVPN-SVC-Keepalive-Frequency	Y	107	整数	シングル	15 ～ 600 秒、0=オフ
WebVPN-SVC-Client-DPD-Frequency	Y	108	整数	シングル	5 ～ 3600 秒、0=オフ
WebVPN-SVC-DTLS-Enable	Y	123	整数	シングル	0 = 無効1 = 有効
WebVPN-SVC-DTLS-MTU	Y	125	整数	シングル	MTU 値は 256 ～ 1406 バイトです。
WebVPN-SVC-Gateway-DPD-Frequency	Y	109	整数	シングル	5 ～ 3600 秒、0=オフ
WebVPN-SVC-Rekey-Time	Y	110	整数	シングル	4 ～ 10080 分、0=オフ

属性名	ASA	属性番号	構文/タイプ	シングルまたはマルチ値	説明または値
WebVPN-SVC-Rekey-Method	Y	111	整数	シングル	0（オフ）、1（SSL）、2（新しいトンネル）
WebVPN-SVC-Compression	Y	112	整数	シングル	0（オフ）、1（デフォルトの圧縮）
WebVPN-UNIX-Group-ID (GID)	Y	222	整数	シングル	UNIX での有効なグループ ID
WebVPN-UNIX-User-ID (UIDs)	Y	221	整数	シングル	UNIX での有効なユーザ ID
WebVPN-Upload-Max-Size	Y	158	整数	シングル	0x7fffffff
WebVPN-URL-Entry-Enable	Y	93	整数	シングル	0 = 無効1 = 有効
WebVPN-URL-List	Y	71	文字列	シングル	URL リスト名
WebVPN-User-Storage	Y	160	文字列	シングル	
WebVPN-VDI	Y	163	文字列	シングル	設定のリスト

サポートされる IETF RADIUS 認証属性

次の表に、サポートされる IETF RADIUS 属性の一覧を示します。

表 *34* : サポートされる *IETF RADIUS* 属性

属性名	ASA	属性番号	構文/タイプ	シングルまたはマルチ値	説明または値
IETF-Radius-Class	Y	25		シングル	バージョン 8.2.x 以降では、Group-Policy 属性（VSA 3076、#25）を使用することをお勧めします。 • グループ ポリシー名 • OU=グループ ポリシー名 • OU=グループ ポリシー名
IETF-Radius-Filter-Id	Y	11	文字列	シングル	フル トンネルの IPsec クライアントと SSL VPN クライアントのみに適用される、ASA で定義された ACL 名。
IETF-Radius-Framed-IP-Address	Y	n/a	文字列	シングル	IP アドレス
IETF-Radius-Framed-IP-Netmask	Y	n/a	文字列	シングル	IP アドレス マスク
IETF-Radius-Idle-Timeout	Y	28	整数	シングル	Seconds

属性名	ASA	属性番号	構文/タイプ	シングルまたはマルチ値	説明または値
IETF-Radius-Service-Type	Y	6	整数	シングル	秒。使用可能なサービス タイプの値： • .Administrative：ユーザは configure プロンプトへのアクセスを許可されています。 • .NAS-Prompt：ユーザは exec プロンプトへのアクセスを許可されています。 • .remote-access：ユーザはネットワーク アクセスを許可されています。
IETF-Radius-Session-Timeout	Y	27	整数	シングル	Seconds

RADIUS アカウンティング切断の理由コード

これらのコードは、パケットを送信するときに ASA が切断された場合に返されます。

切断の理由コード
ACCT_DISC_USER_REQ = 1
ACCT_DISC_LOST_CARRIER = 2
ACCT_DISC_LOST_SERVICE = 3
ACCT_DISC_IDLE_TIMEOUT = 4
ACCT_DISC_SESS_TIMEOUT = 5
ACCT_DISC_ADMIN_RESET = 6

切断の理由コード
ACCT_DISC_ADMIN_REBOOT = 7
ACCT_DISC_PORT_ERROR = 8
ACCT_DISC_NAS_ERROR = 9
ACCT_DISC_NAS_REQUEST = 10
ACCT_DISC_NAS_REBOOT = 11
ACCT_DISC_PORT_UNNEEDED = 12
ACCT_DISC_PORT_PREEMPTED = 13
ACCT_DISC_PORT_SUSPENDED = 14
ACCT_DISC_SERV_UNAVAIL = 15
ACCT_DISC_CALLBACK = 16
ACCT_DISC_USER_ERROR = 17
ACCT_DISC_HOST_REQUEST = 18
ACCT_DISC_ADMIN_SHUTDOWN = 19
ACCT_DISC_SA_EXPIRED = 21
ACCT_DISC_MAX_REASONS = 22

AAA の RADIUS サーバのガイドライン

ここでは、AAA 用の RADIUS サーバを設定する前に確認する必要のあるガイドラインおよび制限事項について説明します。

- シングル モードで最大 100 個のサーバ グループ、またはマルチ モードでコンテキストごとに 4 つのサーバ グループを持つことができます。
- 各グループには、シングル モードで最大 16 台、マルチ モードで最大 4 台のサーバを含めることができます。

IPv6

AAA サーバは IPv4 アドレスを使用する必要がありますが、エンドポイントは IPv6 を使用できます。

AAA 用の RADIUS サーバの設定

ここでは、AAA 用に RADIUS サーバを設定する方法について説明します。

手順

ステップ 1 ASA の属性を RADIUS サーバにロードします。属性をロードするために使用する方法は、使用している RADIUS サーバのタイプによって異なります。

- Cisco ACS を使用している場合：サーバには、これらの属性がすでに統合されています。したがって、この手順をスキップできます。
- 他のベンダーの RADIUS サーバ（たとえば Microsoft Internet Authentication Service）の場合：ASA の各属性を手動で定義する必要があります。属性を定義するには、属性名または番号、タイプ、値、ベンダー コード（3076）を使用します。

ステップ 2 RADIUS サーバ グループの設定 （923 ページ）。

ステップ 3 グループへの RADIUS サーバの追加 （927 ページ）。

RADIUS サーバ グループの設定

認証、許可、またはアカウンティングに外部 RADIUS サーバを使用する場合は、まず AAA プロトコルあたり少なくとも 1 つの RADIUS サーバ グループを作成して、各グループに 1 つ以上のサーバを追加する必要があります。

手順

ステップ 1 RADIUS AAA サーバ グループを作成します。

aaa-server *group_name* **protocol radius**

例：

```
ciscoasa(config)# aaa-server servergroup1 protocol radius
ciscoasa(config-aaa-server-group)#
```

aaa-server protocol コマンドを入力すると、aaa-server グループ コンフィギュレーション モードが開始します。

ステップ 2 （任意）次のサーバを試す前にグループ内の RADIUS サーバでの AAA トランザクションの失敗の最大数を指定します。

max-failed-attempts *number*

範囲は、1 ～ 5 です。デフォルトは 3 です。

ローカルデータベースを使用してフォールバック方式（管理アクセス専用）を設定している場合で、グループ内のすべてのサーバが応答しないとき、グループは応答なしと見なされ、フォールバック方式が試行されます。サーバ グループで、追加の AAA 要求によるアクセスがない、非応答と見なされる時間が 10 分間（デフォルト）続くと、ただちにフォールバック方式が使用されます。非応答時間をデフォルトから変更するには、次のステップの **reactivation-mode** コマンドを参照してください。

フォールバック方式として設定されていない場合、ASA は引き続きグループ内のサーバにアクセスしようとします。

例：

```
ciscoasa(config-aaa-server-group)# max-failed-attempts 2
```

ステップ 3 （任意）グループ内で障害の発生したサーバを再度アクティブ化する方法（再アクティブ化ポリシー）を指定します。

reactivation-mode {**depletion** [**deadtime** *minutes*] | **timed**}

それぞれの説明は次のとおりです。

- **depletion** [**deadtime** *minutes*] は、グループ内のすべてのサーバが非アクティブになった後でのみ、障害が発生したサーバを再アクティブ化します。これがデフォルトの再アクティブ化モードです。グループ内の最後のサーバがディセーブルになってから、その後すべてのサーバを再度イネーブルにするまでの時間を 0 ～ 1440 分の範囲で指定できます。デフォルトは 10 分です。
- **timed** 30 秒のダウン時間の後、障害が発生したサーバを再アクティブ化します。

例：

```
ciscoasa(config-aaa-server-group)# reactivation-mode deadtime 20
```

ステップ 4 （任意）グループ内のすべてのサーバにアカウンティング メッセージを送信します。

accounting-mode simultaneous

アクティブ サーバだけ送信メッセージをデフォルトに戻すには、**accounting-mode single** コマンドを入力します。

例：

```
ciscoasa(config-aaa-server-group)# accounting-mode simultaneous
```

ステップ 5 （任意）RADIUS 中間アカウンティング アップデート メッセージの定期的な生成をイネーブルにします。

interim-accounting-update [**periodic** [*hours*]]

ISE は、ASA などの NAS デバイスから受信するアカウンティング レコードに基づいて、アクティブ セッションのディレクトリを保持します。ただし、セッションがアクティブであるという通知（アカウンティング メッセージまたはポスチャ トランザクション）を 5 日間受信しなかった場合、ISE はデータベースからそのセッションのレコードを削除します。存続時間の長い VPN 接続が削除されないようにするには、すべてのアクティブ セッションについて ISE に定期的に中間アカウンティング更新メッセージを送信するように、グループを設定します。

- **periodic**[*hours*] は、対象のサーバ グループにアカウンティング レコードを送信するように設定されたすべての VPN セッションのアカウンティング レコードの定期的な生成と伝送をイネーブルにします。オプションで、これらの更新の送信間隔（時間単位）を含めることができます。デフォルトは 24 時間で、指定できる範囲は 1 ～ 120 時間です。
- （パラメータなし）。**periodic** キーワードなしでこのコマンドを使用すると、ASA は、VPN トンネル接続がクライアントレス VPN セッションに追加されたときにのみ中間アカウンティング更新メッセージを送信します。これが発生した場合、新たに割り当てられた IP アドレスを RADIUS に通知するためのアカウンティング アップデートが生成されます。

例：

```
hostname(config-aaa-server-group)# interim-accounting-update periodic 12
```

ステップ 6 （任意）AAA サーバ グループの RADIUS の動的認可（ISE 許可変更、CoA）サービスをイネーブルにします。

dynamic-authorization [**port** *number*]

ポートの指定は任意です。デフォルトは 1700 です。指定できる範囲は 1024 ～ 65535 です。

VPN トンネルでサーバ グループを使用すると、対応する RADIUS サーバ グループが CoA 通知用に登録され、ASA は ISE からの CoA ポリシー更新用ポートをリッスンします。このサーバ グループを ISE と併せてリモート アクセス VPN で使用する場合にのみ動的認可をイネーブルにします。

例：

```
ciscoasa(config-aaa-server-group)# dynamic-authorization
```

ステップ 7 （任意）認証に ISE を使用しない場合は、RADIUS サーバ グループに対し認可専用モードを有効にします。（このサーバ グループを ISE と併せてリモート アクセス VPN で使用する場合にのみ認可専用モードをイネーブルにします）。

authorize-only

これは、サーバ グループを認可に使用するときに、RADIUS アクセス要求メッセージが、AAA サーバ用に設定されているパスワード方式に反して、「認可専用」要求として構築されることを示しています。**radius-common-pw** コマンドを使用して RADIUS サーバの共通パスワードを設定すると、そのパスワードは無視されます。

たとえば、認証にこのサーバ グループではなく証明書を使用する場合には、認可専用モードを使用します。VPN トンネルでの認可とアカウンティングにこのサーバ グループを使用する可能性があるからです。

例：

```
ciscoasa(config-aaa-server-group)# authorize-only
```

ステップ 8 （任意）ダウンロード可能 ACL と、RADIUS パケットから Cisco AV ペアで受信した ACL を結合します。

merge-dacl {**before-avpair** | **after-avpair**}

例：

```
ciscoasa(config-aaa-server-group)# merge-dacl before-avpair
```

このオプションは、VPN 接続にのみ適用されます。VPN ユーザの場合は、ACL は Cisco AV ペア ACL、ダウンロード可能 ACL、および ASA で設定される ACL の形式になります。このオプションでは、ダウンロード可能 ACL と AV ペア ACL を結合するかどうかを決定します。ASA で設定されている ACL には適用されません。

デフォルト設定は **no merge dacl** で、ダウンロード可能な ACL は Cisco AV ペア ACL と結合されません。AV ペアおよびダウンロード可能 ACL の両方を受信した場合は、AV ペアが優先し、使用されます。

before-avpair オプションは、ダウンロード可能 ACL エントリが Cisco-AV-Pair エントリの前に配置されるように指定します。

after-avpair オプションは、ダウンロード可能 ACL エントリが Cisco-AV-Pair エントリの後に配置されるように指定します。

例

次に、単一サーバで 1 つの RADIUS グループを追加する例を示します。

```
ciscoasa(config)# aaa-server AuthOutbound protocol radius
ciscoasa(config-aaa-server-group)# exit
ciscoasa(config)# aaa-server AuthOutbound (inside) host 10.1.1.3
ciscoasa(config-aaa-server-host)# key RadUauthKey
ciscoasa(config-aaa-server-host)# exit
```

次の例は、ISE サーバ グループに、動的認可（CoA）のアップデートと時間ごとの定期的なアカウンティングを設定する方法を示しています。ISE によるパスワード認証を設定するトンネル グループ設定が含まれています。

```
ciscoasa(config)# aaa-server ise protocol radius
ciscoasa(config-aaa-server-group)# interim-accounting-update periodic 1
ciscoasa(config-aaa-server-group)# dynamic-authorization
```

```
ciscoasa(config-aaa-server-group)# exit
ciscoasa(config)# aaa-server ise (inside) host 10.1.1.3
ciscoasa(config-aaa-server-host)# key sharedsecret
ciscoasa(config-aaa-server-host)# exit
ciscoasa(config)# tunnel-group aaa-coa general-attributes
ciscoasa(config-tunnel-general)# address-pool vpn
ciscoasa(config-tunnel-general)# authentication-server-group ise
ciscoasa(config-tunnel-general)# accounting-server-group ise
ciscoasa(config-tunnel-general)# exit
```

次に、ISE でローカル証明書の検証と認可用のトンネル グループを設定する例を示します。サーバ グループは認証用に使用されないため、authorize-only コマンドをサーバ グループ コンフィギュレーションに組み込みます。

```
ciscoasa(config)# aaa-server ise protocol radius
ciscoasa(config-aaa-server-group)# authorize-only
ciscoasa(config-aaa-server-group)# interim-accounting-update periodic 1
ciscoasa(config-aaa-server-group)# dynamic-authorization
ciscoasa(config-aaa-server-group)# exit
ciscoasa(config)# aaa-server ise (inside) host 10.1.1.3
ciscoasa(config-aaa-server-host)# key sharedsecret
ciscoasa(config-aaa-server-host)# exit
ciscoasa(config)# tunnel-group aaa-coa general-attributes
ciscoasa(config-tunnel-general)# address-pool vpn
ciscoasa(config-tunnel-general)# authentication certificate
ciscoasa(config-tunnel-general)# authorization-server-group ise
ciscoasa(config-tunnel-general)# accounting-server-group ise
ciscoasa(config-tunnel-general)# exit
```

グループへの RADIUS サーバの追加

RADIUS サーバをグループに追加するには、次の手順を実行します。

手順

ステップ 1 RADIUS サーバと、そのサーバが属する AAA サーバ グループを識別します。

aaa-server *server_group* [**(***interface_name***)**] **host** *server_ip*

例：

```
ciscoasa(config-aaa-server-group)# aaa-server servergroup1 outside host 10.10.1.1
```

(*interface_name***)** を指定していない場合、ASA はデフォルトで**内部**インターフェイスを使用します。

ステップ 2 RADIUS サーバからダウンロード可能な ACL で受信したネットマスクを ASA が処理する方法を指定します。

acl-netmask-convert {**auto-detect** | **standard** | **wildcard**}

例：

```
ciscoasa(config-aaa-server-host)# acl-netmask-convert standard
```

auto-detect キーワードは、使用されているネットマスク表現のタイプの判別を ASA が試みる必要があることを指定します。ASA によってワイルドカード ネットマスク表現が検出された場合は、標準ネットマスク表現に変換されます。

standard キーワードは、RADIUS サーバから受信したダウンロード可能 ACL には、標準ネットマスク表現のみが含まれていると ASA が見なすように指定します。ワイルドカード ネットマスク表現からの変換は実行されません。

wildcard キーワードは、RADIUS サーバから受信したダウンロード可能 ACL には、ワイルドカード ネットマスク表現のみが含まれていると ASA が見なし、ACL をダウンロードしたときにそれらすべてを標準ネットマスク表現に変換するように指定します。

ステップ 3 ASA を介して RADIUS 認可サーバにアクセスするすべてのユーザが使用する共通パスワードを指定します。

radius-common-pw *string*

例：

```
ciscoasa(config-aaa-server-host)# radius-common-pw examplepassword123abc
```

string 引数は、大文字と小文字が区別される最大 127 文字の英数字キーワードです。RADIUS サーバとのすべての認可トランザクションで共通パスワードとして使用されます。

ステップ 4 RADIUS サーバへの MS-CHAPv2 認証要求をイネーブルにします。

mschapv2-capable

例：

```
ciscoasa(config-aaa-server-host)# mschapv2-capable
```

ステップ 5 サーバへの接続試行のタイムアウト値を指定します。

timeout *seconds*

サーバのタイムアウト間隔（1 ～ 300 秒）を指定します。デフォルトは 10 秒です。各 AAA トランザクションに対して、タイムアウトに達するまで（**retry-interval** コマンドで定義された間隔に基づいて）ASA による接続の再試行が行われます。連続して失敗したトランザクションの数が AAA サーバ グループ内の max-failed-attempts コマンドで指定された制限に達すると、AAA サーバは非アクティブ化され、ASA は（設定されている場合は）別の AAA サーバへの要求の送信を開始します。

例：

```
ciscoasa(config-aaa-server-host)# timeout 15
```

ステップ 6 前のコマンドで指定した特定の AAA サーバに対して、再試行間隔を設定します。

retry-interval *seconds*

例：

```
ciscoasa(config-aaa-server-host)# retry-interval 8
```

seconds 引数に要求の再試行間隔（1 ～ 10 秒）を指定します。これは、接続要求を再試行するまでに ASA が待機する時間です。

（注） RADIUS プロトコルの場合、サーバが ICMP ポート到達不能メッセージで応答すると、再試行間隔の設定が無視され、AAA サーバはただちに障害状態になります。このサーバが AAA グループ内の唯一のサーバである場合は、サーバが再アクティブ化され、別の要求がサーバに送信されます。これは意図された動作です。

ステップ 7 グループ内のすべてのサーバにアカウンティング メッセージを送信します。

accounting-mode simultaneous

例：

```
ciscoasa(config-aaa-server-group)# accounting-mode simultaneous
```

アクティブ サーバにのみメッセージを送信するデフォルトに戻すには、**accounting-mode single** コマンドを入力します。

ステップ 8 認証ポートをポート番号 1645 に指定するか、またはユーザ認証に使用するサーバ ポートを指定します。

authentication-port *port*

例：

```
ciscoasa(config-aaa-server-host)# authentication-port 1646
```

ステップ 9 アカウンティング ポートをポート番号 1646 に指定するか、またはこのホストのアカウンティングに使用するサーバ ポートを指定します。

accounting-port *port*

例：

```
ciscoasa(config-aaa-server-host)# accounting-port 1646
```

ステップ 10 ASA に対する RADIUS サーバの認証に使用されるサーバ秘密値を指定します。設定したサーバ秘密キーは、RADIUS サーバで設定されたサーバ秘密キーと一致する必要があります。サーバ秘密キーの値が不明の場合は、RADIUS サーバの管理者に問い合わせてください。最大長は、64 文字です。

key

例：

```
ciscoasa(config-aaa-host)# key myexamplekey1
```

設定したサーバ秘密キーは、RADIUS サーバで設定されたサーバ秘密キーと一致する必要があります。サーバ秘密キーの値が不明の場合は、RADIUS サーバの管理者に問い合わせてください。最大長は、64 文字です。

例

次に、既存の RADIUS サーバ グループに RADIUS サーバを追加する例を示します。

```
ciscoasa(config)# aaa-server svrgrp1 protocol radius
ciscoasa(config-aaa-server-group)# aaa-server svrgrp1 host 192.168.3.4
ciscoasa(config-aaa-server-host)# acl-netmask-convert wildcard
ciscoasa(config-aaa-server-host)# radius-common-pw myexaplepasswordabc123
ciscoasa(config-aaa-server-host)# mschapv2-capable
ciscoasa(config-aaa-server-host)# timeout 9
ciscoasa(config-aaa-server-host)# retry-interval 7
ciscoasa(config-aaa-server-host)# accounting-mode simultaneous
ciscoasa(config-aaa-server-host)# authentication-port 1650
ciscoasa(config-aaa-server-host)# authorization-port 1645
ciscoasa(config-aaa-server-host)# key mysecretkeyexampleiceage2
ciscoasa(config-aaa-server-host)# exit
ciscoasa(config)#
```

AAA 用の RADIUS サーバのモニタリング

AAA 用の RADIUS サーバのステータスのモニタリングについては、次のコマンドを参照してください。

- **show aaa-server**

  このコマンドは、設定された RADIUS サーバの統計情報を表示します。**clear aaa-server statistics** コマンドを使用して、カウンタをゼロにリセットできます。

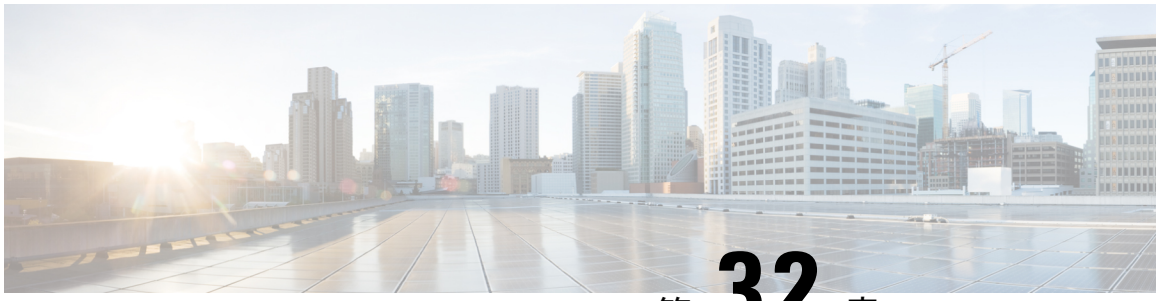
- **show running-config aaa-server**

  このコマンドは、RADIUS サーバの実行コンフィギュレーションを表示します。

AAA 用の RADIUS サーバの履歴

表 *35 : AAA* 用の *RADIUS* サーバの履歴

機能名	プラットフォーム リリース	説明
AAA の RADIUS サーバ	7.0(1)	AAA 用の RADIUS サーバを設定する方法について説明します。 次のコマンドを導入しました。 **aaa-server protocol**、**max-failed-attempts**、**reactivation-mode**、**accounting-mode simultaneous**、**aaa-server host**、**show aaa-server**、**show running-config aaa-server**、**clear aaa-server statistics**、**authentication-port**、**accounting-port**、**retry-interval**、**acl-netmask-convert**、**clear configure aaa-server**、**merge-dacl**、**radius-common-pw**、**key**。
ASA からの RADIUS アクセス要求パケットおよびアカウンティング要求パケットでの主なベンダー固有属性（VSA）の送信	8.4(3)	4 つの新しい VSA：Tunnel Group Name（146）および Client Type（150）は、ASA からの RADIUS アクセス要求パケットで送信されます。Session Type（151）および Session Subtype（152）は、ASA からの RADIUS アカウンティング要求パケットで送信されます。4 つのすべての属性が、すべてのアカウンティング要求パケット タイプ（開始、中間アップデート、および終了）に送信されます。RADIUS サーバ（ACS や ISE など）は、認可属性やポリシー属性を強制適用したり、アカウンティングや課金のためにそれらの属性を使用したりできます。



第 32 章

AAA 用の TACACS+ サーバ

この章では、AAA で使われる TACACS+ サーバの設定方法について説明します。

AAA 用の TACACS+ サーバについて

ASA は、ASCII、PAP、CHAP、MS-CHAPv1 の各プロトコルで TACACS+ サーバ認証をサポートします。

TACACS+ 属性

Cisco ASA は、TACACS+ 属性をサポートします。TACACS+ 属性は、認証、許可、アカウンティングの機能を分離します。プロトコルでは、必須とオプションの 2 種類の属性をサポートします。サーバとクライアントの両方で必須属性を解釈できる必要があり、また、必須属性はユーザに適用する必要があります。オプションの属性は、解釈または使用できることも、できないこともあります。

（注） TACACS+ 属性を使用するには、NAS 上で AAA サービスがイネーブルになっていることを確認してください。

次の表に、カットスループロキシ接続に対してサポートされる TACACS+ 許可応答属性の一覧を示します。

表 *36 :* サポートされる *TACACS+* 許可応答属性

属性	説明
acl	接続に適用する、ローカルで設定済みの ACL を識別します。
idletime	認証済みユーザ セッションが終了する前に許可される非アクティブ時間（分）を示します。
timeout	認証済みユーザ セッションが終了する前に認証クレデンシャルがアクティブな状態でいる絶対時間（分）を指定します。

次の表に、サポートされる TACACS+ アカウンティング属性の一覧を示します。

。

表 *37 :* サポートされる *TACACS+* アカウンティング属性

属性	説明
bytes_in	この接続中に転送される入力バイト数を指定します（ストップ レコードのみ）。
bytes_out	この接続中に転送される出力バイト数を指定します（ストップ レコードのみ）。
cmd	実行するコマンドを定義します（コマンド アカウンティングのみ）。
disc-cause	切断理由を特定する数字コードを示します（ストップ レコードのみ）。
elapsed_time	接続の経過時間（秒）を定義します（ストップ レコードのみ）。
foreign_ip	トンネル接続のクライアントの IP アドレスを指定します。最下位のセキュリティ インターフェイスでカットスルー プロキシ接続のアドレスを定義します。
local_ip	トンネル接続したクライアントの IP アドレスを指定します。最上位のセキュリティインターフェイスでカットスルー プロキシ接続のアドレスを定義します。
NAS port	接続のセッション ID が含まれます。

属性	説明
packs_in	この接続中に転送される入力パケット数を指定します。
packs_out	この接続中に転送される出力パケット数を指定します。
priv-level	コマンド アカウンティング要求の場合はユーザの権限レベル、それ以外の場合は 1 に設定されます。
rem_iddr	クライアントの IP アドレスを示します。
service	使用するサービスを指定します。コマンド アカウンティングの場合にのみ、常に「shell」に設定されます。
task_id	アカウンティング トランザクションに固有のタスク ID を指定します。
username	ユーザの名前を示します。

AAA 用の TACACS+ サーバのガイドライン

ここでは、AAA 用の TACACS+ サーバを設定する前に確認する必要のあるガイドラインおよび制限事項について説明します。

IPv6

AAA サーバは IPv4 アドレスを使用する必要がありますが、エンドポイントは IPv6 を使用できます。

その他のガイドライン

- シングル モードで最大 100 個のサーバ グループ、またはマルチ モードでコンテキストごとに 4 つのサーバ グループを持つことができます。
- 各グループには、シングル モードで最大 16 台、マルチ モードで最大 4 台のサーバを含めることができます。

TACACS+ サーバの設定

ここでは、TACACS+ サーバを設定する方法について説明します。

手順

ステップ 1 TACACS+ サーバ グループの設定 （936 ページ）。
ステップ 2 グループへの TACACS+ サーバの追加 （937 ページ）。

TACACS+ サーバ グループの設定

認証、許可、アカウンティングに TACACS+ サーバを使用する場合は、まず TACACS+ サーバ グループを少なくとも 1 つ作成し、各グループに 1 台以上のサーバを追加する必要があります。TACACS+ サーバ グループは名前で識別されます。

TACACS+ サーバ グループを追加するには、次の手順を実行します。

手順

ステップ 1 サーバ グループ名とプロトコルを指定します。

aaa-server *server_tag* **protocol tacacs+**

例：

```
ciscoasa(config)# aaa-server servergroup1 protocol tacacs+
```

aaa-server protocol コマンドを入力すると、aaa-server グループ コンフィギュレーション モードが開始します。

ステップ 2 次のサーバを試す前にグループ内の AAA サーバでの AAA トランザクションの失敗の最大数を指定します。

max-failed-attempts *number*

例：

```
ciscoasa(config-aaa-server-group)# max-failed-attempts 2
```

number 引数の範囲は 1 ～ 5 です。デフォルトは 3 です。

ローカルデータベースを使用してフォールバック方式（管理アクセス専用）を設定している場合で、グループ内のすべてのサーバが応答しないとき、グループは応答なしと見なされ、フォールバック方式が試行されます。サーバ グループで、追加の AAA 要求によるアクセスがない、非応答と見なされる時間が 10 分間（デフォルト）続くと、ただちにフォールバック方式が使用されます。非応答時間をデフォルトから変更するには、次のステップの **reactivation-mode** コマンドを参照してください。

フォールバック方式として設定されていない場合、ASA は引き続きグループ内のサーバにアクセスしようとします。

ステップ 3 グループ内で障害の発生したサーバを再度アクティブ化する方法（再アクティブ化ポリシー）を指定します。

reactivation-mode {**depletion** [**deadtime** *minutes*] | **timed**}

例：

```
ciscoasa(config-aaa-server-group)# reactivation-mode deadtime 20
```

depletion キーワードを指定すると、グループ内のすべてのサーバが非アクティブになって初めて、障害の発生したサーバが再度アクティブ化されます。

deadtime *minutes* キーワードと引数のペアは、グループ内の最後のサーバをディセーブルにしてから次にすべてのサーバを再度イネーブルにするまでの経過時間を、0 ～ 1440 分の範囲で指定します。デフォルトは 10 分です。

timed キーワードは、30 秒間のダウンタイムの後に障害が発生したサーバを再度アクティブ化します。

ステップ 4 グループ内のすべてのサーバにアカウンティング メッセージを送信します。

accounting-mode simultaneous

例：

```
ciscoasa(config-aaa-server-group)# accounting-mode simultaneous
```

アクティブ サーバにのみメッセージを送信するデフォルトに戻すには、**accounting-mode single** コマンドを入力します。

例

次の例では、1 台のプライマリ サーバと 1 台のバックアップ サーバで構成された 1 つの TACACS+ グループを追加する例を示します。

```
ciscoasa(config)# aaa-server AuthInbound protocol tacacs+
ciscoasa(config-aaa-server-group)# max-failed-attempts 2
ciscoasa(config-aaa-server-group)# reactivation-mode depletion deadtime 20
ciscoasa(config-aaa-server-group)# exit
ciscoasa(config)# aaa-server AuthInbound (inside) host 10.1.1.1
ciscoasa(config-aaa-server-host)# key TACPlusUauthKey
ciscoasa(config-aaa-server-host)# exit
ciscoasa(config)# aaa-server AuthInbound (inside) host 10.1.1.2
ciscoasa(config-aaa-server-host)# key TACPlusUauthKey2
ciscoasa(config-aaa-server-host)# exit
```

グループへの TACACS+ サーバの追加

TACACS+ サーバをグループに追加するには、次の手順を実行します。

手順

ステップ 1 TACACS+ サーバと、そのサーバが属するサーバ グループを識別します。

aaa-server *server_group* [**(***interface_name***)**] **host** *server_ip*

例：

```
ciscoasa(config-aaa-server-group)# aaa-server servergroup1 outside host 10.10.1.1
```

(*interface_name***)** を指定していない場合、ASA はデフォルトで**内部**インターフェイスを使用します。

ステップ 2 サーバへの接続試行のタイムアウト値を指定します。

timeout *seconds*

サーバのタイムアウト間隔（1 ～ 300 秒）を指定します。デフォルトは 10 秒です。各 AAA トランザクションに対して、タイムアウトに達するまで（**retry-interval** コマンドで定義された間隔に基づいて）ASA による接続の再試行が行われます。連続して失敗したトランザクションの数が AAA サーバ グループ内の max-failed-attempts コマンドで指定された制限に達すると、AAA サーバは非アクティブ化され、ASA は（設定されている場合は）別の AAA サーバへの要求の送信を開始します。

例：

```
ciscoasa(config-aaa-server-host)# timeout 15
```

ステップ 3 ポート番号 49、または ASA によって TACACS+ サーバとの通信に使用される TCP ポート番号を指定します。

server-port *port_number*

例：

```
ciscoasa(config-aaa-server-host)# server-port 49
```

ステップ 4 TACACS+ サーバに対する NAS の認証に使用されるサーバ秘密値を指定します。

key

例：

```
ciscoasa(config-aaa-host)# key myexamplekey1
```

この値は大文字と小文字が区別される、最大127文字の英数字から成るキーワードで、TACACS+ サーバ上のキーと同じ値です。127 を超える文字は無視されます。このキーはクライアントとサーバ間でデータを暗号化するために使われ、クライアントとサーバ両方のシステムで同じで

ある必要があります。このキーにスペースを含めることはできませんが、他の特殊文字は使用できます。

AAA 用の TACACS+ サーバのモニタリング

AAA 用の TACACS+ サーバのモニタリングについては、次のコマンドを参照してください。

- **show aaa-server**

  このコマンドは、設定された TACACS+ サーバの統計情報を表示します。TACACS+ サーバの統計情報をクリアするには、**clear aaa-server statistics** コマンドを入力します。

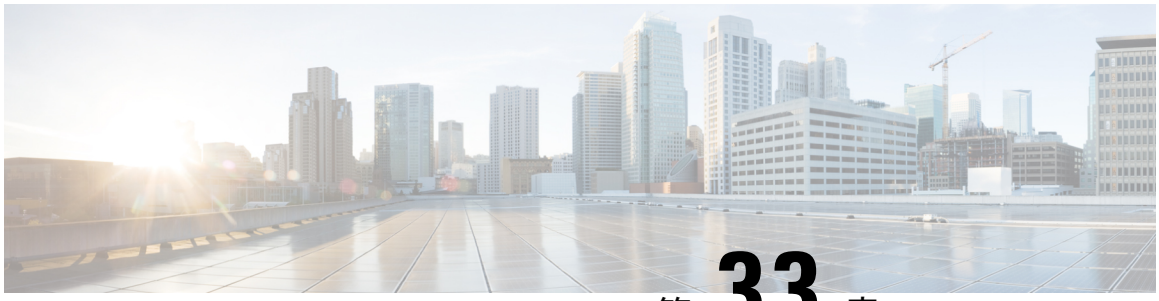
- **show running-config aaa-server**

  このコマンドは、TACACS+サーバの実行コンフィギュレーションを表示します。TACACS+ サーバ コンフィギュレーションをクリアするには、**clear configure aaa-server** コマンドを入力します。

AAA 用の TACACS+ サーバの履歴

表 *38 : AAA* 用の *TACACS+* サーバの履歴

機能名	プラットフォーム リリース	説明
TACACS+ サーバ	7.0(1)	AAA に TACACS+ サーバを設定する方法について説明します。 次のコマンドを導入しました。 **aaa-server protocol**、**max-failed-attempts**、**reactivation-mode**、**accounting-mode simultaneous**、**aaa-server host**、**aaa authorization exec authentication-server**、**server-port**、**key**、**clear aaa-server statistics**、**clear configure aaa-server**、**show aaa-server**、**show running-config aaa-server**、**username**、**service-type**、**timeout**.



第 33 章

AAA の LDAP サーバ

この章では、AAA で使用される LDAP サーバの設定方法について説明します。

LDAP および ASA について

Cisco ASA はほとんどの LDAPv3 ディレクトリ サーバと互換性があり、それには次のものが含まれます。

- Sun Microsystems JAVA System Directory Server（現在は Oracle Directory Server Enterprise Edition の一部、旧名 Sun ONE Directory Server）
- Microsoft Active Directory
- Novell
- OpenLDAP

デフォルトでは、ASA によって Microsoft Active Directory、Sun LDAP、Novell、OpenLDAP、または汎用 LDAPv3 ディレクトリ サーバに接続しているかどうかが自動検出されます。ただし、LDAP サーバ タイプの自動検出による決定が失敗した場合は、手動で設定できます。

LDAP での認証方法

認証中、ASA は、ユーザの LDAP サーバへのクライアント プロキシとして機能し、プレーン テキストまたは Simple Authentication and Security Layer（SASL）プロトコルのいずれかを使って LDAP サーバに対する認証を行います。デフォルトで、ASA は、通常はユーザ名とパスワードである認証パラメータを LDAP サーバにプレーン テキストで渡します。

ASA では、次の SASL メカニズムをサポートしています。次に、強度の低い順番に示します。

- Digest-MD5：ASA は、ユーザ名とパスワードから計算した MD5 値を使用して LDAP サーバに応答します。
- Kerberos：ASA は、GSSAPI Kerberos メカニズムを使用して、ユーザ名とレルムを送信することで LDAP サーバに応答します。

ASA と LDAP サーバは、これらの SASL メカニズムの任意の組み合わせをサポートします。複数のメカニズムを設定した場合、ASA ではサーバに設定されている SASL メカニズムのリストが取得され、認証メカニズムは ASA とサーバの両方に設定されているメカニズムのなかで最も強力なものに設定されます。たとえば、LDAP サーバと ASA の両方がこれら両方のメカニズムをサポートしている場合、ASA は、強力な方の Kerberos メカニズムを選択します。

ユーザ LDAP 認証が成功すると、LDAP サーバは認証されたユーザの属性を返します。VPN 認証の場合、通常これらの属性には、VPN セッションに適用される認可データが含まれます。この場合、LDAP の使用により、認証と許可を 1 ステップで実行できます。

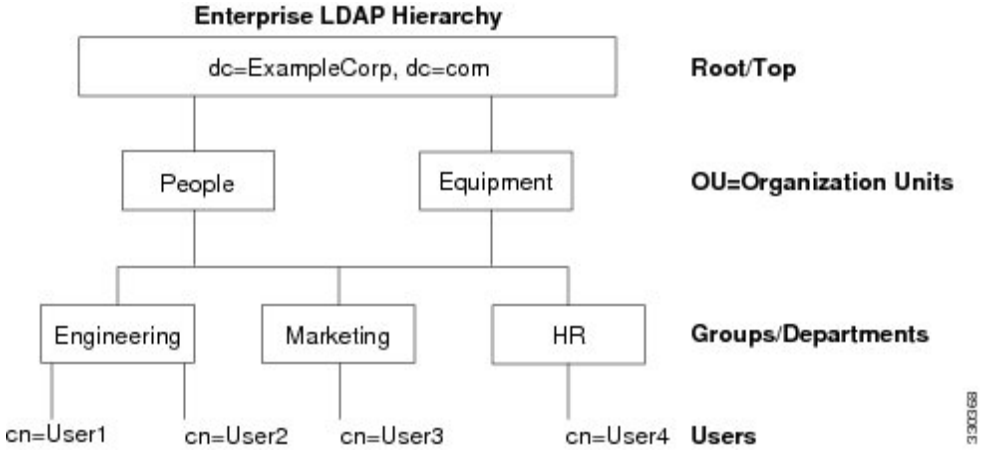
（注） LDAP プロトコルの詳細については、RFC 1777、2251、および 2849 を参照してください。

LDAP 階層

LDAP コンフィギュレーションは、組織の論理階層が反映されたものにする必要があります。たとえば、Example Corporation という企業の従業員 Employee1 を例に考えてみます。Employee1 は Engineering グループに従事しています。この企業の LDAP 階層は 1 つ以上のレベルを持つことができます。たとえば、シングルレベル階層をセットアップします。この中で、Employee1 は Example Corporation のメンバーであると見なされます。あるいは、マルチレベル階層をセットアップします。この中で、Employee1 は Engineering 部門のメンバーであると見なされ、この部門は People という名称の組織ユニットのメンバーであり、この組織ユニットは Example Corporation のメンバーです。マルチレベル階層の例については、次の図を参照してください。

マルチレベル階層の方が詳細ですが、検索結果が速く返されるのはシングルレベル階層の方です。

図 *54 :* マルチレベルの *LDAP* 階層



LDAP 階層の検索

ASA は、LDAP 階層内での検索を調整できます。ASA に次の 3 種類のフィールドを設定すると、LDAP 階層での検索開始場所とその範囲、および検索する情報のタイプを定義できます。これらのフィールドは、ユーザの権限が含まれている部分だけを検索するように階層の検索を限定します。

- LDAP Base DN では、サーバが ASA から認可要求を受信したときに LDAP 階層内のどの場所からユーザ情報の検索を開始するかを定義します。
- Search Scope では、LDAP 階層の検索範囲を定義します。この指定では、LDAP Base DN よりもかなり下位のレベルまで検索します。サーバによる検索を直下の 1 レベルだけにするか、サブツリー全体を検索するかを選択できます。シングルレベルの検索の方が高速ですが、サブツリー検索の方が広範囲に検索できます。
- Naming Attribute では、LDAP サーバのエントリを一意に識別する RDN を定義します。一般的な名前属性には、cn（一般名）、sAMAccountName、および userPrincipalName を含めることができます。

次の図に、Example Corporation の LDAP 階層の例を示します。この階層が指定されると、複数の方法で検索を定義できます。次の表に、2つの検索コンフィギュレーションの例を示します。

最初のコンフィギュレーションの例では、Employee1 が IPSec トンネルを確立するときに LDAP 認可が必要であるため、ASA から LDAP サーバに検索要求が送信され、この中で Employee1 を Engineering グループの中で検索することが指定されます。この検索は短時間でできます。

2 番目のコンフィギュレーションの例では、ASA から送信される検索要求の中で、Employee1 を Example Corporation 全体の中で検索することが指定されています。この検索には時間がかかります。

表 *39 :* 検索コンフィギュレーションの例

番号	LDAP Base DN	検索範囲	名前属性	結果
1	group=Engineering,ou=People,dc=ExampleCorporation,dc=com	1 レベル	cn=Employee1	検索が高速
2	dc=ExampleCorporation,dc=com	サブツリー	cn=Employee1	検索に時間がかかる

LDAP サーバへのバインド

ASA は、ログイン DN とログイン パスワードを使用して、LDAP サーバとの信頼（バインド）を築きます。Microsoft Active Directory の読み取り専用操作（認証、許可、グループ検索など）を行うとき、ASA では特権の低いログイン DN でバインドできます。たとえば、Login DN には、AD の「Member Of」の指定が Domain Users の一部であるユーザを指定することができます。VPN のパスワード管理操作では、Login DN にはより高い特権が必要となり、AD の Account Operators グループの一部を指定する必要があります。

次に、Login DN の例を示します。

```
cn=Binduser1,ou=Admins,ou=Users,dc=company_A,dc=com
```

ASA は次の認証方式をサポートしています。

- 暗号化されていないパスワードを使用したポート 389 での簡易 LDAP 認証
- ポート 636 でのセキュアな LDAP（LDAP-S）
- Simple Authentication and Security Layer（SASL）MD5
- SASL Kerberos

ASA は匿名認証をサポートしていません。

（注） LDAP クライアントとしての ASA は、匿名のバインドや要求の送信をサポートしていません。

LDAP 属性マップ

ASA では、次の目的での認証のために LDAP ディレクトリを使用できます。

- VPN リモート アクセス ユーザ
- ファイアウォール ネットワークのアクセス/カットスルー プロキシ セッション
- ACL、ブックマーク リスト、DNS または WINS 設定、セッション タイマーなどのポリシーの権限（または許可属性と呼ばれる）の設定

- ローカル グループ ポリシーのキー属性の設定

ASA は、LDAP 属性マップを使用して、ネイティブ LDAP ユーザ属性を Cisco ASA 属性に変換します。それらの属性マップを LDAP サーバにバインドしたり、削除したりすることができます。また、属性マップを表示または消去することもできます。

LDAP 属性マップは複数値属性をサポートしません。たとえば、あるユーザが複数の AD グループのメンバで、LDAP 属性マップが複数のグループと一致する場合、選択される値は一致するエントリのアルファベット順に基づくものです。

属性マッピング機能を適切に使用するには、LDAP 属性の名前と値およびユーザ定義の属性の名前と値を理解する必要があります。

頻繁にマッピングされる LDAP 属性の名前と、一般にマッピングされるユーザ定義の属性のタイプは次のとおりです。

- IETF-Radius-Class（ASA バージョン 8.2 以降における Group_Policy）：ディレクトリ部門またはユーザ グループ（たとえば、Microsoft Active Directory memberOf）属性値に基づいてグループ ポリシーを設定します。ASDM バージョン 6.2/ASA バージョン 8.2 以降では、IETF-Radius-Class 属性の代わりに group-policy 属性が使用されます。
- IETF-Radius-Filter-Id：VPN クライアント、IPSec、SSL に対するアクセス コントロール リスト（ACL）に適用されます。
- IETF-Radius-Framed-IP-Address：VPN リモート アクセス クライアント、IPSec、および SSL にスタティック IP アドレスを割り当てます。
- Banner1：VPN リモート アクセス ユーザのログイン時にテキスト バナーを表示します。
- Tunneling-Protocols：アクセス タイプに基づいて、VPN リモート アクセス セッションを許可または拒否します。

（注） 1 つの LDAP 属性マップに、1 つ以上の属性を含めることができます。特定の LADP サーバからは、1 つの LDAP 属性のみをマップすることができます。

AAA の LDAP サーバのガイドライン

この項では、AAA の LDAP サーバを設定する前に確認する必要のあるガイドラインおよび制限事項について説明します。

IPv6

AAA サーバは IPv4 アドレスを使用する必要がありますが、エンドポイントは IPv6 を使用できます。

その他のガイドライン

- Sun ディレクトリ サーバにアクセスするために ASA に設定されている DN が、サーバのデフォルト パスワード ポリシーにアクセスできる必要があります。DN として、ディレクトリ管理者、またはディレクトリ管理者権限を持つユーザを使用することを推奨します。または、デフォルト パスワード ポリシーに ACL を設定できます。
- Microsoft Active Directory および Sun サーバでのパスワード管理をイネーブルにするために LDAP over SSL を設定する必要があります。
- ASA は、Novell、OpenLDAP およびその他の LDAPv3 ディレクトリ サーバによるパスワード管理をサポートしません。
- バージョン 7.1（x）以降、ASA はネイティブ LDAP スキーマを使用して認証および認可を行うため、Cisco スキーマは必要なくなりました。
- シングルモードの場合は最大 100 台の LDAP サーバ グループを使用でき、マルチモードの場合は各コンテキストで最大 4 台の LDAP サーバ グループを使用できます。
- 各グループには、シングル モードで最大 16 台、マルチ モードで最大 4 台の LDAP サーバを含めることができます。
- ユーザがログインすると、コンフィギュレーション内で指定されている最初のサーバから順に、サーバが応答するまで LDAP サーバが 1 つずつアクセスされます。グループ内のすべてのサーバが使用できない場合、ASA は、ローカル データベースがフォールバック方式として設定されていると、ローカルデータベースに接続しようとします（管理認証および認可限定）。フォールバック メソッドとして設定されていない場合、ASA は LDAP サーバに引き続きアクセスしようとします。

AAA の LDAP サーバの設定

この項では、AAA に LDAP サーバを設定する方法について説明します。

手順

ステップ 1 LDAP 属性マップを設定します。LDAP 属性マップの設定 （946 ページ）を参照してください。

ステップ 2 LDAP サーバ グループを追加します。LDAP サーバ グループの設定 （948 ページ）を参照してください。

ステップ 3 （オプション）認証メカニズムとは別の異なる、LDAP サーバからの許可を設定します。「VPN の LDAP 認証の設定 （951 ページ）」を参照してください。

LDAP 属性マップの設定

LDAP 属性マップを設定するには、次の手順を実行します。

手順

ステップ 1 空の LDAP 属性マップ テーブルを作成します。

ldap-attribute-map *map-name*

例：

```
ciscoasa(config)# ldap-attribute-map att_map_1
```

ステップ 2 ユーザ定義の属性名 department を、シスコの属性にマッピングします。

map-name *user-attribute-name Cisco-attribute-name*

例：

```
ciscoasa(config-ldap-attribute-map)# map-name department IETF-Radius-Class
```

ステップ 3 ユーザ定義のマップ値である department をユーザ定義の属性値とシスコの属性値にマッピングします。

map-value *user-attribute-name Cisco-attribute-name*

例：

```
ciscoasa(config-ldap-attribute-map)# map-value department Engineering group1
```

ステップ 4 サーバと、そのサーバが属する AAA サーバ グループを識別します。

aaa-server *server_group* [*interface_name*] **host** *server_ip*

例：

```
ciscoasa(config)# aaa-server ldap_dir_1 host 10.1.1.4
```

ステップ 5 属性マップを LDAP サーバにバインドします。

ldap-attribute-map *map-name*

例：

```
ciscoasa(config-aaa-server-host)# ldap-attribute-map att_map_1
```

例

次の例は、accessType という名前のLDAP 属性に基づいて管理セッションを ASA に制限する方法を示しています。accessType 属性には、以下の値のいずれかが含まれる可能性があります。

- [VPN]
- admin
- helpdesk

次の例では、各値が、ASA でサポートされる有効な IETF-Radius-Service-Type 属性のいずれかにマッピングされる方法を示します。有効なタイプには、remote-access（Service-Type 5）発信、admin（Service-Type 6）管理、および nas-prompt（Service-Type 7）NAS プロンプトがあります。

```
ciscoasa(config)# ldap attribute-map MGMT
ciscoasa(config-ldap-attribute-map)# map-name accessType IETF-Radius-Service-Type
ciscoasa(config-ldap-attribute-map)# map-value accessType VPN 5
ciscoasa(config-ldap-attribute-map)# map-value accessType admin 6
ciscoasa(config-ldap-attribute-map)# map-value accessType helpdesk 7

ciscoasa(config-ldap-attribute-map)# aaa-server LDAP protocol ldap
ciscoasa(config-aaa-server-group)# aaa-server LDAP (inside) host 10.1.254.91
ciscoasa(config-aaa-server-host)# ldap-base-dn CN=Users,DC=cisco,DC=local
ciscoasa(config-aaa-server-host)# ldap-scope subtree
ciscoasa(config-aaa-server-host)# ldap-login-password test
ciscoasa(config-aaa-server-host)# ldap-login-dn CN=Administrator,CN=Users,DC=cisco,DC=local
ciscoasa(config-aaa-server-host)# server-type auto-detect
ciscoasa(config-aaa-server-host)# ldap-attribute-map MGMT
```

次の例では、シスコの LDAP 属性名の全リストを表示します。

```
ciscoasa(config)# ldap attribute-map att_map_1
ciscoasa(config-ldap-attribute-map)# map-name att_map_1?

ldap mode commands/options:
cisco-attribute-names:
  Access-Hours
  Allow-Network-Extension-Mode
  Auth-Service-Type
  Authenticated-User-Idle-Timeout
  Authorization-Required
  Authorization-Type
 :
 :
  X509-Cert-Data
ciscoasa(config-ldap-attribute-map)#
```

LDAP サーバ グループの設定

LDAP サーバ グループを作成して設定し、LDAP サーバをそのグループに追加するには、次の手順を実行します。

始める前に

LDAP サーバを LDAP サーバ グループに追加する前に、属性マップを追加する必要があります。

手順

ステップ 1 サーバ グループ名とプロトコルを指定します。

aaa-server *server_tag* **protocol ldap**

例：

```
ciscoasa(config)# aaa-server servergroup1 protocol ldap
ciscoasa(config-aaa-server-group)#
```

aaa-server protocol コマンドを入力する場合は、コンフィギュレーション モードを開始します。

ステップ 2 次のサーバを試す前にグループ内の LDAP サーバでの AAA トランザクションの失敗の最大数を指定します。

max-failed-attempts *number*

例：

```
ciscoasa(config-aaa-server-group)# max-failed-attempts 2
```

number 引数の範囲は 1 ～ 5 です。デフォルトは 3 です。

ローカルデータベースを使用してフォールバック方式を設定し（管理アクセスだけの場合）、グループ内のすべてのサーバが応答できなかった場合、グループは非応答と見なされ、フォールバック方式が試行されます。サーバ グループで、追加の AAA 要求によるアクセスがない、非応答と見なされる時間が 10 分間（デフォルト）続くと、ただちにフォールバック方式が使用されます。非応答時間をデフォルトから変更するには、次のステップの **reactivation-mode** コマンドを参照してください。

フォールバック方式として設定されていない場合、ASA は引き続きグループ内のサーバにアクセスしようとします。

ステップ 3 グループ内で障害の発生したサーバを再度アクティブ化する方法（再アクティブ化ポリシー）を指定します。

reactivation-mode {**depletion** [**deadtime** *minutes*] | **timed**}

例：

```
ciscoasa(config-aaa-server-group)# reactivation-mode deadtime 20
```

depletion キーワードを指定すると、グループ内のすべてのサーバが非アクティブになった後に、障害の発生したサーバが再度アクティブ化されます。

deadtime *minutes* キーワード引数のペアには、グループ内の最後のサーバをディセーブルにしてから、次にすべてのサーバを再度イネーブルにするまでの経過時間を分単位で 0 ～ 1440 から指定します。デフォルトは 10 分です。

timed キーワードは、30 秒間のダウンタイムの後に障害が発生したサーバを再度アクティブ化します。

ステップ 4 LDAP サーバと、そのサーバが属する AAA サーバ グループを識別します。

aaa-server *server_group* [**(***interface_name***)**] **host** *server_ip*

例：

```
ciscoasa(config)# aaa-server servergroup1 outside host 10.10.1.1
```

(*interface_name***)** を指定していない場合、ASA はデフォルトで**内部**インターフェイスを使用します。

aaa-server host コマンドを入力すると、aaa-server ホスト コンフィギュレーション モードが開始します。必要に応じて、ホスト コンフィギュレーション モード コマンドを使用して、さらに AAA サーバを設定します。

LDAP サーバで使用できるコマンドと、新しい LDAP サーバ定義にそのコマンドのデフォルト値があるかどうかを、次の表に示します。デフォルト値が指定されていない場合（「—」で表示）、コマンドを使用して値を指定します。

表 *40 :* ホスト モード コマンドとデフォルト値

コマンド	デフォルト値	説明
ldap-attribute-map	—	—
ldap-base-dn	—	—
ldap-login-dn	—	—
ldap-login-password	—	—
ldap-naming-attribute	—	—
ldap-over-ssl	636	設定されていない場合は、ASA では LDAP 要求に sAMAccountName を使用します。SASL とプレーン テキストのどちらを使用する場合でも、ASA と LDAP サーバの間での通信のセキュリティは SSL で確保されます。SASL を設定しない場合、SSL で LDAP 通信を保護することを強くお勧めします。
ldap-scope	—	—
sasl-mechanism	—	—
server-port	389	—

コマンド	デフォルト値	説明
server-type	自動検出	自動検出により LDAP サーバのタイプが特定できなくても、そのサーバが、Microsoft Active Directory、Sun LDAP ディレクトリ サーバ、それ以外の LDAP サーバのいずれであるかがわかっている場合は、そのサーバタイプを手動で設定できます。
timeout	10 秒	—

例

次の例では、watchdogs という名前の LDAP サーバ グループを設定し、そのグループに LDAP サーバを追加する方法を示します。この例では、この例ではリトライ インターバルや LDAP サーバがリスンするポートを定義しないため、ASA はこの 2 つのサーバ固有パラメータにデフォルト値を使用します。

```
ciscoasa(config)# aaa-server watchdogs protocol ldap
ciscoasa(config-aaa-server-group)# aaa-server watchdogs host 192.168.3.4
ciscoasa(config-aaa-server-host)# exit
ciscoasa(config)#
```

VPN の LDAP 認証の設定

VPN アクセスのための LDAP ユーザ認証が成功すると、ASA は、LDAP 属性を返す LDAP サーバのクエリーを実行します。通常これらの属性には、VPN セッションに適用される認可データが含まれます。このように LDAP を使用すると、1 つのステップで認証および認可を完了できます。

ただし、場合によっては、認可メカニズムとは別の異なる認可を LDAP ディレクトリ サーバから取得する必要があります。たとえば、認証に SDI または証明書サーバを使用している場合、認可情報は返されません。この場合、ユーザ認可では、認証の成功後に LDAP ディレクトリのクエリーを実行するため、認証と認可は 2 つのステップで行われます。

LDAP を使用した VPN ユーザ許可を設定するには、次の手順を実行します。

手順

ステップ 1 remotegrp という名前の IPsec リモート アクセス トンネル グループを作成します。

tunnel-group *groupname*

例：

```
ciscoasa(config)# tunnel-group remotegrp
```

ステップ 2 サーバ グループとトンネル グループを関連付けます。

tunnel-group *groupname* **general-attributes**

例：

```
ciscoasa(config)# tunnel-group remotegrp general-attributes
```

ステップ 3 以前作成した認証のための AAA サーバ グループに新しいトンネル グループを割り当てます。

authorization-server-group *group-tag*

例：

```
ciscoasa(config-general)# authorization-server-group ldap_dir_1
```

例

特定の要件で使用できる許可関連のコマンドとオプションは他にもありますが、次の例では、LDAP でのユーザ許可をイネーブルにするコマンドを示します。この例では、remote-1 という名前の IPsec リモート アクセス トンネル グループを作成し、すでに作成してある許可用の ldap_dir_1 AAA サーバ グループにその新しいトンネル グループを割り当てています。

```
ciscoasa(config)# tunnel-group remote-1 type ipsec-ra
ciscoasa(config)# tunnel-group remote-1 general-attributes
ciscoasa(config-general)# authorization-server-group ldap_dir_1
ciscoasa(config-general)#
```

この設定が完了したら、次のコマンドを入力して、ディレクトリ パスワード、ディレクトリ検索の開始点、ディレクトリ検索の範囲など、追加の LDAP 許可パラメータを設定できます。

```
ciscoasa(config)# aaa-server ldap_dir_1 protocol ldap
ciscoasa(config-aaa-server-group)# aaa-server ldap_dir_1 host 10.1.1.4
ciscoasa(config-aaa-server-host)# ldap-login-dn obscurepassword
ciscoasa(config-aaa-server-host)# ldap-base-dn starthere
ciscoasa(config-aaa-server-host)# ldap-scope subtree
ciscoasa(config-aaa-server-host)#
```

AAA の LDAP サーバのモニタリング

AAA の LDAP サーバのモニタリングについては、次のコマンドを参照してください。

- **show aaa-server**

  このコマンドは、設定されたAAAサーバの統計情報を表示します。AAAサーバコンフィギュレーションをクリアするには、**clear aaa-server statistics** コマンドを入力します。

- **show running-config aaa-server**

  このコマンドは、AAA サーバの実行コンフィギュレーションを表示します。AAA サーバの統計情報をクリアするには、**clear configure aaa-server** コマンドを使用します。

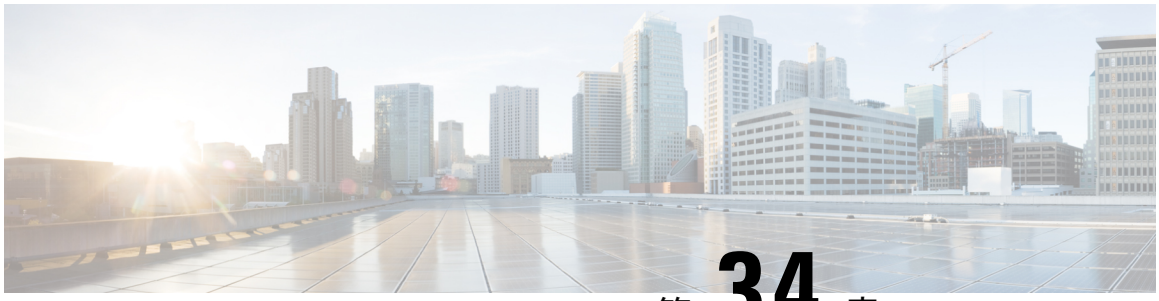
AAA の LDAP サーバの履歴

表 *41 : AAA* サーバの履歴

機能名	プラットフォーム リリース	説明
AAA の LDAP サーバ	7.0(1)	LDAP サーバの AAA のサポートと LDAP サーバの設定方法について説明します。 次のコマンドを導入しました。 **username**、**aaa authorization exec authentication-server**、**aaa authentication console LOCAL**、**aaa authorization exec LOCAL**、**service-type**、**ldap attribute-map**、**aaa-server protocol**、**aaa authentication telnet | ssh | serial} console LOCAL**、**aaa authentication http console LOCAL**、**aaa authentication enable console LOCAL**、**max-failed-attempts**、**reactivation-mode**、**accounting-mode simultaneous**、**aaa-server host**、**authorization-server-group**、**tunnel-group**、**tunnel-group general-attributes**、**map-name**、**map-value**、**ldap-attribute-map**。

第 VII 部

システム管理



第 34 章

管理アクセス

この章では、Telnet、SSH、および HTTPS（ASDM を使用）経由でシステム管理を行うために Cisco ASA にアクセスする方法と、ユーザを認証および許可する方法、ログイン バナーを作成する方法について説明します。

管理リモート アクセスの設定

ここでは、ASDM 用の ASA アクセス、Telnet または SSH、およびログイン バナーなどのその他のパラメータの設定方法について説明します。

SSH アクセスの設定

クライアント IP アドレスを指定して、ASA に SSH を使用して接続できるユーザを定義するには、次の手順を実行します。次のガイドラインを参照してください。

- また、ASA インターフェイスに SSH アクセスの目的でアクセスするために、ホスト IP アドレスを許可するアクセス ルールは必要ありません。このセクションの手順に従って、SSH アクセスを設定する必要があるだけです。
- ASA への通過ルートとなるインターフェイス以外のインターフェイスへの SSH アクセスはサポートされません。たとえば、SSH ホストが外部インターフェイスにある場合、外部インターフェイスへの直接管理接続のみ開始できます。このルールの例外は、VPN 接続を介した場合のみです。VPN トンネルを介した管理アクセスの設定 （967 ページ）を参照してください。
- ASA は、コンテキスト/単一のモードあたり最大 5 つの同時 SSH 接続と、すべてのコンテキストにまたがり分散された最大 100 の接続を許容します。

- （8.4 以降）SSH デフォルト ユーザ名はサポートされなくなりました。**pix** または **asa** ユーザ名とログイン パスワードで SSH を使用して ASA に接続することができなくなりました。SSH を使用するには、**aaa authentication ssh console LOCAL** コマンドを使用して AAA 認証を設定してから、**username** コマンドを入力してローカル ユーザを定義します。ローカル データベースの代わりに AAA サーバを認証に使用する場合、ローカル認証もバックアップの手段として設定しておくことをお勧めします。

始める前に

- マルチ コンテキスト モードでは、コンテキスト実行スペースで次の手順を実行します。システムからコンテキスト コンフィギュレーションに変更するには、**changeto context** *name* を入力します。

手順

ステップ 1 SSH に必要な RSA キー ペアを生成します（物理 ASA の場合のみ）。

crypto key generate rsa modulus *modulus_size*

例：

```
ciscoasa(config)# crypto key generate rsa modulus 2048
```

ASAv の場合、RSA キー ペアは導入後に自動的に作成されます。

係数の値（ビット単位）は 512、768、1024、2048、または 4096 です。指定するキー係数のサイズが大きいほど、RSA キー ペアの生成にかかる時間は長くなります。2048 文字以上の値を推奨します。

ステップ 2 RSA キーを永続的なフラッシュ メモリに保存します。

write memory

例：

```
ciscoasa(config)# write memory
```

ステップ 3 SSH アクセスに使用できるユーザをローカル データベースに作成します。ユーザ アクセスに AAA サーバを使用することもできますが、ローカル ユーザ名の使用を推奨します。

username *name* **password** *password* **privilege** *level*

例：

```
ciscoasa(config)# username admin password Far$cape1999 privilege 15
```

デフォルトの特権レベルは 2 です。0 ～ 15 の範囲でレベルを入力します。15 を指定すると、すべての特権を使用できます。**注**：ユーザ名とパスワードを作成しなければならないという事態を回避するため、**username** コマンド **nopassword** オプションは使用しないようにしてくださ

い。**nopassword** オプションでは、任意のパスワードを入力できますが、パスワードなしは不可能です。ユーザにパスワードを割り当てたが、ユーザが公開キー認証のみを使用するように制限するには、この手順に従ってパスワードの使用に対する AAA 認証を有効にしないでください。

ステップ 4 （任意）パスワード認証ではなく公開キー認証のみ、またはこれら両方の認証をユーザに許可し、ASA で公開キーを入力します。

username *name* **attributes**

ssh authentication {**pkf** | **publickey** *key*}

例：

```
ciscoasa(config)# username admin attributes
ciscoasa(config-username)# ssh authentication pkf

Enter an SSH public key formatted file.
End with the word "quit" on a line by itself:
---- BEGIN SSH2 PUBLIC KEY ----
Comment: "4096-bit RSA, converted by xxx@xxx from OpenSSH"
AAAAB3NzaC1yc2EAAAADAQABAAACAQDNUvkgza37lB/Q/fljpLAv1BbyAd5PJCJXh/U4LO
hleR/qgIROjpnFaS7Az8/+sjHmq0qXC5TXkzWihvRZbhefyPhPHCi0hIt4oUF2ZbXESA/8
jUT4ehXIUE7FrChffBBtbD4d9FkV8A2gwZCDJBxEM26ocbZCSTx9QC//wt6E/zRcdoqiJG
p4ECEdDaM+56l+yf73NUigO7wYkqcrzjmI1rZRDLVcqtj8Q9qD3MqsV+PkJGSGiqZwnyIl
QbfYxXHU9wLdWxhUbA/xOjJuZ15TQMa7KLs2u+RtrpQgeTGTffIh6O+xKh93gwTgzaZTK4
CQ1kuMrRdNRzza0byLeYPtSlv6Lv6F6dGtwlqrX5a+w/tV/aw9WUg/rapekKloz3tsPTDe
p866AFzU+Z7pVR1389iNuNJHQS7IUA2m0cciIuCM2we/tVqMPYJl+xgKAkuHDkBlMS4i8b
Wzyd+4EUMDGGZVeO+corKTLWFO1wIUieRkrUaCzjComGYZdzrQT2mXBcSKQNWlSCBpCHsk
/r5uTGnKpCNWfL7vd/sRCHyHKsxjsXR15C/5zgHmCTAaGOuIq0Rjo34+61+70PCtYXebxM
Wwm19e3eH2PudZd+rj1dedfr2/IrislEBRJWGLoR/N+xsvwVVM1Qqw1uL4r99CbZF9NghY
NRxCQOY/7K77II==
---- END SSH2 PUBLIC KEY ----
quit
INFO: Import of an SSH public key formatted file SUCCEEDED.
```

ローカル **username** の場合、パスワード認証ではなく公開キー認証のみ、またはこれら両方の認証を有効にできます。SSH-RSA raw キー（証明書なし）を生成可能な任意の SSH キー生成ソフトウェア（ssh keygen など）を使用して、公開キー/秘密キーのペアを生成できます。ASA で公開キーを入力します。その後、SSH クライアントは秘密キー（およびキー ペアを作成するために使用したパスフレーズ）を使用して ASA に接続します。

pkf キーの場合、PKF でフォーマットされたキーを最大 4096 ビット貼り付けるよう求められます。Base64 形式では大きすぎてインラインで貼り付けることができないキーにはこのフォーマットを使用します。たとえば、ssh keygen を使って 4096 ビットのキーを生成してから PKF に変換し、そのキーに対して **pkf** キーワードが求められるようにすることができます。**注**：フェールオーバーで **pkf** オプションを使用することはできますが、PKF キーは、スタンバイ システムに自動的に複製されません。PKF キーを同期するには、**write standby** コマンドを入力する必要があります。

publickey キーの場合、これは Base64 でエンコードされた公開キーのことです。SSH-RSA raw キー（証明書なし）を生成可能な任意の SSH キー生成ソフトウェア（ssh keygen など）を使用して、キーを生成できます。

ステップ 5 （パスワードアクセスの場合）SSH アクセスのためにローカル（または AAA サーバ）認証を有効にします。

aaa authentication ssh console {**LOCAL** | *server_group* [**LOCAL**]}

例：

```
ciscoasa(config)# aaa authentication ssh console LOCAL
```

このコマンドは、**ssh authentication** コマンドでのユーザ名のローカル公開キー認証には影響しません。ASA では、公開キー認証に対し、ローカル データベースを暗黙的に使用します。このコマンドは、ユーザ名とパスワードにのみ影響します。ローカルユーザが公開キー認証またはパスワードを使用できるようにするには、パスワードアクセスを有効にするため、このコマンドで明示的にローカル認証を設定する必要があります。

ステップ 6 ASA がアドレスまたはサブネットごとに接続を受け入れる IP アドレスと、SSH を使用可能なインターフェイスを特定します。

ssh *source_IP_address mask source_interface*

- *source_interface*：名前付きインターフェイスを指定します。ブリッジグループの場合、ブリッジ グループ メンバ インターフェイスを指定します。

Telnet と異なり、SSH は最も低いセキュリティ レベルのインターフェイスで実行できます。

例：

```
ciscoasa(config)# ssh 192.168.3.0 255.255.255.0 inside
```

ステップ 7 （任意） ASA がセッションを切断するまでに SSH がアイドル状態を維持する時間の長さを設定します。

ssh timeout *minutes*

例：

```
ciscoasa(config)# ssh timeout 30
```

タイムアウトは 1 ～ 60 分に設定します。デフォルトは 5 分です。デフォルトの期間では一般に短すぎるので、実働前のテストとトラブルシューティングがすべて完了するまでは、長めに設定しておいてください。

ステップ 8 （任意） SSH バージョン 1 または 2 へのアクセスを制限します。デフォルトでは、SSH はバージョン 1 と 2 の両方を許可します。

ssh version *version_number*

例：

```
ciscoasa(config)# ssh version 2
```

ステップ 9 （任意） Diffie-Hellman（DH）キー交換モードを設定します。

ssh key-exchange group {**dh-group1-sha1** | **dh-group14-sha1**}

例：

```
ciscoasa(config)# ssh key-exchange group dh-group14-sha1
```

デフォルトは **dh-group1-sha1**

DH キー交換では、いずれの当事者も単独では決定できない共有秘密を使用します。キー交換を署名およびホストキーと組み合わせることで、ホスト認証が実現します。このキー交換方式により、明示的なサーバ認証が可能となります。DH キー交換の使用方法の詳細については、RFC 4253 を参照してください。

例

次に、PKF 形式のキーを使用して認証する例を示します。

```
ciscoasa(config)# crypto key generate rsa modulus 4096
ciscoasa(config)# write memory
ciscoasa(config)# username exampleuser1 password examplepassword1 privilege 15
ciscoasa(config)# username exampleuser1 attributes
ciscoasa(config-username)# ssh authentication pkf
Enter an SSH public key formatted file.
End with the word "quit" on a line by itself:
---- BEGIN SSH2 PUBLIC KEY ----
Comment: "4096-bit RSA, converted by xxx@xxx from OpenSSH"
AAAAB3NzaC1yc2EAAAADAQABAAACAQDNUvkgza37lB/Q/fljpLAv1BbyAd5PJCJXh/U4LO
hleR/qgIROjpnFaS7Az8/+sjHmq0qXC5TXkzWihvRZbhefyPhPHCi0hIt4oUF2ZbXESA/8
jUT4ehXIUE7FrChffBBtbD4d9FkV8A2gwZCDJBxEM26ocbZCSTx9QC//wt6E/zRcdoqiJG
p4ECEdDaM+56l+yf73NUigO7wYkqcrzjmI1rZRDLVcqtj8Q9qD3MqsV+PkJGSGiqZwnyIl
QbfYxXHU9wLdWxhUbA/xOjJuZ15TQMa7KLs2u+RtrpQgeTGTffIh6O+xKh93gwTgzaZTK4
CQ1kuMrRdNRzza0byLeYPtSlv6Lv6F6dGtwlqrX5a+w/tV/aw9WUg/rapekKloz3tsPTDe
p866AFzU+Z7pVR1389iNuNJHQS7IUA2m0cciIuCM2we/tVqMPYJl+xgKAkuHDkBlMS4i8b
Wzyd+4EUMDGGZVeO+corKTLWFO1wIUieRkrUaCzjComGYZdzrQT2mXBcSKQNWlSCBpCHsk
/r5uTGnKpCNWfL7vd/sRCHyHKsxjsXR15C/5zgHmCTAaGOuIq0Rjo34+61+70PCtYXebxM
Wwm19e3eH2PudZd+rj1dedfr2/IrislEBRJWGLoR/N+xsvwVVM1Qqw1uL4r99CbZF9NghY
NRxCQOY/7K77II==
---- END SSH2 PUBLIC KEY ----
quit
INFO: Import of an SSH public key formatted file SUCCEEDED.
ciscoasa(config)# ssh 192.168.1.2 255.255.255.255 inside
```

次の例では、Linux または Macintosh システムの SSH の共有キーを生成して、ASA にインポートします。

1. コンピュータで 4096 ビットの ssh-rsa 公開キーおよび秘密キーを生成します。

```
jcrichton-mac:~ john$ ssh-keygen -b 4096
Generating public/private rsa key pair.
Enter file in which to save the key (/Users/john/.ssh/id_rsa):
/Users/john/.ssh/id_rsa already exists.
Overwrite (y/n)? y
Enter passphrase (empty for no passphrase): pa$$phrase
Enter same passphrase again: pa$$phrase
```

```
Your identification has been saved in /Users/john/.ssh/id_rsa.
Your public key has been saved in /Users/john/.ssh/id_rsa.pub.
The key fingerprint is:
c0:0a:a2:3c:99:fc:00:62:f1:ee:fa:f8:ef:70:c1:f9 john@jcrichton-mac
The key's randomart image is:
+--[ RSA 4096]----+
| .               |
|  o  .           |
|+...  o          |
|B.+.....         |
|.B ..+  S        |
|  =   o          |
|   + . E         |
|  o o            |
| ooooo           |
+-----------------+
```

2. PKF 形式にキーを変換します。

```
jcrichton-mac:~ john$ cd .ssh
jcrichton-mac:.ssh john$ ssh-keygen -e -f id_rsa.pub
---- BEGIN SSH2 PUBLIC KEY ----
Comment: "4096-bit RSA, converted by ramona@rboersma-mac from OpenSSH"
AAAAB3NzaC1yc2EAAAADAQABAAACAQDNUvkgza37lB/Q/fljpLAv1BbyAd5PJCJXh/U4LO
hleR/qgIROjpnDaS7Az8/+sjHmq0qXC5TXkzWihvRZbhefyPhPHCi0hIt4oUF2ZbXESA/8
jUT4ehXIUE7FrChffBBtbD4d9FkV8A2gwZCDJBxEM26ocbZCSTx9QC//wt6E/zRcdoqiJG
p4ECEdDaM+56l+yf73NUigO7wYkqcrzjmI1rZRDLVcqtj8Q9qD3MqsV+PkJGSGiqZwnyIl
QbfYxXHU9wLdWxhUbA/xOjJuZ15TQMa7KLs2u+RtrpQgeTGTffIh6O+xKh93gwTgzaZTK4
CQ1kuMrRdNRzza0byLeYPtSlv6Lv6F6dGtwlqrX5a+w/tV/aw9WUg/rapekKloz3tsPTDe
p866AFzU+Z7pVR1389iNuNJHQS7IUA2m0cciIuCM2we/tVqMPYJl+xgKAkuHDkBlMS4i8b
Wzyd+4EUMDGGZVeO+corKTLWFO1wIUieRkrUaCzjComGYZdzrQT2mXBcSKQNWlSCBpCHsk
/r5uTGnKpCNWfL7vd/sRCHyHKsxjsXR15C/5zgHmCTAaGOuIq0Rjo34+61+70PCtYXebxM
Wwm19e3eH2PudZd+rj1dedfr2/IrislEBRJWGLoR/N+xsvwVVM1Qqw1uL4r99CbZF9NghY
NRxCQOY/7K77IQ==
---- END SSH2 PUBLIC KEY ----
jcrichton-mac:.ssh john$
```

3. キーをクリップボードにコピーします。
4. ASA CLI に接続し、公開キーをユーザ名に追加します。

```
ciscoasa(config)# username test attributes
ciscoasa(config-username)# ssh authentication pkf
Enter an SSH public key formatted file.
End with the word "quit" on a line by itself:
---- BEGIN SSH2 PUBLIC KEY ----
Comment: "4096-bit RSA, converted by ramona@rboersma-mac from OpenSSH"
AAAAB3NzaC1yc2EAAAADAQABAAACAQDNUvkgza37lB/Q/fljpLAv1BbyAd5PJCJXh/U4LO
hleR/qgIROjpnDaS7Az8/+sjHmq0qXC5TXkzWihvRZbhefyPhPHCi0hIt4oUF2ZbXESA/8
jUT4ehXIUE7FrChffBBtbD4d9FkV8A2gwZCDJBxEM26ocbZCSTx9QC//wt6E/zRcdoqiJG
p4ECEdDaM+56l+yf73NUigO7wYkqcrzjmI1rZRDLVcqtj8Q9qD3MqsV+PkJGSGiqZwnyIl
QbfYxXHU9wLdWxhUbA/xOjJuZ15TQMa7KLs2u+RtrpQgeTGTffIh6O+xKh93gwTgzaZTK4
CQ1kuMrRdNRzza0byLeYPtSlv6Lv6F6dGtwlqrX5a+w/tV/aw9WUg/rapekKloz3tsPTDe
p866AFzU+Z7pVR1389iNuNJHQS7IUA2m0cciIuCM2we/tVqMPYJl+xgKAkuHDkBlMS4i8b
Wzyd+4EUMDGGZVeO+corKTLWFO1wIUieRkrUaCzjComGYZdzrQT2mXBcSKQNWlSCBpCHsk
/r5uTGnKpCNWfL7vd/sRCHyHKsxjsXR15C/5zgHmCTAaGOuIq0Rjo34+61+70PCtYXebxM
Wwm19e3eH2PudZd+rj1dedfr2/IrislEBRJWGLoR/N+xsvwVVM1Qqw1uL4r99CbZF9NghY
NRxCQOY/7K77IQ==
---- END SSH2 PUBLIC KEY ----
quit
```

```
INFO: Import of an SSH public key formatted file completed successfully.
```

5. ユーザが ASA に SSH できることを確認（テスト）します。

```
jcrichton-mac:.ssh john$ ssh test@10.86.118.5
The authenticity of host '10.86.118.5 (10.86.118.5)' can't be established.
RSA key fingerprint is 39:ca:ed:a8:75:5b:cc:8e:e2:1d:96:2b:93:b5:69:94.
Are you sure you want to continue connecting (yes/no)? yes
```

次のダイアログボックスが、パスフレーズを入力するために表示されます。

一方、端末セッションでは、以下が表示されます。

```
Warning: Permanently added '10.86.118.5' (RSA) to the list of known hosts.
Identity added: /Users/john/.ssh/id_rsa (/Users/john/.ssh/id_rsa)
Type help or '?' for a list of available commands.
asa>
```

Telnet アクセスの設定

Telnet を使用して ASA にアクセス可能なクライアント IP アドレスを指定するには、次の手順を実行します。次のガイドラインを参照してください。

- また、ASA インターフェイスに Telnet アクセスの目的でアクセスするために、ホスト IP アドレスを許可するアクセスルールは必要ありません。このセクションの手順に従って、Telnet アクセスを設定する必要があるだけです。
- ASA への通過ルートとなるインターフェイス以外のインターフェイスへの Telnet アクセスはサポートされません。たとえば、Telnet ホストが外部インターフェイスにある場合、外部インターフェイスへの直接 Telnet 接続のみ開始できます。このルールの例外は、VPN 接続を介した場合のみです。VPN トンネルを介した管理アクセスの設定（967 ページ）を参照してください。
- VPN トンネル内で Telnet を使用する場合を除き、最も低いセキュリティ インターフェイスに対して Telnet は使用できません。

- ASA は、コンテキスト/単一のモードあたり最大 5 つの同時 Telnet 接続と、すべてのコンテキストにまたがり分散された最大 100 の接続を許容します。

始める前に

- マルチ コンテキスト モードでは、コンテキスト実行スペースで次の手順を実行します。システムからコンテキスト コンフィギュレーションに変更するには、**changeto context** *name* を入力します。
- Telnet を使用して ASA CLI にアクセスするには、**password** コマンドで設定したログイン パスワードを入力します。Telnet を使用する前に手動でパスワードを設定する必要があります。

手順

ステップ 1 ASA が指定したインターフェイスのアドレスまたはサブネットごとに接続を受け入れる IP アドレスを特定します。

telnet *source_IP_address mask source_interface*

- *source_interface*：名前付きインターフェイスを指定します。ブリッジ グループの場合、ブリッジ グループ メンバ インターフェイスを指定します。

インターフェイスが 1 つしかない場合は、インターフェイスのセキュリティ レベルが 100 である限り、そのインターフェイスにアクセスするように Telnet を設定することができます。

例：

```
ciscoasa(config)# telnet 192.168.1.2 255.255.255.255 inside
```

ステップ 2 ASA がセッションを切断するまで Telnet セッションがアイドル状態を維持する時間の長さを設定します。

telnet timeout *minutes*

例：

```
ciscoasa(config)#  telnet timeout 30
```

タイムアウトは 1 ～ 1440 分に設定します。デフォルトは 5 分です。デフォルトの期間では一般に短すぎるので、実働前のテストとトラブルシューティングがすべて完了するまでは、長めに設定しておいてください。

例

次の例は、アドレスが 192.168.1.2 の内部インターフェイスのホストで ASA にアクセスする方法を示しています。

```
ciscoasa(config)# telnet 192.168.1.2 255.255.255.255 inside
```

次の例は、192.168.3.0 のネットワーク上のすべてのユーザが内部インターフェイス上の ASA にアクセスできるようにする方法を示しています。

```
ciscoasa(config)# telnet 192.168.3.0. 255.255.255.255 inside
```

ASDM、その他のクライアントの HTTPS アクセスの設定

ASDM または CSM などの他の HTTPS クライアントを使用するには、HTTPS サーバを有効にし、ASA への HTTPS 接続を許可する必要があります。HTTPS アクセスは工場出荷時のデフォルト設定の一部として有効化されています。HTTPS アクセスを設定するには、次のステップを実行します。次のガイドラインを参照してください。

- また、ASA インターフェイスに HTTPS アクセスの目的でアクセスするために、ホスト IP アドレスを許可するアクセス ルールは必要ありません。このセクションの手順に従って、HTTPS アクセスを設定する必要があるだけです。ただし、HTTP リダイレクトを設定して HTTP 接続を HTTPS に自動的にリダイレクトするには、HTTP を許可するアクセス ルールを有効化する必要があります。そうしないと、インターフェイスが HTTP ポートをリッスンできません。
- ASA への通過ルートとなるインターフェイス以外のインターフェイスへの管理アクセスはサポートされません。たとえば、管理ホストが外部インターフェイスにある場合、外部インターフェイスへの直接管理接続のみ開始できます。このルールの例外は、VPN 接続を介した場合のみです。VPN トンネルを介した管理アクセスの設定（967 ページ）を参照してください。
- ASA では、コンテキストごとに最大 5 つの同時 ASDM インスタンスを使用でき、全コンテキスト間で最大 32 の ASDM インスタンスの使用が可能です。

  ASDM セッションでは、2 つの HTTPS 接続が使用されます。一方は常に存在するモニタ用で、もう一方は変更を行ったときにだけ存在する設定変更用です。たとえば、ASDM セッションのシステム制限が 32 の場合、HTTPS セッション数は 64 に制限されます。

始める前に

- マルチ コンテキスト モードでは、コンテキスト実行スペースで次の手順を実行します。システムからコンテキスト コンフィギュレーションに変更するには、**changeto context** *name* を入力します。

手順

ステップ 1 ASA が指定したインターフェイスのアドレスまたはサブネットごとに HTTPS 接続を受け入れる IP アドレスを特定します。

http *source_IP_address mask source_interface*

- *source_interface*：名前付きインターフェイスを指定します。ブリッジグループの場合、ブリッジ グループ メンバ インターフェイスを指定します。

例：

```
ciscoasa(config)# http 192.168.1.2 255.255.255.255 inside
```

ステップ 2 HTTPS サーバをイネーブルにします。

http server enable [*port*]

例：

```
ciscoasa(config)# http server enable 444
```

デフォルトでは、port は 443 です。ポート番号を変更する場合は、必ず ASDM アクセス URL に変更したポート番号を含めてください。たとえば、ポート番号を 444 に変更する場合は、次の URL を入力します。

https://10.1.1.1:444

例

次の例は、HTTPS サーバを有効化し、アドレスが 192.168.1.2 の内部インターフェイス上のホストで ASDM にアクセスする方法を示しています。

```
ciscoasa(config)# http server enable
ciscoasa(config)# http 192.168.1.2 255.255.255.255 inside
```

次の例は、192.168.3.0/24 のネットワーク上のすべてのユーザが内部インターフェイス上の ASDM にアクセスできるようにする方法を示しています。

```
ciscoasa(config)# http 192.168.3.0 255.255.255.0 inside
```

ASDM アクセスまたはクライアントレス SSL VPN のための HTTP リダイレクトの設定

ASDM またはクライアントレス SSL VPN を使用して ASA に接続するには、HTTPS を使用する必要があります。利便性のために、HTTP 管理接続を HTTPS にリダイレクトすることができます。たとえば、HTTP をリダイレクトすることによって、**http://10.1.8.4/admin/** または **https://10.1.8.4/admin/** と入力し、ASDM 起動ページで HTTPS アドレスにアクセスできます。

この機能は、IPv4 のリダイレクションのみをサポートします。

始める前に

通常、ホスト IP アドレスを許可するアクセス ルールは必要ありません。ただし、HTTP リダイレクトのためには、HTTP を許可するアクセス ルールを有効化する必要があります。そうしないと、インターフェイスが HTTP ポートをリッスンできません。

手順

Enable HTTP redirect:

http redirect *interface_name* [*port*]

例：

```
ciscoasa(config)# http redirect outside 88
```

port は、インターフェイスが HTTP 接続のリダイレクトに使用するポートを指定します。デフォルトは 80 です。

VPN トンネルを介した管理アクセスの設定

あるインターフェイスで VPN トンネルが終端している場合、別のインターフェイスにアクセスして ASA を管理するには、そのインターフェイスを管理アクセス インターフェイスとして指定する必要があります。たとえば、outside インターフェイスから ASA に入る場合は、この機能を使用して、ASDM、SSH、Telnet、または SNMP 経由で Inside インターフェイスに接続するか、outside インターフェイスから入るときに Inside インターフェイスに ping を実行できます。

ASA への通過ルートとなるインターフェイス以外のインターフェイスへの VPN アクセスはサポートされません。たとえば、VPN アクセスが外部インターフェイスにある場合、外部インターフェイスへの直接接続のみ開始できます。複数のアドレスを覚える必要がないように、ASA の直接アクセス可能インターフェイスの VPN を有効にし、名前解決を使用してください。

管理アクセスは、IPsec クライアント、IPsec サイト間、AnyConnect SSL VPN クライアントの VPN トンネル タイプ経由で行えます。

手順

別のインターフェイスから ASA に入るときにアクセスする管理インターフェイスの名前を指定します。

management-access *management_interface*

ブリッジ グループ インターフェイスはサポートされません。

例：

```
ciscoasa(config)# management-access inside
```

コンソール タイムアウトの変更

コンソール タイムアウトでは、接続を特権 EXEC モードまたはコンフィギュレーション モードにしておくことができる時間を設定します。タイムアウトに達すると、セッションはユーザ EXEC モードになります。デフォルトでは、セッションはタイムアウトしません。この設定は、コンソール ポートへの接続を保持できる時間には影響しません。接続がタイムアウトすることはありません。

手順

特権セッションが終了するまでのアイドル時間を分単位（0 ～ 60）で指定します。

console timeout *number*

例：

```
ciscoasa(config)# console timeout 0
```

デフォルトのタイムアウトは 0 であり、セッションがタイムアウトしないことを示します。

CLI プロンプトのカスタマイズ

プロンプトに情報を追加する機能により、複数のモジュールが存在する場合にログインしている ASA を一目で確認することができます。この機能は、フェールオーバー時に、両方の ASA に同じホスト名が設定されている場合に便利です。

マルチ コンテキスト モードでは、システム実行スペースまたは管理コンテキストにログインするときに、拡張プロンプトを表示できます。非管理コンテキスト内では、デフォルトのプロンプト（ホスト名およびコンテキスト名）のみが表示されます。

デフォルトでは、プロンプトにASAのホスト名が表示されます。マルチ コンテキスト モードでは、プロンプトにコンテキスト名も表示されます。CLIプロンプトには、次の項目を表示できます。

cluster-unit	クラスタ ユニット名を表示します。クラスタの各ユニットは一意の名前を持つことができます。
コンテキスト	（マルチ モードのみ）現在のコンテキストの名前を表示します。
domain	ドメイン名を表示します。
hostname	ホスト名を表示します。
priority	フェールオーバー プライオリティを [pri]（プライマリ）または [sec]（セカンダリ）として表示します。

state	ユニットのトラフィック通過状態またはロールを表示します。 フェールオーバーの場合、state キーワードに対して次の値が表示されます。 • [act]：フェールオーバーが有効であり、装置ではトラフィックをアクティブに通過させています。 • [stby]：フェールオーバーはイネーブルです。ユニットはトラフィックを通過させていません。スタンバイ、失敗、または他の非アクティブ状態です。 • [actNoFailover]：フェールオーバーは無効であり、装置ではトラフィックをアクティブに通過させています。 • [stbyNoFailover]：フェールオーバーは無効であり、装置ではトラフィックを通過させていません。これは、スタンバイ ユニットでしきい値を上回るインターフェイス障害が発生したときに生じることがあります。 クラスタリングの場合、state キーワードに対して次の値が表示されます。 • **master** • **slave** たとえば、**prompt hostname cluster-unit state** と設定して「ciscoasa/cl2/slave>」と表示された場合、ホスト名が ciscoasa、ユニット名が cl2、状態名が slave です。

手順

次のコマンドを入力して、CLI プロンプトをカスタマイズします。

prompt {[**hostname**] [**context**] [**domain**] [**slot**] [**state**] [**priority**] [**cluster-unit**]}

例：

```
ciscoasa(config)# prompt hostname context slot state priority
ciscoasa/admin/pri/act(config)#
```

キーワードを入力する順序によって、プロンプト内の要素の順序が決まります。要素はスラッシュ（/）で区切ります。

ログイン バナーの設定

ユーザが ASA に接続するとき、ログインする前、または特権 EXEC モードに入る前に表示されるメッセージを設定できます。

始める前に

- セキュリティの観点から、バナーで不正アクセスを防止することが重要です。「ウェルカム」や「お願いします」などの表現は侵入者を招き入れているような印象を与えるので使用しないでください。以下のバナーでは、不正アクセスに対して正しい表現を設定しています。

```
You have logged in to a secure device.
If you are not authorized to access this device,
log out immediately or risk possible criminal consequences.
```

- バナーが追加された後、次の場合に ASA に対する Telnet または SSH セッションが終了する可能性があります。
  - バナー メッセージを処理するためのシステム メモリが不足している場合。
  - バナー メッセージの表示を試みたときに、TCP 書き込みエラーが発生した場合。
- バナー メッセージのガイドラインについては、RFC 2196 を参照してください。

手順

ユーザが最初に接続したとき（「今日のお知らせ」（motd））、ユーザがログインしたとき（login）、ユーザが特権 EXEC モードにアクセスしたとき（exec）のいずれかに表示するバナーを追加します。

banner {**exec** | **login** | **motd**} *text*

例：

```
ciscoasa(config)# banner motd Welcome to $(hostname).
```

ユーザが ASA に接続すると、まず「今日のお知らせ」バナーが表示され、その後にログインバナーとプロンプトが表示されます。ユーザが ASA に正常にログインすると、exec バナーが表示されます。

複数の行を追加する場合は、各行の前に **banner** コマンドを追加します。

バナー テキストに関する注意事項：

- スペースは使用できますが、CLI を使用してタブを入力することはできません。
- バナーの長さの制限は、RAM およびフラッシュ メモリに関するもの以外はありません。
- ASA のホスト名またはドメイン名は、**$(hostname)** 文字列と **$(domain)** 文字列を組み込むことによって動的に追加できます。
- システム コンフィギュレーションでバナーを設定する場合は、コンテキスト コンフィギュレーションで **$(system)** 文字列を使用することによって、コンテキスト内でそのバナー テキストを使用できます。

例

以下に、「今日のお知らせ」バナーを追加する例を示します。

```
ciscoasa(config)# banner motd Welcome to $(hostname).

ciscoasa(config)# banner motd Contact me at admin@example.com for any issues.
```

管理セッション クォータの設定

ASA で許可する ASDM、SSH、および Telnet の同時最大セッション数を設定できます。この最大値に達すると、それ以降のセッションは許可されず、syslog メッセージが生成されます。システム ロックアウトを回避するために、管理セッション割り当て量のメカニズムではコンソール セッションをブロックできません。

始める前に

マルチ コンテキスト モードでは、システム実行スペースで次の手順を実行します。 コンテキストをシステム コンフィギュレーションに入力し、**changeto system** コマンドを入力します。

手順

ステップ 1 次のコマンドを入力します。

quota management-session *number*

- *number*：0（無制限）～ 10000 のセッションの集約数を設定します。

例：

例：

```
ciscoasa(config)# quota management-session 1000
```

ステップ 2 使用中の現在のセッションを表示します。

show quota management-session

例：

```
ciscoasa(config)# show quota management-session

quota management-session limit 3
quota management-session warning level 2
quota management-session level 0
quota management-session high water 2
quota management-session errors 0
quota management-session warnings 0
```

システム管理者用 AAA の設定

この項では、システム管理者の認証、管理許可、コマンド許可を設定する方法について説明します。

管理認証の設定

CLI および ASDM アクセスの認証を設定します。

管理認証について

ASA へのログイン方法は、認証を有効にしているかどうかによって異なります。

SSH 認証の概要

認証ありまたは認証なしでの SSH アクセスについては、次の動作を参照してください。

- 認証なし：SSH は認証なしでは使用できません。
- 認証あり：SSH 認証を有効にした場合は、AAA サーバまたはローカルユーザデータベースに定義されているユーザ名とパスワードを入力します。公開キーの認証では、ASA はローカル データベースのみをサポートします。 SSH 公開キー認証を設定した場合、ASA ではローカルデータベースを暗黙的に使用します。ログインにユーザ名とパスワードを使用する場合に必要なのは、SSH認証を明示的に設定することのみです。ユーザEXECモードにアクセスします。

Telnet 認証の概要

認証の有無にかかわらず、Telnet アクセスについては、次の動作を参照してください。

- 認証なし：Telnet の認証を有効にしていない場合は、ユーザ名を入力しません。ログインパスワード（**password** コマンドで設定）を入力します。デフォルトのパスワードはありません。したがって、ASA へ Telnet 接続するには、パスワードを設定する必要があります。ユーザ EXEC モードにアクセスします。

- 認証あり：Telnet認証を有効にした場合は、AAAサーバまたはローカルユーザデータベースに定義されているユーザ名とパスワードを入力します。ユーザEXECモードにアクセスします。

ASDM 認証の概要

認証ありまたは認証なしでのASDMアクセスに関しては、次の動作を参照してください。AAA認証の有無にかかわらず、証明書認証を設定することも可能です。

- 認証なし：デフォルトでは、ブランクのユーザ名と **enable password** コマンドによって設定されたイネーブル パスワード（デフォルトではブランク）を使用して ASDM にログインできます。空白のままにしないように、できるだけ早くイネーブルパスワードを変更することをお勧めします。ホスト名、ドメイン名、およびイネーブル パスワードと Telnet パスワードの設定（583 ページ）を参照してください。ログイン画面で（ユーザ名をブランクのままにしないで）ユーザ名とパスワードを入力した場合は、ASDMによってローカル データベースで一致がチェックされることに注意してください。
- 証明書認証（シングル、ルーテッド モードのみ）：ユーザに有効な証明書を要求できます。証明書のユーザ名とパスワードを入力すると、ASA が PKI トラストポイントに対して証明書を検証します。
- AAA 認証：ASDM（HTTPS）認証を有効にした場合は、AAA サーバまたはローカル ユーザ データベースに定義されているユーザ名とパスワードを入力します。これで、ブランクのユーザ名とイネーブル パスワードで ASDM を使用できなくなりました。
- AAA 認証と証明書認証の併用（シングル、ルーテッド モードのみ）：ASDM（HTTPS）認証を有効にした場合は、AAA サーバまたはローカル ユーザ データベースに定義されているユーザ名とパスワードを入力します。証明書認証用のユーザ名とパスワードが異なる場合は、これらも入力するように求められます。ユーザ名を証明書から取得してあらかじめ入力しておくよう選択できます。

シリアル認証の概要

認証ありまたは認証なしでのシリアル コンソール ポートへのアクセスに関しては、次の動作を参照してください。

- 認証なし：シリアルアクセスの認証を有効にしていない場合は、ユーザ名、パスワードを入力しません。ユーザ EXEC モードにアクセスします。
- 認証あり：シリアルアクセスの認証を有効にした場合は、AAAサーバまたはローカルユーザデータベースで定義されているユーザ名とパスワードを入力します。ユーザEXECモードにアクセスします。

enable 認証の概要

ログイン後に特権EXECモードに入るには、**enable**コマンドを入力します。このコマンドの動作は、認証がイネーブルかどうかによって異なります。

- 認証なし：enable 認証を設定していない場合は、**enable** コマンドを入力するときにシステム イネーブル パスワード（**enable password** コマンドで設定）を入力します。デフォルトは空白です。ただし、enable 認証を使用しない場合、**enable** コマンドを入力した後は、特定のユーザとしてログインしていません。これにより、コマンド認可などユーザベースの各機能が影響を受けることがあります。ユーザ名を維持するには、enable 認証を使用してください。
- 認証あり：enable 認証を設定した場合は、ASA はプロンプトにより AAA サーバまたはローカル ユーザ データベースで定義されているユーザ名とパスワードを要求します。この機能は、ユーザが入力できるコマンドを判別するためにユーザ名が重要な役割を果たすコマンド許可を実行する場合に特に役立ちます。

ローカル データベースを使用する enable 認証の場合は、**enable** コマンドの代わりに **login** コマンドを使用できます。**login** コマンドによりユーザ名が維持されますが、認証をオンにするための設定は必要ありません。

⚠

注意 CLI にアクセスできるユーザや特権 EXEC モードを開始できないようにするユーザをローカル データベースに追加する場合は、コマンド認可を設定する必要があります。コマンド認可がない場合、特権レベルが 2 以上（2 がデフォルト）のユーザは、CLI で自分のパスワードを使用して特権 EXEC モード（およびすべてのコマンド）にアクセスできます。あるいは、認証処理でローカル データベースではなく AAA サーバを使用してログイン コマンドを回避するか、またはすべてのローカル ユーザをレベル 1 に設定することにより、システム イネーブル パスワードを使用して特権 EXEC モードにアクセスできるユーザを制御できます。

ホスト オペレーティング システムから ASA へのセッション

一部のプラットフォームでは、ASA の実行を別のアプリケーションとしてサポートしています（例：Catalyst 6500 の ASASM、Firepower 4100/9300 の ASA）。ホスト オペレーティング システムから ASA へのセッションの場合、接続のタイプに応じてシリアルおよび Telnet 認証を設定できます。

マルチ コンテキスト モードでは、システム コンフィギュレーションで AAA コマンドを設定できません。ただし、Telnet またはシリアル認証を管理コンテキストで設定した場合、認証はこれらのセッションにも適用されます。この場合、管理コンテキストの AAA サーバまたはローカル ユーザ データベースが使用されます。

CLIおよびASDM アクセス認証の設定

始める前に

- Telnet、SSH、または HTTP アクセスを設定します。
- 外部認証の場合は、AAA サーバ グループを設定します。ローカル認証の場合は、ローカル データベースにユーザを追加します。
- HTTP 管理認証では、AAA サーバ グループの SDI プロトコルをサポートしていません。

- この機能は、**ssh authentication** コマンドによるローカル ユーザ名に関する SSH 公開キー認証には影響しません。ASA では、公開キー認証に対し、ローカル データベースを暗黙的に使用します。この機能は、ユーザ名とパスワードにのみ影響します。ローカル ユーザが公開キー認証またはパスワードを使用できるようにするには、この手順を使用してローカル認証を明示的に設定し、パスワード アクセスを許可する必要があります。

手順

管理アクセス用のユーザを認証します。

aaa authentication {**telnet** | **ssh** | **http** | **serial**} **console** {**LOCAL** | *server_group* [**LOCAL**]}

例：

```
ciscoasa(config)# aaa authentication ssh console radius_1 LOCAL
ciscoasa(config)# aaa authentication http console radius_1 LOCAL
ciscoasa(config)# aaa authentication serial console LOCAL
```

telnet キーワードは Telnet アクセスを制御します。ASASM の場合、このキーワードは **session** コマンドを使用するスイッチからのセッションにも影響します。**ssh** キーワードは SSH アクセスを制御します（パスワードのみ。公開キー認証では暗黙のうちにローカルデータベースが使用されます）。**http** キーワードは ASDM アクセスを制御します。**serial** キーワードはコンソール ポート アクセスを制御します。ASASM の場合、たとえば、このキーワードは **service-module session** コマンドを使用してスイッチからアクセスする仮想コンソールに影響します。

認証に AAA サーバ グループを使用する場合は、AAA サーバが使用できないときにローカル データベースをフォールバック方式として使用するように ASA を設定できます。サーバ グループ名を指定し、その後に **LOCAL**（大文字と小文字の区別あり）を追加します。ローカルデータベースでは AAA サーバと同じユーザ名およびパスワードを使用することを推奨します。これは、ASA のプロンプトでは、どの方式が使用されているかが示されないためです。**LOCAL** だけを入力して、ローカルデータベースを認証の主要方式として（フォールバックなしで）使用することもできます。

enable コマンド認証の設定（特権 EXEC モード）

ユーザが **enable** コマンドを入力する際に、そのユーザを認証できます。

始める前に

enable 認証の概要 （974 ページ）を参照してください。

手順

ユーザを認証するための次のオプションのいずれかを選択します。

- AAA サーバまたはLOCALデータベースを使用してユーザを認証するには、次のコマンドを入力します。

  aaa authentication enable console {**LOCAL** | *server_group* [**LOCAL**]}

  例：

  ```
  ciscoasa(config)# aaa authentication enable console LOCAL
  ```

  ユーザ名とパスワードの入力を求めるプロンプトがユーザに対して表示されます。

  認証に AAA サーバ グループを使用する場合は、AAA サーバが使用できないときにローカルデータベースをフォールバック方式として使用するようにASAを設定できます。サーバ グループ名を指定し、その後に**LOCAL**（大文字と小文字の区別あり）を追加します。ローカル データベースでは AAA サーバと同じユーザ名およびパスワードを使用することを推奨します。これは、ASAのプロンプトでは、どの方式が使用されているかが示されないためです。

  LOCALだけを入力して、ローカルデータベースを認証の主要方式として（フォールバックなしで）使用することもできます。

- ローカルデータベースからユーザとしてログインするには、次のコマンドを入力します。

  login

  例：

  ```
  ciscoasa# login
  ```

  ASAにより、ユーザ名とパスワードの入力を求めるプロンプトが表示されます。パスワードを入力すると、ASA により、ユーザはローカル データベースで指定されている特権レベルに置かれます。

  ユーザは独自のユーザ名とパスワードでログインして特権EXECモードにアクセスすることができるので、システム イネーブル パスワードを全員に提供する必要がなくなります。ユーザがログイン時に特権EXECモード（およびすべてのコマンド）にアクセスできるようにするには、ユーザの特権レベルを 2（デフォルト）～ 15 に設定します。ローカル コマンド認可を設定した場合、ユーザは、その特権レベル以下のレベルに割り当てられているコマンドのみを入力できます。

ASDM 証明書認証の設定

AAA 認証の有無にかかわらず証明書認証を必須にできます。ASA は証明書を PKI トラストポイントに照合して検証します。

始める前に

この機能は、シングル ルーテッド モードでのみサポートされます。

手順

ステップ 1 証明書認証をイネーブルにします。

http authentication-certificate *interface_name*

例：

```
ciscoasa(config)# http authentication-certificate outside
```

証明書認証はインターフェイスごとに設定できます。その結果、信頼できるインターフェイスまたは内部インターフェイス上の接続については証明書の提示が不要になります。コマンドを複数回使用すれば、複数のインターフェイス上で証明書認証をイネーブルにできます。

ステップ 2 （任意） ASDM で証明書からユーザ名を抽出する際に使用する属性を設定します。

http username-from-certificate {*primary-attr* [*secondary-attr*] | **use-entire-name** | **use-script**} [**pre-fill-username**]

例：

```
ciscoasa(config)# http username-from-certificate CN pre-fill-username
```

デフォルトでは、ASDM は CN OU 属性を使用します。

- *primary-attr* 引数は、ユーザ名の抽出に使用する属性を指定します。*secondary-attr* 引数は、オプションで、ユーザ名を抽出するためにプライマリ属性と一緒に使用する追加の属性を指定します。次の属性を使用できます。
  - C：国
  - CN：共通名
  - DNQ：DN 修飾子
  - EA：電子メール アドレス
  - GENQ：世代修飾子
  - GN：名
  - I：イニシャル
  - L：局所性
  - N：名前
  - O：組織
  - OU：組織単位
  - SER：シリアル番号
  - SN：姓

- SP：都道府県
- T：役職
- UID：ユーザ ID
- UPN：ユーザ プリンシパル名

- **use-entire-name** キーワードでは DN 名全体を使用します。
- **use-script** キーワードでは ASDM によって生成された Lua スクリプトを使用します。
- **pre-fill-username** キーワードでは、認証を求めるプロンプトにユーザ名が事前入力されています。そのユーザ名が最初に入力したものと異なる場合、最初のユーザ名が事前入力された新しいダイアログボックスが表示されます。そこに、認証用のパスワードを入力できます。

管理許可による CLI および ASDM アクセスの制限

ASA ではユーザの認証時に管理アクセス ユーザとリモート アクセス ユーザを区別できるようになっています。ユーザ ロールを区別することで、リモート アクセス VPN ユーザやネットワーク アクセス ユーザが ASA に管理接続を確立するのを防ぐことができます。

始める前に

RADIUS または LDAP（マッピング済み）ユーザ

ユーザが LDAP 経由で認証されると、ネイティブ LDAP 属性およびその値が Cisco ASA 属性にマッピングされ、特定の許可機能が提供されます。Cisco VSA CVPN3000-Privilege-Level の値を 0 ～ 15 の範囲で設定した後、ldap map-attributes**ldap map-attributes** コマンドを使用して、LDAP 属性を Cisco VAS CVPN3000-Privilege-Level にマッピングします。

RADIUS IETF の **service-type** 属性が、RADIUS 認証および許可要求の結果として access-accept メッセージで送信される場合、この属性は認証されたユーザにどのタイプのサービスを付与するかを指定するために使用されます。

RADIUS Cisco VSA **privilege-level** 属性（ベンダー ID 3076、サブ ID 220）が access-accept メッセージで送信される場合は、ユーザの権限レベルを指定するために使用されます。

TACACS+ ユーザ

「service=shell」で許可が要求され、サーバは PASS または FAIL で応答します。

ローカル ユーザ

指定したユーザ名に対する **service-type** コマンドを設定します。デフォルトでは、service-type は admin で、**aaa authentication console** コマンドで指定されたすべてのサービスに対してフルアクセスが許可されます。

管理許可の属性

管理許可の AAA サーバ タイプおよび有効な値については、次の表を参照してください。ASA ではこれらの値を使用して管理アクセス レベルを決定します。

Management Level	RADIUS/LDAP の（マッピングされた）属性	TACACS+ 属性	ローカル データベースの属性
[Full Access]： **aaa authentication console** コマンド	Service-Type 6（アドミニストレーティブ）、Privilege-Level 1	PASS、特権レベル 1	admin
[Partial Access]： **aaa authentication console** コマンドで設定すると、CLI または ASDM に対するアクセスが許可されます。ただし、**aaa authentication enable console** コマンドを使用して **enable** 認証を設定する場合、CLI y ユーザは **enable** コマンドを使用して特権 EXEC モードにアクセスすることはできません。	Service-Type 7（NAS プロンプト）、Privilege-Level 2 以上 Framed (2) および Login (1) サービス タイプは同様に扱われます。	PASS、特権レベル 2 以上	nas-prompt
[No Access]：管理アクセスが拒否されます。ユーザは **aaa authentication console** コマンドで指定されたいずれのサービスも使用できません（**serial** キーワードは除きます。つまり、シリアル アクセスは許可されます）。リモート アクセス（IPsec および SSL）ユーザは、引き続き自身のリモート アクセスセッションを認証および終了できます。他のすべてのサービスタイプ（ボイス、ファクスなど）も同様に処理されます。	Service-Type 5（アウトバウンド）	FAIL	remote-access

その他のガイドライン

- シリアル コンソール アクセスは管理許可に含まれません。
- この機能を使用するには、管理アクセスに AAA 認証も設定する必要があります。CLIおよびASDM アクセス認証の設定 （975 ページ）を参照してください。
- 外部認証を使用する場合は、この機能をイネーブルにする前に、AAA サーバ グループを設定しておく必要があります。
- HTTP 許可は、シングル ルーテッド モードでのみサポートされます。

手順

ステップ 1 Telnet と SSH の管理許可をイネーブルにします。

aaa authorization exec {**authentication-server** | **LOCAL**} [**auto-enable**]

auto-enable キーワードを使用して、十分な認証特権を持つ管理者が、ログインするときに特権 EXEC モードに自動的に入ることができます。

例：

```
ciscoasa(config)# aaa authentication ssh console RADIUS
ciscoasa(config)# aaa authorization exec authentication-server auto-enable
```

ステップ 2 HTTPS の管理許可をイネーブルにします（ASDM）。

aaa authorization http console {**authentication-server** | **LOCAL**}

例：

```
ciscoasa(config)# aaa authentication http console RADIUS
ciscoasa(config)# aaa authorization http console authentication-server
```

ステップ 3

例

次の例は、LDAP 属性マップを定義する方法を示しています。この例では、セキュリティ ポリシーによって、LDAP によって認証されているユーザが、ユーザ レコードのフィールドまたはパラメータの title と company を、IETF-RADIUS service-type と privilege-level にそれぞれマップすることを指定しています。

```
ciscoasa(config)# ldap attribute-map admin-control
ciscoasa(config-ldap-attribute-map)# map-name title IETF-RADIUS-Service-Type
ciscoasa(config-ldap-attribute-map)# map-name company
```

次の例では、LDAP 属性マップを LDAP AAA サーバに適用します。

```
ciscoasa(config)# aaa-server ldap-server (dmz1) host 10.20.30.1
ciscoasa(config-aaa-server-host)# ldap attribute-map admin-control
```

コマンド認可の設定

コマンドへのアクセスを制御する場合、ASA ではコマンド許可を設定でき、ユーザが使用できるコマンドを決定できます。デフォルトでは、ログインするとユーザ EXEC モードにアクセスでき、最低限のコマンドだけが提供されます。**enable** コマンド（または、ローカルデータベースを使用するときは **login** コマンド）を入力すると、特権 EXEC モードおよびコンフィギュレーション コマンドを含む高度なコマンドにアクセスできます。

次の 2 つのコマンド許可方式のいずれかを使用できます。

- ローカル特権レベル
- TACACS+ サーバ特権レベル

コマンド認可について

コマンド認可を有効にし、承認済みのユーザにのみコマンド入力を許容することができます。

サポートされるコマンド認可方式

次の 2 つのコマンド許可方式のいずれかを使用できます。

- ローカル特権レベル：ASA でコマンド特権レベルを設定します。ローカルユーザ、RADIUS ユーザ、または LDAP ユーザ（LDAP 属性を RADIUS 属性にマッピングする場合）を CLI アクセスについて認証する場合、ASA はそのユーザをローカルデータベース、RADIUS、または LDAP サーバで定義されている特権レベルに所属させます。ユーザは、割り当てられた特権レベル以下のコマンドにアクセスできます。すべてのユーザは、初めてログインするときに、ユーザ EXEC モード（レベル 0 または 1 のコマンド）にアクセスします。ユーザは、特権 EXEC モード（レベル 2 以上のコマンド）にアクセスするために再び **enable** コマンドで認証するか、**login** コマンドでログイン（ローカル データベースに限る）できます。

  （注） ローカルデータベース内にユーザが存在しなくても、また CLI 認証や **enable** 認証がない場合でも、ローカル コマンド許可を使用できます。代わりに、**enable** コマンドを入力するときにシステム イネーブル パスワードを入力すると、ASA によってレベル 15 に置かれます。次に、すべてのレベルのイネーブル パスワードを作成します。これにより、**enable** *n*（2 ～ 15）を入力したときに、ASA によってレベル *n* に置かれるようになります。これらのレベルは、ローカル コマンド許可を有効にするまで使用されません。

- TACACS+ サーバ特権レベル：TACACS+ サーバで、ユーザまたはグループが CLI アクセスについて認証した後で使用できるコマンドを設定します。CLI でユーザが入力するすべてのコマンドは、TACACS+ サーバで検証されます。

セキュリティ コンテキストとコマンド許可

AAA 設定はコンテキストごとに個別であり、コンテキスト間で共有されません。

コマンド許可を設定する場合は、各セキュリティ コンテキストを別々に設定する必要があります。この設定により、異なるセキュリティ コンテキストに対して異なるコマンド許可を実行できます。

セキュリティ コンテキストを切り替える場合、管理者は、ログイン時に指定したユーザ名で許可されるコマンドが新しいコンテキスト セッションでは異なる可能性があることや、新しいコンテキストではコマンド許可がまったく設定されていない可能性があることを念頭に置いてください。コマンド許可がセキュリティ コンテキストによって異なる場合があることを管理者が

理解していないと、混乱が生じる可能性があります。この動作は、次の仕組みによってさらに複雑になります。

（注） システム実行スペースでは AAA コマンドがサポートされないため、システム実行スペースではコマンド許可を使用できません。

コマンド権限レベル

デフォルトでは、次のコマンドが特権レベル 0 に割り当てられます。その他のすべてのコマンドは特権レベル 15 に割り当てられます。

- **show checksum**
- **show curpriv**
- **enable**
- **help**
- **show history**
- **login**
- **logout**
- **pager**
- **show pager**
- **clear pager**
- **quit**
- **show version**

コンフィギュレーション モード コマンドを 15 より低いレベルに移動する場合は、configure コマンドも同じレベルに移動してください。このようにしないと、ユーザはコンフィギュレーション モードに入ることができません。

ローカル コマンド許可の設定

ローカル コマンド許可を使用して、コマンドを 16 の特権レベル（0 ～ 15）の 1 つに割り当てることができます。デフォルトでは、各コマンドは特権レベル 0 または 15 に割り当てられます。各ユーザを特定の特権レベルに定義でき、各ユーザは割り当てられた特権レベル以下のコマンドを入力できます。ASA は、ローカル データベース、RADIUS サーバ、または LDAP サーバ（LDAP 属性を RADIUS 属性にマッピングする場合）に定義されているユーザ特権レベルをサポートしています。

手順

ステップ 1 特権レベルにコマンドを割り当てます。

privilege [**show** | **clear** | **cmd**] **level** *level* [**mode** {**enable** | **cmd**}] **command** コマンド

例：

```
ciscoasa(config)# privilege show level 5 command filter
```

再割り当てする各コマンドに対してこのコマンドを繰り返します。

このコマンドのオプションは、次のとおりです。

- **show**|**clear**|**cmd**：これらのオプション キーワードを使用すると、コマンドの show、clear、または configure 形式に対してだけ特権を設定できます。コマンドの configure 形式は、通常、未修正コマンド（**show** または **clear** プレフィックスなしで）または **no** 形式として、コンフィギュレーションの変更を引き起こす形式です。これらのキーワードのいずれかを使用しない場合は、コマンドのすべての形式が影響を受けます。
- **level** *level*：0 ～ 15 の重大度。
- **mode** {**enable** | **configure**}：ユーザ EXEC モードまたは特権 EXEC モードおよびコンフィギュレーション モードでコマンドを入力することができ、そのコマンドが各モードで異なるアクションを実行する場合は、それらのモードの特権レベルを個別に設定することができます。
  - **enable**：ユーザ EXEC モードと特権 EXEC モードの両方を指定します。
  - **configure**：**configure terminal** コマンドを使用してアクセスされるコンフィギュレーション モードを指定します。
- **command** *command*：設定しているコマンド。設定できるのは、*main* コマンドの特権レベルだけです。たとえば、すべての **aaa** コマンドのレベルを設定できますが、**aaa authentication** コマンドと **aaa authorization** コマンドのレベルを個別に設定できません。

ステップ 2 （任意） コマンド認可のための AAA ユーザを有効にします。このコマンドを入力しない場合、ASA は、ローカル データベース ユーザの特権レベルだけをサポートし、他のタイプのユーザをすべてデフォルトでレベル 15 に割り当てます。

aaa authorization exec authentication-server [auto-enable]

例：

```
ciscoasa(config)# aaa authorization exec authentication-server
```

さらに、このコマンドは管理認証を有効にします。管理許可による CLI および ASDM アクセスの制限 （979 ページ）を参照してください。

ステップ 3 ローカルのコマンド特権レベルの使用を有効にします。

aaa authorization command LOCAL

例：

```
ciscoasa(config)# aaa authorization command LOCAL
```

コマンド特権レベルを設定する場合は、このコマンドでコマンド許可を設定しない限り、コマンド許可は実行されません。

例

filter コマンドの形式は次のとおりです。

- **filter**（**configure** オプションにより表されます）
- **show running-config filter**
- **clear configure filter**

特権レベルを形式ごとに個別に設定することができます。または、このオプションを省略してすべての形式に同じ特権レベルを設定することもできます。次は、各形式を個別に設定する方法の例です。

```
ciscoasa(config)# privilege show level 5 command filter
ciscoasa(config)# privilege clear level 10 command filter
ciscoasa(config)# privilege cmd level 10 command filter
```

また、次の例では、すべての filter コマンドを同じレベルに設定する例を示します。

```
ciscoasa(config)# privilege level 5 command filter
```

show privilege コマンドは、形式を分けて表示します。

次の例では、**mode** キーワードの使用方法を示します。**enable** コマンドは、ユーザ EXEC モードから入力する必要があります。一方、**enable password** コマンドは、コンフィギュレーション モードでアクセスでき、最も高い特権レベルが必要です。

```
ciscoasa(config)# privilege cmd level 0 mode enable command enable
ciscoasa(config)# privilege cmd level 15 mode cmd command enable
ciscoasa(config)# privilege show level 15 mode cmd command enable
```

次の例では、**mode** キーワードを使用する追加コマンド（**configure** コマンド）を示します。

```
ciscoasa(config)# privilege show level 5 mode cmd command configure
ciscoasa(config)# privilege clear level 15 mode cmd command configure
ciscoasa(config)# privilege cmd level 15 mode cmd command configure
```

```
ciscoasa(config)# privilege cmd level 15 mode enable command configure
```

（注） この最後の行は、**configure terminal** コマンドに関する行です。

TACACS+ サーバでのコマンドの設定

グループまたは個々のユーザの共有プロファイル コンポーネントとしての Cisco Secure Access Control Server（ACS）TACACS+ サーバでコマンドを設定できます。サードパーティの TACACS+ サーバの場合は、コマンド許可サポートの詳細については、ご使用のサーバのマニュアルを参照してください。

Cisco Secure ACS バージョン 3.1 でコマンドを設定する場合は、次のガイドラインを参照してください。

- ASA は、シェル コマンドとして許可するコマンドを送信し、TACACS+ サーバでシェル コマンドとしてコマンドを設定します。

  （注） Cisco Secure ACS には、「pix-shell」と呼ばれるコマンド タイプが含まれている場合があります。このタイプは ASA コマンド許可に使用しないでください。

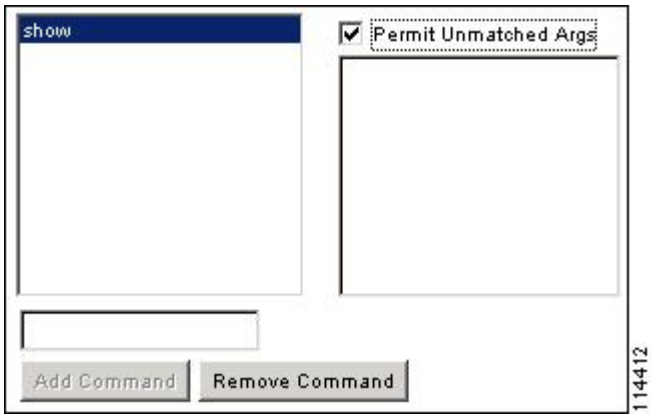
- コマンドの最初のワードは、メイン コマンドと見なされます。その他のワードはすべて引数と見なされます。これは、**permit** または **deny** の後に置く必要があります。

  たとえば、**show running-configuration aaa-server** コマンドを許可するには、コマンド フィールドに **show running-configuration** を追加し、引数フィールドに **permit aaa-server** を入力します。

- [Permit Unmatched Args] チェックボックスをオンにすると、明示的に拒否していないすべてのコマンド引数を許可できます。

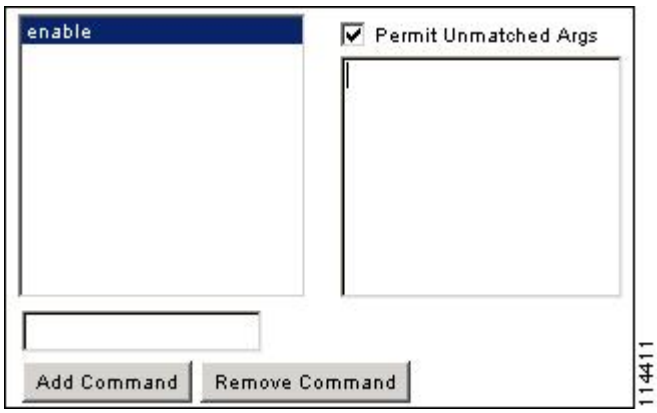
  たとえば、特定の **show** コマンドを設定するだけで、すべての **show** コマンドが許可されます。CLI の使用法を示す疑問符や省略形など、コマンドの変形をすべて予想する必要がなくなるので、この方法を使用することをお勧めします（次の図を参照）。

図 *55* : 関連するすべてのコマンドの許可



- **enable** や **help** など、単一ワードのコマンドについては、そのコマンドに引数がない場合でも、一致しない引数を許可する必要があります（次の図を参照）。

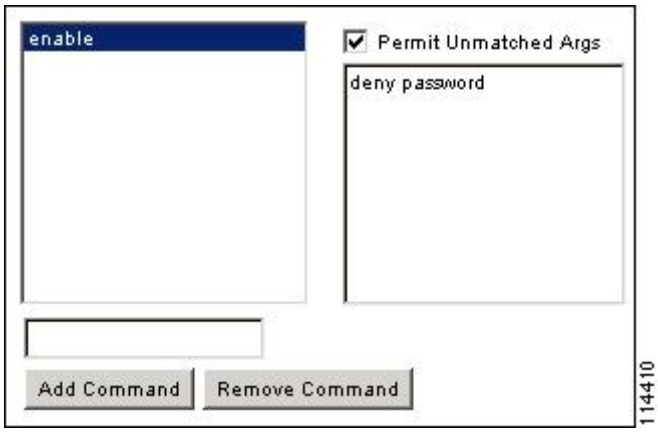
図 *56* : 単一ワードのコマンドの許可



- 引数を拒否するには、その引数の前に **deny** を入力します。

  たとえば、**enable** コマンドを許可し、**enable password** コマンドを許可しない場合には、コマンドフィールドに **enable** を入力し、引数フィールドに **deny password** を入力します。**enable** だけが許可されるように、必ず、[Permit Unmatched Args] チェックボックスをオンにしてください（次の図を参照）。

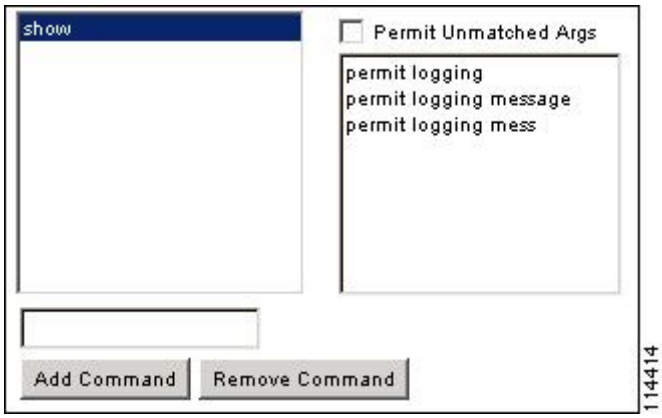
図 *57 :* 引数の拒否



- コマンドラインでコマンドを省略形で入力した場合、ASA はプレフィックスとメイン コマンドを完全なテキストに展開しますが、その他の引数は入力したとおりに TACACS+ サーバに送信します。

  たとえば、**sh log** と入力すると、ASA は完全なコマンド **show logging** を TACACS+ サーバに送信します。一方、**sh log mess** と入力すると、ASA は展開されたコマンド **show logging message** ではなく、**show logging mess** を TACACS+ サーバに送信します。省略形を予想して同じ引数の複数のスペルを設定できます（次の図を参照）。

図 *58 :* 省略形の指定



- すべてのユーザに対して次の基本コマンドを許可することをお勧めします。
  - **show checksum**
  - **show curpriv**
  - **enable**
  - **help**
  - **show history**
  - **login**

- **logout**
- **pager**
- **show pager**
- **clear pager**
- **quit**
- **show version**

TACACS+ コマンド許可の設定

TACACS+ コマンド認可をイネーブルにし、ユーザが CLI でコマンドを入力すると、ASA はそのコマンドとユーザ名を TACACS+ サーバに送信し、コマンドが認可されているかどうかを判別します。

TACACS+ コマンド許可をイネーブルにする前に、TACACS+ サーバで定義されたユーザとして ASA にログインしていること、および ASA の設定を続けるために必要なコマンド許可があることを確認してください。たとえば、すべてのコマンドが認可された管理ユーザとしてログインする必要があります。このようにしないと、意図せずロックアウトされる可能性があります。

意図したとおりに機能することが確認できるまで、設定を保存しないでください。間違いによりロック アウトされた場合、通常はASA を再始動することによってアクセスを回復できます。

TACACS+ システムが完全に安定して信頼できることを確認します。必要な信頼性レベルについて、通常は、完全冗長 TACACS+ サーバ システムと ASA への完全冗長接続が必要です。たとえば、TACACS+ サーバ プールに、インターフェイス 1 に接続された 1 つのサーバとインターフェイス 2 に接続された別のサーバを含めます。TACACS+ サーバが使用できない場合にフォールバック方式としてローカル コマンド許可を設定することもできます。

TACACS+ サーバを使用したコマンド許可を設定するには、次の手順を実行します。

手順

次のコマンドを入力します。

aaa authorization command *tacacs+_server_group* [**LOCAL**]

例：

```
ciscoasa(config)# aaa authorization command tacacs+_server_group [LOCAL]
```

TACACS+ サーバを使用できない場合は、ローカル データベースをフォールバック方式として使用するように ASA を設定できます。フォールバックを有効にするには、サーバ グループ名の後ろに **LOCAL** を指定します（**LOCAL** は大文字と小文字を区別します）。ローカル データベースでは TACACS+ サーバと同じユーザ名およびパスワードを使用することを推奨します。

これは、ASA のプロンプトでは、どの方式が使用されているかが示されないためです。必ずローカル データベースのユーザとコマンド特権レベルを設定してください。

ローカル データベース ユーザのパスワード ポリシーの設定

ローカル データベースを使用して CLI または ASDM アクセスの認証を設定する場合は、指定期間を過ぎるとユーザにパスワードの変更を要求し、パスワードの最短長と最低変更文字数などのパスワード標準に従うことを要求するパスワード ポリシーを設定できます。

パスワード ポリシーはローカル データベースを使用する管理ユーザに対してのみ適用されます。ローカル データベースを使用するその他のタイプのトラフィック（VPN や AAA によるネットワーク アクセスなど）や、AAA サーバによって認証されたユーザには適用されません。

パスワードポリシーの設定後は、自分または別のユーザのパスワードを変更すると、新しいパスワードに対してパスワードポリシーが適用されます。既存のパスワードについては、現行のポリシーが適用されます。新しいポリシーは、 **username** コマンドおよび **change-password** コマンドを使用したパスワードの変更に適用されます。

始める前に

- ローカルデータベースを使用して CLI または ASDM アクセスの AAA 認証を設定します。
- ローカル データベース内にユーザ名を指定します。

手順

ステップ 1 （オプション）リモート ユーザのパスワードの有効期間を日数で設定します。

password-policy lifetime *days*

例：

```
ciscoasa(config)# password-policy lifetime 180
```

（注） コンソール ポートを使用しているユーザは、パスワードの有効期限が切れてもロックアウトされません。

有効な値は、0 ～ 65536 です。デフォルト値は 0 日です。この場合、パスワードは決して期限切れになりません。

パスワードの有効期限が切れる 7 日前に、警告メッセージが表示されます。パスワードの有効期限が切れると、リモート ユーザのシステム アクセスは拒否されます。有効期限が切れた後アクセスするには、次のいずれかの手順を実行します。

- 他の管理者に **username** コマンドを使用してパスワードを変更してもらいます。
- 物理コンソール ポートにログインして、パスワードを変更します。

ステップ 2 （オプション）新しいパスワードと古いパスワードで違わなければならない最小文字数を設定します。

password-policy minimum-changes *value*

例：

```
ciscoasa(config)# password-policy minimum-changes 2
```

有効な値は、0 ～ 64 文字です。デフォルト値は 0 です

文字マッチングは位置に依存しません。したがって、新しいパスワードで使用される文字が、現在のパスワードのどこにも使用されていない場合に限り、パスワードが変更されたとみなされます。

ステップ 3 （オプション）パスワードの最小長を設定します。

password-policy minimum-length *value*

例：

```
ciscoasa(config)# password-policy minimum-length 8
```

有効な値は、3 ～ 64 文字です。推奨されるパスワードの最小長は 8 文字です。

ステップ 4 （オプション）パスワードに含める大文字の最小個数を設定します。

password-policy minimum-uppercase *value*

例：

```
ciscoasa(config)# password-policy  minimum-uppercase 3
```

有効な値は、0 ～ 64 文字です。デフォルト値は、最小個数がないことを意味する 0 です。

ステップ 5 （オプション）パスワードに含める小文字の最小個数を設定します。

password-policy minimum-lowercase *value*

例：

```
ciscoasa(config)# password-policy minimum-lowercase 6
```

有効な値は、0 ～ 64 文字です。デフォルト値は、最小個数がないことを意味する 0 です。

ステップ 6 （オプション）パスワードに含める数字の最小個数を設定します。

password-policy minimum-numeric *value*

例：

```
ciscoasa(config)# password-policy minimum-numeric 1
```

有効な値は、0 ～ 64 文字です。デフォルト値は、最小個数がないことを意味する 0 です。

ステップ 7 （オプション）パスワードに含める特殊文字の最小個数を設定します。

password-policy minimum-special *value*

例：

```
ciscoasa(config)# password-policy minimum-special 2
```

有効な値は、0 ～ 64 文字です。特殊文字には、!、@、#、$、%、^、&、*、(、および) が含まれます。デフォルト値は、最小個数がないことを意味する 0 です。

ステップ 8 （オプション）ユーザが自分のパスワードの変更に **username** コマンドではなく **change-password** コマンドを使用する必要があるかを設定します。

password-policy authenticate enable

例：

```
ciscoasa(config)# password-policy authenticate enable
```

デフォルト設定はディセーブルです。どちらの方法でも、ユーザはパスワードを変更することができます。

この機能を有効にして、**username** コマンドを使用してパスワードを変更しようとすると、次のエラー メッセージが表示されます。

```
ERROR: Changing your own password is prohibited
```

clear configure username コマンドを使用して自分のアカウントを削除することもできません。消去を試みた場合は、次のエラー メッセージが表示されます。

```
ERROR: You cannot delete all usernames because you are not allowed to delete yourself
```

パスワードの変更

パスワードポリシーでパスワードの有効期間を設定した場合、有効期間を過ぎるとパスワードを新しいパスワードに変更する必要があります。パスワードポリシー認証をイネーブルにした場合は、このパスワード変更のスキームが必須です。パスワードポリシー認証がイネーブルでない場合は、このメソッドを使用することも、直接ユーザアカウントを変更することもできます。

username パスワードを変更するには、次の手順を実行します。

手順

次のコマンドを入力します。

change-password [**old-password** *old_password* [**new-password** *new_password*]]

例：

```
ciscoasa# change-password old-password j0hncr1chton new-password a3rynsun
```

コマンドに新旧のパスワードを入力していない場合は、ASA によって入力が求められます。

管理アクセス アカウンティングの設定

CLI で **show** コマンド以外のコマンドを入力する場合、アカウンティング メッセージを TACACS+ アカウンティング サーバに送信できます。ユーザがログインするとき、ユーザが **enable** コマンドを入力するとき、またはユーザがコマンドを発行するときのアカウンティングを設定できます。

コマンド アカウンティングに使用できるサーバは、TACACS+ だけです。

管理アクセスおよびイネーブル コマンド アカウンティングを設定するには、次の手順を実行します。

手順

ステップ 1 次のコマンドを入力します。
aaa accounting {**serial** | **telnet** | **ssh** | **enable**} **console** *server-tag*

例：

```
ciscoasa(config)# aaa accounting telnet console group_1
```

有効なサーバ グループ プロトコルは RADIUS と TACACS+ です。

ステップ 2 コマンドアカウンティングをイネーブルにします。TACACS+ サーバだけがコマンドアカウンティングをサポートします。

aaa accounting command [**privilege** *level*] *server-tag*

例：

```
ciscoasa(config)# aaa accounting command privilege 15 group_1
```

privilege *level* というキーワードと引数のペアは最小特権レベルであり、*server-tag* 引数は ASA がコマンド アカウンティング メッセージを送信する TACACS+ サーバ グループの名前です。

ロックアウトからの回復

状況によっては、コマンド許可やCLI認証をオンにすると、ASA CLIからロックアウトされる場合があります。通常は、ASAを再起動することによってアクセスを回復できます。ただし、すでにコンフィギュレーションを保存した場合は、ロックアウトされたままになる可能性があります。

次の表に、一般的なロックアウト条件とその回復方法を示します。

表 *42 : CLI* 認証およびコマンド許可のロックアウト シナリオ

機能	ロックアウト条件	説明	対応策：シングル モード	対応策：マルチ モード
ローカル CLI 認証	ローカル データベースにユーザが設定していない。	ローカル データベース内にユーザが存在しない場合は、ログインできず、ユーザの追加もできません。	ログインし、パスワードと **aaa** コマンドをリセットします。	スイッチからASAへのセッションを接続します。システム実行スペースから、コンテキストに切り替えてユーザを追加することができます。
TACACS+ コマンド許可 TACACS+ CLI 認証 RADIUS CLI 認証	サーバがダウンしているか到達不能で、フォールバック方式を設定していない。	サーバが到達不能である場合は、ログインもコマンドの入力もできません。	**1.** ログインし、パスワードと AAA コマンドをリセットします。 **2.** サーバがダウンしたときにロックアウトされないように、ローカル データベースをフォールバック方式として設定します。	**1.** ASAでネットワーク コンフィギュレーションが正しくないためにサーバが到達不能である場合は、スイッチからASAへのセッションを接続します。システム実行スペースから、コンテキストに切り替えてネットワークを再設定することができます。 **2.** サーバがダウンしたときにロックアウトされないように、ローカル データベースをフォールバック方式として設定します。

機能	ロックアウト条件	説明	対応策：シングル モード	対応策：マルチ モード
TACACS+ コマンド許可	十分な特権のないユーザまたは存在しないユーザとしてログインした。	コマンド許可がイネーブルになりますが、ユーザはこれ以上コマンドを入力できなくなります。	TACACS+ サーバのユーザアカウントを修正します。 TACACS+ サーバへのアクセス権がなく、ASA をすぐに設定する必要がある場合は、メンテナンス パーティションにログインして、パスワードと **aaa** コマンドをリセットします。	スイッチから ASA へのセッションを接続します。システム実行スペースから、コンテキストに切り替えてコンフィギュレーションの変更を完了することができます。また、TACACS+ コンフィギュレーションを修正するまでコマンド許可をディセーブルにすることもできます。
ローカル コマンド許可	十分な特権のないユーザとしてログインしている。	コマンド許可がイネーブルになりますが、ユーザはこれ以上コマンドを入力できなくなります。	ログインし、パスワードと **aaa** コマンドをリセットします。	スイッチから ASA へのセッションを接続します。システム実行スペースから、コンテキストに切り替えてユーザ レベルを変更することができます。

デバイス アクセスのモニタリング

デバイス アクセスのモニタリングについては、次のコマンドを参照してください。

- **show running-config all privilege all**

  このコマンドは、すべてのコマンドの特権レベルを表示します。

  show running-config all privilege all コマンドの場合、ASA は特権レベルに対する各 CLI コマンドの現在の割り当てを表示します。次に、このコマンドの出力例を示します。

```
ciscoasa(config)# show running-config all  privilege all
privilege show level 15 command aaa
privilege clear level 15 command aaa
privilege configure level 15 command aaa
privilege show level 15 command aaa-server
privilege clear level 15 command aaa-server
privilege configure level 15 command aaa-server
privilege show level 15 command access-group
privilege clear level 15 command access-group
privilege configure level 15 command access-group
privilege show level 15 command access-list
privilege clear level 15 command access-list
privilege configure level 15 command access-list
privilege show level 15 command activation-key
privilege configure level 15 command activation-key
...
```

- **show running-config privilege level** *level*

  このコマンドは、特定の特権レベルのコマンドを示します。level 引数は、0 ～ 15 の範囲の整数になります。

  次の例は、特権レベル 10 に対するコマンド割り当てを示しています。

```
ciscoasa(config)# show running-config all privilege level 10
privilege show level 10 command aaa
```

- **show running-config privilege command** コマンド

  このコマンドは、特定のコマンドの特権レベルを表示します。

  次の例は、**access-list** コマンドに対するコマンド割り当てを示しています。

```
ciscoasa(config)# show running-config all privilege command access-list
privilege show level 15 command access-list
privilege clear level 15 command access-list
privilege configure level 15 command access-list
```

- **show curpriv**

  このコマンドは、現在のログイン ユーザを表示します。

  次に、**show curpriv** コマンドの出力例を示します。

```
ciscoasa# show curpriv
Username: admin
Current privilege level: 15
Current Mode/s: P_PRIV
```

次の表で、**show curpriv** コマンドの出力について説明します。

表 *43 : show curpriv* コマンド出力の説明

フィールド	説明
[Username]	[Username]。デフォルト ユーザとしてログインすると、名前は enable_1（ユーザ EXEC）または enable_15（特権 EXEC）になります。
Current privilege level	レベルの範囲は 0 ～ 15 です。ローカル コマンド許可を設定してコマンドを中間特権レベルに割り当てない限り、使用されるレベルはレベル 0 と 15 だけです。

フィールド	説明
Current Modes	使用可能なアクセス モードは次のとおりです。 • P_UNPR：ユーザ EXEC モード（レベル 0 と 1） • P_PRIV：特権 EXEC モード（レベル 2 ～ 15） • P_CONF：コンフィギュレーション モード

- **show quota management-session**

  このコマンドは、使用中の現在のセッションを表示します。

  次に、**show quota management-session** コマンドの出力例を示します。

```
ciscoasa(config)# show quota management-session

quota management-session limit 3
quota management-session warning level 2
quota management-session level 0
quota management-session high water 2
quota management-session errors 0
quota management-session warnings 0
```

管理アクセスの履歴

表 *44 :* 管理アクセスの履歴

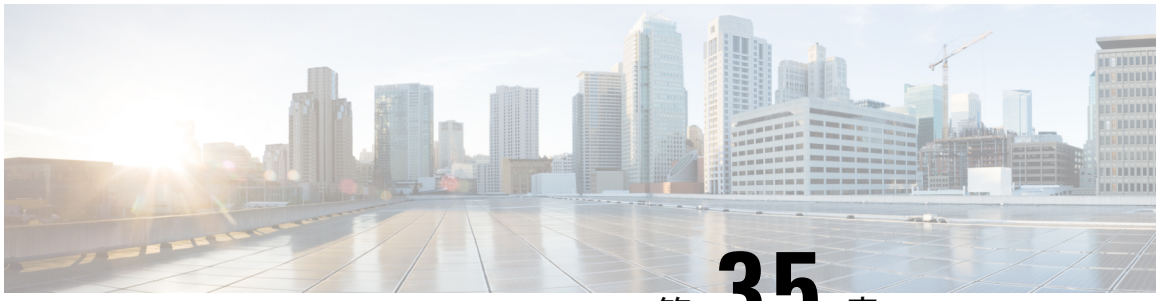
機能名	プラットフォーム リリース	説明
ASDM 管理認証	9.4(1)	HTTP アクセスと Telnet および SSH アクセス別に管理認証を設定できるようになりました。 次のコマンドが導入されました。 **aaa authorization http console**

機能名	プラットフォーム リリース	説明
証明書コンフィギュレーションのASDM ユーザ名	9.4(1)	ASDM の証明書認証（**http authentication-certificate**）を有効にすると、ASDMが証明書からユーザ名を抽出する方法を設定できます。また、ログインプロンプトでユーザ名を事前に入力して表示できます。 次のコマンドが導入されました。**http username-from-certificate**
改善されたワンタイムパスワード認証	9.2(1)	十分な認可特権を持つ管理者は、認証クレデンシャルを一度入力すると特権EXEC モードに移行できます。**auto-enable** オプションが **aaa authorization exec** コマンドに追加されました。 次のコマンドが変更されました。**aaa authorization exec**。
設定可能なSSH暗号機能と整合性アルゴリズム	9.1(7)/9.4(3)	ユーザはSSH暗号化を管理するときに暗号化モードを選択し、さまざまなキー交換アルゴリズムに対してHMACと暗号化を設定できます。アプリケーションに応じて、暗号の強度を強くしたり弱くする必要がある場合があります。セキュアなコピーのパフォーマンスは暗号化アルゴリズムに一部依存します。デフォルトで、ASA は 3des-cbc aes128-cbc aes192-cbc aes256-cbc aes128-ctr aes192-ctr aes256-ctr の順にアルゴリズムをネゴシエートします。提示された最初のアルゴリズム（3des-cbc）が選択された場合、aes128-cbc などの一層効率的なアルゴリズムが選択された場合よりも大幅にパフォーマンスが低下します。たとえば、提示された暗号方式に変更するには、**ssh cipher encryption custom aes128-cbc** を使用します。 次のコマンドが導入されました。**ssh cipher encryption**、**ssh cipher integrity**。

機能名	プラットフォーム リリース	説明
SSH の AES-CTR 暗号化	9.1(2)	ASA での SSH サーバの実装が、AES-CTR モードの暗号化をサポートするようになりました。
SSH キー再生成間隔の改善	9.1(2)	SSH 接続は、接続時間 60 分間またはデータ トラフィック 1 GB ごとに再生成されます。 次のコマンドが導入されました。**show ssh sessions detail**。
マルチ コンテキスト モードの ASASM において、スイッチからの Telnet 認証および仮想コンソール認証をサポートしました。	8.5(1)	マルチ コンテキスト モードのスイッチから ASASM への接続はシステム実行スペースに接続しますが、これらの接続を制御するために管理コンテキストでの認証を設定できます。
ローカルデータベースを使用する場合の管理者パスワードポリシーのサポート	8.4(4.1)、9.1(2)	ローカルデータベースを使用して CLI または ASDM アクセスの認証を設定する場合は、指定期間を過ぎるとユーザにパスワードの変更を要求し、パスワードの最短長と最低変更文字数などのパスワード標準に従うことを要求するパスワード ポリシーを設定できます。 次のコマンドが導入されました。**change-password**、**password-policy lifetime**、**password-policy minimum changes**、**password-policy minimum-length**、**password-policy minimum-lowercase**、**password-policy minimum-uppercase**、**password-policy minimum-numeric**、**password-policy minimum-special**、**password-policy authenticate enable**、**clear configure password-policy**、**show running-config password-policy**.

機能名	プラットフォーム リリース	説明
SSH 公開キー認証のサポート	8.4(4.1)、9.1(2)	ASA への SSH 接続の公開キー認証は、ユーザ単位で有効にできます。公開キー ファイル（PKF）でフォーマットされたキーまたは Base64 キーを指定できます。PKF キーは、4096 ビットまで使用できます。ASA がサポートする Base64 形式（最大 2048 ビット）では大きすぎるキーについては、PKF 形式を使用します。 次のコマンドが導入されました。**ssh authenticaion**。 *PKF* キー形式のサポートは *9.1(2)* 以降のみです。
SSH キー交換の Diffie-Hellman グループ 14 のサポート	8.4(4.1)、9.1(2)	SSH キー交換に Diffie-Hellman グループ 14 が追加されました。これまでは、グループ 1 だけがサポートされていました。 次のコマンドが導入されました。**ssh key-exchange**。
管理セッションの最大数のサポート	8.4(4.1)、9.1(2)	同時 ASDM、SSH、Telnet セッションの最大数を設定できます。 次のコマンドが導入されました。**quota management-session**、**show running-config quota management-session**、**show quota management-session**。

機能名	プラットフォーム リリース	説明
SSH セキュリティが向上し、SSH デフォルトユーザ名はサポートされなくなりました。	8.4(2)	8.4(2) 以降、pix または asa ユーザ名とログイン パスワードで SSH を使用して ASA に接続することができなくなりました。SSH を使用するには、**aaa authentication ssh console LOCAL** コマンド（CLI）または [Configuration] > [Device Management] > [Users/AAA] > [AAA Access] > [Authentication (ASDM)] を使用して AAA 認証を設定してから、ローカルユーザを定義する必要があります。定義するには、**username** コマンド（CLI）を入力するか、[Configuration] > [Device Management] > [Users/AAA] > [User Accounts (ASDM)] を選択します。ローカルデータベースの代わりに AAA サーバを認証に使用する場合、ローカル認証もバックアップの手段として設定しておくことをお勧めします。
管理アクセス	7.0(1)	この機能が導入されました。 次のコマンドを導入しました。 **show running-config all privilege all**、**show running-config privilege level**、**show running-config privilege command**、**telnet**、**telnet timeout**、**ssh**、**ssh timeout**、**http**、**http server enable**、**asdm image disk**、**banner**、**console timeout**、**icmp**、**ipv6 icmp**、**management access**、**aaa authentication console**、**aaa authentication enable console**、**aaa authentication telnet | ssh console**、**service-type**、**login**、**privilege**、**aaa authentication exec authentication-server**、**aaa authentication command LOCAL**、**aaa accounting serial | telnet | ssh | enable console**、**show curpriv**、**aaa accounting command privilege**。



第 35 章

ソフトウェアおよびコンフィギュレーション

この章では、Cisco ASA ソフトウェアおよびコンフィギュレーションの管理方法について説明します。

ソフトウェアのアップグレード

完全なアップグレードの手順については、『Cisco ASA Upgrade Guide』を参照してください。

ROMMON を使用したイメージのロード

TFTP を使用して ROMMON モードから ASA へソフトウェア イメージをロードするには、次の手順を実行します。

手順

ステップ 1 アプライアンス コンソールへのアクセス （23 ページ）に従って、ASA のコンソール ポートに接続します。

ステップ 2 ASA の電源を切ってから、再び電源をオンにします。

ステップ 3 スタートアップの間に、ROMMON モードに入るようにプロンプト表示されたら、**Escape** キーを押します。

ステップ 4 ROMMON モードで、IP アドレス、TFTP サーバ アドレス、ゲートウェイ アドレス、ソフトウェア イメージ ファイル、およびポートを含む、ASA に対するインターフェイス設定を次のように定義します。

```
rommon #1> interface gigabitethernet0/0
rommon #2> address 10.86.118.4
rommon #3> server 10.86.118.21
rommon #4> gateway 10.86.118.21
rommon #5> file asa961-smp-k8.bin
```

（注） ネットワークへの接続がすでに存在することを確認してください。

インターフェイス コマンドは ASA 5506-X、ASA 5508-X、および ASA 5516-X プラットフォームで無視されるため、これらのプラットフォームで Management 1/1 インターフェイスから TFTP リカバリを実行する必要があります。

ステップ 5 設定を検証します。

```
rommon #6> set
ROMMON Variable Settings:
  ADDRESS=10.86.118.3
  SERVER=10.86.118.21
  GATEWAY=10.86.118.21
  PORT=GigabitEthernet0/0
  VLAN=untagged
  IMAGE=asa961-smp-k8.bin
  CONFIG=
  LINKTIMEOUT=20
  PKTTIMEOUT=4
  RETRY=20
```

ステップ 6 TFTP サーバに ping を送信します。

```
rommon #7> ping server
Sending 20, 100-byte ICMP Echoes to server 10.86.118.21, timeout is 4 seconds:

Success rate is 100 percent (20/20)
```

ステップ 7 ネットワーク設定を、後で使用できるように保管しておきます。

```
rommon #8> sync
Updating NVRAM Parameters...
```

ステップ 8 システム ソフトウェア イメージをロードします。

```
rommon #9> tftpdnld
ROMMON Variable Settings:
  ADDRESS=10.86.118.3
  SERVER=10.86.118.21
  GATEWAY=10.86.118.21
  PORT=GigabitEthernet0/0
  VLAN=untagged
  IMAGE=asa961-smp-k8.bin
  CONFIG=
  LINKTIMEOUT=20
  PKTTIMEOUT=4
  RETRY=20

tftp asa961-smp-k8.bin@10.86.118.21 via 10.86.118.21

Received 14450688 bytes

Launching TFTP Image...
Cisco ASA Security Appliance admin loader (3.0) #0: Mon Mar 5 16:00:07 MST 2016

Loading...
```

ソフトウェア イメージが正常にロードされると、ASA は自動的に ROMMON モードを終了します。

ステップ 9 ROMMON モードから ASA を起動する場合、システム イメージはリロード間で保持されないため、やはりイメージをフラッシュ メモリにダウンロードする必要があります。「ソフトウェアのアップグレード （1003 ページ）」を参照してください。

ROMMON を使用した ASASM のイメージのロード

TFTP を使用して ROMMON モードから ASASM へソフトウェア イメージをロードするには、次の手順を実行します。

手順

ステップ 1 ASA サービス モジュール コンソールへのアクセス （26 ページ）に従って、ASA のコンソール ポートに接続します。

ステップ 2 ASASM イメージをリロードすることを確認してください。

ステップ 3 スタートアップの間に、ROMMON モードに入るようにプロンプト表示されたら、**Escape** キーを押します。

ステップ 4 ROMMON モードで、IP アドレス、TFTP サーバ アドレス、ゲートウェイ アドレス、ソフトウェア イメージ ファイル、ポートおよび VLAN を含む、ASASM に対するインターフェイス設定を次のように定義します。

```
rommon #2> address 10.86.118.4
rommon #3> server 10.86.118.21
rommon #4> gateway 10.86.118.21
rommon #5> file asa961-smp-k8.bin
rommon #5> interface Data0
rommon #6> vlan 1
Data0
Link is UP
MAC Address: 0012.d949.15b8
```

（注） ネットワークへの接続がすでに存在することを確認してください。

ステップ 5 設定を検証します。

```
rommon #7> set
ROMMON Variable Settings:
  ADDRESS=10.86.118.4
  SERVER=10.86.118.21
  GATEWAY=10.86.118.21
  PORT=Data0
  VLAN=1
  IMAGE=asa961-smp-k8.bin
  CONFIG=
  LINKTIMEOUT=20
  PKTTIMEOUT=2
  RETRY=20
```

ステップ 6 TFTP サーバに ping を送信します。

```
rommon #8> ping server
Sending 20, 100-byte ICMP Echoes to server 10.86.118.21, timeout is 2 seconds:

Success rate is 100 percent (20/20)
```

ステップ 7 システム ソフトウェア イメージをロードします。

```
rommon #9> tftpdnld
Clearing EOBC receive queue ...
cmostime_set = 1
ROMMON Variable Settings:
  ADDRESS=10.86.118.3
  SERVER=10.86.118.21
  GATEWAY=10.86.118.21
  PORT=Data0
  VLAN=1
  IMAGE=asa961-smp-k8.bin
  CONFIG=
  LINKTIMEOUT=20
  PKTTIMEOUT=4
  RETRY=20

tftp asa961-smp-k8.bin@10.86.118.21 via 10.86.118.21
Starting download. Press ESC to abort.
```

ソフトウェア イメージが正常にロードされると、ASASM は自動的に ROMMON モードを終了します。

ステップ 8 ROMMONモードからモジュールを起動する場合、システムイメージはリロード間で保持されないため、やはりイメージをフラッシュ メモリにダウンロードする必要があります。「ソフトウェアのアップグレード （1003 ページ）」を参照してください。

ROMMON イメージのアップグレード（ASA 5506-X、5508-X、および 5516-X）

ASA 5506-X シリーズ、ASA 5508-X、および ASA 5516-X の ROMMON イメージをアップグレードするには、次の手順に従います。システムの ROMMON バージョンは 1.1.8 以上でなければなりません。

注意 1.1.15 の ROMMON のアップグレードには、以前の ROMMON バージョンの 2 倍の時間がかかります（約 15 分）。アップグレード中はデバイスの電源を**再投入しないでください**。アップグレードが 30 分以内に完了しないか、または失敗した場合は、シスコ テクニカル サポートに連絡してください。デバイスの電源を再投入したり、リセットしたり**しないでください**。

始める前に

新バージョンへのアップグレードのみ可能です。ダウングレードはできません。現在のバージョンを確認するには、**show module** コマンドを入力して、MAC アドレス範囲テーブルの Mod 1 の出力で Fw バージョンを調べます。

```
ciscoasa# show module
[...]
Mod  MAC Address Range                 Hw Version   Fw Version   Sw Version
---- --------------------------------- ------------ ------------ ---------------
   1 7426.aceb.ccea to 7426.aceb.ccf2  0.3          1.1.5        9.4(1)
 sfr 7426.aceb.cce9 to 7426.aceb.cce9  N/A          N/A
```

手順

ステップ 1 Cisco.com から新しい ROMMON イメージを取得して、サーバ上に置いて ASA にコピーします。この手順では、TFTP コピーの方法を説明します。

次の URL からイメージをダウンロードします。

https://software.cisco.com/download/type.html?mdfid=286283326&flowid=77251

ステップ 2 ROMMON イメージを ASA フラッシュ メモリにコピーします。

copy tftp://*server_ip***/asa5500-firmware-***xxxx***.SPA disk0:asa5500-firmware-***xxxx***.SPA**

ステップ 3 ROMMON イメージをアップグレードします。

upgrade rommon disk0:asa5500-firmware-*xxxx***.SPA**

例：

```
ciscoasa# upgrade rommon disk0:asa5500-firmware-1108.SPA
Verifying file integrity of disk0:/asa5500-firmware-1108.SPA

Computed Hash   SHA2: d824bdeecee1308fc64427367fa559e9
                      eefe8f182491652ee4c05e6e751f7a4f
                      5cdea28540cf60acde3ab9b65ff55a9f
                      4e0cfb84b9e2317a856580576612f4af

Embedded Hash   SHA2: d824bdeecee1308fc64427367fa559e9
                      eefe8f182491652ee4c05e6e751f7a4f
                      5cdea28540cf60acde3ab9b65ff55a9f
                      4e0cfb84b9e2317a856580576612f4af


Digital signature successfully validated
File Name                     : disk0:/asa5500-firmware-1108.SPA
Image type                    : Release
    Signer Information
        Common Name           : abraxas
        Organization Unit     : NCS_Kenton_ASA
        Organization Name     : CiscoSystems
    Certificate Serial Number : 553156F4
    Hash Algorithm            : SHA2 512
    Signature Algorithm       : 2048-bit RSA
    Key Version               : A
Verification successful.
Proceed with reload? [confirm]
```

ステップ 4 プロンプトが表示されたら、確認して ASA をリロードします。

ASA が ROMMON イメージをアップグレードした後、ASA の OS をリロードします。

ASA 5506W-X ワイヤレス アクセス ポイントのイメージの回復およびロード

TFTP を使用してソフトウェア イメージを回復して ASA 5506W-X にロードするには、次の手順を実行します。

手順

ステップ 1 アクセス ポイント（AP）へのセッションを確立し、AP ROMMON（ASA ROMMON ではなく）を開始します。

```
ciscoasa# hw-module module wlan recover image
```

ステップ 2 Cisco Aironet アクセス ポイント Cisco IOS ソフトウェア コンフィギュレーション ガイド [英語] の手順に従います。

ソフトウェアのダウングレード

ダウングレードでは、以下の機能を完了するためのショートカットが存在します。

- ブート イメージ コンフィギュレーションのクリア（**clear configure boot**）。
- 古いイメージへのブート イメージの設定（**boot system**）。
- （オプション）新たなアクティベーション キーの入力（**activation-key**）。
- 実行コンフィギュレーションのスタートアップへの保存（**write memory**）。これにより、BOOT 環境変数を古いイメージに設定します。このため、リロードすると古いイメージがロードされます。
- スタートアップ コンフィギュレーションへの古いコンフィギュレーションのコピー（**copy old_config_url startup-config**）。
- リロード（**reload**）。

始める前に

- クラスタリング用の公式のゼロ ダウンタイム ダウングレードのサポートはありません。ただし場合によっては、ゼロ ダウンタイム ダウングレードが機能します。ダウングレードに関する次の既知の問題を参照してください。この他の問題が原因でクラスタ ユニットのリロードが必要になることもあり、その場合はダウンタイムが発生します。
  - クラスタリングを使用する場合に 9.2(1) 以降から 9.1 以前にダウングレードする：ゼロ ダウンタイム ダウングレードはサポートされません。
- PBKDF2（パスワード ベースのキー派生関数 2）ハッシュをパスワードで使用する場合に 9.5 以前のバージョンにダウングレードする：9.6 より前のバージョンは PBKDF2 ハッシュをサポートしていません。9.6(1) では、32 文字より長い **enable** パスワードおよび **username** パスワードで PBKDF2 ハッシュを使用します。ダウングレードすると、**enable** パスワードがデフォルト（空白）に戻ります。ユーザ名は正しく解析されず、**username** コマンドが削除されます。ローカル ユーザをもう一度作成する必要があります。
- ASAv 用のバージョン 9.5(2.200) からのダウングレード：ASAv はライセンス登録状態を保持しません。**license smart register idtoken id_token force** コマンドで再登録する必要があります（ASDM の場合、[Configuration] > [Device Management] > [Licensing] > [Smart Licensing] ページで [Force registration] オプションを使用）。Smart Software Manager から ID トークンを取得します。

- 設定を移行すると、ダウングレードの可否に影響を与える可能性があります。そのため、ダウングレード時に使用できる古い設定のバックアップを保持することを推奨します。8.3 へのアップグレード時には、バックアップが自動的に作成されます（<old_version>_startup_cfg.sav）。他の移行ではバックアップが作成されません。古いバージョンでは利用できなかったコマンドが新しい設定に含まれていると、設定がロードされたときにそれらのコマンドのエラーが表示されます。ただし、エラーは無視できます。各バージョンの設定の移行または廃止の詳細については、各バージョンのアップグレードガイドを参照してください。
- 元のトンネルがネゴシエートした暗号スイートをサポートしないソフトウェアバージョンをスタンバイ装置が実行している場合でも、VPN トンネルがスタンバイ装置に複製されます。このシナリオは、ダウングレード時に発生します。その場合、VPN 接続を切断して再接続してください。

手順

次のコマンドを入力します。

downgrade [**/noconfirm**] *old_image_url old_config_url* [**activation-key** *old_key*]

例：

```
ciscoasa(config)# downgrade /noconfirm disk0:/asa821-k8.bin disk0:/8_2_1_0_startup_cfg.sav
```

/noconfirm オプションを指定すると、プロンプトが表示されずにダウングレードされます。*image_url* は、disk0、disk1、tftp、ftp、または smb 上の古いイメージへのパスです。*old_config_url* は、保存された移行前の設定へのパスです。8.3 よりも前のアクティベーション キーに戻る必要がある場合は、そのアクティベーション キーを入力できます。

ファイルの管理

フラッシュ メモリ内のファイルの表示

フラッシュ メモリ内のファイルを表示して、そのファイルに関する情報を参照できます。

手順

ステップ 1 フラッシュ メモリ内のファイルを表示します。

dir [**disk0:** | **disk1:**]

例：

```
hostname# dir

Directory of disk0:/
500    -rw-  4958208     22:56:20 Nov 29 2004  cdisk.bin
2513   -rw-  4634        19:32:48 Sep 17 2004  first-backup
2788   -rw-  21601       20:51:46 Nov 23 2004  backup.cfg
2927   -rw-  8670632     20:42:48 Dec 08 2004  asdmfile.bin
```

内部フラッシュ メモリの場合、**disk0:** と入力します。**disk1:** キーワードは外部フラッシュ メモリを表します。デフォルトは、内部フラッシュ メモリです。

ステップ 2 特定のファイルに関する追加情報を表示します。

show file information [path:/]*filename*

例：

```
hostname# show file information cdisk.bin

disk0:/cdisk.bin:
  type is image (XXX) []
  file size is 4976640 bytes version 7.0(1)
```

示されているファイル サイズは例にすぎません。

デフォルト パスは、内部フラッシュ メモリのルート ディレクトリ（disk0:/）です。

フラッシュ メモリからのファイルの削除

不要になったファイルはフラッシュ メモリから削除できます。

手順

フラッシュ メモリからファイルを削除します。

delete disk0: *filename*

パスを指定しないと、デフォルトにより、ファイルは現在の作業ディレクトリから削除されます。ファイルを削除するときは、ワイルドカードを使用できます。削除するファイル名を求めるプロンプトが表示されます。その後、削除を確認する必要があります。

フラッシュ ファイル システムの削除

フラッシュ ファイル システムを消去するには、次の手順を実行します。

手順

ステップ 1 ASA サービス モジュール コンソールへのアクセス （26 ページ） または アプライアンス コンソールへのアクセス （23 ページ） の手順に従って、ASA のコンソールポートに接続します。

ステップ 2 ASA の電源を切ってから、再び電源をオンにします。

ステップ 3 スタートアップの間に、ROMMON モードに入るようにプロンプト表示されたら、**Escape** キーを押します。

ステップ 4 **erase** コマンドを入力します。これにより、すべてのファイルが上書きされてファイル システムが消去されます（非表示のシステム ファイルを含む）。

rommon #1> **erase** [**disk0:** | **disk1:** | **flash:**]

ファイル アクセスの設定

ASA では、FTP クライアント、セキュア コピー クライアント、または TFTP クライアントを使用できます。また、ASA をセキュア コピー サーバとして設定することもできるため、コンピュータでセキュア コピー クライアントを使用できます。

FTP クライアント モードの設定

ASA では、FTP サーバとの間で、イメージ ファイルやコンフィギュレーション ファイルのアップロードおよびダウンロードを実行できます。パッシブ FTP では、クライアントは制御接続およびデータ接続の両方を開始します。パッシブ モードではデータ接続の受け入れ側となるサーバは、今回の特定の接続においてリッスンするポート番号を応答として返します。

手順

FTP モードをパッシブに設定します。

ftp mode passive

例：

```
ciscoasa(config)# ftp mode passive
```

セキュア コピー サーバとしての ASA の設定

ASA 上でセキュア コピー（SCP）サーバをイネーブルにできます。SSH による ASA へのアクセスを許可されたクライアントだけが、セキュア コピー接続を確立できます。

始める前に

- サーバにはディレクトリ サポートがありません。ディレクトリ サポートがないため、ASA の内部ファイルへのリモート クライアント アクセスは制限されます。
- サーバでは、バナーまたはワイルドカードがサポートされていません。
- SSH アクセスの設定 （957 ページ） に従って、ASA で SSH を有効にします。
- SSH バージョン 2 接続をサポートするには、ASA のライセンスに強力な暗号化（3DES/AES）ライセンスが必要です。
- 特に指定されていないかぎり、マルチ コンテキスト モードでは、システム実行スペースで次の手順を実行します。コンテキストからシステム実行スペースに切り替えるには、**changeto system** コマンドを入力します。
- セキュア コピーのパフォーマンスは、使用する暗号化アルゴリズムにある程度依存します。デフォルトで、ASA は 3des-cbc aes128-cbc aes192-cbc aes256-cbc aes128-ctr aes192-ctr aes256-ctr の順にアルゴリズムをネゴシエートします。提示された最初のアルゴリズム（3des-cbc）が選択された場合、aes128-cbc などの一層効率的なアルゴリズムが選択された場合よりも大幅にパフォーマンスが低下します。提示された暗号方式を変更するには、**ssh cipher encryption** コマンド。たとえば、**ssh cipher encryption custom aes128-cbc**

手順

ステップ 1 SCP サーバをイネーブルにします。

ssh scopy enable

ステップ 2 （オプション）ASA データベースから手動でサーバとそのキーを追加または削除します。

ssh pubkey-chain [**no**] **server** *ip_address* {**key-string** *key_string* **exit**| **key-hash** {**md5** | **sha256**} *fingerprint*}

例：

```
ciscoasa(config)# ssh pubkey-chain
ciscoasa(config-ssh-pubkey-chain)# server 10.7.8.9
ciscoasa(config-ssh-pubkey-server)# key-string
Enter the base 64 encoded RSA public key.
End with the word "exit" on a line by itself
ciscoasa(config-ssh-pubkey-server-string)# c1:b1:30:29:d7:b8:de:6c:97:77:10:d7:46:41:63:87
ciscoasa(config-ssh-pubkey-server-string)# exit
ciscoasa(config-ssh-pubkey-server)# show running-config ssh pubkey-chain
ssh pubkey-chain
  server 10.7.8.9
    key-hash sha256 f1:22:49:47:b6:76:74:b2:db:26:fb:13:65:d8:99:19:
e7:9e:24:46:59:be:13:7f:25:27:70:9b:0e:d2:86:12
```

ASA は接続先の各 SCP サーバの SSH ホストキーを保存します。必要に応じて、手動でキーを管理できます。

各サーバについて、SSH ホストの **key-string**（公開キー） または **key-hash**（ハッシュ値）を指定できます。

key_string はリモート ピアの Base64 で符号化された RSA 公開キーです。オープン SSH クライアントから（言い換えると .ssh/id_rsa.pub ファイルから）公開キー値を取得できます。Base64 で符号化された公開キーを送信した後、SHA-256 によってそのキーがハッシュされます。

key-hash {**md5** | **sha256**} *fingerprint* では、たとえば、**show** コマンドの出力からコピーしたキーなどの、すでにハッシュされているキー（MD5 または SHA-256 キーを使用）が入力されます。

ステップ 3 （任意） SSH ホスト キー チェックを有効または無効にします。マルチ コンテキスト モードでは、管理コンテキストでこのコマンドを入力します。

[**no**] **ssh stricthostkeycheck**

例：

```
ciscoasa# ssh stricthostkeycheck
ciscoasa# copy x scp://cisco@10.86.95.9/x
The authenticity of host '10.86.95.9 (10.86.95.9)' can't be established.
RSA key fingerprint is dc:2e:b3:e4:e1:b7:21:eb:24:e9:37:81:cf:bb:c3:2a.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '10.86.95.9' (RSA) to the list of known hosts.
Source filename [x]?

Address or name of remote host [10.86.95.9]?

Destination username [cisco]?

Destination password []? cisco123

Destination filename [x]?
```

デフォルトで、このオプションは有効になっています。このオプションがイネーブルになっている場合、ASA にまだ格納されていないホストキーを許可または拒否するように求められます。このオプションがディセーブルになっている場合、ASA は過去に保存されたことがないホストキーを自動的に許可します。

例

外部ホストのクライアントから、SCP ファイル転送を実行します。たとえば、Linux では次のコマンドを入力します。

scp -v -pw *password source_filename username@asa_address***:{disk0|disk1}:/***dest_filename*

-v は冗長を表します。**-pw** が指定されていない場合は、パスワードの入力を求めるプロンプトが表示されます。

次に、10.86.94.170 にあるサーバのすでにハッシュされているホスト キーを追加する例を示します。

```
ciscoasa(config)# ssh pubkey-chain
ciscoasa(config-ssh-pubkey-chain)# server 10.86.94.170
ciscoasa(config-ssh-pubkey-server)# key-hash sha256 65:d9:9d:fe:1a:bc:61:aa:
64:9d:fc:ee:99:87:38:df:a8:8e:d9:e9:ff:42:de:e8:8d:2d:bf:a9:2b:85:2e:19
```

次に、10.7.8.9 にあるサーバのホスト ストリング キーを追加する例を示します。

```
ciscoasa(config)# ssh pubkey-chain
ciscoasa(config-ssh-pubkey-chain)# server 10.7.8.9
ciscoasa(config-ssh-pubkey-server)# key-string
Enter the base 64 encoded RSA public key.
End with the word "exit" on a line by itself
ciscoasa(config-ssh-pubkey-server-string)# c1:b1:30:29:d7:b8:de:6c:97:77:10:d7:
46:41:63:87
ciscoasa(config-ssh-pubkey-server-string)# exit
```

ASA TFTP クライアントのパス設定

TFTP は、単純なクライアント/サーバ ファイル転送プロトコルで、RFC 783 および RFC 1350 Rev. 2 で規定されています。TFTP サーバとの間でファイルをコピーできるように、ASA を TFTP クライアントとして設定できます。これにより、コンフィギュレーション ファイルをバックアップし、それらを複数の ASA にプロパゲートできます。

ここでは、TFTP サーバへのパスを事前定義できるため、**copy** および **configure net** などのコマンドで入力する必要がなくなります。

手順

---

configure net および **copy** コマンドで使用するために、TFTP サーバのアドレスおよびファイル名を事前定義します。

tftp-server *interface_name server_ip filename*

例：

```
ciscoasa(config)# tftp-server inside 10.1.4.7 files/config1.cfg
ciscoasa(config)# copy tftp: test.cfg

Address or name of remote host [10.1.4.7]?

Source filename [files/config1.cfg]?config2.cfg

Destination filename [test.cfg]?

Accessing tftp://10.1.4.7/files/config2.cfg;int=outside...
```

コマンドを入力するとファイル名を上書きできます。たとえば、**copy** コマンドを使用するときに事前定義された TFTP サーバのアドレスを利用できますが、インタラクティブ プロンプトでファイル名を入力することもできます。

copy コマンドに、**tftp:**//*url* ではなく **tftp:** を入力して tftp-server の値を使用します。

ASA へのファイルのコピー

この項では、アプリケーションイメージ、ASDM ソフトウェア、コンフィギュレーション ファイル、または TFTP、FTP、SMB、HTTP、HTTPS、または SCP サーバから内部または外部フラッシュ メモリにダウンロードする必要があるその他のファイルをコピーする方法について説明します。

始める前に

- IPS SSP ソフトウェア モジュールの場合、IPS ソフトウェアを disk0 にダウンロードする前に、フラッシュ メモリに少なくとも 50% の空きがあることを確認してください。IPS をインストールするときに、IPS のファイル システム用に内部フラッシュ メモリの 50% が予約されます。
- 文字の大文字と小文字が異なっていても、同じ名前の 2 つのファイルをフラッシュ メモリの同じディレクトリに保存できません。たとえば、config.cfg というファイルが存在する場所に Config.cfg というファイルをダウンロードしようとすると、次のエラー メッセージが表示されます。

```
%Error opening disk0:/Config.cfg (File exists)
```

- Cisco SSL VPN Client をインストールする方法の詳細については、『*Cisco AnyConnect VPN Client Administrator Guide*』を参照してください。ASA に Cisco Secure Desktop をインストールする方法の詳細については、『*Cisco Secure Desktop Configuration Guide for Cisco ASA 5500 Series Administrators*（*Cisco ASA 5500* シリーズ管理者向け *Cisco Secure Desktop* コンフィギュレーション ガイド）』を参照してください。
- 複数のイメージがインストールされている場合、または外部フラッシュ メモリにイメージがインストールされている場合に特定のアプリケーション イメージまたは ASDM イメージを使用するように ASA を設定するには、ASA イメージ、ASDM、およびスタートアップ コンフィギュレーションの設定 （1020 ページ）を参照してください。
- マルチ コンテキスト モードの場合は、システム実行スペース内にいる必要があります。

手順

次のサーバ タイプの 1 つを使用してファイルをコピーします。

- TFTP サーバからコピーします。

  copy [**/noconfirm**] **tftp://***server*[*/path*]*/src_filename* {**disk0**|**disk1**}**:/**[*path*/]*dest_filename*

  例：

```
ciscoasa# copy tftp://10.1.1.67/files/context1.cfg disk0:/context1.cfg

Address or name of remote host [10.1.1.67]?

Source filename [files/context1.cfg]?
```

```
Destination filename [context1.cfg]?
Cryptochecksum: db8ba196 9ad189a8 7f5f501f 1bec469b
!!!!!!!!!!!
11143 bytes copied in 5.710 secs (2228 bytes/sec)
```

- FTP サーバからコピーします。

  copy [**/noconfirm**] **ftp:**//[*user*[**:***password*]**@**]*server*[*/path*]/*src_filename* {**disk0**|**disk1**}**:/**[*path*/]*dest_filename*

  例：

```
ciscoasa# copy ftp://jcrichton:aeryn@10.1.1.67/files/context1.cfg
disk0:/contexts/context1.cfg

Address or name of remote host [10.1.1.67]?

Source username [jcrichton]?

Source password [aeryn]?

Source filename [files/context1.cfg]?

Destination filename [contexts/context1.cfg]?
Cryptochecksum: db8ba196 9ad189a8 7f5f501f 1bec469b
!!!!!!!!!!!
11143 bytes copied in 5.710 secs (2228 bytes/sec)
```

- HTTP（S） サーバからコピーします。

  copy [**/noconfirm**] **http**[**s**]**:**//[*user*[**:***password*]**@**]*server*[**:***port*][*/path*]/*src_filename* {**disk0**|**disk1**}**:/**[*path*/]*dest_filename*

  例：

```
ciscoasa# copy https://asun:john@10.1.1.67/files/moya.cfg disk0:/contexts/moya.cfg

Address or name of remote host [10.1.1.67]?

Source username [asun]?

Source password [john]?

Source filename [files/moya.cfg]?

Destination filename [contexts/moya.cfg]?
Cryptochecksum: db8ba196 9ad189a8 7f5f501f 1bec469b
!!!!!!!!!!!
11143 bytes copied in 5.710 secs (2228 bytes/sec)
```

- SMB サーバからコピーします。

  copy [**/noconfirm**] **smb:**//[*user*[**:***password*]**@**]*server*[*/path*]/*src_filename* {**disk0**|**disk1**}**:/**[*path*/]*dest_filename*

  例：

```
ciscoasa# copy /noconfirm smb://chiana:dargo@10.1.1.67/test.xml disk0:/test.xml

Cryptochecksum: db8ba196 9ad189a8 7f5f501f 1bec469b
!!!!!!!!!!!
11143 bytes copied in 5.710 secs (2228 bytes/sec)
```

- SCP サーバからコピーします。

  ;int=*interface* オプションは、ルート ルックアップをバイパスして、常に指定されたインターフェイスを使用して SCP サーバに到達します。

  copy [**/noconfirm**] **scp://**[*user*[**:***password*]**@**]*server*[*/path*]*/src_filename*[**;int=***interface_name*] {**disk0**|**disk1**}**:/**[*path/*]*dest_filename*

  例：

```
ciscoasa# copy scp://pilot@10.86.94.170/test.cfg disk0:/test.cfg

Address or name of remote host [10.86.94.170]?

Source username [pilot]?

Destination filename [test.cfg]?

The authenticity of host '10.86.94.170 (10.86.94.170)' can't be established.
RSA key fingerprint is
<65:d9:9d:fe:1a:bc:61:aa:64:9d:fc:ee:99:87:38:df:a8:8e:d9:e9:ff:42:de:e8:8d:2d:bf:a9:2b:85:2e:19>(SHA256).
Are you sure you want to continue connecting (yes/no)? yes

Please use the following commands to add the hash key to the configuration:
  ssh pubkey-chain
    server 10.86.94.170
      key-hash sha256
65:d9:9d:fe:1a:bc:61:aa:64:9d:fc:ee:99:87:38:df:a8:8e:d9:e9:ff:42:de:e8:8d:2d:bf:a9:2b:85:2e:19


Password: <type in password>
!!!!!!
6006 bytes copied in 8.160 secs (750 bytes/sec)
```

スタートアップコンフィギュレーションまたは実行コンフィギュレーションへのファイルのコピー

テキストファイルは、TFTP、FTP、SMB、HTTP（S）、またはSCPサーバから、またはフラッシュ メモリから、実行コンフィギュレーションまたはスタートアップ コンフィギュレーションにダウンロードできます。

始める前に

コンフィギュレーションを実行コンフィギュレーションにコピーするには、2つのコンフィギュレーションをマージします。マージによって、新しいコンフィギュレーションから実行コン

フィギュレーションに新しいコマンドが追加されます。コンフィギュレーションが同じ場合、変更は発生しません。コマンドが衝突する場合、またはコマンドがコンテキストの実行に影響を与える場合、マージの結果はコマンドによって異なります。エラーが発生することも、予期できない結果が生じることもあります。

手順

スタートアップ コンフィギュレーションまたは実行コンフィギュレーションにファイルをコピーするには、適切なダウンロード サーバに対して次のコマンドのいずれかを入力します。

- TFTP サーバからコピーします。

  copy [**/noconfirm**] **tftp://***server*[*/path*]*/src_filename* {**startup-config** | **running-config**}

  例：

  ```
  ciscoasa# copy tftp://10.1.1.67/files/old-running.cfg running-config
  ```

- FTP サーバからコピーします。

  copy [**/noconfirm**] **ftp://**[*user*[**:***password*]**@**]*server*[*/path*]*/src_filename* {**startup-config** | **running-config**}

  例：

  ```
  ciscoasa# copy ftp://jcrichton:aeryn@10.1.1.67/files/old-startup.cfg startup-config
  ```

- HTTP（S） サーバからコピーします。

  copy [**/noconfirm**] **http**[**s**]**://**[*user*[**:***password*]**@**]*server*[**:***port*][*/path*]*/src_filename* {**startup-config** | **running-config**}

  例：

  ```
  ciscoasa# copy https://asun:john@10.1.1.67/files/new-running.cfg running-config
  ```

- SMB サーバからコピーします。

  copy [**/noconfirm**] **smb://**[*user*[**:***password*]**@**]*server*[*/path*]*/src_filename* {**startup-config** | **running-config**}

  例：

  ```
  ciscoasa# copy /noconfirm smb://chiana:dargo@10.1.1.67/new-running.cfg running-config
  ```

- SCP サーバからコピーします。

  copy [**/noconfirm**] **scp://**[*user*[**:***password*]**@**]*server*[*/path*]*/src_filename*[**;int=***interface_name*] {**startup-config** | **running-config**}

例：

```
ciscoasa# copy scp://pilot:moya@10.86.94.170/new-startup.cfg startup-config
```

;int=*interface* オプションは、ルート ルックアップをバイパスして、常に指定されたインターフェイスを使用して SCP サーバに到達します。

例

たとえば、TFTP サーバからコンフィギュレーションをコピーするには、次のコマンドを入力します。

```
ciscoasa# copy tftp://209.165.200.226/configs/startup.cfg startup-config
```

FTP サーバからコンフィギュレーションをコピーするには、次のコマンドを入力します。

```
ciscoasa# copy ftp://admin:letmein@209.165.200.227/configs/startup.cfg startup-config
```

HTTP サーバからコンフィギュレーションをコピーするには、次のコマンドを入力します。

```
ciscoasa# copy http://209.165.200.228/configs/startup.cfg startup-config
```

ASA イメージ、ASDM、およびスタートアップ コンフィギュレーションの設定

複数の ASA または ASDM イメージがある場合は、ブートするイメージを指定する必要があります。イメージを設定しない場合はデフォルトのブートイメージが使用され、そのイメージは意図されたものではない可能性があります。スタートアップ コンフィギュレーションでは、コンフィギュレーション ファイルを任意で指定できます。

次のモデルのガイドラインを参照してください。

- Firepower 9300 シャーシ：ASA のアップグレードは FXOS によって管理されます。ASA オペレーティング システム内で ASA をアップグレードすることはできません。したがって、この手順を ASA イメージに使用しないでください。ASA と FXOS を別々にアップグレードすることができ、FXOS ディレクトリ リストに別々にリストされます。ASA パッケージには常に ASDM が含まれています。

- Firepower 2100：ASA、ASDM、および FXOS のイメージは 1 つのパッケージに一緒にバンドルされています。パッケージ更新は FXOS によって管理されます。ASA オペレーティング システム内で ASA をアップグレードすることはできません。したがって、この手順を ASA イメージに使用しないでください。ASA と FXOS を個別にアップグレードすることはできません。常にバンドルされています。
- Firepower モデルの ASDM：ASDM は ASA オペレーティング システム内からアップグレードできるため、バンドルされた ASDM イメージのみを使用する必要はありません。手動でアップロードする ASDM イメージは FXOS イメージリストに表示されません。ASA から ASDM イメージを管理する必要があります。

（注） ASA バンドルをアップグレードすると、同じ名前（**asdm.bin**）であるため、バンドル内の ASDM イメージが ASA 上の前の ASDM バンドルイメージに置き換わります。ただし、アップロードした別の ASDM イメージ（たとえば **asdm-782.bin**）を手動で選択すると、バンドルアップグレード後も引き続き同じイメージが使用されます。互換性のある ASDM バージョンを実行していることを確認するには、バンドルをアップグレードする前に ASDM をアップグレードするか、または ASA バンドルをアップグレードする直前に、バンドルされた ASDM イメージ（**asdm.bin**）を使用するように ASA を再設定する必要があります。

- ASAv：初期展開の ASAv パッケージでは、ASA イメージが読み取り専用 boot:/ パーティションに配置されます。ASAv をアップグレードするときは、フラッシュ メモリに別のイメージを指定します。後でコンフィギュレーションをクリアすると（**clear configure all**）、ASAv は元の展開のイメージをロードするようになることに注意してください。初期展開の ASAv パッケージには、フラッシュ メモリに配置される ASDM イメージも含まれています。ASDM イメージを個別にアップグレードできます。

次のデフォルト設定を参照してください。

- ASA イメージ：
  - 物理 ASA：内部フラッシュ メモリ内で見つかった最初のアプリケーション イメージをブートします。
  - ASAv：最初に展開したときに作成された、読み取り専用の boot:/ パーティションにあるイメージをブートします。
  - Firepower 9300 シャーシ：どの ASA イメージをブートするかは FXOS システムによって決定されます。この手順を使用して ASA イメージを設定することはできません。
- すべての ASA の ASDM イメージ：内部フラッシュ メモリ内で見つかった（またはここにイメージがない場合は、外部フラッシュ メモリ内で見つかった）最初の ASDM イメージをブートします。

- スタートアップ コンフィギュレーション：デフォルトでは、ASA は、隠しファイルであるスタートアップ コンフィギュレーションからブートします。

手順

ステップ 1 ASA ブート イメージの場所を設定します。

boot system *url*

例：

```
ciscoasa(config)# boot system disk0:/images/asa921.bin
```

URL は次のようになります。

- {**disk0:/** | **disk1:/**}[*path*/]*filename*
- **tftp:**//[*user*[**:***password*]**@**]*server*[**:***port*]/[*path*/]*filename*

  TFTP オプションは、すべてのモデルでサポートされるわけではありません。

最大 4 つの **boot system** コマンド エントリを入力して、ブートする複数のイメージを順番に指定することができます。ASA は、最初に検出に成功したイメージをブートします。**boot system** コマンドを入力すると、エントリがリストの最後に追加されます。ブートエントリの順序を変更するには、**clear configure boot system** コマンドを使用してすべてのエントリを削除してから、エントリを目的の順序で再入力する必要があります。設定できる **boot system tftp** コマンドは 1 つだけです。これは、最初に設定する必要があります。

（注） ASA が連続ブートのサイクルから抜け出せない場合は、ASA を ROMMON モードにリブートします。ROMMON モードの詳細については、デバッグ メッセージの表示（1069 ページ）を参照してください。

ステップ 2 ブートする ASDM イメージを設定します。

asdm image {**disk0:/** | **disk1:/**}[*path*/]*filename*

例：

```
ciscoasa(config)# asdm image disk0:/images/asdm721.bin
```

ブートするイメージを指定しない場合、インストールされているイメージが 1 つしかなくても、ASA によって **asdm image** コマンドが実行コンフィギュレーションに挿入されます。Auto Update（設定されている場合）の問題を避けるため、また起動時ごとのイメージ検索を回避するため、ブートする ASDM イメージをスタートアップ コンフィギュレーションで指定する必要があります。

ステップ 3 （オプション）スタートアップ コンフィギュレーションをデフォルトの隠しファイルではなく既知のファイルになるように設定します。

boot config {**disk0:/** | **disk1:/**}[*path*/]*filename*

例：

```
ciscoasa(config)# boot config disk0:/configs/startup1.cfg
```

コンフィギュレーションまたはその他のファイルのバックアップおよび復元

システム障害から保護するために、コンフィギュレーションおよびその他のファイルの定期的なバックアップを実行することを推奨します。

完全なシステム バックアップまたは復元の実行

次の手順では、コンフィギュレーションおよびイメージの zipバックアップ tar.gz ファイルへのバックアップおよび復元方法と、そのファイルのローカル コンピュータへの転送方法について説明します。

バックアップまた復元を開始する前に

- バックアップまたは復元を開始する前に、バックアップまたは復元場所に使用可能なディスク領域が少なくとも 300 MB ある必要があります。
- バックアップ中またはバックアップ後にコンフィギュレーションを変更した場合、その変更内容はバックアップに含められません。バックアップの実行後にコンフィギュレーションを変更してから復元を実行した場合、このコンフィギュレーションの変更は上書きされます。結果として、ASA は異なる挙動をすることもあります。
- 一度に開始できるバックアップまたは復元は 1 つだけです。
- コンフィギュレーションは、元のバックアップを実行したときと同じ ASA バージョンにのみ復元できます。復元ツールを使用して、ASA の異なるバージョン間でコンフィギュレーションを移行することはできません。コンフィギュレーションの移行が必要な場合、ASA は、新しい ASA OS をロードした時に常駐するスタートアップ コンフィギュレーションを自動的にアップグレードします。
- クラスタリングを使用する場合、バックアップまたは復元できるのは、スタートアップ コンフィギュレーション、実行コンフィギュレーション、およびアイデンティティ証明書のみです。ユニットごとに別々にバックアップを作成および復元する必要があります。
- フェールオーバーを使用する場合、バックアップの作成および復元は、アクティブ ユニットとスタンバイ ユニットに対して別々に行う必要があります。
- ASA にマスター パスフレーズを設定している場合は、この手順で作成したバックアップ コンフィギュレーションの復元時にそのマスター パスフレーズが必要となります。ASA

のマスターパスフレーズが不明な場合は、マスターパスフレーズの設定（590ページ）を参照して、バックアップを続行する前に、マスターパスフレーズをリセットする方法を確認してください。

- PKCS12 データをインポート（**crypto ca trustpoint** コマンドを使用）する際にトラストポイントが RSA キーを使用している場合、インポートされたキー ペアにはトラストポイントと同じ名前が割り当てられます。この制約のため、ASDM コンフィギュレーションを復元した後でトラストポイントおよびそのキー ペアに別の名前を指定した場合、スタートアップ コンフィギュレーションは元のコンフィギュレーションと同じになるのに、実行コンフィギュレーションには異なるキー ペア名が含まれることになります。つまり、キー ペアとトラストポイントに別の名前を使用した場合は、元のコンフィギュレーションを復元できないということです。この問題を回避するため、トラストポイントとそのキーペアには必ず同じ名前を使用してください。
- CLI を使用してバックアップしてから ASDM を使用して復元したり、その逆を行うことはできません。
- 各バックアップ ファイルに含まれる内容は次のとおりです。
  - 実行コンフィギュレーション
  - スタートアップ コンフィギュレーション
  - すべてのセキュリティ イメージ

    Cisco Secure Desktop およびホスト スキャンのイメージ

    Cisco Secure Desktop およびホスト スキャンの設定

    AnyConnect（SVC）クライアントのイメージおよびプロファイル

    AnyConnect（SVC）のカスタマイズおよびトランスフォーム
  - アイデンティティ証明書（アイデンティティ証明書に関連付けられた RSA キー ペアは含まれるが、スタンドアロン キーは除外される）
  - VPN 事前共有キー
  - SSL VPN コンフィギュレーション
  - アプリケーション プロファイルのカスタム フレームワーク（APCF）
  - ブックマーク
  - カスタマイゼーション
  - ダイナミック アクセス ポリシー（DAP）
  - プラグイン
  - 接続プロファイル用の事前入力スクリプト
  - プロキシ自動設定
  - 変換テーブル

- Web コンテンツ
- バージョン情報

システムのバックアップ

この手順では、完全なシステム バックアップを実行する方法について説明します。

手順

ステップ 1 システムをバックアップします。

backup [/**noconfirm**] [**context** *ctx-name*] [**interface** *name*] [**passphrase** *value*] [**location** *path*]

例：

```
ciscoasa# backup location disk0:/sample-backup]
Backup location [disk0:/sample-backup]?
```

システム実行スペースからのマルチ コンテキスト モードで、**context** キーワードを入力して、指定したコンテキストをバックアップします。各コンテキストは個別にバックアップする必要があります。つまり、ファイルごとに **backup** コマンドを再入力する必要があります。

VPN 証明書および事前共有キーのバックアップ中、証明書を符号化するために、**passphrase** キーワードで指定された秘密キーが必要です。PKCS12 形式の証明書を符号化および復号化するために使用するパスフレーズを入力する必要があります。バックアップに含まれるのは証明書に関連する RSA キー ペアだけであり、スタンドアロン証明書は除外されます。

バックアップの **location** にはローカル ディスクまたはリモート URL を指定できます。location を指定しない場合は、次のデフォルト名が使用されます。

- シングル モード：disk0:*hostname*.backup.*timestamp*.tar.gz
- マルチ モード：disk0:*hostname*.context-*ctx-name*.backup.*timestamp*.tar.gz

ステップ 2 プロンプトに従います。

例：

```
ciscoasa# backup location disk0:/sample-backup
Backup location [disk0:/sample-backup]?

Begin backup…
Backing up [ASA version] … Done!
Backing up [Running Config] … Done!
Backing up [Startup Config]  … Done!

Enter a passphrase to encrypt identity certificates. The default is cisco.
You will be required to enter the same passphrase while doing a restore: cisco
Backing up [Identity Certificates] … Done!

IMPORTANT: This device uses master passphrase encryption. If this backup file
is used to restore to a device with a different master passphrase,
```

```
you will need to provide the current master passphrase during restore.
Backing up [VPN Pre-shared keys] … Done!
Backing up [SSL VPN Configurations: Application Profile Custom Framework] … Done!
Backing up [SSL VPN Configurations: Bookmarks]… Done!
Backing up [SSL VPN Configurations: Customization] … Done!
Backing up [SSL VPN Configurations: Dynamic Access Policy] … Done!
Backing up [SSL VPN Configurations: Plug-in] … Done!
Backing up [SSL VPN Configurations: Pre-fill scripts for Connection Profile] … Done!
Backing up [SSL VPN Configurations: Proxy auto-config] … Done!
Backing up [SSL VPN Configurations: Translation table] … Done!
Backing up [SSL VPN Configurations: Web Content] … Done!
Backing up [Anyconnect(SVC) client images and profiles] … Done!
Backing up [Anyconnect(SVC) customizations and transforms] … Done!
Backing up [Cisco Secure Desktop and Host Scan images] … Done!
Backing up [UC-IME tickets] … Done!
Compressing the backup directory ... Done!
Copying Backup ... Done!
Cleaning up ... Done!
Backup finished!
```

バックアップの復元

zip tar.gz ファイルからローカル PC に復元するコンフィギュレーションやイメージを指定します。

手順

ステップ 1 バックアップ ファイルからシステムを復元します。

restore [**/noconfirm**] [**context** *ctx-name*] [**passphrase** *value*] [**location** *path*]

例：

```
ciscoasa# restore location disk0:/5525-2051.backup.2014-07-09-223$
restore location [disk0:/5525-2051.backup.2014-07-09-223251.tar.gz]?
```

context キーワードを使用して複数のコンテキストを復元する場合、バック アップされた各コンテキスト ファイルは個別に復元する必要があります。つまり、**restore** コマンドをファイルごとに再入力する必要があります。

ステップ 2 プロンプトに従います。

例：

```
ciscoasa# restore location disk0:/5525-2051.backup.2014-07-09-223$
restore location [disk0:/5525-2051.backup.2014-07-09-223251.tar.gz]?

Copying Backup file to local disk... Done!
Extracting the backup file ... Done!
Warning: The ASA version of the device is not the same as the backup version,
some configurations might not work after restore!
 Do you want to continue? [confirm] y
Begin restore ...
IMPORTANT: This backup configuration uses master passphrase encryption.
```

```
Master passphrase is required to restore running configuration,
startup configuration and VPN pre-shared keys.
Backing up [VPN Pre-shared keys] … Done!
Backing up [SSL VPN Configurations: Application Profile Custom Framework] … Done!
Backing up [SSL VPN Configurations: Bookmarks]… Done!
Backing up [SSL VPN Configurations: Customization] … Done!
Backing up [SSL VPN Configurations: Dynamic Access Policy] … Done!
Backing up [SSL VPN Configurations: Plug-in] … Done!
Backing up [SSL VPN Configurations: Pre-fill scripts for Connection Profile] … Done!
Backing up [SSL VPN Configurations: Proxy auto-config] … Done!
Backing up [SSL VPN Configurations: Translation table] … Done!
Backing up [SSL VPN Configurations: Web Content] … Done!
Backing up [Anyconnect(SVC) client images and profiles] … Done!
Backing up [Anyconnect(SVC) customizations and transforms] … Done!
Backing up [Cisco Secure Desktop and Host Scan images] … Done!
Backing up [UC-IME tickets] … Done!
Restoring [Running Configuration]
Following messages are as a result of applying the backup running-configuration to
this device, please note them for future reference.

ERROR: Interface description was set by failover and cannot be changed
ERROR: Unable to set this url, it has already been set
Remove the first instance before adding this one
INFO: No change to the stateful interface
Failed to update LU link information
.Range already exists.
WARNING: Advanced settings and commands should only be altered or used
under Cisco supervision.
ERROR: Failed to apply media termination address 198.0.1.228 to interface outside,
the IP is already used as media-termination address on interface outside.
ERROR: Failed to apply media termination address 198.0.0.223 to interface inside,
the IP is already used as media-termination address on interface inside.
WARNING: PAC settings will override http- and https-proxy configurations.
Do not overwrite configuration file if you want to preserve the old http-
and https-proxy configurations.

Cryptochecksum (changed): 98d23c2c ccb31dc3 e51acf88 19f04e28
 Done!
Restoring UC-IME ticket ... Done!
Enter the passphrase used while backup to encrypt identity certificates.
The default is cisco. If the passphrase is not correct, certificates will not be restored.

No passphrase was provided for identity certificates.
Using the default value: cisco. If the passphrase is not correct,
certificates will not be restored.
Restoring Certificates ...
Enter the PKCS12 data in base64 representation....
ERROR: A keypair named Main already exists.
INFO: Import PKCS12 operation completed successfully
. Done!
Cleaning up ... Done!
Restore finished!
```

シングル モード コンフィギュレーションまたはマルチ モード システム コンフィギュレーションのバックアップ

シングルコンテキスト モードで、またはマルチモードのシステム コンフィギュレーションから、スタートアップ コンフィギュレーションまたは実行コンフィギュレーションを外部サーバまたはローカル フラッシュ メモリにコピーできます。

手順

次のサーバ タイプの 1 つを使用してコンフィギュレーションをバックアップします。

- TFTP サーバにコピーします。

  copy [**/noconfirm**] {**startup-config** | **running-config**} **tftp:**//*server*[/*path*]/*dst_filename*

  例：

  ```
  ciscoasa# copy running-config tftp://10.1.1.67/files/new-running.cfg
  ```

- FTP サーバにコピーします。

  copy [**/noconfirm**] {**startup-config** | **running-config**}
  ftp://[*user*[**:***password*]**@**]*server*[/*path*]/*dst_filename*

  例：

  ```
  ciscoasa# copy startup-config ftp://jcrichton:aeryn@10.1.1.67/files/new-startup.cfg
  ```

- SMB サーバにコピーします。

  copy [**/noconfirm**] {**startup-config** | **running-config**}
  smb://[*user*[**:***password*]**@**]*server*[/*path*]/*dst_filename*

  例：

  ```
  ciscoasa# copy /noconfirm running-config smb://chiana:dargo@10.1.1.67/new-running.cfg
  ```

- SCP サーバにコピーします。

  copy [**/noconfirm**] {**startup-config** | **running-config**}
  scp://[*user*[**:***password*]**@**]*server*[/*path*]/*dst_filename*[**;int=***interface_name*]

  例：

  ```
  ciscoasa# copy startup-config
  scp://pilot:moya@10.86.94.170/new-startup.cfg
  ```

;int=*interface* オプションは、ルート ルックアップをバイパスして、常に指定されたインターフェイスを使用して SCP サーバに到達します。

- ローカル フラッシュ メモリにコピーします。

  copy [**/noconfirm**] {**startup-config** | **running-config**} {**disk0**|**disk1**}**:/**[*path*/]*dst_filename*

  例：

  ```
  ciscoasa# copy /noconfirm running-config disk0:/new-running.cfg
  ```

  宛先ディレクトリが存在することを確認してください。存在しない場合は、まず **mkdir** コマンドを使用してディレクトリを作成します。

フラッシュ メモリ内のコンテキスト コンフィギュレーションまたはその他のファイルのバック アップ

システム実行スペースで次のいずれかのコマンドを入力することによって、ローカル フラッシュ メモリにあるコンテキスト コンフィギュレーションまたは他のファイルをコピーします。

手順

次のサーバ タイプの 1 つを使用してコンテキスト コンフィギュレーション バックアップをバックアップします。

- フラッシュから TFTP サーバにコピーします。

  copy [**/noconfirm**] {**disk0**|**disk1**}**:/**[*path*/]*src_filename* **tftp://***server*[/*path*]/*dst_filename*

  例：

  ```
  ciscoasa# copy disk0:/asa-os.bin tftp://10.1.1.67/files/asa-os.bin
  ```

- フラッシュから FTP サーバにコピーします。

  copy [**/noconfirm**] {**disk0**|**disk1**}**:/**[*path*/]*src_filename*
  ftp://[*user*[**:***password*]**@**]*server*[/*path*]/*dst_filename*

  例：

  ```
  ciscoasa# copy disk0:/asa-os.bin ftp://jcrichton:aeryn@10.1.1.67/files/asa-os.bin
  ```

- フラッシュから SMB サーバにコピーします。

  copy [**/noconfirm**] {**disk0**|**disk1**}**:/**[*path*/]*src_filename*
  smb://[*user*[**:***password*]**@**]*server*[/*path*]/*dst_filename*

例：

```
ciscoasa# copy /noconfirm copy disk0:/asdm.bin
smb://chiana:dargo@10.1.1.67/asdm.bin
```

- フラッシュから SCP サーバにコピーします。

  copy [**/noconfirm**] {**disk0**|**disk1**}**:/**[*path*/]*src_filename*
  scp://[*user*[**:***password*]**@**]*server*[*/path*]*/dst_filename*[**;int=***interface_name*]

  例：

  ```
  ciscoasa# copy disk0:/context1.cfg
  scp://pilot:moya@10.86.94.170/context1.cfg
  ```

  ;int=*interface* オプションは、ルート ルックアップをバイパスして、常に指定されたインターフェイスを使用して SCP サーバに到達します。

- フラッシュからローカル フラッシュ メモリにコピーします。

  copy [**/noconfirm**] {**disk0**|**disk1**}**:/**[*path*/]*src_filename* {**disk0**|**disk1**}**:/**[*path*/]*dst_filename*

  例：

  ```
  ciscoasa# copy /noconfirm disk1:/file1.cfg disk0:/file1.cfgnew-running.cfg
  ```

  宛先ディレクトリが存在することを確認してください。存在しない場合は、まず **mkdir** コマンドを使用してディレクトリを作成します。

コンテキスト内でのコンテキスト コンフィギュレーションのバックアップ

マルチ コンテキスト モードでは、コンテキスト内から次のバックアップを実行できます。

手順

ステップ 1 （admin コンテキストに接続された）スタートアップ コンフィギュレーション サーバに実行コンフィギュレーションをコピーします。

```
ciscoasa/contexta# copy running-config startup-config
```

ステップ 2 コンテキスト ネットワークに接続された TFTP サーバに実行コンフィギュレーションをコピーします。

```
ciscoasa/contexta# copy running-config tftp:/server[/path]/filename
```

端末ディスプレイからのコンフィギュレーションのコピー

手順

ステップ 1 コンフィギュレーションを端末に表示します。

more system:running-config

ステップ 2 コマンドから出力をコピーして、コンフィギュレーションをテキスト ファイルに貼り付けます。

export および import コマンドを使用した追加ファイルのバックアップ

コンフィギュレーションに欠かせない追加ファイルは次のとおりです。

- **import webvpn** コマンドを使用してインポートするファイル。現在これらのファイルには、カスタマイゼーション、URL リスト、Web コンテンツ、プラグイン、および言語翻訳などがあります。
- DAP ポリシー（dap.xml）。
- CSD コンフィギュレーション（data.xml）。
- デジタル キーおよびデジタル証明書。
- ローカル CA ユーザ データベース ファイルと証明書ステータス ファイル。

CLI では、**export** コマンドと **import** コマンドを使用して、コンフィギュレーションの個々の要素をバックアップおよび復元できます。

これらのファイル（たとえば、**import webvpn** コマンドを使用してインポートしたこれらのファイルや証明書など）をバックアップするには、次の手順を実行します。

手順

ステップ 1 次のように、適用可能な **show** コマンドを実行します。

```
ciscoasa # show import webvpn plug-in
ica
rdp
ssh, telnet
```

```
vnc
```

ステップ 2 バックアップするファイルに対して **export** コマンドを発行します（この例では rdp ファイルです）。

```
ciscoasa # export webvpn plug-in protocol rdp tftp://tftpserver/backupfilename
```

スクリプトを使用したファイルのバックアップおよび復元

スクリプトを使用して、ASA のコンフィギュレーション ファイルをバックアップおよび復元できます。これには、**import webvpn** CLI によってインポートする拡張機能のすべて、CSD コンフィギュレーションの XML ファイル、および DAP コンフィギュレーションの XML ファイルが含まれます。セキュリティ上の理由により、デジタル キーと証明書、またはローカル CA キーの自動バックアップを実行することはお勧めしません。

この項では、自動バックアップの手順について説明します。また、そのまま使用することも、環境要件に合わせて修正することもできるサンプル スクリプトを示します。サンプル スクリプトは Linux システムに固有のスクリプトです。Microsoft Windows システムで使用するには、サンプルのロジックを使用して修正する必要があります。

（注） 代わりに、**backup** コマンドと **restore** コマンドを使用することもできます。詳細については、「完全なシステム バックアップまたは復元の実行 （1023 ページ）」を参照してください。

バックアップおよび復元スクリプトを使用する前に

スクリプトを使用して ASA コンフィギュレーションをバックアップおよび復元するには、まず次の作業を実行します。

- Expect モジュールとともに Perl をインストールする。
- ASA に到達可能な SSH クライアントをインストールする。
- TFTP サーバをインストールして、ASA からバックアップ サイトにファイルを送信する。

別の選択肢としては、市販のツールを使用します。このスクリプトのロジックをそれらのツールに取り入れることができます。

スクリプトを実行する

バックアップおよび復元のスクリプトを実行するには、次の手順を実行します。

手順

ステップ 1 システムの任意の場所に、スクリプト ファイルをダウンロードまたはカットアンドペーストします。

ステップ 2 コマンド ラインで、**Perl***scriptname* と入力します。*scriptname* はスクリプト ファイルの名前です。

ステップ 3 Enter を押します。

ステップ 4 オプションごとに値を入力するように、プロンプトが表示されます。あるいは、**Perl***scriptname* コマンドを入力するときにオプションの値を入力してから、**Enter** を押すこともできます。どちらの方法でも、スクリプトによりオプションごとに値を入力するよう求められます。

ステップ 5 このスクリプトが実行され、発行されるコマンドが出力されます。この出力はCLIの記録となります。これらのCLIは後で行われる復元に使用できます。特に、ファイルを1つまたは2つだけ復元する場合に便利です。

サンプル スクリプト

```
#!/usr/bin/perl
#Description: The objective of this script is to show how to back up
configurations/extensions.
# It currently backs up the running configuration, all extensions imported via "import
webvpn" command, the CSD configuration XML file, and the DAP configuration XML file.
#Requirements: Perl with Expect, SSH to the ASA, and a TFTP server.
#Usage: backupasa -option option_value
#       -h: ASA hostname or IP address
#       -u: User name to log in via SSH
#       -w: Password to log in via SSH
#       -e: The Enable password on the security appliance
#       -p: Global configuration mode prompt
#       -s: Host name or IP address of the TFTP server to store the configurations
#      -r: Restore with an argument that specifies the file name. This file is produced
 during backup.
#If you don't enter an option, the script will prompt for it prior to backup.
#
#Make sure that you can SSH to the ASA.

use Expect;
use Getopt::Std;

#global variables
%options=();
$restore = 0; #does backup by default
$restore_file = '';
$asa = '';
$storage = '';
$user = '';
$password = '';
$enable = '';
$prompt = '';
$date = `date +%F`;
chop($date);
my $exp = new Expect();

getopts("h:u:p:w:e:s:r:",\%options);
```

```
do process_options();

do login($exp);
do enable($exp);
if ($restore) {
   do restore($exp,$restore_file);
}
else {
   $restore_file = "$prompt-restore-$date.cli";
   open(OUT,">$restore_file") or die "Can't open $restore_file\n";
   do running_config($exp);
   do lang_trans($exp);
   do customization($exp);
   do plugin($exp);
   do url_list($exp);
   do webcontent($exp);
   do dap($exp);
   do csd($exp);
   close(OUT);
}
do finish($exp);

sub enable {
   $obj = shift;
   $obj->send("enable\n");
   unless ($obj->expect(15, 'Password:')) {
      print "timed out waiting for Password:\n";
   }
   $obj->send("$enable\n");
   unless ($obj->expect(15, "$prompt#")) {
      print "timed out waiting for $prompt#\n";
   }
}

sub lang_trans {
   $obj = shift;
   $obj->clear_accum();
   $obj->send("show import webvpn translation-table\n");
   $obj->expect(15, "$prompt#" );
   $output = $obj->before();
   @items = split(/\n+/, $output);

   for (@items) {
     s/^\s+//;
     s/\s+$//;
     next if /show import/ or /Translation Tables/;
     next unless (/^.+\s+.+$/);
     ($lang, $transtable) = split(/\s+/,$_);
     $cli = "export webvpn translation-table $transtable language $lang
$storage/$prompt-$date-$transtable-$lang.po";
     $ocli = $cli;
     $ocli =~ s/^export/import/;
     print "$cli\n";
     print OUT "$ocli\n";
     $obj->send("$cli\n");
     $obj->expect(15, "$prompt#" );
   }
}

sub running_config {
  $obj = shift;
  $obj->clear_accum();
  $cli ="copy /noconfirm running-config $storage/$prompt-$date.cfg";
  print "$cli\n";
```

```
  $obj->send("$cli\n");
  $obj->expect(15, "$prompt#" );
}


sub customization {
  $obj = shift;
  $obj->clear_accum();
  $obj->send("show import webvpn customization\n");
  $obj->expect(15, "$prompt#" );
  $output = $obj->before();
  @items = split(/\n+/, $output);

  for (@items) {
    chop;
    next if /^Template/ or /show import/ or /^\s*$/;
    $cli = "export webvpn customization $_ $storage/$prompt-$date-cust-$_.xml";
    $ocli = $cli;
    $ocli =~ s/^export/import/;
    print "$cli\n";
    print OUT "$ocli\n";
    $obj->send("$cli\n");
    $obj->expect(15, "$prompt#" );
  }
}

sub plugin {
   $obj = shift;
   $obj->clear_accum();
   $obj->send("show import webvpn plug-in\n");
   $obj->expect(15, "$prompt#" );
   $output = $obj->before();
   @items = split(/\n+/, $output);

   for (@items) {
     chop;
     next if /^Template/ or /show import/ or /^\s*$/;
     $cli = "export webvpn plug-in protocol $_ $storage/$prompt-$date-plugin-$_.jar";
     $ocli = $cli;
     $ocli =~ s/^export/import/;
     print "$cli\n";
     print OUT "$ocli\n";
     $obj->send("$cli\n");
     $obj->expect(15, "$prompt#" );
   }
}

sub url_list {
   $obj = shift;
   $obj->clear_accum();
   $obj->send("show import webvpn url-list\n");
   $obj->expect(15, "$prompt#" );
   $output = $obj->before();
   @items = split(/\n+/, $output);

   for (@items) {
     chop;
     next if /^Template/ or /show import/ or /^\s*$/ or /No bookmarks/;
     $cli="export webvpn url-list $_ $storage/$prompt-$date-urllist-$_.xml";
     $ocli = $cli;
     $ocli =~ s/^export/import/;
     print "$cli\n";
     print OUT "$ocli\n";
     $obj->send("$cli\n");
```

```
      $obj->expect(15, "$prompt#" );
   }
}

sub dap {
   $obj = shift;
   $obj->clear_accum();
   $obj->send("dir dap.xml\n");
   $obj->expect(15, "$prompt#" );

   $output = $obj->before();
   return 0 if($output =~ /Error/);

   $cli="copy /noconfirm dap.xml $storage/$prompt-$date-dap.xml";
   $ocli="copy /noconfirm $storage/$prompt-$date-dap.xml disk0:/dap.xml";
   print "$cli\n";
   print OUT "$ocli\n";
   $obj->send("$cli\n");
   $obj->expect(15, "$prompt#" );
}

sub csd {
   $obj = shift;
   $obj->clear_accum();
   $obj->send("dir sdesktop\n");
   $obj->expect(15, "$prompt#" );

   $output = $obj->before();
   return 0 if($output =~ /Error/);

   $cli="copy /noconfirm sdesktop/data.xml $storage/$prompt-$date-data.xml";
   $ocli="copy /noconfirm $storage/$prompt-$date-data.xml disk0:/sdesktop/data.xml";
   print "$cli\n";
   print OUT "$ocli\n";
   $obj->send("$cli\n");
   $obj->expect(15, "$prompt#" );
}

sub webcontent {
   $obj = shift;
   $obj->clear_accum();
   $obj->send("show import webvpn webcontent\n");
   $obj->expect(15, "$prompt#" );
   $output = $obj->before();
   @items = split(/\n+/, $output);

   for (@items) {
     s/^\s+//;
     s/\s+$//;
     next if /show import/ or /No custom/;
     next unless (/^.+\s+.+$/);
     ($url, $type) = split(/\s+/,$_);
     $turl = $url;
     $turl =~ s/\/\+//;
     $turl =~ s/\+\//-/;
     $cli = "export webvpn webcontent $url $storage/$prompt-$date-$turl";
     $ocli = $cli;
     $ocli =~ s/^export/import/;
     print "$cli\n";
     print OUT "$ocli\n";
     $obj->send("$cli\n");
     $obj->expect(15, "$prompt#" );
   }
}
```

```
sub login {
    $obj = shift;
    $obj->raw_pty(1);
    $obj->log_stdout(0); #turn off console logging.
    $obj->spawn("/usr/bin/ssh $user\@$asa") or die "can't spawn ssh\n";
    unless ($obj->expect(15, "password:" )) {
        die "timeout waiting for password:\n";
    }

    $obj->send("$password\n");

    unless ($obj->expect(15, "$prompt>" )) {
        die "timeout waiting for $prompt>\n";
    }
}

sub finish {
    $obj = shift;
    $obj->hard_close();
    print "\n\n";

}

sub restore {
   $obj = shift;
   my $file = shift;
   my $output;
   open(IN,"$file") or die "can't open $file\n";
   while (<IN>) {
      $obj->send("$_");
      $obj->expect(15, "$prompt#" );
      $output = $obj->before();
      print "$output\n";
   }
   close(IN);
}

sub process_options {
  if (defined($options{s})) {
      $tstr= $options{s};
      $storage = "tftp://$tstr";
  }
  else {
      print "Enter TFTP host name or IP address:";
      chop($tstr=<>);
      $storage = "tftp://$tstr";
  }
  if (defined($options{h})) {
      $asa = $options{h};
  }
  else {
      print "Enter ASA host name or IP address:";
      chop($asa=<>);
  }

  if (defined ($options{u})) {
      $user= $options{u};
  }
  else {
      print "Enter user name:";
      chop($user=<>);
  }
```

```
  if (defined ($options{w})) {
      $password= $options{w};
  }
  else {
      print "Enter password:";
      chop($password=<>);
  }
  if (defined ($options{p})) {
      $prompt= $options{p};
  }
  else {
      print "Enter ASA prompt:";
      chop($prompt=<>);
  }
  if (defined ($options{e})) {
      $enable = $options{e};
  }
  else {
      print "Enter enable password:";
      chop($enable=<>);
  }

  if (defined ($options{r})) {
     $restore = 1;
     $restore_file = $options{r};
  }
}
```

Auto Update の設定

Auto Update は、Auto Update サーバがコンフィギュレーションおよびソフトウェア イメージを多数の ASA にダウンロードすることを許可し、中央からの ASA の基本的なモニタリングを提供するプロトコル仕様です。

Auto Update について

この項では、Auto Update の実装方法と Auto Update が必要になる理由について説明します。

Auto Update クライアントまたはサーバ

ASA は、クライアントまたはサーバとして設定できます。Auto Update クライアントとして動作する場合は、ソフトウェアイメージおよびコンフィギュレーション ファイルへのアップデートのため、Auto Update サーバを定期的にポーリングします。Auto Update サーバとして動作する場合は、Auto Update クライアントとして設定された ASA のアップデートを発行します。

Auto Update の利点

Auto Update は、次のように、管理者が ASA の管理で直面するさまざまな問題を解決できる便利な機能です。

- ダイナミック アドレッシングおよび NAT に関する問題点の解決。
- コンフィギュレーションの変更を 1 つのアクションでコミット。

- ソフトウェア更新用の信頼度の高い方式の提供。
- ハイ アベイラビリティ用の十分実績のある方式の活用（フェールオーバー）。
- オープン インターフェイスによる柔軟性の提供。
- サービス プロバイダー環境のセキュリティ ソリューションの簡素化。

Auto Update仕様は、中央、または複数の場所から、リモート管理アプリケーションによりASAのコンフィギュレーションやソフトウェアイメージをダウンロードしたり、基本的な監視機能を実行したりする場合に必要なインフラストラクチャです。

Auto Update仕様に従うと、Auto UpdateサーバからASAにコンフィギュレーション情報をプッシュしたり、要求を送信して情報を取得したりすることも、ASAからAuto Updateサーバに定期的にポーリングすることによって、最新のコンフィギュレーション情報を引き出す（プルする）こともできます。また、Auto Updateサーバはいつでも ASA にコマンドを送信し、ただちにポーリング要求を送信させることもできます。Auto Update サーバと ASA の通信では、通信パスとローカル CLI コンフィギュレーションをすべての ASA に設定する必要があります。

フェールオーバー設定での Auto Update サーバ サポート

Auto Update サーバを使用して、ソフトウェア イメージとコンフィギュレーション ファイルを、アクティブ/スタンバイ フェールオーバー コンフィギュレーションの ASA に配置できます。アクティブ/スタンバイ フェールオーバー コンフィギュレーションでAuto Updateをイネーブルにするには、フェールオーバー ペアのプライマリ装置に Auto Update サーバのコンフィギュレーションを入力します。

フェールオーバー コンフィギュレーションのAuto Updateサーバ サポートには、次の制限と動作が適用されます。

- アクティブ/スタンバイ コンフィギュレーションがサポートされるのは、シングル モードだけです。
- 新しいプラットフォーム ソフトウェア イメージをロードする際、フェールオーバー ペアはトラフィックの転送を停止します。
- LAN ベースのフェールオーバーを使用する場合、新しいコンフィギュレーションによってフェールオーバー リンクのコンフィギュレーションが変更されてはいけません。フェールオーバー リンクのコンフィギュレーションが変更されると、装置間の通信は失敗します。
- Auto Update サーバへの Call Home を実行するのはプライマリ装置だけです。Call Home を実行するには、プライマリ装置がアクティブ状態である必要があります。そうでない場合、ASA は自動的にプライマリ装置にフェールオーバーします。
- ソフトウェアイメージまたはコンフィギュレーションファイルをダウンロードするのは、プライマリ装置だけです。その後、ソフトウェアイメージまたはコンフィギュレーションファイルはセカンダリ装置にコピーされます。
- インターフェイス MAC アドレスとハードウェアのシリアル番号は、プライマリ装置のものです。

- Auto Update サーバまたは HTTP サーバに保存されたコンフィギュレーション ファイルは、プライマリ装置専用です。

Auto Update プロセスの概要

次に、フェールオーバー コンフィギュレーションでの Auto Update プロセスの概要を示します。このプロセスは、フェールオーバーがイネーブルであり、動作していることを前提としています。装置がコンフィギュレーションを同期化している場合、SSM カードの不具合以外の理由でスタンバイ装置に障害が発生している場合、または、フェールオーバー リンクがダウンしている場合、Auto Update プロセスは実行できません。

1. 両方の装置は、プラットフォームおよび ASDM ソフトウェア チェックサムとバージョン情報を交換します。
2. プライマリ装置は Auto Update サーバにアクセスします。プライマリ装置がアクティブ状態でない場合、ASA はプライマリ装置にフェールオーバーした後、Auto Update サーバにアクセスします。
3. Auto Update サーバは、ソフトウェア チェックサムと URL 情報を返します。
4. プライマリ装置が、アクティブまたはスタンバイ装置のプラットフォーム イメージ ファイルをアップデートする必要があると判断した場合は、次の処理が実行されます。
    1. プライマリ装置は、Auto Update サーバの URL を使用して、HTTP サーバから適切なファイルを取得します。
    2. プライマリ装置は、そのイメージをスタンバイ装置にコピーしてから、自身のイメージをアップデートします。
    3. 両方の装置に新しいイメージがある場合は、セカンダリ（スタンバイ）装置が最初にリロードされます。
        - セカンダリ装置のブート時にヒットレス アップグレードが可能な場合は、セカンダリ装置がアクティブ装置になり、プライマリ装置がリロードされます。リロードが終了すると、プライマリ装置がアクティブ装置になります。
        - スタンバイ装置のブート時にヒットレス アップグレードができない場合は、両方の装置が同時にリロードされます。
    4. セカンダリ（スタンバイ）装置だけに新しいイメージがある場合は、セカンダリ装置だけがリロードされます。プライマリ装置は、セカンダリ装置のリロードが終了するまで待機します。
    5. プライマリ（アクティブ）装置だけに新しいイメージがある場合は、セカンダリ装置がアクティブ装置になり、プライマリ装置がリロードされます。
    6. もう一度アップデート プロセスが手順 1 から開始されます。
5. ASA が、プライマリまたはセカンダリ装置の ASDM ファイルをアップデートする必要があると判断した場合は、次の処理が実行されます。

1. プライマリ装置は、Auto Update サーバから提供された URL を使用して、HTTP サーバから ASDM イメージ ファイルを取得します。
2. プライマリ装置は、必要に応じてそのイメージをスタンバイ装置にコピーします。
3. プライマリ装置は、自身の ASDM イメージをアップデートします。
4. もう一度アップデート プロセスが手順 1 から開始されます。

6. プライマリ装置が、コンフィギュレーション ファイルをアップデートする必要があると判断した場合は、次の処理が実行されます。
   1. プライマリ装置は、指定された URL を使用して、からコンフィギュレーション ファイルを取得します。
   2. 両方の装置で同時に、古いコンフィギュレーションが新しいコンフィギュレーションに置換されます。
   3. もう一度アップデート プロセスが手順 1 から開始されます。
7. チェックサムがすべてのイメージおよびコンフィギュレーション ファイルと一致している場合、アップデートは必要ありません。このプロセスは、次のポーリング時間まで中断されます。

Auto Update のガイドライン

コンテキスト モード

Auto Update は、シングル コンテキスト モードでのみサポートされます。

クラスタ

クラスタリングはサポートされません。

モデル

次のモデルではサポートされません。

- ASA 5506-X、5508-X、5516-X
- Firepower 4100、および 9300
- ASAv

その他のガイドライン

- Auto Update サーバと通信するためのプロトコルとして HTTPS が選択されている場合は、ASA は SSL を使用します。これは、ASA による DES または 3DES ライセンスの保有が必須です。

Auto Update サーバとの通信の設定

手順

ステップ 1 Auto Update サーバの URL を指定するには、次のコマンドを入力します。

auto-update server *url* [**source** *interface*] [**verify-certificate** | **no-verification**]

ここで、*url* には次の構文があります。

http[**s**]**://**[*user***:***password***@**]*server_ip*[**:***port*]/*pathname*

source *interface* キーワードおよび引数は、Auto Update サーバに要求を送信するときに使用するインターフェイスを指定します。**management-access** コマンドで指定したインターフェイスと同じインターフェイスを指定すると、Auto Update 要求は管理アクセスに使用されるのと同じ IPsec VPN トンネルを通過します。

HTTPS の場合、**verify-certificate** キーワード（デフォルト）は、Auto Update サーバが返す証明書を検証します。検証をディセーブルにするには（推奨されません）、**no-verification** キーワードを指定します。

ステップ 2 （任意）Auto Update サーバと通信する際に送信するデバイス ID を識別するには、次のコマンドを入力します。

auto-update device-id {*hardware-serial* | **hostname** | **ipaddress** [*if-name*] | **mac-address** [*if-name*] | **string** *text*}

使用する ID は、次のいずれかのパラメータによって決まります。

- hardware-serial 引数は、ASA のシリアル番号を指定します。
- hostname 引数は、ASA のホスト名を指定します。
- **ipaddress** キーワードは、指定したインターフェイスの IP アドレスを指定します。インターフェイス名を指定しない場合、Auto Update サーバとの通信に使用するインターフェイスの IP アドレスが使用されます。
- **mac-address** キーワードは、指定のインターフェイスの MAC アドレスを指定します。インターフェイス名を指定しない場合、Auto Update サーバとの通信に使用するインターフェイスの MAC アドレスが使用されます。
- **string** キーワードは、指定のテキスト識別子を指定します。空白や ’、“、>、&、? は使用できません。

ステップ 3 （任意）コンフィギュレーション、またはイメージのアップデートを要求するために Auto Update サーバにポーリングする回数を指定するには、次のコマンドを入力します。

auto-update poll-period *poll-period* [*retry-count* [*retry-period*]]

poll-period 引数は、更新を確認する間隔（分単位）を指定します。デフォルトは 720 分（12 時間）です。

retry-count 引数は、サーバへの最初の接続に失敗した場合に、再試行する回数を指定します。デフォルトは 0 です。

retry-period 引数は、リトライの間の待機時間（分単位）を指定します。デフォルトは 5 分です。

ステップ 4 （オプション）ASA から Auto Update サーバにポーリングする特定の時刻をスケジュールするには、次のコマンドを入力します。

auto-update poll-at *days-of-the-week time* [**randomize** *minutes*] [*retry_count* [*retry_period*]]

days-of-the-week 引数は、Monday、Tuesday、Wednesday、Thursday、Friday、Saturday、および Sunday の中の任意の曜日または曜日の組み合わせです。それ以外に、daily（月曜日から日曜日）、weekdays（月曜日から金曜日）、および weekend（土曜日と日曜日）の値が設定可能です。

time 引数は、ポーリングの開始時刻を HH:MM 形式で指定します。たとえば、午前 8 時は 8:00、午後 8 時は 20:00 とします。

randomize *minutes* キーワードおよび引数は、指定した開始時刻に続いてポーリングをランダムに実行する期間を指定します。範囲は 1 ～ 1439 分です。

retry_count 引数は、最初の接続に失敗したときに、Auto Update サーバへの再接続を試みる回数を指定します。デフォルトは 0 です。

retry_period 引数は、接続の試行から次の試行までの待機時間を指定します。デフォルトは 5 分です。範囲は 1 ～ 35791 分です。

ステップ 5 （オプション）Auto Update サーバに一定期間アクセスがなかった場合にトラフィックの通過を中断するには、次のコマンドを入力します。

auto-update timeout *period*

period 引数は、1 ～ 35791 の範囲で分単位のタイムアウト期間を指定します。デフォルトはタイムアウトなし（0 分）です。デフォルトに戻すには、このコマンドの **no** 形式を使用します。

auto-update timeout コマンドを使用して、最新のイメージと設定が ASA に存在することを確認します。この状態は、システム ログ メッセージ 201008 で報告されます。

例

次の例では、ASA が外部インターフェイスから証明書の検証付きで、IP アドレス 209.165.200.224、ポート番号 1742 で Auto Update サーバをポーリングするように設定されています。

また、ASA は、デバイス ID としてホスト名を使用し、Auto Update サーバへのポーリングを毎週金曜日と土曜日の 10:00 p.m から 11:00 p.m. の間の任意の時刻に実行するように設定されます。次の例のように、ポーリングに失敗した場合は、ASA によって Auto Update サーバへの再接続が 10 回試みられます。再接続と再接続の間は、3 分間の待機時間が設定されます。

```
ciscoasa(config)# auto-update server
https://jcrichton:farscape@209.165.200.224:1742/management source outside
verify-certificate
ciscoasa (config)# auto-update device-id hostname
hostname (config)# auto-update poll-at Friday Saturday 22:00 randomize 60 2 10
```

Auto Update サーバとしてのクライアント アップデートの設定

client-update コマンドを入力すると、Auto Update クライアントとして設定された ASA のアップデートがイネーブルになり、ソフトウェア コンポーネントのタイプ（ASDM またはブート イメージ）、ASA のタイプまたはファミリ、アップデートが適用されるリビジョン番号、アップデートを取得した URL または IP アドレスを指定できるようになります。

ASA を Auto Update サーバとして設定するには、次の手順を実行します。

手順

ステップ 1 クライアント アップデートをイネーブルにするには、次のコマンドを入力します。

```
ciscoasa(config)# client-update enable
```

ステップ 2 ASA に適用する **client-update** コマンドに、次のパラメータを設定します。

client-update {**component** {**asdm** | **image**} | **device-id** dev_string | **family** family_name | **type** type} **url**url-string **rev-nums** rev-nums}

component {**asdm** | **image**} パラメータでは、ASDM または ASA のブート イメージのいずれかをソフトウェア コンポーネントとして指定します。

device-id dev_string パラメータでは、Auto Update クライアントが自身を識別するために使用する固有の文字列を指定します。最大で 63 文字です。

family family_name パラメータでは、Auto Update クライアントが自身を識別するために使用するファミリ名を指定します。asa、pix、または 7 文字以内のテキスト文字列を指定します。

rev-nums rev-nums パラメータでは、このクライアントのソフトウェアまたはファームウェア イメージを指定します。最大 4 個のイメージを、任意の順序でカンマで区切って指定します。

type *type* パラメータでは、クライアント アップデートを通知するクライアントのタイプを指定します。このコマンドは、Windows クライアントのアップデートでも使用されるため、クライアントのリストには Windows オペレーティング システムも複数含まれています。

url url-string パラメータでは、ソフトウェアまたはファームウェア イメージの URL を指定します。この URL は、クライアントに適合するファイルを指している必要があります。すべての Auto Update クライアントでは、URL のプレフィックスとしてプロトコル「http://」または「https://」を使用する必要があります。

特定のタイプのASAすべてに適用するクライアントアップデートのパラメータを設定します。つまり、ASA のタイプ、および更新されたイメージの取得元となる URL または IP アドレスを指定します。また、リビジョン番号も指定する必要があります。リモートの ASA のリビジョン番号が、指定したリビジョン番号の 1 つと一致する場合は、クライアントのアップデートは不要です。アップデートは無視されます。

Cisco 5525-X ASA にクライアントアップデートを設定するには、次のコマンドを入力します。

```
ciscoasa(config)# client-update type asa5525 component asdm url
http://192.168.1.114/aus/asdm601.bin rev-nums 8.0(1)
```

Auto Update のモニタリング

Auto Update プロセスのモニタリング

debug auto-update client または **debug fover cmd-exe** コマンドを使用して、Auto Update プロセスで実行される処理を表示できます。次に、**debug auto-update client** コマンドの出力例を示します。

```
Auto-update client: Sent DeviceDetails to /cgi-bin/dda.pl of server 192.168.0.21
Auto-update client: Processing UpdateInfo from server 192.168.0.21
   Component: asdm, URL: http://192.168.0.21/asdm.bint, checksum:
0x94bced0261cc992ae710faf8d244cf32
   Component: config, URL: http://192.168.0.21/config-rms.xml, checksum:
0x67358553572688a805a155af312f6898
   Component: image, URL: http://192.168.0.21/cdisk73.bin, checksum:
0x6d091b43ce96243e29a62f2330139419
Auto-update client: need to update img, act: yes, stby yes
name
ciscoasa(config)# Auto-update client: update img on stby unit...
auto-update: Fover copyfile, seq = 4 type = 1, pseq = 1, len = 1024
auto-update: Fover copyfile, seq = 4 type = 1, pseq = 501, len = 1024
auto-update: Fover copyfile, seq = 4 type = 1, pseq = 1001, len = 1024
auto-update: Fover copyfile, seq = 4 type = 1, pseq = 1501, len = 1024
auto-update: Fover copyfile, seq = 4 type = 1, pseq = 2001, len = 1024
auto-update: Fover copyfile, seq = 4 type = 1, pseq = 2501, len = 1024
auto-update: Fover copyfile, seq = 4 type = 1, pseq = 3001, len = 1024
auto-update: Fover copyfile, seq = 4 type = 1, pseq = 3501, len = 1024
auto-update: Fover copyfile, seq = 4 type = 1, pseq = 4001, len = 1024
auto-update: Fover copyfile, seq = 4 type = 1, pseq = 4501, len = 1024
auto-update: Fover copyfile, seq = 4 type = 1, pseq = 5001, len = 1024
auto-update: Fover copyfile, seq = 4 type = 1, pseq = 5501, len = 1024
auto-update: Fover copyfile, seq = 4 type = 1, pseq = 6001, len = 1024
auto-update: Fover copyfile, seq = 4 type = 1, pseq = 6501, len = 1024
auto-update: Fover copyfile, seq = 4 type = 1, pseq = 7001, len = 1024
auto-update: Fover copyfile, seq = 4 type = 1, pseq = 7501, len = 1024
auto-update: Fover copyfile, seq = 4 type = 1, pseq = 8001, len = 1024
auto-update: Fover copyfile, seq = 4 type = 1, pseq = 8501, len = 1024
auto-update: Fover copyfile, seq = 4 type = 1, pseq = 9001, len = 1024
auto-update: Fover file copy waiting at clock tick 6129280
fover_parse: Rcvd file copy ack, ret = 0, seq = 4
auto-update: Fover filecopy returns value: 0 at clock tick 6150260, upd time 145980 msecs
Auto-update client: update img on active unit...
```

```
fover_parse: Rcvd image info from mate
auto-update: HA safe reload: reload active waiting with mate state: 20
auto-update: HA safe reload: reload active waiting with mate state: 20
auto-update: HA safe reload: reload active waiting with mate state: 20
auto-update: HA safe reload: reload active waiting with mate state: 20
auto-update: HA safe reload: reload active waiting with mate state: 20
auto-update: HA safe reload: reload active waiting with mate state: 20
auto-update: HA safe reload: reload active waiting with mate state: 20
auto-update: HA safe reload: reload active waiting with mate state: 20
auto-update: HA safe reload: reload active waiting with mate state: 20
auto-update: HA safe reload: reload active waiting with mate state: 20
auto-update: HA safe reload: reload active waiting with mate state: 20
auto-update: HA safe reload: reload active waiting with mate state: 20
auto-update: HA safe reload: reload active waiting with mate state: 20
auto-update: HA safe reload: reload active waiting with mate state: 20
auto-update: HA safe reload: reload active waiting with mate state: 20
Beginning configuration replication: Sending to mate.
auto-update: HA safe reload: reload active waiting with mate state: 50
auto-update: HA safe reload: reload active waiting with mate state: 50

auto-update: HA safe reload: reload active waiting with mate state: 80
        Sauto-update: HA safe reload: reload active unit at clock tick: 6266860
Auto-update client: Succeeded: Image, version: 0x6d091b43ce96243e29a62f2330139419
```

Auto Update プロセスが失敗すると、次の syslog メッセージが生成されます。

```
%ASA4-612002: Auto Update failed: file version: version reason: reason
```

file は、失敗したアップデートに応じて “image”、“asdm”、または “configuration” になります。*version* は、アップデートのバージョン番号です。*reason* は、アップデートが失敗した原因です。

Auto Update ステータスのモニタリング

Auto Update ステータスのモニタリングについては、次のコマンドを参照してください。

show auto-update

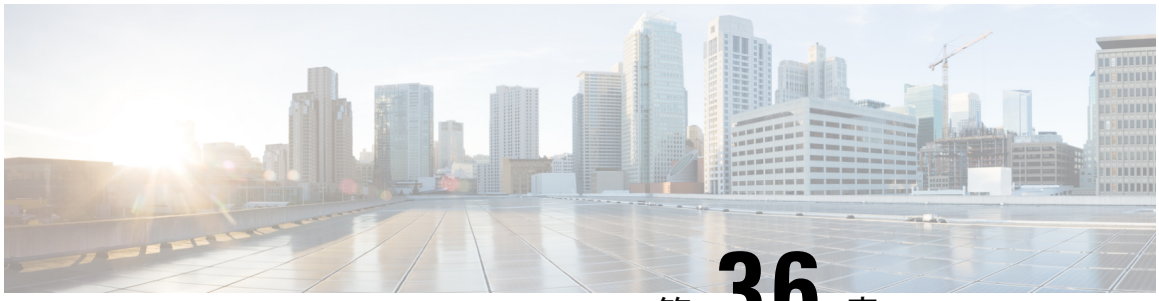
次に、**show auto-update** コマンドの出力例を示します。

```
ciscoasa(config)# show auto-update

Server: https://********@209.165.200.224:1742/management.cgi?1276
Certificate will be verified
Poll period: 720 minutes, retry count: 2, retry period: 5 minutes
Timeout: none
Device ID: host name [corporate]
Next poll in 4.93 minutes
Last poll: 11:36:46 PST Tue Nov 13 2004
Last PDM update: 23:36:46 PST Tue Nov 12 2004
```

ソフトウェアとコンフィギュレーションの履歴

機能名	プラットフォーム リリース	機能情報
セキュア コピー クライアント	9.1(5)/9.2(1)	SCP サーバとの間でファイルを転送するため、ASA は Secure Copy（SCP）クライアントをサポートするようになりました。 **ssh pubkey-chain**、**server (ssh pubkey-chain)**、**key-string**、**key-hash**、**ssh stricthostkeycheck** の各コマンドが導入されました。 **copy scp** コマンドが変更されました。
設定可能な SSH 暗号機能と整合性アルゴリズム	9.1(7)/9.4(3)	ユーザは SSH 暗号化を管理するときに暗号化モードを選択し、さまざまなキー交換アルゴリズムに対して HMAC と暗号化を設定できます。アプリケーションに応じて、暗号の強度を強くしたり弱くする必要がある場合があります。セキュアなコピーのパフォーマンスは暗号化アルゴリズムに一部依存します。デフォルトで、ASA は 3des-cbc aes128-cbc aes192-cbc aes256-cbc aes128-ctr aes192-ctr aes256-ctr の順にアルゴリズムをネゴシエートします。提示された最初のアルゴリズム（3des-cbc）が選択された場合、aes128-cbc などの一層効率的なアルゴリズムが選択された場合よりも大幅にパフォーマンスが低下します。たとえば、提示された暗号方式に変更するには、**ssh cipher encryption custom aes128-cbc** を使用します。 次のコマンドが導入されました。**ssh cipher encryption**、**ssh cipher integrity**

機能名	プラットフォーム リリース	機能情報
デフォルトでイネーブルになっている Auto Update サーバ証明書の検証	9.2(1)	Auto Update サーバ証明書の検証がデフォルトでイネーブルになりました。新しいコンフィギュレーションでは証明書の検証を明示的にディセーブルにする必要があります。証明書の確認をイネーブルにしていなかった場合に、以前のリリースからアップグレードしようとすると、証明書の確認はイネーブルではなく、次の警告が表示されます。 `WARNING: The certificate provided by the auto-update servers will not be verified. In order to verify this certificate please use the verify-certificate option.` 設定を移行する場合は、次のように確認なしを明示的に設定します。 **auto-update server no-verification** **auto-update server** {**verify-certificate** | **no-verification**} コマンドが変更されました。
CLI を使用したシステムのバックアップと復元	9.3(2)	CLI を使用してイメージや証明書を含む完全なシステムコンフィギュレーションをバックアップおよび復元できるようになりました。 **backup** および **restore** の各コマンドが導入されました。
新しい ASA 5506W-X イメージの回復およびロード	9.4(1)	新しい ASA 5506W-X イメージのリカバリおよびロードがサポートされています。 **hw-module module wlan recover image** コマンドが導入されました。



第 36 章

システム イベントに対する応答の自動化

この章では、Embedded Event Manager（EEM）を設定する方法について説明します。

EEM について

EEM サービスを利用することで、問題をデバッグし、トラブルシューティングに対して汎用ロギングを提供できます。EEM サービスには 2 つのコンポーネント、つまり EEM が応答またはリッスンするイベント、およびアクションと EEM が応答するイベントを定義するイベント マネージャ アプレットがあります。さまざまなイベントに応答し、さまざまなアクションを実行するために、複数のイベント マネージャ アプレットを設定できます。

サポートされるイベント

EEM は次のイベントをサポートします。

- Syslog：ASA は、syslog メッセージの ID を使用して、イベント マネージャ アプレットをトリガーする syslog メッセージを識別します。複数の syslog イベントを設定できますが、単一のイベント マネージャ アプレット内で syslog メッセージの ID が重複することはできません。
- タイマー：タイマーを使用して、イベントをトリガーできます。各タイマーは、各イベント マネージャ アプレットに対して一度だけ設定できます。各イベント マネージャ アプレットには最大で 3 つのタイマーがあります。3 種類のタイマーは次のとおりです。
  - ウォッチドッグ（定期的）タイマーは、アプレットアクションの完了後に指定された期間が経過するとイベント マネージャ アプレットをトリガーし、自動的にリスタートします。

- カウントダウン（ワンショット）タイマーは、指定された期間が経過するとイベントマネージャアプレットを1回トリガーします。削除および再追加されない限りはリスタートしません。
- 絶対（1 日 1 回）タイマーは、イベントを 1 日 1 回指定された時刻に発生させ、自動的にリスタートします。時刻の形式は hh:mm:ss です。

  各イベント マネージャ アプレットに対して、各タイプのタイマー イベントを 1 つだけ設定できます。

- なし：CLI または ASDM を使用してイベント マネージャ アプレットを手動で実行する場合、イベントはトリガーされません。
- クラッシュ：ASA がクラッシュした場合、クラッシュ イベントがトリガーされます。**output** コマンドの値に関係なく、**action** コマンドはクラッシュ情報ファイルを対象とします。出力は **show tech** コマンドの前に生成されます。

イベント マネージャ アプレットのアクション

イベント マネージャ アプレットがトリガーされると、そのイベント マネージャ アプレットのアクションが実行されます。各アクションには、アクションの順序を指定するために使用される番号があります。このシーケンス番号は、イベント マネージャ アプレット内で一意である必要があります。イベント マネージャ アプレットには複数のアクションを設定できます。コマンドは典型的な CLI コマンドです（**show blocks** など）。

出力先

output コマンドを使用すると、アクションの出力を指定した場所に送信できます。一度にイネーブルにできる出力値は1つだけです。デフォルト値は **output none** です。この値は、**action** コマンドによるすべての出力を破棄します。このコマンドは、特権レベル 15（最高）を持つユーザとして、グローバル コンフィギュレーション モードで実行されます。ディセーブルになっているため、このコマンドは入力を受け付けない場合があります。次の3つの場所のいずれかに **action** CLI コマンドの出力を送信できます。

- **なし**：デフォルトの設定です。出力を破棄します。
- **コンソール**：出力を ASA コンソールに送信します。
- **ファイル**：出力をファイルに送信します。次の 4 つのファイル オプションを使用できます。
  - **一意のファイルを作成する**：イベントマネージャアプレットが呼び出されるたびに、一意の名前を持つ新しいファイルを作成します。
  - **ファイルを作成する/ファイルを上書きする**：イベント マネージャ アプレットが呼び出されるたびに、指定されたファイルを上書きします。

- **ファイルを作成する/ファイルに付加する**：イベント マネージャ アプレットが呼び出されるたびに、指定されたファイルに付加します。ファイルがまだ存在しない場合は作成されます。
- **一連のファイルを作成する**：イベント マネージャ アプレットが呼び出されるたびにローテーションされる、一意の名前を持つ一連のファイルを作成します。

EEM のガイドライン

ここでは、EEM を設定する前に確認する必要のあるガイドラインおよび制限事項について説明します。

コンテキスト モードのガイドライン

マルチ コンテキスト モードではサポートされません。

その他のガイドライン

- 通常、クラッシュ時は、ASA の状態は不明です。こうした状況では、一部のコマンドの実行は安全ではない可能性があります。
- イベント マネージャ アプレットの名前にはスペースを含めることができません。
- None イベントおよび Crashinfo イベント パラメータは変更できません。
- syslog メッセージが EEM に送信されて処理されるため、パフォーマンスが影響を受ける可能性があります。
- 各イベント マネージャ アプレットのデフォルトの出力は **output none** です。この設定を変更するには、異なる出力値を入力する必要があります。
- 各イベント マネージャ アプレットに定義できる出力オプションは 1 つだけです。

EEM の設定

EEM の設定は、次のタスクで構成されています。

手順

ステップ 1 イベント マネージャ アプレットの作成とイベントの設定 （1052 ページ）。
ステップ 2 アクションおよびアクションの出力先の設定（1054 ページ）を使用して無効にすることができます。
ステップ 3 イベントマネージャ アプレットの実行（1056ページ）を使用して無効にすることができます。

ステップ 4 トラック メモリ割り当ておよびメモリ使用量（1056ページ）を使用して無効にすることができます。

イベント マネージャ アプレットの作成とイベントの設定

イベントマネージャアプレットを作成してイベントを設定するには、次の手順を実行します。

手順

ステップ 1 イベント マネージャ アプレットを作成し、イベント マネージャ アプレットのコンフィギュレーション モードを開始します。

event manager applet *name*

例：

```
ciscoasa(config)# event manager applet exampleapplet1
```

name 引数には、最大 32 文字の英数字を指定できます。スペースは使用できません。

イベント マネージャ アプレットを削除するには、このコマンドを **no** 形式で入力します。

ステップ 2 イベント マネージャ アプレットの説明を入力します。

description *text*

例：

```
ciscoasa(config-applet)# description applet1example
```

text 引数は、最大 256 文字です。引用符内であれば、説明テキストにスペースを含めることができます。

ステップ 3 指定されたイベントを設定するには、次のコマンドのいずれかを入力します。設定されたイベントを削除するには、それぞれのコマンドを **no** 形式で入力します。

- syslog イベントを設定するには、イベント マネージャ アプレットをトリガーする単一の syslog メッセージまたは syslog メッセージの範囲を指定します。

  event syslog id *nnnnnn* [*-nnnnnn*] [**occurs** *n*] [**period** *seconds*]

  例：

  ```
  ciscoasa(config-applet)# event syslog id 106201
  ```

  nnnnnn 引数には、syslog メッセージの ID を指定します。キーワードと引数のペアである **occurs** *n* は、イベント マネージャ アプレットを呼び出すために syslog メッセージが発生しなければならない回数を示しています。デフォルトの発生回数は 0 秒ごとに 1 回です。

有効な値は、1 ～ 4294967295 です。キーワードと引数のペアである **period** *seconds* は、イベントが発生する際の許容時間（秒数）を示しています。また、イベント マネージャ アプレットが設定された期間に 1 回呼び出される際の最大の間隔を制限します。有効な値は、0 ～ 604800 です。値 0 は、期間が定義されていないことを示しています。

- イベントを設定された期間ごとに1回発生させ、自動的にリスタートするように設定します。

  event timer watchdog time *seconds*

  例：

  ```
  ciscoasa(config-applet)# event timer watchdog time 30
  ```

  秒数は、1 ～ 604800 の範囲で設定してください。

- イベントを1回発生させ、削除および再追加されない限りはリスタートしないように設定します。

  event timer countdown time *seconds*

  例：

  ```
  ciscoasa(config-applet)# event timer countdown time 60
  ```

  秒数は、1 ～ 604800 の範囲で設定してください。カウントダウン タイマー イベントを削除するには、このコマンドの **no** 形式を使用します。

  （注） スタートアップ コンフィギュレーションである場合、このタイマーはリブート時に再実行されます。

- イベントを 1 日 1 回指定された時刻に発生させ、自動的にリスタートするように設定します。

  event timer absolute time *hh:mm:ss*

  例：

  ```
  ciscoasa(config-applet)# event timer absolute time 10:30:20
  ```

  時刻の形式は hh:mm:ss です。時刻の範囲は 00:00:00（真夜中）から 23:59:59 です。

- ASA のクラッシュ時にクラッシュ イベントをトリガーします。

  event crashinfo

  例：

  ```
  ciscoasa(config-applet)# event crashinfo
  ```

output コマンドの値に関係なく、**action** コマンドはクラッシュ情報ファイルを対象とします。出力は **show tech** コマンドの前に生成されます。

アクションおよびアクションの出力先の設定

アクションおよびアクションの出力を送信する特定の宛先を設定するには、次の手順を実行します。

手順

ステップ 1 イベント マネージャ アプレットにアクションを設定します。

action *n* **cli command** *"command"*

例：

```
ciscoasa(config-applet)# action 1 cli command "show version"
```

n オプションはアクション ID です。有効な ID の範囲は、0 ～ 4294967295 です。*command* オプションの値は、引用符で囲む必要があります。引用符で囲んでいない場合、コマンドが 2 つ以上の単語で構成されているとエラーが発生します。このコマンドは、特権レベル 15（最高）を持つユーザとして、グローバル コンフィギュレーション モードで実行されます。ディセーブルになっているため、このコマンドは入力を受け付けない場合があります。コマンドで使用可能な場合は、**noconfirm** オプションを使用します。

ステップ 2 使用可能な出力先オプションを 1 つ選択します。出力先を削除するには、各コマンドの **no** 形式を使用します。

- **None** オプションは、**action** コマンドからのあらゆる出力を破棄します。これがデフォルト設定です。

  output none

  例：

  ```
  ciscoasa(config-applet)# output none
  ```

- **Console** オプションは、**action** コマンドの出力をコンソールに送信します。

  output console

  例：

  ```
  ciscoasa(config-applet)# output console
  ```

  （注）　このコマンドを実行すると、パフォーマンスに影響を及ぼします。

- **New File** オプションは、呼び出された各イベント マネージャ アプレットの新しいファイルに **action** コマンドの出力を送信します。

  output file new

  例：

  ```
  ciscoasa(config-applet)# output file new
  ```

  ファイル名の形式は、eem-*applet-timestamp*.log です。ここで、*applet* はイベント マネージャ アプレットの名前、*timestamp* は日付のタイム スタンプ（形式は YYYYMMDD-hhmmss）を示しています。

- **New Set of Rotated Files** オプションは、ローテーションされる一連のファイルを作成します。新しいファイルが書き込まれる場合、最も古いファイルが削除され、最初のファイルが書き込まれる前に後続のすべてのファイルに番号が再度割り振られます。

  output file rotate *n*

  例：

  ```
  ciscoasa(config-applet)# output file rotate 50
  ```

  最も新しいファイルが 0 で示され、最も古いファイルが最大数（*n* -1）で示されます。*n* オプションはローテーションの値です。有効な値の範囲は 2 ～ 100 です。ファイル名の形式は、eem-*applet-x*.log です。ここで、*applet* はアプレットの名前、*x* はファイル番号を示しています。

- **Single Overwritten File** オプションは、**action** コマンドの出力を単一のファイルに書き込みます。このファイルは毎回上書きされます。

  output file overwrite *filename*

  例：

  ```
  ciscoasa(config-applet)# output file overwrite examplefile1
  ```

  filename 引数は、（ASA に対して）ローカルのファイル名です。このコマンドは、FTP、TFTP、および SMB のターゲット ファイルを使用する場合もあります。

- **Single Appended File** オプションは、**action** コマンドの出力を単一のファイルに書き込みますが、このファイルは毎回上書きされます。

  output file append *filename*

  例：

  ```
  ciscoasa(config-applet)# output file append examplefile1
  ```

filename 引数は、（ASA に対して）ローカルのファイル名です。

イベント マネージャ アプレットの実行

イベント マネージャ アプレットを実行するには、次の手順を実行します。

手順

イベント マネージャ アプレットを実行します。

event manager run *applet*

例：

```
ciscoasa# event manager run exampleapplet1
```

event none コマンドで設定されていないイベント マネージャ アプレットを実行すると、エラーが発生します。*applet*引数は、イベント マネージャ アプレットの名前です。

トラック メモリ割り当ておよびメモリ使用量

メモリ割り当てとメモリ使用量をログに記録するには、次の手順を実行します。

手順

ステップ 1 メモリ ロギングをイネーブルにします。

memory logging [1024-4194304] [**wrap**] [**size** [1-2147483647]] [**process** *process-name*] [**context** *context-name*]

例：

```
ciscoasa(config)# memory logging 202980
```

必要な唯一の引数は、メモリ ロギング バッファ内のエントリ数です。**wrap** オプションは、ラップ時にバッファを保存するようメモリ ロギング ユーティリティに指示します。保存できるのは一度だけです。

メモリ ロギング バッファが複数回ラップした場合は、上書きされます。バッファがラップすると、そのデータの保存をイネーブルにするトリガーがイベント マネージャに送信されます。**size** オプションは、特定のサイズをモニタします。**process** オプションは、特定のプロセスをモニタします。

（注） Checkheaps プロセスは、非標準の方法でメモリ アロケータを使用するため、プロセスとして完全に無視されます。

context オプションは、指定した名前で特定の仮想コンテキストのメモリ ロギングを記録します。

メモリ ロギング パラメータを変更するには、それをディセーブルにしてから、再度イネーブルにします。

ステップ 2 メモリ ロギング結果を表示します。

```
show memory logging [brief | wrap]
show memory logging include [address] [caller] [operator] [size] [process] [time] [context]
```

例：

```
ciscoasa# show memory logging
Number of free                          6
Number of calloc                        0
Number of malloc                        8
Number of realloc-new                   0
Number of realloc-free                  0
Number of realloc-null                  0
Number of realloc-same                  0
Number of calloc-fail                   0
Number of malloc-fail                   0
Number of realloc-fail                  0
Total operations 14
Buffer size: 50 (3688 x2 bytes)
process=[ci/console] time=[13:26:33.407] oper=[malloc]
addr=0x00007fff2cd0a6c0 size=72 @ 0x00000000016466ea 0x0000000002124542
0x000000000131911a 0x0000000000442bfd process=[ci/console] time=[13:26:33.407] oper=[free]
addr=0x00007fff2cd0a6c0 size=72 @ 0x00000000021246ef 0x000000000013193e8
0x0000000000443455 0x0000000001318f5b
process=[CMGR Server Process] time=[13:26:35.964] oper=[malloc]
addr=0x00007fff2cd0aa00 size=16 @ 0x00000000016466ea 0x0000000002124542
0x000000000182774d 0x000000000182cc8a process=[CMGR Server Process]
time=[13:26:35.964] oper=[malloc]
addr=0x00007fff224bb9f0 size=512 @ 0x00000000016466ea 0x0000000002124542
0x0000000000bfef9a 0x0000000000bff606 process=[CMGR Server Process]
time=[13:26:35.964] oper=[free]
addr=0x00007fff224bb9f0 size=512 @ 0x00000000021246ef 0x0000000000bff3d8
0x0000000000bff606 0x000000000182ccb0
process=[CMGR Server Process] time=[13:26:35.964] oper=[malloc]
addr=0x00007fff224b9460 size=40 @ 0x00000000016466ea 0x0000000002124542
0x0000000001834188 0x000000000182ce83
process=[CMGR Server Process] time=[13:26:37.964] oper=[free]
addr=0x00007fff2cd0aa00 size=16 @ 0x00000000021246ef 0x0000000001827098
0x000000000182c08d 0x000000000182c262 process=[CMGR Server Process]
time=[13:26:37.964] oper=[free]
addr=0x00007fff224b9460 size=40 @ 0x00000000021246ef 0x000000000182711b
0x000000000182c08d 0x000000000182c262 process=[CMGR Server Process]
time=[13:26:38.464] oper=[malloc]
addr=0x00007fff2cd0aa00 size=16 @ 0x00000000016466ea 0x0000000002124542
0x000000000182774d 0x000000000182cc8a process=[CMGR Server Process]
time=[13:26:38.464] oper=[malloc]
addr=0x00007fff224bb9f0 size=512 @ 0x00000000016466ea 0x0000000002124542
0x0000000000bfef9a 0x0000000000bff606 process=[CMGR Server Process]
```

```
time=[13:26:38.464] oper=[free]
addr=0x00007fff224bb9f0 size=512 @ 0x00000000021246ef 0x0000000000bff3d8
0x0000000000bff606 0x000000000182ccb0
process=[CMGR Server Process] time=[13:26:38.464] oper=[malloc]
addr=0x00007fff224b9460 size=40 @ 0x00000000016466ea 0x0000000002124542
0x0000000001834188 0x000000000182ce83
process=[ci/console] time=[13:26:38.557] oper=[malloc]
addr=0x00007fff2cd0a6c0 size=72 @ 0x00000000016466ea 0x0000000002124542
0x000000000131911a 0x0000000000442bfd process=[ci/console] time=[13:26:38.557] oper=[free]
addr=0x00007fff2cd0a6c0 size=72 @ 0x00000000021246ef 0x00000000013193e8
0x0000000000443455 0x0000000001318f5b

ciscoasa# show memory logging include process operation size
Number of free                          6
Number of calloc                        0
Number of malloc                        8
Number of realloc-new                   0
Number of realloc-free                  0
Number of realloc-null                  0
Number of realloc-same                  0
Number of calloc-fail                   0
Number of malloc-fail                   0
Number of realloc-fail                  0
Total operations 14
Buffer size: 50 (3688 x2 bytes)
process=[ci/console] oper=[malloc] size=72 process=[ci/console] oper=[free]
size=72 process=[CMGR Server Process] oper=[malloc] size=16
process=[CMGR Server Process] oper=[malloc] size=512 process=[CMGR Server Process]
oper=[free] size=512 process=[CMGR Server Process] oper=[malloc] size=40
process=[CMGR Server Process] oper=[free] size=16 process=[CMGR Server Process]
oper=[free] size=40 process=[CMGR Server Process] oper=[malloc] size=16
process=[CMGR Server Process] oper=[malloc] size=512 process=[CMGR Server Process]
oper=[free] size=512 process=[CMGR Server Process] oper=[malloc] size=40
process=[ci/console] oper=[malloc] size=72 process=[ci/console]
oper=[free] size=72 ciscoasa# show memory logging brief
Number of free                          6
Number of calloc                        0
Number of malloc                        8
Number of realloc-new                   0
Number of realloc-free                  0
Number of realloc-null                  0
Number of realloc-same                  0
Number of calloc-fail                   0
Number of malloc-fail                   0
Number of realloc-fail                  0
Total operations 14
Buffer size: 50 (3688 x2 bytes)
```

どのオプションも指定しない場合、**show memory logging** は統計情報を表示し、記録された処理を表示します。**brief** オプションは、統計情報だけを表示します。**wrap** オプションは、重複したデータが表示または保存されないように、ラップ時点でバッファを表示してから、そのデータを消去します。**include** オプションは、指定されたフィールドのみを出力に含めます。任意の順序でフィールドを指定できますが、必ず次の順序で表示されます。

1. プロセス
2. 時刻
3. コンテキスト（シングル モード以外）
4. 処理（free/malloc/など）

5. アドレス
6. サイズ
7. 発信者

出力形式は、次のとおりです。

process=[XXX] time=[XXX] context=[XXX] oper=[XXX] address=0xXXXXXXXX size=XX @ XXXXXXXX XXXXXXXX XXXXXXXX XXXXXXXX

最大4つの発信者アドレスが表示されます。例に示すように、処理の種類（番号）が出力に列挙されます。

ステップ3 メモリ ロギング ラップ イベントに応答します。

event memory-logging-wrap

例：

```
ciscoasa(config)# event manager applet memlog
ciscoasa(config)# event memory-logging-wrap
ciscoasa(config)# action 0 cli command "show memory logging wrap"
ciscoasa(config)# output file append disk0:/memlog.log
```

この例では、すべてのメモリ割り当てを記録するアプレットを示します。メモリ ロギングに対してラップがイネーブルになっている場合は、メモリ ロガーが、設定されたアプレットをトリガーするイベントをイベント マネージャに送信します。

EEM の例

次に、ブロックの漏えい情報を1時間ごとに記録し、その出力をローテーションされる一連のログ ファイルに書き込み、1 日分のログを保持するイベント マネージャ アプレットの例を示します。

```
ciscoasa(config)# event manager applet blockcheck
ciscoasa(config-applet)# description "Log block usage"
ciscoasa(config-applet)# event timer watchdog time 3600
ciscoasa(config-applet)# output rotate 24
ciscoasa(config-applet)# action 1 cli command "show blocks old"
```

次に、毎日午前 1 時に ASA をリブートし、必要に応じて設定を保存するイベント マネージャ アプレットの例を示します。

```
ciscoasa(config)# event manager applet dailyreboot
ciscoasa(config-applet)# description "Reboot every night"
ciscoasa(config-applet)# event timer absolute time 1:00:00
ciscoasa(config-applet)# output none
ciscoasa(config-applet)# action 1 cli command "reload save-config noconfirm"
```

次に、午前 0 時から午前 3 時の間に特定のインターフェイスをディセーブルにするイベント マネージャ アプレットの例を示します。

```
ciscoasa(config)# event manager applet disableintf
ciscoasa(config-applet)# description "Disable the interface at midnight"
ciscoasa(config-applet)# event timer absolute time 0:00:00
ciscoasa(config-applet)# output none
ciscoasa(config-applet)# action 1 cli command "interface GigabitEthernet 0/0"
ciscoasa(config-applet)# action 2 cli command "shutdown"
ciscoasa(config-applet)# action 3 cli command "write memory"

ciscoasa(config)# event manager applet enableintf
ciscoasa(config-applet)# description "Enable the interface at 3am"
ciscoasa(config-applet)# event timer absolute time 3:00:00
ciscoasa(config-applet)# output none
ciscoasa(config-applet)# action 1 cli command "interface GigabitEthernet 0/0"
ciscoasa(config-applet)# action 2 cli command "no shutdown"
ciscoasa(config-applet)# action 3 cli command "write memory"
```

EEM のモニタリング

EEM をモニタするには、次のコマンドを参照してください。

- **clear configure event manager**

  このコマンドは、イベント マネージャの実行コンフィギュレーションを削除します。

- **clear configure event manager applet** *appletname*

  このコマンドは、コンフィギュレーションから指定のイベント マネージャ アプレットを削除します。

- **show counters protocol eem**

  このコマンドは、イベント マネージャのカウンタを表示します。

- **show event manager**

  このコマンドは、ヒット カウントやイベント マネージャ アプレットが最後に呼び出されたのはいつかなど、設定されたイベント マネージャ アプレットに関する情報を表示します。

- **show memory logging**、**show memory logging include**

  これらのコマンドは、メモリ割り当てとメモリ使用量に関する統計情報を表示します。

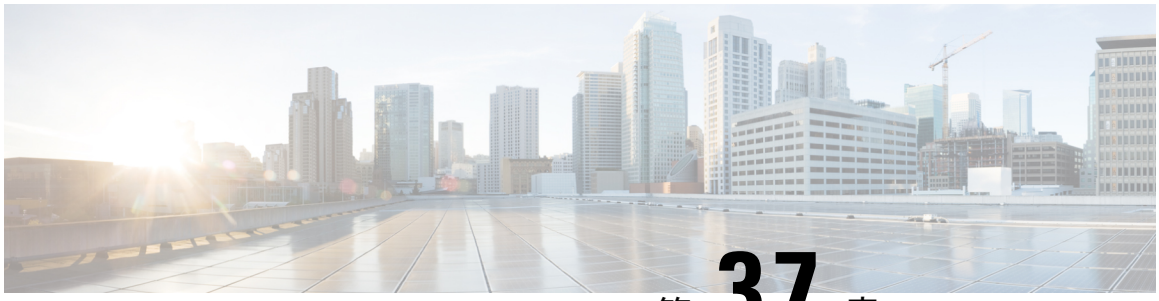
- **show running-config event manager**

  このコマンドは、イベント マネージャの実行コンフィギュレーションを表示します。

EEM の履歴

表 *45 : EEM* の履歴

機能名	プラットフォーム リリース	説明
Embedded Event Manager（EEM）	9.2(1)	EEMサービスを利用することで、問題をデバッグし、トラブルシューティングに対して汎用ロギングを提供できます。EEMサービスには2つのコンポーネント、つまりEEMが応答またはリッスンするイベント、およびアクションと EEM が応答するイベントを定義するイベント マネージャ アプレットがあります。さまざまなイベントに応答し、さまざまなアクションを実行するために、複数のイベント マネージャ アプレットを設定できます。 **event manager applet**、**description**、**event syslog id**、**event none**、**event timer** {**watchdog time** *seconds* | **countdown time** *seconds* | **absolute time** *hh:mm:ss*}、**event crashinfo**、**action cli command**、**output** {**none** | **console** | **file** {**append** *filename* | **new** | **overwrite** *filename* | **rotate** *n*}}、**show running-config event manager**、**event manager run**、**show event manager**、**show counters protocol eem**、**clear configure event manager**、**debug event manager**、**debug menu eem** の各コマンドが導入または変更されました。
EEM のメモリ トラッキング	9.4(1)	メモリ割り当てとメモリ使用量をログに記録し、メモリ ロギング ラップ イベントに応答する新しいデバッグ機能が追加されました。 **memory logging**、**show memory logging**、**show memory logging include**、**event memory-logging-wrap** の各コマンドが導入または変更されました。



第 37 章

テストとトラブルシューティング

この章では、Cisco ASA のトラブルシューティング方法および基本接続のテスト方法について説明します。

イネーブル パスワードと Telnet パスワードの回復

イネーブル パスワードまたは Telnet パスワードを忘れた場合は、それらを回復できます。手順は、デバイス タイプによって異なります。CLI を使用してタスクを実行する必要があります。

ASA のパスワードの回復

ASA のパスワードを回復するには、次の手順を実行します。

手順

ステップ 1 ASA のコンソール ポートに接続します。

ステップ 2 ASA の電源を切ってから、再び電源をオンにします。

ステップ 3 スタートアップ後、ROMMON モードに入るようにプロンプトが表示されたら、**Escape** キーを押します。

ステップ 4 コンフィギュレーション レジスタ値をアップデートするには、次のコマンドを入力します。

```
rommon #1> confreg 0x41
Update Config Register (0x41) in NVRAM...
```

ステップ 5 スタートアップ コンフィギュレーションを無視するように ASA を設定するには、次のコマンドを入力します。

```
rommon #1> confreg
```

ASAによって現在のコンフィギュレーションのレジスタ値が表示され、それを変更するかどうかが尋ねられます。

```
Current Configuration Register: 0x00000041
Configuration Summary:
  boot default image from Flash
  ignore system configuration

Do you wish to change this configuration? y/n [n]: y
```

ステップ 6 後で回復できるように、現在のコンフィギュレーションのレジスタ値を記録します。

ステップ 7 値を変更する場合は、プロンプトに対して **Y** を入力します。

ASA によって、新しい値の入力を求めるプロンプトが表示されます。

ステップ 8 「disable system configuration?」の値を除き、すべての設定についてデフォルト値を受け入れます。

ステップ 9 プロンプトに対して、**Y** を入力します。

ステップ 10 次のコマンドを入力して、ASA をリロードします。

```
rommon #2> boot
Launching BootLoader...
Boot configuration file contains 1 entry.

Loading disk0:/asa800-226-k8.bin... Booting...Loading...
```

ASAは、スタートアップ コンフィギュレーションの代わりにデフォルト コンフィギュレーションをロードします。

ステップ 11 次のコマンドを入力して、特権 EXEC モードにアクセスします。

```
ciscoasa# enable
```

ステップ 12 パスワードの入力を求められたら、**Enter** キーを押します。

パスワードは空白です。

ステップ 13 次のコマンドを入力して、スタートアップ コンフィギュレーションをロードします。

```
ciscoasa# copy startup-config running-config
```

ステップ 14 次のコマンドを入力して、グローバル コンフィギュレーション モードにアクセスします。

```
ciscoasa# configure terminal
```

ステップ 15 次のコマンドを入力して、デフォルト コンフィギュレーションで必要に応じてパスワードを変更します。

```
ciscoasa(config)# password password
ciscoasa(config)# enable password password
ciscoasa(config)# username name password password
```

ステップ 16 次のコマンドを入力して、デフォルト コンフィギュレーションをロードします。

```
ciscoasa(config)# no config-register
```

デフォルト コンフィギュレーションのレジスタ値は 0x1 です。コンフィギュレーション レジスタの詳細については、コマンド リファレンスを参照してください。

ステップ 17 次のコマンドを入力して、新しいパスワードをスタートアップ コンフィギュレーションに保存します。

```
ciscoasa(config)# copy running-config startup-config
```

ASA 5506-X、ASA 5508-X、ASA 5516-X でのパスワードの回復

ASA 5506-X、ASA 5508-X、ASA 5516-X のパスワードの回復には、次の手順を実行します。

手順

ステップ 1 ASA のコンソール ポートに接続します。

ステップ 2 ASA の電源を切ってから、再び電源をオンにします。

ステップ 3 スタートアップ後、ROMMON モードに入るようにプロンプトが表示されたら、**Escape** キーを押します。

ステップ 4 コンフィギュレーション レジスタ値をアップデートするには、次のコマンドを入力します。

```
rommon #1> confreg 0x41

You must reset or power cycle for new config to take effect
```

ASA で現在のコンフィギュレーション レジスタ値と構成オプションのリストが表示されます。後で回復できるように、現在のコンフィギュレーションのレジスタ値を記録します。

```
Configuration Register: 0x00000041

Configuration Summary
 [ 0 ] password recovery
 [ 1 ] display break prompt
 [ 2 ] ignore system configuration
 [ 3 ] auto-boot image in disks
 [ 4 ] console baud: 9600
 boot: ...... auto-boot index 1 image in disks
```

ステップ 5 次のコマンドを入力して、ASA をリロードします。

```
rommon #2> boot
Launching BootLoader...
Boot configuration file contains 1 entry.

Loading disk0:/asa932-226-k8.bin... Booting...Loading...
```

ASAは、スタートアップ コンフィギュレーションの代わりにデフォルト コンフィギュレーションをロードします。

ステップ 6 次のコマンドを入力して、特権 EXEC モードにアクセスします。

```
ciscoasa# enable
```

ステップ 7 パスワードの入力を求められたら、**Enter** キーを押します。

パスワードは空白です。

ステップ 8 次のコマンドを入力して、スタートアップ コンフィギュレーションをロードします。

```
ciscoasa# copy startup-config running-config
```

ステップ 9 次のコマンドを入力して、グローバル コンフィギュレーション モードにアクセスします。

```
ciscoasa# configure terminal
```

ステップ 10 次のコマンドを入力して、デフォルト コンフィギュレーションで必要に応じてパスワードを変更します。

```
ciscoasa(config)# password password
ciscoasa(config)# enable password password
ciscoasa(config)# username name password password
```

ステップ 11 次のコマンドを入力して、デフォルト コンフィギュレーションをロードします。

```
ciscoasa(config)# no config-register
```

デフォルト コンフィギュレーションのレジスタ値は 0x1 です。コンフィギュレーション レジスタの詳細については、コマンド リファレンスを参照してください。

ステップ 12 次のコマンドを入力して、新しいパスワードをスタートアップ コンフィギュレーションに保存します。

```
ciscoasa(config)# copy running-config startup-config
```

ASAv でのパスワードまたはイメージの回復

ASAv のパスワードまたはイメージを回復するには、次の手順を実行します。

手順

ステップ 1 実行コンフィギュレーションを ASAv のバックアップ ファイルにコピーします。

copy running-config *filename*

例：

```
ciscoasa# copy running-config backup.cfg
```

ステップ 2 ASAv を再始動します。

reload

ステップ 3 [GNU GRUB] メニューから、下矢印を押し、**コンフィギュレーションをロードしない**オプションで <**filename**> を選択し、Enter キーを押します。ファイル名は、ASAv のデフォルトのブート イメージのファイル名です。デフォルトのブート イメージは、**fallback** コマンドによって自動的にブートされることはありません。その後、選択したブート イメージをロードします。

```
GNU GRUB version 2.0(12)4
bootflash:/asa100123-20-smp-k8.bin
bootflash: /asa100123-20-smp-k8.bin with no configuration load
```

例：

```
GNU GRUB version 2.0(12)4
bootflash: /asa100123-20-smp-k8.bin with no configuration load
```

ステップ 4 実行コンフィギュレーションにバックアップ コンフィギュレーション ファイルをコピーします。

copy *filename* **running-config**

例：

```
ciscoasa (config)# copy backup.cfg running-config
```

ステップ 5 パスワードのリセット。

enable password *password*

例：

```
ciscoasa(config)# enable password cisco123
```

ステップ 6 新しい設定を保存します。

write memory

例：

```
ciscoasa(config)# write memory
```

パスワード回復のディセーブル化

（注） ASAv 上でパスワード回復をディセーブルにすることはできません。

権限のないユーザがパスワード回復メカニズムを使用して ASA を危険にさらすことがないように、パスワード回復をディセーブルにするには、次の手順を実行します。

始める前に

ASA で、**no service password-recovery** コマンドを使用すると ROMMON モードに入って、コンフィギュレーションの変更を防ぐことができます。ROMMON モードに入ると、ASA では、すべてのフラッシュ ファイル システムの消去を求めるプロンプトが表示されます。最初に消去を実行しないと、ROMMON モードを開始できません。フラッシュ ファイル システムを消去しない場合、ASA はリロードされます。パスワード回復は ROMMON モードの使用と既存のコンフィギュレーションの保持に依存しているので、この消去によって、パスワードの回復ができなくなります。ただし、パスワードを回復できなくすることで、不正なユーザがコンフィギュレーションを表示したり、別のパスワードを挿入したりすることがなくなります。この場合、システムを動作可能な状態に回復するには、新しいイメージとバックアップ コンフィギュレーション ファイル（入手できる場合）をロードします。

service password-recovery コマンドは、コンフィギュレーション ファイルに通知用としてのみ表示されます。CLI プロンプトに対してコマンドを入力すると、設定は NVRAM に保存されます。設定を変更する唯一の方法は、CLI プロンプトでコマンドを入力することです。このコマンドの異なるバージョンで新規コンフィギュレーションをロードしても、設定は変更されません。（パスワード回復の準備段階で）スタートアップ時にスタートアップ コンフィギュレー

ションを無視するようASAが設定されている場合にパスワード回復をディセーブルにすると、通常どおりスタートアップ コンフィギュレーションをロードするようにASAの設定が変更されます。フェールオーバーを使用し、スタートアップコンフィギュレーションを無視するようにスタンバイ装置が設定されている場合は、**no service password- recovery** コマンドでスタンバイ装置に複製したときに、コンフィギュレーション レジスタに同じ変更が加えられます。

手順

パスワード回復をディセーブルにします。

no service password-recovery

例：

```
ciscoasa (config)# no service password-recovery
```

デバッグ メッセージの表示

デバッグ出力はCPUプロセスで高プライオリティが割り当てられているため、デバッグ出力を行うとシステムが使用できなくなることがあります。このため、特定の問題のトラブルシューティングを行う場合や、Cisco TACとのトラブルシューティング セッションの間に限り **debug** コマンドを使用してください。さらに、ネットワーク トラフィック量やユーザ数が少ない期間に **debug** コマンドを使用することをお勧めします。デバッギングをこのような時間帯に行うと、**debug** コマンド処理のオーバーヘッドの増加によりシステムの使用に影響が及ぶ可能性が少なくなります。デバッグ メッセージを有効にするには、コマンド リファレンスの **debug** コマンドを参照してください。

パケット キャプチャ

パケットキャプチャは、接続の問題のトラブルシューティングまたは不審なアクティビティのモニタリングを行うときに役立つことがあります。パケット キャプチャ サービスを使用する場合は、Cisco TACに連絡することをお勧めします。

パケット キャプチャのガイドライン

コンテキスト モード

- コンテキスト内のクラスタ制御リンクでキャプチャを設定できます。この場合、そのクラスタ制御リンクで送信されるコンテキストに関連付けられているパケットだけがキャプチャされます。

- VLAN ごとに設定できるキャプチャは 1 つだけです。共有 VLAN の複数のコンテキストでキャプチャを設定した場合は、最後に設定したキャプチャだけが使用されます。
- 最後に設定した（アクティブ）キャプチャを削除した場合は、別のコンテキストで事前に設定したキャプチャがあっても、アクティブになるキャプチャはありません。キャプチャをアクティブにするには、キャプチャを削除して追加し直す必要があります。
- キャプチャを指定したインターフェイスに着信するすべてのトラフィックがキャプチャされます。これには、共有 VLAN 上の他のコンテキストへのトラフィックも含まれます。したがって、ある VLAN のコンテキスト A でのキャプチャをイネーブルにしたときに、その VLAN がコンテキスト B でも使用される場合は、コンテキスト A とコンテキスト B の両方の入力トラフィックがキャプチャされます。
- 出力トラフィックの場合は、アクティブキャプチャのあるコンテキストのトラフィックだけがキャプチャされます。唯一の例外は、ICMP検査をイネーブルにしない（したがって、ICMP トラフィックのセッションが高速パスにない）場合です。この場合は、共有 VLAN のすべてのコンテキストで入力と出力の ICMP トラフィックがキャプチャされます。

その他のガイドライン

- ASA が不正な形式の TCP ヘッダーを持つパケットを受信し、ASP が *invalid-tcp-hdr-length* であるというドロップ理由でそのパケットをドロップする場合、そのパケットを受信したインターフェイス上の **show capture** コマンド出力は、そのパケットを表示しません。
- IP トラフィックだけをキャプチャできます。ARP などの非 IP パケットはキャプチャできません。
- インライン SGT タグ付きパケットの場合、キャプチャされたパケットに含まれている追加 CMD ヘッダーを、PCAP ビューアが認識しないことがあります。
- パケットキャプチャには、システムを変更する、またはインスペクションのために接続に挿入されるパケット、NAT、TCPの正規化、パケットの内容を調整するその他の機能が含まれます。

パケットのキャプチャ

パケットをキャプチャするには、次の手順を実行します。

手順

ステップ 1 パケット スニッフィングおよびネットワーク障害の切り分けのためにパケット キャプチャ機能をイネーブルにします。

capture *capture_name* [**type** {**asp-drop** [**all** | *drop-code*] | **tls-proxy** | **raw-data** | **isakmp** [**ikev1** | **ikev2**] | **inline-tag** [*tag*] | **webvpn user** *webvpn-user*}] [**access-list** *access_list_name*] {**interface** {*interface_name* | **asa_dataplane** | **asa_mgmt_plane** | **cplane**} } [**buffer** *buf_size*] [**ethernet-type** *type*] [**reeinject-hide**] [**packet-length** *bytes*] [**circular-buffer**] [**trace** [**trace-count** *number*]] [**real-time** [**dump**] [**detail**]] [

match *protocol* { **host** *source-ip* | *source-ip mask* | **any**} [*operator src_port*] { **host** *dest_ip* |*dest_ip mask* | **any**} [*operator dest_port*]]

例：

```
ciscoasa# capture captest interface inside
```

キャプチャするすべてのパケットのインターフェイスを設定する必要があります。複数のタイプのトラフィックをキャプチャするには、複数の **capture** ステートメントで同じ *capture_name* を使用します。

type asp-dropキーワードは、高速セキュリティ パスでドロップされるパケットをキャプチャします。クラスタでは、ドロップされた、ユニット間の転送データ パケットもキャプチャされます。マルチ コンテキスト モードでは、このオプションがシステム実行スペースで発行されると、すべてのドロップされたデータ パケットがキャプチャされます。このオプションがコンテキストで発行されたときは、ドロップされたデータ パケットのうち、そのコンテキストに属するインターフェイスから入ったものだけがキャプチャされます。

type raw-data キーワードは、着信パケットと発信パケットをキャプチャします。この設定は、デフォルトです。

inline-tag *tag* のキーワードと引数のペアは、特定の SGT 値のタグを指定します。指定しない場合は、任意の SGT 値を持つタグ付きパケットをキャプチャします。

buffer キーワードは、パケットを保存するために使用するバッファ サイズを定義します。このバイト バッファがいっぱいになると、パケット キャプチャは停止します。クラスタ内で使用されるときは、これはユニットあたりのサイズです（全ユニットの合計ではありません）。**circular-buffer** キーワードを指定すると、バッファがいっぱいになったときに、バッファが先頭から順に上書きされます。

interface キーワードは、パケット キャプチャを使用するインターフェイスの名前を設定します。

データプレーン上のパケットをキャプチャするには、**asa_dataplane** キーワードを使用します。追加モジュール バックプレーン上でキャプチャされたパケットをフィルタ処理するには、**asa_dataplane** オプションを使用し、これらのガイドラインに従います。シングル モードでは、バックプレーン制御パケットは、アクセス リストをバイパスしてキャプチャされます。マルチ コンテキスト モードでは、制御パケットのみがシステム実行スペースでキャプチャされます。データ パケットは、コンテキストでキャプチャされます。

match キーワードは、一致するプロトコルおよび送信元と宛先 IP アドレス、およびオプションのポートをキャプチャします。このキーワードは、1 つのコマンドで 3 回まで使用できます。**any**キーワードは、IPv4 トラフィックだけをキャプチャします。operator には次のいずれかを指定できます。

- lt：より小さい
- gt：より大きい
- eq：等しい

real-time キーワードを指定すると、キャプチャしたパケットがリアルタイムで連続して表示されます。

reinject-hide キーワードを指定すると、再注入されたパケットはキャプチャされません。これは、クラスタリング環境にのみ適用されます。

（注） ACL の最適化が設定されている場合、**access-list** コマンドはキャプチャでは使用できません。**access-group** コマンドのみ使用できます。この場合、**access-list** コマンドを使用しようとするとエラーが表示されます。

ステップ 2 クラスタ制御リンク トラフィックをキャプチャします。

capture*capture_name*{ **type lacp interface** *interface_id* [**buffer** *buf_size*] [**packet-length** *bytes*] [**circular-buffer**] [**real-time** [**dump**] [**detail**]

capture *capture_name* **interface cluster** [**buffer** *buf_size*] [**ethernet-type** *type*] [**packet-length** *bytes*] [**circular-buffer**] [**trace** [**trace-count** *number*]] [**real-time** [**dump**] [**detail**]] [**trace**] [**match** *protocol* { **host** *source-ip* | *source-ip mask* | **any**} [*operator src_port*] { **host** *dest_ip* |*dest_ip mask* | **any**} [*operator dest_port*]]

例：

```
ciscoasa# capture ccl type lacp interface GigabitEthernet0/0
ciscoasa# capture ccl interface cluster match udp any eq 49495 any
ciscoasa# capture ccl interface cluster match udp any any eq 49495
```

次の2つの方法でクラスタ制御リンクのトラフィックをキャプチャできます。クラスタ制御リンクのすべてのトラフィックをキャプチャするには、インターフェイス名に **cluster** キーワードを使用します。cLACPパケットのみをキャプチャするには**type lacp** を指定し、インターフェイス名ではなく物理インターフェイス ID を指定します。クラスタ制御リンク上のパケットには、コントロール プレーン パケットとデータ プレーン パケットの 2 種類があり、どちらも、転送されたデータ トラフィックとクラスタ LU メッセージが含まれています。IPアドレスヘッダーの TTL フィールドは、この 2 種類のパケットを区別できるように符号化されます。転送されたデータ パケットがキャプチャされるときは、デバッグのためにクラスタリング トレーラもキャプチャ ファイルに出力されます。

ステップ 3 クラスタ全体のパケットをキャプチャします。

cluster exec capture *capture_name arguments*

ステップ 4 パケット キャプチャを停止します。

no capture *capture_name*

リアルタイム パケット キャプチャを終了するには、**Ctrl + c** を入力します。キャプチャを完全に削除するには、このコマンドの **no** 形式を使用します。リアルタイム オプションは、**raw-data** キャプチャおよび **asp-drop** キャプチャにのみ適用されます。

ステップ 5 キャプチャをクリアします。

clear capture *capture_name*

例

コントロール プレーン パケット

コントロールプレーンと通信するすべてのパケットはTTLが255に設定されており、ポート番号49495がクラスタリング コントロール プレーン リッスン ポートに使用されます。次の例では、クラスタリング環境のLACPキャプチャを作成する方法を示します。

```
ciscoasa# capture lacp type lacp interface GigabitEthernet0/0
```

次の例では、クラスタリングリンクでの制御パスパケットのキャプチャを作成する方法を示します。

```
ciscoasa# capture cp interface cluster match udp any eq 49495 any
ciscoasa# capture cp interface cluster match udp any any eq 49495
```

データ プレーン パケット

データ パケットには、1つのユニットから別のユニット（その接続の所有者）に転送されるパケットと、クラスタLUメッセージが含まれます。通常のクラスタLU更新メッセージは、TTLが254に設定されており、TTLが253に設定された特別なLUパケットがあります。この特別なLUパケットはTCPのみで、ディレクタが新しいフローの所有者を選択した場合にのみ発生します。ディレクタはCLU_FULLアップデートパケットとともに要求パケットを送り返します。LUパケットには、元のパケットのL3/L4ヘッダーが書き込まれます。これにより、受信者側で潜在的な競合状態が発生するのを回避できます。転送されるデータパケットは、TTLが4未満に設定されます。次の例では、クラスタ制御リンクでデータパスパケットのキャプチャを作成する方法を示します。クラスタ間データプレーンの「flow logical update」メッセージをすべてキャプチャするには、ポート4193を使用します。

```
ciscoasa# access-list cc1 extended permit udp any any eq 4193
ciscoasa# access-list cc1 extended permit udp any eq 4193 any
ciscoasa# capture dp interface cluster access-list cc1
```

パケット キャプチャの表示

CLIでパケット キャプチャをブラウザ上に表示したり、任意のサーバにキャプチャをダウンロードしたりすることができます。

手順

ステップ1 CLIでキャプチャを表示するには：

[**cluster exec**] **show capture** [*capture_name*] [**access-list** *access_list_name*] [**count** *number*] [**decode**] [**detail**] [**dump**] [**packet-number** *number*]

例：

```
ciscoasa# show capture capin

 8 packets captured

 1: 03:24:35.526812       192.168.10.10 > 203.0.113.3: icmp: echo request
 2: 03:24:35.527224       203.0.113.3 > 192.168.10.10: icmp: echo reply
 3: 03:24:35.528247       192.168.10.10 > 203.0.113.3: icmp: echo request
 4: 03:24:35.528582       203.0.113.3 > 192.168.10.10: icmp: echo reply
 5: 03:24:35.529345       192.168.10.10 > 203.0.113.3: icmp: echo request
 6: 03:24:35.529681       203.0.113.3 > 192.168.10.10: icmp: echo reply
 7: 03:24:57.440162       192.168.10.10 > 203.0.113.3: icmp: echo request
 8: 03:24:57.440757       203.0.113.3 > 192.168.10.10: icmp: echo reply
```

access-list キーワードは、特定のアクセス リスト ID の IP フィールドまたはより高位のフィールドに基づいて、パケットに関する情報を表示します。

cluster exec キーワードを使用すると、あるユニットで **show capture** コマンドを発行し、他のすべてのユニットでそのコマンドを同時に実行できます。

count キーワードは、指定したデータのパケット数を表示します。

decode キーワードは、**isakmp** タイプのキャプチャがインターフェイスに適用される場合に役立ちます。当該のインターフェイスを通過する ISAKMP データは、復号化の後にすべてキャプチャされ、フィールドをデコードした後にその他の情報とともに表示されます。

detail キーワードは、各パケットの追加のプロトコル情報を表示します。

dump キーワードは、データ リンク経由で転送されたパケットの 16 進ダンプを表示します。

packet-number キーワードは、指定したパケット番号で表示を開始します。

ステップ 2 ブラウザでパケット キャプチャを表示するには：

https://*ip_of_asa*/**admin/capture/***capture_name*/**pcap**

pcap キーワードを省略すると、**show capture** *capture_name* コマンド出力に相当する内容のみが表示されます。

マルチ コンテキスト モードでは、システム実行スペースでのみ **copy capture** コマンドを使用できます。

ステップ 3 パケット キャプチャをサーバにコピーします。この例では FTP を示します。

[**cluster exec**] **copy /pcap capture:**[*context-name/*]*capture_name* **ftp://***username***:***password***@***server_ip***/***path*

pcap キーワードを省略すると、**show capture** *capture_name* コマンド出力に相当する内容のみが表示されます。

例

次の例は、asp-drop タイプのキャプチャを示します。

```
ciscoasa# capture asp-drop type asp-drop acl-drop
ciscoasa# show capture asp-drop

 2 packets captured

 1: 04:12:10.428093       192.168.10.10.34327 > 10.94.0.51.15868: S
    2669456341:2669456341(0) win 4128 <mss 536> Drop-reason: (acl-drop)
    Flow is denied by configured rule
 2: 04:12:12.427330       192.168.10.10.34327 > 10.94.0.51.15868: S
    2669456341:2669456341(0) win 4128 <mss 536> Drop-reason: (acl-drop)
    Flow is denied by configured rule
 2 packets shown

ciscoasa# show capture asp-drop

 2 packets captured

 1: 04:12:10.428093       192.168.10.10.34327 > 10.94.0.51.15868: S
    2669456341:2669456341(0) win 4128 <mss 536> Drop-reason: (acl-drop)
    Flow is denied by configured rule
 2: 04:12:12.427330       192.168.10.10.34327 > 10.94.0.51.15868: S
    2669456341:2669456341(0) win 4128 <mss 536> Drop-reason: (acl-drop)
    Flow is denied by configured rule
 2 packets shown
```

次の例は、ethernet タイプのキャプチャを示します。

```
ciscoasa# capture arp ethernet-type arp interface inside
ciscoasa# show cap arp

22 packets captured

   1: 05:32:52.119485       arp who-has 10.10.3.13 tell 10.10.3.12
   2: 05:32:52.481862       arp who-has 192.168.10.123 tell 192.168.100.100
   3: 05:32:52.481878       arp who-has 192.168.10.50 tell 192.168.100.10
   4: 05:32:53.409723       arp who-has 10.106.44.135 tell 10.106.44.244
   5: 05:32:53.772085       arp who-has 10.106.44.108 tell 10.106.44.248
   6: 05:32:54.782429       arp who-has 10.106.44.135 tell 10.106.44.244
   7: 05:32:54.784695       arp who-has 10.106.44.1 tell 11.11.11.112:
```

クラッシュ ダンプの表示

ASA または ASAv がクラッシュした場合に、クラッシュ ダンプ情報を表示できます。クラッシュ ダンプの内容を調べる必要がある場合は、Cisco TAC に連絡することを推奨します。コマンド リファレンスで **show crashdump** コマンドを参照してください。

コア ダンプの表示

コア ダンプは、プログラムが異常終了（クラッシュ）したときの、実行中のプログラムのスナップショットです。コア ダンプは、エラーを診断またはデバッグするため、および障害を後からオフサイトで分析できるよう、クラッシュを保存するために使用されます。ASA または ASAv でのアプリケーション/システム クラッシュをトラブルシューティングするために、コア ダンプ機能を有効にするよう Cisco TAC から要請される場合があります。コマンド リファレンスで **coredump** コマンドを参照してください。

ASAv の vCPU 使用量

ASAv の vCPU 使用率では、データ パス、制御ポイント、および外部プロセスで使用されている vCPU の量を表示します。

vSphere で報告される vCPU の使用率には、この ASAv の使用率に加えて、次のものが含まれます。

- ASAv アイドル時間
- ASAv VM に使用された %SYS オーバーヘッド
- vSwitch、vNIC および pNIC の間を移動するパケットのオーバーヘッド。このオーバーヘッドは非常に大きくなる場合があります。

CPU 使用率の例

報告された vCPU の使用率が大幅に異なる例を次に示します。

- ASAv のレポート：40%
- DP：35%
- 外部プロセス：5%
- vSphere のレポート：95%
- ASA（ASAv レポートとして）：40%
- ASA アイドル ポーリング：10%
- オーバーヘッド：45%

オーバーヘッドは、ハイパーバイザ機能の実行、および vSwitch を使用した NIC と vNIC の間のパケット転送に使用されています。

ASAv のためのオーバーヘッドとして、ESXi サーバが追加のコンピューティング リソースを使用する場合があるため、使用率は 100% を超えることがあります。

VMware の CPU 使用率のレポート

vSphere で [VM Performance] タブをクリックし、[Advanced] をクリックすると [Chart Options] ドロップダウンリストが表示されます。ここには VM の各ステート（%USER、%IDLE、%SYS など）の vCPU 使用率が表示されます。この情報は、VMware の観点から CPU リソースが使用されている場所を理解するのに役立ちます。

ESXi サーバのシェル（ホストへの接続に SSH を使用してシェルにアクセスします）では、esxtop を使用できます。Esxtop は Linux の **top** コマンドに似た操作性と外観を持ち、次の内容を含む vSphere のパフォーマンスに関する VM のステート情報を提供します。

- vCPU、メモリ、ネットワーク使用率の詳細
- 各 VM のステートごとの vCPU 使用率
- メモリ（実行中に「M」と入力）とネットワーク（実行中に「N」と入力）に加えて、統計情報と RX ドロップ数

ASAv のグラフと vCenter のグラフ

ASAv と vCenter の間で CPU 使用率の数字に違いがあります。

- vCenter のグラフの数値は常に ASAv の数値よりも大きくなります。
- vCenter ではこの値は「%CPU usage」と呼ばれ、ASAv ではこの値は「%CPU utilization」と呼ばれます。

用語「%CPU utilization」と「%CPU usage」は別のものを意味しています。

- CPU utilization は、物理 CPU の統計情報を提供します。
- CPU usage は CPU のハイパースレッディングに基づいた論理 CPU の統計情報を提供します。しかし、1 つの vCPU のみが使用されるため、ハイパースレッディングは動作しません。

vCenter は CPU % usage を次のように計算します。

アクティブに使用された仮想 CPU の量。使用可能な CPU の合計に対する割合として指定されます。

この計算は、ホストから見た CPU 使用率であり、ゲスト オペレーティング システムから見た CPU 使用率ではありません。また、これは仮想マシンで使用可能なすべての仮想 CPU の平均 CPU 使用率になります。

たとえば、1 個の仮想 CPU を搭載した 1 つの仮想マシンが、4 個の物理 CPU を搭載した 1 台のホストで実行されており、その CPU 使用率が 100% の場合、仮想マシンは、1 個の物理 CPU をすべて使用しています。仮想 CPU の使用率は、「MHz 単位の使用率 / 仮想 CPU の数 x コア周波数」として計算されます。

使用率を MHz で比較すると、vCenter と ASAv の両方の数値は一致します。vCenter グラフから、MHz % CPU 使用率は 60/(2499 x 1 vCPU) = 2.4 と求められます。

設定のテスト

ここでは、シングル モード ASA または各セキュリティ コンテキストの接続性のテスト方法、ASA インターフェイスを ping する方法、およびあるインターフェイス上のホストから他のインターフェイス上のホストに ping できるようにする方法について説明します。

基本接続のテスト：アドレス向けの ping の実行

ping は、特定のアドレスが使用可能で、応答するかどうかを確認するための単純なコマンドです。次のトピックでは、このコマンドの詳細とそれを使って実行可能なテストについて説明します。

ping で実行可能なテスト

デバイスを ping すると、そのデバイスにパケットが送信され、デバイスが応答を返します。このプロセスを使用して、ネットワーク デバイスは、相互に検出、識別、およびテストすることができます。

ping を使用して、次のテストを実行できます。

- 2 つのインターフェイスのループバック テスト：同じ ASA で一方のインターフェイスからもう一方のインターフェイスに ping を外部ループバック テストとして起動すると、双方のインターフェイスの基本的な「アップ」ステータスおよび動作を検証できます。
- ASA の ping：別の ASA のインターフェイスを ping し、そのインターフェイスがアップしていて応答することを確認できます。
- ASA 経由の ping：ASA の反対側のデバイスを ping することによって、中間 ASA 経由で ping することができます。パケットは、それぞれの方向に移動するときに、2 つの中間 ASA のインターフェイスを通過します。このアクションは、中間ユニットのインターフェイス、動作、および応答時間の基本テストになります。
- ネットワーク デバイスの疑わしい動作をテストするための ping：ASA インターフェイスから、正常に機能していないと思われるネットワーク デバイスに ping することができます。インターフェイスが正しく設定されているにもかかわらずエコーが受信されない場合は、デバイスに問題があると考えられます。
- 中間通信をテストするための ping：ASA インターフェイスから、正常に機能することがわかっているネットワーク デバイスに ping することができます。エコーを受信した場合、中間にあるデバイスがすべて正常に動作し、物理的に正しく接続されていることが確認されたことになります。

ICMP ping と TCP ping の選択

ASA には、ICMP エコー要求パケットを送信して、エコー応答パケットを受信する従来の ping が付属しています。これは、標準ツールで、すべての仲介ネットワーク デバイスで ICMP トラ

フィックが許可される場合にうまく機能します。ICMP ping を使用して、IPv4/IPv6 アドレスまたはホスト名を ping することができます。

ただし、ICMP を禁止しているネットワークもあります。ご使用のネットワークがこれに該当する場合は、代わりに、TCP ping を使用してネットワーク接続をテストできます。TCP ping では、ping から TCP SYN パケットが送信され、応答で SYN-ACK が受信された段階でその ping が成功したと見なされます。また、TCP ping では、IPv4 アドレスまたはホスト名は ping できますが、IPv6 アドレスは ping できません。

正常な ICMP または TCP ping とは、使用されているアドレスが有効で特定のタイプのトラフィックに応答することを意味しているにすぎません。これは基本接続が機能していることを意味します。デバイス上で動作する他のポリシーで、特定のタイプのトラフィックがデバイスを通過できないようにすることができます。

ICMP の有効化

デフォルトでは、セキュリティの高いインターフェイスからセキュリティの低いインターフェイスへの ping を実行できます。リターン トラフィックを通過させるように ICMP インスペクションをイネーブルにすることだけが必要です。セキュリティの低いインターフェイスから高いインターフェイスに ping するには、トラフィックを許可する ACL を適用する必要があります。

ASA インターフェイスを ping する場合は、そのインターフェイスに適用された ICMP ルールによって、エコー要求パケットとエコー応答パケットが許可される必要があります。ICMP ルールは省略可能です。このルールを設定しなかった場合は、インターフェイスへのすべての ICMP トラフィックが許可されます。

この手順では、ASA インターフェイスの ICMP ping をイネーブルにするため、または、ASA 経由の ping 用に構成する必要のある ICMP コンフィギュレーションのすべてについて説明します。

手順

ステップ 1 ICMP ルールでエコー要求/エコー応答が許可されることを確認します。

ICMP ルールは、省略可能で、インターフェイスに直接送信される ICMP パケットに適用されます。ICMP ルールを適用しなかった場合は、すべての ICMP アクセスが許可されます。この場合は、アクションが不要です。

ただし、ICMP ルールを実装する場合は、少なくとも以下の「inside」をご使用のデバイスのインターフェイス名に置き換えたものが各インターフェイスに含まれていることを確認します。

```
ciscoasa(config)# icmp permit 0.0.0.0 0.0.0.0 echo inside
ciscoasa(config)# icmp permit 0.0.0.0 0.0.0.0 echo-reply inside
```

ステップ 2 アクセス ルールで ICMP が許可されることを確認します。

ASA 経由でホストを ping する場合は、アクセス ルールで ICMP トラフィックの送受信が許可される必要があります。アクセス ルールは、少なくとも、エコー要求/エコー応答 ICMP パケッ

トを許可する必要があります。これらのルールはグローバルルールとして追加することができます。

アクセスルールがインターフェイスに適用されている、または、グローバルに適用されている場合は、次のようなルールを関連 ACL に追加するだけです。

```
ciscoasa(config)# access-list outside_access_in extendedpermit icmp any
anyecho
ciscoasa(config)# access-list outside_access_in extendedpermit icmp any
anyecho-reply
```

または、すべての ICMP を許可するだけです。

```
ciscoasa(config)# access-list outside_access_in extendedpermit icmp any any
```

アクセスルールを使用しない場合は、必要な他のタイプのトラフィックも許可する必要があります。これは、インターフェイスにアクセス ルールを適用すると、暗黙の deny が追加されるため、他のすべてのトラフィックが破棄されるためです。ACL をインターフェイスに適用する、または、グローバルに適用するには、**access-group** コマンドを使用します。

単にテスト目的でルールを追加する場合は、**access-list** コマンドの **no** 形式を使用して ACL からルールを削除できます。ACL 全体をテストするだけの場合は、**no access-group** コマンドを使用してインターフェイスから ACL を削除します。

ステップ 3 ICMP インスペクションをイネーブルにします。

インターフェイスの ping とは対照的に、ASA 経由で ping する場合は、ICMP インスペクションが必要です。インスペクションを使用すれば、リターントラフィック（つまり、エコー応答パケット）を ping を開始したホストに返すことができるうえ、パケットあたり 1 つの応答の存在が保証されるため、特定のタイプの攻撃を防止することができます。

ICMPインスペクションは、デフォルトのグローバルインスペクションポリシーでイネーブルにできます。

```
ciscoasa(config)# policy-map  global_policy
ciscoasa(config-pmap)# class inspection_default
ciscoasa(config-pmap-c)# inspect icmp
```

ホストの ping

デバイスを ping するには、**ping 10.1.1.1** や **ping www.example.com** のように IP アドレスやホスト名と一緒に **ping** を入力します。TCP ping の場合は、**ping tcp www.example.com 80** のように **tcp** キーワードと宛先ポートを含めます。通常は、実行する必要のあるテストの範囲にします。

成功した ping の出力例：

```
Sending 5, 100-byte ICMP Echos to out-pc, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
```

ping が失敗した場合は、失敗した試行が？で示され、成功率が 100% 未満になります（すべて失敗した場合は 0% になります）。

```
Sending 5, 100-byte ICMP Echos to 10.132.80.101, timeout is 2 seconds:
?????
Success rate is 0 percent (0/5)
```

ただし、pingの一部の側面を制御するパラメータを追加することもできます。以下に基本オプションを示します。

- ICMP ping。

  ping [*if_name*] *host* [**repeat** *count*] [**timeout** *seconds*] [**data** *pattern*] [**size** *bytes*] [**validate**]

  それぞれの説明は次のとおりです。

  - *if_name* は、ホストにアクセス可能なインターフェイスの名前です。名前を含めない場合は、ルーティングテーブルを使用して、使用するインターフェイスが決定されます。
  - *host* は、ping するホストの IPv4 アドレス、IPv6 アドレス、またはホスト名です。
  - **repeat** *count* は、送信するパケット数です。デフォルトは 5 分です。
  - **timeout** *seconds* は、応答がなかった場合にタイムアウトするパケットごとの秒数です。デフォルトは 2 です。
  - **data** *pattern* は、送信するパケットに使用される 16 進数のパターンです。デフォルトは 0xabcd です。
  - **size** *bytes* は、送信するパケットの長さです。デフォルト値は 100 バイトです。
  - **validate** は、応答データを検証する必要があることを示します。

- TCP ping。

  ping tcp [*if_name*] *host* [*port*] [**repeat** *count*] [**timeout** *seconds*] [**source** *host* [*ports*]

  それぞれの説明は次のとおりです。

  - *if_name* は、送信元が ping を送信するインターフェイスです。名前を含めなかった場合は、ルーティング テーブルが使用されます。
  - *host* は、ping する宛先の IPv4 アドレスまたはホスト名です。TCP ping は IPv6 アドレスと一緒に使用できません。
  - *port* は、ping するホストの TCP ポートです。
  - **repeat** と **timeout** は、上記と同じ意味です。

- **source** *host port* は、ping 用の送信元ホストとポートを示します。ランダム ポートを取得するには、ポート 0 を使用します。

- インタラクティブ ping。

  ping

  パラメータを指定せずに ping を入力した場合は、インターフェイス、宛先、およびキーワードとして使用できない拡張パラメータを含むその他のパラメータが要求されます。ping パケットを細かく制御する必要がある場合は、この方式を使用します。

ASA 接続の体系的なテスト

ASA 接続のさらに体系的なテストを実行する場合は、次の一般的な手順を使用できます。

始める前に

手順で説明した syslog メッセージを確認する場合は、ロギングをイネーブルにします（**logging enable** コマンドまたは ASDM の [Configuration] > [Device Management] > [Logging] > [Logging Setup]）。

また、必須ではありませんが、ICMP デバッグをイネーブルにして、外部デバイスから ASA インターフェイスを ping したときのメッセージを ASA コンソールに表示することもできます（ASA を通過する ping に関するデバッグ メッセージは表示されません）。ping メッセージとデバッグ メッセージをイネーブルにするのはトラブルシューティング中だけにすることをお勧めします。これらのメッセージはパフォーマンスに影響する可能性があります。次に、ICMP デバッグをイネーブルにして、Telnet または SSH セッションに送信する syslog メッセージを設定し、それらをセッションに送信して、ロギングをイネーブルにする例を示します。または、**logging monitor debug** コマンドの代わりに、**logging buffer debug** コマンドを使用してログ メッセージをバッファに送信し、後で **show logging** コマンドを使用してそれらを表示することもできます。

```
ciscoasa(config)# debug icmp trace
ciscoasa(config)# logging monitor debug
ciscoasa(config)# terminal monitor
ciscoasa(config)# logging enable
```

この設定では、外部ホスト（209.165.201.2）から ASA の外部インターフェイス（209.165.201.1）への ping が成功すると、次のように表示されます。

```
ciscoasa(config)# debug icmp trace
Inbound ICMP echo reply (len 32 id 1 seq 256) 209.165.201.1 > 209.165.201.2
Outbound ICMP echo request (len 32 id 1 seq 512) 209.165.201.2 > 209.165.201.1
Inbound ICMP echo reply (len 32 id 1 seq 512) 209.165.201.1 > 209.165.201.2
Outbound ICMP echo request (len 32 id 1 seq 768) 209.165.201.2 > 209.165.201.1
Inbound ICMP echo reply (len 32 id 1 seq 768) 209.165.201.1 > 209.165.201.2
Outbound ICMP echo request (len 32 id 1 seq 1024) 209.165.201.2 > 209.165.201.1
Inbound ICMP echo reply (len 32 id 1 seq 1024) 209.165.201.1 > 209.165.201.2
```

この出力では、ICMP パケット長（32 バイト）、ICMP パケット識別子（1）、および ICMP シーケンス番号（ICMP シーケンス番号は 0 から始まり、要求が送信されるたびに増分されます）が示されています。

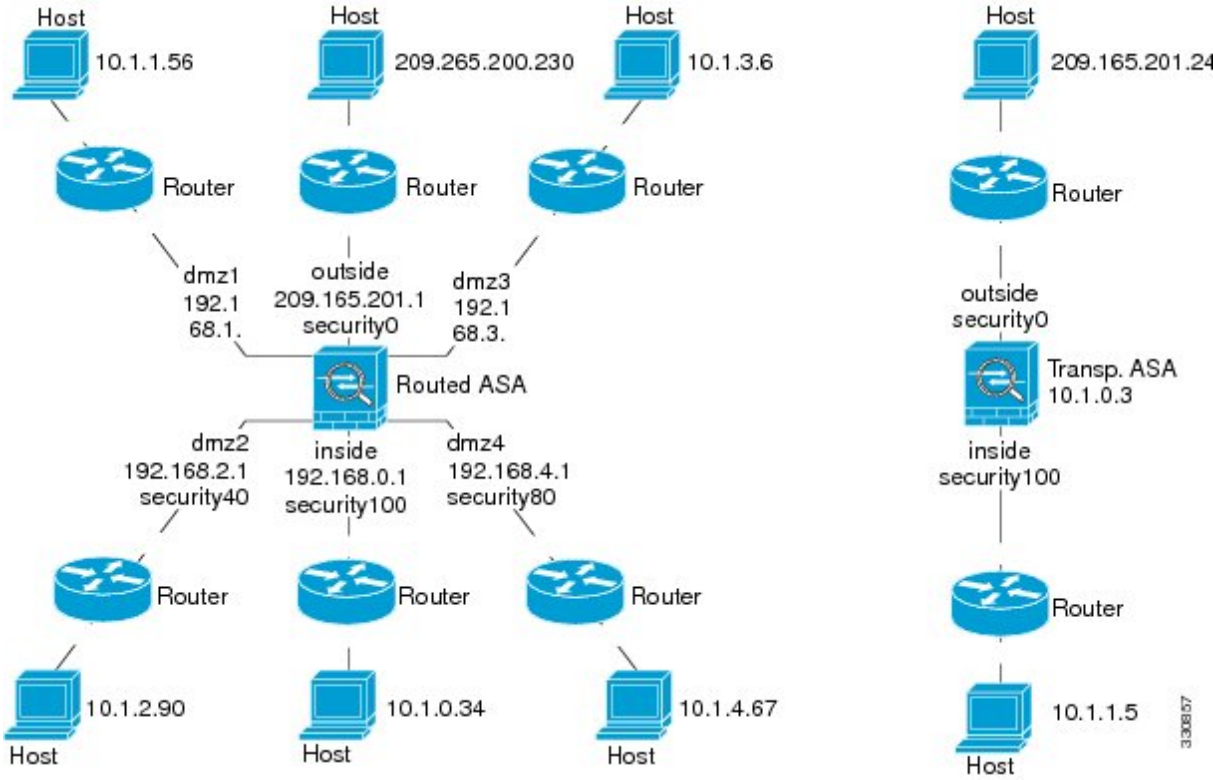
テストが終了したら、デバッグをディセーブルにします。この設定をそのままにしておくと、パフォーマンスとセキュリティのリスクが高まります。テストのためだけにロギングをイネーブルにした場合は、それもディセーブルにできます。

```
ciscoasa(config)# no debug icmp trace
ciscoasa(config)# no logging monitor debug
ciscoasa(config)# no terminal monitor
ciscoasa(config)# no logging enable
```

手順

ステップ 1 インターフェイス名、セキュリティ レベル、および IP アドレスを示すシングル モードの ASA またはセキュリティ コンテキストの図を作成します。図には、直接接続されたすべてのルータ、および ASA を ping するルータの反対側にあるホストも含める必要があります。

図 *59*：インターフェイス、ルータ、およびホストを含むネットワーク図



ステップ 2 直接接続されたルータから各 ASA インターフェイスを ping します。トランスペアレント モードでは、BVI IP アドレスを ping します。このテストでは、ASA インターフェイスがアクティブであること、およびインターフェイス コンフィギュレーションが正しいことを確認します。

ASA インターフェイスがアクティブではない場合、インターフェイス コンフィギュレーションが正しくない場合、または ASA とルータの間でスイッチがダウンしている場合、ping は失敗する可能性があります（次の図を参照）。この場合は、パケットが ASA に到達しないので、デバッグ メッセージや syslog メッセージは表示されません。

図 *60 : ASA* インターフェイスでの *ping* の失敗

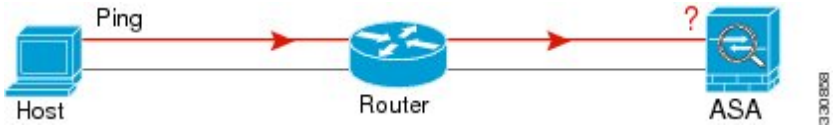
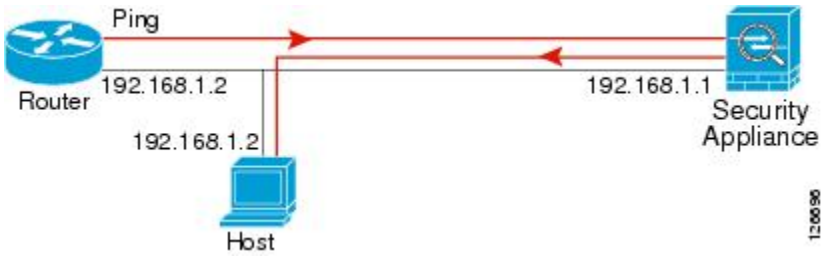


図 *61 : IP* アドレッシングの問題による *ping* の失敗



ping 応答がルータに戻されない場合は、スイッチ ループまたは冗長 IP アドレスが存在する可能性があります（次の図を参照）。

ステップ 3 リモート ホストから各 ASA インターフェイスを ping します。トランスペアレント モードでは、BVI IP アドレスを ping します。このテストでは、直接接続されたルータがホストと ASA の間でパケットをルーティングできるかどうか、および ASA がパケットを正確にルーティングしてホストに戻せるかどうかを確認します。

中間ルータを通ってホストに戻るルートが ASA にない場合、ping は失敗する可能性があります（次の図を参照）。この場合は、デバッグ メッセージは ping が成功したことを示しますが、ルーティングの失敗を示す syslog メッセージ 110001 が表示されます。

図 *62 : ASA* の戻りルート未設定による *ping* の失敗

ステップ 4 ASA インターフェイスから既知のネットワーク デバイスへの ping は正しく機能しています。

- ping を受信しない場合は、送信ハードウェアまたはインターフェイスのコンフィギュレーションに問題がある可能性があります。
- ASA のインターフェイスが正しく設定されているにもかかわらず、「既知の正常な」デバイスからエコー応答を受信しない場合は、インターフェイス ハードウェアの受信機能に問題があると考えられます。「既知の正常な」受信機能を持つ別のインターフェイスで、同じ「既知の正常な」デバイスに対して ping を送信してエコーを受信できる場合、最初のインターフェイスのハードウェアの受信機能に問題があると確認されたことになります。

ステップ 5 ホストまたはルータから発信元インターフェイスを介して別のインターフェイス上の別のホストまたはルータに ping します。確認が必要なすべてのインターフェイス ペアに対して、このステップを繰り返します。NAT を使用する場合は、このテストを行うと NAT が正しく動作していることがわかります。

ping が成功すると、ルーテッド モードのアドレス変換（305009 または 305011）と ICMP 接続が確立されたこと（302020）を確認する syslog メッセージが表示されます。**show xlate** コマンドまたは **show conns** コマンドを入力してこの情報を表示することもできます。

NAT が正しく設定されていないことが原因で、ping に失敗することもあります。この場合、NAT が失敗したことを示す syslog メッセージが表示されます（305005 または 305006）。ping が外部ホストから内部ホストへ送信され、スタティック変換が存在しない場合は、メッセージ 106010 が表示されます。

図 *63 : ASA* のアドレス変換の問題による *ping* の失敗

ホストまでのルートの追跡

IP アドレスへのトラフィックの送信で問題が発生している場合は、ホストまでのルートを追跡することによってネットワーク パスに問題がないかどうかを確認できます。

手順

ステップ 1 トレース ルート上の ASA の表示 （1085 ページ）。

ステップ 2 パケット ルートの決定 （1087 ページ）を使用して無効にすることができます。

トレース ルート上の ASA の表示

デフォルトで、ASA はトレース ルート上にホップとして表示されません。これを表示するには、ASA を通過するパケットの存続可能時間を減らして、ICMP 到達不能メッセージのレート制限を増やす必要があります。

手順

ステップ 1 L3/L4 クラスマップを作成して、接続の設定をカスタマイズするトラフィックを識別します。

class-map *name*

match *parameter*

例：

```
ciscoasa(config)# class-map CONNS
ciscoasa(config-cmap)# match any
```

照合文の詳細については、ファイアウォール設定ガイドのサービス ポリシーに関する章を参照してください。

ステップ 2 クラスマップ トラフィックで実行するアクションを設定するポリシーマップを追加または編集して、クラス マップを指定します。

policy-map *name* **class** *name*

例：

```
ciscoasa(config)# policy-map global_policy
ciscoasa(config-pmap)# class CONNS
```

デフォルト設定では、global_policy ポリシーマップはすべてのインターフェイスにグローバルに割り当てられます。global_policy を編集する場合は、ポリシー名として global_policy を入力します。クラス マップの場合、この手順ですでに作成したクラスを指定します。

ステップ 3 クラスと一致するパケットの存続可能時間（TTL）を減らします。

```
set connection decrement-ttl
```

ステップ 4 既存のサービス ポリシー（global_policy という名前のデフォルト グローバル ポリシーなど）を編集している場合は、このステップを省略できます。それ以外の場合は、1 つまたは複数のインターフェイスでポリシー マップをアクティブにします。

service-policy *policymap_name* {**global** | **interface** *interface_name* }

例：

```
ciscoasa(config)# service-policy global_policy global
```

global キーワードはポリシー マップをすべてのインターフェイスに適用し、**interface** はポリシーを 1 つのインターフェイスに適用します。グローバル ポリシーは 1 つしか適用できません。インターフェイスのグローバル ポリシーは、そのインターフェイスにサービス ポリシーを適用することで上書きできます。各インターフェイスには、ポリシーマップを 1 つだけ適用できます。

ステップ 5 トレース ルートの出力に ASA が表示されるように、ICMP 到達不能メッセージのレート制限を増やします。

icmp unreachable rate-limit *rate* **burst-size** *size*

例：

```
ciscoasa(config)# icmp unreachable rate-limit 50 burst-size 1
```

レート制限は 1 ～ 100 の範囲で設定できます。デフォルトは 1 です。バースト サイズは動作には影響しませんが、1 ～ 10 の範囲で設定する必要があります。

例

次の例では、すべてのトラフィックの TTL をグローバルに減らして、ICMP 到達不能制限を 50 に増やします。

```
ciscoasa(config)# class-map global-policy
ciscoasa(config-cmap)# match any
ciscoasa(config-cmap)# exit
ciscoasa(config)# policy-map global_policy
ciscoasa(config-pmap)# class global-policy
ciscoasa(config-pmap-c)# set connection decrement-ttl
ciscoasa(config-pmap-c)# exit
ciscoasa(config)# icmp unreachable rate-limit 50 burst-size 6
```

パケット ルートの決定

traceroute を使用すれば、パケットが宛先に到着するまでのルートを特定できます。traceroute は、無効なポート上の宛先に UDP パケットを送信することで機能します。ポートが有効でないため、宛先への途中にあるルータは ICMP Time Exceeded Message で応答し、そのエラーを ASA に報告します。

traceroute は送信された各プローブの結果を表示します。出力の各行が 1 つの TTL 値に対応します（昇順）。次の表に、出力記号の説明を示します。

出力記号	説明
*	タイムアウトの期間内にプローブへの応答を受信しませんでした。
nn msec	各ノードに対する、指定した数のプローブのラウンドトリップ時間（ミリ秒）。
!N.	ICMP ネットワークに到達できません。
!H	ICMP ホストに到達できません。
!P	ICMP に到達できません。
!A	ICMP が設定によって禁止されています。
?	ICMP の原因不明のエラーが発生しました。

始める前に

traceroute は IPv6 をサポートしません。

手順

宛先までのルートを追跡します。

traceroute [*destination_ip* | *hostname*} [**source** {*source_ip* | *source-interface*}] [**numeric**] [**timeout** *timeout_value*] [**probe** *probe_num*] [**ttl** *min_ttl max_ttl*] [**port** *port_value*] [**use-icmp**]

例：

```
ciscoasa# traceroute 209.165.200.225

Type escape sequence to abort.
Tracing the route to 209.165.200.225

1 10.83.194.1 0 msec 10 msec 0 msec
2 10.83.193.65 0 msec 0 msec 0 msec
3 10.88.193.101 0 msec 10 msec 0 msec
4 10.88.193.97 0 msec 0 msec 10 msec
5 10.88.239.9 0 msec 10 msec 0 msec
6 10.88.238.65 10 msec 10 msec 0 msec
7 172.16.7.221 70 msec 70 msec 80 msec
8 209.165.200.225 70 msec 70 msec 70 msec
```

通常は、宛先 IP アドレスまたはホスト名を含める（**traceroute www.example.com** など）だけです。ただし、必要に応じて、トレースの特性を調整できます。

- **source** {*source_ip*|*source-interface*}：トレースの送信元として使用するインターフェイスを指定します。インターフェイスは、名前または IP アドレスで指定できます。トランスペアレント モードでは、管理アドレスを使用する必要があります。
- **numeric**：IP アドレスのみをトレース ルートに表示するように指示します。このキーワードを指定しなかった場合は、DNS が設定されていれば、トレースルートでアドレスの DNS 参照が実行され、DNS 名が追加されます。
- **timeout** *timeout_value*：タイムアウトするまで応答を待機する時間。デフォルトは 3 秒です。
- **probe** *probe_num*：各 TTL レベルで送信するプローブの数。デフォルトは 3 です。
- **ttl** *min_ttl* max_ttl：プローブの最小および最大存続可能時間。デフォルトの最小値は 1 ですが、この値を増やして、既知のホップの表示を抑制することができます。デフォルトの最大値は 30 です。トレースルートは、パケットが宛先に到達するか、または最大値に達すると終了します。
- **port** *port_value*：使用する UDP ポート。デフォルトは 33434 です。
- **use-icmp**：プローブの UDP パケットの代わりに ICMP パケットを送信します。

パケット トレーサを使用したポリシー設定のテスト

送信元と宛先のアドレスおよびプロトコルの特性に基づいてパケットをモデル化することによってポリシー設定をテストできます。トレースは、ポリシー参照を実行してアクセスルールや NAT などをテストし、パケットを許可するか、拒否するかを確認します。

このようにパケットをテストすることによって、ポリシーの結果を確認し、必要に応じて、許可または拒否するトラフィックのタイプが処理されるかどうかをテストできます。設定の確認に加えて、トレーサを使用して許可すべきパケットが拒否されるなどの予期せぬ動作をデバッグできます。

手順

ステップ 1 このコマンドは複雑なため、複数の部分に分けて説明します。トレース用のインターフェイスとプロトコルを選択することから始めます。

packet-tracer input *ifc_name* {**icmp** | **tcp** | **udp** | **rawip**} [**inline-tag** *tag*] ...

それぞれの説明は次のとおりです。

- **input** *ifc_name*：トレースを開始するインターフェイスの名前。
- **icmp**、**tcp**、**udp**、**rawip**：使用するプロトコル。「rawip」は未加工の IP、つまり、TCP/UDP 以外の IP パケットです。
- **inline-tag** *tag*：（オプション）。レイヤ 2 CMD ヘッダーに埋め込まれたセキュリティ グループ タグの値。有効な値の範囲は 0 ～ 65533 です。

ステップ 2 次に、送信元アドレスとプロトコル基準を入力します。

...{*src_ip* | **user** *username* | **security-group** {**name** *name* | **tag** *tag*} | **fqdn** *fqdn-string*}...

それぞれの説明は次のとおりです。

- *src_ip*：パケット トレース用の送信元 IPv4 または IPv6 アドレス。
- **user** *username*：domain\user の形式のユーザ ID。ユーザに対して最後にマッピングされたアドレス（複数ある場合）がトレースに使用されます。
- **security-group**{**name***name* | **tag***tag*}：TrustSec の IP-SGT 参照に基づく送信元セキュリティ グループ。セキュリティ グループの名前またはタグ番号を指定できます。
- **fqdn** *fqdn-string*：送信元ホストの完全修飾ドメイン名、IPv4 のみ。

ステップ 3 次に、プロトコルの特性を入力します。

- [ICMP]：ICMP タイプ（1 ～ 255）、ICMP コード（0 ～ 255）、およびオプションで ICMP 識別子を入力します。各変数に対応する数字（エコーに対応する 8 など）を使用する必要があります。

  type code... [*ident*]...

- TCP/UDP：送信元ポート番号を入力します。

  ...src_port ...

- [Raw IP]：プロトコル番号（0 ～ 255）を入力します。

  ... protocol ...

ステップ 4 最後に、宛先アドレス基準、TCP/UDP トレース用の宛先ポート、およびオプションのキーワードを入力して、**Enter** キーを押します。

... {*dst_ip* | **security-group** { **name** *name* | **tag** *tag*} | **fqdn** *fqdn-string*} *dst_port* [**detailed**] [**xml**]

それぞれの説明は次のとおりです。

- *dst_ip*：パケット トレース用の宛先 IPv4 または IPv6 アドレス。
- **security-group** {**name** *name* **| tag** *tag*}：TrustSec の IP-SGT 参照に基づく宛先セキュリティ グループ。セキュリティ グループの名前またはタグ番号を指定できます。
- **fqdn** *fqdn-string*：宛先ホストの完全修飾ドメイン名、IPv4 のみ。
- *dst_port*：TCP/UDP トレース用の宛先ポート。ICMP または未加工 IP トレースの場合はこの値を含めないでください。
- **detailed**：標準出力に加えて詳細なトレース結果情報を提供します。
- **xml**：トレース結果を XML 形式で表示します。

例

次に、HTTP ポート 10.100.10.10 から 10.100.11.11 への TCP パケットをトレースする例を示します。暗黙の拒否アクセス ルールによってパケットがドロップされることを示す結果が表示されます。

```
ciscoasa(config)# packet-tracer input outside tcp 10.100.10.10 80
10.100.11.11 80

Phase: 1
Type: ROUTE-LOOKUP
Subtype: Resolve Egress Interface
Result: ALLOW
Config:
Additional Information:
found next-hop 10.86.116.1 using egress ifc  outside

Phase: 2
Type: ACCESS-LIST
Subtype:
Result: DROP
Config:
Implicit Rule
Additional Information:

Result:
```

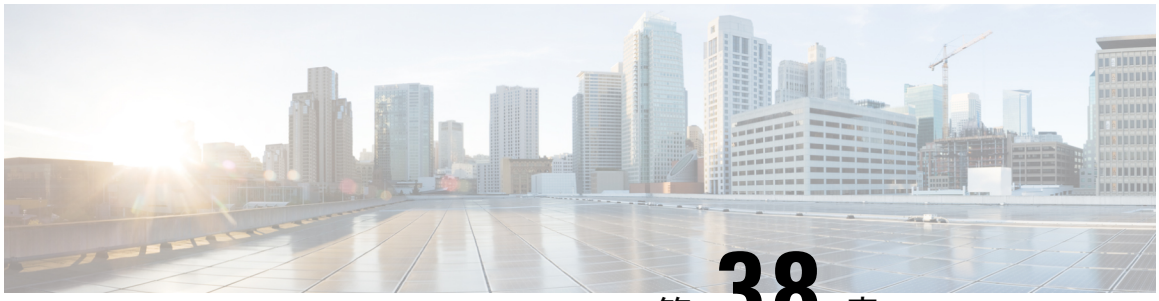
```
input-interface: outside
input-status: up
input-line-status: up
output-interface: NP Identity Ifc
output-status: up
output-line-status: up
Action: drop
Drop-reason: (acl-drop) Flow is denied by configured rule
```

接続のモニタリング

送信元、宛先、プロトコルなどに関する情報を含む現在の接続を表示するには、**show conn all detail** コマンドを使用します。

第 VIII 部

モニタリング



第 38 章

ロギング

この章では、システム メッセージを記録して、トラブルシューティングに使用する方法について説明します。

ロギングの概要

システム ロギングは、デバイスから syslog デーモンを実行するサーバへのメッセージを収集する方法です。中央の syslog サーバへロギングは、ログおよびアラートの集約に役立ちます。シスコ デバイスでは、これらのログ メッセージを UNIX スタイルの syslog サービスに送信できます。syslog サービスは、シンプル コンフィギュレーション ファイルに従って、メッセージを受信してファイルに保存するか、出力します。この形式のロギングは、保護された長期的な保存場所をログに提供します。ログは、ルーチン トラブルシューティングおよびインシデント処理の両方で役立ちます。

ASAのシステム ログにより、ASAのモニタリングおよびトラブルシューティングで必要な情報を得ることができます。ロギング機能を使用して、次の操作を実行できます。

- ログに記録する syslog メッセージを指定する。
- Syslog メッセージの重大度のディセーブル化または変更
- 次を含む、syslog メッセージ送信先となる、1 つ以上の場所を指定する。
  - 内部バッファ
  - 1 台以上の syslog サーバ
  - ASDM
  - SNMP 管理ステーション

- 指定の電子メール アドレス
- コンソール
- Telnet と SSH セッション

- 重大度レベルやメッセージ クラスなどによる、グループ内での syslog メッセージを設定および管理する。
- syslog の生成にレート制限を適用するかどうかを指定する。
- 内部ログ バッファがいっぱいになった場合に、その内容に対して実行する処理（バッファを上書きする、バッファの内容を FTP サーバに送信する、または内容を内部フラッシュ メモリに保存する）を指定する。
- 場所、重大度レベル、クラス、またはカスタム メッセージ リストにより、syslog メッセージをフィルタリングする。

マルチ コンテキスト モードでのロギング

それぞれのセキュリティ コンテキストには、独自のロギング コンフィギュレーションが含まれており、独自のメッセージが生成されます。システム コンテキストまたは管理コンテキストにログインし、別のコンテキストに変更した場合、セッションで表示されるメッセージは現在のコンテキストに関連するメッセージに限定されます。

システム実行スペースで生成されるフェールオーバー メッセージなどの syslog メッセージは、管理コンテキストで生成されるメッセージとともに管理コンテキストで表示できます。システム実行スペースでは、ロギングの設定やロギング情報の表示はできません。

ASA は、各メッセージとともにコンテキスト名を含めるように設定できます。これによって、単一の syslog サーバに送信されるコンテキスト メッセージを区別できます。この機能は、管理コンテキストから送信されたメッセージとシステムから送信されたメッセージの判別にも役立ちます。これが可能なのは、送信元がシステム実行スペースであるメッセージでは**システム**のデバイス ID が使用され、管理コンテキストが送信元であるメッセージではデバイス ID として管理コンテキストの名前が使用されるからです。

syslog メッセージ分析

次に、さまざまな syslog メッセージを確認することで取得できる情報タイプの例を示します。

- ASA セキュリティ ポリシーで許可された接続。これらのメッセージは、セキュリティ ポリシーで開いたままのホールを発見するのに役立ちます。
- ASA セキュリティ ポリシーで拒否された接続。これらのメッセージは、セキュアな内部ネットワークに転送されているアクティビティのタイプを示します。
- ACE 拒否率ロギング機能を使用すると、使用している ASA に対して発生している攻撃が表示されます。

- IDS アクティビティ メッセージには、発生した攻撃が示されます。
- ユーザ認証とコマンドの使用により、セキュリティ ポリシーの変更を監査証跡することができます。
- 帯域幅使用状況メッセージには、確立および切断された各接続のほか、使用された時間とトラフィック量が示されます。
- プロトコル使用状況メッセージには、各接続で使用されたプロトコルとポート番号が示されます。
- アドレス変換監査証跡メッセージは、確立または切断されている NAT または PAT 接続を記録します。この情報は、内部ネットワークから外部に送信される悪意のあるアクティビティのレポートを受信した場合に役立ちます。

syslog メッセージ形式

syslog メッセージはパーセントの記号（%）で始まり、次のように構造化されています。

```
%ASA Level Message_number: Message_text
```

次の表に、フィールドの説明を示します。

ASA	ASA が生成するメッセージの syslog メッセージ ファシリティ コード。この値は常に ASA です。
Level	1 ～ 7。レベルは、syslog メッセージに記述されている状況の重大度を示します。値が低いほどその状況の重大度は高くなります。
Message_number	syslog メッセージを特定する 6 桁の固有の番号。
Message_text	状況を説明するテキスト文字列。syslog メッセージのこの部分には、IP アドレス、ポート番号、またはユーザ名が含まれていることがあります。

重大度

次の表に、syslog メッセージの重大度の一覧を示します。それぞれの重大度にカスタム カラーを割り当て、ASDM ログ ビューアで重大度を識別しやすくできます。syslog メッセージの色設定を行うには、[Tools] > [Preferences] > [Syslog] タブを選択するか、またはログ ビューア自体のツールバーで [Color Settings] をクリックします。

表 *46 : Syslog* メッセージの重大度

レベル番号	重大度	説明
0	**緊急**	システムが使用不可能な状態。
1	**アラート**	すぐに措置する必要があります。

レベル番号	重大度	説明
2	重大	深刻な状況です。
3	エラー	エラー状態です。
4	警告	警告状態。
5	通知	正常ですが、注意を必要とする状況です。
6	情報	情報メッセージです。
7	デバッグ	デバッグ メッセージです。

（注） ASAは、重大度 0（emergencies）の syslog メッセージを生成しません。

syslog メッセージ フィルタリング

生成される syslog メッセージは、特定の syslog メッセージだけが特定の出力先に送信されるようにフィルタリングできます。たとえば、ASAを設定して、すべての syslog メッセージを 1 つの出力先に送信し、それらの syslog メッセージのサブセットを別の出力先に送信することができます。

具体的には、syslog メッセージが次の基準に従って出力先に転送されるようにできます。

- syslog メッセージの ID 番号
- syslog メッセージの重大度
- syslog メッセージ クラス（機能エリアと同等）

これらの基準は、出力先を設定するときに指定可能なメッセージ リストを作成して、カスタマイズできます。あるいは、メッセージ リストとは無関係に、特定のメッセージ クラスを各タイプの出力先に送信するようにASAを設定することもできます。

syslog メッセージ クラス

syslog メッセージのクラスは次の 2 つの方法で使用できます。

- syslog メッセージのカテゴリ全体の出力場所を指定します。**logging class** コマンドを使用します。
- メッセージ クラスを指定するメッセージ リストを作成します。**logging list** コマンドを使用します。

syslog メッセージ クラスは、デバイスの特徴または機能と同等のタイプによって syslog メッセージを分類する方法を提供します。たとえば、RIP クラスは RIP ルーティングを示します。

特定のクラスに属する syslog メッセージの ID 番号はすべて、最初の 3 桁が同じです。たとえば、611 で始まるすべての syslog メッセージ ID は、vpnc（VPN クライアント）クラスに関連付けられています。VPN クライアント機能に関連付けられている syslog メッセージの範囲は、611101 ～ 611323 です。

また、ほとんどの ISAKMP syslog メッセージには先頭に付加されたオブジェクトの共通セットが含まれているため、トンネルを識別するのに役立ちます。これらのオブジェクトは、使用可能なときに、syslog メッセージの説明テキストの前に付加されます。syslog メッセージ生成時にオブジェクトが不明な場合、特定の heading = value の組み合わせは表示されません。

オブジェクトは次のように先頭に付加されます。

Group = *groupname*, Username = *user*, IP = *IP_address*

Group はトンネル グループ、Username はローカル データベースまたは AAA サーバから取得したユーザ名、IP アドレスはリモート アクセス クライアントまたはレイヤ 2 ピアのパブリック IP アドレスです。

次の表に、メッセージ クラスと各クラスのメッセージ ID の範囲をリストします。

表 *47 : syslog* メッセージ クラスおよび関連付けられているメッセージ *ID* 番号

クラス	定義	Syslog メッセージ ID 番号
auth	User Authentication	109、113
—	アクセス リスト	106
—	アプリケーション ファイアウォール	415
bridge	トランスペアレント ファイアウォール	110、220
ca	PKI 認証局	717
citrix	Citrix Client	723
—	クラスタ	747
—	カード管理	323
config	コマンド インターフェイス	111、112、208、308
csd	Secure Desktop	724
cts	Cisco TrustSec	776
dap	ダイナミック アクセス ポリシー	734
eap、eapoudp	ネットワーク アドミッション コントロールの EAP または EAPoUDP	333、334
eigrp	EIGRP ルーティング	336

クラス	定義	Syslog メッセージ ID 番号
電子メール	電子メール プロキシ	719
—	環境モニタリング	735
ha	フェールオーバー	101、102、103、104、105、210、311、709
—	Identity-Based ファイアウォール	746
ids	侵入検知システム	400、733
—	IKEv2 ツールキット	750、751、752
ip	IP スタック	209、215、313、317、408
ipaa	IP アドレス割り当て	735
ips	侵入防御システム	400、401、420
—	IPv6	325
—	ブラック リスト、ホワイト リスト、およびグレー リスト	338
—	ライセンス	444
mdm-proxy	MDM プロキシ	802
nac	ネットワーク アドミッション コントロール	731、732
nacpolicy	NAC ポリシー	731
nacsettings	NAC ポリシーを適用する NAC 設定	732
—	ネットワーク アクセス ポイント	713
np	ネットワーク プロセッサ	319
—	NP SSL	725
ospf	OSPF ルーティング	318、409、503、613
—	パスワードの暗号化	742
—	電話プロキシ	337
rip	RIP ルーティング	107、312
rm	Resource Manager	321
—	Smart Call Home	120

クラス	定義	Syslog メッセージ ID 番号
session	ユーザ セッション	106、108、201、202、204、302、303、304、305、314、405、406、407、500、502、607、608、609、616、620、703、710
snmp	SNMP	212
—	ScanSafe	775
ssl	SSL スタック	725
svc	SSL VPN クライアント	722
sys	システム	199、211、214、216、306、307、315、414、604、605、606、610、612、614、615、701、711、741
—	脅威の検出	733
tre	トランザクション ルール エンジン	780
—	UC-IME	339
tag-switching	サービス タグ スイッチング	779
vm	VLAN マッピング	730
vpdn	PPTP および L2TP セッション	213、403、603
vpn	IKE および IPsec	316、320、402、404、501、602、702、713、714、715
vpnc	VPN クライアント	611
vpnfo	VPN フェールオーバー	720
vpnlb	VPN ロード バランシング	718
—	VXLAN	778
webfo	WebVPN フェールオーバー	721
webvpn	WebVPN と AnyConnect Client	716
—	NAT および PAT	305

カスタム メッセージ リスト

カスタム メッセージ リストを作成して、送信する syslog メッセージとその出力先を柔軟に制御できます。カスタム syslog メッセージのリストで、次の条件のいずれかまたはすべてを使用して syslog メッセージのグループを指定します。

- 重大度
- メッセージ ID
- syslog メッセージ ID の範囲
- メッセージ クラス

たとえば、メッセージ リストを使用して次の操作を実行できます。

- 重大度が 1 および 2 の syslog メッセージを選択し、1 つ以上の電子メール アドレスに送信する。
- メッセージ クラス（「ha」など）に関連付けられたすべての syslog メッセージを選択し、内部バッファに保存する。

メッセージ リストには、メッセージを選択するための複数の基準を含めることができます。ただし、メッセージ選択基準の追加は、それぞれ個別のコマンドエントリで行う必要があります。重複したメッセージ選択基準を含むメッセージ リストが作成される可能性もあります。メッセージリストの 2 つの基準によって同じメッセージが選択される場合、そのメッセージは一度だけログに記録されます。

クラスタ

syslog メッセージは、クラスタリング環境でのアカウンティング、モニタリング、およびトラブルシューティングのための非常に重要なツールです。クラスタ内の各 ASA ユニット（最大 8 ユニットを使用できます）は、syslog メッセージを個別に生成します。特定の **logging** コマンドを使用すると、タイム スタンプおよびデバイス ID を含むヘッダー フィールドを制御できます。syslog サーバは、syslog ジェネレータを識別するためにデバイス ID を使用します。**logging device-id** コマンドを使用すると、同一または異なるデバイス ID 付きで syslog メッセージを生成することができ、クラスタ内の同一または異なるユニットからのメッセージのように見せることができます。

ロギングのガイドライン

この項では、ロギングを設定する前に確認する必要のある制限事項とガイドラインについて説明します。

IPv6 のガイドライン

IPv6 はサポートされません。

その他のガイドライン

- syslogサーバでは、syslogdというサーバプログラムを実行する必要があります。Windowsでは、オペレーティング システムの一部として syslog サーバを提供しています。
- ASAが生成したログを表示するには、ロギングの出力先を指定する必要があります。ロギングの出力先を指定せずにロギングをイネーブルにすると、ASAはメッセージを生成しますが、それらのメッセージは後で表示できる場所に保存されません。各ロギングの出力先は個別に指定する必要があります。たとえば、出力先として複数のsyslogサーバを指定するには、新しいコマンドを入力し、で、個別のエントリを指定します。
- スタンドバイ デバイスでは、TCP 上での syslog の送信はサポートされません。
- 2 つの異なるリストまたはクラスを、異なる syslog サーバまたは同じロケーションに割り当てることはできません。
- 最大 16 台の syslog サーバを設定できます。ただし、マルチ コンテキスト モードでは、コンテキストごとに 4 サーバに制限されています。
- syslog サーバは、ASA 経由で到達できなければなりません。syslog サーバが到達できるインターフェイス上で、デバイスがICMP到達不能メッセージを拒否し、同じサーバにsyslogを送信するように設定する必要があります。すべての重大度に対してロギングがイネーブルであることを確認します。syslog サーバがクラッシュしないようにするため、syslog 313001、 313004、および 313005 の生成を抑制します。
- アクセス リストのヒット数だけを照合するためにカスタム メッセージ リストを使用すると、ロギング重大度がデバッグ（レベル7）のアクセスリストに対しては、アクセスリストのログは生成されません。**logging list** コマンドのロギング重大度のデフォルトは、6 に設定されています。このデフォルト動作は設計によるものです。アクセスリストコンフィギュレーションのロギング重大度をデバッグに明示的に変更する場合は、ロギング コンフィギュレーション自体も変更する必要があります。

  ロギング重大度がデバッグに変更されたため、アクセスリストのヒットが含まれていない **show running-config logging** コマンドの出力例を次に示します。

```
ciscoasa# show running-config logging
logging enable
logging timestamp
logging list test message 106100
logging buffered test
```

  次に、アクセス リスト ヒットを含む **show running-config logging** コマンドの出力例を示します。

```
ciscoasa# show running-config logging
logging enable
logging timestamp
logging buffered debugging
```

  この場合、アクセス リスト コンフィギュレーションは変更せず、アクセス リスト ヒット数が次の例のように表示されます。

```
ciscoasa(config)# access-list global line 1 extended
permit icmp any host 4.2.2.2 log debugging interval 1 (hitcnt=7) 0xf36b5386
ciscoasa(config)# access-list global line 2 extended
permit tcp host 10.1.1.2 any eq www log informational interval 1 (hitcnt=18) 0xe7e7c3b8
ciscoasa(config)# access-list global line 3 extended
permit ip any any (hitcnt=543) 0x25f9e609
```

- ASA が TCP 経由で syslog を送信すると、syslogd サービスの再起動後、接続の開始に約 1 分かかります。

ロギングの設定

ここでは、ロギングの設定方法について説明します。

ロギングのイネーブル化

ロギングをイネーブルにするには、次の手順を実行します。

手順

ロギングをイネーブルにします。

logging enable

例：

```
ciscoasa(config)# logging enable
```

出力先の設定

トラブルシューティングおよびパフォーマンスのモニタリング用にsyslogメッセージの使用状況を最適化するには、syslog メッセージの送信先（内部ログ バッファ、1 つまたは複数の外部 syslog サーバ、ASDM、SNMP 管理ステーション、コンソール ポート、指定した電子メール アドレス、または Telnet および SSH セッションなど）を 1 つまたは複数指定することをお勧めします。

外部 syslog サーバへの syslog メッセージの送信

外部 syslog サーバで利用可能なディスク領域に応じてメッセージをアーカイブし、その保存後、ロギング データを操作できます。たとえば、特定タイプの syslog メッセージがログに記録されたり、ログからデータが抽出されてレポート用の別のファイルにその記録が保存された

り、あるいはサイト固有のスクリプトを使用して統計情報が追跡されたりした場合に、特別なアクションが実行されるように指定できます。

外部 syslog サーバに syslog メッセージを送信するには、次の手順を実行します。

手順

ステップ 1 syslog サーバにメッセージを送信するために ASA を設定します。

logging host *interface_name syslog_ip* [**tcp**[/*port*] | **udp** [/*port*] [**format emblem**]]

例：

```
ciscoasa(config)# logging host dmz1 192.168.1.5 udp/1026
```

format emblem キーワードは、UDP 限定で syslog サーバでの EMBLEM 形式ロギングを有効にします。*interface_name* 引数には、syslog サーバにアクセスするときのインターフェイスを指定します。*syslog_ip* 引数には、syslog サーバの IP アドレスを指定します。**tcp**[/*port*] または **udp**[/*port*] キーワードと引数のペアは、syslog サーバに syslog メッセージを送信するために ASA で TCP を使用するか、UDP を使用するかを指定します。

UDP または TCP のいずれかを使用して syslog サーバにデータを送信するように ASA を設定することはできますが、両方を使用するように設定することはできません。プロトコルを指定しない場合、デフォルトのプロトコルは UDP です。

TCP を指定すると、ASA は syslog サーバの障害を検出し、セキュリティ保護として ASA 経由の新しい接続をブロックします。TCP syslog サーバへの接続に関係なく新しい接続を許可するには、手順 3 を参照してください。UDP を指定すると、ASA は、syslog サーバが動作しているかどうかに関係なく新しい接続を許可し続けます。有効なポート値は、どちらのプロトコルでも 1025 ～ 65535 です。デフォルトの UDP ポートは 514 です。デフォルトの TCP ポートは 1470 です。

ステップ 2 syslog サーバに送信する syslog メッセージを指定します。

logging trap {*severity_level* | *message_list*}

例：

```
ciscoasa(config)# logging trap errors
```

重大度として、値（1 ～ 7）または名前を指定できます。たとえば重大度を 3 に設定すると、ASA は、重大度が 3、2、および 1 の syslog メッセージを送信します。syslog サーバに送信する syslog メッセージを特定したカスタム メッセージ リストを指定することもできます。

ステップ 3 （オプション）TCP 接続された syslog サーバがダウンした場合、新しい接続をブロックする機能をディセーブルにします。

logging permit-hostdown

例：

```
ciscoasa(config)# logging permit-hostdown
```

ASA が syslog メッセージを TCP ベースの syslog サーバに送信するように設定されている場合、および syslog サーバがダウンしているか、ログキューがいっぱいの場合、新しい接続はブロックされます。新しい接続は、syslog サーバがバック アップされ、ログ キューがいっぱいでなくなった後に再度許可されます。

ステップ 4 （オプション）ロギング ファシリティを 20 以外の値に設定します。これは、ほとんどの UNIX システムで想定されています。

logging facility *number*

例：

```
ciscoasa(config)# logging facility 21
```

セキュア ロギングの有効化

手順

logging host コマンドで **secure** キーワードを指定して、セキュア ロギングを有効にします。

logging host *interface_name syslog_ip* [**tcp**/*port* | **udp**/*port*] [**format emblem**] [**secure**]

それぞれの説明は次のとおりです。

- **logging host***interface_name syslog_ip* には、syslog サーバが常駐するインターフェイスと syslog サーバの IP アドレスを指定します。
- [**tcp**/*port* | **udp**/*port*] には、syslog サーバが syslog メッセージをリスンするポート（TCP または UDP）を指定します。**tcp** キーワードは、ASA が TCP を使用して syslog メッセージを syslog サーバに送信することを指定します。**udp** キーワードは、ASA が UDP を使用して syslog メッセージを syslog サーバに送信することを指定します。
- **format emblem** キーワードは、syslog サーバに対して EMBLEM 形式のロギングを有効にします。
- **secure** キーワードは、リモート ロギング ホストへの接続で、TCP の場合にだけ SSL/TLS を使用するように指定します。セキュア ロギングでは UDP をサポートしていないため、このプロトコルを使用しようとするとエラーが発生します。

例：

```
ciscoasa(config)# logging host inside 10.0.0.1 TCP/1500 secure
```

syslog サーバに送信する EMBLEM 形式の syslog メッセージの生成

syslog サーバへの EMBLEM 形式の syslog メッセージを生成するには、次の手順を実行します。

手順

EMBLEM 形式の syslog メッセージを、UDP のポート 514 を使用して syslog サーバに送信します。

logging host *interface_name ip_address*{**tcp** [*/port*] | **udp** [*/ port*]] [**format emblem**]

例：

```
ciscoasa(config)# logging host interface_1 127.0.0.1 udp format emblem
ciscoasa(config)# logging host interface_1 2001::1 udp format emblem
```

format emblem キーワードは、syslog サーバでの EMBLEM 形式ロギングを有効にします（UDP 限定）。*interface_name* 引数には、syslog サーバにアクセスするときのインターフェイスを指定します。*ip_address* 引数には、syslog サーバの IP アドレスを指定します。 **tcp**[*/port*] または **udp**[*/port*] キーワードと引数のペアは、syslog サーバに syslog メッセージを送信するために ASA で TCP を使用するか、UDP を使用するかを指定します。

UDP または TCP のいずれかを使用して syslog サーバにデータを送信するように ASA を設定することができます。プロトコルを指定しない場合、デフォルトのプロトコルは UDP です。

複数の **logging host** コマンドを使用して、syslog メッセージを受信するすべての追加サーバを指定できます。2 つ以上のロギング サーバを設定する場合は、必ず、すべてのロギング サーバにおいて、ロギングの重大度の上限を warnings にしてください。

TCP を指定すると、ASA は syslog サーバの障害を検出し、セキュリティ保護として ASA を経由する新しい接続をブロックします。UDP を指定すると、ASA は、syslog サーバが動作しているかどうかに関係なく新しい接続を許可し続けます。有効なポート値は、どちらのプロトコルでも 1025 ～ 65535 です。デフォルトの UDP ポートは 514 です。デフォルトの TCP ポートは 1470 です。

他の出力先への EMBLEM 形式の syslog メッセージの生成

他の出力先への EMBLEM 形式の syslog メッセージを生成するには、次の手順を実行します。

手順

syslog サーバ以外の出力先（たとえば Telnet または SSH セッション）に EMBLEM 形式の syslog メッセージを送信します。

logging emblem

例：

```
ciscoasa(config)# logging emblem
```

内部ログ バッファへの syslog メッセージの送信

一時的な保存場所となる内部ログ バッファに送信する syslog メッセージを指定する必要があります。新しいメッセージは、リストの最後に追加されます。バッファがいっぱいになったとき、つまりバッファ ラップが発生した場合、ASA がいっぱいになったバッファを別の場所に保存するように設定されていない限り、古いメッセージは生成される新しいメッセージによって上書きされます。

syslog メッセージを内部ログ バッファに送信するには、次の手順を実行します。

手順

ステップ 1 一時的な保存場所となる内部ログ バッファに送信する syslog メッセージを指定します。

logging buffered {*severity_level* | *message_list*}

例：

```
ciscoasa(config)# logging buffered critical
ciscoasa(config)# logging buffered level 2
ciscoasa(config)# logging buffered notif-list
```

新しいメッセージは、リストの最後に追加されます。バッファがいっぱいになったとき、つまりバッファ ラップが発生した場合、ASA がいっぱいになったバッファを別の場所に保存するように設定されていない限り、古いメッセージは生成される新しいメッセージによって上書きされます。内部ログ バッファを空にするには、**clear logging buffer** コマンドを入力します。

ステップ 2 内部ログ バッファのサイズを変更します。デフォルトのバッファ サイズは 4 KB です。

logging buffer-size *bytes*

例：

```
ciscoasa(config)# logging buffer-size 16384
```

ステップ 3 次のいずれかのオプションを選択します。

- 新しいメッセージを内部ログ バッファに保存し、いっぱいになったログ バッファの内容を内部フラッシュ メモリに保存します。

  logging flash-bufferwrap

  例：

  ```
  ciscoasa(config)# logging flash-bufferwrap
  ```

- 新しいメッセージを内部ログ バッファに保存し、いっぱいになったログ バッファの内容を FTP サーバに保存します。

  logging ftp-bufferwrap

  例：

  ```
  ciscoasa(config)# logging flash-bufferwrap
  ```

  バッファの内容を別の場所に保存するとき、ASAは、次のタイムスタンプ形式を使用する名前でログ ファイルを作成します。

  ```
  LOG-YYYY-MM-DD-HHMMSS.TXT
  ```

  *YYYY*は年、*MM*は月、*DD*は日付、*HHMMSS*は時間、分、および秒で示された時刻です。

- ログ バッファの内容を保存する FTP サーバを指定します。

  logging ftp-server *server pathusername password*

  例：

  ```
  ciscoasa(config)# logging ftp-server 10.1.1.1 /syslogs logsupervisor 1luvMy10gs
  ```

  server 引数には、外部 FTP サーバの IP アドレスを指定します。*path* 引数には、ログ バッファのデータを保存する FTP サーバへのディレクトリ パスを指定します。このパスは、FTP ルート ディレクトリに対する相対パスです。*username* 引数には、FTP サーバへのロギングで有効なユーザ名を指定します。*password*引数は、指定したユーザ名に対するパスワードを示します。

- 現在のログ バッファの内容を内部フラッシュ メモリに保存します。

  logging savelog [*savefile*]

  例：

  ```
  ciscoasa(config)# logging savelog latest-logfile.txt
  ```

ログの記録で使用可能な内部フラッシュ メモリの容量の変更

ログの記録で使用可能な内部フラッシュ メモリの容量を変更するには、次の手順を実行します。

手順

ステップ 1 ログ ファイルの保存で使用可能な内部フラッシュ メモリの最大容量を指定します。

logging flash-maximum-allocation *kbytes*

例：

```
ciscoasa(config)# logging flash-maximum-allocation 1200
```

デフォルトでは、ASAは、内部フラッシュメモリの最大1MBをログデータに使用できます。ASA でログ データを保存するために必要な内部フラッシュ メモリの最小空き容量は 3 MB です。

内部フラッシュ メモリに保存されているログ ファイルにより、内部フラッシュ メモリの空き容量が設定された最小限の容量を下回ってしまう場合、ASA は最も古いログ ファイルを削除し、新しいログファイルの保存後も最小限の容量が確保されるようにします。削除するファイルがない場合、または古いファイルをすべて削除しても空きメモリの容量が最小限の容量を下回っている場合、ASA はその新しいログファイルを保存できません。

ステップ 2 ASAでログファイルを保存するために必要な内部フラッシュメモリの最小空き容量を指定します。

logging flash-minimum-free *kbytes*

例：

```
ciscoasa(config)# logging flash-minimum-free 4000
```

電子メール アドレスへの syslog メッセージの送信

syslog メッセージを電子メール アドレスに送信するには、次の手順を実行します。

手順

ステップ 1 電子メール アドレスに送信する syslog メッセージを指定します。

logging mail {*severity_level* | *message_list*}

例：

```
ciscoasa(config)# logging mail high-priority
```

電子メールで送信される場合、syslogメッセージは電子メールメッセージの件名行に表示されます。このため、このオプションでは、critical、alert、および emergency など、重大度の高い syslog メッセージを管理者に通知するように設定することをお勧めします。

ステップ 2 電子メール アドレスに syslog メッセージを送信するときに使用する送信元電子メール アドレスを指定します。

logging from-address *email_address*

例：

```
ciscoasa(config)# logging from-address xxx-001@example.com
```

ステップ 3 電子メール アドレスに syslog メッセージを送信するときに使用する宛先の電子メール アドレスを指定します。

logging recipient-address *e-mail_address*[*severity_level*]

例：

```
ciscoasa(config)# logging recipient-address admin@example.com
```

ステップ 4 電子メール アドレスに syslog メッセージを送信するときに使用する SMTP サーバを指定します。

例：

```
ciscoasa(config)# smtp-server 10.1.1.24
```

ASDM への syslog メッセージの送信

syslog メッセージを ASDM に送信するには、次の手順を実行します。

手順

ステップ 1 ASDM に送信する syslog メッセージを指定します。

logging asdm {*severity_level* | *message_list*}

例：

```
ciscoasa(config)# logging asdm 2
```

ASA は、ASDM への送信を待機している syslog メッセージのバッファ領域を確保し、メッセージが生成されるとバッファに保存します。ASDM ログ バッファは、内部ログ バッファとは別のバッファです。ASDM のログバッファがいっぱいになると、ASA は最も古い syslog メッセージを削除し、新しい syslog メッセージのバッファ領域を確保します。最も古い syslog メッセージを削除して新しい syslog メッセージのためのスペースを確保するのは、ASDM のデフォルト設定です。ASDM ログ バッファに保持される syslog メッセージの数を制御するために、バッファのサイズを変更できます。

ステップ 2 ASDM ログ バッファに保持される syslog メッセージの数を指定します。

logging asdm-buffer-size *num_of_msgs*

例：

```
ciscoasa(config)# logging asdm-buffer-size 200
```

ASDM ログ バッファの現在の内容を空にするには、**clear logging asdm** コマンドを入力します。

ロギング キューの設定

ロギング キューを設定するには、次の手順を実行します。

手順

設定された出力先に送信されるまでの間、ASA がそのキューに保持できる syslog メッセージの数を指定します。

logging queue *message_count*

例：

```
ciscoasa(config)# logging queue 300
```

ASA のメモリ内には、設定された出力先への送信を待機している syslog メッセージをバッファするために割り当てられる、一定数のブロックがあります。必要なブロックの数は、syslog メッセージ キューの長さと、指定した syslog サーバの数によって異なります。デフォルトのキューのサイズは 512 syslog メッセージです。キューのサイズは、使用可能なブロック メモリのサイズが上限です。有効値は 0 ～ 8192 メッセージです。値はプラットフォームによって異なります。ロギング キューをゼロに設定した場合、そのキューは設定可能な最大サイズ（8192 メッセージ）になります。

コンソール ポートへの syslog メッセージの送信

syslog メッセージをコンソール ポートに送信するには、次の手順を実行します。

手順

コンソール ポートに送信する syslog メッセージを指定します。

logging console { *severity_level* | *message_list*}

例：

```
ciscoasa(config)# logging console errors
```

SNMP サーバへの syslog メッセージの送信

SNMP サーバへのロギングをイネーブルにするには、次の手順を実行します。

手順

SNMP ロギングをイネーブルにし、SNMP サーバに送信するメッセージを指定します。

logging history [*logging_list* | *level*]

例：

```
ciscoasa(config)# logging history errors
```

SNMP ロギングを無効にするには、**no logging history** コマンドを入力します。

Telnet または SSH セッションへの syslog メッセージの送信

syslog メッセージを Telnet または SSH セッションに送信するには、次の手順を実行します。

手順

ステップ 1 Telnet または SSH セッションに送信する syslog メッセージを指定します。

logging monitor {*severity_level* | *message_list*}

例：

```
ciscoasa(config)# logging monitor 6
```

ステップ 2 現在のセッションへのロギングだけをイネーブルにします。

terminal monitor

例：

```
ciscoasa(config)# terminal monitor
```

一度ログアウトして再びログインする場合は、このコマンドを再入力する必要があります。現在のセッションへのロギングを無効にするには、**terminal no monitor** コマンドを入力します。

syslog メッセージの設定

Syslog での無効なユーザ名の表示または非表示

ログイン試行に失敗した場合の無効なユーザ名をsyslogメッセージに表示または非表示にできます。デフォルト設定では、ユーザ名が無効な場合、または有効かどうか不明な場合、ユーザ名は非表示です。たとえば、ユーザが誤ってユーザ名の代わりにパスワードを入力した場合、結果として生成されるsyslogメッセージで「ユーザ名」を隠すのが安全です。ログインに関するトラブルシューティングに役立てるために、無効なユーザ名を表示することもできます。

手順

ステップ 1 無効なユーザ名を表示するには、次のようにします。

no logging hide username

ステップ 2 無効なユーザ名を非表示にするには、次のようにします。

logging hide username

syslog メッセージに日付と時刻を含める

syslog メッセージに日付と時刻を含めるには、次の手順を実行します。

手順

syslog メッセージにメッセージが生成された日付と時刻が含まれるように指定します。

logging timestamp

例：

```
ciscoasa(config)# logging timestamp
LOG-2008-10-24-081856.TXT
```

syslog メッセージから日付と時刻を削除するには、**no logging timestamp** コマンドを入力します。

syslog メッセージの無効化

指定した syslog メッセージをディセーブルにするには、次の手順を実行します。

手順

ASA が特定の syslog メッセージを生成しないように指定します。

no logging message *syslog_id*

例：

```
ciscoasa(config)# no logging message 113019
```

無効にした syslog メッセージを再び有効にするには、**logging message** *syslog_id* コマンドを入力します（例：**logging message 113019**）。無効にしたすべての syslog メッセージのロギングを再び有効にするには、**clear configure logging disabled** コマンドを入力します。

syslog メッセージの重大度の変更

syslog メッセージの重大度を変更するには、次の手順を実行します。

手順

syslog メッセージの重大度を指定します。

logging message *syslog_id* **level** *severity_level*

例：

```
ciscoasa(config)# logging message 113019 level 5
```

syslog メッセージの重大度をその設定にリセットするには、**no logging message** *syslog_id* **level** *severity_level* コマンド（**no logging message 113019 level 5** など）を入力します。変更されたすべての syslog メッセージの重大度をそれぞれの設定にリセットするには、**clear configure logging level** コマンドを入力します。

スタンバイ装置の syslog メッセージのブロック

スタンバイ装置で特定の syslog メッセージが生成されないようにするには、次の手順を実行します。

手順

スタンバイ装置での生成を以前ブロックされていた特定の syslog メッセージのブロックを解除します。

logging message *syslog-id* **standby**

例：

```
ciscoasa(config)# logging message 403503 standby
```

スタンバイ装置で特定のsyslogメッセージが生成されないようにブロックするには、このコマンドの **no** 形式を使用します。

フェールオーバー発生時に、フェールオーバー スタンバイ ASA の syslog メッセージの同期が継続されるようにするには、**logging standby** コマンドを使用します。

（注） **logging standby** コマンドを使用すると、syslog サーバ、SNMP サーバ、FTP サーバなどの共有ロギング先でのトラフィックは 2 倍になります。

非 EMBLEM 形式の syslog メッセージにデバイス ID を含める

デバイス ID を非 EMBLEM 形式の syslog メッセージに含めるには、次の手順を実行します。

手順

デバイス ID を非 EMBLEM 形式の syslog メッセージに含めるように ASA を設定します。syslog メッセージに対して指定できるデバイス ID のタイプは 1 つだけです。

logging device-id {**cluster-id** | **context-name** | **hostname** | **ipaddress** *interface_name* [**system**] | **string** *text*}

例：

```
ciscoasa(config)# logging device-id hostname
ciscoasa(config)# logging device-id context-name
```

context-name キーワードは、現在のコンテキストの名前をデバイス ID として使用することを示します（マルチ コンテキスト モードにだけ適用されます）。マルチ コンテキスト モードの管理コンテキストでデバイス ID のロギングをイネーブルにすると、そのシステム実行スペースで生成されるメッセージは**system**のデバイス ID を使用し、管理コンテキストで生成されるメッセージは管理コンテキストの名前をデバイス ID として使用します。

（注） ASA クラスタでは、選択したインターフェイスのマスター ユニットの IP アドレスを常に使用します。

cluster-id キーワードは、デバイス ID として、クラスタの個別の ASA ユニットのブート設定に一意の名前を指定します。**hostname** キーワードは、ASA のホスト名をデバイス ID として使用するように指定します。**ipaddress** *interface_name* キーワード引数のペアは、*interface_name* として指定されたインターフェイスの IP アドレスをデバイス ID として使用することを指定します。**ipaddress** キーワードを使用すると、syslog メッセージの送信元となるインターフェイスに関係なく、そのデバイス ID は指定された ASA のインターフェイス IP アドレスとなります。

クラスタ環境では、**system** キーワードは、デバイス ID がインターフェイスのシステム IP アドレスとなることを指定します。このキーワードにより、デバイスから送信されるすべての syslog メッセージに単一の一貫したデバイス ID を指定できます。**string** *text* キーワード引数のペアは、テキスト文字列をデバイス ID として使用することを指定します。文字列の長さは、最大で 16 文字です。

空白スペースを入れたり、次の文字を使用したりすることはできません。

- &（アンパサンド）
- '（一重引用符）
- "（二重引用符）
- <（小なり記号）
- >（大なり記号）
- ?（疑問符）

（注） イネーブルにすると、EMBLEM 形式の syslog メッセージや SNMP トラップにデバイス ID は表示されません。

カスタム イベント リストの作成

イベント リストの定義には、次の 3 つの基準を使用します。

- イベント クラス
- 重大度
- メッセージ ID

特定のロギングの宛先（SNMP サーバなど）に送信するカスタム イベント リストを作成するには、次の手順を実行します。

手順

ステップ 1 内部ログ バッファに保存されるメッセージの選択基準を指定します。たとえば重大度を 3 に設定すると、ASA は、重大度が 3、2、および 1 の syslog メッセージを送信します。

logging list *name* {**level** *level* [**class** *message_class*] | **message** *start_id*[*-end_id*]}

例：

```
ciscoasa(config)# logging list list-notif level 3
```

name 引数には、リストの名前を指定します。**level** *level* キーワードと引数のペアは、重大度を指定します。**class** *message_class* キーワードと引数のペアは、特定のメッセージ クラスを指定します。**message** *start_id* [*-end_id*] キーワードと引数のペアは、個々の syslog メッセージ番号または番号の範囲を指定します。

（注） 重大度の名前を syslog メッセージ リストの名前として使用しないでください。使用禁止の名前には、emergencies、alert、critical、error、warning、notification、informational、および debugging が含まれます。同様に、イベント リスト名の先頭にこれらの単語の最初の 3 文字は使用しないでください。たとえば、「err」で始まるイベント リスト名は使用しないでください。

ステップ 2 （オプション）リストにメッセージの選択基準をさらに追加します。

logging list *name* {**level** *level* [**class** *message_class*] | **message** *start_id*[*-end_id*]}

例：

```
ciscoasa(config)# logging list list-notif message 104024-105999
ciscoasa(config)# logging list list-notif level critical
ciscoasa(config)# logging list list-notif level warning class ha
```

前回の手順で使用したものと同じコマンドを入力し、既存のメッセージリストの名前と追加基準を指定します。リストに追加する基準ごとに、新しいコマンドを入力します。たとえば、リストに追加される syslog メッセージの基準として、次の基準を指定できます。

- ID が 104024 ～ 105999 の範囲の syslog メッセージ。
- 重大度が critical 以上（emergency、alert、または critical）のすべての syslog メッセージ。
- 重大度が warning 以上（emergency、alert、critical、error、または warning）のすべての ha クラスの syslog メッセージ。

（注） syslog メッセージは、これらの条件のいずれかを満たす場合にログに記録されます。syslog メッセージが複数の条件を満たす場合、そのメッセージは一度だけログに記録されます。

ロギング フィルタの設定

指定した出力先へのクラス内のすべての syslog メッセージの送信

クラス内のすべての syslog メッセージを指定した出力先に送信するには、次の手順を実行します。

手順

指定した出力先コマンドでコンフィギュレーションを上書きします。たとえば、重大度 7 のメッセージが内部ログ バッファに送信されるように指定し、重大度 3 の ha クラスのメッセージが内部ログバッファに送信されるように指定すると、後のコンフィギュレーションが優先されます。

logging class*message_class* {**buffered** |**console** |**history** |**mail** |**monitor** |**trap**} [*severity_level*]

例：

```
ciscoasa(config)# logging class ha buffered alerts
```

buffered、**history**、**mail**、**monitor**、および **trap** キーワードは、このクラスの syslog メッセージの出力先を指定します。**history** キーワードは、SNMP でのロギングを有効にします。**monitor** キーワードは、Telnet および SSH でのロギングを有効にします。**trap** キーワードは、syslog サーバでのロギングを有効にします。コマンドライン エントリあたり 1 つの出力先を指定します。1 つのクラスが複数の出力先に送信されるように指定する場合は、出力先ごとに新しいコマンドを入力します。

syslog メッセージの生成レートの制限

syslog メッセージの生成レートを制限するには、次の手順を実行します。

手順

指定された重大度（1 ～ 7）を、指定の時間内でメッセージセットまたは個々のメッセージ（出力先ではない）に適用します。

logging rate-limit {**unlimited** | {*num* [*interval*]}} **message** *syslog_id* | **level** *severity_level*

例：

```
ciscoasa(config)# logging rate-limit 1000 600 level 6
```

レート制限は、すべての設定された出力先に送信されるメッセージの量に影響します。ロギング レート制限をデフォルト値にリセットするには、**clear running-config logging rate-limit** コマンドを入力します。ロギング レート制限をリセットするには、**clear configure logging rate-limit** コマンドを入力します。

ログのモニタリング

ロギング ステータスの監視については、次のコマンドを参照してください。

- **show logging**

  このコマンドは、重大度を含む syslog メッセージを表示します。

  （注） 表示できる syslog メッセージの最大数は、1000 です。これはデフォルト設定です。表示できる syslog メッセージの最大数は、2000 です。

- **show logging message**

  このコマンドは、変更された重大度とディセーブルにされた syslog メッセージを含む syslog メッセージのリストを示します。

- **show logging message** *message_ID*

  このコマンドは、特定の syslog メッセージの重大度を示します。

- **show logging queue**

  このコマンドは、ロギング キューとキュー統計情報を示します。

- **show running-config logging rate-limit**

  このコマンドは、現在のロギング レート制限の設定を表示します。

ロギングの例

次の例は、**show logging** コマンドで表示されるロギング情報を示しています。

```
ciscoasa(config)# show logging
Syslog logging: enabled
    Facility: 16
    Timestamp logging: disabled
    Standby logging: disabled
    Deny Conn when Queue Full: disabled
    Console logging: disabled
    Monitor logging: disabled
    Buffer logging: disabled
    Trap logging: level errors, facility 16, 3607 messages logged
        Logging to infrastructure 10.1.2.3
    History logging: disabled
    Device ID: 'inside' interface IP address “10.1.1.1”
    Mail logging: disabled
    ASDM logging: disabled
```

次の例は、syslog メッセージをイネーブルにするかどうかを制御する方法と、指定した syslog メッセージの重大度を制御する方法を示しています。

```
ciscoasa(config)# show logging message 403503
syslog 403503: -level errors (enabled)

ciscoasa(config)# logging message 403503 level 1
ciscoasa(config)# show logging message 403503
syslog 403503: -level errors, current-level alerts (enabled)

ciscoasa(config)# no logging message 403503
ciscoasa(config)# show logging message 403503
syslog 403503: -level errors, current-level alerts (disabled)

ciscoasa(config)# logging message 403503
ciscoasa(config)# show logging message 403503
syslog 403503: -level errors, current-level alerts (enabled)

ciscoasa(config)# no logging message 403503 level 3
ciscoasa(config)# show logging message 403503
syslog 403503: -level errors (enabled)
```

ロギングの履歴

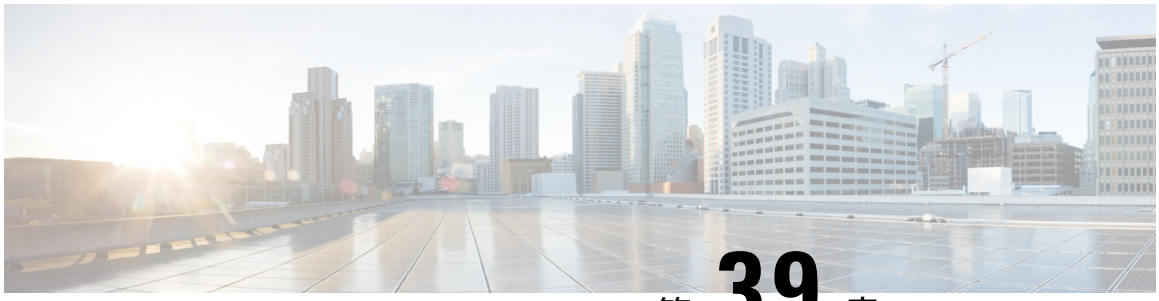
表 *48 :* ロギングの履歴

機能名	プラットフォーム リリース	説明
Logging	7.0(1)	さまざまな出力先を経由して ASA ネットワーク ロギング情報を提供します。ログ ファイルを表示して保存するオプションも含まれています。
レート制限	7.0(4)	syslog メッセージが生成されるレートを制限します。 **logging rate-limit** コマンドが導入されました。
ロギング リスト	7.2(1)	さまざまな基準（ロギング レベル、イベント クラス、およびメッセージ ID）でメッセージを指定するために他のコマンドで使用されるロギング リストを作成します。 次のコマンドが導入されました。 **logging list**

機能名	プラットフォーム リリース	説明
セキュア ロギング	8.0(2)	リモート ロギング ホストへの接続に SSL/TLS を使用するように指定します。このオプションは、選択されたプロトコルが TCP の場合にだけ有効です。 **logging host** コマンドが変更されました。
ロギング クラス	8.0(4)、8.1(1)	ロギング メッセージの ipaa イベント クラスに対するサポートが追加されました。 **logging class** コマンドが変更されました。
ロギング クラスと保存されたロギング バッファ	8.2(1)	ロギング メッセージの dap イベント クラスに対するサポートが追加されました。 **logging class** コマンドが変更されました。 保存されたロギング バッファ（ASDM、内部、FTP、およびフラッシュ）をクリアする追加サポート。 **clear logging queue bufferwrap** コマンドが導入されました。
パスワードの暗号化	8.3(1)	パスワードの暗号化に対するサポートが追加されました。 **logging ftp server** コマンドが変更されました。
ログ ビューア	8.3(1)	送信元 IP アドレスおよび宛先 IP アドレスがログ ビューアに追加されました。

機能名	プラットフォーム リリース	説明
拡張ロギングと接続ブロック	8.3(2)	TCP を使用するように syslog サーバを設定すると、syslog サーバを使用できない場合、ASA はサーバが再び使用可能になるまで syslog メッセージを生成する新しい接続をブロックします（たとえば、VPN、ファイアウォール、カットスループロキシ接続）。この機能は、ASA のロギング キューがいっぱいのときにも新しい接続をブロックするように拡張されました。接続は、ロギング キューがクリアされると再開されます。 この機能は、Common Criteria EAL4+ への準拠のために追加されました。必要でない限り、syslog メッセージを送受信できない場合でも接続を許可することを推奨します。接続を許可するには、**logging permit-hostdown** コマンドを使用します。 414005、414006、414007、414008 の各 syslog メッセージが導入されました。 **show logging** コマンドが変更されました。
syslog メッセージのフィルタリングとソート	8.4(1)	次のサポートが追加されました。 • さまざまなカラムに対応する複数のテキスト文字列に基づく syslog メッセージ フィルタリング。 • カスタム フィルタの作成。 • メッセージのカラムによるソート。詳細については、『ASDM 構成ガイド』を参照してください。 この機能は、すべての ASA バージョンと相互運用性があります。

機能名	プラットフォーム リリース	説明
クラスタ	9.0(1)	ASA 5580 および 5585-X のクラスタリング環境での syslog メッセージ生成のサポートが追加されました。 **logging device-id** コマンドが変更されました。
スタンバイ装置の syslog のブロック	9.4(1)	フェールオーバー コンフィギュレーションのスタンバイ装置で特定の syslog メッセージの生成をブロックするためのサポートを追加しました。 **logging message** *syslog-id* **standby** コマンドが導入されました。
syslog サーバでの IPv6 アドレスのサポート	9.7(1)	TCP と UDP 経由で syslog を記録、送信、受信するために、syslog サーバを IPv6 アドレスで設定できるようになりました。 次のコマンドが変更されました。**logging host**



第 39 章

SNMP

この章では、Simple Network Management Protocol（SNMP）に Cisco ASA をモニタさせるための設定方法について説明します。

SNMP の概要

SNMPは、ネットワーク デバイス間での管理情報の交換を容易にするアプリケーション層プロトコルで、TCP/IP プロトコル スイートの一部です。ASAは SNMP バージョン 1、2c、および 3 を使用したネットワーク監視に対するサポートを提供し、3 つのバージョンの同時使用をサポートします。ASA のインターフェイス上で動作する SNMP エージェントを使用すると、HP OpenView などのネットワーク管理システム（NMS）を使用してネットワーク デバイスをモニタできます。ASAはGET要求の発行を通じてSNMP読み取り専用アクセスをサポートします。SNMP書き込みアクセスは許可されていないため、SNMPを使用して変更することはできません。さらに、SNMP SET 要求はサポートされていません。

NMS（ネットワーク管理システム）に特定のイベント（イベント通知）を送信するために、管理対象デバイスから管理ステーションへの要求外のメッセージであるトラップを送信するように ASA を設定したり、NMS を使用してセキュリティ デバイス上で管理情報ベース（MIB）を検索できます。MIBは定義の集合であり、ASAは各定義に対応する値のデータベースを保持しています。MIB をブラウズすることは、NMS から MIB ツリーの一連の GET-NEXT または GET-BULK 要求を発行して値を決定することを意味します。

ASA には SNMP エージェントが含まれています。このエージェントは、通知を必要とすることが事前に定義されているイベント（たとえば、ネットワーク内のリンクがアップ状態またはダウン状態になる）が発生すると、指定した管理ステーションに通知します。このエージェントが送信する通知には、管理ステーションに対して自身を識別するSNMP OIDが含まれています。ASA エージェントは、管理ステーションが情報を要求した場合にも応答します。

SNMP の用語

次の表に、SNMP で頻繁に使用される用語を示します。

表 *49 : SNMP* の用語

用語	説明
エージェント	ASAで稼働する SNMP サーバ。SNMP エージェントは、次の機能を搭載しています。 • ネットワーク管理ステーションからの情報の要求およびアクションに応答する。 • 管理情報ベース（SNMP マネージャが表示または変更できるオブジェクトの集合）へのアクセスを制御する。 • SET 操作を許可しない。
ブラウジング	デバイス上の SNMP エージェントから必要な情報をポーリングすることによって、ネットワーク管理ステーションからデバイスのヘルスをモニタすること。このアクティビティには、ネットワーク管理ステーションから MIB ツリーの一連の GET-NEXT または GET-BULK 要求を発行して、値を決定することが含まれる場合があります。
管理情報ベース（MIB）	パケット、接続、バッファ、フェールオーバーなどに関する情報を収集するための標準化されたデータ構造。MIBは、大部分のネットワークデバイスで使用される製品、プロトコル、およびハードウェア標準によって定義されます。SNMP ネットワーク管理ステーションは、MIB をブラウズし、特定のデータまたはイベントの発生時にこれらを要求できます。
ネットワーク管理ステーション（NMS）	SNMP イベントのモニタやASAなどのデバイスの管理用に設定されている、PC またはワークステーション。
オブジェクト ID（OID）	NMS に対してデバイスを識別し、モニタおよび表示される情報の源をユーザに示すシステム。
Trap	SNMP エージェントから NMS へのメッセージを生成する、事前定義済みのイベント。イベントには、リンクアップ、リンクダウン、コールドスタート、ウォームスタート、認証、syslog メッセージなどのアラーム状態が含まれます。

MIB およびトラップ

MIB は、標準またはエンタープライズ固有です。標準 MIB はインターネット技術特別調査委員会（IETF）によって作成され、さまざまな Request for Comment（RFC）に記載されています。トラップは、ネットワークデバイスで発生する重要なイベント（多くの場合、エラーまたは障害）を報告します。SNMP トラップは、標準またはエンタープライズ固有の MIB のいずれかで定義されます。標準トラップは IETF によって作成され、さまざまな RFC に記載されています。SNMP トラップは、ASA ソフトウェアにコンパイルされています。

必要に応じて、次の場所から RFC、標準 MIB、および標準トラップをダウンロードすることもできます。

http://www.ietf.org/

次の場所から Cisco MIB、トラップ、および OID の完全なリストを参照してください。

ftp://ftp.cisco.com/pub/mibs/supportlists/asa/asa-supportlist.html

また、Cisco OID を次の場所から FTP でダウンロードしてください。

ftp://ftp.cisco.com/pub/mibs/oid/oid.tar.gz

（注） ソフトウェア バージョン 7.2(1)、8.0(2) 以降では、SNMP を介してアクセスされるインターフェイス情報は 5 秒ごとにリフレッシュされます。そのため、連続するポーリングの間に少なくとも 5 秒間は待機することをお勧めします。

MIB のすべての OID がサポートされているわけではありません。特定の ASA に対してサポートされている SNMP MIB および OID のリストを取得するには、次のコマンドを入力します。

```
ciscoasa(config)# show snmp-server oidlist
```

（注） **oidlist** キーワードは **show snmp-server** コマンドのヘルプのオプション リストには表示されませんが、使用できます。ただし、このコマンドは Cisco TAC でのみ使用されます。このコマンドを使用する前に TAC にお問い合わせください。

次に、**show snmp-server oidlist** コマンドの出力例を示します。

```
ciscoasa(config)# show snmp-server oidlist
[0]     1.3.6.1.2.1.1.1.        sysDescr
[1]     1.3.6.1.2.1.1.2.        sysObjectID
[2]     1.3.6.1.2.1.1.3.        sysUpTime
[3]     1.3.6.1.2.1.1.4.        sysContact
[4]     1.3.6.1.2.1.1.5.        sysName
[5]     1.3.6.1.2.1.1.6.        sysLocation
[6]     1.3.6.1.2.1.1.7.        sysServices
[7]     1.3.6.1.2.1.2.1.        ifNumber
[8]     1.3.6.1.2.1.2.2.1.1.    ifIndex
[9]     1.3.6.1.2.1.2.2.1.2.    ifDescr
[10]    1.3.6.1.2.1.2.2.1.3.    ifType
[11]    1.3.6.1.2.1.2.2.1.4.    ifMtu
[12]    1.3.6.1.2.1.2.2.1.5.    ifSpeed
[13]    1.3.6.1.2.1.2.2.1.6.    ifPhysAddress
[14]    1.3.6.1.2.1.2.2.1.7.    ifAdminStatus
[15]    1.3.6.1.2.1.2.2.1.8.    ifOperStatus
[16]    1.3.6.1.2.1.2.2.1.9.    ifLastChange
[17]    1.3.6.1.2.1.2.2.1.10.   ifInOctets
[18]    1.3.6.1.2.1.2.2.1.11.   ifInUcastPkts
[19]    1.3.6.1.2.1.2.2.1.12.   ifInNUcastPkts
[20]    1.3.6.1.2.1.2.2.1.13.   ifInDiscards
[21]    1.3.6.1.2.1.2.2.1.14.   ifInErrors
[22]    1.3.6.1.2.1.2.2.1.16.   ifOutOctets
```

```
[23]    1.3.6.1.2.1.2.2.1.17.   ifOutUcastPkts
[24]    1.3.6.1.2.1.2.2.1.18.   ifOutNUcastPkts
[25]    1.3.6.1.2.1.2.2.1.19.   ifOutDiscards
[26]    1.3.6.1.2.1.2.2.1.20.   ifOutErrors
[27]    1.3.6.1.2.1.2.2.1.21.   ifOutQLen
[28]    1.3.6.1.2.1.2.2.1.22.   ifSpecific
[29]    1.3.6.1.2.1.4.1.        ipForwarding
[30]    1.3.6.1.2.1.4.20.1.1.   ipAdEntAddr
[31]    1.3.6.1.2.1.4.20.1.2.   ipAdEntIfIndex
[32]    1.3.6.1.2.1.4.20.1.3.   ipAdEntNetMask
[33]    1.3.6.1.2.1.4.20.1.4.   ipAdEntBcastAddr
[34]    1.3.6.1.2.1.4.20.1.5.   ipAdEntReasmMaxSize
[35]    1.3.6.1.2.1.11.1.       snmpInPkts
[36]    1.3.6.1.2.1.11.2.       snmpOutPkts
[37]    1.3.6.1.2.1.11.3.       snmpInBadVersions
[38]    1.3.6.1.2.1.11.4.       snmpInBadCommunityNames
[39]    1.3.6.1.2.1.11.5.       snmpInBadCommunityUses
[40]    1.3.6.1.2.1.11.6.       snmpInASNParseErrs
[41]    1.3.6.1.2.1.11.8.       snmpInTooBigs
[42]    1.3.6.1.2.1.11.9.       snmpInNoSuchNames
[43]    1.3.6.1.2.1.11.10.      snmpInBadValues
[44]    1.3.6.1.2.1.11.11.      snmpInReadOnlys
[45]    1.3.6.1.2.1.11.12.      snmpInGenErrs
[46]    1.3.6.1.2.1.11.13.      snmpInTotalReqVars
[47]    1.3.6.1.2.1.11.14.      snmpInTotalSetVars
[48]    1.3.6.1.2.1.11.15.      snmpInGetRequests
[49]    1.3.6.1.2.1.11.16.      snmpInGetNexts
[50]    1.3.6.1.2.1.11.17.      snmpInSetRequests
[51]    1.3.6.1.2.1.11.18.      snmpInGetResponses
[52]    1.3.6.1.2.1.11.19.      snmpInTraps
[53]    1.3.6.1.2.1.11.20.      snmpOutTooBigs
[54]    1.3.6.1.2.1.11.21.      snmpOutNoSuchNames
[55]    1.3.6.1.2.1.11.22.      snmpOutBadValues
[56]    1.3.6.1.2.1.11.24.      snmpOutGenErrs
[57]    1.3.6.1.2.1.11.25.      snmpOutGetRequests
[58]    1.3.6.1.2.1.11.26.      snmpOutGetNexts
[59]    1.3.6.1.2.1.11.27.      snmpOutSetRequests
[60]    1.3.6.1.2.1.11.28.      snmpOutGetResponses
[61]    1.3.6.1.2.1.11.29.      snmpOutTraps
[62]    1.3.6.1.2.1.11.30.      snmpEnableAuthenTraps
[63]    1.3.6.1.2.1.11.31.      snmpSilentDrops
[64]    1.3.6.1.2.1.11.32.      snmpProxyDrops
[65]    1.3.6.1.2.1.31.1.1.1.1. ifName
[66]    1.3.6.1.2.1.31.1.1.1.2. ifInMulticastPkts
[67]    1.3.6.1.2.1.31.1.1.1.3. ifInBroadcastPkts
[68]    1.3.6.1.2.1.31.1.1.1.4. ifOutMulticastPkts
[69]    1.3.6.1.2.1.31.1.1.1.5. ifOutBroadcastPkts
[70]    1.3.6.1.2.1.31.1.1.1.6. ifHCInOctets
--More--
```

SNMP オブジェクト識別子

シスコのシステムレベルの各製品には、MIB-II の sysObjectID として使用される SNMP オブジェクト ID（OID）があります。CISCO-PRODUCTS-MIB と CISCO-ENTITY-VENDORTYPE-OID-MIB は、SNMPv2-MIB、Entity Sensor MIB および Entity Sensor Threshold Ext MIB の sysObjectID オブジェクト内で報告できる OID が含まれています。モデル タイプを識別するためにこの値を使用できます。次の表に、ASA および ISA モデルの sysObjectID OID を示します。

表 *50 : SNMP* オブジェクト識別子

製品識別子	sysObjectID	モデル番号
ASA 5506 適応型セキュリティ アプライアンス	ciscoASA5506（ciscoProducts 2114）	ASA 5506-X
ASA 5506 適応型セキュリティ アプライアンスのセキュリティ コンテキスト	ciscoASA5506sc（ciscoProducts 2115）	ASA 5506-X セキュリティ コンテキスト
ASA 5506 適応型セキュリティ アプライアンスのシステム コンテキスト	ciscoASA5506sy（ciscoProducts 2116）	ASA 5506-X システム コンテキスト
ASA 5506W 適応型セキュリティ アプライアンス	ciscoASA5506W（ciscoProducts 2117）	ASA 5506W-X
ASA 5506W 適応型セキュリティ アプライアンスのセキュリティ コンテキスト	ciscoASA5506Wsc（ciscoProducts 2118）	ASA 5506W-X セキュリティ コンテキスト
ASA 5506W 適応型セキュリティ アプライアンスのシステム コンテキスト	ciscoASA5506Wsy（ciscoProducts 2119）	ASA 5506W-X システム コンテキスト
ASA 5508 適応型セキュリティ アプライアンス	ciscoASA5508（ciscoProducts 2120）	ASA 5508-X
ASA 5508 適応型セキュリティ アプライアンスのセキュリティ コンテキスト	ciscoASA5508sc（ciscoProducts 2121）	ASA 5508-X セキュリティ コンテキスト
ASA 5508 適応型セキュリティ アプライアンスのシステム コンテキスト	ciscoASA5508sy（ciscoProducts 2122）	ASA 5508-X システム コンテキスト
ASA 5506 ペイロード暗号化なし適応型セキュリティ アプライアンス	ciscoASA5506K7（ciscoProducts 2123）	ASA 5506-X ペイロード暗号化なし適応型セキュリティ アプライアンス
ASA 5506 ペイロード暗号化なし適応型セキュリティ アプライアンスのセキュリティ コンテキスト	ciscoASA5506K7sc（ciscoProducts 2124）	ASA 5506-X ペイロード暗号化なし適応型セキュリティアプライアンスのセキュリティ コンテキスト
ASA 5506 ペイロード暗号化なし適応型セキュリティアプライアンスのシステム コンテキスト	ciscoASA5506K7sy（ciscoProducts 2125）	ASA 5506-X ペイロード暗号化なし適応型セキュリティアプライアンスのシステム コンテキスト
ASA 5508 ペイロード暗号化なし適応型セキュリティ アプライアンス	ciscoASA5508K7（ciscoProducts 2126）	ASA 5508-X ペイロード暗号化なし適応型セキュリティアプライアンスのシステム コンテキスト
ASA 5508 ペイロード暗号化なし適応型セキュリティ アプライアンスのセキュリティ コンテキスト	ciscoASA5508K7sc（ciscoProducts 2127）	ASA 5508-X ペイロード暗号化なし適応型セキュリティアプライアンスのセキュリティ コンテキスト

製品識別子	sysObjectID	モデル番号
ASA 5508 ペイロード暗号化なし適応型セキュリティ アプライアンスのシステム コンテキスト	ciscoASA5508K7sy（ciscoProducts 2128）	ASA 5508-X ペイロード暗号化なし適応型セキュリティ アプライアンスのシステム コンテキスト
ASA5585-SSP10	ciscoASA5585Ssp10（ciscoProducts 1194）	ASA 5585-X SSP-10
ASA5585-SSP20	ciscoASA5585Ssp20（ciscoProducts 1195）	ASA 5585-X SSP-20
ASA5585-SSP40	ciscoASA5585Ssp40（ciscoProducts 1196）	ASA 5585-X SSP-40
ASA5585-SSP60	ciscoASA5585Ssp60（ciscoProducts 1197）	ASA 5585-X SSP-60
ASA5585-SSP10	ciscoASA5585Ssp10sc（ciscoProducts 1198）	ASA 5585-X SSP-10 セキュリティ コンテキスト
ASA5585-SSP20	ciscoASA5585Ssp20sc（ciscoProducts 1199）	ASA 5585-X SSP-20 セキュリティ コンテキスト
ASA5585-SSP40	ciscoASA5585Ssp40sc（ciscoProducts 1200）	ASA 5585-X SSP-40 セキュリティ コンテキスト
ASA5585-SSP60	ciscoASA5585Ssp60sc（ciscoProducts 1201）	ASA 5585-X SSP-60 セキュリティ コンテキスト
ASA5585-SSP10	ciscoASA5585Ssp10sy（ciscoProducts 1202）	ASA 5585-X SSP-10 システム コンテキスト
ASA5585-SSP20	ciscoASA5585Ssp20sy（ciscoProducts 1203）	ASA 5585-X SSP-20 システム コンテキスト
ASA5585-SSP40	ciscoASA5585Ssp40sy（ciscoProducts 1204）	ASA 5585-X SSP-40 システム コンテキスト
ASA5585-SSP60	ciscoASA5585Ssp60sy（ciscoProducts 1205）	ASA 5585-X SSP-60 システム コンテキスト
Catalyst スイッチ/7600 ルータ向け ASA サービス モジュール	ciscoAsaSm1（ciscoProducts 1277）	Catalyst スイッチ/7600 ルータ向け適応型セキュリティ アプライアンス（ASA）サービス モジュール

製品識別子	sysObjectID	モデル番号
Catalyst スイッチ/7600 ルータ セキュリティ コンテキスト向け ASA サービス モジュール	ciscoAsaSm1sc（ciscoProducts 1275）	Catalyst スイッチ/7600 ルータ セキュリティ コンテキスト向け適応型セキュリティ アプライアンス（ASA）サービス モジュール
ペイロード暗号化なし Catalyst スイッチ/7600 ルータ セキュリティ コンテキスト向け ASA サービス モジュール	ciscoAsaSm1K7sc（ciscoProducts 1334）	ペイロード暗号化なし Catalyst スイッチ/7600 ルータ セキュリティ コンテキスト向け適応型セキュリティ アプライアンス（ASA）サービス モジュール
Catalyst スイッチ/7600 ルータ システム コンテキスト向け ASA サービス モジュール	ciscoAsaSm1sy（ciscoProducts 1276）	Catalyst スイッチ/7600 ルータ システム コンテキスト向け適応型セキュリティ アプライアンス（ASA）サービス モジュール
ペイロード暗号化なし Catalyst スイッチ システム コンテキスト/7600 ルータ向け ASA サービス モジュール	ciscoAsaSm1K7sy（ciscoProducts 1335）	ペイロード暗号化なし Catalyst スイッチ/7600 ルータ システム コンテキスト向け適応型セキュリティ アプライアンス（ASA）サービス モジュール
ペイロード暗号化なし Catalyst スイッチ/7600 ルータ システム コンテキスト向け ASA サービス モジュール	ciscoAsaSm1K7（ciscoProducts 1336）	ペイロード暗号化なし Catalyst スイッチ/7600 ルータ向け適応型セキュリティ アプライアンス（ASA）サービス モジュール
ASA 5512	ciscoASA5512（ciscoProducts 1407）	ASA 5512 適応型セキュリティ アプライアンス
ASA 5525	ciscoASA5525（ciscoProducts 1408）	ASA 5525 適応型セキュリティ アプライアンス
ASA 5545	ciscoASA5545（ciscoProducts 1409）	ASA 5545 適応型セキュリティ アプライアンス
ASA 5555	ciscoASA5555（ciscoProducts 1410）	ASA 5555 適応型セキュリティ アプライアンス
ASA 5512 セキュリティ コンテキスト	ciscoASA5512sc（ciscoProducts 1411）	ASA 5512 適応型セキュリティ アプライアンスのセキュリティ コンテキスト
ASA 5525 セキュリティ コンテキスト	ciscoASA5525sc（ciscoProducts 1412）	ASA 5525 適応型セキュリティ アプライアンスのセキュリティ コンテキスト
ASA 5545 セキュリティ コンテキスト	ciscoASA5545sc（ciscoProducts 1413）	ASA 5545 適応型セキュリティ アプライアンスのセキュリティ コンテキスト

製品識別子	sysObjectID	モデル番号
ASA 5555 セキュリティ コンテキスト	ciscoASA5555sc（ciscoProducts 1414）	ASA 5555 適応型セキュリティ アプライアンスのセキュリティ コンテキスト
ASA 5512 システム コンテキスト	ciscoASA5512sy（ciscoProducts 1415）	ASA 5512 適応型セキュリティ アプライアンスのシステム コンテキスト
ASA 5515 システム コンテキスト	ciscoASA5515sy（ciscoProducts 1416）	ASA 5515 適応型セキュリティ アプライアンスのシステム コンテキスト
ASA 5525 システム コンテキスト	ciscoASA5525sy（ciscoProducts1417）	ASA 5525 適応型セキュリティ アプライアンスのシステム コンテキスト
ASA 5545 システム コンテキスト	ciscoASA5545sy（ciscoProducts 1418）	ASA 5545 適応型セキュリティ アプライアンスのシステム コンテキスト
ASA 5555 システム コンテキスト	ciscoASA5555sy（ciscoProducts 1419）	ASA 5555 適応型セキュリティ アプライアンスのシステム コンテキスト
ASA 5515 セキュリティ コンテキスト	ciscoASA5515sc（ciscoProducts 1420）	ASA 5515 適応型セキュリティ アプライアンスのシステム コンテキスト
ASA 5515	ciscoASA5515（ciscoProducts 1421）	ASA 5515 適応型セキュリティ アプライアンス
ASAv	ciscoASAv（ciscoProducts 1902）	Cisco 適応型セキュリティ仮想アプライアンス（ASAv）
ASAv システム コンテキスト	ciscoASAvsy（ciscoProducts 1903）	Cisco 適応型セキュリティ仮想アプライアンス（ASAv）システム コンテキスト
ASAv セキュリティ コンテキスト	ciscoASAvsc（ciscoProducts 1904）	Cisco 適応型セキュリティ仮想アプライアンス（ASAv）セキュリティ コンテキスト
ISA 30004C 産業用セキュリティ アプライアンス	ciscoProducts 2268	ciscoISA30004C
CISCO ISA30004C（4 GE Copper セキュリティ コンテキスト）	ciscoProducts 2139	ciscoISA30004Csc
CISCO ISA30004C（4 GE Copper システム コンテキスト）	ciscoProducts 2140	ciscoISA30004Csy
ISA 30002C2F 産業用セキュリティ アプライアンス	ciscoProducts 2267	ciscoISA30002C2F

製品識別子	sysObjectID	モデル番号
CISCO ISA30002C2F（2 GE 銅線ポート、2 GE 光ファイバ セキュリティ コンテキスト）	ciscoProducts 2142	ciscoISA30002C2Fsc
CISCO ISA30002C2F（2 GE 銅線ポート、2 GE 光ファイバ システム コンテキスト）	ciscoProducts 2143	ciscoISA30002C2Fsy
Cisco 産業用セキュリティ アプライアンス（ISA）30004C シャーシ	cevChassis 1677	cevChassisISA30004C
Cisco 産業用セキュリティ アプライアンス（ISA）30002C2F シャーシ	cevChassis 1678	cevChassisISA30002C2F
ISA30004C Copper SKU 向け中央演算処理装置温度センサー	cevSensor 187	cevSensorISA30004CCpuTempSensor
ISA30002C2F 光ファイバ向け中央演算処理装置温度センサー	cevSensor 189	cevSensorISA30002C2FCpuTempSensor
ISA30004C Copper SKU 向けプロセッサ カード温度センサー	cevSensor 192	cevSensorISA30004CPTS
ISA30002C2F Fiber SKU 向けプロセッサ カード温度センサー	cevSensor 193	cevSensorISA30002C2FPTS
ISA30004C Copper SKU 向けパワー カード温度センサー	cevSensor 197	cevSensorISA30004CPowercardTS
ISA30002C2F Fiber SKU 向けパワー カード温度センサー	cevSensor 198	cevSensorISA30002C2FPowercardTS
ISA30004C 向けポート カード温度センサー	cevSensor 199	cevSensorISA30004CPortcardTS
ISA30002C2F 向けポート カード温度センサー	cevSensor 200	cevSensorISA30002C2FPortcardTS
ISA30004C Copper SKU 向け中央演算処理装置	cevModuleCpuType 329	cevCpuISA30004C
ISA30002C2F 光ファイバ SKU 向け中央演算処理装置	cevModuleCpuType 330	cevCpuISA30002C2F
モジュール ISA30004C、ISA30002C2F	cevModule 111	cevModuleISA3000Type
30004C 産業用セキュリティ アプライアンス ソリッド ステート ドライブ	cevModuleISA3000Type 1	cevModuleISA30004CSSD64

製品識別子	sysObjectID	モデル番号
30002C2F 産業用セキュリティ アプライアンス ソリッド ステート ドライブ	cevModuleISA3000Type 2	cevModuleISA30002C2FSSD64
Cisco ISA30004C/ISA30002C2F ハードウェア バイパス	cevModuleISA3000Type 5	cevModuleISA3000HardwareBypass

物理ベンダー タイプ値

シスコの各シャーシまたはスタンドアロン システムには、SNMP で使用する一意のタイプ番号があります。entPhysicalVendorType OID は CISCO-ENTITY-VENDORTYPE-OID-MIB で定義されます。この値は、ASA、ASAv または ASASM の SNMP エージェントから entPhysicalVendorType オブジェクトで返されます。この値を使用してコンポーネントのタイプ（モジュール、電源装置、ファン、センサー、CPU など）を識別できます。次の表に、ASA モデルの物理ベンダー タイプ値を示します。

表 *51* : 物理ベンダー タイプ値

項目	entPhysicalVendorType OID の説明
Catalyst スイッチ/7600 ルータ向け ASA サービス モジュール	cevCat6kWsSvcAsaSm1（cevModuleCat6000Type 169）
ペイロード暗号化なし Catalyst スイッチ/7600 ルータ向け ASA サービス モジュール	cevCat6kWsSvcAsaSm1K7（cevModuleCat6000Type 186）
5506適応型セキュリティアプライアンス向けアクセラレータ	cevAcceleratorAsa5506（cevOther 10）
5506W 適応型セキュリティ アプライアンス向けアクセラレータ	cevAcceleratorAsa5506W（cevOther 11）
5508適応型セキュリティアプライアンス向けアクセラレータ	cevAcceleratorAsa5508（cevOther 12）
5506 ペイロード暗号化なし適応型セキュリティ アプライアンス向けアクセラレータ	cevAcceleratorAsa5506K7（cevOther 13）
5508 ペイロード暗号化なし適応型セキュリティ アプライアンス向けアクセラレータ	cevAcceleratorAsa5508K7（cevOther 14）
Cisco 適応型セキュリティ アプライアンス（ASA）5506 シャーシ	cevChassisAsa5506（cevChassis 1600）
Cisco 適応型セキュリティ アプライアンス（ASA）5506W シャーシ	cevChassisAsa5506W（cevChassis 1601）

項目	entPhysicalVendorType OID の説明
Cisco 適応型セキュリティ アプライアンス（ASA）5508 シャーシ	cevChassisAsa5508（cevChassis 1602）
ペイロード暗号化なしCisco適応型セキュリティ アプライアンス（ASA）5506 シャーシ	cevChassisAsa5506K7（cevChassis 1603）
ペイロード暗号化なしCisco適応型セキュリティ アプライアンス（ASA）5508 シャーシ	cevChassisAsa5508K7（cevChassis 1604）
5506 適応型セキュリティ アプライアンス向け中央演算処理装置	cevCpuAsa5506（cevModuleCpuType 312）
5506W 適応型セキュリティ アプライアンス向け中央演算処理装置	cevCpuAsa5506W（cevModuleCpuType 313）
5508 適応型セキュリティ アプライアンス向け中央演算処理装置	cevCpuAsa5508（cevModuleCpuType 314）
5506 ペイロード暗号化なし適応型セキュリティ アプライアンス向け中央演算処理装置	cevCpuAsa5506K7（cevModuleCpuType 315）
5508 ペイロード暗号化なし適応型セキュリティ アプライアンス向け中央演算処理装置	cevCpuAsa5508K7（cevModuleCpuType 316）
cevModuleASA5506 型のシャーシ	cevModuleASA5506Type（cevModule 107）
5506 適応型セキュリティ アプライアンス向け現場交換可能ソリッド ステート ドライブ	cevModuleAsa5506SSD（cevModuleASA5506Type 1）
5506W 適応型セキュリティ アプライアンス向け現場交換可能ソリッド ステート ドライブ	cevModuleAsa5506WSSD（cevModuleASA5506Type 2）
5506 ペイロード暗号化なし適応型セキュリティ アプライアンス向け現場交換可能ソリッド ステート ドライブ	cevModuleAsa5506K7SSD（cevModuleASA5506Type 3）
cevModuleASA5508 型のシャーシ	cevModuleASA5508Type（cevModule 108）
5508 適応型セキュリティ アプライアンス向け現場交換可能ソリッド ステート ドライブ	cevModuleAsa5508SSD（cevModuleASA5508Type 1）
5508 ペイロード暗号化なし適応型セキュリティ アプライアンス向け現場交換可能ソリッド ステート ドライブ	cevModuleAsa5508K7SSD（cevModuleASA5508Type 2）
適応型セキュリティ アプライアンス 5508 向けシャーシ冷却ファン	cevFanAsa5508ChassisFan（cevFan 247）
ペイロード暗号化なし適応型セキュリティ アプライアンス 5508 向けシャーシ冷却ファン	cevFanAsa5508K7ChassisFan（cevFan 248）

項目	entPhysicalVendorType OID の説明
適応型セキュリティ アプライアンス 5508 向けシャーシ冷却ファン センサー	cevSensorAsa5508ChassisFanSensor（cevSensor 162）
ペイロード暗号化なし適応型セキュリティ アプライアンス 5508 向けシャーシ冷却ファン センサー	cevSensorAsa5508K7ChassisFanSensor（cevSensor 163）
5506 適応型セキュリティ アプライアンス向け中央演算処理装置温度センサー	cevSensorAsa5506CpuTempSensor（cevSensor 164）
5506W 適応型セキュリティ アプライアンス向け中央演算処理装置温度センサー	cevSensorAsa5506WCpuTempSensor（cevSensor 165）
5508 適応型セキュリティ アプライアンス向け中央演算処理装置温度センサー	cevSensorAsa5508CpuTempSensor（cevSensor 166）
5506 ペイロード暗号化なし適応型セキュリティ アプライアンス向け中央演算処理装置温度センサー	cevSensorAsa5506K7CpuTempSensor（cevSensor 167）
5508 ペイロード暗号化なし適応型セキュリティ アプライアンス向け中央演算処理装置温度センサー	cevSensorAsa5508K7CpuTempSensor（cevSensor 168）
5506適応型セキュリティアプライアンス向けアクセラレータ温度センサー	cevSensorAsa5506AcceleratorTempSensor（cevSensor 169）
5506W 適応型セキュリティ アプライアンス向けアクセラレータ温度センサー	cevSensorAsa5506WAcceleratorTempSensor（cevSensor 170）
5508適応型セキュリティアプライアンス向けアクセラレータ温度センサー	cevSensorAsa5508AcceleratorTempSensor（cevSensor 171）
5506 ペイロード暗号化なし適応型セキュリティ アプライアンス向けアクセラレータ温度センサー	cevSensorAsa5506K7AcceleratorTempSensor（cevSensor 172）
5508 ペイロード暗号化なし適応型セキュリティ アプライアンス向けアクセラレータ温度センサー	cevSensorAsa5508K7AcceleratorTempSensor（cevSensor 173）
5506 適応型セキュリティ アプライアンス向けシャーシ周囲温度センサー	cevSensorAsa5506ChassisTempSensor（cevSensor 174）
5506W 適応型セキュリティ アプライアンス向けシャーシ周囲温度センサー	cevSensorAsa5506WChassisTempSensor（cevSensor 175）
5508 適応型セキュリティ アプライアンス向けシャーシ周囲温度センサー	cevSensorAsa5508ChassisTempSensor（cevSensor 176）
5506 ペイロード暗号化なし適応型セキュリティ アプライアンス向けシャーシ周囲温度センサー	cevSensorAsa5506K7ChassisTempSensor（cevSensor 177）

項目	entPhysicalVendorType OID の説明
5508 ペイロード暗号化なし適応型セキュリティ アプライアンス向けシャーシ周囲温度センサー	cevSensorAsa5508K7ChassisTempSensor（cevSensor 178）
Cisco Adaptive Security Appliance（ASA）5512 適応型セキュリティ アプライアンス	cevChassisASA5512（cevChassis 1113）
Cisco Adaptive Security Appliance（ASA）5512 ペイロード暗号化なし適応型セキュリティ アプライアンス	cevChassisASA5512K7（cevChassis 1108）
Cisco Adaptive Security Appliance（ASA）5515 適応型セキュリティ アプライアンス	cevChassisASA5515（cevChassis 1114）
Cisco Adaptive Security Appliance（ASA）5515 ペイロード暗号化なし適応型セキュリティ アプライアンス	cevChassisASA5515K7（cevChassis 1109）
Cisco Adaptive Security Appliance（ASA）5525 適応型セキュリティ アプライアンス	cevChassisASA5525（cevChassis 1115）
Cisco Adaptive Security Appliance（ASA）5525 ペイロード暗号化なし適応型セキュリティ アプライアンス	cevChassisASA5525K7（cevChassis 1110）
Cisco Adaptive Security Appliance（ASA）5545 適応型セキュリティ アプライアンス	cevChassisASA5545（cevChassis 1116）
Cisco Adaptive Security Appliance（ASA）5545 ペイロード暗号化なし適応型セキュリティ アプライアンス	cevChassisASA5545K7（cevChassis 1111）
Cisco Adaptive Security Appliance（ASA）5555 適応型セキュリティ アプライアンス	cevChassisASA5555（cevChassis 1117）
Cisco Adaptive Security Appliance（ASA）5555 ペイロード暗号化なし適応型セキュリティ アプライアンス	cevChassisASA5555K7（cevChassis 1112）
Cisco Adaptive Security Appliance（ASA）5512 向け中央演算処理装置	cevCpuAsa5512（cevModuleCpuType 229）
ペイロード暗号化なし Cisco Adaptive Security Appliance（ASA）5512 向け中央演算処理装置	cevCpuAsa5512K7（cevModuleCpuType 224）
Cisco Adaptive Security Appliance（ASA）5515 向け中央演算処理装置	cevCpuAsa5515（cevModuleCpuType 230）
ペイロード暗号化なし Cisco Adaptive Security Appliance（ASA）5515 向け中央演算処理装置	cevCpuAsa5515K7（cevModuleCpuType 225）
Cisco Adaptive Security Appliance（ASA）5525 向け中央演算処理装置	cevCpuAsa5525（cevModuleCpuType 231）

項目	entPhysicalVendorType OID の説明
ペイロード暗号化なし Cisco Adaptive Security Appliance（ASA）5525 向け中央演算処理装置	cevCpuAsa5525K7（cevModuleCpuType 226）
Cisco Adaptive Security Appliance（ASA）5545 向け中央演算処理装置	cevCpuAsa5545（cevModuleCpuType 232）
ペイロード暗号化なし Cisco Adaptive Security Appliance（ASA）5545 向け中央演算処理装置	cevCpuAsa5545K7（cevModuleCpuType 227）
Cisco Adaptive Security Appliance（ASA）5555 向け中央演算処理装置	cevCpuAsa5555（cevModuleCpuType 233）
ペイロード暗号化なし Cisco Adaptive Security Appliance（ASA）5555 向け中央演算処理装置	cevCpuAsa5555K7（cevModuleCpuType 228）
ASA 5585 SSP-10 向け CPU	cevCpuAsa5585Ssp10（cevModuleCpuType 204）
ペイロード暗号化なし ASA 5585 SSP-10 向け CPU	cevCpuAsa5585Ssp10K7（cevModuleCpuType 205）
ASA 5585 SSP-20 向け CPU	cevCpuAsa5585Ssp20（cevModuleCpuType 206）
ペイロード暗号化なし ASA 5585 SSP-20 向け CPU	cevCpuAsa5585Ssp20K7（cevModuleCpuType 207）
ASA 5585 SSP-40 向け CPU	cevCpuAsa5585Ssp40（cevModuleCpuType 208）
ペイロード暗号化なし ASA 5585 SSP-40 向け CPU	cevCpuAsa5585Ssp40K7（cevModuleCpuType 209）
ASA 5585 SSP-60 向け CPU	cevCpuAsa5585Ssp60（cevModuleCpuType 210）
ペイロード暗号化なし ASA 5585 SSP-60 向け CPU	cevCpuAsa5585Ssp60K（cevModuleCpuType 211）
Catalyst スイッチ/7600 ルータ向け Cisco ASA サービス モジュールの CPU	cevCpuAsaSm1（cevModuleCpuType 222）
Catalyst スイッチ/7600 ルータ向けペイロード暗号化なし Cisco ASA サービス モジュールの CPU	cevCpuAsaSm1K7（cevModuleCpuType 223）
適応型セキュリティ アプライアンス 5512 シャーシ冷却ファン	cevFanASA5512ChassisFan（cevFan 163）
ペイロード暗号化なし適応型セキュリティ アプライアンス 5512 シャーシ冷却ファン	cevFanASA5512K7ChassisFan（cevFan 172）
適応型セキュリティ アプライアンス 5515 シャーシ冷却ファン	cevFanASA5515ChassisFan（cevFan 164）
ペイロード暗号化なし適応型セキュリティ アプライアンス 5515 シャーシ冷却ファン	cevFanASA5515K7ChassisFan（cevFan 171）

項目	entPhysicalVendorType OID の説明
適応型セキュリティ アプライアンス 5525 シャーシ冷却ファン	cevFanASA5525ChassisFan（cevFan 165）
ペイロード暗号化なし適応型セキュリティ アプライアンス 5525 シャーシ冷却ファン	cevFanASA5525K7ChassisFan（cevFan 170）
適応型セキュリティ アプライアンス 5545 シャーシ冷却ファン	cevFanASA5545ChassisFan（cevFan 166）
ペイロード暗号化なし適応型セキュリティ アプライアンス 5545 シャーシ冷却ファン	cevFanASA5545K7ChassisFan（cevFan 169）
ペイロード暗号化なし適応型セキュリティ アプライアンス 5545 電源ファン	cevFanASA5545K7PSFan（cevFan 161）
適応型セキュリティ アプライアンス 5545 電源ファン	cevFanASA5545PSFan（cevFan 159）
適応型セキュリティ アプライアンス 5555 シャーシ冷却ファン	cevFanASA5555ChassisFan（cevFan 167）
ペイロード暗号化なし適応型セキュリティ アプライアンス 5555 シャーシ冷却ファン	cevFanASA5555K7ChassisFan（cevFan 168）
適応型セキュリティ アプライアンス 5555 電源ファン	cevFanASA5555PSFan（cevFan 160）
ペイロード暗号化なし適応型セキュリティ アプライアンス 5555 電源ファン	cevFanASA5555PSFanK7（cevFan 162）
ASA 5585-X 向け電源ファン	cevFanASA5585PSFan（cevFan 146）
10 ギガビット イーサネット インターフェイス	cevPort10GigEthernet（cevPort 315）
ギガビット イーサネット ポート	cevPortGe（cevPort 109）
適応型セキュリティ アプライアンス 5545 電源装置	cevPowerSupplyASA5545PSInput（cevPowerSupply 323）
適応型セキュリティ アプライアンス 5545 電源入力のプレゼンス センサー	cevPowerSupplyASA5545PSPresence（cevPowerSupply 321）
適応型セキュリティ アプライアンス 5555 電源装置	cevPowerSupplyASA5555PSInput（cevPowerSupply 324）
適応型セキュリティ アプライアンス 5555 電源入力のプレゼンス センサー	cevPowerSupplyASA5555PSPresence（cevPowerSupply 322）
ASA 5585 向け電源入力	cevPowerSupplyASA5585PSInput（cevPowerSupply 304）
Cisco Adaptive Security Appliance（ASA）5512 シャーシ ファン センサー	cevSensorASA5512ChassisFanSensor（cevSensor 120）

項目	entPhysicalVendorType OID の説明
Cisco Adaptive Security Appliance（ASA）5512 向けシャーシ周囲温度センサー	cevSensorASA5512ChassisTemp（cevSensor 107）
Cisco Adaptive Security Appliance（ASA）5512 向け中央演算処理装置温度センサー	cevSensorASA5512CPUTemp（cevSensor 96）
ペイロード暗号化なし Cisco Adaptive Security Appliance（ASA）5512 シャーシ ファン センサー	cevSensorASA5512K7ChassisFanSensor（cevSensor 125）
ペイロード暗号化なし Cisco Adaptive Security Appliance（ASA）5512 向け中央演算処理装置温度センサー	cevSensorASA5512K7CPUTemp（cevSensor 102）
ペイロード暗号化なし適応型セキュリティ アプライアンス 5512 シャーシ冷却ファンのセンサー	cevSensorASA5512K7PSFanSensor（cevSensor 116）
適応型セキュリティ アプライアンス 5512 シャーシ冷却ファンのセンサー	cevSensorASA5512PSFanSensor（cevSensor 119）
Cisco Adaptive Security Appliance（ASA）5515 シャーシ ファン センサー	cevSensorASA5515ChassisFanSensor（cevSensor 121）
Cisco Adaptive Security Appliance（ASA）5515 向けシャーシ周囲温度センサー	cevSensorASA5515ChassisTemp（cevSensor 98）
Cisco Adaptive Security Appliance（ASA）5515 向け中央演算処理装置温度センサー	cevSensorASA5515CPUTemp（cevSensor 97）
ペイロード暗号化なし Cisco Adaptive Security Appliance（ASA）5515 シャーシ ファン センサー	cevSensorASA5515K7ChassisFanSensor（cevSensor 126）
ペイロード暗号化なし Cisco Adaptive Security Appliance（ASA）5515 向け中央演算処理装置温度センサー	cevSensorASA5515K7CPUTemp（cevSensor 103）
ペイロード暗号化なし適応型セキュリティ アプライアンス 5515 シャーシ冷却ファンのセンサー	cevSensorASA5515K7PSFanSensor（cevSensor 115）
適応型セキュリティ アプライアンス 5515 シャーシ冷却ファンのセンサー	cevSensorASA5515PSFanSensor（cevSensor 118）
Cisco Adaptive Security Appliance（ASA）5525 シャーシ ファン センサー	cevSensorASA5525ChassisFanSensor（cevSensor 122）
Cisco Adaptive Security Appliance（ASA）5525 向けシャーシ周囲温度センサー	cevSensorASA5525ChassisTemp（cevSensor 108）
Cisco Adaptive Security Appliance（ASA）5525 向け中央演算処理装置温度センサー	cevSensorASA5525CPUTemp（cevSensor 99）

項目	entPhysicalVendorType OID の説明
ペイロード暗号化なし Cisco Adaptive Security Appliance（ASA）5525 シャーシ ファン センサー	cevSensorASA5525K7ChassisFanSensor（cevSensor 127）
ペイロード暗号化なし Cisco Adaptive Security Appliance（ASA）5525 向け中央演算処理装置温度センサー	cevSensorASA5525K7CPUTemp（cevSensor 104）
ペイロード暗号化なし適応型セキュリティ アプライアンス 5525 シャーシ冷却ファンのセンサー	cevSensorASA5525K7PSFanSensor（cevSensor 114）
適応型セキュリティ アプライアンス 5525 シャーシ冷却ファンのセンサー	cevSensorASA5525PSFanSensor（cevSensor 117）
Cisco Adaptive Security Appliance（ASA）5545 シャーシ ファン センサー	cevSensorASA5545ChassisFanSensor（cevSensor 123）
Cisco Adaptive Security Appliance（ASA）5545 向けシャーシ周囲温度センサー	cevSensorASA5545ChassisTemp（cevSensor 109）
Cisco Adaptive Security Appliance（ASA）5545 向け中央演算処理装置温度センサー	cevSensorASA5545CPUTemp（cevSensor 100）
ペイロード暗号化なし Cisco Adaptive Security Appliance（ASA）5545 シャーシ ファン センサー	cevSensorASA5545K7ChassisFanSensor（cevSensor 128）
ペイロード暗号化なし Cisco Adaptive Security Appliance（ASA）5545 向けシャーシ周囲温度センサー	cevSensorASA5545K7ChassisTemp（cevSensor 90）
ペイロード暗号化なし Cisco Adaptive Security Appliance（ASA）5545 向け中央演算処理装置温度センサー	cevSensorASA5545K7CPUTemp（cevSensor 105）
ペイロード暗号化なし適応型セキュリティ アプライアンス 5545 シャーシ冷却ファンのセンサー	cevSensorASA5545K7PSFanSensor（cevSensor 113）
ペイロード暗号化なし適応型セキュリティ アプライアンス 5545 電源入力のプレゼンス センサー	cevSensorASA5545K7PSPresence（cevSensor 87）
ペイロード暗号化なし適応型セキュリティ アプライアンス 5545 電源ファンの温度センサー	cevSensorASA5545K7PSTempSensor（cevSensor 94）
ペイロード暗号化なし適応型セキュリティ アプライアンス 5545 電源ファンのセンサー	cevSensorASA5545PSFanSensor（cevSensor 89）
適応型セキュリティ アプライアンス 5545 電源入力のプレゼンス センサー	cevSensorASA5545PSPresence（cevSensor 130）
適応型セキュリティ アプライアンス 5555 電源入力のプレゼンス センサー	cevSensorASA5545PSPresence（cevSensor 131）

項目	entPhysicalVendorType OID の説明
適応型セキュリティ アプライアンス 5545 電源ファンの温度センサー	cevSensorASA5545PSTempSensor（cevSensor 92）
Cisco Adaptive Security Appliance（ASA）5555 シャーシ ファン センサー	cevSensorASA5555ChassisFanSensor（cevSensor 124）
Cisco Adaptive Security Appliance（ASA）5555 向けシャーシ周囲温度センサー	cevSensorASA5555ChassisTemp（cevSensor 110）
Cisco Adaptive Security Appliance（ASA）5555 向け中央演算処理装置温度センサー	cevSensorASA5555CPUTemp（cevSensor 101）
ペイロード暗号化なし Cisco Adaptive Security Appliance（ASA）5555 シャーシ ファン センサー	cevSensorASA5555K7ChassisFanSensor（cevSensor 129）
ペイロード暗号化なし Cisco Adaptive Security Appliance（ASA）5555 向けシャーシ周囲温度センサー	cevSensorASA5555K7ChassisTemp（cevSensor 111）
ペイロード暗号化なし Cisco Adaptive Security Appliance（ASA）5555 向け中央演算処理装置温度センサー	cevSensorASA5555K7CPUTemp（cevSensor 106）
ペイロード暗号化なし適応型セキュリティ アプライアンス 5555 シャーシ冷却ファンのセンサー	cevSensorASA5555K7PSFanSensor（cevSensor 112）
ペイロード暗号化なし適応型セキュリティ アプライアンス 5555 電源入力のプレゼンス センサー	cevSensorASA5555K7PSPresence（cevSensor 88）
ペイロード暗号化なし適応型セキュリティ アプライアンス 5555 電源ファンの温度センサー	cevSensorASA5555K7PSTempSensor（cevSensor 95）
適応型セキュリティ アプライアンス 5555 電源ファンのセンサー	cevSensorASA5555PSFanSensor（cevSensor 91）
適応型セキュリティ アプライアンス 5555 電源ファンの温度センサー	cevSensorASA5555PSTempSensor（cevSensor 93）
ASA 5585-X 向け電源ファン	cevSensorASA5585PSFanSensor（cevSensor 86）
ASA 5585-X 向け電源入力のセンサー	cevSensorASA5585PSInput（cevSensor 85）
ASA 5585 SSP-10 向け CPU 温度センサー	cevSensorASA5585SSp10CPUTemp（cevSensor 77）
ペイロード暗号化なし ASA 5585 SSP-10 向け CPU 温度センサー	cevSensorASA5585SSp10K7CPUTemp（cevSensor 78）
ASA 5585 SSP-20 向け CPU 温度センサー	cevSensorASA5585SSp20CPUTemp（cevSensor 79）

項目	entPhysicalVendorType OID の説明
ペイロード暗号化なし ASA 5585 SSP-20 向け CPU 温度センサー	cevSensorASA5585SSp20K7CPUTemp（cevSensor 80）
ASA 5585 SSP-40 向け CPU 温度センサー	cevSensorASA5585SSp40CPUTemp（cevSensor 81）
ペイロード暗号化なし ASA 5585 SSP-40 向け CPU 温度センサー	cevSensorASA5585SSp40K7CPUTemp（cevSensor 82）
ASA 5585 SSP-60 向け CPU 温度センサー	cevSensorASA5585SSp60CPUTemp（cevSensor 83）
ペイロード暗号化なし ASA 5585 SSP-60 向け CPU 温度センサー	cevSensorASA5585SSp60K7CPUTemp（cevSensor 84）
適応型セキュリティ アプライアンス 5555-X 現場交換可能ソリッド ステート ドライブ	cevModuleASA5555XFRSSD (cevModuleCommonCards 396)
適応型セキュリティ アプライアンス 5545-X 現場交換可能ソリッド ステート ドライブ	cevModuleASA5545XFRSSD (cevModuleCommonCards 397)
適応型セキュリティ アプライアンス 5525-X 現場交換可能ソリッド ステート ドライブ	cevModuleASA5525XFRSSD (cevModuleCommonCards 398)
適応型セキュリティ アプライアンス 5515-X 現場交換可能ソリッド ステート ドライブ	cevModuleASA5515XFRSSD (cevModuleCommonCards 399)
適応型セキュリティ アプライアンス 5512-X 現場交換可能ソリッド ステート ドライブ	cevModuleASA5512XFRSSD (cevModuleCommonCards 400)
Cisco 適応型セキュリティ仮想アプライアンス	cevChassisASAv（cevChassis 1451）

MIB でサポートされるテーブルおよびオブジェクト

次の表 に、指定された MIB でサポートされるテーブルおよびオブジェクトを示します。

表 *52 : MIB* でサポートされるテーブルおよびオブジェクト

MIB 名	サポートされているテーブルとオブジェクト
CISCO-ENHANCED-MEMPOOL-MIB	cempMemPoolTable、cempMemPoolIndex、cempMemPoolType、cempMemPoolName、cempMemPoolAlternate、cempMemPoolValid、cempMemPoolUsed、cempMemPoolFree、cempMemPoolUsedOvrflw、cempMemPoolHCUsed、cempMemPoolFreeOvrflw、cempMemPoolHCFree

MIB 名	サポートされているテーブルとオブジェクト
CISCO-ENTITY-SENSOR-EXT-MIB （注） Catalyst 6500 スイッチ/7600 ルータ向け ASA サービス モジュールではサポートされていません。	ceSensorExtThresholdTable
CISCO-L4L7MODULE-RESOURCE-LIMIT-MIB	ciscoL4L7ResourceLimitTable
CISCO-TRUSTSEC-SXP-MIB （注） Cisco 適応型セキュリティ仮想アプライアンス（ASAv）ではサポートされていません。	ctsxSxpGlobalObjects、ctsxSxpConnectionObjects、ctsxSxpSgtObjects
DISMAN-EVENT-MIB	mteTriggerTable、mteTriggerThresholdTable、mteObjectsTable、mteEventTable、mteEventNotificationTable
DISMAN-EXPRESSION-MIB （注） Catalyst 6500 スイッチ/7600 ルータ向け ASA サービス モジュールではサポートされていません。	expExpressionTable、expObjectTable、expValueTable
ENTITY-SENSOR-MIB （注） Catalyst 6500 スイッチ/7600 ルータ向け ASA サービス モジュールではサポートされていません。 （注） シャーシの温度、ファン RPM、電源電圧などの物理センサーに関連する情報を提供します。Cisco ASAv プラットフォームではサポートされていません。	entPhySensorTable
NAT-MIB	natAddrMapTable、natAddrMapIndex、natAddrMapName、natAddrMapGlobalAddrType、natAddrMapGlobalAddrFrom、natAddrMapGlobalAddrTo、natAddrMapGlobalPortFrom、natAddrMapGlobalPortTo、natAddrMapProtocol、natAddrMapAddrUsed、natAddrMapRowStatus
CISCO-PTP-MIB （注） E2E トランスペアレント クロック モードに対応する MIB のみがサポートされます。	ciscoPtpMIBSystemInfo、cPtpClockDefaultDSTable、cPtpClockTransDefaultDSTable、cPtpClockPortTransDSTable

サポートされるトラップ（通知）

次の表 に、サポートされているトラップ（通知）および関連する MIB を示します。

表 *53 :* サポートされるトラップ（通知）

トラップおよび **MIB** 名	変数バインド リスト	説明
authenticationFailure （SNMPv2-MIB）	—	SNMP バージョン 1 または 2 の場合は、SNMP 要求で指定されたコミュニティ ストリングが正しくありません。SNMP バージョン 3 では、auth または priv パスワードまたはユーザ名が間違っている場合、レポート PDU がトラップの代わりに生成されます。 **snmp-server enable traps snmp authentication** コマンドは、これらのトラップの伝送をイネーブルおよびディセーブルにするために使用されます。
ccmCLIRunningConfigChanged （CISCO-CONFIG-MAN-MIB）	—	**snmp-server enable traps config** コマンドは、このトラップの送信をイネーブルにするために使用されます。
cefcFRUInserted (CISCO-ENTITY-FRU-CONTROL -MIB)	—	**snmp-server enable traps entity fru-insert** コマンドはこの通知をイネーブルにするために使用されます。このトラップは、ASA 5506-X および ASA 5508-X には適用されません。
cefcFRURemoved (CISCO-ENTITY-FRU-CONTROL -MIB)	—	**snmp-server enable traps entity fru-remove** コマンドはこの通知をイネーブルにするために使用されます。このトラップは、ASA 5506-X および ASA 5508-X には適用されません。

トラップおよび MIB 名	変数バインド リスト	説明
ceSensorExtThresholdNotification (CISCO-ENTITY-SENSOR-EXT -MIB) （注） Catalyst 6500 スイッチ/7600 ルータ向け ASA サービス モジュールではサポートされていません。	ceSensorExtThresholdValue、entPhySensorValue、entPhySensorType、entPhysicalName	

トラップおよび MIB 名	変数バインド リスト	説明
		snmp-server enable traps entity [**power-supply-failure** | **fan-failure** | **cpu-temperature**] コマンドは、エンティティしきい値通知の伝送をイネーブルにするために使用されます。この通知は、電源障害に対して送信されます。送信されるオブジェクトは、ファンおよび CPU の温度を指定します。 **snmp-server enable traps entity fan-failure** コマンドは、ファン障害トラップの送信をイネーブルにするために使用されます。このトラップは、ASA 5506-X および ASA 5508-X には適用されません。 **snmp-server enable traps entity power-supply-failure** コマンドは、電源障害トラップの送信をイネーブルにするために使用されます。このトラップは、ASA 5506-X および ASA 5508-X には適用されません。 **snmp-server enable traps entity chassis-fan-failure** コマンドは、シャーシファン障害トラップの送信をイネーブルにするために使用されます。このトラップは、ASA 5506-X および ASA 5508-X には適用されません。 **snmp-server enable traps entity cpu-temperature** コマンドは、高 CPU 温度トラップの送信をイネーブルにするために使用されます。 **snmp-server enable traps entity power-supply-presence** コマンドは、電源プレゼンス障害トラップの送信をイネーブルにするために使用されます。このトラップは、ASA 5506-X および ASA 5508-X には適用されません。 **snmp-server enable traps entity power-supply-temperature** コマンドは、電源温度しきい値トラップの送信をイネーブルにするために使用されます。このトラップは、ASA 5506-X および ASA 5508-X には適用されません。

トラップおよび **MIB** 名	変数バインド リスト	説明
		snmp-server enable traps entity chassis-temperature コマンドは、シャーシ周囲温度トラップの送信をイネーブルにするために使用されます。 **snmp-server enable traps entity accelerator-temperature** コマンドは、シャーシアクセラレータ温度トラップの送信をイネーブルにするために使用されます。このトラップは、ASA 5506-X および ASA 5508-X には適用されません。
cipSecTunnelStart (CISCO-IPSEC-FLOW-MONITOR -MIB)	cipSecTunLifeTime、cipSecTunLifeSize	**snmp-server enable traps ipsec start** コマンドは、このトラップの送信をイネーブルにするために使用されます。
cipSecTunnelStop (CISCO-IPSEC-FLOW-MONITOR -MIB)	cipSecTunActiveTime	**snmp-server enable traps ipsec stop** コマンドは、このトラップの送信をイネーブルにするために使用されます。
ciscoConfigManEvent （CISCO-CONFIG-MAN-MIB）	—	**snmp-server enable traps config** コマンドは、このトラップの送信をイネーブルにするために使用されます。
ciscoRasTooManySessions (CISCO-REMOTE-ACCESS -MONITOR-MIB)	crasNumSessions、crasNumUsers、crasMaxSessionsSupportable、crasMaxUsersSupportable、crasThrMaxSessions	**snmp-server enable traps remote-access session-threshold-exceeded** コマンドは、これらのトラップの送信をイネーブルにするために使用されます。
clogMessageGenerated （CISCO-SYSLOG-MIB）	clogHistFacility、clogHistSeverity、clogHistMsgName、clogHistMsgText、clogHistTimestamp	syslog メッセージが生成されます。 clogMaxSeverity オブジェクトの値は、トラップとして送信する syslog メッセージを決定するために使用されます。 **snmp-server enable traps syslog** コマンドは、これらのトラップの伝送をイネーブルおよびディセーブルにするために使用されます。

トラップおよび **MIB** 名	変数バインド リスト	説明
clrResourceLimitReached (CISCO-L4L7MODULE-RESOURCE-LIMIT-MIB)	crlResourceLimitValueType、crlResourceLimitMax、clogOriginIDType、clogOriginID	**snmp-server enable traps connection-limit-reached** コマンドは、この connection-limit-reached 通知の伝送を有効にするために使用されます。clogOriginID オブジェクトには、トラップを発信したコンテキスト名が含まれています。
coldStart （SNMPv2-MIB）	—	SNMP エージェントが起動されました。 **snmp-server enable traps snmp coldstart** コマンドは、これらのトラップの伝送をイネーブルおよびディセーブルにするために使用されます。
cpmCPURisingThreshold （CISCO-PROCESS-MIB）	cpmCPURisingThresholdValue、cpmCPUTotalMonIntervalValue、cpmCPUInterruptMonIntervalValue、cpmCPURisingThresholdPeriod、cpmProcessTimeCreated、cpmProcExtUtil5SecRev	**snmp-server enable traps cpu threshold rising** コマンドは、CPU threshold rising 通知の伝送を有効にするために使用されます。cpmCPURisingThresholdPeriod オブジェクトは、他のオブジェクトとともに送信されます。
entConfigChange （ENTITY-MIB）	—	**snmp-server enable traps entity config-change fru-insert fru-remove** コマンドは、この通知をイネーブルにするために使用されます。 （注） この通知は、セキュリティ コンテキストが作成または削除された場合にマルチ モードでのみ送信されます。
linkDown （IF-MIB）	ifIndex、ifAdminStatus、ifOperStatus	インターフェイスのリンクダウン トラップ。 **snmp-server enable traps snmp linkdown** コマンドは、これらのトラップの伝送をイネーブルおよびディセーブルにするために使用されます。

トラップおよび **MIB** 名	変数バインド リスト	説明
linkUp （IF-MIB）	ifIndex、ifAdminStatus、ifOperStatus	インターフェイスのリンクアップ トラップ。 **snmp-server enable traps snmp linkup** コマンドは、これらのトラップの伝送をイネーブルおよびディセーブルにするために使用されます。
mteTriggerFired （DISMAN-EVENT-MIB）	mteHotTrigger、mteHotTargetName、mteHotContextName、mteHotOID、mteHotValue、cempMemPoolName、cempMemPoolHCUsed	**snmp-server enable traps memory-threshold** コマンドは、memory threshold 通知を有効にするために使用されてます。mteHotOID が cempMemPoolHCUsed に設定されます。cempMemPoolName および cempMemPoolHCUsed オブジェクトは、他のオブジェクトとともに送信されます。
mteTriggerFired （DISMAN-EVENT-MIB） （注） Catalyst 6500 スイッチ/7600 ルータ向け ASA サービス モジュールではサポートされていません。	mteHotTrigger、mteHotTargetName、mteHotContextName、mteHotOID、mteHotValue、ifHCInOctets、ifHCOutOctets、ifHighSpeed、entPhysicalName	**snmp-server enable traps interface-threshold** コマンドは、interface threshold 通知を有効にするために使用されます。entPhysicalName オブジェクトは、他のオブジェクトと共に送信されます。
natPacketDiscard （NAT-MIB）	ifIndex	**snmp-server enable traps nat packet-discard** コマンドは、NAT packet discard 通知を有効にするために使用されます。この通知は、マッピング スペースを使用できないため、5 分間にレート制限され、IP パケットが NAT により廃棄された場合に生成されます。ifIndex は、マッピング インターフェイスの ID を提供します。
warmStart （SNMPv2-MIB）	—	**snmp-server enable traps snmp warmstart** コマンドは、これらのトラップの伝送をイネーブルおよびディセーブルにするために使用されます。

インターフェイスの種類と例

SNMP トラフィック統計情報を生成するインターフェイスの種類には次のものがあります。

- 論理：物理統計情報のサブセットであり、ソフトウェア ドライバによって収集される統計情報。
- 物理：ハードウェア ドライバによって収集される統計情報。物理的な名前の付いた各インターフェイスは、それに関連付けられている論理統計情報と物理統計情報のセットを1つ持っています。各物理インターフェイスは、関連付けられている VLAN インターフェイスを複数持っている場合があります。VLANインターフェイスは論理統計情報だけを持っています。

（注） 複数の VLAN インターフェイスが関連付けられている物理インターフェイスでは、ifInOctets と ifOutoctets の OID の SNMP カウンタがその物理インターフェイスの集約トラフィック カウンタと一致していることに注意してください。

- VLAN-only：SNMP は ifInOctets と ifOutOctets に対して論理統計情報を使用します。

次の表の例で、SNMP トラフィック統計情報における差異を示します。例1では、**show interface** コマンドと **show traffic** コマンドの物理出力統計情報と論理出力統計情報の差異を示します。例 2 では、**show interface** コマンドと **show traffic** コマンドの VLAN だけのインターフェイスに対する出力統計情報を示します。この例は、統計情報が **show traffic** コマンドに対して表示される出力に近いことを示しています。

表 *54 :* 物理インターフェイスと *VLAN* インターフェイスの *SNMP* トラフィック統計情報

例 1	例 2
ciscoasa# **show interface GigabitEthernet3/2** interface GigabitEthernet3/2 description fullt-mgmt nameif mgmt security-level 10 ip address 10.7.14.201 255.255.255.0 management-only ciscoasa# **show traffic** (Condensed output) Physical Statistics GigabitEthernet3/2: received (in 121.760 secs) **36 packets 3428 bytes** 0 pkts/sec 28 bytes/sec Logical Statistics mgmt: received (in 117.780 secs) **36 packets 2780 bytes** 0 pkts/sec 23 bytes/sec 次の例は、管理インターフェイスと物理インターフェイスの SNMP 出力統計情報を示しています。ifInOctets 値は、**show traffic** コマンド出力で表示される物理統計情報出力に近くなりますが、論理統計情報出力には近くなりません。 mgmt インターフェイスの ifIndex： IF_MIB::ifDescr.6 = Adaptive Security Appliance 'mgmt' interface 物理インターフェイス統計情報に対応する物理インターフェイス統計： **IF-MIB::ifInOctets.6 = Counter32:3246**	ciscoasa# **show interface GigabitEthernet0/0.100** interface GigabitEthernet0/0.100 vlan 100 nameif inside security-level 100 ip address 10.7.1.101 255.255.255.0 standby 10.7.1.102 ciscoasa# **show traffic** inside received (in 9921.450 secs) **1977 packets 126528 bytes** 0 pkts/sec 12 bytes/sec transmitted (in 9921.450 secs) **1978 packets 126556 bytes** 0 pkts/sec 12 bytes/sec 内部の VLAN の ifIndex： IF-MIB::ifDescr.9 = Adaptive Security Appliance 'inside' interface **IF-MIB::ifInOctets.9 = Counter32: 126318**

SNMP バージョン 3 の概要

SNMP バージョン 3 は SNMP バージョン 1 またはバージョン 2c では使用できなかったセキュリティ拡張機能を提供します。SNMP バージョン 1 とバージョン 2c は SNMP サーバと SNMP エージェント間でデータをクリアテキストで転送します。SNMP バージョン 3 は認証とプライバシー オプションを追加してプロトコル オペレーションをセキュリティ保護します。また、このバージョンはユーザベース セキュリティ モデル（USM）とビューベース アクセス コント

ロール モデル（VACM）を通して SNMP エージェントと MIB オブジェクトへのアクセスをコントロールします。ASA は、SNMP グループとユーザの作成、およびセキュアな SNMP 通信の転送の認証と暗号化を有効にするために必要なホストの作成もサポートします。

セキュリティ モデル

設定上の目的のために、認証とプライバシーのオプションはセキュリティ モデルにまとめられます。セキュリティ モデルはユーザとグループに適用され、次の 3 つのタイプに分けられます。

- NoAuthPriv：認証もプライバシーもありません。メッセージにどのようなセキュリティも適用されないことを意味します。
- AuthNoPriv：認証はありますがプライバシーはありません。メッセージが認証されることを意味します。
- AuthPriv：認証とプライバシーがあります。メッセージが認証および暗号化されることを意味します。

SNMP グループ

SNMP グループはユーザを追加できるアクセス コントロール ポリシーです。各 SNMP グループはセキュリティ モデルを使用して設定され、SNMP ビューに関連付けられます。SNMP グループ内のユーザは、SNMP グループのセキュリティ モデルに一致する必要があります。これらのパラメータは、SNMP グループ内のユーザがどのタイプの認証とプライバシーを使用するかを指定します。各 SNMP グループ名とセキュリティ モデルのペアは固有である必要があります。

SNMP ユーザ

SNMPユーザは、指定されたユーザ名、ユーザが属するグループ、認証パスワード、暗号化パスワード、および使用する認証アルゴリズムと暗号化アルゴリズムを持ちます。認証アルゴリズムのオプションは MD5 と SHA です。暗号化アルゴリズムのオプションは DES、3DES、およびAES（128、192、および256バージョンで使用可能）です。ユーザを作成した場合は、それをSNMPグループに関連付ける必要があります。その後、そのユーザはグループのセキュリティ モデルを継承します。

SNMP ホスト

SNMP ホストは SNMP 通知とトラップの送信先となる IP アドレスです。トラップは設定されたユーザだけに送信されるため、ターゲット IP アドレスとともに SNMP バージョン 3 のホストを設定するには、ユーザ名を設定する必要があります。SNMP ターゲット IP アドレスとターゲットパラメータ名は ASA で一意である必要があります。各 SNMP ホストはそれぞれに関連付けられているユーザ名を 1 つだけ持つことができます。SNMP トラップを受信するには、**snmp-server host** コマンドを追加した後に、NMS のユーザクレデンシャルが ASA のクレデンシャルと一致するように設定してください。

ASA と Cisco IOS ソフトウェアの実装の相違点

ASA での SNMP バージョン 3 の実装は、Cisco IOS ソフトウェアでの SNMP バージョン 3 の実装とは次の点で異なります。

- ローカル エンジン ID とリモート エンジン ID は設定できません。ローカルエンジン ID は、ASA が起動されたとき、またはコンテキストが作成されたときに生成されます。
- ビューベースのアクセス コントロールに対するサポートはないため、結果として MIB のブラウジングは無制限になります。
- サポートは、USM、VACM、FRAMEWORK、および TARGET という MIB に制限されます。
- 正しいセキュリティ モデルを使用してユーザとグループを作成する必要があります。
- 正しい順序でユーザ、グループ、およびホストを削除する必要があります。
- snmp-server host コマンドを使用すると、着信 SNMP トラフィックを許可する ASA ルールが作成されます。

SNMP syslog メッセージ

SNMP では、212*nnn* という番号が付いた詳細な syslog メッセージが生成されます。syslog メッセージは、ASA または ASASM から、SNMP 要求、SNMP トラップ、SNMP チャネルのステータスを、指定のインターフェイスの指定のホストに表示します。

syslog メッセージの詳細については、『syslog メッセージ ガイド』を参照してください。

（注） SNMP syslog メッセージがレート制限（毎秒約 4000）を超えた場合、SNMP ポーリングは失敗します。

アプリケーション サービスとサードパーティ ツール

SNMP サポートについては、次の URL を参照してください。

http://www.cisco.com/en/US/tech/tk648/tk362/tk605/tsd_technology_support_sub-protocol_home.html

SNMP バージョン 3 MIB をウォークするためのサードパーティ ツールの使い方については、次の URL を参照してください。

http://www.cisco.com/en/US/docs/security/asa/asa83/snmp/snmpv3_tools.html

SNMP のガイドライン

この項では、SNMP を設定する前に考慮する必要のあるガイドラインおよび制限事項について説明します。

フェールオーバーのガイドライン

各 ASA の SNMP クライアントはそれぞれのピアとエンジン データを共有します。エンジン データには、SNMP-FRAMEWORK-MIB の engineID、engineBoots、および engineTime オブジェクトが含まれます。エンジン データは flash:/snmp/*contextname* にバイナリ ファイルとして書き込まれます。

その他のガイドライン

- SNMP トラップを受信するか MIB をブラウズするには、CiscoWorks for Windows か別の SNMP MIB-II 互換ブラウザを持っている必要があります。
- ビューベースのアクセス コントロールはサポートされませんが、ブラウジングに VACM MIB を使用してデフォルトのビュー設定を決定できます。
- ENTITY-MIB は管理外コンテキストでは使用できません。代わりに IF-MIB を使用して、管理外コンテキストでクエリーを実行します。
- ENTITY-MIB は Firepower 9300 では使用できません。代わりに、CISCO-FIREPOWER-EQUIPMENT-MIB および CISCO-FIREPOWER-SM-MIB を使用します。
- AIP SSM または AIP SSC では、SNMP バージョン 3 はサポートされません。
- SNMP デバッグはサポートされません。
- ARP 情報の取得はサポートされません。
- SNMP SET コマンドはサポートされません。
- NET-SNMP バージョン 5.4.2.1 を使用する場合、暗号化アルゴリズム バージョン AES128 だけがサポートされます。暗号化アルゴリズム バージョンの AES256 または AES192 はサポートされません。
- 結果として SNMP 機能の整合性が取れない状態になる場合、既存の設定への変更は拒否されます。
- SNMP バージョン 3 の設定は、グループ、ユーザ、ホストの順に行う必要があります。
- グループを削除する前に、そのグループに関連付けられているすべてのユーザが削除されていることを確認する必要があります。
- ユーザを削除する前に、そのユーザ名に関連付けられているホストが設定されていないことを確認する必要があります。

- 特定のセキュリティモデルを使用して特定のグループに属するようにユーザが設定されている場合にそのグループのセキュリティレベルを変更する場合は、次の順に操作を実行する必要があります。
  - そのグループからユーザを削除します。
  - グループのセキュリティ レベルを変更します。
  - 新しいグループに属するユーザを追加します。
- MIB オブジェクトのサブセットへのユーザ アクセスを制限するためのカスタム ビューの作成はサポートされていません。
- すべての要求とトラップは、デフォルトの読み取り/通知ビューだけで使用できます。
- connection-limit-reached トラップは管理コンテキストで生成されます。このトラップを生成するには、接続制限に達したユーザ コンテキストで設定された SNMP サーバ ホストが少なくとも 1 つ必要です。
- ASA 5585 SSP-40（NPE）のシャーシ温度を問い合わせることはできません。
- 最大 4000 個までホストを追加できます。ただし、トラップの対象として設定できるのはそのうちの 128 個だけです。
- サポートされるアクティブなポーリング先の総数は 128 個です。
- ホスト グループとして追加する個々のホストを示すためにネットワーク オブジェクトを指定できます。
- 1 つのホストに複数のユーザを関連付けることができます。
- ネットワーク オブジェクトは、別の **host-group** コマンドと重複して指定することができます。異なるネットワーク オブジェクトの共通のホストに対しては、最後のホスト グループに指定した値が適用されます。
- ホスト グループや他のホスト グループと重複するホストを削除すると、設定済みのホスト グループで指定されている値を使用してホストが再設定されます。
- ホストで取得される値は、コマンドの実行に使用するように指定したシーケンスによって異なります。
- SNMP で送信できるメッセージのサイズは 1472 バイトまでです。
- SNMPv3 エンジン ID はクラスタのメンバー間で同期されません。そのため、SNMPv3 については、クラスタの各ユニットでそれぞれ設定する必要があります。
- バージョン 9.4(1) では、ASA がサポートするコンテキストあたりの SNMP サーバのトラップ ホスト数に制限はありません。**show snmp-server host** コマンドの出力には ASA をポーリングしているアクティブなホストと、静的に設定されたホストのみが表示されます。

トラブルシューティングのヒント

- NMS からの着信パケットを受信する SNMP プロセスが実行されていることを確認するには、次のコマンドを入力します。

```
ciscoasa(config)# show process | grep snmp
```

- SNMP からの syslog メッセージをキャプチャし、ASA コンソールに表示するには、次のコマンドを入力します。

```
ciscoasa(config)# logging list snmp message 212001-212015
ciscoasa(config)# logging console snmp
```

- SNMPプロセスがパケットを送受信していることを確認するには、次のコマンドを入力します。

```
ciscoasa(config)# clear snmp-server statistics
ciscoasa(config)# show snmp-server statistics
```

出力は SNMPv2-MIB の SNMP グループに基づきます。

- SNMPパケットがASAを通過し、SNMPプロセスに送信されていることを確認するには、次のコマンドを入力します。

```
ciscoasa(config)# clear asp drop
ciscoasa(config)# show asp drop
```

- NMS が正常にオブジェクトを要求できない場合、またはASA からの着信トラップを処理していない場合は、次のコマンドを入力し、パケットキャプチャを使用して問題を切り離します。

```
ciscoasa (config)# access-list snmp permit udp any eq snmptrap any
ciscoasa (config)# access-list snmp permit udp any any eq snmp
ciscoasa (config)# capture snmp type raw-data access-list snmp interface mgmt
ciscoasa (config)# copy /pcap capture:snmp tftp://192.0.2.5/exampledir/snmp.pcap
```

- ASAが期待どおりに動作していない場合は、次の操作を実行して、ネットワークトポロジとトラフィックに関する情報を取得します。
  - NMS の設定について、次の情報を取得します。

    タイムアウトの回数

    リトライ回数

    エンジン ID キャッシング

    使用されるユーザ名とパスワード

  - 次のコマンドを発行します。

show block

show interface

show process

show cpu

show vm

- 重大エラーが発生した場合は、エラーの再現を支援するために、Cisco TAC にトレースバック ファイルと **show tech-support** コマンドの出力を送信します。
- SNMP トラフィックが ASA インターフェイスを通過できない場合、**icmp permit** コマンドを使用して、リモート SNMP サーバから ICMP トラフィックを許可する必要がある場合があります。
- トラブルシューティングの追加情報については、次の URL を参照してください。
http://www.cisco.com/c/en/us/support/docs/security/asa-5500-x-series-next-generation-firewalls/116423-troubleshoot-asa-snmp.html

SNMP を設定します。

ここでは、SNMP の設定方法について説明します。

手順

ステップ 1 SNMP エージェントおよび SNMP サーバをイネーブルにします。

ステップ 2 SNMP トラップを設定します。

ステップ 3 SNMP バージョン 1 および 2c のパラメータまたは SNMP バージョン 3 のパラメータを設定します。

SNMP エージェントおよび SNMP サーバの有効化

SNMP エージェントおよび SNMP サーバをイネーブルにするには、次の手順を実行します。

手順

ASA で SNMP エージェントおよび SNMP サーバを有効にします。デフォルトでは、SNMP サーバはイネーブルになっています。

snmp-server enable

例：

```
ciscoasa(config)# snmp-server enable
```

Configure SNMP Traps

SNMP エージェントが生成するトラップ、およびそのトラップを収集し、NMS に送信する方法を指定するには、次の手順を実行します。

手順

個別のトラップ、トラップのセット、またはすべてのトラップを NMS に送信します。

snmp-server enable traps [**all** | **syslog** | **snmp** [**authentication** | **linkup** | *linkdown* | *coldstart* | *warmstart*] | **config** | **entity** [**config-change** | **fru-insert** | **fru-remove** | **fan-failure** | **cpu-temperature** | **chassis-fan-failure** | **power-supply-failure**] | *chassis-temperature* | *power-supply-presence* | *power-supply-temperature* | *accelerator-temperature* | *l1-bypass-status*] | **ikev2** [*start* | *stop*] | **ipsec** [*start* | *stop*] | **remote-access** [**session-threshold-exceeded**] | **connection-limit-reached** | **cpu threshold rising** | **interface-threshold** | **memory-threshold** | **nat** [*packet-discard*]

例：

```
ciscoasa(config)# snmp-server enable traps snmp authentication linkup linkdown coldstart
 warmstart
```

このコマンドでは、トラップとして NMS に送信する syslog メッセージをイネーブルにしています。デフォルトコンフィギュレーションでは、例に示すように、すべての SNMP 標準トラップがイネーブルになっています。このトラップを無効にするには、**no snmp-server enable traps snmp** コマンドを使用します。このコマンドを入力するときにトラップ タイプを指定しない場合、デフォルトでは **syslog** トラップになります。デフォルトでは、**syslog** トラップはイネーブルになっています。デフォルトの SNMP トラップは、**syslog** トラップとともにイネーブルの状態を続けます。syslog MIB からのトラップを生成するには、**logging history** コマンドと **snmp-server enable traps syslog** コマンドの両方を設定する必要があります。SNMP トラップがイネーブルにされたデフォルトの状態を復元するには、**clear configure snmp-server** コマンドを使用します。デフォルトでは他のトラップはすべてディセーブルです。

管理コンテキストでのみ使用できるトラップ：

- **connection-limit-reached**
- **entity**
- **memory-threshold**

システム コンテキストの物理的に接続されたインターフェイスに対してだけ管理コンテキストを介して生成されたトラップ：

- **interface-threshold**

（注） **interface-threshold** トラップは、Catalyst 6500 スイッチ/7600 ルータ向け ASA サービス モジュールではサポートされていません。

その他すべてのトラップは、シングル モードの管理およびユーザ コンテキストで使用できます。

マルチ コンテキスト モードでは、**fan-failure** トラップ、**power-supply-failure** トラップ、および **cpu-temperature** トラップは、ユーザ コンテキストではなく管理コンテキストからのみ生成されます（ASA 5512-X、5515-X、5525-X、5545-X、および 5555-X にのみ適用されます）。

accelerator-temperature しきい値トラップは、ASA 5506-X および ASA 5508-X にのみ適用されます。

chassis-fan-failure トラップは、ASA 5506-X には適用されません。

config トラップを指定すると、ciscoConfigManEvent 通知と ccmCLIRunningConfigChanged 通知がイネーブルになります。これらの通知は、コンフィギュレーション モードを終了した後に生成されます。

次のトラップは ASA 5506-x および ASA 5508-x に適用されません：**fan-failure**、 **fru-insert**、**fru-remove**、 **power-supply**、 **power-supply-failure**、 **power-supply-presence**、および **power-supply-temperature**。

CPU 使用率が、設定されたモニタリング期間に設定済みしきい値を超えると、**cpu threshold rising** トラップが生成されます。

使用されたシステム コンテキストのメモリが総システム メモリの 80 % に達すると、**memory-threshold** トラップが管理コンテキストから生成されます。他のすべてのユーザ コンテキストでは、このトラップは使用メモリが特定のコンテキストの総システム メモリの 80 % に到達した場合に生成されます。

（注） SNMP は電圧センサーをモニタしません。

CPU 使用率のしきい値の設定

CPU 使用率のしきい値を設定するには、次の手順を実行します。

手順

高 CPU しきい値の値とモニタリング期間を設定します。

snmp cpu threshold rising *threshold_value monitoring_period*

例：

```
ciscoasa(config)# snmp cpu threshold rising 75% 30 minutes
```

CPU 使用率のしきい値およびモニタリング期間をクリアするには、このコマンドの **no** 形式を使用します。**snmp cpu threshold rising** コマンドが設定されていない場合、上限しきい値レベルのデフォルトは 70 % を超え、クリティカルしきい値レベルのデフォルトは 95 % を超えます。デフォルトのモニタリング期間は 1 分に設定されます。

CPU のクリティカルしきい値レベルは設定できません。この値は 95 % に固定されています。高 CPU しきい値の有効値の範囲は 10 ～ 94 % です。モニタリング期間の有効値は 1～60 分です。

物理インターフェイスのしきい値の設定

物理インターフェイスのしきい値を設定するには、次の手順を実行します。

手順

SNMP 物理インターフェイスのしきい値を設定します。

snmp interface threshold *threshold_value*

例：

```
ciscoasa(config)# snmp interface threshold 75%
```

SNMP 物理インターフェイスのしきい値をクリアするには、このコマンドの **no** 形式を使用します。しきい値は、インターフェイス帯域幅利用率の割合として定義されます。有効なしきい値の範囲は 30～99 % です。デフォルト値は 70 % です。

snmp interface threshold コマンドを使用できるのは、管理コンテキストのみです。

物理インターフェイスの使用状況はシングル モードおよびマルチ モードでモニタされ、システム コンテキストの物理インターフェイスのトラップは管理コンテキストを通して送信されます。物理インターフェイスだけがしきい値の使用状況を計算するために使用されます。

（注） このコマンドは、Catalyst 6500 スイッチ/7600 ルータ向け ASA サービス モジュールではサポートされていません。

SNMP バージョン 1 または 2c のパラメータの設定

SNMP バージョン 1 または 2c のパラメータを設定するには、次の手順を実行します。

手順

ステップ 1 SNMP通知の受信者を指定し、トラップの送信元のインターフェイスを指定し、ASAに接続できるNMSまたはSNMPマネージャの名前およびIPアドレスを指定します。

snmp-server host{*interface hostname* | *ip_address*} [**trap**| **poll**] [**community** *community-string*] [**version** {**1 2c**| *username*}] [**udp-port** *port*]

例：

trap キーワードは、NMS をトラップの受信だけに制限します。**poll** キーワードは、NMS を要求の送信（ポーリング）だけに制限します。デフォルトでは、SNMP トラップはイネーブルになっています。デフォルトでは、UDP ポートは 162 です。コミュニティ ストリングは、ASA と NMS の間の共有秘密キーです。キーは、大文字と小文字が区別される最大 32 文字の英数字の値です。スペースは使用できません。デフォルトのコミュニティ ストリングは public です。ASA では、このキーを使用して着信 SNMP 要求が有効かどうかを判別します。たとえば、コミュニティ ストリングを使用してサイトを指定し、同じストリングを使ってASAと管理ステーションを設定できます。ASA は指定されたストリングを使用し、無効なコミュニティ ストリングを使用した要求には応答しません。暗号化されたコミュニティ ストリングを使用した後は、暗号化された形式だけがすべてのシステム（CLI、ASDM、CSM など）に表示されます。クリア テキストのパスワードは表示されません。暗号化されたコミュニティ ストリングは常に ASA によって生成されます。通常は、クリア テキストの形式で入力します。

（注） ASA ソフトウェアをバージョン 8.3(1) から下のバージョンにダウングレードし、暗号化されたパスワードを設定した場合、まず **no key config-key password encryption** コマンドを使用して暗号化されたパスワードをクリアテキストに戻してから結果を保存する必要があります。

トラップを受信するには、**snmp-server host** コマンドを追加した後に、ASA で設定されたクレデンシャルと同じクレデンシャルを使用して NMS でユーザを確実に設定するようにします。

ステップ 2 SNMP バージョン 1 または 2c だけで使用するコミュニティ ストリングを設定します。

snmp-server community *community-string*

例：

```
ciscoasa(config)# snmp-server community onceuponatime
```

ステップ 3 SNMP サーバの場所または担当者情報を設定します。

snmp-server [**contact** | **location**] *text*

例：

```
ciscoasa(config)# snmp-server location building 42
ciscoasa(config)# snmp-server contact EmployeeA
```

text 引数には、担当者または ASA システム管理者の名前を指定します。名前は大文字と小文字が区別され、最大 127 文字です。スペースを使用できますが、複数のスペースを入力しても 1 つのスペースになります。

ステップ 4 SNMP 要求のリスニング ポートを設定します。

snmp-server listen-port *lport*

例：

```
ciscoasa(config)# snmp-server lport 192
```

lport 引数には、着信要求を受け取るポートを指定します。デフォルトのリスニング ポートは 161 です。**snmp-server listen-port** コマンドは管理コンテキストでのみ使用でき、システム コンテキストでは使用できません。現在使用中のポートで **snmp-server listen-port** コマンドを設定すると、次のメッセージが表示されます。

```
The UDP port port is in use by another feature. SNMP requests to the device
will fail until the snmp-server listen-port command is configured to use a different
port.
```

既存の SNMP スレッドはポートが使用可能になるまで 60 秒ごとにポーリングを続け、ポートがまだ使用中の場合は syslog メッセージ %ASA-1-212001 を発行します。

SNMP バージョン 3 のパラメータの設定

SNMP バージョン 3 のパラメータを設定するには、次の手順を実行します。

手順

ステップ 1 SNMP バージョン 3 だけで使用する、新しい SNMP グループを指定します。

snmp-server group *group-name***v3** [**auth** | **noauth** | **priv**]

例：

```
ciscoasa(config)# snmp-server group testgroup1 v3 auth
```

コミュニティ ストリングが設定されている場合は、コミュニティ ストリングに一致する名前を持つ 2 つの追加グループが自動生成されます。1 つはバージョン 1 のセキュリティ モデルのグループであり、もう 1 つはバージョン 2 のセキュリティ モデルのグループです。**auth** キーワードは、パケット認証を有効にします。**noauth** キーワードは、パケット認証や暗号化が使用されていないことを示します。**priv** キーワードは、パケット暗号化と認証を有効にします。**auth** または **priv** キーワードには、デフォルト値がありません。

ステップ 2 SNMP バージョン 3 だけで使用する、SNMP グループの新しいユーザを設定します。

snmp-server user*username group-name* {**v3** [**engineID** *engineID*] [**encrypted**]] [**auth** {**md5** | **sha**]} *auth-password* [**priv**] [**des** | **3des** | **aes**] [**128** | **192**| **256**] *priv-password*

例：

```
ciscoasa(config)# snmp-server user testuser1 testgroup1 v3 auth md5 testpassword
aes 128 mypassword
ciscoasa(config)# snmp-server user testuser1 public v3 encrypted auth md5
00:11:22:33:44:55:66:77:88:99:AA:BB:CC:DD:EE:FF
```

username 引数は、SNMP エージェントに属するホスト上のユーザの名前です。group-name 引数は、ユーザが属するグループの名前です。**v3** キーワードは、SNMP バージョン 3 のセキュリティ モデルを使用することを指定し、**encrypted**、**priv**、および **auth** キーワードの使用を有効化します。**engineID** キーワードはオプションで、ユーザの認証と暗号化の情報をローカライズするために使用される ASA のエンジン ID を指定します。engineID 引数には、有効な ASA エンジン ID を指定する必要があります。**encrypted** キーワードは、暗号化された形式でパスワードを指定します。暗号化されたパスワードは、16 進数の形式である必要があります。**auth** キーワードは、使用される認証レベル（**md5** または **sha**）を指定します。**priv** キーワードは、暗号化レベルを指定します。**auth** または **priv** キーワードのデフォルト値はありません。また、デフォルト パスワードもありません。暗号化アルゴリズムには、**des**、**3des**、または **aes** キーワードを指定できます。使用する AES 暗号化アルゴリズムのバージョンとして、**128**、**192**、**256** のいずれかを指定することもできます。auth-password 引数は、認証ユーザ パスワードを指定します。priv-password 引数は、暗号化ユーザ パスワードを指定します。

（注） パスワードを忘れた場合は、回復できないため、ユーザを再設定する必要があります。プレーンテキストのパスワードまたはローカライズされたダイジェストを指定できます。ローカライズされたダイジェストは、ユーザに対して選択した認証アルゴリズム（MD5 または SHA にすることができます）に一致する必要があります。ユーザ設定がコンソールに表示される場合、またはファイル（スタートアップ コンフィギュレーション ファイルなど）に書き込まれる場合、ローカライズされた認証ダイジェストとプライバシー ダイジェストが常にプレーン テキストのパスワードの代わりに表示されます（2 番目の例を参照してください）。パスワードの最小長は、英数字 1 文字です。ただし、セキュリティを確保するために 8 文字以上の英数字を使用することを推奨します。

クラスタリング環境では、クラスタ化されたそれぞれの ASA について手動で SNMPv3 ユーザを更新する必要があります。これを行うには、マスター ユニットに対する **snmp-server user** *username group-name* **v3** コマンドを入力し、ローカライズされていない形式で *priv-password* オプションおよび *auth-password* オプションを指定します。

クラスタリングの複製または設定時に、SNMPv3 ユーザ コマンドが複製されないことを通知するエラー メッセージが表示されます。この場合、SNMPv3 ユーザおよびグループのコマンドをスレーブの ASA に対して個別に設定します。また、複製の実行時に既存の SNMPv3 ユーザおよびグループのコマンドがクリアされない場合にもメッセージが表示されます。この場合は、クラスタのすべてのスレーブに対して SNMPv3 ユーザおよびグループのコマンドを入力します。次に例を示します。

マスター ユニットに対するコマンドで入力したキーがすでにローカライズされている場合：

```
ciscoasa(config)# snmp-server user defe abc v3 encrypted auth sha
c0:e7:08:50:47:eb:2e:e4:3f:a3:bc:45:f6:dd:c3:46:25:a0:22:9a
priv aes 256 cf:ad:85:5b:e9:14:26:ae:8f:92:51:12:91:16:a3:ed:de:91:6b:f7:
f6:86:cf:18:c0:f0:47:d6:94:e5:da:01
ERROR: This command cannot be replicated because it contains localized keys.
```

クラスタ複製時のスレーブ ユニットの場合（**snmp-server user** コマンドが設定にある場合にのみ表示されます）：

```
ciscoasa(cfg-cluster)#
Detected Cluster Master.
Beginning configuration replication from Master.
WARNING: existing snmp-server user CLI will not be cleared.
```

ステップ 3 SNMP通知の受信者を指定します。トラップの送信元となるインターフェイスを指定します。ASA に接続できる NMS または SNMP マネージャの名前と IP アドレスを指定します。

snmp-server host *interface* {*hostname* | *ip_address*} [**trap**| **poll**] [**community** *community-string*] [**version** {**1** | **2c** | **3** *username*}] [**udp-port** *port*]

例：

trap キーワードは、NMS をトラップの受信だけに制限します。**poll** キーワードは、NMS を要求の送信（ポーリング）だけに制限します。デフォルトでは、SNMP トラップはイネーブルになっています。デフォルトでは、UDP ポートは 162 です。コミュニティ ストリングは、ASA と NMS の間の共有秘密キーです。キーは、大文字と小文字が区別される最大 32 文字の英数字の値です。スペースは使用できません。デフォルト コミュニティ ストリングは public です。ASA は、このキーを使用して、着信 SNMP 要求が有効かどうかを判断します。たとえば、コミュニティストリングを使用してサイトを指定すると、ASA と NMS を同じストリングを使用して設定できます。ASA は指定されたストリングを使用し、無効なコミュニティ ストリングを使用した要求には応答しません。暗号化されたコミュニティ ストリングを使用した後は、暗号化された形式だけがすべてのシステム（CLI、ASDM、CSM など）に表示されます。クリアテキストのパスワードは表示されません。暗号化されたコミュニティ ストリングは常に ASA によって生成されます。通常は、クリア テキストの形式で入力します。

（注） ASA ソフトウェアをバージョン 8.3(1) から下のバージョンにダウングレードし、暗号化されたパスワードを設定した場合、まず **no key config-key password encryption** コマンドを使用して暗号化されたパスワードをクリアテキストに戻してから結果を保存する必要があります。

version キーワードは、SNMP トラップのバージョンを指定します。ASA では、SNMP 要求（ポーリング）に基づくフィルタリングはサポートされません。

SNMP バージョン 3 のホストを ASA に設定する場合は、ユーザをそのホストに関連付ける必要があります。

トラップを受信するには、**snmp-server host** コマンドを追加した後に、ASA で設定されたクレデンシャルと同じクレデンシャルを使用して NMS でユーザを確実に設定するようにします。

ステップ 4 SNMP サーバの場所または担当者情報を設定します。

snmp-server [**contact** | **location**] *text*

例：

```
ciscoasa(config)# snmp-server location building 42
ciscoasa(config)# snmp-server contact EmployeeA
```

*text*引数には、担当者またはASAシステム管理者の名前を指定します。名前は大文字と小文字が区別され、最大 127 文字です。スペースを使用できますが、複数のスペースを入力しても 1 つのスペースになります。

ステップ 5 SNMP 要求のリスニング ポートを設定します。

snmp-server listen-port *lport*

例：

```
ciscoasa(config)# snmp-server lport 192
```

lport 引数には、着信要求を受け取るポートを指定します。デフォルトのリスニング ポートは 161 です。**snmp-server listen-port** コマンドは管理コンテキストでのみ使用でき、システム コンテキストでは使用できません。現在使用中のポートで **snmp-server listen-port** コマンドを設定すると、次のメッセージが表示されます。

```
The UDP port port is in use by another feature. SNMP requests to the device
will fail until the snmp-server listen-port command is configured to use a different
port.
```

既存の SNMP スレッドはポートが使用可能になるまで 60 秒ごとにポーリングを続け、ポートがまだ使用中の場合は syslog メッセージ %ASA-1-212001 を発行します。

ユーザのグループの設定

指定したユーザのグループからなる SNMP ユーザ リストを設定するには、次の手順を実行します。

手順

SNMP ユーザ リストを設定します。

snmp-server user-list *list_name* **username** *user_name*

例：

```
ciscoasa(config)# snmp-server user-list engineering username user1
```

*listname*引数には、ユーザ リストの名前を指定します。最大33 文字まで指定できます。**username** *user_name* のキーワードと引数のペアで、ユーザ リストに設定するユーザを指定します。ユー

ザ リストのユーザは、**snmp-server user** *username* コマンドで設定します。このコマンドは、SNMP バージョン 3 を使用している場合にのみ使用できます。ユーザ リストには複数のユーザを含める必要があり、ホスト名または IP アドレスの範囲に関連付けることができます。

ネットワーク オブジェクトへのユーザの関連付け

ユーザ リストの単一のユーザまたはユーザのグループをネットワーク オブジェクトに関連付けるには、次の手順を実行します。

手順

ユーザ リストの単一のユーザまたはユーザのグループをネットワーク オブジェクトに関連付けます。

snmp-server host-group *net_obj_name* [**trap**| **poll**] [**community** *community-string*] [**version** {**1** | **2c** | **3** {*username* | **user-list** *list_name*}] [**udp-port** *port*]

例：

```
ciscoasa(config)# snmp-server host-group inside net1 trap community public version 1
ciscoasa(config)# snmp-server host-group inside net1 trap community public version 2c
ciscoasa(config)# snmp-server host-group inside net1 trap version 3 user1
ciscoasa(config)# snmp-server host-group inside net1 trap version 3 user-list engineering
```

net_obj_name 引数は、ユーザまたはユーザ グループを関連付けるインターフェイスのネットワーク オブジェクト名を指定します。**trap** キーワードは、トラップの送信のみが可能であり、このホストはブラウズ（ポーリング）できないことを指定します。**poll** キーワードは、ホストでブラウズ（ポーリング）が可能であるものの、トラップの送信はできないことを指定します。**community** キーワードは、NMS からの要求に対して、または NMS に送信されるトラップを生成するときに、デフォルト以外のストリングが必要であることを指定します。このキーワードは、SNMP バージョン 1 または 2c でのみ使用できます。*community-string* 引数には、通知または NMS からの要求で送信されるコミュニティ ストリングを指定します。コミュニティ ストリングはパスワードのような役割を果たします。このコミュニティ ストリングは最大 32 文字です。**version** キーワードは、トラップの送信に使用する SNMP 通知のバージョン（バージョン 1、2c、または 3）を設定します。*username* 引数には、SNMP バージョン 3 を使用する場合にユーザの名前を指定します。**user-list** キーワードと *list_name* 引数で、ユーザ リストの名前を指定します。**udp-port** *port* のキーワードと引数の組み合わせは、NMS ホストへの SNMP トラップの送信にデフォルト以外のポートを使用する場合に、NMS ホストの UDP ポート番号を設定します。デフォルトの UDP ポートは 162 です。デフォルトのバージョンは 1 です。SNMP トラップはデフォルトでイネーブルになっています。

SNMP モニタリング

次の SNMP モニタリング用のコマンドを参照してください。

- **show running-config snmp-server** [**default**]

  すべての SNMP サーバのコンフィギュレーション情報を表示します。

- **show running-config snmp-server group**

  SNMP グループのコンフィギュレーション設定を表示します。

- **show running-config snmp-server host**

  リモート ホストに送信されるメッセージと通知を制御するために SNMP によって使用されているコンフィギュレーション設定を表示します。

- **show running-config snmp-server host-group**

  SNMP ホスト グループのコンフィギュレーションを表示します。

- **show running-config snmp-server user**

  SNMP ユーザベースのコンフィギュレーション設定を表示します。

- **show running-config snmp-server user-list**

  SNMP ユーザ リストのコンフィギュレーションを表示します。

- **show snmp-server engineid**

  設定されている SNMP エンジンの ID を表示します。

- **show snmp-server group**

  設定されている SNMP グループの名前を表示します。コミュニティ ストリングがすでに設定されている場合、デフォルトでは2つの別のグループが出力に表示されます。この動作は通常のものです。

- **show snmp-server statistics**

  SNMPサーバの設定済み特性を表示します。すべてのSNMPカウンタをゼロにリセットするには、**clear snmp-server statistics** コマンドを使用します。

- **show snmp-server user**

  ユーザの設定済み特性を表示します。

例

次の例は、SNMP サーバの統計情報を表示する方法を示しています。

```
ciscoasa(config)# show snmp-server statistics
0 SNMP packets input
    0 Bad SNMP version errors
    0 Unknown community name
```

```
    0 Illegal operation for community name supplied
    0 Encoding errors
    0 Number of requested variables
    0 Number of altered variables
    0 Get-request PDUs
    0 Get-next PDUs
    0 Get-bulk PDUs
    0 Set-request PDUs (Not supported)
0 SNMP packets output
    0 Too big errors (Maximum packet size 512)
    0 No such name errors
    0 Bad values errors
    0 General errors
    0 Response PDUs
    0 Trap PDUs
```

次の例は、SNMP サーバの実行コンフィギュレーションを表示する方法を示しています。

```
ciscoasa(config)# show running-config snmp-server
no snmp-server location
no snmp-server contact
snmp-server enable traps snmp authentication linkup linkdown coldstart
```

SNMP の例

次の項では、すべての SNMP バージョンの参考として使用できる例を示します。

SNMP バージョン 1 および 2c

次の例は、どのホストにも SNMP syslog 要求を送信せずに、ASA が内部インターフェイスでホスト 192.0.2.5 からの SNMP 要求を受信する方法を示しています。

```
ciscoasa(config)# snmp-server host 192.0.2.5
ciscoasa(config)# snmp-server location building 42
ciscoasa(config)# snmp-server contact EmployeeA
ciscoasa(config)# snmp-server community ohwhatakeyisthee
```

SNMP バージョン 3

次の例は、ASA が SNMP バージョン 3 のセキュリティ モデルを使用して SNMP 要求を受信する方法を示しています。このモデルでは、グループ、ユーザ、ホストという一定の順序で設定する必要があります。

```
ciscoasa(config)# snmp-server group v3 vpn-group priv
ciscoasa(config)# snmp-server user admin vpn group v3 auth sha letmein priv 3des cisco123
ciscoasa(config)# snmp-server host mgmt 10.0.0.1 version 3 priv admin
```

SNMP の履歴

表 *55 : SNMP* の履歴

機能名	バージョン	説明
SNMP バージョン 1 および 2c	7.0(1)	クリア テキスト コミュニティ ストリングを使用した SNMP サーバと SNMP エージェント間のデータ送信によって、ASA ネットワークモニタリングとイベント情報を提供します。
SNMP バージョン 3	8.2(1)	3DES または AES 暗号化、およびサポートされているセキュリティ モデルの中で最もセキュアな形式である SNMP バージョン 3 のサポートを提供します。このバージョンでは、USM を使用して、ユーザ、グループ、ホスト、および認証の特性を設定できます。さらに、このバージョンでは、エージェントと MIB オブジェクトへのアクセス コントロールが許可され、追加の MIB サポートが含まれます。 次のコマンドが導入または変更されました。**show snmp-server engineid**、**show snmp-server group**、**show snmp-server user**、**snmp-server group**, **snmp-server user**、**snmp-server host**
パスワードの暗号化	8.3(1)	パスワードの暗号化がサポートされます。 **snmp-server community**、**snmp-server host** コマンドが変更されました。
SNMP トラップと MIB	8.4(1)	追加のキーワードとして、**connection-limit-reached**、**cpu threshold rising**、**entity cpu-temperature**、**entity fan-failure**、**entity power-supply**、**ikev2 stop | start**、**interface-threshold**、**memory-threshold**、**nat packet-discard**、**warmstart** をサポートします。 entPhysicalTable によって、センサー、ファン、電源、および関連コンポーネントのエントリがレポートされます。 追加の MIB として、CISCO-ENTITY-SENSOR-EXT-MIB、CISCO-ENTITY-FRU-CONTROL-MIB、CISCO-PROCESS-MIB、CISCO-ENHANCED-MEMPOOL-MIB、CISCO-L4L7MODULE-RESOURCE-LIMIT-MIB、DISMAN-EVENT-MIB、DISMAN-EXPRESSION-MIB、ENTITY-SENSOR-MIB、NAT-MIB をサポートします。 さらに ceSensorExtThresholdNotification、clrResourceLimitReached、cpmCPURisingThreshold、mteTriggerFired、natPacketDiscard、warmStart トラップをサポートしています。 **snmp cpu threshold rising**、**snmp interface threshold**、**snmp-server enable traps** コマンドが導入または変更されました。
IF-MIB ifAlias OID のサポート	8.2(5)/8.4(2)	ASA は、ifAlias OID をサポートするようになりました。IF-MIB をブラウズする際、fAlias OID はインターフェイスの記述に設定済みの値に設定されます。

機能名	バージョン	説明
ASA サービス モジュール（ASASM）	8.5(1)	ASASM は、次を除く 8.4(1) にあるすべての MIB およびトラップをサポートします。 8.5(1) のサポートされていない MIB： • CISCO-ENTITY-SENSOR-EXT-MIB（entPhySensorTable グループのオブジェクトだけがサポートされます）。 • ENTITY-SENSOR-MIB（entPhySensorTable グループのオブジェクトだけがサポートされます）。 • DISMAN-EXPRESSION-MIB（expExpressionTable、expObjectTable、および expValueTable グループのオブジェクトだけがサポートされます）。 8.5(1) のサポートされていないトラップ： • ceSensorExtThresholdNotification（CISCO-ENTITY-SENSOR-EXT-MIB）。このトラップは、電源障害、ファン障害および高CPU温度のイベントだけに使用されます。 • InterfacesBandwidthUtilization。
SNMP トラップ	8.6(1)	ASA 5512-X、5515-X、5525-X、5545-X、および 5555-X の追加のキーワードとして、**entity power-supply-presence**、**entity power-supply-failure**、**entity chassis-temperature**、**entity chassis-fan-failure, entity power-supply-temperature** をサポートします。 次のコマンドが変更されました。**snmp-server enable traps**。
VPN-related MIB	9.0(1)	CISCO-IPSEC-FLOW-MONITOR-MIB.my MIB の更新バージョンが、次世代の暗号化機能をサポートするために実装されました。 ASASM では、次の MIB が有効になりました。 • ALTIGA-GLOBAL-REG.my • ALTIGA-LBSSF-STATS-MIB.my • ALTIGA-MIB.my • ALTIGA-SSL-STATS-MIB.my • CISCO-IPSEC-FLOW-MONITOR-MIB.my • CISCO-REMOTE-ACCESS-MONITOR-MIB.my
Cisco TrustSec MIB	9.0(1)	CISCO-TRUSTSEC-SXP-MIB のサポートが追加されました。
SNMP OID	9.1(1)	ASA 5512-X、5515-X、5525-X、5545-X、および 5555-X をサポートするために 5 つの新しい SNMP 物理ベンダー タイプ OID が追加されました。

機能名	バージョン	説明
NAT MIB	9.1(2)	cnatAddrBindNumberOfEntries および cnatAddrBindSessionCount OID が、xlate_count および max_xlate_count エントリをサポートするようになりました。これは、**show xlate count** コマンドを使用したポーリングの許可と同等です。
SNMP のホスト、ホスト グループ、ユーザ リスト	9.1(5)	最大 4000 個までホストを追加できるようになりました。サポートされるアクティブなポーリング先の数は 128 個です。ホスト グループとして追加する個々のホストを示すためにネットワーク オブジェクトを指定できます。1 つのホストに複数のユーザを関連付けることができます。 **snmp-server host-group**、**snmp-server user-list**、**show running-config snmp-server**、**clear configure snmp-server** の各コマンドが導入または変更されました。
SNMP メッセージのサイズ	9.2(1)	SNMP で送信できるメッセージのサイズが 1472 バイトまでに増えました。
SNMP の MIB および OID	9.2(1)	ASA は、cpmCPUTotal5minRev OID をサポートするようになりました。 SNMP の sysObjectID OID および entPhysicalVendorType OID に、新しい製品として ASAv が追加されました。 新しい ASAv プラットフォームをサポートするよう、CISCO-PRODUCTS-MIB および CISCO-ENTITY-VENDORTYPE-OID-MIB が更新されました。 VPN 共有ライセンスの使用状況をモニタするための新しい SNMP MIB が追加されました。
SNMP の MIB および OID	9.3(1)	ASASM 用に CISCO-REMOTE-ACCESS-MONITOR-MIB（OID 1.3.6.1.4.1.9.9.392）のサポートが追加されました。
SNMP の MIB およびトラップ	9.3(2)	ASA 5506-X をサポートするように CISCO-PRODUCTS-MIB および CISCO-ENTITY-VENDORTYPE-OID-MIB が更新されました。 SNMP の sysObjectID OID および entPhysicalVendorType OID のテーブルに、新しい製品として ASA 5506-X が追加されました。 ASA で CISCO-CONFIG-MAN-MIB がサポートされるようになりました。以下が可能です。 • 特定のコンフィギュレーションについて入力されたコマンドを確認する。 • 実行コンフィギュレーションに変更が発生したときに NMS に通知する。 • 実行コンフィギュレーションが最後に変更または保存されたときのタイム スタンプを追跡する。 • 端末の詳細やコマンドのソースなど、コマンドに対するその他の変更を追跡する。 次のコマンドが変更されました。**snmp-server enable traps**。

機能名	バージョン	説明
SNMP の MIB およびトラップ	9.4(1)	SNMP の sysObjectID OID および entPhysicalVendorType OID のテーブルに、新しい製品として ASA 5506W-X、ASA 5506H-X、ASA 5508-X、および ASA 5516-X が追加されました。
コンテキストごとに無制限の SNMP サーバ トラップ ホスト	9.4(1)	ASA は、コンテキストごとに無制限の SNMP サーバ トラップ ホストをサポートします。**show snmp-server host** コマンドの出力には ASA をポーリングしているアクティブなホストと、静的に設定されたホストのみが表示されます。 **show snmp-server host** コマンドが変更されました。
ISA 3000 のサポートが追加されました。	9.4(1.225)	ISA 3000 製品ファミリーで SNMP がサポートされました。このプラットフォームに新しい OID が追加されました。**snmp-server enable traps entity** コマンドが変更され、新しい変数 *l1-bypass-status* が追加されました。これにより、ハードウェアのバイパス状態の変更が可能になりました。 次のコマンドが変更されました。**snmp-server enable traps entity**
CISCO-ENHANCED-MEMPOOL-MIB の cempMemPoolTable のサポート	9.6(1)	CISCO-ENHANCED-MEMPOOL-MIB の cempMemPoolTable がサポートされました。これは、管理型システムのすべての物理エンティティのメモリプール モニタリング エントリのテーブルです。 （注） CISCO-ENHANCED-MEMPOOL-MIB は 64 ビットのカウンタを使用して、プラットフォーム上の 4 GB 以上のメモリのレポーティングをサポートします。
Precision Time Protocol（PTP）の E2E トランスペアレント クロック モード MIB のサポート	9.7(1)	E2E トランスペアレント クロック モードに対応する MIB がサポートされます。 （注） SNMP の bulkget、getnext、walk 機能のみがサポートされています。

機能名	バージョン	説明
SNMP over IPv6	9.9(2)	ASA は、IPv6 経由での SNMP サーバとの通信、IPv6 経由でのクエリとトラップの実行許可、既存の MIB に対する IPv6 アドレスのサポートなど、SNMP over IPv6 をサポートするようになりました。RFC 8096 で説明されているように、次の新しい SNMP IPv6 MIB オブジェクトが追加されました。 • ipv6InterfaceTable（OID：1.3.6.1.2.1.4.30）：インターフェイスごとの IPv6 固有の情報が含まれています。 • ipAddressPrefixTable（OID：1.3.6.1.2.1.4.32）：このエンティティによって学習されたすべてのプレフィックスが含まれています。 • ipAddressTable（OID：1.3.6.1.2.1.4.34）：エンティティのインターフェイスに関連するアドレッシング情報が含まれています。 • ipNetToPhysicalTable（OID：1.3.6.1.2.1.4.35）：IP アドレスから物理アドレスへのマッピングが含まれています。 新規または変更されたコマンド：**snmp-server host** （注） **snmp-server host-group** コマンドは IPv6 をサポートしていません。
SNMP ウォーク操作中の空きメモリおよび使用済みメモリの統計情報の結果を有効または無効にするためのサポート	9.10(1)	CPU リソースが過剰に使用されないようにするには、SNMP ウォーク操作によって収集された空きメモリと使用済みメモリの統計情報のクエリを有効または無効にすることができます。 新規/変更されたコマンド：**snmp-server enable oid**
SNMP ウォーク操作中の空きメモリおよび使用済みメモリの統計情報の結果を有効または無効にするためのサポート	9.12(1)	CPU リソースが過剰に使用されないようにするには、SNMP ウォーク操作によって収集された空きメモリと使用済みメモリの統計情報のクエリを有効または無効にすることができます。 変更されたコマンドはありません。

第 40 章

Anonymous Reporting および Smart Call Home

この章では、Anonymous Reporting および Smart Call Home サービスを設定する方法について説明します。

Anonymous Reporting について

Anonymous Reporting をイネーブルにして、Cisco ASA プラットフォームを強化することができます。Anonymous Reporting により、エラーおよびヘルスに関する最小限の情報をデバイスからシスコに安全に送信できます。この機能をイネーブルにした場合、お客様のアイデンティティは匿名のままとなり、識別情報は送信されません。

Anonymous Reporting をイネーブルにすると、トラスト ポイントが作成され、証明書がインストールされます。CA 証明書は、ASA でメッセージを安全に送信できるように、Smart Call Home Web サーバ上のサーバ証明書を検証して、HTTPS セッションを形成するために必要です。ソフトウェアに事前定義済みの証明書が、シスコによってインポートされます。Anonymous Reporting をイネーブルにする場合は、ハードコードされたトラスト ポイント名の _SmartCallHome_ServerCA で証明書が ASA にインストールされます。Anonymous Reporting をイネーブルにすると、このトラスト ポイントが作成され、適切な証明書がインストールされて、このアクションに関するメッセージが表示されます。これで、証明書が設定の中に存在するようになります。

Anonymous Reporting をイネーブルにしたときに、適切な証明書がすでに設定に存在する場合、トラスト ポイントは作成されず、証明書はインストールされません。

（注） Anonymous Reporting をイネーブルにすると、指定されたデータをシスコまたはシスコの代わりに運用するベンダー（米国以外の国を含む）に転送することに同意することになります。シスコでは、すべてのお客様のプライバシーを保護しています。シスコの個人情報の取り扱いに関する詳細については、次の URL にあるシスコのプライバシー声明を参照してください。
http://www.cisco.com/web/siteassets/legal/privacy.html

DNS 要件

ASA が Cisco Smart Call Home サーバに到達してシスコにメッセージを送信できるように DNS サーバを正しく設定する必要があります。ASA をプライベート ネットワークに配置し、パブリック ネットワークにはアクセスできないようにすることが可能なため、シスコでは DNS 設定を検証し、必要な場合には次の手順を実行して、ユーザの代わりにこれを設定します。

1. 設定されているすべての DNS サーバに対して DNS ルックアップを実行します。
2. 最もセキュリティレベルの高いインターフェイスで DHCPINFORM メッセージを送信して、DHCP サーバから DNS サーバを取得します。
3. ルックアップにシスコの DNS サーバを使用します。
4. tools.cisco.com に対してランダムに静的 IP アドレスを使用します。

これらの作業は、現在の設定を変更せずに実行されます。（たとえば、DHCPから学習された DNS サーバは設定には追加されません）。

設定されている DNS サーバがなく、ASA が Cisco Smart Call Home サーバに到達できない場合は、各 Smart Call Home メッセージに対して、重大度「warning」の syslog メッセージが生成されます。これは、DNS を適切に設定するようお願いするためです。

syslog メッセージについては、『syslog メッセージ ガイド』を参照してください。

Smart Call Home の概要

完全に設定が終わると、Smart Call Home は設置場所での問題を検出し、多くの場合はそのような問題があることにユーザが気付く前に、シスコにレポートを返すか、別のユーザ定義のチャネル（ユーザ宛の電子メールまたはユーザに直接など）を使用してレポートを返します。シスコでは、これらの問題の重大度に応じて次のサービスを提供することにより、システム コンフィギュレーションの問題、製品ライフサイクル終了通知の発表、セキュリティ勧告問題などに対応します。

- 継続的モニタリング、リアルタイムの予防的なアラート、および詳細な診断により、問題を迅速に識別する。
- サービス要求が開かれ、すべての診断データが添付された Smart Call Home 通知を使用して、潜在的な問題をユーザに認識させる。

- Cisco TAC の専門家に自動的に直接アクセスすることにより、重大な問題を迅速に解決する。
- トラブルシューティングに必要な時間を短縮することにより、スタッフ リソースを効率よく使用する。
- Cisco TAC へのサービス リクエストを自動的に生成し（サービス契約がある場合）、適切なサポート チームに提出する。問題解決の時間を短縮する、詳細な診断情報を提供します。

Smart Call Home ポータルを使用すると必要な情報に迅速にアクセスできるため、以下の事項が実現されます。

- すべての Smart Call Home メッセージ、診断、および推奨事項を一箇所で確認する。
- サービス リクエスト ステータスを確認する。
- すべての Smart Call Home 対応デバイスに関する最新のインベントリ情報およびコンフィギュレーション情報を表示する。

アラート グループへの登録

アラート グループは、ASA でサポートされる Smart Call Home アラートの定義済みサブセットです。Smart Call Home アラートにはさまざまなタイプがあり、タイプに応じてさまざまなアラート グループにグループ化されます。各アラート グループは、特定の CLI の出力を報告します。サポートされる Smart Call Home アラート グループは次のとおりです。

- syslog
- diagnostic
- 環境
- インベントリ
- 設定
- 脅威
- snapshot
- telemetry
- test

アラート グループの属性

アラート グループには次の属性があります。

- イベントはまず 1 個のアラート グループに登録します。
- 1 個のグループを、複数のイベントに関連付けることができます。

- 個々のアラート グループに登録できます。
- 個々のアラート グループをイネーブルまたはディセーブルにできます。デフォルト設定では、すべてのアラート グループに対してイネーブルです。
- 診断および環境アラート グループは定期的なメッセージのサブスクリプションをサポートします。
- syslog アラート グループは、メッセージ ID ベースのサブスクリプションをサポートします。
- 環境アラート グループの CPU とメモリの使用率のしきい値を設定できます。特定のパラメータが定義済みしきい値を超えると、メッセージが送信されます。しきい値のほとんどは、プラットフォームによって決まっており、変更できません。
- 指定する CLI 出力を送信するようスナップショット アラート グループを設定します。

アラート グループによって Cisco に送信されるメッセージ

メッセージは、定期的に、および ASA がリロードされるたびにシスコに送信されます。これらのメッセージは、アラート グループによって分類されます。

インベントリ アラートは、次のコマンドによる出力で構成されます。

- **show version**：ASA ソフトウェア バージョン、ハードウェア構成、ライセンス キー、および関連するデバイスの稼働時間を表示します。
- **show inventory**—ネットワーキング デバイスにインストールされている各 Cisco 製品のインベントリ情報を取得および表示します。各製品は UDI と呼ばれる一意のデバイス情報で識別されます。UDI は、製品 ID（PID）、バージョン ID（VID）、およびシリアル番号（SN）の 3 つの異なるデータ要素の組み合わせです。
- **show failover state**：フェールオーバー ペアの両方のユニットのフェールオーバー状態を表示します。表示される情報は、ユニットのプライマリまたはセカンダリ ステータス、ユニットのアクティブ/スタンバイ ステータス、最後にレポートされたフェールオーバーの理由などがあります。
- **show module**：ASA にインストールされているすべてのモジュールに関する情報を表示します。例：ASA 5585-X にインストールされている SSP に関する情報、ASA 5585-X にインストールされている IPS SSP に関する情報。
- **show environment**：シャーシ、ドライバ、ファン、および電源のハードウェア動作ステータスや、温度ステータス、電圧、CPU 使用率などの、ASA システム コンポーネントのシステム環境情報を表示します。

コンフィギュレーション アラートは、次のコマンドによる出力で構成されます。

- **show context**：割り当てられているインターフェイスと設定ファイルの URL、設定済みコンテキストの数を表示します。または、システム実行スペースで Anonymous Reporting を有効にしている場合には、すべてのコンテキストのリストを表示します。

- **show call-home registered-module status**：登録されたモジュールのステータスを表示します。システム コンフィギュレーション モードを使用している場合、コマンドによって、コンテキストごとではなく、デバイス全体に基づくシステムモジュールのステータスが表示されます。
- **show running-config**：ASA で現在実行されている設定を表示します。
- **show startup-config**：スタートアップ コンフィギュレーションを表示します。
- **show access-list | include elements**：アクセス リストのヒット カウンタおよびタイム スタンプ値を表示します。

診断アラートは、次のコマンドによる出力で構成されます。

- **show failover**：ユニットのフェールオーバー ステータスに関する情報を表示します。
- **show interface**：インターフェイス統計情報を表示します。
- **show cluster info**：クラスタ情報を表示します。
- **show cluster history**：クラスタの履歴を表示します。
- **show crashinfo**（切り捨て）：予期しないソフトウェアのリロード後に、デバイスは、変更されたクラッシュ情報ファイルをファイルのトレースバック セクションだけを含めて送信します。したがって、ファンクション コール、レジスタ値、およびスタック ダンプだけがシスコに報告されます。
- **show tech-support no-config**：テクニカル サポート アナリストによる診断に使用される情報を表示します。

環境アラートは、次のコマンドによる出力で構成されます。

- **show environment**：シャーシ、ドライバ、ファン、および電源のハードウェア動作ステータスや、温度ステータス、電圧、CPU 使用率などの、ASA システム コンポーネントのシステム環境情報を表示します。
- **show cpu usage**：CPU 使用率情報を表示します。
- **show memory detail**：空きおよび割り当て済みのシステム メモリの詳細情報を表示します。

脅威アラートは、次のコマンドによる出力で構成されます。

- **show threat-detection rate**：脅威検出統計情報を表示します。
- **show threat-detection shun**：現在排除されているホストを表示します。
- **show shun**：排除情報を表示します。
- **show dynamic-filter reports top**：ボットネット トラフィック フィルタによって分類された上位 10 のマルウェア サイト、ポート、および感染ホストのレポートを生成します。

スナップショット アラートは、次のコマンドによる出力で構成されます。

- **show conn count**：アクティブな接続の数を表示します。
- **show asp drop**：高速セキュリティ パスでドロップされたパケットまたは接続を表示します。

テレメトリ アラートは、次のコマンドによる出力で構成されます。

- **show perfmon detail**：ASA パフォーマンスの詳細を表示します。
- **show traffic**：インターフェイスの送受信アクティビティを表示します。
- **show conn count**：アクティブな接続の数を表示します。
- **show vpn-sessiondb summary**：VPN セッションのサマリー情報を表示します。
- **show vpn load-balancing**：VPN ロードバランシングの仮想クラスタ コンフィギュレーションの実行時統計情報を表示します。
- **show local-host | include interface**：ローカル ホストのネットワーク状態を表示します。
- **show memory**：物理メモリの最大量とオペレーティング システムで現在使用可能な空きメモリ量について要約を表示します。
- **show context**：割り当てられているインターフェイスと設定ファイルの URL、設定済みコンテキストの数を表示します。または、システム実行スペースで Anonymous Reporting を有効にしている場合には、すべてのコンテキストのリストを表示します。
- **show access-list | include elements**：アクセス リストのヒット カウンタおよびタイム スタンプ値を表示します。
- **show interface**：インターフェイス統計情報を表示します。
- **show threat-detection statistics protocol**：IP プロトコルの統計情報を表示します。
- **show phone-proxy media-sessions count**：電話プロキシによって保存されている、対応するメディア セッションの数を表示します。
- **show phone-proxy secure-phones count**：データベースに保存されているセキュア モード対応の電話機の数を表示します。
- **show route**：ルーティング テーブルを表示します。
- **show xlate count**：NAT セッション（xlates）の数を表示します。

メッセージ重大度しきい値

特定のアラート グループに宛先プロファイルを登録すると、メッセージの重大度に基づいてアラート グループ メッセージを送信するしきい値を設定できます。宛先プロファイルに指定したしきい値より低い値のメッセージは、宛先に送信されません。

次の表にメッセージの重大度と syslog の重大度のマッピングを示します。

表 *56 :* メッセージの重大度と *syslog* レベルのマッピング

レベル	メメッセージ重大度レベル	Syslog 重大度レベル	説明
9	Catastrophic	該当なし	ネットワーク全体に壊滅的な障害が発生しています。
8	Disaster	該当なし	ネットワークに重大な影響が及びます。
7	指定された CLI キーワードによって決定： **subscribe-to-alert-group** *name of alert group* **severity** *severity level*	0	緊急事態。システムが使用不可能な状態。
6	指定された CLI キーワードによって決定： **subscribe-to-alert-group** *name of alert group* **severity** *severity level*	1	アラート。クリティカルな状態。ただちに注意が必要。
5	指定された CLI キーワードによって決定： **subscribe-to-alert-group** *name of alert group* **severity** *severity level*	2	Critical 重大な状態。
4	指定された CLI キーワードによって決定： **subscribe-to-alert-group** *name of alert group* **severity** *severity level*	3	エラー。軽微な状態。
3	警告	4	警告状態。
2	通知	5	基本的な通知および情報メッセージです。他と関係しない、重要性の低い障害です。
1	標準	6	Information。通常のイベント。通常の状態に戻ることを意味します。
0	Debugging	7	デバッグ メッセージ（デフォルト設定）。

サブスクリプション プロファイル

サブスクリプションプロファイルを使用すると宛先受信者と関心のあるグループを関連付けることができます。プロファイルにあるサブスクライブされたグループに登録されているイベン

トがトリガーされると、イベントに関連付けられたメッセージが設定された受信者に送信されます。サブスクリプション プロファイルには次の属性があります。

- 複数のプロファイルを作成および設定できます。
- 1 個のプロファイルに複数の電子メールまたは HTTPS の受信者を設定できます。
- 1 個のプロファイルで、指定した重大度に複数のグループを登録できます。
- 1 個のプロファイルで、3 種類のメッセージ フォーマット（ショート テキスト、ロング テキスト、XML）をサポートします。
- 特定のプロファイルをイネーブルまたはディセーブルにできます。デフォルトでは、プロファイルはディセーブルです。
- 最大メッセージ サイズを指定できます。デフォルトは 3 MB です。

デフォルト プロファイル「Cisco TAC」が提供されました。デフォルト プロファイルには、事前定義されたモニタ対象グループ（診断、環境、インベントリ、コンフィギュレーション、テレメトリ）のセットと、事前定義された宛先電子メールおよび HTTPS URL があります。デフォルト プロファイルは、Smart Call Home を初めて設定するときに自動的に作成されます。宛先電子メールは callhome@cisco.com で、宛先 URL は https://tools.cisco.com/its/service/oddce/services/DDCEService です。

（注） デフォルト プロファイルの宛先電子メールと宛先 URL は変更できません。

コンフィギュレーション、インベントリ、テレメトリ、またはスナップショット アラート グループに宛先プロファイルを登録すると、アラート グループ メッセージを非同期に、または定期的に指定の時間に受信するよう選択できます。

次の表に、デフォルトのアラート グループと重大度のサブスクリプションおよび期間（該当する場合）のマッピングを示します。

表 *57*：アラート グループと重大度のサブスクリプションのマッピング

アラート グループ	重大度	Period
設定（Configuration）	Informational	Monthly
診断	Informational 以上	該当なし
環境	Notification 以上	該当なし
インベントリ	Informational	Monthly
Snapshot	Informational	該当なし
Syslog	同等の syslog	該当なし
Telemetry	Informational	Daily

アラート グループ	重大度	Period
Test	該当なし	該当なし
Threat	通知	該当なし

Anonymous Reporting および Smart Call Home のガイドライン

この項では、Anonymous Reporting と Smart Call Home を設定する前に考慮する必要のあるガイドラインおよび制限事項について説明します。

Anonymous Reporting のガイドライン

- DNS が設定されていること。
- Anonymous Reporting のメッセージを最初の試行で送信できなかった場合、ASA はメッセージをドロップする前にさらに 2 回試行します。
- Anonymous Reporting は、既存の設定を変更せずに、他の Smart Call Home 設定と共存させることができます。たとえば、Anonymous Reporting をイネーブルにする前に Smart Call Home がディセーブルになっている場合、Anonymous Reporting をイネーブルにした後でも、ディセーブルのままです。
- Anonymous Reporting をイネーブルにしている場合、トラスト ポイントを削除することはできません。また、Anonymous Reporting をディセーブルにした場合、トラスト ポイントはそのまま残ります。Anonymous Reporting がディセーブルの場合は、トラスト ポイントを削除できますが、Anonymous Reporting をディセーブルにしてもトラスト ポイントは削除されません。
- マルチ コンテキスト モード設定を使用している場合は、**dns**、**interface**、**trustpoint** コマンドは管理コンテキストにあり、**call-home** コマンドはシステム コンテキストにあります。
-

Smart Call Home のガイドライン

- マルチ コンテキスト モードでは、subscribe-to-alert-group snapshot periodic コマンドは、システム コンフィギュレーションから情報を取得するコマンドと、ユーザ コンテキストから情報を取得するコマンドの 2 つのコマンドに分割されます。
- Smart Call Home のバックエンド サーバは、XML 書式のメッセージのみ受け取ることができます。
- Smart Call Home メッセージは、クラスタリングをイネーブルにしており、クリティカルな重大度を持つ診断アラート グループに登録するように Smart Call Home を設定してある場

合に、重要なクラスタ イベントをレポートするためにシスコに送信されます。Smart Call Home クラスタリング メッセージは、次のイベントに対してのみ送信されます。

- ユニットがクラスタに参加したとき
- ユニットがクラスタから脱退したとき
- クラスタ ユニットがクラスタ マスターになったとき
- クラスタのセカンダリ ユニットが故障したとき

送信される各メッセージには次の情報が含まれています。

- アクティブ クラスタのメンバ数
- クラスタ マスターでの **show cluster info** コマンドおよび **show cluster history** コマンドの出力

Anonymous Reporting および Smart Call Home の設定

Anonymous Reporting は Smart Call Home サービスの一部であり、これを使用すると、エラーおよびヘルスに関する最小限の情報をデバイスからシスコに匿名で送信できます。一方、Smart Call Home サービスは、システム ヘルスのサポートをカスタマイズする機能です。Cisco TAC がお客様のデバイスをモニタして、問題があるときにケースを開くことができるようになります。多くの場合は、お客様がその問題に気付く前に発見できます。

両方のサービスをシステム上で同時に設定できますが、Smart Call Home サービスを設定すれば、Anonymous Reporting と同じ機能に加えて、カスタマイズされたサービスも使用できるようになります。

コンフィギュレーション モードに入ると、次のガイドラインに従って Anonymous Reporting および Smart Call Home サービスをイネーブルにすることを要求するプロンプトが出ます。

- このプロンプトで、[Y]es、[N]o、または [A]sk later を選択できます。[[A]sk later] を選択した場合、7 日後または ASA をリロードしたときに再度通知されます。[[A]sk later] を連続で選択すると、さらに ASA で 7 日ごとに 2 回プロンプトが表示されたのち、[[N]o] という答えだと見なされて再度表示されることはなくなります。
- プロンプトが表示されない場合は、Anonymous Reporting の設定 （1184 ページ）またはSmart Call Home の設定 （1185 ページ）の手順を実行して、Anonymous Reporting または Smart Call Home をイネーブルにすることができます。

Anonymous Reporting の設定

Anonymous Reporting を設定するには、次の手順を実行します。

手順

ステップ 1 Anonymous Reporting 機能をイネーブルにし、新しい匿名のプロファイルを作成します。

call-home reporting anonymous

例：

```
ciscoasa(config)# call-home reporting anonymous
```

このコマンドを入力すると、トラスト ポイントが作成され、シスコの Web サーバの識別情報を検証するために使用する証明書がインストールされます。

ステップ 2 （オプション）このサーバへの接続があり、システムがメッセージを送信できることを確認します。

call-home test reporting anonymous

例：

```
ciscoasa(config)# call-home test reporting anonymous

INFO: Sending test message to
https://tools.cisco.com/its/service/oddce/services/DDCEService...

INFO: Succeeded
```

成功またはエラー メッセージは、テスト結果を返します。

Smart Call Home の設定

ASA で Smart Call Home サービスを設定するには、次のタスクを実行します。

手順

ステップ 1 Smart Call Home サービスをイネーブルにします。Smart Call Home のイネーブル化 （1186 ページ）を参照してください。

ステップ 2 Smart Call Home メッセージがサブスクライバに配信される際に通過するメール サーバを設定します。メール サーバの設定 （1191 ページ）を参照してください。

ステップ 3 Smart Call Home メッセージの連絡先情報を設定します。顧客連絡先情報の設定 （1189 ページ）を参照してください。

ステップ 4 処理できるイベントの最大レートなどのアラート処理パラメータを定義します。アラート グループ サブスクリプションの設定 （1188 ページ）を参照してください。

ステップ 5 アラート サブスクリプション プロファイルを設定します。宛先プロファイルの設定 （1193 ページ）を参照してください。

個々のアラート サブスクリプション プロファイルによって、次の内容が特定されます。

- シスコの Smart Call Home サーバや電子メール受信者のリストなど、Smart Call Home メッセージの送信先となるサブスクライバ。
- コンフィギュレーション情報またはインベントリ情報など、受信するアラートの情報カテゴリ。

Smart Call Home のイネーブル化

Smart Call Home をイネーブルにして、Call Home プロファイルをアクティブにするには、次の手順を実行します。

手順

ステップ 1 Smart Call Home サービスをイネーブルにします。

service call-home

例：

```
ciscoasa(config)# service call-home
```

ステップ 2 Call Home コンフィギュレーション モードを開始します。

call-home

例：

```
ciscoasa(config)# call home
```

認証局のトラスト ポイントの宣言および認証

HTTPS 経由で Web サーバにメッセージを送信するように Smart Call Home が設定されている場合、Web サーバの証明書または証明書を発行した認証局（CA）の証明書を信頼するように ASA を設定する必要があります。Cisco Smart Call Home 実稼働サーバ証明書は、Verisign によって発行されます。Cisco Smart Call Home Staging サーバの証明書は Digital Signature Trust Company によって発行されます。

（注） VPN 検証に使用されないために、no client-types および no validation-usage 用のトラスト ポイントを設定する必要があります。

Cisco サーバ セキュリティの証明書を宣言および認証し、Smart Call Home サービス用に Cisco HTTPS サーバとの通信を確立するには、次の手順を実行します。

手順

ステップ 1 （マルチ コンテキスト モードのみ）管理コンテキストで証明書をインストールします。

changeto context *admincontext*

例：

```
ciscoasa(config)# changeto context contextA
```

ステップ 2 トラスト ポイントを設定し、証明書登録の準備を整えます。

crypto ca trustpoint *trustpoint-name*

例：

```
ciscoasa(config)# crypto ca trustpoint cisco
```

（注） 転送方法として HTTP を使用する場合は、セキュリティ証明書をトラスト ポイント経由でインストールする必要があります。HTTPS には、これが必須です。次の URL で、インストールする指定の証明書を探します。

http://www.cisco.com/en/US/docs/switches/lan/smart_call_home/SCH31_Ch6.html#wp1035380

ステップ 3 証明書登録に、手動でのカットアンドペースト方式を指定します。

enroll terminal

例：

```
ciscoasa(ca-trustpoint)# enroll terminal
```

ステップ 4 指定した CA を認証します。CA の名前は、**crypto ca trustpoint** コマンドで指定したトラスト ポイント名と一致している必要があります。プロンプトで、セキュリティ証明書のテキストを貼り付けます。

crypto ca authenticate trustpoint

例：

```
ciscoasa(ca-trustpoint)# crypto ca authenticate cisco
```

ステップ 5 セキュリティ証明書のテキストの終わりを指定し、入力されたセキュリティ証明書の受け入れを確認します。

quit

例：

```
ciscoasa(ca-trustpoint)# quit

%Do you accept this certificate [yes/no]:

yes
```

環境およびスナップショット アラート グループの設定

環境およびスナップショット アラート グループを設定するには、次の手順を実行します。

手順

アラート グループ コンフィギュレーション モードを開始します。

alert-group-config {**environment** | **snapshot**}

例：

```
ciscoasa(config)# alert-group-config environment
```

アラート グループ サブスクリプションの設定

宛先プロファイルをアラート グループに登録するには、次の手順を実行します。

手順

ステップ 1 Call Home コンフィギュレーション モードを開始します。

call-home

例：

```
ciscoasa(config)# call-home
```

ステップ 2 指定した Smart Call Home アラート グループをイネーブルにします。

alert-group {**all** |**configuration** |**diagnostic** |**environment** |**inventory** |**syslog**}

例：

```
ciscoasa(cfg-call-home)# alert-group syslog
```

すべてのアラート グループをイネーブルにするには、**all** キーワードを使用します。デフォルトでは、すべてのアラート グループがイネーブルになります。

ステップ 3 指定された宛先プロファイルに対するプロファイル コンフィギュレーション モードを開始します。

profile *profile-name*

例：

```
ciscoasa(cfg-call-home)# profile CiscoTAC-1
```

ステップ 4 使用可能なすべてのアラート グループに登録します。

subscribe-to-alert-group all

例：

```
ciscoasa(cfg-call-home-profile)# subscribe-to-alert-group all
```

ステップ 5 この宛先プロファイルをコンフィギュレーション アラート グループに登録します。

subscribe-to-alert-group configuration periodic {**daily** *hh:mm* | **monthly** *date hh:mm* | **weekly** *day hh:mm*}

例：

```
ciscoasa(cfg-call-home-profile)# subscribe-to-alert-group configuration periodic weekly
 Wednesday 23:30
```

periodic キーワードを指定すると、定期的に通知するようにコンフィギュレーション アラート グループが設定されます。デフォルトの間隔は daily です。

daily キーワードでは、送信する時刻を 24 時間制の *hh:mm* 形式（例：14:30）で指定します。

weekly キーワードでは、曜日と時刻を *day hh:mm* 形式で指定します。曜日は英語で記述します（例：Monday）。

monthly キーワードでは、1 ～ 31 の日付と時刻を *date hh:mm* 形式で指定します。

顧客連絡先情報の設定

顧客連絡先情報を設定するには、次の手順を実行します。

手順

ステップ 1 Call Home コンフィギュレーション モードを開始します。

call-home

例：

```
ciscoasa(config)# call-home
```

ステップ 2 顧客電話番号を指定します。スペースを使用できますが、スペースが含まれる場合はストリングの前後に引用符を付ける必要があります。

phone-number *phone-number-string*

例：

```
ciscoasa(cfg-call-home)# phone-number 8005551122
```

ステップ 3 顧客の住所（自由形式の文字列、最長255文字）を指定します。スペースを使用できますが、スペースが含まれる場合はストリングの前後に引用符を付ける必要があります。

street-address *street-address*

例：

```
ciscoasa(cfg-call-home)# street-address “1234 Any Street, Any city, Any state, 12345”
```

ステップ 4 顧客名（最長128文字）を指定します。スペースを使用できますが、スペースが含まれる場合はストリングの前後に引用符を付ける必要があります。

contact-name *contact-name*

例：

```
ciscoasa(cfg-call-home)# contact-name contactname1234
```

ステップ 5 シスコ カスタマー ID（最長 64 文字）を指定します。スペースを使用できますが、スペースが含まれる場合はストリングの前後に引用符を付ける必要があります。

customer-id *customer-id-string*

例：

```
ciscoasa(cfg-call-home)# customer-id customer1234
```

ステップ 6 顧客サイト ID（最長 64 文字）を指定します。スペースを使用できますが、スペースが含まれる場合はストリングの前後に引用符を付ける必要があります。

site-id *site-id-string*

例：

```
ciscoasa(cfg-call-home)# site-id site1234
```

ステップ 7 顧客連絡先 ID（最長 128 文字）を指定します。スペースを使用できますが、スペースが含まれる場合はストリングの前後に引用符を付ける必要があります。

contract-id *contract-id-string*

例：

```
ciscoasa(cfg-call-home)# contract-id contract1234
```

例

次に、連絡先情報を設定する例を示します。

```
ciscoasa(config)# call-home
ciscoasa(cfg-call-home)# contact-email-addr username@example.com
ciscoasa(cfg-call-home)# phone-number 8005551122
ciscoasa(cfg-call-home)# street-address "1234 Any Street, Any city, Any state, 12345"
ciscoasa(cfg-call-home)# contact-name contactname1234
ciscoasa(cfg-call-home)# customer-id customer1234
ciscoasa(cfg-call-home)# site-id site1234
ciscoasa(cfg-call-home)# contract-id contract1234
```

メール サーバの設定

メッセージの転送には、最もセキュアなHTTPSを使用することをお勧めします。ただし、Smart Call Home宛ての電子メールを設定し、電子メール メッセージ転送を使用するようメール サーバを設定できます。

電子メール サーバを設定するには、次の手順を実行します。

手順

ステップ 1 Call Home コンフィギュレーション モードを開始します。

call-home

例：

```
ciscoasa(config)# call-home
```

ステップ 2 SMTP メール サーバを指定します。

mail-server*ip-address* **name priority** [**1-100**] [**all**]

例：

```
ciscoasa(cfg-call-home)# mail-server 10.10.1.1 smtp.example.com priority 1
```

最大5つのメールサーバを指定できます。その場合は、コマンドを5回実行します。Smart Call Home メッセージの電子メール転送を使用するには、最低 1 つのメール サーバを設定する必要があります。

番号が小さいほどメール サーバの優先順位が高くなります。

ip-address 引数には、IPv4 と IPv6 のどちらのメール サーバ アドレスも指定できます。

例

次に、プライマリ メール サーバ（smtp.example.com）および IP アドレス 10.10.1.1 にあるセカンダリ メール サーバを設定する例を示します。

```
ciscoasa(config)# call-home
ciscoasa(cfg-call-home)# mail-server smtp.example.com priority 1
ciscoasa(cfg-call-home)# mail-server 10.10.1.1 priority 2
ciscoasa(cfg-call-home)# exit
ciscoasa(config)#
```

トラフィック レートの制限の設定

トラフィック レートの制限を設定するには、次の手順を実行します。

手順

ステップ 1 Call Home コンフィギュレーション モードを開始します。

call-home

例：

```
ciscoasa(config)# call-home
```

ステップ 2 Smart Call Home が 1 分間に送信できるメッセージの数を指定します。デフォルト値は、1 分間に 10 のメッセージです。

rate-limit *msg-count*

例：

```
ciscoasa(cfg-call-home)# rate-limit 5
```

Smart Call Home 通信の送信

特定の Smart Call Home 通信を送信するには、次の手順を実行します。

手順

次のいずれかのオプションを選択します。

- オプション1：プロファイル コンフィギュレーションを使用して、テスト メッセージを送信します。

  call-home test [*test-message*] **profile** *profile-name*

  例：

  ```
  ciscoasa# call-home test [testing123] profile CiscoTAC-1
  ```

- オプション2：アラート グループ メッセージを1つの宛先プロファイルに送信します（指定されている場合）。プロファイルが指定されていない場合は、インベントリ、コンフィギュレーション、スナップショット、またはテレメトリ アラート グループの通知を受け取るように設定されたすべてのプロファイルにメッセージが送信されます。

  call-home send alert-group inventory { | **configuration** | **snapshot** | **telemetry**} [**profile** *profile-name*]

  例：

  ```
  ciscoasa# call-home send alert-group inventory
  ```

- オプション3：コマンド出力を電子メールアドレスに送信します。指定するCLIコマンドは、どのようなコマンドでもかまいません。これには、すべての登録済みモジュールのコマンドも含まれます。

  call-home send*cli command* [**email** *email*]

  例：

  ```
  ciscoasa# call-home send cli destination email username@example.com
  ```

  電子メールアドレスを指定した場合、コマンド出力はそのアドレスに送信されます。電子メール アドレスを指定していない場合、出力はCisco TACに送信されます。電子メールは、件名行にサービス番号を付けて（指定した場合）ログテキスト形式で送信されます。

  電子メール アドレスを指定しない場合、またはCisco TAC電子メール アドレスを指定した場合に限り、サービス番号が必要になります。

宛先プロファイルの設定

電子メールまたはHTTPの宛先プロファイルを設定するには、次の手順を実行します。

手順

ステップ1 Call Home コンフィギュレーション モードを開始します。

call-home

例：

```
ciscoasa(config)# call-home
```

ステップ 2 指定された宛先プロファイルに対するプロファイル コンフィギュレーション モードを開始します。指定された宛先プロファイルが存在しない場合、作成されます。

profile *profile-name*

例：

```
ciscoasa(cfg-call-home)# profile newprofile
```

最大10個のアクティブプロファイルを作成できます。デフォルトプロファイルは、CiscoTACに報告するように設定されています。Call Home 情報を別の場所（たとえば、自社のサーバ）に送信するには、別のプロファイルを設定します。

ステップ 3 宛先、メッセージのサイズ、メッセージの形式、および Smart Call Home メッセージ受信者への転送方法を設定します。デフォルトのメッセージ形式は XML です。デフォルトでイネーブルになっている転送方法は、電子メールです。

destination address { **email** *address* | **http** *url*} |**message-size-limit** *size* | **preferred-msg-format** {**long-text** | **short-text** | **xml**} **transport-method** {**email** | **http**}}

例：

```
ciscoasa(cfg-call-home-profile)# destination address email username@example.com
ciscoasa(cfg-call-home-profile)# destination preferred-msg-format long-text
```

電子メールアドレスは、SmartCallHomeのメッセージを受け取る電子メールアドレスです（最長 100 文字）。デフォルトの最大 URL サイズは 5 MB です。

モバイル デバイスでメッセージを送信し、読み取るにはショート テキスト形式を使用し、コンピュータでメッセージを送信し、読み取るにはロング テキスト形式を使用します。

メッセージの受信者が Smart Call Home バックエンド サーバの場合、バックエンド サーバは XML 形式のメッセージのみ受け入れられるため **preferred-msg-format** の値が XML であることを確認します。

電子メールの転送方式をメールに戻すには、このコマンドを使用します。

宛先プロファイルのコピー

既存の宛先プロファイルをコピーして新しい宛先プロファイルを作成するには、次の手順を実行します。

手順

ステップ 1 Call Home コンフィギュレーション モードを開始します。

call-home

例：

```
ciscoasa(config)# call-home
```

ステップ 2 コピーするプロファイルを指定します。

profile *profile-name*

例：

```
ciscoasa(cfg-call-home)# profile newprofile
```

ステップ 3 既存のプロファイルの内容を新しいプロファイルにコピーします。

copy profile *src-profile-name dest-profile-name*

例：

```
ciscoasa(cfg-call-home)# copy profile newprofile profile1
```

既存のプロファイル（*src-profile-name*) と新しいプロファイル (*dest-profile-name*）は最大 23 文字です。

例

次に、既存のプロファイルをコピーする例を示します。

```
ciscoasa(config)# call-home
ciscoasa(cfg-call-home)# profile newprofile
ciscoasa(cfg-call-home-profile)# copy profile newprofile profile1
```

宛先プロファイルの名前の変更

既存のプロファイルの名前を変更するには、次の手順を実行します。

手順

ステップ 1 Call Home コンフィギュレーション モードを開始します。

call-home

例：

```
ciscoasa(config)# call-home
```

ステップ 2 名前を変更するプロファイルを指定します。

profile *profilename*

例：

```
ciscoasa(cfg-call-home)# profile newprofile
```

ステップ 3 既存のプロファイルの名前を変更します。

rename profile *src-profile-name dest-profile-name*

例：

```
ciscoasa(cfg-call-home)# rename profile newprofile profile1
```

既存のプロファイル（*src-profile-name*) と新しいプロファイル (*dest-profile-name*）は最大 23 文字です。

例

次に、既存のプロファイルの名前を変更する例を示します。

```
ciscoasa(config)# call-home
ciscoasa(cfg-call-home)# profile newprofile
ciscoasa(cfg-call-home-profile)# rename profile newprofile profile1
```

Anonymous Reporting および Smart Call Home のモニタリング

Anonymous Reporting および Smart Call Home サービスのモニタリングについては、次のコマンドを参照してください。

- **show call-home detail**

  このコマンドは、現在の Smart Call Home の詳細設定を表示します。

- **show call-home mail-server status**

  このコマンドは、現在のメール サーバのステータスを表示します。

- **show call-home profile** {profile name | **all**}

  このコマンドは、Smart Call Home プロファイルのコンフィギュレーションを表示します。

- **show call-home registered-module status** [**all**]

  このコマンドは、登録されているモジュールのステータスを表示します。

- **show call-home statistics**

  このコマンドは、Call Home の詳細ステータスを表示します。

- **show call-home**

  このコマンドは、現在の Smart Call Home のコンフィギュレーションを表示します。

- **show running-config call-home**

  このコマンドは、現在の Smart Call Home の実行コンフィギュレーションを表示します。

- **show smart-call-home alert-group**

  このコマンドは、Smart Call Home アラート グループの現在のステータスを表示します。

- **show running-config all**

  このコマンドは、Anonymous Reporting ユーザ プロファイルに関する詳細を表示します。

Smart Call Home の例

次の例は、Smart Call Home サービスを設定する方法を示しています。

```
ciscoasa (config)# service call-home
ciscoasa (config)# call-home
ciscoasa (cfg-call-home)# contact-email-addr customer@example.com
ciscoasa (cfg-call-home)# profile CiscoTAC-1
ciscoasa (cfg-call-home-profile)# destination address http
https://example.cisco.com/its/service/example/services/ExampleService
ciscoasa (cfg-call-home-profile)# destination address email callhome@example.com
ciscoasa (cfg-call-home-profile)# destination transport-method http
ciscoasa (cfg-call-home-profile)# subscribe-to-alert-group inventory periodic daily 23:30
ciscoasa (cfg-call-home-profile)# subscribe-to-alert-group configuration periodic weekly
 Wednesday 23:30
ciscoasa (cfg-call-home-profile)# subscribe-to-alert-group environment
ciscoasa (cfg-call-home-profile)# subscribe-to-alert-group diagnostic
ciscoasa (cfg-call-home-profile)# subscribe-to-alert-group telemetry periodic weekly
Monday 23:30
```

Anonymous Reporting および Smart Call Home の履歴

表 *58 : Anonymous Reporting* および *Smart Call Home* の履歴

機能名	プラットフォーム リリース	説明
Smart Call Home	8.2(2)	Smart Call Home サービスは、ASA に関するプロアクティブ診断およびリアルタイム アラートを提供し、ネットワークの可用性と運用効率を向上させます。 次のコマンドを導入または変更しました。 **active (call home)**、**call-home**、**call-home send alert-group**、**call-home test**、**contact-email-addr**、**customer-id (call home)**、**destination (call home)**、**profile**、**rename profile**、**service call-home**、**show call-home**、**show call-home detail**、**show smart-call-home alert-group**、**show call-home profile**、**show call-home statistics**、**show call-home mail-server status**、**show running-config call-home**、**show call-home registered-module status all**、**site-id**、**street-address**、**subscribe-to-alert-group all**、**alert-group-config**、**subscribe-to-alert-group configuration**、**subscribe-to-alert-group diagnostic**、**subscribe-to-alert-group environment**、**subscribe-to-alert-group inventory periodic**、**subscribe-to-alert-group snapshot periodic**、**subscribe-to-alert-group syslog**、**subscribe-to-alert-group telemetry periodic**。

機能名	プラットフォーム リリース	説明
Anonymous Reporting	9.0(1)	Anonymous Reporting をイネーブルにして、ASA プラットフォームを強化することができます。Anonymous Reporting により、エラーおよびヘルスに関する最小限の情報をデバイスからシスコに安全に送信できます。 **call-home reporting anonymous**、**call-home test reporting anonymous** コマンドが導入されました。
Smart Call Home	9.1(2)	テレメトリ アラート グループ レポートのための **show local-host** コマンドは、**show local-host | include interface** コマンドに変更になりました。
Smart Call Home	9.1(3)	Smart Call Home メッセージは、クラスタリングをイネーブルにしており、クリティカルな重大度を持つ診断アラート グループに登録するように Smart Call Home を設定してある場合に、重要なクラスタ イベントをレポートするためにシスコに送信されます。Smart Call Home クラスタリング メッセージは、次の 3 種類のイベントに対してのみ送信されます。 • ユニットがクラスタに参加したとき • ユニットがクラスタから脱退したとき • クラスタ ユニットがクラスタ マスターになったとき 送信される各メッセージには次の情報が含まれています。 • アクティブ クラスタのメンバ数 • クラスタ マスターでの **show cluster info** コマンドおよび **show cluster history** コマンドの出力

第 IX 部

参照先

第 41 章

コマンドライン インターフェイスの使用

この章では、Cisco ASA 上の CLI を使用する方法について説明します。

（注） CLI は、Cisco IOS CLI と類似したシンタックスや他の規則を使用しますが、ASA オペレーティング システムは Cisco IOS ソフトウェアのバージョンではありません。Cisco IOS CLI コマンドが、ASA の機能で動作したり、ASA と同じ機能を有しているものだと思わないでください。

ファイアウォール モードとセキュリティ コンテキスト モード

ASA は、次のモードの組み合わせで動作します。

- トランスペアレント ファイアウォール モードまたはルーテッド ファイアウォール モード

ファイアウォール モードは、ASA がレイヤ 2 ファイアウォールまたはレイヤ 3 ファイアウォールとして動作するかどうかを決定します。

- マルチ コンテキスト モードまたはシングル コンテキスト モード

  セキュリティ コンテキスト モードは、ASA が単一のデバイスとして動作するか、またはマルチ セキュリティ コンテキストとして動作する（仮想デバイスのように動作する）かを決定します。

特定のモードでしか使用できないコマンドもあります。

コマンドのモードとプロンプト

ASA の CLI にはコマンド モードが含まれています。特定のモードでしか入力できないコマンドもあります。たとえば、機密情報を表示するコマンドを入力するには、パスワードを入力して特権モードに入る必要があります。次に、コンフィギュレーション変更が誤って入力されないようにするために、コンフィギュレーション モードに入る必要があります。下位のコマンドはすべて、高位のモードで入力できます。たとえば、グローバル コンフィギュレーション モードで特権 EXEC コマンドを入力することができます。

（注） さまざまなタイプのプロンプトはすべてデフォルトで、別々のプロンプトとして設定できます。

- システム コンフィギュレーション モードまたはシングル コンテキスト モードに入っている場合、プロンプトはホスト名で始まります。

  ```
  ciscoasa
  ```

- プロンプト文字列を表示するときに、プロンプト コンフィギュレーションが解析され、設定されたキーワード値が prompt コマンドで設定された順に表示されます。キーワード引数は、ホスト名、ドメイン、コンテキスト、プライオリティ、状態のいずれかで、任意の順になります。

  prompt hostname context priority state

- コンテキスト内では、プロンプトはホスト名の後にコンテキスト名が表示されます。

  ```
  ciscoasa/context
  ```

プロンプトは、アクセス モードに応じて変化します。

- ユーザ EXEC モード

  ユーザ EXEC モードでは、最小限の ASA 設定が表示されます。ユーザ EXEC モードのプロンプトは、初めて ASA にアクセスしたときに次のように表示されます。

```
ciscoasa>

ciscoasa/context>
```

- 特権 EXEC モード

  特権EXECモードでは、ユーザの特権レベルまでの現在の設定がすべて表示されます。すべてのユーザEXECモードコマンドは、特権EXECモードで動作します。特権EXECモードを開始するには、ユーザ EXEC モードで **enable** コマンドを入力します。これにはパスワードが必要です。プロンプトにはシャープ記号（#）が含まれています。

```
ciscoasa#

ciscoasa/context#
```

- グローバル コンフィギュレーション モード

  グローバル コンフィギュレーション モードでは、ASA コンフィギュレーションを変更できます。このモードでは、ユーザEXEC、特権EXEC、およびグローバルの各コンフィギュレーション コマンドをすべて使用できます。グローバル コンフィギュレーション モードを開始するには、特権 EXEC モードで **configure terminal** コマンドを入力します。プロンプトが次のように変化します。

```
ciscoasa(config)#

ciscoasa/context(config)#
```

- コマンド固有のコンフィギュレーション モード

  いくつかのコマンドは、グローバル コンフィギュレーション モードから、コマンド固有のコンフィギュレーション モードに移行します。このモードでは、ユーザ EXEC、特権 EXEC、グローバルの各コンフィギュレーション コマンド、およびコマンド固有のコンフィギュレーション コマンドをすべて使用できます。たとえば、**interface** コマンドを使用すると、インターフェイス コンフィギュレーション モードに移行します。プロンプトが次のように変化します。

```
ciscoasa(config-if)#

ciscoasa/context(config-if)#
```

構文の書式

コマンド構文の説明では、次の表に記載されている表記法を使用します。

表 *59 :* 構文の表記法

表記法	説明
bold	記載されているとおりに入力するコマンドおよびキーワードは、太字で示しています。
イタリック体	イタリック体の文字は、ユーザが値を指定する引数です。
[x]	省略可能な要素（キーワードまたは引数）は、角かっこで囲んで示しています。
|	省略可能または必須のキーワードや引数の中から選択する場合は、縦棒で区切って示しています。
[x | y]	いずれか1つを選択できる省略可能なキーワードや引数は、角カッコで囲み、縦棒で区切って示しています。
{x | y}	必ずいずれか1つを選択しなければならない必須キーワードや引数は、波かっこで囲み、縦棒で区切って示しています。
[x {y | z}]	省略可能または必須の要素内に、さらに省略可能または必須の選択肢を含める場合は、角カッコや波カッコを入れ子にして示しています。角カッコ内の波カッコと縦棒は、省略可能な要素内で選択すべき必須の要素を示しています。

コマンドの短縮形

ほとんどのコマンドは、コマンドに固有の最小文字数まで短縮できます。たとえば、設定を表示するには完全なコマンド **write terminal** を入力する代わりに **wr t** と入力できます。また、特権モードを開始するには **en**、設定モードを開始するには **conf t** と入力できます。さらに、**0** を入力して **0.0.0.0** を表すこともできます。

コマンドラインの編集

ASA では、Cisco IOS ソフトウェアと同じコマンドライン編集ルールが使用されます。以前に入力したすべてのコマンドを表示するには、**show history** コマンドを使用します。個々のコマンドを表示するには、上矢印キーまたは **^p** コマンドを使用します。前に入力したコマンドを確認したら、下矢印や **^n** コマンドでリスト内を前に進むことができます。再利用するコマンドに到達したら、そのコマンドを編集することも、**Enter** キーを押して実行することもできます。**^w** を使用してカーソルの左側にある単語を削除することも、**^u** を使用して行を消去することもできます。

ASA では、1 つのコマンドに 512 文字まで入力できます。512 文字を超えて入力した文字は無視されます。

コマンドの補完

部分的な文字列を入力してからコマンドまたはキーワードを完成させるには、**Tab** キーを押します。ASA は、部分的な文字列がコマンドまたはキーワード 1 つだけと一致する場合に限り、コマンドまたはキーワードを完成させます。たとえば、**s** と入力して Tab キーを押した場合は、一致するコマンドが複数あるため、ASA はコマンドを完成させません。一方、**dis** と入力して [Tab] キーを押した場合、**disable** コマンドが完成します。

コマンドのヘルプ

次のコマンドを入力すると、コマンドラインからヘルプ情報を利用できます。

- **help** *command_name*

  特定のコマンドのヘルプを表示します。

- *command_name* **?**

  使用可能な引数のリストを表示します。

- *string***?**（スペースなし）

  その文字列で始まるコマンドをリストします。

- **?** および **+?**

  使用できるすべてのコマンドをリストします。**?** と入力すると、ASA は現在のモードで使用できるコマンドだけを表示します。下位モードのコマンドも含め、使用できるすべてのコマンドを表示するには、**+?** と入力します。

（注） コマンド文字列に疑問符（?）を組み込む場合は、誤って CLI ヘルプを起動しないよう、疑問符を入力する前に Ctrl+V を押す必要があります。

実行コンフィギュレーションの確認

実行コンフィギュレーションを確認するには、次のいずれかのコマンドを使用します。

- **show running-config** [**all**] [*command*]

  all を指定すると、すべてのデフォルト設定も表示されます。*Command* を指定すると、関連するコマンドだけが出力に含まれます。

（注） 多くのパスワードは ***** として表示されます。パスワードをプレーン テキストまたは暗号化された形式（マスター パスフレーズを有効にしている場合）で表示するには、**more** コマンドを使用します。

- **more system:running-config**

show コマンドおよび more コマンドの出力のフィルタリング

縦棒（|）はどの **show** コマンドでも使用できます。これには、フィルタ オプションとフィルタリング式を組み込むことができます。フィルタリングは、Cisco IOS ソフトウェアと同様に、各出力行を正規表現と照合することによって行われます。選択するフィルタ オプションによって、正規表現に一致するすべての出力を含めたり除外したりできます。また、正規表現に一致する行で始まるすべての出力を表示することもできます。

show コマンドでフィルタリング オプションを使用する場合の構文は、次のとおりです。

show *command* | {**include**| **exclude** | **begin** | **grep** [**-v**]} *regexp*

または

more system:running-config| {**include**| **exclude** | **begin** | **grep** [**-v**]} *regexp*

（注） **more** コマンドを入力すると、実行コンフィギュレーションだけでなく、任意のファイルの内容を表示できます。詳細については、コマンド リファレンスを参照してください。

このコマンド文字列の最初の縦棒（|）は演算子であり、コマンド内に含める必要があります。この演算子は、**show** コマンドの出力をフィルタに組み込みます。構文内に含まれるその他の縦棒（|）は代替オプションを示すものであり、コマンドの一部ではありません。

include オプションを指定すると、正規表現に一致するすべての出力行が表示されます。**-v** を付けずに **grep** オプションを使用する場合も、同じ結果となります。**exclude** オプションを指定すると、正規表現に一致するすべての出力行が除外されます。**-v** を付けて **grep** オプションを使用する場合も、同じ結果となります。**begin** オプションを指定すると、正規表現に一致する行で始まるすべての出力行が表示されます。

regexp には、Cisco IOS の正規表現を指定します。正規表現は一重引用符または二重引用符で囲まれていません。したがって、末尾の空白スペースが正規表現の一部と解釈されるため、末尾の空白スペースに注意してください。

正規表現を作成する場合は、照合する任意の文字または数字を使用できます。また、メタ文字と呼ばれるキーボード文字は、正規表現で使用されると特別な意味を持ちます。

疑問符（?）やタブなど、CLI の特殊文字をすべてエスケープするには、**Ctrl+V** を使用します。たとえば、コンフィギュレーションで **d?g** と入力するには、**d[Ctrl+V]?g** とキー入力します。

show コマンド出力のリダイレクトと追加

show コマンドの出力を画面に表示するのではなく、デバイス上またはリモート ロケーション内のファイルにリダイレクトすることができます。デバイス上のファイルへのリダイレクトの場合は、ファイルにコマンド出力を追加することもできます。

show *command* | {**append | redirect**} *url*

- **append** *url* により、出力が既存のファイルに追加されます。次のいずれかを使ってファイルを指定します。
  - **disk0:/**[[*path/*]*filename*] または **flash:/**[[*path/*]*filename*]：**flash** と **disk0** はどちらも内部フラッシュ メモリを示します。どちらのオプションを使用してもかまいません。
  - **disk1:/**[[*path/*]*filename*]：外部メモリを意味します。
- **redirect** *url* により、指定されたファイルが作成されます。または、ファイルがすでに存在している場合は、上書きされます。
  - **disk0:/**[[*path/*]*filename*] または **flash:/**[[*path/*]*filename*]：**flash** と **disk0** はどちらも内部フラッシュ メモリを示します。どちらのオプションを使用してもかまいません。
  - **disk1:/**[[*path/*]*filename*]：外部メモリを意味します。
  - **smb:/**[[*path/*]*filename*]：サーバ メッセージ ブロック、UNIX サーバのローカル ファイル システムを示します。
  - **ftp://**[[*user*[**:***password*]@] *server*[:*port*]/[*path/*] *filename*[**;type=***xx*]]：SCP サーバを示します。**type** には次のいずれかのキーワードを使用できます。**ap**（ASCII パッシブ モード）、**an**（ASCII 通常モード）、**ip**（デフォルト：バイナリ パッシブ モード）、**in**（バイナリ通常モード）。
  - **scp://**[[*user*[:*password*]@] *server*[/*path*]/*filename*[**;int=***interface_name*]]：**;int=***interface* オプションを指定すると、ルート ルックアップがバイパスされ、常に指定したインターフェイスを使用してセキュア コピー（SCP）サーバに接続するようになります。
  - **tftp://**[[*user*[**:***password*]@] *server*[:*port*] /[*path/*]*filename*[**;int=***interface_name*]]：TFTP サーバを示します。パス名にスペースを含めることはできません。**;int=***interface* オプションを指定すると、ルートルックアップをバイパスし、常に指定したインターフェイスを使用して TFTP サーバに接続するようになります。

コマンド出力のページング

help や **?**、**show**、**show xlate** など、長いリストが出力されるコマンドでは、1 画面分ずつ表示して停止させるか、リストの最後まで表示させるかを決めることができます。**pager** コマンドを使用すると、画面上に表示する行数を選択してから More プロンプトを表示するようにできます。

ページングがイネーブルになっているときには、次のプロンプトが表示されます。

```
<--- More --->
```

More プロンプトの構文は、UNIX の **more** コマンドと似ています。

- 次の 1 画面を表示するには、Space バーを押します。
- 次の行を表示するには、Enter キーを押します。
- コマンド ラインに戻るには、q キーを押します。

コメントの追加

行の先頭にコロン（:）を置いて、コメントを作成できます。しかし、コメントが表示されるのはコマンド ヒストリ バッファだけで、コンフィギュレーションには表示されません。したがって、コメントは、**show history** コマンドを使用するか、矢印キーを押して前のコマンドを取得することによって表示できますが、コンフィギュレーションには含まれないので、**write terminal** コマンドでは表示できません。

テキスト コンフィギュレーション ファイル

この項では、ASA にダウンロードできるテキスト コンフィギュレーション ファイルをフォーマットする方法について説明します。

テキスト ファイルでコマンドと行が対応する仕組み

テキスト コンフィギュレーション ファイルには、このガイドで説明するコマンドに対応する行が含まれています。

例では、コマンドの前に CLI プロンプトがあります。次の例でのプロンプトは「ciscoasa(config)#」です。

```
ciscoasa(config)# context a
```

テキスト コンフィギュレーション ファイルでは、コマンドの入力を求めるプロンプトが表示されないので、プロンプトは省略されています。

```
context a
```

コマンド固有のコンフィギュレーション モード コマンド

コマンド固有のコンフィギュレーション モード コマンドは、コマンドラインで入力されたときに、メイン コマンドの下に字下げして表示されます。テキスト ファイルの行は、コマンドがメイン コマンドのすぐ後に表示される限り、字下げする必要はありません。たとえば、次のテキストは字下げされていませんが、字下げしたテキストと同じように読み取られます。

```
interface gigabitethernet0/0
nameif inside
interface gigabitethernet0/1
    nameif outside
```

自動テキスト入力

コンフィギュレーションを ASA にダウンロードすると、それにより一部の行が自動的に挿入されます。たとえば、ASA は、デフォルト設定のため、またはコンフィギュレーションが変更されたときのための行を挿入します。テキスト ファイルを作成するときは、これらの自動入力を行う必要はありません。

行の順序

ほとんどの場合、コマンドはファイル内で任意の順序に置くことができます。ただし、ACE などいくつかの行は表示された順に処理されるので、順序がアクセス リストの機能に影響する場合があります。その他のコマンドでも、順序の要件がある場合があります。たとえば、あるインターフェイスの名前を多数の後続コマンドが使用する場合は、そのインターフェイスの **nameif** コマンドをまず入力する必要があります。また、コマンド固有のコンフィギュレーション モードのコマンドは、メイン コマンドの直後に置く必要があります。

テキスト コンフィギュレーションに含まれないコマンド

いくつかのコマンドは、コンフィギュレーションに行を挿入しません。たとえば、**show running-config** などのランタイム コマンドは、テキスト ファイル内に対応する行がありません。

パスワード

ログイン パスワード、イネーブル パスワード、およびユーザ パスワードは、コンフィギュレーションに保存される前に自動的に暗号化されます。たとえば、パスワード「cisco」の暗号化さ

れた形式はjMorNbK0514fadBhのようになります。コンフィギュレーションパスワードは暗号化された形式で別の ASA にコピーできますが、そのパスワードの暗号を解読することはできません。

暗号化されていないパスワードをテキストファイルに入力した場合、コンフィギュレーションを ASA にコピーしても、ASA は自動的にパスワードを暗号化しません。ASA がパスワードを暗号化するのは、**copy running-config startup-config** または **write memory** コマンドを使用して、コマンドラインから実行コンフィギュレーションを保存した場合のみです。

マルチセキュリティ コンテキスト ファイル

マルチ セキュリティ コンテキストの場合、コンフィギュレーション全体は次に示す複数の部分で構成されます。

- セキュリティ コンテキスト コンフィギュレーション
- コンテキストのリストなど、ASA の基本設定を示すシステム コンフィギュレーション
- システム コンフィギュレーション用のネットワーク インターフェイスを提供する管理コンテキスト

  システム コンフィギュレーションには、それ自体のインターフェイスまたはネットワーク設定は含まれていません。代わりに、システムは、ネットワーク リソースにアクセスする必要があるときに（サーバからコンテキストをダウンロードするときなど）、管理コンテキストとして指定されたコンテキストを使用します。

各コンテキストは、シングル コンテキスト モード コンフィギュレーションに似ています。システム コンフィギュレーションにはシステム限定のコマンド（全コンテキストのリストなど）が含まれており、その他の一般的なコマンド（多数のインターフェイス パラメータなど）は存在しない点で、システム コンフィギュレーションは、コンテキスト コンフィギュレーションとは異なっています。

サポートされている文字セット

ASA CLI は、現在 UTF-8 の符号化方式だけをサポートしています。UTF-8 は Unicode 文字の特定の符号化スキームであり、ASCII 文字のサブセットと互換性を持つように設計されています。ASCII 文字は UTF-8 で 1 バイト文字として表現されます。その他のすべての文字は、UTF-8 でマルチバイト文字として表現されます。

ASCII の印刷可能文字（0x20 ～ 0x7e）はすべてサポートされています。印刷可能な ASCII 文字は、ISO 8859-1 の文字と同じです。UTF-8 は ISO 8859-1 のスーパーセットであるため、最初の 256 文字（0 ～ 255）は ISO 8859-1 の文字と同じになります。ASA CLI は、ISO 8859-1 の文字を 255 文字（マルチバイト文字）までサポートしています。

第 42 章

アドレス、プロトコル、およびポート

この章では、IP アドレス、プロトコル、およびアプリケーションのクイック リファレンスを提供します。

IPv4 アドレスとサブネット マスク

この項では、Cisco ASA で IPv4 アドレスを使用する方法について説明します。IPv4 アドレスはドット付き 10 進数表記の 32 ビットの数値であり、バイナリから 10 進数に変換されドットで区切られた 4 つの 8 ビット フィールド（オクテット）で構成されます。IP アドレスの最初の部分はホストが常駐するネットワークを示し、2 番目の部分は所定のネットワーク上の特定のホストを示します。ネットワーク番号フィールドは、ネットワーク プレフィックスと呼ばれます。所定のネットワーク上のホストはすべて、同じネットワーク プレフィックスを共有しますが、固有のホスト番号を持つ必要があります。クラスフル IP では、アドレスのクラスがネットワーク プレフィックスとホスト番号の間の境界を決定します。

クラス

IP ホスト アドレスは、Class A、Class B、Class C の 3 つの異なるアドレス クラスに分かれています。各クラスは、32 ビット アドレス内の異なるポイントで、ネットワーク プレフィックスとホスト番号の間の境界を決定します。Class D アドレスは、マルチキャスト IP 用に予約されています。

- Class A アドレス（1.xxx.xxx.xxx ～ 126.xxx.xxx.xxx）は、最初のオクテットのみをネットワーク プレフィックスとして使用します。

- Class B アドレス（128.0.xxx.xxx ～ 191.255.xxx.xxx）は、最初の 2 つのオクテットをネットワーク プレフィックスとして使用します。
- Class C アドレス（192.0.0.xxx ～ 223.255.255.xxx）は、最初の 3 つのオクテットをネットワーク プレフィックスとして使用します。

Class A アドレスには 16,777,214 個のホスト アドレス、Class B アドレスには 65,534 個のホストがあるので、サブネットマスクを使用してこれらの膨大なネットワークを小さいサブネットに分割することができます。

プライベート ネットワーク

ネットワーク上に多数のアドレスが必要な場合、それらをインターネットでルーティングする必要がないときは、インターネット割り当て番号局（IANA）が推奨するプライベート IP アドレスを使用できます（RFC 1918 を参照）。次のアドレス範囲が、アドバタイズされないプライベート ネットワークとして指定されています。

- 10.0.0.0 ～ 10.255.255.255
- 172.16.0.0 ～ 172.31.255.255
- 192.168.0.0 ～ 192.168.255.255

サブネット マスク

サブネット マスクを使用すると、単一の Class A、B、または C ネットワークを複数のネットワークに変換できます。サブネット マスクを使用して、ホスト番号からネットワーク プレフィックスにビットを追加する拡張ネットワーク プレフィックスを作成することができます。たとえば、Class C ネットワーク プレフィックスは常に、IP アドレスの最初の 3 つのオクテットで構成されます。一方、Class C 拡張ネットワーク プレフィックスは、4 番目のオクテットの一部も使用します。

ドット付き 10 進数の代わりにバイナリ表記を使用している場合は、サブネット マスクを容易に理解できます。サブネット マスク内のビットには、インターネット アドレスとの 1 対 1 の対応関係があります。

- IP アドレス内の対応するビットが拡張ネットワーク プレフィックスの一部である場合、ビットは 1 に設定されます。
- ビットがホスト番号の一部である場合、ビットは 0 に設定されます。

例 1：Class B アドレスが 129.10.0.0 の場合に 3 番目のオクテット全体をホスト番号ではなく拡張ネットワーク プレフィックスの一部として使用するには、サブネット マスクとして 11111111.11111111.11111111.00000000 を指定する必要があります。このサブネット マスクによって、Class B アドレスは、ホスト番号が最後のオクテットだけで構成される Class C アドレスに相当するものに変換されます。

例 2：3 番目のオクテットの一部だけを拡張ネットワーク プレフィックスに使用する場合は、11111111.11111111.11111000.00000000 のようなサブネット マスクを指定する必要があります。ここでは、3 番目のオクテットのうち 5 ビットだけが拡張ネットワーク プレフィックスに使用されます。

サブネット マスクは、ドット付き 10 進数マスクまたは /ビット（「スラッシュ ビット」）マスクとして記述できます。例 1 では、ドット付き 10 進数マスクに対して、各バイナリ オクテットを 10 進数の 255.255.255.0 に変換します。/ビット マスクの場合は、1s: /24 の数値を追加します。例 2 では、10 進数は 255.255.248.0 で、/ビットは /21 です。

3 番目のオクテットの一部を拡張ネットワーク プレフィックスに使用して、複数の Class C ネットワークを大規模なネットワークにスーパーネット化することもできます。たとえば、192.168.0.0/20 です。

サブネットマスクの決定

必要なホストの数に基づいてサブネットマスクを決定するには、次の表を参照してください。

（注） 単一のホストを示す /32 を除き、サブネットの最初と最後の数は予約されています。

表 *60*：ホスト、ビット、ドット区切りの *10* 進数マスク

ホスト	/ビット マスク	ドット付き 10 進数マスク
16,777,216	/8	255.0.0.0 Class A ネットワーク
65,536	/16	255.255.0.0 Class B ネットワーク
32,768	/17	255.255.128.0
16,384	/18	255.255.192.0
8192	/19	255.255.224.0
4096	/20	255.255.240.0
2048	/21	255.255.248.0
1024	/22	255.255.252.0
512	/23	255.255.254.0
256	/24	255.255.255.0 Class C ネットワーク
128	/25	255.255.255.128
64	/26	255.255.255.192

ホスト	/ビット マスク	ドット付き 10 進数マスク
32	/27	255.255.255.224
16	/28	255.255.255.240
8	/29	255.255.255.248
4	/30	255.255.255.252
使用不可	/31	255.255.255.254
1	/32	255.255.255.255 単一ホスト アドレス

サブネットマスクに使用するアドレスの決定

次の各項では、Class C サイズおよび Class B サイズのネットワークに対してサブネット マスクで使用するネットワーク アドレスを判別する方法について説明します。

クラス C 規模ネットワーク アドレス

2 ～ 254 のホストを持つネットワークの場合、4 番目のオクテットは、0 から始まるホスト アドレスの数の倍数になります。例として、次の表に 8 個のホストを持つサブネット（/29）、192.168.0.x を示します。

（注） サブネットの最初と最後のアドレスは予約されています。最初のサブネットの例では、192.168.0.0 と 192.168.0.7 は使用できません。

表 *61 :* クラス *C* 規模ネットワーク アドレス

マスク /29（255.255.255.248）でのサブネット	アドレス範囲
192.168.0.0	192.168.0.0 ～ 192.168.0.7
192.168.0.8	192.168.0.8 ～ 192.168.0.15
192.168.0.16	192.168.0.16 ～ 192.168.0.31
—	—
192.168.0.248	192.168.0.248 ～ 192.168.0.255

クラス B 規模ネットワーク アドレス

254 ～ 65,534 のホストを持つネットワークのサブネット マスクで使用するネットワーク アドレスを判別するには、可能な拡張ネットワーク プレフィックスそれぞれについて 3 番目のオクテットの値を判別する必要があります。たとえば、10.1.*x*.0 のようなアドレスをサブネット化

することができます。ここで、最初の2つのオクテットは拡張ネットワーク プレフィックスで使用されるため固定されています。4 番目のオクテットは、すべてのビットがホスト番号に使用されるため、0 です。

3 番目のオクテットの値を判別するには、次の手順を実行します。

1. 65,536（3 番目と 4 番目のオクテットを使用するアドレスの合計）を必要なホスト アドレスの数で割って、ネットワークから作成できるサブネットの数を計算します。

   たとえば、65,536 を 4096 のホストで割ると、16 になります。したがって、Class B サイズのネットワークでは、それぞれ 4096 個のアドレスを持つサブネットが 16 個できます。

2. 256（3 番目のオクテットの値の数）をサブネットの数で割って、3 番目のオクテット値の倍数を判別します。

   この例では、256/16 = 16 です。

   3 番目のオクテットは、0 から始まる 16 の倍数になります。

次の表に、ネットワーク 10.1 の 16 個のサブネットを示します。

（注） サブネットの最初と最後のアドレスは予約されています。最初のサブネットの例では、10.1.0.0 と 10.1.15.255 は使用できません。

表 *62 :* ネットワークのサブネット

マスク /20（255.255.240.0）でのサブネット	アドレス範囲
10.1.0.0	10.1.0.0 ～ 10.1.15.255
10.1.16.0	10.1.16.0 ～ 10.1.31.255
10.1.32.0	10.1.32.0 ～ 10.1.47.255
—	—
10.1.240.0	10.1.240.0 ～ 10.1.255.255

IPv6 アドレス

IPv6 は、IPv4 後の次世代インターネット プロトコルです。これにより、アドレス空間の拡張、ヘッダー形式の簡略化、拡張子とオプションのサポートの向上、フローラベル機能、および認証とプライバシーの機能が提供されます。IPv6 については RFC 2460 で説明されています。IPv6 アドレッシング アーキテクチャについては RFC 3513 で説明されています。

この項では、IPv6 のアドレス形式とアーキテクチャについて説明します。

IPv6 アドレスの形式

IPv6 アドレスは、x:x:x:x:x:x:x:x のように、コロン（:）で区切られた 8 つの一連の 16 ビット 16 進数フィールドとして表されます。次に、IPv6 アドレスの例を 2 つ示します。

- 2001:0DB8:7654:3210:FEDC:BA98:7654:3210
- 2001:0DB8:0000:0000:0008:0800:200C:417A

（注） IPv6 アドレスの 16 進文字は大文字と小文字が区別されません。

アドレスの個々のフィールドに先行ゼロを入れる必要はありませんが、各フィールドに 1 個以上の桁が含まれている必要があります。したがって、例のアドレス 2001:0DB8:0000:0000:0008:0800:200C:417A は、左から 3 番目～ 6 番目のフィールドから先行ゼロを削除して、2001:0DB8:0:0:8:800:200C:417A のように短縮することができます。ゼロだけを含むフィールド（左から 3 番目と 4 番目のフィールド）は、単一のゼロに短縮されています。左から 5 番目のフィールドでは、3 つの先行ゼロが削除され、単一の 8 がフィールドに残されています。左から 6 番目のフィールドでは、1 つの先行ゼロが削除され、800 がフィールドに残されています。

IPv6 アドレスには、ゼロの 16 進数フィールドがいくつか連続して含まれていることがよくあります。IPv6 アドレスの先頭、中間、または末尾で 2 つのコロン（::）を使用して、ゼロの連続フィールドを圧縮することができます（コロンは、ゼロの 16 進数フィールドが連続していることを表します）。次の表に、さまざまなタイプの IPv6 アドレスでのアドレス圧縮の例をいくつか示します。

表 *63 : IPv6* アドレスの圧縮例

アドレスタイプ	標準形式	圧縮形式
ユニキャスト	2001:0DB8:0:0:0:BA98:0:3210	2001:0DB8::BA98:0:3210
マルチキャスト	FF01:0:0:0:0:0:0:101	FF01::101
ループバック	0:0:0:0:0:0:0:1	::1
未指定	0:0:0:0:0:0:0:0	::

（注） ゼロのフィールドが連続することを表す 2 つのコロン（::）は、IPv6 アドレスの中で一度だけ使用できます。

IPv4 アドレスと IPv6 アドレスの両方を含む環境に対処するため、別の IPv6 形式がよく使用されます。その形式は x:x:x:x:x:x:y.y.y.y です。ここで、x は IPv6 アドレスの 6 つの高次の部分の 16 進数値を表し、y はアドレスの 32 ビット IPv4 部分（IPv6 アドレスの残りの 2 つの 16 ビッ

ト部分を占める）の 10 進数値を表します。たとえば、IPv4 アドレス 192.168.1.1 は、IPv6 アドレス 0:0:0:0:0:0:FFFF:192.168.1.1 または ::FFFF:192.168.1.1 として表すことができます。

IPv6 アドレス タイプ

次に、IPv6 アドレスの 3 つの主なタイプを示します。

- **ユニキャスト**：ユニキャストアドレスは、単一インターフェイスの識別子です。ユニキャストアドレスに送信されたパケットは、そのアドレスで示されたインターフェイスに送信されます。1 つのインターフェイスに複数のユニキャストアドレスが割り当てられている場合もあります。
- **マルチキャスト**：マルチキャストアドレスは、インターフェイスのセットを表す識別子です。マルチキャストアドレスに送信されたパケットは、そのアドレスで示されたすべてのアドレスに送信されます。
- **エニーキャスト**：エニーキャストアドレスは、インターフェイスのセットを表す識別子です。マルチキャストアドレスと違い、エニーキャストアドレスに送信されたパケットは、ルーティングプロトコルの距離測定によって判別された「最も近い」インターフェイスにだけ送信されます。

（注） IPv6 にはブロードキャスト アドレスはありません。マルチキャスト アドレスにブロードキャスト機能があります。

ユニキャスト アドレス

この項では、IPv6ユニキャストアドレスについて説明します。ユニキャストアドレスは、ネットワーク ノード上のインターフェイスを識別します。

グローバル アドレス

IPv6 グローバル ユニキャスト アドレスの一般的な形式では、グローバル ルーティング プレフィックス、サブネット ID、インターフェイス ID の順に並んでいます。グローバル ルーティング プレフィックスは、別の IPv6 アドレス タイプによって予約されていない任意のプレフィックスです。

バイナリ 000 で始まるものを除くすべてのグローバル ユニキャスト アドレスが、Modified EUI-64 形式で 64 ビットのインターフェイス ID を持っています。

バイナリ 000 で始まるグローバル ユニキャスト アドレスには、アドレスのインターフェイス ID部分のサイズまたは構造に対する制約がありません。このタイプのアドレスの一例として、IPv4 アドレスが埋め込まれた IPv6 アドレスがあります。

サイトローカル アドレス

サイトローカルアドレスは、サイト内のアドレッシングに使用されます。このアドレスを使用すると、グローバルで一意のプレフィックスを使用せずにサイト全体をアドレッシングするこ

とができます。サイトローカルアドレスでは、プレフィックス FEC0::/10、54 ビット サブネット ID、64 ビット インターフェイス ID（Modified EUI-64 形式）の順に並んでいます。

サイトローカル ルータは、サイト外の送信元または宛先にサイトローカル アドレスを持つパケットを転送しません。したがって、サイトローカル アドレスは、プライベート アドレスと見なされます。

リンクローカル アドレス

すべてのインターフェイスに、少なくとも 1 つのリンクローカル アドレスが必要です。インターフェイスごとに複数の IPv6 アドレスを設定できますが、設定できるリンクローカル アドレスは 1 つだけです。

リンクローカル アドレスは、Modified EUI-64 形式でリンクローカル プレフィックス FE80::/10 とインターフェイス識別子を使用して任意のインターフェイスで自動的に設定できる IPv6 ユニキャスト アドレスです。リンクローカル アドレスは、ネイバー探索プロトコルとステートレス自動設定プロセスで使用されます。リンクローカルアドレスを持つノードは、通信が可能です。これらのノードは通信にサイトローカルアドレスまたはグローバルに固有なアドレスを必要としません。

ルータは、送信元または宛先にリンクローカルアドレスを持つパケットを送信しません。したがって、リンクローカル アドレスは、プライベート アドレスと見なされます。

IPv4 互換 IPv6 アドレス

IPv4 アドレスを組み込むことができる IPv6 アドレスのタイプは 2 つあります。

最初のタイプは、IPv4 互換 IPv6 アドレスです。IPv6 移行メカニズムには、IPv4 ルーティング インフラストラクチャ上で IPv6 パケットを動的にトンネリングさせるためのホストおよびルータの技術が実装されています。この技術を使用する IPv6 ノードには、低次 32 ビットでグローバル IPv4 アドレスを伝送する特別な IPv6 ユニキャスト アドレスが割り当てられます。このタイプのアドレスは「IPv4 互換 IPv6 アドレス」と呼ばれ、形式は ::y.y.y.y です。この y.y.y.y は IPv4 ユニキャスト アドレスになります。

（注） 「IPv4 互換 IPv6 アドレス」で使用する IPv4 アドレスは、グローバルに固有な IPv4 ユニキャスト アドレスである必要があります。

2 つ目のタイプの IPv6 アドレスは、IPv4 アドレスが埋め込まれたもので、「IPv4 マッピング IPv6 アドレス」と呼ばれます。このアドレス タイプは、IPv4 ノードのアドレスを IPv6 アドレスとして表すために使用されます。このタイプのアドレス形式は ::FFFF:y.y.y.y です。ここで、y.y.y.y は IPv4 ユニキャスト アドレスです。

未指定アドレス

未指定アドレス 0:0:0:0:0:0:0:0 は、IPv6 アドレスがないことを示しています。たとえば、IPv6 ネットワーク上で新しく初期化されたノードは、IPv6 アドレスを受信するまで、パケットで未指定アドレスを送信元アドレスとして使用できます。

（注） IPv6 未指定アドレスは、インターフェイスに割り当てることができません。未指定 IPv6 アドレスを IPv6 パケットまたは IPv6 ルーティング ヘッダーで宛先アドレスとして使用することはできません。

ループバック アドレス

ループバック アドレス 0:0:0:0:0:0:0:1 は、ノードが IPv6 パケットをそれ自体に送信するために使用できます。IPv6 のループバック アドレスは、IPv4 のループバック アドレス（127.0.0.1）と同じように機能します。

（注） IPv6 ループバック アドレスは、物理インターフェイスに割り当てることができません。IPv6 ループバック アドレスを送信元アドレスまたは宛先アドレスとするパケットは、そのパケットを作成したノード内に留まっている必要があります。IPv6 ルータは、IPv6 ループバック アドレスを送信元アドレスまたは宛先アドレスとするパケットを転送しません。

インターフェイス識別子

IPv6 ユニキャスト アドレス内のインターフェイス識別子は、リンク上でインターフェイスを識別するために使用されます。これらの識別子は、サブネットプレフィックス内で固有である必要があります。多くの場合、インターフェイス識別子はインターフェイス リンク層アドレスから導出されます。各インターフェイスが異なるサブネットに接続されていれば、単一ノードの複数のインターフェイスで同一のインターフェイス識別子を使用することもできます。

バイナリ 000 で始まるものを除くすべてのユニキャストアドレスで、インターフェイス識別子は、64 ビットの長さで Modified EUI-64 形式で構築されている必要があります。Modified EUI-64 形式は、アドレス内のユニバーサル/ローカル ビットを逆にし、MAC アドレスの上の 3 つのバイトと下の 3 つのバイトの間に 16 進数 FFFE を挿入することによって、48 ビット MAC アドレスから作成されます。

たとえば、MAC アドレスが 00E0.b601.3B7A のインターフェイスの場合、64 ビット インターフェイス ID は 02E0:B6FF:FE01:3B7A になります。

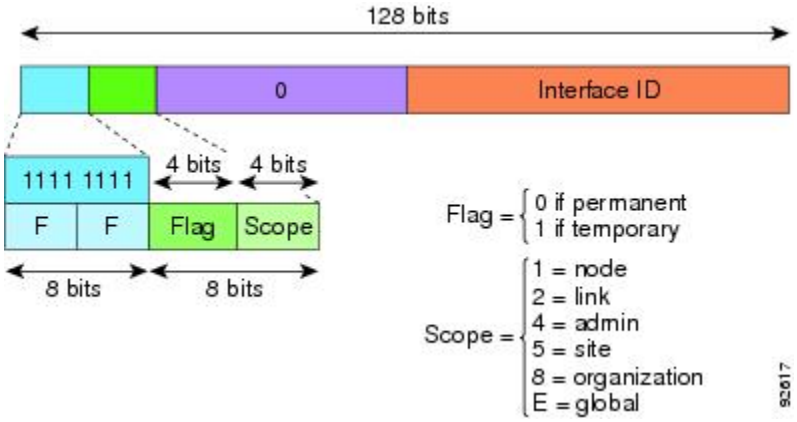
マルチキャスト アドレス

IPv6 マルチキャスト アドレスは、通常は異なるノード上にある、インターフェイスのグループの識別子です。マルチキャスト アドレスに送信されたパケットは、マルチキャスト アドレスが示すすべてのインターフェイスに配信されます。1 つのインターフェイスが任意の数のマルチキャスト グループに属すことができます。

IPv6 マルチキャスト アドレスのプレフィックスは FF00::/8（1111 1111）です。オクテットとそれに続くプレフィックスは、マルチキャストアドレスのタイプとスコープを定義します。永続的に割り当てられた（周知の）マルチキャストアドレスには、0 に等しいフラグ パラメータがあり、一時的な（過渡）マルチキャスト アドレスには 1 に等しいフラグ パラメータがあります。ノード、リンク、サイト、組織のスコープ、またはグローバル スコープを持つマルチ

キャスト アドレスのスコープ パラメータは、それぞれ 1、2、5、8、または E です。たとえば、プレフィックスが FF02::/16 のマルチキャスト アドレスは、リンク スコープを持つ永続マルチキャスト アドレスです。次の図に、IPv6 マルチキャスト アドレスの形式を示します。

図 *64 : IPv6* マルチキャスト アドレス形式



IPv6 ノード（ホストとルータ）は、次のマルチキャスト グループに参加する必要があります。

- All Nodes マルチキャスト アドレス：
  - FF01::（インターフェイスローカル）
  - FF02::（リンクローカル）
- ノード FF02:0:0:0:0:1:FFXX:XXXX/104 上の各 IPv6 ユニキャスト アドレスおよびエニーキャスト アドレスの送信要求ノード アドレス。ここで、XX:XXXX は低次 24 ビットのユニキャスト アドレスまたはエニーキャスト アドレスです。

（注） 送信要求ノードアドレスは、ネイバー送信要求メッセージで使用されます。

IPv6 ルータは、次のマルチキャスト グループに参加する必要があります。

- FF01::2（インターフェイスローカル）
- FF02::2（リンクローカル）
- FF05::2（サイトローカル）

マルチキャスト アドレスは、IPv6 パケットで送信元アドレスとして使用できません。

（注） IPv6 にはブロードキャスト アドレスはありません。ブロードキャスト アドレスの代わりに IPv6 マルチキャスト アドレスが使用されます。

エニーキャスト アドレス

IPv6 エニーキャスト アドレスは、複数のインターフェイス（通常は異なるノードに属す）に割り当てられたユニキャスト アドレスです。エニーキャスト アドレスにルーティングされたパケットは、そのアドレスを持ち、有効なルーティング プロトコルによって最も近いと判別されたインターフェイスにルーティングされます。

エニーキャスト アドレスは、ユニキャスト アドレス空間から割り当てられます。エニーキャスト アドレスは、複数のインターフェイスに割り当てられたユニキャスト アドレスにすぎません。インターフェイスは、アドレスをエニーキャストアドレスとして認識するように設定されている必要があります。

エニーキャスト アドレスには次の制限が適用されます。

- エニーキャスト アドレスは、IPv6 パケットの送信元アドレスとして使用できません。
- エニーキャスト アドレスは、IPv6 ホストに割り当てることはできません。IPv6 ルータにだけ割り当てるこができます。

（注） ASA では、エニーキャスト アドレスをサポートされていません。

必須アドレス

IPv6 ホストには、少なくとも次のアドレスが（自動または手動で）設定されている必要があります。

- 各インターフェイスのリンクローカル アドレス
- ループバック アドレス
- All-Nodes マルチキャスト アドレス
- 各ユニキャスト アドレスまたはエニーキャスト アドレスの送信要求ノード マルチキャスト アドレス

IPv6 ルータには、少なくとも次のアドレスが（自動または手動で）設定されている必要があります。

- 必須ホスト アドレス
- このルータがルータとして動作するように設定されているすべてのインターフェイスのサブネットルータ エニーキャスト アドレス
- All-Routers マルチキャスト アドレス

IPv6 アドレス プレフィックス

IPv6 アドレス プレフィックスは、ipv6-prefix/prefix-length の形式で、アドレス空間全体のビット連続ブロックを表すために使用できます。IPv6-prefix は、RFC 2373 に記述されている形式にする必要があります。コロン区切りの 16 ビット値を使用して、アドレスを 16 進数で指定します。プレフィックス長は、アドレスの高次の連続ビットのうち、何個がプレフィックス（アドレスのネットワーク部分）を構成しているかを指定する 10 進数値です。たとえば、2001:0DB8:8086:6502::/32 は有効な IPv6 プレフィックスです。

IPv6 プレフィックスは、IPv6 アドレスのタイプを特定します。次の表に、各 IPv6 アドレス タイプのプレフィックスを示します。

表 *64 : IPv6* アドレス タイプのプレフィックス

アドレスタイプ	バイナリ プレフィックス	IPv6 表記
未指定	000...0（128 ビット）	::/128
ループバック	000...1（128 ビット）	::1/128
マルチキャスト	11111111	FF00::/8
リンクローカル（ユニキャスト）	1111111010	FE80::/10
サイトローカル（ユニキャスト）	1111111111	FEC0::/10
グローバル（ユニキャスト）	その他すべてのアドレス。	
エニーキャスト	ユニキャスト アドレス空間から取得。	

プロトコルとアプリケーション

次の表に、プロトコルのリテラル値とポート番号を示します。いずれも ASA のコマンドで入力できます。

表 *65 :* プロトコルのリテラル値

リテラル	値	説明
ah	51	IPv6 の認証ヘッダー（RFC 1826）。
eigrp	88	Enhanced Interior Gateway Routing Protocol（Enhanced IGRP）。
esp	50	IPv6 の暗号ペイロード（RFC 1827）。
gre	47	総称ルーティング カプセル化。

リテラル	値	説明
icmp	1	インターネット制御メッセージ プロトコル（RPC 792）。
icmp6	58	IPv6 のインターネット制御メッセージ プロトコル（RFC 2463）。
igmp	2	インターネット グループ管理プロトコル（RFC 1112）。
igrp	9	Interior Gateway Routing Protocol。
ip	0	インターネット プロトコル。
ipinip	4	IP-in-IP カプセル化。
ipsec	50	IP セキュリティ。ipsec プロトコル リテラルを入力すると、esp プロトコル リテラルを入力した場合と同じ結果が得られます。
nos	94	ネットワーク オペレーティング システム（Novell の NetWare）。
ospf	89	OSPF ルーティング プロトコル（RFC 1247）。
pcp	108	ペイロード圧縮プロトコル。
pim	103	プロトコル独立型マルチキャスト。
pptp	47	ポイントツーポイント トンネリング プロトコル。pptp プロトコル リテラルを入力すると、gre プロトコル リテラルを入力した場合と同じ結果が得られます。
snp	109	Sitara Networks Protocol。
tcp	6	伝送制御プロトコル（RFC 793）。
udp	17	ユーザ データグラム プロトコル（RFC 768）。

IANA の Web サイトでオンラインでプロトコル番号を確認できます。

http://www.iana.org/assignments/protocol-numbers

TCP ポートおよび UDP ポート

次の表に、リテラル値とポート番号を示します。いずれも ASA のコマンドで入力できます。次の警告を参照してください。

- ASA は、SQL*Net 用にポート 1521 を使用します。これは、Oracle が SQL*Net に使用するデフォルトのポートです。ただし、この値は IANA ポート割り当てとは一致しません。
- ASA は、ポート 1645 と 1646 で RADIUS をリッスンしています。RADIUS サーバが標準ポート 1812 と 1813 を使用している場合は、**authentication-port** コマンドと **accounting-port** コマンドを使用して、それらのポートでリッスンするように ASA を設定できます。

- DNSアクセスにポートを割り当てるには、**dns**ではなく**domain**リテラル値を使用します。**dns** を使用した場合、ASA では、**dnsix** リテラル値を使用すると見なされます。

IANA の Web サイトでオンラインでポート番号を確認できます。

http://www.iana.org/assignments/port-numbers

表 *66 :* ポートのリテラル値

リテラル	**TCP** または **UDP**	値	説明
aol	TCP	5190	America Online
bgp	TCP	179	ボーダー ゲートウェイ プロトコル（RFC 1163）
biff	UDP	512	新しいメールの受信をユーザに通知するために、メール システムが使用
bootpc	UDP	68	ブートストラップ プロトコル クライアント
bootps	UDP	67	ブートストラップ プロトコル サーバ
chargen	TCP	19	キャラクタ ジェネレータ
cifs	TCP、UDP	3020	Common Internet File System
citrix-ica	TCP	1494	Citrix Independent Computing Architecture（ICA）プロトコル
cmd	TCP	514	cmd は自動認証機能がある点を除いて、exec と同様。
ctiqbe	TCP	2748	Computer Telephony Interface Quick Buffer Encoding
daytime	TCP	13	Day time（日時）（RFC 867）
discard	TCP、UDP	9	廃棄
dnsix	UDP	195	DNSIX Session Management Module Audit Redirector
domain	TCP、UDP	53	DNS
echo	TCP、UDP	7	Echo
exec	TCP	512	リモート プロセスの実行
finger	TCP	79	Finger
ftp	TCP	21	ファイル転送プロトコル（コンソールポート）

リテラル	TCP または UDP	値	説明
ftp-data	TCP	20	ファイル転送プロトコル（データ ポート）
gopher	TCP	70	Gopher
h323	TCP	1720	H.323 発呼信号
hostname	TCP	101	NIC ホスト ネーム サーバ
http	TCP、UDP	80	World Wide Web HTTP
https	TCP	443	HTTP over SSL
ident	TCP	113	ID 認証サービス
imap4	TCP	143	Internet Message Access Protocol バージョン 4
irc	TCP	194	インターネット リレー チャット プロトコル
isakmp	UDP	500	Internet Security Association and Key Management Protocol
kerberos	TCP、UDP	750	Kerberos
klogin	TCP	543	KLOGIN
kshell	TCP	544	Korn シェル
ldap	TCP	389	Lightweight Directory Access Protocol。
ldaps	TCP	636	ライトウェイトディレクトリ アクセス プロトコル（SSL）
login	TCP	513	リモート ログイン
lotusnotes	TCP	1352	IBM Lotus Notes
lpd	TCP	515	ライン プリンタ デーモン（プリンタ スプーラー）
mobile-ip	UDP	434	モバイル IP-Agent
nameserver	UDP	42	ホスト ネーム サーバ
netbios-dgm	UDP	138	NetBIOS データグラム サービス
netbios-ns	UDP	137	NetBIOS ネーム サービス
netbios-ssn	TCP	139	NetBIOS セッション サービス

リテラル	TCP または UDP	値	説明
nfs	TCP、UDP	2049	ネットワーク ファイル システム（Sun Microsystems）
nntp	TCP	119	Network News Transfer Protocol
ntp	UDP	123	ネットワーク タイム プロトコル
pcanywhere-data	TCP	5631	pcAnywhere データ
pcanywhere-status	UDP	5632	pcAnywhere ステータス
pim-auto-rp	TCP、UDP	496	Protocol Independent Multicast、逆パス フラッド、デンス モード
pop2	TCP	109	Post Office Protocol（POP）Version 2
pop3	TCP	110	Post Office Protocol - Version 3
pptp	TCP	1723	ポイントツーポイント トンネリング プロトコル
radius	UDP	1645	リモート認証ダイヤルイン ユーザ サービス
radius-acct	UDP	1646	リモート認証ダイヤルイン ユーザ サービス（アカウンティング）
rip	UDP	520	ルーティング情報プロトコル
rsh	TCP	514	リモート シェル
rtsp	TCP	554	Real Time Streaming Protocol
secureid-udp	UDP	5510	SecureID over UDP
sip	TCP、UDP	5060	Session Initiation Protocol
smtp	TCP	25	シンプル メール転送プロトコル
snmp	UDP	161	簡易ネットワーク管理プロトコル
snmptrap	UDP	162	簡易ネットワーク管理プロトコル（トラップ）
sqlnet	TCP	1521	構造化照会言語ネットワーク
ssh	TCP	22	セキュア シェル
sunrpc	TCP、UDP	111	Sun Remote Procedure Call
syslog	UDP	514	システム ログ

リテラル	TCP または UDP	値	説明
tacacs	TCP、UDP	49	Terminal Access Controller Access Control System Plus
talk	TCP、UDP	517	Talk
Telnet	TCP	23	Telnet（RFC 854）
tftp	UDP	69	『Trivial File Transfer Protocol』
time	UDP	37	時刻
uucp	TCP	540	UNIX 間コピー プログラム
vxlan	UDP	4789	Virtual eXtensible Local Area Network（VXLAN）
who	UDP	513	Who
whois	TCP	43	Who Is
www	TCP、UDP	80	ワールドワイド ウェブ
xdmcp	UDP	177	X Display Manager Control Protocol

ローカル ポートとプロトコル

次の表に、ASA に向かうトラフィックを処理するために ASA が開くプロトコル、TCP ポート、および UDP ポートを示します。この表に記載されている機能とサービスをイネーブルにしない限り、ASA は、TCP または UDP ポートでローカル プロトコルを開きません。ASA がデフォルトのリスニング プロトコルまたはポートを開くように機能またはサービスを設定する必要があります。多くの場合、機能またはサービスをイネーブルにすると、デフォルト ポート以外のポートを設定できます。

表 *67*：機能とサービスによって開かれるプロトコルとポート

機能またはサービス	プロトコル	Port Number	注
DHCP	UDP	67、68	—
フェールオーバー制御	105	該当なし	—
HTTP	TCP	80	—
HTTPS	TCP	443	—
ICMP	1	該当なし	—

機能またはサービス	プロトコル	Port Number	注
IGMP	2	該当なし	プロトコルは宛先 IP アドレス 224.0.0.1 でだけ開かれます
ISAKMP/IKE	UDP	500	設定可能。
IPsec（ESP）	50	該当なし	—
IPsec over UDP（NAT-T）	UDP	4500	—
IPsec over TCP（CTCP）	TCP	—	デフォルト ポートは使用されません。IPsec over TCP の設定時にポート番号を指定する必要があります。
NTP	UDP	123	—
OSPF	89	該当なし	プロトコルは宛先 IP アドレス 224.0.0.5 および 224.0.0.6 でだけ開かれます
PIM	103	該当なし	プロトコルは宛先 IP アドレス 224.0.0.13 でだけ開かれます
RIP	UDP	520	—
RIPv2	UDP	520	ポートは宛先 IP アドレス 224.0.0.9 でだけ開かれます
SNMP	UDP	161	設定可能。
SSH	TCP	22	—
ステートフルアップデート	8（ノンセキュア）9（セキュア）	該当なし	—
Telnet	TCP	23	—
VPN ロードバランシング	UDP	9023	設定可能。
VPN 個別ユーザ認証プロキシ	UDP	1645、1646	ポートは VPN トンネルでだけアクセスできます。

ICMP タイプ

次の表に、ASA のコマンドで入力できる ICMP タイプの番号と名前を示します。

表 *68 : ICMP* タイプ

ICMP 番号	ICMP 名
0	echo-reply
3	unreachable
4	source-quench
5	redirect
6	alternate-address
8	echo
9	router-advertisement
10	router-solicitation
11	time-exceeded
12	parameter-problem
13	timestamp-request
14	timestamp-reply
15	information-request
16	information-reply
17	mask-request
18	mask-reply
30	traceroute
31	conversion-error
32	mobile-redirect