RADIUS の設定

- RADIUS を設定するための前提条件 （1 ページ）
- RADIUS の設定に関する制約事項 （2 ページ）
- RADIUS に関する情報 （3 ページ）
- RADIUS の設定 （30 ページ）
- CoA 機能のモニタリング （47 ページ）
- RADIUS の機能の履歴 （48 ページ）

RADIUS を設定するための前提条件

ここでは、RADIUS によるdevice アクセスの制御の前提条件を示します。

全般：

- この章のいずれかのコンフィギュレーション コマンドを使用するには、RADIUSおよび認証、許可、ならびにアカウンティング（AAA）を有効にする必要があります。
- RADIUS は、AAA を介して実装され、AAA コマンドを使用してのみ有効にできます。
- **aaa new-model** グローバル コンフィギュレーション コマンドを使用して、AAA を有効にします。
- **aaa authentication** グローバル コンフィギュレーション コマンドを使用して、RADIUS 認証の方式リストを定義します。
- **line** および **interface** コマンドを使用して、使用する定義済みの方式リストを有効にします。
- 最低限、RADIUS サーバ ソフトウェアが稼働するホスト（1 つまたは複数）を特定し、RADIUS認証の方式リストを定義する必要があります。また、任意でRADIUS許可およびアカウンティングの方式リストを定義できます。
- device上で RADIUS 機能の設定を行う前に、RADIUS サーバにアクセスし、サーバを設定する必要があります。

- RADIUS ホストは、通常、シスコ（Cisco Secure Access Control Server バージョン 3.0）、Livingston、Merit、Microsoft、または他のソフトウェア プロバイダーの RADIUS サーバ ソフトウェアが稼働しているマルチユーザ システムです。詳細については、RADIUS サーバのマニュアルを参照してください。
- Change-of-Authorization（CoA）インターフェイスを使用するには、スイッチにセッションがすでに存在している必要があります。CoA を使用すると、セッションの識別と接続解除要求を実行できます。アップデートは、指定されたセッションにだけ作用します。

RADIUS の動作：

- ユーザーは RADIUS 許可に進む前に、まず RADIUS 認証を正常に完了する必要があります（有効になっている場合）。
- RADIUS over IPv6 構成の場合、ユーザーは **ipv6 unicast-routing** コマンドを有効にして、IPv6 ユニキャストルーティングを有効にする必要があります。

RADIUS の設定に関する制約事項

全般：

- セキュリティの失効を防止するため、ネットワーク管理アプリケーションを使用して RADIUS を設定することはできません。
- RADIUS および AAA サーバーは、標準のデフォルトポートでのみ実行するように設定できます。
  - 1812 および 1813
  - 1645 および 1646

RADIUS は次のネットワーク セキュリティ状況には適していません。

- マルチプロトコルアクセス環境。RADIUS は、AppleTalk Remote Access（ARA）、NetBIOS Frame Control Protocol（NBFCP）、NetWare Asynchronous Services Interface（NASI）、または X.25 PAD 接続をサポートしません。
- スイッチ間またはルータ間状態。RADIUS は、双方向認証を行いません。RADIUS は、他社製のデバイスが認証を必要とする場合に、あるデバイスから他社製のデバイスへの認証に使用できます。
- 各種のサービスを使用するネットワーク。RADIUS は、一般に 1 人のユーザを 1 つのサービス モデルにバインドします。

RADIUS パケットの DSCP マーキングサポート：

- 認証とアカウンティングの DSCP マーキングは、プライベートサーバー、完全修飾ドメイン名（FQDN）サーバー、および radsec サーバーではサポートされていません。

- 有線IEEE 802.1x認証の場合、送信元ポート拡張が有効になっていないと、デフォルトポートが使用されます。DSCP マーキングはデフォルトポートに設定され、すべての要求は同じ DSCP 値でマーキングされます。
- 送信元ポート拡張がデフォルトで有効になっている無線 IEEE 802.1x 認証の場合、DSCP マーキングはサポートされません。

RADIUS に関する情報

RADIUS およびスイッチ アクセス

この項では、RADIUS を有効にし、設定する方法について説明します。RADIUS を使用すると、アカウンティングの詳細を取得したり、認証および許可プロセスの柔軟な管理制御を実現できます。

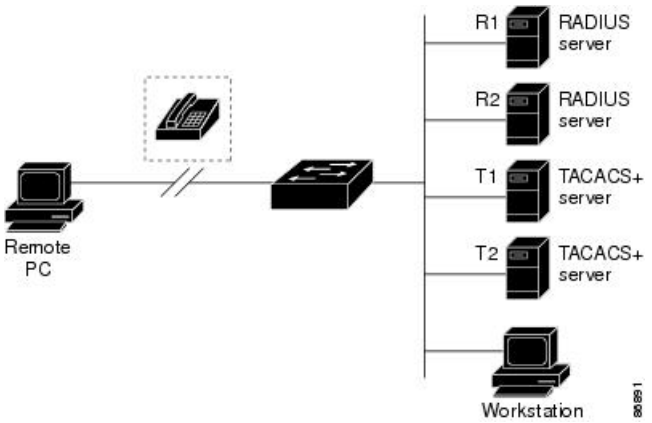
RADIUS の概要

RADIUS は、不正なアクセスからネットワークのセキュリティを保護する分散クライアント/サーバ システムです。RADIUS クライアントは、サポート対象のシスコ デバイス上で稼働します。クライアントは中央の RADIUS サーバに認証要求を送ります。中央の RADIUS サーバにはすべてのユーザ認証情報、ネットワーク サービス アクセス情報が登録されています。

RADIUS は、アクセスのセキュリティが必要な、次のネットワーク環境で使用します。

- それぞれが RADIUS をサポートする、マルチベンダー アクセス サーバによるネットワーク。たとえば、複数のベンダーのアクセス サーバが、1 つの RADIUS サーバベース セキュリティ データベースを使用します。複数ベンダーのアクセス サーバからなる IP ベースのネットワークでは、ダイヤルイン ユーザは RADIUS サーバを通じて認証されます。RADIUS サーバは、Kerberos セキュリティ システムで動作するようにカスタマイズされています。
- アプリケーションが RADIUS プロトコルをサポートするターンキー ネットワーク セキュリティ環境。たとえば、スマート カード アクセス コントロール システムを使用するアクセス環境。
- すでに RADIUS を使用中のネットワーク。RADIUS クライアント装備のシスコ deviceをネットワークに追加できます。これが TACACS+ サーバへの移行の最初のステップとなることもあります。下の図 「RADIUS サービスから TACACS+ サービスへの移行」を参照してください。

図 *1 : RADIUS* サービスから *TACACS+* サービスへの移行



- ユーザが 1 つのサービスにしかアクセスできないネットワーク。RADIUS を使用すると、ユーザのアクセスを 1 つのホスト、Telnet などの 1 つのユーティリティ、または IEEE 802.1x などのプロトコルを使用するネットワークに制御できます。このプロトコルの詳細については、「IEEE 802.1x ポートベースの認証の設定」を参照してください。
- リソース アカウンティングが必要なネットワーク。RADIUS 認証または許可とは別個に RADIUS アカウンティングを使用できます。RADIUS アカウンティング機能によって、サービスの開始および終了時点でデータを送信し、このセッション中に使用されるリソース（時間、パケット、バイトなど）の量を表示できます。インターネット サービス プロバイダーは、RADIUS アクセス コントロールおよびアカウンティング ソフトウェアのフリーウェア バージョンを使用して、特殊なセキュリティおよび課金に対するニーズを満たすこともできます。

RADIUS の動作

RADIUS サーバによってアクセス コントロールされるdeviceに、ユーザがログインおよび認証を試みると、次のイベントが発生します。

1. ユーザ名およびパスワードの入力を要求するプロンプトが表示されます。
2. ユーザ名および暗号化されたパスワードが、ネットワーク経由でRADIUSサーバに送信されます。
3. ユーザは、RADIUS サーバから次のいずれかの応答を受信します。
   - ACCEPT：ユーザーが認証されたことを表します。
   - REJECT：ユーザーの認証が失敗し、ユーザー名およびパスワードの再入力が要求されるか、またはアクセスが拒否されます。
   - CHALLENGE：ユーザーに追加データを要求します。
   - CHALLENGE PASSWORD：ユーザーは新しいパスワードを選択するように要求されます。

ACCEPT または REJECT 応答には、特権 EXEC またはネットワーク許可に使用する追加データがバンドルされています。ACCEPT または REJECT パケットには次の追加データが含まれます。

- Telnet、SSH、rlogin、または特権 EXEC サービス
- 接続パラメータ（ホストまたはクライアントの IP アドレス、アクセス リスト、およびユーザ タイムアウトを含む）

RADIUS 許可の変更

RADIUS 許可の変更（CoA）は、認証、認可、およびアカウンティング（AAA）セッションの属性を認証された後に変更するためのメカニズムを提供します。AAA でユーザー、またはユーザー グループのポリシーが変更された場合、管理者は、AAA サーバーから Cisco Secure Access Control Server（ACS）などの RADIUS CoA パケットを送信し、認証を再初期化して新しいポリシーを適用することができます。このセクションでは、使用可能なプリミティブおよびそれらの CoA での使用方法を含む、RADIUS インターフェイスの概要について説明します。

- Change-of-Authorization 要求
- CoA 要求応答コード
- CoA 要求コマンド
- セッション再認証
- セッション強制終了のスタック構成ガイドライン

標準 RADIUS インターフェイスは通常、ネットワークに接続しているデバイスから要求が送信され、クエリーが送信されたサーバーが応答するプル モデルで使用されます。シスコ デバイスは、RFC 5176 で規定された（通常はプッシュモデルで使用される）RADIUS CoA 拡張機能をサポートし、外部の AAA またはポリシーサーバーからのセッションを動的に再設定できるようにします。

シスコ デバイスは、次のセッション単位の CoA 要求をサポートしています。

- セッション再認証
- セッションの終了
- ポート シャットダウンでのセッション終了
- ポート バウンスでのセッション終了

この機能は、Cisco Secure Access Control Server（ACS）5.1 に統合されています。

シスコデバイスで、RADIUS インターフェイスはデフォルトで有効に設定されています。ただし、次の属性については、一部の基本的な設定が必要になります。

- セキュリティおよびパスワード：このガイドの「スイッチへの不正アクセスの防止」を参照してください。

- アカウンティング：このガイドの「スイッチベース認証の設定」の章の「RADIUS アカウンティングの起動」の項を参照してください。

Cisco IOS XE ソフトウェアは、RFC 5176 で定義されている RADIUS CoA の拡張をサポートします。この拡張は、一般に、外部 AAA またはポリシーサーバーからのセッションの動的な再構成を可能にするプッシュモデルで使用されます。セッションの特定、セッションの終了、ホストの再認証、ポートのシャットダウン、およびポートバウンスでは、セッションごとの CoA 要求がサポートされます。このモデルは、次のように、1 つの要求（CoA-Request）と 2 つの考えられる応答コードで構成されます。

- CoA acknowledgement（ACK）[CoA-ACK]
- CoA nonacknowledgement（NAK）[CoA-NAK]

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

次の表は、Identity-Based Networking Services でサポートされている RADIUS CoA コマンドとベンダー固有属性（VSA）を示します。すべての CoA コマンドには、デバイスと CoA クライアント間のセッション ID が含まれている必要があります。

表 *1 : Identity-Based Networking Services* でサポートされている *RADIUS CoA* コマンド

CoA コマンド	**シスコの VSA**
Activate service	Cisco:Avpair=“subscriber:command=activate-service” Cisco:Avpair=“subscriber:service-name=<*service-name*>” Cisco:Avpair=“subscriber:precedence=<*precedence-number*>” Cisco:Avpair=“subscriber:activation-mode=replace-all”
Deactivate service	Cisco:Avpair=“subscriber:command=deactivate-service” Cisco:Avpair=“subscriber:service-name=<*service-name*>”
Bounce host port	Cisco:Avpair="subscriber:command=bounce-host-port"
Disable host port	Cisco:Avpair="subscriber:command=disable-host-port"
Session query	Cisco:Avpair=“subscriber:command=session-query”
Session reauthenticate	Cisco:Avpair="subscriber:command=reauthenticate" Cisco:Avpair=“subscriber:reauthenticate-type=last” または Cisco:Avpair=“subscriber:reauthenticate-type=rerun”
Session terminate	これは、VSA を必要としない、標準の接続解除要求です。
Interface template	Cisco:AVpair="interface-template-name=<*interfacetemplate*>"

Change-of-Authorization 要求

Change of Authorization（CoA）要求は、RFC 5176 に記載されているように、プッシュ モデルで使用することによって、セッション識別、ホスト再認証、およびセッション終了を行うことができます。このモデルは、1 つの要求（CoA-Request）と 2 つの可能な応答コードで構成されています。

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

要求は CoA クライアント（通常は RADIUS またはポリシー サーバー）から発信されて、リスナーとして動作するスイッチに送信されます。

RFC 5176 規定

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

次の表に、この機能でサポートされている IETF 属性を示します。

表 *2 :* サポートされている *IETF* 属性

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

次の表に、Error-Cause 属性で取ることができる値を示します。

表 *3 : Error-Cause* の値

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

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

CoA 要求応答コード

CoA 要求応答コードを使用すると、スイッチにコマンドを伝達できます。

RFC 5176 で定義されている CoA 要求応答コードのパケットの形式は、コード、ID、長さ、オーセンティケータ、およびタイプ、長さ、値（TLV）形式の属性から構成されます。属性フィールドは、シスコのベンダー固有属性（VSA）を送信するために使用します。

セッションの識別

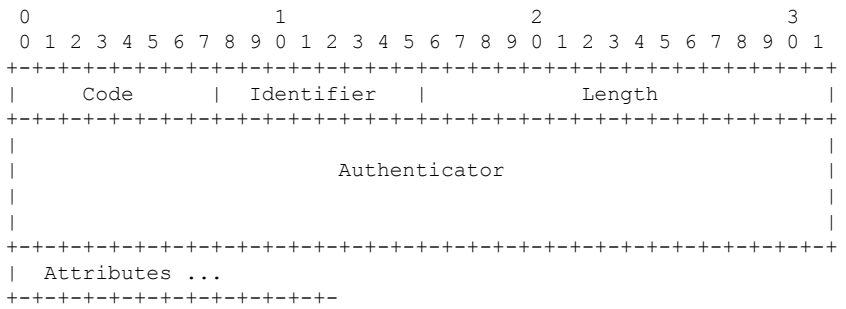
特定のセッションに向けられた切断と CoA 要求については、スイッチは 1 つ以上の次の属性に基づいて、セッションを検索します。

- Acct-Session-Id（IETF 属性 #44）
- Audit-Session-Id VSA（シスコの VSA）
- Calling-Station-Id（ホスト MAC アドレスを含む IETF 属性 #31）
- 次のいずれかの IPv6 属性。
  - Framed-IPv6-Prefix（IETF 属性 #97）および Framed-Interface-Id（IETF 属性 #96）。ともに RFC 3162 に従った完全な IPv6 アドレスを作成する
  - Framed-IPv6-Address
- プレーン IP アドレス（IETF 属性 #8）

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

複数のセッション ID 属性がメッセージ含まれる場合は、すべての属性がセッションと一致しなければなりません。そうでない場合は、スイッチが Disconnect - negative acknowledgement（NAK）または CoA -NAK と、「Invalid Attribute Value」エラー コードを返します。

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



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

特定の適用ポリシーを対象とする CoA 要求の場合、上記のセッション ID 属性のいずれかがメッセージに含まれていると、デバイスはエラー コードが「Invalid Attribute Value」の CoA-NAK を返します。

CoA ACK 応答コード

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

CoA NAK 応答コード

否定応答（NAK）は許可ステートの変更に失敗したことを示し、エラーの理由を示す属性を含めることができます。CoA が成功したかを確認するには、**show** コマンドを使用します。

CoA 要求コマンド

表 *4*：サポートされる *CoA* コマンド

コマンド [1]	シスコの VSA
Reauthenticate host	Cisco:Avpair="subscriber:command=reauthenticate"
Terminate session	これは、VSA を要求しない、標準の接続解除要求です。
Bounce host port	Cisco:Avpair="subscriber:command=bounce-host-port"

コマンド [1]	シスコの VSA
Disable host port	Cisco:Avpair="subscriber:command=disable-host-port"

[1] すべての CoA コマンドには、デバイスと CoA クライアント間のセッション ID が含まれている必要があります。

セッション再認証

不明な ID またはポスチャを持つホストがネットワークに加入して、制限されたアクセス許可プロファイル（たとえば、ゲスト VLAN）に関連付けられると、AAA サーバーは通常、セッション再認証要求を生成します。再認証要求は、クレデンシャルが不明である場合にホストが適切な認証グループに配置されることを許可します。

セッション認証を開始するために、AAA サーバーは Cisco:Avpair="subscriber:command=reauthenticate" の形式で Cisco VSA と 1 つ以上のセッション ID 属性を含む標準 CoA 要求メッセージを送信します。

現在のセッション ステートは、メッセージに対するスイッチの応答を決定します。セッションが現在、IEEE 802.1x によって認証されている場合、スイッチは EAPOL（LAN 経由の拡張認証プロトコル）RequestId メッセージをサーバーに送信することで応答します。

現在、セッションが MAC 認証バイパス（MAB）で認証されている場合は、スイッチはサーバーにアクセス要求を送信し、初期正常認証で使用されるものと同じ ID 属性を渡します。

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

セッションがまだ認証されてない、あるいはゲスト VLAN、クリティカル VLAN、または同様のポリシーで認証されている場合は、再認証メッセージがアクセス コントロール方式を再開し、最初に試行されるように設定された方式で開始します。セッションの現在の許可は、再認証によって異なる認証結果になるまで維持されます。

セッションの終了

セッションを終了させる 3 種類の CoA 要求があります。CoA 接続解除要求は、ホストポートを無効にせずにセッションを終了します。このコマンドを使用すると、指定されたホストのオーセンティケータ ステート マシンが再初期化されますが、そのホストのネットワークへのアクセスは制限されません。

ホストのネットワークへのアクセスを制限するには、Cisco:Avpair="subscriber:command=disable-host-port" VSA の設定で CoA 要求を使用します。このコマンドは、ネットワーク上で障害を引き起こしたと認識されているホストがある場合に便利であり、そのホストに対してネットワーク アクセスをただちにブロックする必要があります。ポートへのネットワークアクセスを復旧する場合は、非 RADIUS メカニズムを使用して再び有効にします。

プリンタなどのサプリカントを持たないデバイスが新しい IP アドレスを取得する必要がある場合（たとえば、VLAN変更後）は、ポートバウンスでホストポート上のセッションを終了します（ポートを一時的に無効した後、再び有効にする）。

CoA 接続解除要求

このコマンドは標準の接続解除要求です。セッションが見つからない場合、デバイスは「Session Context Not Found」エラー コード属性を使用して Disconnect-NAK メッセージを返します。セッションが見つかった場合、デバイスはセッションを終了します。セッションが完全に削除されると、デバイスは Disconnect-ACK を返します。

デバイスがクライアントに接続解除 ACK を返す前にスタンバイデバイスにフェールオーバーする場合は、クライアントから要求が再送信される際に、新しいアクティブデバイス上でそのプロセスが繰り返されます。再送信後もセッションが見つからない場合は、Disconnect-ACK と「Session Context Not Found」エラー コード属性が送信されます。

CoA 要求：ホストポートの無効化

RADIUS サーバーの CoA disable port コマンドを実行すると、セッションをホストしている認証ポートが管理的にシャットダウンされます。その結果、セッションは終了します。このコマンドは、ホストがネットワーク上で問題を起こしていることを把握し、ホストのネットワークアクセスを即座にブロックする必要がある場合に便利です。ポートのネットワークアクセスを復元するには、非RADIUSメカニズムを使用して再び有効にします。このコマンドは、次の新しいベンダー固有属性（VSA）が含まれている標準 CoA 要求メッセージで伝達されます。

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

このコマンドはセッション指向であるため、「セッション ID」セクションに示されている 1 つ以上のセッション ID 属性とともに使用する必要があります。セッションが見つからない場合、デバイスは「Session Context Not Found」エラー コード属性を使用して CoA-NAK メッセージを返します。このセッションがある場合は、デバイスはホストポートを無効にし、CoA-ACK メッセージを返します。

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

（注） 再送信コマンドの後に接続解除要求が失敗すると、（接続解除ACKが送信されてない場合に）チェンジオーバー前にセッションが正常終了するか、または元のコマンドが実行されてスタンバイデバイスがアクティブになるまでの間に発生した他の方法（たとえば、リンク障害）によりセッションが終了することがあります。

CoA 要求：バウンス ポート

RADIUS サーバーの CoA bounce port が RADIUS サーバーから送信されると、認証ポートでリンクのフラップが発生します。その結果、このポートに接続している1つまたは複数のホストから、DHCP の再ネゴシエーションが開始されます。この状況は、VLAN の変更があり、この

認証ポートに関する変化を検出するメカニズムがないデバイス（プリンタなど）がエンドポイントの場合に発生する可能性があります。CoA bounce port は、次の新しい VSA を含む標準の CoA-Request メッセージで伝達されます。

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

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

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

RADIUS のデフォルト設定

RADIUS および AAA は、デフォルトでは無効に設定されています。

セキュリティの失効を防止するため、ネットワーク管理アプリケーションを使用して RADIUS を設定することはできません。RADIUS を有効にすると、CLI 経由でデバイスにアクセスするユーザーを認証できます。

RADIUS サーバ ホスト

デバイスと RADIUS サーバー間の通信には、次の要素が関係します。

- ホスト名または IP アドレス
- 認証の宛先ポート
- アカウンティングの宛先ポート
- 鍵文字列
- タイムアウト時間
- 再送信回数

RADIUS セキュリティ サーバは、ホスト名または IP アドレス、ホスト名と特定の UDP ポート番号、または IP アドレスと特定の UDP ポート番号によって特定します。IP アドレスと UDP ポート番号の組み合わせによって、一意の ID が作成され、特定の AAA サービスを提供する RADIUS ホストとして個々のポートを定義できます。この一意の ID を使用することによって、同じ IP アドレスにあるサーバ上の複数の UDP ポートに、RADIUS 要求を送信できます。

同じ RADIUS サーバー上の異なる 2 つのホスト エントリに同じサービス（たとえばアカウンティング）を設定した場合、2 番めに設定したホストエントリは、最初に設定したホストエントリのフェールオーバーバックアップとして動作します。この例では、最初のホストエントリ

がアカウンティングサービスを提供できなかった場合、デバイスは「%RADIUS-4-RADIUS_DEAD」メッセージを表示し、その後、同じデバイス上で 2 番目に設定されたホストエントリでアカウンティングサービスを試みます（RADIUS ホスト エントリは、設定した順序に従って試行されます）。

RADIUS サーバーとデバイスは、共有秘密テキスト文字列を使用して、パスワードの暗号化および応答の交換を行います。RADIUS で AAA セキュリティコマンドを使用するように設定するには、RADIUS サーバーデーモンが稼働するホストと、そのホストがデバイスと共有する秘密テキスト（鍵）文字列を指定する必要があります。

タイムアウト、再送信回数、および暗号鍵の値は、すべての RADIUS サーバーに対してグローバルに設定することもできますし、サーバー単位で設定することもできます。また、グローバルな設定とサーバー単位での設定を組み合わせることもできます。

RADIUS ログイン認証

AAA 認証を設定するには、認証方式の名前付きリストを作成してから、各種ポートにそのリストを適用します。方式リストは実行される認証のタイプと実行順序を定義します。このリストを特定のポートに適用してから、定義済み認証方式を実行する必要があります。唯一の例外は、デフォルトの方式リストです。デフォルトの方式リストは、名前付き方式リストを明示的に定義されたインターフェイスを除いて、自動的にすべてのポートに適用されます。

方式リストは、ユーザ認証のためクエリ送信を行う手順と認証方式を記述したものです。認証に使用する 1 つまたは複数のセキュリティ プロトコルを指定できるので、最初の方式が失敗した場合のバックアップ システムが確保されます。ソフトウェアは、リスト内の最初の方式を使用してユーザを認証します。その方式で応答が得られなかった場合、ソフトウェアはそのリストから次の認証方式を選択します。このプロセスは、リスト内の認証方式による通信が成功するか、定義された方式をすべて試し終わるまで繰り返されます。この処理のある時点で認証が失敗した場合（つまり、セキュリティ サーバまたはローカルのユーザ名データベースがユーザ アクセスを拒否すると応答した場合）、認証プロセスは停止し、それ以上認証方式が試行されることはありません。

AAA サーバグループ

既存のサーバ ホストを認証用にグループ化するため、AAA サーバ グループを使用するようにデバイスを設定できます。設定済みのサーバ ホストのサブセットを選択して、それを特定のサービスに使用します。サーバ グループは、選択されたサーバ ホストの IP アドレスのリストを含むグローバルなサーバ ホスト リストとともに使用されます。

サーバ グループには、同じサーバの複数のホスト エントリを含めることもできますが、各エントリが一意の ID（IP アドレスと UDP ポート番号の組み合わせ）を持っていることが条件です。この場合、個々のポートをそれぞれ特定の AAA サービスを提供する RADIUS ホストとして定義できます。この一意の ID を使用することによって、同じ IP アドレスにあるサーバ上の異なる UDP ポートに、RADIUS 要求を送信できます。同じ RADIUS サーバ上の異なる 2 つのホストエントリに同じサービス（たとえばアカウンティング）を設定した場合、2 番めに設定したホスト エントリは、最初に設定したホスト エントリのフェールオーバー バックアップとして動作します。最初のホスト エントリがアカウンティング サービスの提供に失敗すると、

ネットワーク アクセス サーバは同じデバイスに設定されている 2 番めのホスト エントリを使用してアカウンティング サービスを提供するように試行します。（試行される RADIUS ホスト エントリの順番は、設定されている順序に従います）。

AAA 許可

AAA 許可によってユーザが使用できるサービスが制限されます。AAA 許可が有効になっていると、デバイスはユーザのプロファイルから取得した情報を使用します。このプロファイルは、ローカルのユーザデータベースまたはセキュリティサーバ上にあり、ユーザのセッションを設定します。ユーザは、ユーザプロファイル内の情報で認められている場合に限り、要求したサービスのアクセスが認可されます。

RADIUS アカウンティング

AAA アカウンティング機能は、ユーザが使用したサービスと、消費したネットワーク リソース量を追跡します。AAA アカウンティングを有効にすると、デバイスはユーザーアクティビティをアカウンティングレコードの形式でRADIUSセキュリティサーバーに報告します。各アカウンティング レコードにはアカウンティングの Attribute-Value（AV）ペアが含まれ、レコードはセキュリティ サーバに格納されます。これらのデータは、ネットワーク管理、クライアントへの課金、または監査のために後で分析できます。

ベンダー固有の RADIUS 属性

Internet Engineering Task Force（IETF）ドラフト規格に、ベンダー固有の属性（属性 26）を使用して、デバイスとRADIUSサーバ間でベンダー固有の情報を通信するための方式が定められています。各ベンダーは、Vendor-Specific Attribute（VSA）を使用することによって、一般的な用途には適さない独自の拡張属性をサポートできます。シスコが実装するRADIUSでは、この仕様で推奨されるフォーマットを使用して、ベンダー固有のオプションを1つサポートしています。シスコのベンダーIDは9であり、サポート対象のオプションはベンダータイプ1（名前は *cisco-avpair*）です。この値は、次のフォーマットの文字列です。

```
protocol : attribute sep value *
```

protocol は、特定の認証タイプに使用するシスコのプロトコル属性の値です。*attribute* および *value* は、シスコの TACACS+ 仕様で定義されている適切な属性値（AV）ペアです。*sep* は、必須の属性の場合は =、任意指定の属性の場合は * です。TACACS+ 認証で使用できるすべての機能は、RADIUS でも使用できます。

たとえば、次の AV ペアにより、IP 認証中（PPP の IPCP アドレス割り当て中）には、シスコの「multiple named IP address pools」機能がアクティブになります。

```
cisco-avpair= ”ip:addr-pool=first“
```

「*」を挿入すると、AV ペア「ip:addr-pool=first」は省略可能になります。任意の AV ペアを省略可能にすることができます。

```
cisco-avpair= ”ip:addr-pool*first“
```

次に、ネットワーク アクセス サーバからユーザがログインしたときに、すぐに EXEC コマンドを実行する方法の例を示します。

```
cisco-avpair= ”shell:priv-lvl=15“
```

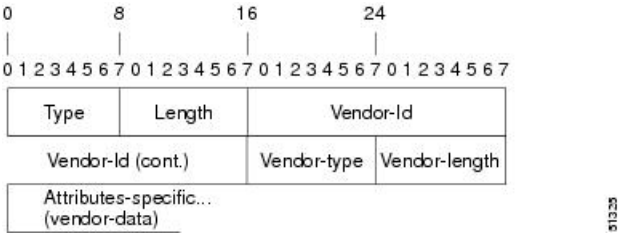
他のベンダーにも、それぞれ独自のベンダー ID、オプション、および対応する VSA があります。ベンダー ID および VSA の詳細については、RFC 2138『Remote Authentication Dial-In User Service (RADIUS)』を参照してください。

属性 26 には、次の 3 つの要素が含まれています。

- タイプ
- 長さ
- 文字列（またはデータ）
  - Vendor-ID
  - Vendor-Type
  - Vendor-Length
  - Vendor-Data

次の図は、属性 26 の「背後で」カプセル化される VSA のパケット形式を示します。

図 *2*：属性 *26* の背後でカプセル化される *VSA*



（注） VSA の形式はベンダーが指定します。Attribute-Specific フィールド（Vendor-Data とも呼ばれる）は、ベンダーによるその属性の定義によって異なります。

次の表に、「ベンダー固有 RADIUS IETF 属性テーブル」（次の 2 番目の表）で表示される重要なフィールドを示します。これは、サポート対象のベンダー固有 RADIUS 属性（IETF 属性 26）を表示します。

表 *5*：ベンダー固有属性表のフィールドの説明

フィールド	説明
番号	次の表に示されるすべての属性は、IETF 属性 26 の拡張です。

フィールド	説明
ベンダー固有のコマンドコード	特定のベンダーの識別に使用する定義されたコード。コード 9 は Cisco VSA、311 は Microsoft VSA、529 は Ascend VSA を定義します。
サブタイプ番号	属性 ID 番号。この番号は、属性 26 の背後でカプセル化される「2 番めのレイヤ」の ID 番号であること以外、IETF 属性の ID 番号に似ています。
属性	属性の ASCII 文字列名。
説明	属性の説明。

表 *6 :* ベンダー固有 *RADIUS IETF* 属性

番号	ベンダー固有の企業コード	サブタイプ番号	属性	説明
MS-CHAP 属性				
26	311	1	MSCHAP-Response	PPP MS-CHAP ユーザがチャレンジに対する応答で提供するレスポンス値が含まれます。Access-Request パケットでしか使用されません。この属性は、PPP CHAP ID と同じです（RFC 2548）
26	311	11	MSCHAP-Challenge	ネットワーク アクセス サーバが MS-CHAP ユーザに送信するチャレンジが含まれます。これは、Access-Request パケットと Access-Challenge パケットの両方で使用できます。（RFC 2548）
VPDN 属性				
26	9	1	l2tp-cm-local-window-size	L2TP 制御メッセージの最大受信ウィンドウ サイズを指定します。この値は、トンネルの確立中にピアにアドバタイズされます。

番号	ベンダー固有の企業コード	サブタイプ番号	属性	説明
26	9	1	l2tp-drop-out-of-order	正しくない順序で受信したデータパケットを破棄して、シーケンス番号を順守します。これは受信した場合の処理方法であって、データ パケット上でシーケンス番号が送信されるわけではありません。
26	9	1	l2tp-hello-interval	hello キープアライブインターバルの秒数を指定します。ここで指定した秒数、トンネルでデータが送信されないと、hello パケットが送信されます。
26	9	1	l2tp-hidden-avp	有効にすると、L2TP制御メッセージで、大文字小文字を区別する AVP にスクランブルがかけられるか、または非表示になります。
26	9	1	l2tp-nosession-timeout	タイムアウトおよびシャットダウンまでに、セッションなしでトンネルがアクティブのままになる秒数を指定します。
26	9	1	tunnel-tos-reflect	LNS でトンネルに入るパケットに対して、IP ToS フィールドを各ペイロードパケットの IP ヘッダーからトンネルパケットの IP ヘッダーにコピーします。
26	9	1	l2tp-tunnel-authen	この属性を設定すると、L2TP トンネル認証が実行されます。

番号	ベンダー固有の企業コード	サブタイプ番号	属性	説明
26	9	1	l2tp-tunnel-password	L2TP トンネル認証および AVP 隠蔽に使用される共有秘密。
26	9	1	l2tp-udp-checksum	これは認可属性で、L2TP がデータ パケットに対して UDP チェックサムを実行する必要があるかどうかを定義します。有効な値は「yes」と「no」です。デフォルトは「no」です。
Store and Forward Fax 属性				
26	9	3	Fax-Account-Id-Origin	**mmoip aaa receive-id** コマンドまたは **mmoip aaa send-id** コマンドについて、システム管理者によって定義されたものとしてアカウント ID の発信元を示します。
26	9	4	Fax-Msg-Id=	Store and Forward Fax 機能によって割り当てられた一意のファクス メッセージ識別番号を示します。
26	9	5	Fax-Pages	このファクス セッション中に送信または受信したページ数を示します。このページ数には、カバー ページも含まれます。

番号	ベンダー固有の企業コード	サブタイプ番号	属性	説明
26	9	6	Fax-Coverpage-Flag	カバー ページがこのファクス セッションのオフランプ ゲートウェイで生成されたかどうかを示します。true はカバー ページが生成されたことを示します。false はカバー ページが生成されなかったことを意味します。
26	9	7	Fax-Modem-Time	モデムがファクス データを送信した時間（x）、およびファクス セッションの合計時間（y）を秒単位で示します。これには、fax-mail および PSTN 時間が x/y の形式で含まれます。たとえば、10/15 は送信時間が 10 秒で、合計ファクス セッションが 15 秒であったことを示します。
26	9	8	Fax-Connect-Speed	この fax-mail が最初に送信または受信された時点のモデム速度を示します。有効値は、1200、4800、9600、および 14400 です。
26	9	9	Fax-Recipient-Count	このファクス送信の受信者数を示します。E メール サーバがセッション モードをサポートするまで、この数字は 1 にする必要があります。

番号	ベンダー固有の企業コード	サブタイプ番号	属性	説明
26	9	10	Fax-Process-Abort-Flag	ファクスセッションが中断したこと、または正常に終了したことを示します。true はセッションが中断したことを示します。false はセッションが成功したことを示します。
26	9	11	Fax-Dsn-Address	DSN の送信先のアドレスを示します。
26	9	12	Fax-Dsn-Flag	DSN が有効にされているかどうかを示します。true は DSN が有効にされていることを示します。false は DSN が有効にされていないことを示します。
26	9	13	Fax-Mdn-Address	MDN の送信先のアドレスを示します。
26	9	14	Fax-Mdn-Flag	メッセージ配信通知（MDN）が有効にされているかどうかを示します。true は MDN が有効にされていることを示します。false は MDN が有効にされていないことを示します。
26	9	15	Fax-Auth-Status	このファクスセッションに対する認証が成功したかどうかを示します。このフィールドに対する有効値は、success、failed、bypassed、または unknown です。

番号	ベンダー固有の企業コード	サブタイプ番号	属性	説明
26	9	16	Email-Server-Address	オンランプ fax-mail メッセージを処理する E メール サーバの IP アドレスを示します。
26	9	17	Email-Server-Ack-Flag	オンランプ ゲートウェイが fax-mail メッセージを受け入れる E メール サーバから肯定確認応答を受信したことを示します。
26	9	18	Gateway-Id	ファクス セッションを処理したゲートウェイの名前を示します。名前は、hostname.domain-name という形式で表示されます。
26	9	19	Call-Type	ファクスのアクティビティのタイプを、fax receive または fax send のどちらかで記述します。
26	9	20	Port-Used	この fax-mail の送受信いずれかに使用される Cisco AS5300 のスロット/ポート番号を示します。

番号	ベンダー固有の企業コード	サブタイプ番号	属性	説明
26	9	21	Abort-Cause	ファクスセッションが中断した場合、中断の信号を送信したシステムコンポーネントを示します。中断する可能性のあるシステムコンポーネントには、FAP（Fax Application Process）、TIFF（TIFF リーダーまたは TIFF ライター）、fax-mail クライアント、fax-mail サーバー、ESMTP クライアント、ESMTP サーバーなどがあります。
H323 属性				
26	9	23	Remote-Gateway-ID（h323-remote-address）	リモート ゲートウェイの IP アドレスを示します。
26	9	24	Connection-ID（h323-conf-id）	会議 ID を識別します。
26	9	25	Setup-Time（h323-setup-time）	以前、グリニッジ標準時（GMT）およびズール タイムと呼ばれていた協定世界時（UTC）でのこの接続のセットアップ時間を示します。
26	9	26	Call-Origin（h323-call-origin）	ゲートウェイに対するコールの発行元を示します。有効値は、originating および terminating です（回答）。
26	9	27	Call-Type（h323-call-type）	コールのレグ タイプを示します。使用可能な値は **telephony** と **VoIP** です。

番号	ベンダー固有の企業コード	サブタイプ番号	属性	説明
26	9	28	Connect-Time（h323-connect-time）	このコール レッグの UTC での接続時間を示します。
26	9	29	Disconnect-Time（h323-disconnect-time）	このコール レッグが UTC で接続解除された時間を示します。
26	9	30	Disconnect-Cause（h323-disconnect-cause）	Q.931 仕様によって、接続がオフラインにされた理由を示します。
26	9	31	Voice-Quality（h323-voice-quality）	コールの音声品質に影響する Impairment Factor（ICPIF）を指定します。
26	9	33	Gateway-ID（h323-gw-id）	下位のゲートウェイの名前を示します。
大規模のダイヤルアウト属性				
26	9	1	callback-dialstring	コールバックに使用するダイヤリング文字列を定義します。
26	9	1	data-service	説明はありません。
26	9	1	dial-number	ダイヤルする番号を定義します。
26	9	1	force-56	チャネルの 64 K すべてが使用可能に見える場合でも、ネットワーク アクセス サーバが 56 K の部分のみを使用するかどうかを指定します。

番号	ベンダー固有の企業コード	サブタイプ番号	属性	説明
26	9	1	map-class	ユーザ プロファイルに、ダイヤルアウトするネットワーク アクセス サーバ上で同じ名前のマップ クラスで設定される情報の参照を許可します。
26	9	1	send-auth	CLID 認証に続く、username-password 認証で使用するプロトコル（PAP または CHAP）を定義します。

番号	ベンダー固有の企業コード	サブタイプ番号	属性	説明
26	9	1	send-name	

番号	ベンダー固有の企業コード	サブタイプ番号	属性	説明
				PPP 名前認証。PAP に適用する場合、インターフェイスで **ppp pap sent-name password** コマンドは設定しないでください。PAP の場合、アウトバウンド認証の PAP ユーザ名および PAP パスワードとして、「preauth:send-name」および「preauth:send-secret」が使用されます。CHAP の場合、「preauth:send-name」は、アウトバウンド認証だけでなく、インバウンド認証にも使用されます。CHAP インバウンドの場合、NAS は発信元のボックスへのチャレンジ パケットに、「preauth:send-name」で定義された名前を使用します。 （注） send-name 属性は時間の経過とともに変わっています。最初は、現在 send-name および remote-name 属性の両方で提供されている機能を実行していました。remote-name 属性が追加されたため、send-name 属性

番号	ベンダー固有の企業コード	サブタイプ番号	属性	説明
				は現在の動作に制限されています。
26	9	1	send-secret	PPP パスワード認証。ベンダー固有属性（VSA）の場合、アウトバウンド認証の PAP ユーザ名および PAP パスワードとして、「preauth:send-name」および「preauth:send-secret」が使用されます。CHAP アウトバウンドの場合、「preauth:send-name」と「preauth:send-secret」の両方が応答パケットで使用されます。
26	9	1	remote-name	大規模のダイヤルアウトで使用するリモートホストの名前を提供します。ダイヤラは、大規模のダイヤルアウトのリモート名が認証された名前と一致することを確認し、偶発的なユーザ RADIUS 設定ミスから保護します（有効な電話番号にダイヤルしたが誤ったデバイスに接続されるなどのミスです）。
その他の属性				

番号	ベンダー固有の企業コード	サブタイプ番号	属性	説明
26	9	2	Cisco-NAS-Port	NAS-Port アカウンティングに追加的なベンダー固有属性（VSA）を指定します。追加的な NAS-Port 情報を属性値ペア（AVPair）の形式で指定するには、**radius-server vsa send** グローバル コンフィギュレーション コマンドを使用します。 （注） この VSA は、通常アカウンティングで使用されますが認証（Access-Request）パケットで使用される場合もあります。
26	9	1	min-links	MLP に対するリンクの最小数を設定します。
26	9	1	proxyacl#<n>	ダウンロード可能なユーザ プロファイル（ダイナミック ACL）を、認証プロキシを使用して設定でき、これにより設定されたインターフェイスのトラフィックの通過を許可するよう、認証を設定できます。

番号	ベンダー固有の企業コード	サブタイプ番号	属性	説明
26	9	1	spi	登録中にホーム エージェントがモバイル ノードの認証で必要とする認証情報を伝送します。この情報は、**ip mobile secure host <addr>** コンフィギュレーション コマンドと同じ構文です。基本的に、この文字列に続く残りのコンフィギュレーション コマンドはそのまま含まれます。これにはセキュリティ パラメータ インデックス（SPI）、鍵、認証アルゴリズム、認証モード、およびリプレイ保護タイムスタンプ範囲が含まれています。

ベンダー独自仕様の RADIUS サーバ通信

RADIUS に関する IETF ドラフト規格では、デバイスと RADIUS サーバー間でベンダー独自仕様の情報を通信する方式について定められていますが、RADIUS 属性セットを独自に機能拡張しているベンダーもあります。Cisco IOS XE ソフトウェアは、ベンダー独自仕様の RADIUS 属性のサブセットをサポートしています。

前述のように、（ベンダー固有かIETF ドラフト準拠かに関係なく）RADIUS を設定するには、RADIUS サーバーデーモンを実行するホストと、デバイスと共有する秘密テキスト文字列を指定する必要があります。RADIUS ホストおよび秘密テキスト文字列を指定するには、**radius server** グローバル コンフィギュレーション コマンドを使用します。

RADIUS パケットの DSCP マーキング

差別化サービス（DiffServ）は、他のトラフィッククラスよりも優先的に処理するためにトラフィックを分類および管理する Quality of Service（QoS）モデルです。DiffServ は、IP パケットの 6 ビット DiffServ コードポイント（DSCP）設定を使用して、トラフィッククラスに相対的な優先順位をマークします。Cisco IOS XE ソフトウェアは、RADIUS パケットの DSCP マーキングをサポートして、RADIUS パケットの認証とアカウンティングを高速化します。

RADIUS サーバー、RADIUS サーバーグループ、およびグローバル コンフィギュレーション モードで DSCP マーキングを設定できます。DSCP マーキングが RADIUS サーバー、サーバー グループ、およびグローバル コンフィギュレーション モードに設定されると、RADIUS サーバーに入力された DSCP マーキング値が優先されます。

- RADIUS サーバーに DSCP マーキング設定がない場合、サーバーグループに設定された DSCP マーキング値が RADIUS パケットに適用されます。
- RADIUS サーバーまたは RADIUS サーバーグループに DSCP マーキング設定がない場合、グローバル コンフィギュレーション モードで設定された DSCP マーキング値が RADIUS パケットに適用されます。

RADIUS の設定

RADIUS サーバ ホストの識別

デバイスと通信するすべての RADIUS サーバーにこのような設定をグローバルに適用するには、**radius-server timeout**、**radius-server retransmit**、および **key** *string* という 3 つの固有なグローバル コンフィギュレーション コマンドを使用します。

既存のサーバー ホストを認証用にグループ化するため、AAA サーバー グループを使用するようにデバイスを設定できます。

RADIUS サーバ上でも、いくつかの値を設定する必要があります。deviceの IP アドレス、およびサーバーとdeviceの双方で共有する鍵文字列などの設定値です。

サーバ単位で RADIUS サーバとの通信を設定するには、次の手順を実行します。

始める前に

device上にグローバルな機能とサーバ単位での機能（タイムアウト、再送信回数、および鍵コマンド）を設定した場合、サーバ単位で設定したタイムアウト、再送信回数、および鍵値コマンドは、グローバルに設定したタイムアウト、再送信回数、および鍵値コマンドを上書きします。

（注） RADIUS および AAA サーバーは、標準のデフォルトポートでのみ実行するように設定できます。

- 1812 および 1813
- 1645 および 1646

手順の概要

1. **enable**

2. **configure terminal**
3. **radius server** *server name*
4. **address** {**ipv4 | ipv6**}*ip address*{ **auth-port** *port number* | **acct-port** *port number*}
5. **key** *string*
6. **retransmit** *value*
7. **timeout** *seconds*
8. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	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。
ステップ 3	**radius server** *server name* 例： `Device(config)# radius server rsim`	RADIUS サーバ設定の名前を Protected Access Credential（PAC）のプロビジョニング用に指定し、RADIUS サーバ設定モードを開始します。
ステップ 4	**address** {**ipv4	ipv6**}*ip address*{ **auth-port** *port number*	**acct-port** *port number*} 例： `Device(config-radius-server)# address ipv4 124.2.2.12 auth-port 1612`	（任意）RADIUS サーバーのパラメータを指定します。 **auth-port** *port-number* には、認証要求の UDP 宛先ポートを指定します。デフォルトは 1645 です。指定できる範囲は 0 ～ 65536 です。 **acct-port** *port-number* には、アカウンティング要求の UDP 宛先ポートを指定します。デフォルトは 1646 です。
ステップ 5	**key** *string* 例： `Device(config-radius-server)# key rad123`	（任意）**key** *string* には、デバイスと RADIUS サーバーで動作する RADIUS デーモンの間で使用される認証と暗号鍵を指定します。

	コマンドまたはアクション	目的
		（注） 鍵は、RADIUS サーバーで使用する暗号鍵に一致するテキスト文字列でなければなりません。必ず **radius server** コマンドの最終項目として鍵を設定してください。先頭のスペースは無視されますが、鍵の中間および末尾のスペースは使用されます。鍵にスペースを使用する場合は、引用符が鍵の一部分である場合を除き、引用符で鍵を囲まないでください。
ステップ 6	**retransmit** *value* 例： `Device(config-radius-server)# retransmit 10`	（任意）サーバが応答しない、または応答が遅い場合に、RADIUS 要求をリセットする回数を指定します。指定できる範囲は 1 ～ 100 です。この設定は、**radius-server retransmit** グローバル コンフィギュレーション コマンドによる設定を上書きします。
ステップ 7	**timeout** *seconds* 例： `Device(config-radius-server)# timeout 60`	（任意）deviceが要求を再送信する前にRADIUSサーバからの応答を待機する時間間隔を指定します。指定できる範囲は 1 ～ 1000 です。この設定は、**radius-server timeout** グローバル コンフィギュレーション コマンドによる設定を上書きします。
ステップ 8	**end** 例： `Device(config-radius-server)# end`	RADIUS サーバー コンフィギュレーション モードを終了し、特権 EXEC モードを開始します。

RADIUS ログイン認証の設定

RADIUS ログイン認証を設定するには、次の手順を実行します。

始める前に

AAA 方式を使用して HTTP アクセスに対しデバイスのセキュリティを確保するには、**ip http authentication aaa** グローバル コンフィギュレーション コマンドを設定する必要があります。AAA 認証を設定しても、AAA 方式を使用した HTTP アクセスに対しデバイスのセキュリティは確保されません。

手順の概要

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

4. **aaa authentication login** {**default** | *list-name*} *method1* [*method2...*]
5. **line** [**console** | **tty** | **vty**] *line-number* [*ending-line-number*]
6. **login authentication** {**default** | *list-name*}
7. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	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。
ステップ 3	**aaa new-model** 例： `Device(config)# aaa new-model`	AAA を有効にします。
ステップ 4	**aaa authentication login** {**default** | *list-name*} *method1* [*method2...*] 例： `Device(config)# aaa authentication login default local`	ログイン認証方式リストを作成します。 • **login authentication** コマンドにリストが指定されていない場合に使用するデフォルトのリストを作成するには、**default** キーワードの後ろにデフォルト状況で使用される方式を指定します。デフォルトの方式リストは、自動的にすべてのポートに適用されます。 • *list-name* には、作成するリストの名前として使用する文字列を指定します。 • *method1...* には、認証アルゴリズムが試行する実際の方式を指定します。追加の認証方式は、その前の方式でエラーが返された場合に限り使用されます。前の方式が失敗した場合は使用されません。 次のいずれかの方式を選択します。 • *enable*：イネーブル パスワードを認証に使用します。この認証方式を使用するには、あらかじめ **enable** *password* グローバル コンフィギュレーション コマンドを使用してイネーブルパスワードを定義しておく必要があります。

	コマンドまたはアクション	目的
		• *group radius*：RADIUS 認証を使用します。この認証方式を使用するには、あらかじめ RADIUS サーバーを設定しておく必要があります。 • *line*：回線パスワードを認証に使用します。この認証方式を使用するには、あらかじめ回線パスワードを定義しておく必要があります。**password** *password* ライン コンフィギュレーション コマンドを使用します。 • *local*：ローカル ユーザー名データベースを認証に使用します。データベースにユーザ名情報を入力しておく必要があります。**username** *name* **password** グローバル コンフィギュレーション コマンドを使用します。 • *local-case*：大文字と小文字が区別されるローカル ユーザー名データベースを認証に使用します。**username** *password* グローバル コンフィギュレーション コマンドを使用して、ユーザー名情報をデータベースに入力する必要があります。 • *none*：ログインに認証を使用しません。
ステップ 5	**line** [**console** | **tty** | **vty**] *line-number* [*ending-line-number*] 例： `Device(config)# line 1 4`	ライン コンフィギュレーション モードを開始し、認証リストを適用する回線を設定します。
ステップ 6	**login authentication** {**default** | *list-name*} 例： `Device(config-line)# login authentication default`	1 つの回線または複数回線に認証リストを適用します。 • **default** を指定する場合は、**aaa authentication login** コマンドで作成したデフォルトのリストを使用します。 • *list-name* には、**aaa authentication login** コマンドで作成したリストを指定します。
ステップ 7	**end** 例： `Device(config-line)# end`	ライン コンフィギュレーション モードを終了して、特権 EXEC モードを開始します。

AAA サーバ グループの定義

定義したグループサーバに特定のサーバを対応付けるには、**server** グループ サーバ コンフィギュレーション コマンドを使用します。サーバを IP アドレスで特定することもできますし、任意指定の **auth-port** および **acct-port** キーワードを使用して複数のホストインスタンスまたはエントリを特定することもできます。

AAA サーバ グループを定義するには、次の手順を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **radius server** *name*
4. **address** {**ipv4** | **ipv6**} {*ip-address* | *hostname*} **auth-port** *port-number* **acct-port** *port-number*
5. **key** *string*
6. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	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。
ステップ 3	**radius server** *name* 例： `Device(config)# radius server ISE`	RADIUS サーバの設定の名前を Protected Access Credential（PAC）のプロビジョニング用に指定し、RADIUS サーバ設定モードを開始します。 deviceは、IPv6 対応の RADIUS をサポートしています。
ステップ 4	**address** {**ipv4** | **ipv6**} {*ip-address* | *hostname*} **auth-port** *port-number* **acct-port** *port-number* 例： `Device(config-radius-server)# address ipv4 10.1.1.1 auth-port 1645 acct-port 1646`	RADIUS サーバのアカウンティングおよび認証パラメータの IPv4 アドレスを設定します。

	コマンドまたはアクション	目的
ステップ 5	**key** *string* 例： `Device(config-radius-server)# key cisco123`	デバイスと RADIUS サーバーとの間におけるすべての RADIUS 通信用の認証および暗号鍵を指定します。
ステップ 6	**end** 例： `Device(config-radius-server)# end`	RADIUS サーバ コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

ユーザー特権アクセスおよびネットワークサービスに関する RADIUS 許可の設定

（注） 許可が設定されていても、CLI を使用してログインし、認証されたユーザに対しては、許可は省略されます。

ユーザ特権アクセスおよびネットワーク サービスに関する RADIUS 許可を設定するには、次の手順を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **aaa authorization network** *authorization-list***radius**
4. **aaa authorization exec** *authorization-list***radius**
5. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	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。

	コマンドまたはアクション	目的
ステップ 3	**aaa authorization network** *authorization-list***radius** 例： `Device(config)# aaa authorization network list1 radius`	ネットワーク関連のすべてのサービス要求に対して、ユーザーが RADIUS 許可を受けるように device を設定します。
ステップ 4	**aaa authorization exec** *authorization-list***radius** 例： `Device(config)# aaa authorization exec list1 radius`	ユーザに特権 EXEC のアクセス権限がある場合、ユーザが RADIUS 許可を受けるように device を設定します。 **exec** キーワードを指定すると、ユーザープロファイル情報（**autocommand** 情報など）が返される場合があります。
ステップ 5	**end** 例： `Device(config)# end`	グローバル コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

次のタスク

aaa authorization グローバル コンフィギュレーション コマンドと **radius** キーワードを使用すると、ユーザのネットワーク アクセスを特権 EXEC モードに制限するパラメータを設定できます。

aaa authorization exec radius local コマンドは、次の許可パラメータを設定します。

- RADIUS を使用して認証を行った場合は、RADIUS を使用して特権 EXEC アクセスを許可します。
- 認証に RADIUS を使用しなかった場合は、ローカル データベースを使用します。

RADIUS アカウンティングの起動

RADIUS アカウンティングを開始するには、次の手順を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **aaa accounting network** *accounting-list***start-stop radius**
4. **aaa accounting exec** *accounting-list***start-stop radius**
5. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	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。
ステップ 3	**aaa accounting network** *accounting-list***start-stop radius** 例： `Device(config)# aaa accounting network start-stop radius`	ネットワーク関連のあらゆるサービス要求に関して、RADIUS アカウンティングを有効にします。
ステップ 4	**aaa accounting exec** *accounting-list***start-stop radius** 例： `Device(config)# aaa accounting exec acc-list start-stop radius`	RADIUSアカウンティングを有効にして、特権EXECプロセスの最初に記録開始アカウンティング通知、最後に記録停止通知を送信します。
ステップ 5	**end** 例： `Device(config)# end`	グローバル コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

すべての RADIUS サーバの設定

すべての RADIUS サーバーを設定するには、特権 EXEC モードで次の手順を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **radius server** *server name*
4. **key** *string*
5. **retransmit** *retries*
6. **timeout** *seconds*
7. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	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。
ステップ 3	**radius server** *server name* 例： `Device(config)# radius server rsim`	RADIUS サーバ設定の名前を Protected Access Credential（PAC）のプロビジョニング用に指定し、RADIUS サーバ設定モードを開始します。
ステップ 4	**key** *string* 例： `Device(config-radius-server)# key your_server_key`	スイッチとすべての RADIUS サーバ間で共有される秘密テキスト文字列を指定します。 （注） 鍵は、RADIUS サーバで使用する暗号鍵に一致するテキスト文字列でなければなりません。先頭のスペースは無視されますが、鍵の中間および末尾のスペースは使用されます。鍵にスペースを使用する場合は、引用符が鍵の一部分である場合を除き、引用符で鍵を囲まないでください。
ステップ 5	**retransmit** *retries* 例： `Device(config-radius-server)# retransmit 5`	スイッチが RADIUS 要求をサーバに再送信する回数を指定します。デフォルトは 3 です。指定できる範囲は 1 ～ 1000 です。
ステップ 6	**timeout** *seconds* 例： `Device(config-radius-server)# timeout 3`	スイッチが RADIUS 要求に対する応答を待って、要求を再送信するまでの時間（秒）を指定します。デフォルトは 5 秒です。指定できる範囲は 1 ～ 1000 です。
ステップ 7	**end** 例： `Device(config-radius-server)# end`	RADIUS サーバー コンフィギュレーション モードを終了し、特権 EXEC モードを開始します。

ベンダー固有の RADIUS 属性を使用するデバイスの設定

ベンダー固有の RADIUS 属性を設定するには、次の手順を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **radius-server vsa send** [**accounting** | **authentication**]
4. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	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。
ステップ 3	**radius-server vsa send** [**accounting**	**authentication**] 例： `Device(config)# radius-server vsa send accounting`	device が VSA（RADIUS IETF 属性 26 で定義）を認識して使用できるようにします。 • （任意）認識されるベンダー固有属性の集合をアカウンティング属性だけに限定するには、**accounting** キーワードを使用します。 • （任意）認識されるベンダー固有属性の集合を認証属性だけに限定するには、**authentication** キーワードを使用します。 キーワードを指定せずにこのコマンドを入力すると、アカウンティングおよび認証のベンダー固有属性の両方が使用されます。
ステップ 4	**end** 例： `Device(config)# end`	グローバル コンフィギュレーション モードを終了し、特権 EXEC モードを開始します。

ベンダー独自仕様の RADIUS サーバ通信に関するデバイスの設定

ベンダー独自仕様の RADIUS サーバー通信を設定するには、次の手順を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **radius server** *server name*
4. **address** { **ipv4 | ipv6** } *ip address*
5. **non-standard**
6. **key** *string*
7. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	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。
ステップ 3	**radius server** *server name* 例： `Device(config)# radius server rsim`	RADIUS サーバ設定の名前を Protected Access Credential（PAC）のプロビジョニング用に指定し、RADIUS サーバ設定モードを開始します。
ステップ 4	**address** { **ipv4 | ipv6** } *ip address* 例： `Device(config-radius-server)# address ipv4 172.24.25.10`	（任意）RADIUS サーバの IP アドレスを指定します。
ステップ 5	**non-standard** 例： `Device(config-radius-server)# non-standard`	RADIUS サーバが RADIUS ベンダー独自の実装を使用していることを示します。
ステップ 6	**key** *string* 例： `Device(config-radius-server)# key rad123`	デバイスとベンダー独自仕様の RADIUS サーバーとの間で使用される共有秘密テキスト文字列を指定します。デバイスと RADIUS サーバーはこのテキスト文字列を使用してパスワードを暗号化し、応答を交換します。

	コマンドまたはアクション	目的
ステップ 7	**end** 例： `Device(config-radius-server)# end`	RADIUS サーバーモードを終了し、特権 EXEC モードを開始します。

RADIUS サーバーでの DSCP マーキングの設定

RADIUS サーバーでの認証とアカウンティング用の DSCP マーキングを設定するには、次の手順に従います。

手順の概要

1. **enable**
2. **configure terminal**
3. **radius server** *server_name*
4. **address** { **ipv4 | ipv6** } *ip address* [**auth-port** *auth_port_number* **acct-port** *acct_port_number*]
5. **dscp** {**acct** *dscp_acct_value* | **auth** *dscp_auth_value*}
6. **key** *string*
7. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	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。
ステップ 3	**radius server** *server_name* 例： `Device(config)# radius server rsim`	RADIUS サーバー設定の名前を Protected Access Credential（PAC）のプロビジョニング用に指定し、RADIUS サーバー設定モードを開始します。
ステップ 4	**address** { **ipv4	ipv6** } *ip address* [**auth-port** *auth_port_number* **acct-port** *acct_port_number*] 例： `Device(config-radius-server)# address ipv4`	（任意）RADIUS サーバーの IP アドレスを指定します。 • **auth-port** は、RADIUS 認証サーバーのポート値を設定します。デフォルト値は 1812 です。

	コマンドまたはアクション	目的
	`10.1.1.1 auth-port 1645 acct-port 1646`	• **acct-port** は、RADIUS アカウンティングサーバーのポート値を設定します。デフォルト値は 1813 です。
ステップ 5	**dscp** {**acct** *dscp_acct_value* | **auth** *dscp_auth_value*} 例： `Device(config-radius-server)# dscp auth 10 acct 20`	RADIUS サーバーでの認証とアカウンティング用の DSCP マーキングを設定します。 • **acct** はアカウンティングの RADIUS DSCP マーキング値を設定します。有効な範囲は 1 ～ 63 です。デフォルト値は 0 です • **auth** は認証の RADIUS DSCP マーキング値を設定します。有効な範囲は 1 ～ 63 です。デフォルト値は 0 です
ステップ 6	**key** *string* 例： `Device(config-radius-server)# key rad123`	デバイスとベンダー独自仕様の RADIUS サーバーとの間で使用される共有秘密テキスト文字列を指定します。デバイスと RADIUS サーバーはこのテキスト文字列を使用してパスワードを暗号化し、応答を交換します。
ステップ 7	**end** 例： `Device(config-radius-server)# end`	RADIUS サーバーモードを終了し、特権 EXEC モードを開始します。

RADIUS サーバーグループでの送信元インターフェイスと DSCP マーキングの設定

次の手順に従って、RADIUS サーバーグループでの認証とアカウンティング用の送信元インターフェイスと DSCP マーキングを設定します。

手順の概要

1. **enable**
2. **configure terminal**
3. **aaa group server radius** *group_name*
4. **server name** *name*
5. {**ip** | **ipv6**} **radius source-interface** *type number*
6. **dscp** {**acct** *dscp_acct_value* | **auth** *dscp_auth_value*}
7. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	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。
ステップ 3	**aaa group server radius** *group_name* 例： `Device(config)# aaa group server radius abc`	RADIUS サーバー グループ コンフィギュレーションを定義し、RADIUS サーバー グループ コンフィギュレーション モードを開始します。
ステップ 4	**server name** *name* 例： `Device(config-sg-radius)# server name serv1`	RADIUS サーバーをサーバーグループに関連付けます。
ステップ 5	{**ip** | **ipv6**} **radius source-interface** *type number* 例： `Device(config-sg-radius)# ipv6 radius source-interface ethernet 0/0`	RADIUS サーバーの送信元アドレスに使用するインターフェイスを指定します。
ステップ 6	**dscp** {**acct** *dscp_acct_value* | **auth** *dscp_auth_value*} 例： `Device(config-sg-radius)# dscp auth 10 acct 20`	RADIUS サーバーグループでの認証とアカウンティング用の DSCP マーキングを設定します。 • **acct** はアカウンティングの RADIUS DSCP マーキング値を設定します。有効な範囲は 1 ～ 63 です。デフォルト値は 0 です • **auth** は認証の RADIUS DSCP マーキング値を設定します。有効な範囲は 1 ～ 63 です。デフォルト値は 0 です
ステップ 7	**end** 例： `Device(config-radius-server)# end`	RADIUS サーバーモードを終了し、特権 EXEC モードを開始します。

デバイス上での CoA の設定

CoA をdeviceで設定するには、次の手順を実行します。この手順は必須です。

手順の概要

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

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	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。
ステップ 3	**aaa new-model** 例： `Device(config)# aaa new-model`	AAA を有効にします。
ステップ 4	**aaa server radius dynamic-author** 例： `Device(config)# aaa server radius dynamic-author`	デバイスを認証、許可、アカウンティング（AAA）サーバーとして設定して外部ポリシーサーバーとの通信を容易にし、ダイナミック許可ローカル サーバー コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 5	**client** {*ip-address* | *name*} [**vrf** *vrfname*] [**server-key** *string*] 例： `Device(config-locsvr-da-radius)# client client1 vrf vrf1`	デバイスが CoA を受け取り、要求を取り外す RADIUS クライアントを指定します。
ステップ 6	**server-key** [**0** | **7**] *string* 例： `Device(config-locsvr-da-radius)# server-key your_server_key`	RADIUS 鍵をデバイスと RADIUS クライアントとの間で共有されるように設定します。
ステップ 7	**port** *port-number* 例： `Device(config-locsvr-da-radius)# port 25`	設定された RADIUS クライアントから RADIUS 要求をデバイスが受信するポートを指定します。
ステップ 8	**auth-type** {**any** | **all** | **session-key**} 例： `Device(config-locsvr-da-radius)# auth-type any`	deviceが RADIUS クライアントに使用する許可のタイプを指定します。 クライアントは、許可用に設定されたすべての属性と一致していなければなりません。
ステップ 9	**ignore server-key** 例： `Device(config-locsvr-da-radius)# ignore server-key`	（任意）server-key を無視するように device を設定します。
ステップ 10	**exit** 例： `Device(config-locsvr-da-radius)# exit`	ダイナミック認可ローカル サーバー コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードに戻ります。
ステップ 11	**authentication command bounce-port ignore** 例： `Device(config)# authentication command bounce-port ignore`	（任意）CoA 要求を無視して、セッションをホスティングするポートを一時的に無効にするようにdeviceを設定します。ポートを一時的に無効にする目的は、VLAN の変更が発生しても、その変更を検出するサプリカントがエンドポイント上にない場合に、ホストから DHCP 再ネゴシエーションを行わせることです。

	コマンドまたはアクション	目的
ステップ 12	**authentication command disable-port ignore** 例： `Device(config)# authentication command disable-port ignore`	（任意）セッションをホスティングしているポートを管理上のシャットダウン状態にするよう要求する非標準コマンドを無視するようにdeviceを設定します。ポートをシャットダウンすると、セッションが終了します。 ポートを再び有効にするには、標準の CLI または SNMP コマンドを使用します。
ステップ 13	**end** 例： `Device(config)# end`	グローバル コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

CoA 機能のモニタリング

表 *7*：特権 *EXEC* 表示コマンド

コマンド	目的
show aaa attributes protocol radius	RADIUS コマンドの AAA 属性を表示します。

表 *8*：グローバル トラブルシューティング コマンド

コマンド	目的
debug radius	RADIUS のトラブルシューティングを行うための情報を表示します。
debug aaa coa	CoA 処理のトラブルシューティングを行うための情報を表示します。
debug aaa pod	POD パケットのトラブルシューティングを行うための情報を表示します。
debug aaa subsys	POD パケットのトラブルシューティングを行うための情報を表示します。
debug cmdhd[**detail** |**error** |**events**]	コマンド ヘッダーのトラブルシューティングを行うための情報を表示します。

RADIUS の機能の履歴

次の表に、このモジュールで説明する機能のリリースおよび関連情報を示します。

これらの機能は、特に明記されていない限り、導入されたリリース以降のすべてのリリースで使用できます。

機能	機能情報	リリース
RADIUS サーバーでの DSCP マーキング	**dscp** コマンドを使用して、RADIUS サーバーおよび RADIUS サーバーグループで DiffServ コードポイント（DSCP）マーキングを設定できます。**radius-server dscp** 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 RADIUS サーバーの認証およびアカウンティングのために DSCP マーキングを設定するために使用します。	IE 3x00 および ESS 3300：Cisco IOS XE Cupertino 17.8.1
RADIUS	RADIUS は、不正なアクセスからネットワークのセキュリティを保護する分散クライアント/サーバ システムです。RADIUS クライアントは、サポート対象のシスコ デバイス上で稼働します。クライアントは中央の RADIUS サーバに認証要求を送ります。中央の RADIUS サーバにはすべてのユーザ認証情報、ネットワーク サービス アクセス情報が登録されています。	IE 3x00：Cisco IOS XE Gibraltar 16.11.1 ESS 3300：Cisco IOS XE Gibraltar 16.9.1

Cisco Feature Navigator を使用すると、プラットフォームおよびソフトウェアイメージのサポート情報を検索できます。Cisco Feature Navigator には、http://www.cisco.com/go/cfn [英語] からアクセスします。

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。