
# IEEE 802.1x ポートベース認証の設定

この章では、Catalyst 3560 スイッチ上で IEEE 802.1x ポートベース認証を設定する方法について説明します。IEEE 802.1x 認証は、不正なデバイス（クライアント）によるネットワーク アクセスを防止します。

（注） この章で使用するコマンドの構文および使用方法の詳細については、『*Cisco IOS Security Command Reference*』Release 12.2 の「RADIUS Commands」およびこのリリースに対応するコマンド リファレンスを参照してください。

この章で説明する内容は、次のとおりです。

# IEEE 802.1x ポートベース認証の概要

IEEE 802.1x 規格では、一般の人がアクセス可能なポートからクライアントが LAN に接続しないように規制する（認証されている場合を除く）、クライアント / サーバ型のアクセス コントロールおよび認証プロトコルを定めています。認証サーバがスイッチ ポートに接続する各クライアントを認証したうえで、スイッチまたは LAN が提供するサービスを利用できるようにします。

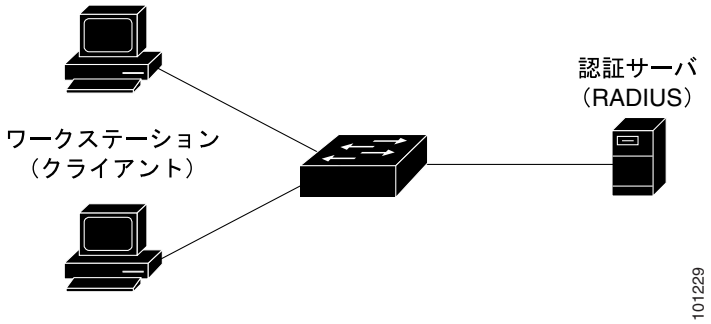
IEEE 802.1x アクセス コントロールでは、クライアントを認証するまでの間、そのクライアントが接続しているポート経由では Extensible Authentication Protocol over LAN（EAPOL）、Cisco Discovery Protocol（CDP）、および Spanning-Tree Protocol（STP; スパニングツリー プロトコル）トラフィックしか許可されません。認証後、通常のトラフィックをポート経由で送受信できます。

ここでは、IEEE 802.1x ポートベース認証について説明します。

## デバイスの役割

IEEE 802.1x ポートベース認証では、ネットワーク上のデバイスにはそれぞれ固有の役割があります（図 9-1 を参照）。

**図 9-1　IEEE 802.1x におけるデバイスの役割**




- *クライアント* — LAN およびスイッチ サービスへのアクセスを要求し、スイッチからの要求に応答するデバイス（ワークステーション）。ワークステーションでは、Microsoft Windows XP OS（オペレーティング システム）に付属しているような IEEE 802.1x 準拠のクライアント ソフトウェアを実行する必要があります（クライアントは、IEEE 802.1x 標準では*サプリカント*といいます）。

（注）　Windows XP のネットワーク接続および IEEE 802.1x 認証については、次の URL にある「Microsoft Knowledge Base」を参照してください。
http://support.microsoft.com/support/kb/articles/Q303/5/97.ASP

- *認証サーバ* — クライアントの実際の認証を行います。認証サーバはクライアントの識別情報を確認し、そのクライアントに LAN およびスイッチ サービスへのアクセスを許可すべきかどうかをスイッチに通知します。スイッチはプロキシとして動作するので、認証サービスはクライアントに対してトランスペアレントに行われます。今回のリリースでサポートされる認証サーバは、Extensible Authentication Protocol（EAP）拡張機能を備えた Remote Authentication Dial-In User Service（RADIUS）セキュリティ システムだけです。これは Cisco Secure Access Control Server バージョン 3.0 以降で利用できます。RADIUS はクライアント / サーバ モデルで動作し、RADIUS サーバと 1 つまたは複数の RADIUS クライアントとの間でセキュア認証情報を交換します。
- *スイッチ*(エッジ スイッチまたはワイヤレス アクセス ポイント) — クライアントの認証ステータスに基づいて、ネットワークへの物理アクセスを制御します。スイッチはクライアントと認証サーバとの仲介デバイス（プロキシ）として動作し、クライアントに識別情報を要求し、その情報を認証サーバで確認し、クライアントに応答をリレーします。スイッチには、EAP フレームのカプセル化とカプセル化解除、および認証サーバとの対話を処理する RADIUS クライアントが含まれています。（スイッチは、IEEE 802.1x 標準では*オーセンティケータ*といいます）。

  スイッチが EAPOL フレームを受信して認証サーバにリレーする場合、イーサネット ヘッダーが取り除かれ、残りの EAP フレームが RADIUS フォーマットに再カプセル化されます。カプセル化では EAP フレームの変更は行われないため、認証サーバはネイティブ フレーム フォーマットの EAP をサポートしなければなりません。スイッチが認証サーバからフレームを受信すると、サーバのフレーム ヘッダーが削除され、残りの EAP フレームがイーサネット用にカプセル化され、クライアントに送信されます。

  仲介デバイスとして動作できるものには、Catalyst 3750-E、Catalyst 3560-E、Catalyst 3750、Catalyst 3560、Catalyst 3550、Catalyst 2970、Catalyst 2960、Catalyst 2955、Catalyst 2950、Catalyst 2940、またはワイヤレス アクセス ポイントがあります。これらのデバイスでは、RADIUS クライアントおよび IEEE 802.1x 認証をサポートするソフトウェアが稼働している必要があります。

## 認証プロセス

IEEE 802.1x ポートベース認証がイネーブルであり、クライアントが IEEE 802.1x 準拠のクライアント ソフトウェアをサポートしている場合、次のイベントが発生します。

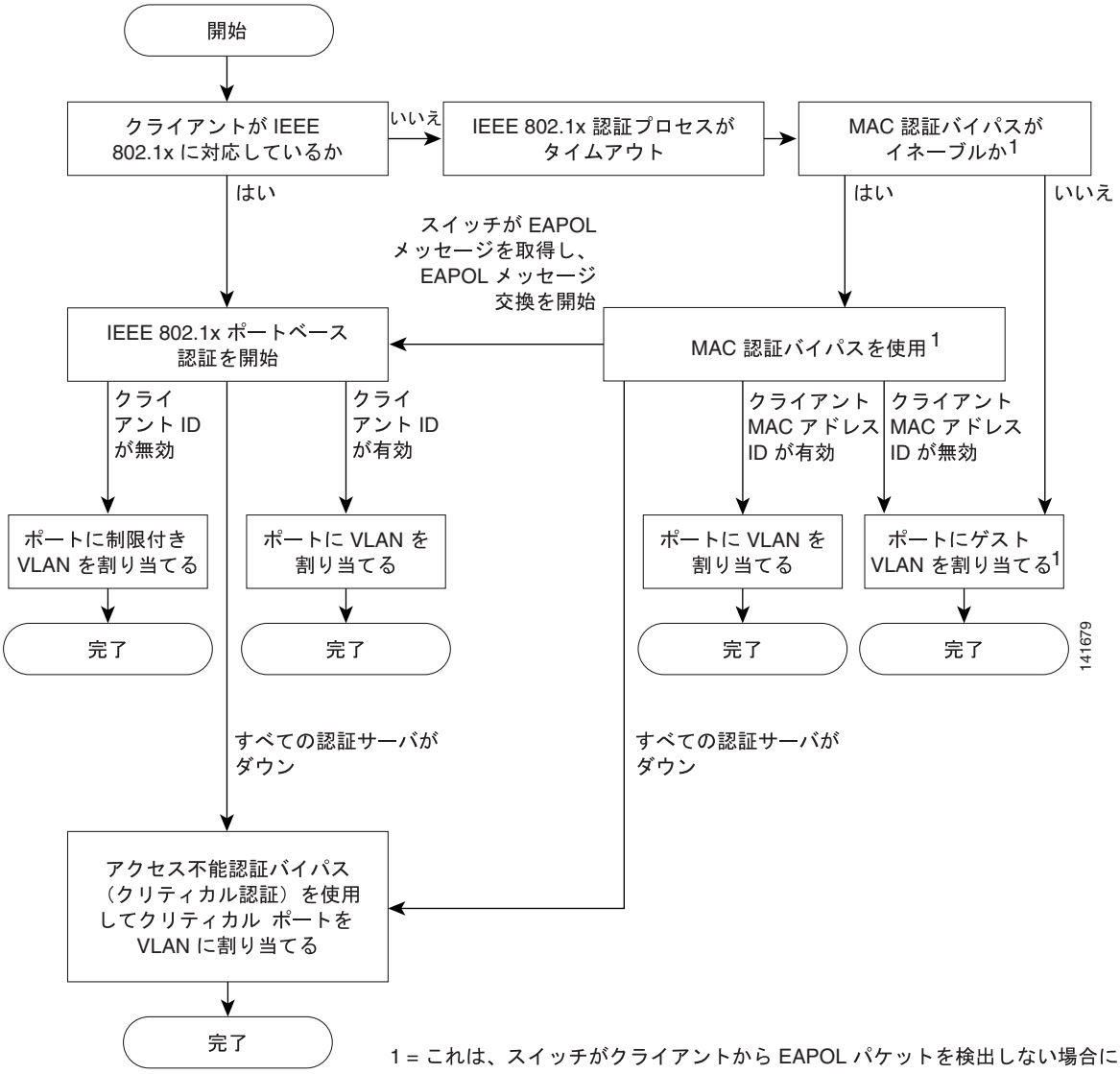
- クライアント ID が有効で IEEE 802.1x 認証に成功した場合、スイッチはクライアントにネットワークへのアクセスを許可します。
- EAPOL メッセージ交換の待機中に IEEE 802.1x 認証がタイムアウトし、MAC 認証バイパスがイネーブルの場合、スイッチはクライアント MAC アドレスを認証用に使用します。このクライアント MAC アドレスが有効で認証に成功した場合、スイッチはクライアントにネットワークへのアクセスを許可します。クライアント MAC アドレスが無効で認証に失敗した場合、ゲスト VLAN が設定されていれば、スイッチはクライアントに限定的なサービスを提供するゲスト VLAN を割り当てます。
- スイッチが IEEE 802.1x 対応クライアントから無効な ID を取得し、制限付き VLAN が指定されている場合、スイッチはクライアントに限定的なサービスを提供する制限付き VLAN を割り当てることができます。
- RADIUS 認証サーバが使用できず（ダウンしていて）アクセスできない認証バイパスがイネーブルの場合、スイッチは、RADIUS 設定 VLAN またはユーザ指定アクセス VLAN で、ポートをクリティカル認証ステートにして、クライアントにネットワークのアクセスを許可します。

**（注）** アクセスできない認証バイパスは、クリティカル認証、または Authentication, Authorization, Accounting（AAA; 認証、許可、アカウンティング）失敗ポリシーとも呼ばれます。

図 9-2 に、認証プロセスを示します。

Multidomain Authentication（MDA; マルチ ドメイン認証）がポートでイネーブルの場合、音声認証に適用可能ないくつかの例外とともにこのフローを使用することができます。MDA の詳細については、「マルチドメイン認証の使用」（p.9-19）を参照してください。

**図 9-2　認証フローチャート**




次の状況のいずれかが発生すると、スイッチはクライアントを再認証します。

- 定期的な再認証がイネーブルで、再認証タイマーの期限が切れている場合。

  スイッチ固有の値を使用するか、RADIUS サーバからの値に基づいて再認証タイマーを設定できます。

  RADIUS サーバを使用する IEEE 802.1x 認証を設定したあと、スイッチは、Session-Timeout RADIUS アトリビュート（アトリビュート [27]）と Termination-Action RADIUS アトリビュート（アトリビュート [29]）に基づいてタイマーを使用します。

  Session-Timeout RADIUS アトリビュート（アトリビュート [27]）は、再認証が発生するまでの時間を指定します。

  Termination-Action RADIUS アトリビュート（アトリビュート [29]）は、再認証中に行うアクションを指定します。アクションは *Initialize* および *ReAuthenticate* に設定できます。*Initialize* アクションが設定されていると（アトリビュートの値は *DEFAULT*）、IEEE 802.1x セッションが終了し、再認証中に接続が切断されます。*ReAuthenticate* アクションが設定されていると（アトリビュートの値は RADIUS-Request）、再認証中にセッションは影響を受けません。

- クライアントを手動で再認証するには、**dot1x re-authenticate interface** *interface-id* 特権 EXEC コマンドを入力します。

## 認証の開始およびメッセージ交換

IEEE 802.1x 認証中に、スイッチまたはクライアントは認証を開始できます。**dot1x port-control auto** インターフェイス コンフィギュレーション コマンドを使用してポート上で認証をイネーブルにした場合、スイッチはポートのリンク ステートがダウンからアップに変更した時点で、またはポートが認証されてないままアップの状態であるかぎり定期的に、認証を開始しなければなりません。スイッチはクライアントに EAP-Request/Identity フレームを送信し、その ID を要求します。クライアントはフレームを受信すると、EAP-Response/Identity フレームで応答します。

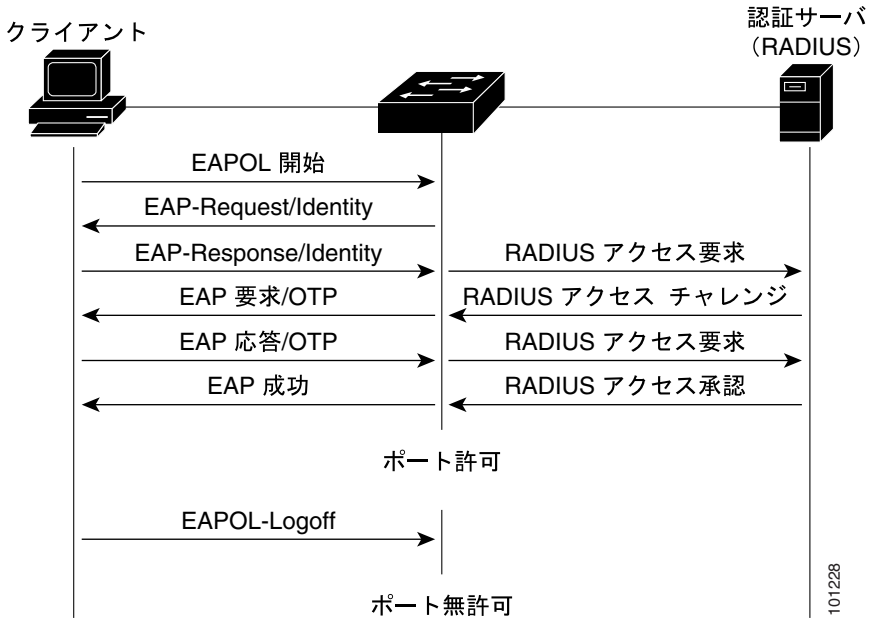
ただし、クライアントが起動時にスイッチからの EAP-Request/Identity フレームを受信しなかった場合、クライアントは EAPOL-Start フレームを送信して認証を開始できます。このフレームはスイッチに対し、クライアントの識別情報を要求するように指示します。

（注）　ネットワーク アクセス デバイスで IEEE 802.1x 認証がイネーブルに設定されていない、またはサポートされていない場合には、クライアントからの EAPOL フレームはすべて廃棄されます。クライアントが認証の開始を 3 回試みても EAP-Request/Identity フレームを受信しなかった場合、クライアントはポートが許可ステートであるものとしてフレームを送信します。ポートが許可ステートであるということは、クライアントの認証が成功したことを実質的に意味します。詳細については、「許可ステートおよび無許可ステートのポート」（p.9-7）を参照してください。

クライアントが自らの識別情報を提示すると、スイッチは仲介デバイスとしての役割を開始し、認証が成功または失敗するまで、クライアントと認証サーバの間で EAP フレームを送受信します。認証が成功すると、スイッチ ポートは許可ステートになります。認証に失敗した場合、認証が再試行されるか、ポートが限定的なサービスを提供する VLAN に割り当てられるか、あるいはネットワーク アクセスが許可されないかのいずれかになります。詳細については、「許可ステートおよび無許可ステートのポート」（p.9-7）を参照してください。

実際に行われる EAP フレーム交換は、使用する認証方式によって異なります。図 9-3 に、クライアントが RADIUS サーバとの間で OTP（ワンタイム パスワード）認証方式を使用する際に行われるメッセージ交換を示します。

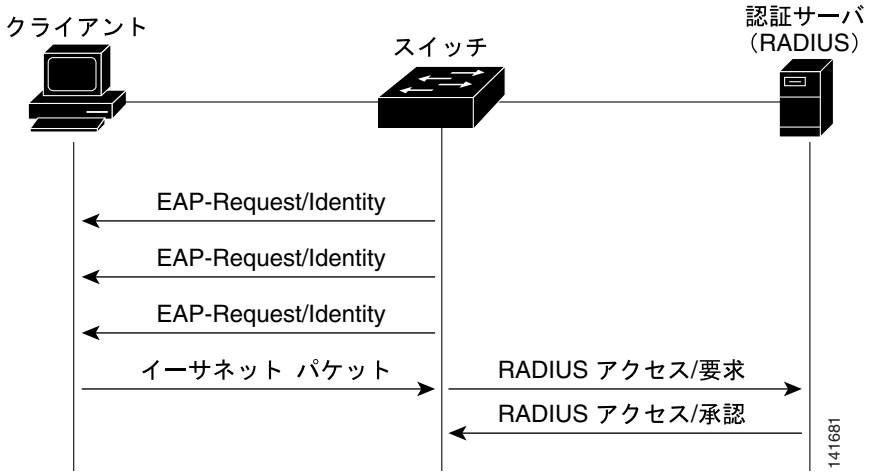
**図 9-3　メッセージ交換**



EAPOL メッセージ交換の待機中に IEEE 802.1x 認証がタイムアウトし、MAC 認証バイパスがイネーブルの場合、スイッチはクライアントからイーサネット パケットを検出するとそのクライアントを認証できます。スイッチは、クライアントの MAC アドレスを ID として使用し、RADIUS サーバに送信される RADIUS アクセス/要求フレームにこの情報を保存します。サーバがスイッチに RADIUS アクセス / 承認フレームを送信（認証が成功）すると、ポートが許可されます。認証に失敗してゲスト VLAN が指定されている場合、スイッチはポートをゲスト VLAN に割り当てます。イーサネット パケットの待機中にスイッチが EAPOL パケットを検出すると、スイッチは MAC 認証バイパス プロセスを停止して、IEEE 802.1x 認証を停止します。

図 9-4 に、MAC 認証バイパス中のメッセージ交換を示します。

**図 9-4　MAC 認証バイパス中のメッセージ交換**




## 許可ステートおよび無許可ステートのポート

IEEE 802.1x 認証中に、スイッチのポート ステートによって、スイッチはネットワークへのクライアント アクセスを許可します。ポートは最初、*無許可*ステートです。このステートでは、音声 VLAN（仮想 LAN）ポートとして設定されていないポートは IEEE 802.1x 認証、CDP、および STP パケットを除くすべての入力および出力トラフィックを禁止します。クライアントの認証が成功すると、ポートは*許可*ステートに変更し、クライアントのトラフィック送受信を通常どおりに許可します。ポートが音声 VLAN として設定されている場合、VoIP トラフィックおよび IEEE 802.1x プロトコル パケットが許可されたあとクライアントが正常に認証されます。

IEEE 802.1x をサポートしていないクライアントが、無許可ステートの IEEE 802.1x ポートに接続すると、スイッチはそのクライアントの識別情報を要求します。この状況では、クライアントは要求に応答せず、ポートは引き続き無許可ステートとなり、クライアントはネットワーク アクセスを許可されません。

反対に、IEEE 802.1x 対応のクライアントが、IEEE 802.1x 標準が稼働していないポートに接続すると、クライアントは EAPOL-Start フレームを送信して認証プロセスを開始します。応答がなければ、クライアントは同じ要求を所定の回数だけ送信します。また、応答がない場合は、クライアントはポートが許可ステートであるものとしてフレーム送信を開始します。

**dot1x port-control** インターフェイス コンフィギュレーション コマンドおよび次のキーワードを使用して、ポートの許可ステートを制御できます。

- **force-authorized** — IEEE 802.1x 認証をディセーブルにし、認証情報の交換を必要とせずに、ポートを許可ステートに変更します。ポートはクライアントの IEEE 802.1x ベース認証を行わずに、通常のトラフィックを送受信します。これがデフォルトの設定です。
- **force-unauthorized** — クライアントからの認証の試みをすべて無視し、ポートを無許可ステートのままにします。スイッチは、ポートを介してクライアントに認証サービスを提供できません。
- **auto** — IEEE 802.1x 認証をイネーブルにします。ポートは最初、無許可ステートであり、ポート経由で送受信できるのは EAPOL フレームだけです。ポートのリンク ステートがダウンからアップに変更したとき、または EAPOL-Start フレームを受信したときに、認証プロセスが開始されます。スイッチはクライアントの識別情報を要求し、クライアントと認証サーバとの間で認証メッセージのリレーを開始します。スイッチはクライアントの MAC（メディア アクセス制御）アドレスを使用して、ネットワーク アクセスを試みる各クライアントを一意に識別します。

クライアントが認証に成功すると（認証サーバから Accept フレームを受信すると）、ポートが許可ステートに変わり、認証されたクライアントからのすべてのフレームがポート経由での送受信を許可されます。認証に失敗すると、ポートは無許可ステートのままですが、認証を再試行することはできます。認証サーバに到達できない場合、スイッチは要求を再送信します。所定の回数だけ試行してもサーバから応答が得られない場合には、認証が失敗し、ネットワーク アクセスは許可されません。

クライアントはログオフするとき、EAPOL-Logoff メッセージを送信します。このメッセージによって、スイッチ ポートが無許可ステートになります。

ポートのリンク ステートがアップからダウンに変更した場合、または EAPOL-Logoff フレームを受信した場合に、ポートは無許可ステートに戻ります。

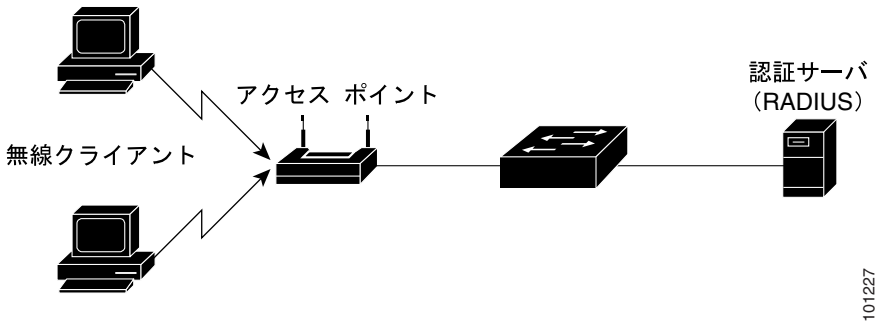
## IEEE 802.1x のホスト モード

IEEE 802.1x ポートは、シングル ホスト モードまたはマルチ ホスト モードで設定できます。シングル ホスト モード（図 9-1 を参照）では、IEEE 802.1x 対応のスイッチ ポートに接続できるのはクライアント 1 つのみです。スイッチは、ポートのリンク ステートがアップに変化したときに、EAPOL フレームを送信することでクライアントを検出します。クライアントがログオフしたとき、または別のクライアントに代わったときには、スイッチはポートのリンク ステートをダウンに変更し、ポートは無許可ステートに戻ります。

マルチ ホスト モードでは、複数のホストを単一の IEEE 802.1x 対応ポートに接続できます。図 9-5 に、ワイヤレス LAN における IEEE 802.1x ポートベース認証を示します。このモードでは、接続されたクライアントのうち 1 つが許可されれば、クライアントすべてのネットワーク アクセスが許可されます。ポートが無許可ステートになると（再認証が失敗するか、または EAPOL-Logoff メッセージを受信した場合）、スイッチは接続しているクライアントのネットワーク アクセスをすべて禁止します。このトポロジでは、ワイヤレス アクセス ポイントが接続しているクライアントの認証を処理し、スイッチに対してクライアントとしての役割を果たします。

マルチ ホスト モードがイネーブルの場合、IEEE 802.1x 認証を使用してポートおよびポート セキュリティを認証し、クライアントを含むすべての MAC アドレスのネットワーク アクセスを管理できます。

図 9-5　マルチ ホスト モードの例




Cisco IOS Release 12.2(35)SE 以降では、Multi-Domain Authentication（MDA; マルチドメイン認証）をサポートしています。これにより、データ デバイスと （シスコまたはシスコ以外の）IP 電話のような音声デバイスの両方が、独立して同一の IEEE 802.1x 対応スイッチ ポートを認証することができます。詳細については、「マルチドメイン認証の使用」（p.9-19）を参照してください。

## IEEE 802.1x アカウンティング

IEEE 802.1x 標準では、ユーザの認証およびユーザのネットワーク アクセスに対する許可方法を定義しています。ただし、ネットワークの使用法については監視しません。IEEE 802.1x アカウンティングは、デフォルトでディセーブルです。IEEE 802.1x アカウンティングをイネーブルにすると、次のアクティビティを IEEE 802.1x 対応のポート上でモニタできます。

- 正常にユーザを認証します。
- ユーザがログ オフします。
- リンクダウンが発生します。
- 再認証が正常に行われます。
- 再認証が失敗します。

スイッチは IEEE 802.1x アカウンティング情報を記録しません。その代わり、スイッチはこの情報を RADIUS サーバに送信します。RADIUS サーバは、アカウンティング メッセージを記録するように設定する必要があります。

## IEEE 802.1x アカウンティング アトリビュート値（AV）ペア

RADIUS サーバに送信された情報は、アトリビュート値（AV）ペアの形式で表示されます。これらの AV ペアのデータは、各種アプリケーションによって使用されます（たとえば課金アプリケーションの場合、RADIUS パケットの Acct-Input-Octets または Acct-Output-Octets アトリビュートの情報が必要です）。

AV ペアは、IEEE 802.1x アカウンティングが設定されているスイッチによって自動的に送信されます。次の種類の RADIUS アカウンティング パケットがスイッチによって送信されます。

- START — 新規ユーザ セッションが始まると送信されます。
- INTERIM — 既存のセッションが更新されると送信されます。
- STOP — セッションが終了すると送信されます。

次の表 9-1 に、AV ペアおよびスイッチによって送信される AV ペアの条件を示します。

表 9-1　アカウンティング AV ペア

| アトリビュート番号 | AV ペア名 | START | INTERIM | STOP |
|---|---|---|---|---|
| アトリビュート [1] | User-Name | 常時送信 | 常時送信 | 常時送信 |
| アトリビュート [4] | NAS-IP-Address | 常時送信 | 常時送信 | 常時送信 |
| アトリビュート [5] | NAS-Port | 常時送信 | 常時送信 | 常時送信 |
| アトリビュート [8] | Framed-IP-Address | 非送信 | 条件に応じて送信[1] | 条件に応じて送信[1] |
| アトリビュート [25] | Class | 常時送信 | 常時送信 | 常時送信 |
| アトリビュート [30] | Called-Station-ID | 常時送信 | 常時送信 | 常時送信 |
| アトリビュート [31] | Calling-Station-ID | 常時送信 | 常時送信 | 常時送信 |
| アトリビュート [40] | Acct-Status-Type | 常時送信 | 常時送信 | 常時送信 |
| アトリビュート [41] | Acct-Delay-Time | 常時送信 | 常時送信 | 常時送信 |
| アトリビュート [42] | Acct-Input-Octets | 非送信 | 非送信 | 常時送信 |
| アトリビュート [43] | Acct-Output-Octets | 非送信 | 非送信 | 常時送信 |
| アトリビュート [44] | Acct-Session-ID | 常時送信 | 常時送信 | 常時送信 |
| アトリビュート [45] | Acct-Authentic | 常時送信 | 常時送信 | 常時送信 |
| アトリビュート [46] | Acct-Session-Time | 非送信 | 非送信 | 常時送信 |
| アトリビュート [49] | Acct-Terminate-Cause | 非送信 | 非送信 | 常時送信 |
| アトリビュート [61] | NAS-Port-Type | 常時送信 | 常時送信 | 常時送信 |

1. ホストに対して有効な Dynamic Host Control Protocol（DHCP）バインディングが DHCP スヌーピング バインディング テーブルに存在している場合にのみ、Framed-IP-Address の AV ペアは送信されます。

スイッチによって送信された AV ペアは、**debug radius accounting** 特権 EXEC コマンドを入力することで表示できます。このコマンドの詳細については、次の URL で『*Cisco IOS Debug Command Reference*』Release 12.2 を参照してください。

http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/products_command_reference_book09186a00800872ce.html

AV ペアの詳細については、RFC 3580『*IEEE 802.1x Remote Authentication Dial In User Service (RADIUS) Usage Guidelines*』を参照してください。

## VLAN 割り当てを使用した IEEE 802.1x 認証の利用

RADIUS サーバは、VLAN 割り当てを送信してスイッチ ポートを設定します。RADIUS サーバ データベースは、ユーザ名と VLAN のマッピングを維持し、スイッチ ポートに接続するクライアントのユーザ名に基づいて VLAN を割り当てます。この機能を使用して、特定のユーザのネットワーク アクセスを制限できます。

スイッチと RADIUS サーバ上で設定された場合、VLAN 割り当てを使用した IEEE 802.1x 認証には次の特性があります。

- RADIUS サーバから VLAN が提供されない場合、または IEEE 802.1x 認証がディセーブルの場合、認証が成功するとポートはアクセス VLAN に設定されます。アクセス VLAN は、アクセス ポートに割り当てられた VLAN です。このポート上で送受信されるパケットはすべてこの VLAN に所属します。
- IEEE 802.1x 認証がイネーブルで、RADIUS サーバからの VLAN 情報が無効の場合、ポートは無許可ステートに戻り、設定済みのアクセス VLAN にとどまります。これにより、設定エラーによって不適切な VLAN に予期せぬポートが現れることを防ぎます。

設定エラーには、ルーテッド ポートの VLAN、間違った VLAN ID、存在しないまたは内部（ルーテッド ポート）の VLAN ID、あるいは音声 VLAN ID への割り当て試行の指定などがあります。

- IEEE 802.1x 認証がイネーブルで、サーバからのすべての情報が有効の場合、ポートは認証後、指定した VLAN に配置されます。
- IEEE 802.1x ポートでマルチ ホスト モードがイネーブルの場合、すべてのホストは最初に認証されたホストと同じ VLAN（RADIUS サーバにより指定）に配置されます。
- ポート上で IEEE 802.1x 認証およびポート セキュリティがイネーブルの場合、ポートは RADIUS サーバによって割り当てられた VLAN に配置されます。
- IEEE 802.1x 認証がポートでディセーブルの場合、設定済みのアクセス VLAN に戻ります。

ポートが、強制許可（force-authorized）ステート、強制無許可（force-unauthorized）ステート、無許可ステート、またはシャットダウン ステートの場合、ポートは設定済みのアクセス VLAN に配置されます。

IEEE 802.1x ポートが認証され、RADIUS サーバによって割り当てられた VLAN に配置されると、そのポートのアクセス VLAN 設定への変更は有効になりません。

トランク ポート、ダイナミック ポート、または VLAN Membership Policy Server（VMPS; VLAN メンバーシップ ポリシー サーバ）によるダイナミック アクセス ポート割り当ての場合、VLAN 割り当て機能を使用した IEEE 802.1x 認証はサポートされません。

VLAN 割り当てを設定するには、次の作業を実行する必要があります。

- **network** キーワードを使用して AAA 許可をイネーブルにし、RADIUS サーバからのインターフェイス設定を可能にします。
- IEEE 802.1x 認証をイネーブルにします。（アクセス ポートで IEEE 802.1x 認証を設定すると、VLAN 割り当て機能は自動的にイネーブルになります）。
- RADIUS サーバにベンダー固有のトンネル アトリビュートを割り当てます。RADIUS サーバは次のアトリビュートをスイッチに返す必要があります。
  - [64] Tunnel-Type = VLAN
  - [65] Tunnel-Medium-Type = 802
  - [81] Tunnel-Private-Group-ID = VLAN 名または VLAN ID

  アトリビュート [64] は、値 *VLAN*（タイプ 13）でなければなりません。アトリビュート [65] は、値 *802*（タイプ 6）でなければなりません。アトリビュート [81] は、IEEE 802.1x 認証ユーザに割り当てられた *VLAN 名*または *VLAN ID* を指定します。

トンネル アトリビュートの例については、「ベンダー固有の RADIUS アトリビュートを使用するスイッチ設定」（p.8-30）を参照してください。

## ユーザ単位 ACL を使用した IEEE 802.1x 認証の利用

ユーザ単位の Access Control List（ACL; アクセス コントロール リスト）をイネーブルにして、IEEE 802.1x 認証ユーザに対して異なるレベルのネットワーク アクセスおよびサービスを提供します。RADIUS サーバが IEEE 802.1x ポートに接続されたユーザを認証すると、ユーザ ID に基づいて ACL アトリビュートを取得してスイッチに送信します。スイッチは、ユーザ セッションの期間中、そのアトリビュートを IEEE 802.1x ポートに適用します。セッションが終了した場合、認証が失敗した場合、またはリンクダウン状態になった場合には、スイッチはユーザ単位の ACL を削除します。スイッチは、RADIUS 指定の ACL を実行コンフィギュレーションに保存しません。ポートが無許可の場合、スイッチはそのポートから ACL を削除します。

同じスイッチ上で、ルータ ACL の設定およびポート ACL の入力を行うことができます。ただし、ポート ACL はルータ ACL よりも優先されます。入力済みのポート ACL を VLAN に属するインターフェイスに適用する場合、ポート ACL は VLAN インターフェイスに適用する入力済みのルータ ACL よりも優先されます。ポート ACL が適用されたポート上で受信した着信パケットは、ポート ACL によってフィルタリングされます。その他のポートに着信したルーテッド パケットは、ルータ ACL によってフィルタリングされます。発信するルーテッド パケットは、ルータ ACL によってフィルタリングされます。設定の矛盾を避けるために、RADIUS サーバに格納するユーザ プロファイルを慎重に計画します。

RADIUS は、ベンダー固有のアトリビュートなどのユーザ単位アトリビュートをサポートします。これらのベンダー固有のアトリビュート（VSA）は、オクテット ストリング形式で、認証プロセス中にスイッチに渡されます。ユーザ単位 ACL に使用される VSA は、入力方向では `inacl#<n>` で、出力方向では `outacl#<n>` です。MAC ACL は、入力方向でのみサポートされます。スイッチは、入力方向でのみ VSA をサポートします。このスイッチでは、レイヤ 2 ポートで出力方向のポート ACL はサポートされません。詳細は、第 31 章「ACL によるネットワーク セキュリティの設定」を参照してください。

拡張 ACL 構文形式のみを使用して、RADIUS サーバに保存するユーザ単位の設定を定義します。RADIUS サーバから定義が渡されると、拡張命名規則を使用して作成されます。ただし、Filter-Id アトリビュートを使用する場合、標準 ACL を示すことができます。

Filter-Id アトリビュートを使用して、すでにスイッチに設定されている着信または発信 ACL を指定できます。アトリビュートには、ACL 番号と、その後ろに入力フィルタリング、出力フィルタリングを示す *.in* または *.out* が含まれています。RADIUS サーバが *.in* または *.out* 構文を許可しない場合、アクセス リストはデフォルトで発信 ACL に適用されます。スイッチでの Cisco IOS のアクセス リストに関するサポートが制限されているため、Filter-ID アトリビュートは 1 ～ 199 および 1300 ～ 2699 の IP ACL（IP 標準 ACL および IP 拡張 ACL）に対してのみサポートされます。

1 ポートがサポートする IEEE 802.1x 認証ユーザは 1 ユーザのみです。マルチ ホスト モードがポートでイネーブルの場合、ユーザ単位 ACL アトリビュートは関連ポートでディセーブルです。

ユーザ単位 ACL の最大サイズは 4000 ASCII 文字ですが、RADIUS サーバのユーザ単位 ACL の最大サイズによって制限されます。

ベンダー固有のアトリビュートの例については、「ベンダー固有の RADIUS アトリビュートを使用するスイッチ設定」（p.8-30）を参照してください。ACL の設定の詳細については、第 31 章「ACL によるネットワーク セキュリティの設定」を参照してください。

ユーザ単位の ACL を設定するには、次の作業を実行する必要があります。

- AAA 認証をイネーブルにします。
- **network** キーワードを使用して AAA 許可をイネーブルにし、RADIUS サーバからのインターフェイス設定を可能にします。
- IEEE 802.1x 認証をイネーブルにします。
- RADIUS サーバにユーザ プロファイルと VSA を設定します。
- シングル ホスト モードの IEEE 802.1x ポートを設定します。

## ゲスト VLAN を使用した IEEE 802.1x 認証の利用

スイッチ上の各 IEEE 802.1x ポートにゲスト VLAN を設定し、クライアントに対して限定的なサービスを提供できます（IEEE 802.1x クライアントのダウンロードなど）。これらのクライアントは IEEE 802.1x 認証用にシステムをアップグレードできる場合がありますが、一部のホスト（Windows 98 システムなど）は IEEE 802.1x 対応ではありません。

スイッチが EAP Request/Identity フレームに対する応答を受信していない場合、または EAPOL パケットがクライアントによって送信されない場合に、IEEE 802.1x ポート上でゲスト VLAN をイネーブルにすると、スイッチはクライアントにゲスト VLAN を割り当てます。

Cisco IOS RELEASE 12.2(25)SE 以降では、スイッチは EAPOL パケット履歴を維持します。EAPOL パケットがリンクの存続時間中にインターフェイスで検出された場合、スイッチはそのインターフェイスに接続されているデバイスが IEEE 802.1x 対応のものであると判断します。インターフェイスはゲスト VLAN ステートにはなりません。インターフェイスのリンク ステータスがダウンした場合、EAPOL 履歴はクリアされます。EAPOL パケットがインターフェイスで検出されない場合、そのインターフェイスはゲスト VLAN のステートになります。

Cisco IOS Release 12.2(25)SE より前のリリースでは、スイッチは EAPOL パケット履歴を維持せずに、インターフェイスで EAPOL パケットが検出されているかどうかにかかわらず、ゲスト VLAN への認証アクセスに失敗したクライアントを許可しました。**dot1x guest-vlan supplicant** 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このオプション機能をイネーブルにできます。ただし、Cisco IOS Release 12.2(25)SEE では、**dot1x guest-vlan supplicant** グローバル コンフィギュレーション コマンドはサポートされていません。制限付き VLAN を使用してネットワーク アクセスの認証に失敗したクライアントを許可するには、**dot1x auth-fail vlan** *vlan-id* インターフェイス コンフィギュレーション コマンドを入力します。

Cisco IOS Release 12.2(25)SEE 以降では、リンクの存続時間中にデバイスが EAPOL パケットを送信した場合、スイッチはゲスト VLAN への認証アクセスに失敗したクライアントを許可しません。

（注）　インターフェイスがゲスト VLAN に変わってから EAPOL パケットが検出された場合、無許可ステートに戻って 802.1x 認証を再起動します。

スイッチ ポートがゲスト VLAN に変わると、IEEE 802.1x 非対応クライアントはすべてアクセスを許可されます。ゲスト VLAN が設定されているポートに IEEE 802.1x 対応クライアントが加入すると、ポートは、ユーザ設定によるアクセス VLAN で無許可ステートになり、認証が再起動されます。

ゲスト VLAN は、IEEE 802.1x ポート上でシングル ホスト モードまたはマルチ ホスト モードでサポートされています。

RSPAN VLAN、プライベート VLAN、音声 VLAN を除いて、アクティブ VLAN を IEEE 802.1x ゲスト VLAN として設定できます。ゲスト VLAN 機能は、内部 VLAN（ルーテッド ポート）またはトランク ポートではサポートされていません。アクセス ポート上でのみサポートされます。

Cisco IOS Release 12.2(25)SEE 以降のリリースでは、スイッチが、*MAC 認証バイパス* をサポートしています。MAC 認証バイパスが IEEE 802.1x ポートでイネーブルの場合、スイッチは、IEEE 802.1x 認証のタイムアウト時に EAPOL メッセージ交換を待機している間、クライアント MAC アドレスに基づいてクライアントを許可できます。IEEE 802.1x ポートでクライアントを検出したあと、スイッチはクライアントからイーサネット パケットを待ちます。スイッチは MAC アドレスに基づいて、ユーザ名とパスワードとともに RADIUS アクセス / 要求フレームを認証サーバに送信します。認証に成功した場合、スイッチはクライアントにネットワークへのアクセスを許可します。認証に失敗した場合、ゲスト VLAN が指定されていれば、スイッチはポートをゲスト VLAN に割り当てます。詳細については、「MAC 認証バイパスを使用した IEEE 802.1x 認証の利用」（p.9-18）を参照してください。

詳細については、「ゲスト VLAN の設定」（p.9-34）を参照してください。

## 制限付き VLAN による IEEE 802.1x 認証の利用

ゲスト VLAN にアクセスできないクライアント向けに、限定されたサービスを提供するために、スイッチの各 IEEE 802.1x ポートに対して制限付き VLAN（*認証失敗 VLAN* と呼ばれることもあります）を設定できます。これらのクライアントは、認証プロセスに失敗したため他の VLAN にアクセスできない IEEE 802.1x 対応クライアントです。制限付き VLAN を使用すると、認証サーバの有効な証明書を持っていないユーザ（通常、企業にアクセスするユーザ）に、サービスを制限したアクセスを提供できます。管理者は制限付き VLAN のサービスを制御できます。

（注）　両方のタイプのユーザに同じサービスを提供する場合、ゲスト VLAN と制限付き VLAN の両方を同じに設定できます。

この機能がないと、クライアントは認証失敗を永遠に繰り返すことになるため、スイッチ ポートがスパニングツリーのブロッキング ステートから変わることができなくなります。制限付き VLAN の機能を使用することで、クライアントの認証試行回数を指定し（デフォルト値は 3 回）、一定回数後にスイッチ ポートを制限付き VLAN の状態に移行させることができます。

認証サーバはクライアントの認証試行回数をカウントします。このカウントが設定した認証試行回数を超えると、ポートが制限付き VLAN の状態に変わります。失敗した試行回数は、RADIUS サーバが *EAP failure* で応答したときや、EAP パケットなしの空の応答を返したときからカウントされます。ポートが制限付き VLAN に変わったら、このカウント数はリセットされます。

認証に失敗したユーザの VLAN は、もう一度認証を実行するまで制限された状態が続きます。制限付き VLAN 内のポートは設定された間隔に従って再認証を試みます（デフォルトは 60 秒）。再認証に失敗している間は、ポートの VLAN は制限された状態が続きます。再認証に成功した場合、ポートは設定された VLAN もしくは RADIUS サーバによって送信された VLAN に移行します。再認証はディセーブルにすることもできますが、ディセーブルにすると、*link down* または *EAP logoff* イベントを受信しないかぎり、ポートの認証プロセスを再起動できません。クライアントがハブを介して接続している場合、再認証機能はイネーブルにしておくことを推奨します。クライアントの接続をハブから切り離すと、ポートに *link down* や *EAP logoff* イベントが送信されない場合があります。

ポートが制限付き VLAN に移行すると、EAP 成功の擬似メッセージがクライアントに送信されます。このメッセージによって、繰り返し実行している再認証を停止させることができます。クライアントによっては（Windows XP が稼働しているデバイスなど）、EAP なしで DHCP を実装できません。

制限付き VLAN は、レイヤ 2 ポートにある IEEE 802.1x ポート上でシングル ホスト モードの場合のみサポートされます。

RSPAN VLAN、プライマリ プライベート VLAN、音声 VLAN を除いて、アクティブ VLAN を IEEE 802.1x 制限付き VLAN として設定できます。制限付き VLAN 機能は、内部 VLAN（ルーテッド ポート）またはトランク ポートではサポートされていません。アクセス ポート上でのみサポートされます。

この機能はポート セキュリティと連動します。ポートが認証されると、すぐに MAC アドレスがポート セキュリティに提供されます。ポート セキュリティがその MAC アドレスを許可しない場合、またはセキュア アドレス カウントが最大数に達している場合、ポートは無許可になり、errordisable ステートに移行します。

ダイナミック Address Resolution Protocol（ARP; アドレス解決プロトコル）検査、DHCP スヌーピング、および IP 送信元ガードのような他のポート セキュリティ機能は、制限付き VLAN に対して個別に設定できます。

詳細については、「制限付き VLAN の設定」（p.9-35）を参照してください。

## アクセス不能認証バイパスによる IEEE 802.1x 認証の使用

Cisco IOS Release 12.2(25)SED 以降では、スイッチが設定された RADIUS サーバに到達できず、ホストが認証されない場合、*クリティカル* ポートに接続されたホストにネットワーク アクセスできるようスイッチを設定できます。クリティカル ポートは、アクセス不能認証バイパス機能（*クリティカル認証*、または *AAA 失敗ポリシー*とも呼ばれます）に対してイネーブルになっています。

この機能がイネーブルの場合、スイッチはクリティカル ポートに接続されたホストの認証を行う際に、RADIUS サーバのステータスを確認します。利用可能なサーバが 1 つあれば、スイッチはホストを認証できます。ただし、すべての RADIUS サーバが利用不可能な場合は、スイッチはホストへのネットワーク アクセスを許可して、ポートを認証ステートの特別なケースであるクリティカル認証ステートにします。

アクセス不能認証バイパス機能の動作は、ポートの許可ステートにより異なります。

- クリティカル　ポートに接続されているホストが認証しようとする際にポートが無許可ですべてのサーバが利用できない場合、スイッチは RADIUS 設定済み VLAN またはユーザ指定のアクセス VLAN にあるポートをクリティカル認証ステートにします。
- ポートが許可済みで、再認証が行われた場合、スイッチは現在の VLAN（事前に RADIUS サーバにより割り当てられた）でクリティカル ポートをクリティカル認証ステートにします。
- 認証交換中に RADIUS サーバが利用不可能となった場合、現在の交換はタイム アウトとなり、スイッチは次の認証試行の間にクリティカル ポートをクリティカル認証ステートとします。

ホストを認証できる RADIUS サーバが利用可能な場合、クリティカル認証ステートのすべてのクリティカル ポートは自動的に再認証されます。

アクセス不能認証バイパスは、次の機能と相互に作用します。

- ゲスト VLAN — アクセス不能認証バイパスは、ゲスト VLAN と互換性があります。ゲスト VLAN が IEEE 802.1x ポートでイネーブルの場合、この機能は次のように相互に作用します。
  - スイッチが EAP Request/Identity フレームへの応答を受信しないとき、または EAPOL パケットがクライアントによって送信されないときに、少なくとも 1 つの RADIUS サーバが使用できれば、スイッチはクライアントにゲスト VLAN を割り当てます。
  - すべての RADIUS サーバが使用できず、クライアントがクリティカル ポートに接続されている場合、スイッチはクライアントを認証して、クリティカル ポートを RADIUS 認証済み VLAN またはユーザ指定のアクセス VLAN でクリティカル認証ステートにします。
  - すべての RADIUS サーバが使用できず、クライアントがクリティカル ポートに接続されていない場合、ゲスト VLAN が設定されていても、スイッチはクライアントにゲスト VLAN を割り当てられません。
  - すべての RADIUS サーバが使用できず、クライアントがクリティカル ポートに接続されていて、すでにゲスト VLAN が割り当てられている場合、スイッチはそのポートをゲスト VLAN に保持します。
- 制限付き VLAN — ポートがすでに制限付き VLAN で許可されていて RADIUS サーバが使用できない場合、スイッチはクリティカル ポートを制限付き VLAN でクリティカル認証ステートにします。
- IEEE 802.1x アカウンティング — RADIUS サーバが使用できない場合、アカウンティングは影響を受けません。
- プライベート VLAN — プライベート VLAN ホスト ポートにアクセス不能認証バイパスを設定できます。アクセス VLAN は、セカンダリ VLAN でなければなりません。
- 音声 VLAN — アクセス不能認証バイパスは音声 VLAN と互換性がありますが、RADIUS 設定済み VLAN またはユーザ指定のアクセス VLAN は、音声 VLAN と異なっていなければなりません。
- Remote Switched Port Analyzer（RSPAN）— アクセス不能認証バイパスの RADIUS 設定またはユーザ指定のアクセス VLAN として RSPAN VLAN を指定しないでください。

## 音声 VLAN ポートを使用した IEEE 802.1x 認証の利用

音声 VLAN ポートは特殊なアクセス ポートで、次の 2 つの VLAN ID が対応付けられています。

- IP Phone との間で音声トラフィックを伝送する VVID。VVID は、ポートに接続された IP Phone を設定するために使用されます。
- IP Phone を通じて、スイッチと接続しているワークステーションとの間でデータ トラフィックを伝送する PVID。PVID は、ポートのネイティブ VLAN です。

IP Phone は、ポートの認証ステートにかかわらず、音声トラフィック用に VVID を使用します。これにより、IP Phone は IEEE 802.1x 認証とは独立して動作できます。

シングル ホスト モードでは、IP Phone だけが音声 VLAN で許可されます。マルチ ホスト モードでは、サプリカントが PVID で認証されたあと、追加のクライアントがトラフィックを音声 VLAN 上で送信できます。マルチ ホスト モードがイネーブルの場合、サプリカント認証は PVID と VVID の両方に影響します。

リンクがあるとき、音声 VLAN ポートはアクティブになり、IP Phone からの最初の CDP メッセージを受け取るとデバイスの MAC アドレスが表示されます。Cisco IP Phone は、他のデバイスから受け取った CDP メッセージをリレーしません。その結果、複数の IP Phone が直列に接続されている場合、スイッチは直接接続されている 1 台の IP Phone のみを認識します。音声 VLAN ポートで IEEE 802.1x 認証がイネーブルの場合、スイッチは 2 ホップ以上離れた認識されない IP Phone からのパケットを廃棄します。

IEEE 802.1x 認証をポート上でイネーブルにすると、音声 VLAN の機能を持つポート VLAN は設定できません。

（注）　音声 VLAN が設定され、Cisco IP Phone が接続されているアクセス ポートで IEEE 802.1x 認証をイネーブルにした場合、Cisco IP Phone のスイッチへの接続が最大 30 秒間失われます。

音声 VLAN の詳細については、第 15 章「音声 VLAN の設定」を参照してください。

## ポート セキュリティを使用した IEEE 802.1x 認証の利用

シングル ホスト モードまたはマルチ ホスト モードのどちらでもポート セキュリティを備えた IEEE 802.1x ポートを設定できます（**switchport port-security** インターフェイス コンフィギュレーション コマンドを使用してポートにポート セキュリティを設定する必要があります）。ポートでポート セキュリティおよび IEEE 802.1x 認証をイネーブルに設定すると、IEEE 802.1x 認証はそのポートを認証し、ポート セキュリティはそのクライアントを含むすべての MAC アドレスに対するネットワーク アクセスを管理します。この場合、IEEE 802.1x ポートを介してネットワークへアクセスできるクライアントの数とグループを制限できます。

次に、スイッチ上での IEEE 802.1x 認証とポート セキュリティ間における相互関係の例を示します。

- クライアントが認証され、ポート セキュリティ テーブルがいっぱいになっていない場合、クライアントの MAC アドレスがセキュア ホストのポート セキュリティ リストに追加されます。追加されると、ポートが通常どおりアクティブになります。

  クライアントが認証されて、ポート セキュリティが手動で設定された場合、セキュア ホスト テーブル内のエントリは保証されます（ポート セキュリティのスタティック エージングがイネーブルになっていない場合）。

クライアントが認証されてもポート セキュリティ テーブルがいっぱいの場合、セキュリティ違反が発生します。これは、セキュア ホストの最大数がスタティックに設定されているか、またはセキュア ホスト テーブルでのクライアントの有効期限が切れた場合に発生します。クライアントのアドレスの有効期限が切れた場合、そのクライアントのセキュア ホスト テーブル内でのエントリは他のホストに取って代わられます。

最初に認証されたホストが原因でセキュリティ違反が発生すると、ポートは error-disabled ステートになり、ただちにシャットダウンします。

セキュリティ違反発生時の動作は、ポート セキュリティ違反モードによって決まります。詳細については、「セキュリティ違反」（p.24-11）を参照してください。

- **no switchport port-security mac-address** *mac-address* インターフェイス コンフィギュレーション コマンドを使用して、ポート セキュリティ テーブルから IEEE 802.1x クライアント アドレスを手動で削除する場合、**dot1x re-authenticate interface** *interface-id* 特権 EXEC コマンドを使用して、IEEE 802.1x クライアントを再認証する必要があります。
- IEEE 802.1x クライアントがログオフすると、ポートが未認証ステートに変更され、クライアントのエントリを含むセキュア ホスト テーブル内のダイナミック エントリがすべてクリアされます。ここで通常の認証が実行されます。
- ポートが管理上のシャットダウン状態になると、ポートは未認証ステートになり、ダイナミック エントリはすべてセキュア ホスト テーブルから削除されます。
- シングル ホスト モードまたはマルチ ホスト モードのいずれの場合でも、IEEE 802.1x ポート上でポート セキュリティと音声 VLAN を同時に設定できます。ポート セキュリティは、Voice VLAN Identifier（VVID）および Port VLAN Identifier（PVID）の両方に適用されます。

スイッチ上でポート セキュリティをイネーブルにする手順については、「ポート セキュリティの設定」（p.24-10）を参照してください。

## WoL 機能を使用した IEEE 802.1x 認証の利用

IEEE 802.1x 認証の Wake-on-LAN（WoL）機能を使用すると、スイッチにマジック パケットと呼ばれる特定のイーサネット フレームを受信させて、休止状態の PC を起動させることができます。この機能は、管理者が休止状態のシステムへ接続しなければならない場合に役立ちます。

WoL を使用するホストが IEEE 802.1x ポートを通じて接続され、ホストの電源がオフになると、IEEE 802.1x ポートは無許可になります。無許可になったポートは EAPOL パケットしか送受信できないため、WoL マジック パケットはホストに届きません。さらに PC が休止状態になると、PC が認証されなくなるため、スイッチ ポートは閉じたままになります。

スイッチが WoL 機能を有効にした IEEE 802.1x 認証を使用している場合、スイッチはマジック パケットを含むトラフィックを無許可の IEEE 802.1x ポートに転送します。ポートが無許可の間、スイッチは EAPOL パケット以外の入力トラフィックをブロックし続けます。ホストはパケットを受信できますが、パケットをネットワーク内にある他のデバイスに送信できません。

（注）　PortFast がポートでイネーブルになっていないと、そのポートは強制的に双方向ステートになります。

**dot1x control-direction in** インターフェイス コンフィギュレーション コマンドを使用してポートを単一方向に設定すると、そのポートはスパニングツリー フォワーディング ステートに変わります。ポートはパケットをホストに送信できますが、ホストからパケットを受信できません。

**dot1x control-direction both** インターフェイス コンフィギュレーション コマンドを使用してポートを双方向に設定すると、そのポートのアクセスが双方向で制御されます。ポートは、ホストとの間でパケットを送受信しません。

## MAC 認証バイパスを使用した IEEE 802.1x 認証の利用

MAC 認証バイパス機能を使用し、クライアント MAC アドレス（図 9-2 参照）に基づいてクライアントを許可するようにスイッチを設定できます。たとえば、プリンタなどのデバイスに接続された IEEE 802.1x ポートでこの機能をイネーブルにできます。

クライアントからの EAPOL 応答の待機中に IEEE 802.1x 認証がタイムアウトした場合、スイッチは MAC 認証バイパスを使用してクライアントを許可しようとします。

MAC 認証バイパス機能が IEEE 802.1x ポートでイネーブルの場合、スイッチはクライアント ID として MAC アドレスを使用します。認証サーバには、ネットワーク アクセスを許可されたクライアント MAC アドレスのデータベースがあります。IEEE 802.1x ポートでクライアントを検出したあと、スイッチはクライアントからイーサネット パケットを待ちます。スイッチは MAC アドレスに基づいて、ユーザ名とパスワードとともに RADIUS アクセス / 要求フレームを認証サーバに送信します。認証に成功した場合、スイッチはクライアントにネットワークへのアクセスを許可します。許可が失敗した場合、ゲスト VLAN が設定されていれば、スイッチはポートをゲスト VLAN に割り当てます。

リンクの存続時間中にインターフェイスで EAPOL パケットが検出された場合、スイッチはそのインターフェイスに接続されているデバイスが IEEE 802.1x 対応サプリカントであると判断し、インターフェイスを許可するために（MAC 認証バイパスではなく）IEEE 802.1x 認証を使用します。インターフェイスのリンク ステータスがダウンした場合、EAPOL 履歴はクリアされます。

スイッチがすでに MAC 認証バイパスを使用してポートを許可し、IEEE 802.1x サプリカントを検出している場合、スイッチはポートに接続されているクライアントを許可します。再認証が発生するときに、Termination-Action RADIUS アトリビュート値が DEFAULT であるために前のセッションが終了した場合、スイッチは優先再認証プロセスとして IEEE 802.1x 認証を使用します。

MAC 認証バイパスを使用して許可されたクライアントを再認証できます。再認証プロセスは、IEEE 802.1x を使用して認証されたクライアントに対するプロセスと同じです。再認証中は、ポートは前に割り当てられた VLAN のままです。再認証に成功すると、スイッチはポートを同じ VLAN に保持します。再認証に失敗した場合、ゲスト VLAN が設定されていれば、スイッチはポートをゲスト VLAN に割り当てます。

再認証が Session-Timeout RADIUS アトリビュート（アトリビュート [27]）と Termination-Action RADIUS アトリビュート（アトリビュート [29]）に基づいており、Termination-Action RADIUS アトリビュート（アトリビュート [29]）のアクションが *Initialize*（*初期化*）される場合（アトリビュート値が *DEFALUT*）、MAC 認証バイパス セッションが終了して、再認証中に接続が切断されます。MAC 認証バイパス機能が IEEE 802.1x 認証がタイムアウトした場合、スイッチは MAC 認証バイパス機能を使用して再認証を開始します。AV ペアの詳細については、RFC 3580『*IEEE 802.1x Remote Authentication Dial In User Service (RADIUS) Usage Guidelines*』を参照してください。

MAC 認証バイパスは、次の機能と相互に作用します。

- IEEE 802.1x 認証 — IEEE 802.1x 認証がポートでイネーブルの場合にのみ MAC 認証バイパスをイネーブルにできます。
- ゲスト VLAN — クライアントの MAC アドレス ID が無効な場合、ゲスト VLAN が設定されていれば、スイッチは VLAN にクライアントを割り当てます。
- 制限付き VLAN — IEEE 802.1x ポートに接続されているクライアントが MAC 認証バイパスで認証されている場合には、この機能はサポートされません。
- ポート セキュリティ — 「ポート セキュリティを使用した IEEE 802.1x 認証の利用」（p.9-16）を参照してください。
- 音声 VLAN — 「音声 VLAN ポートを使用した IEEE 802.1x 認証の利用」（p.9-16）を参照してください。
- VLAN Menbership Policy Server（VMPS; VLAN メンバーシップ ポリシー サーバ）— IEEE 802.1x および VMPS は相互に排他的です。

- プライベート VLAN — クライアントをプライベート VLAN に割り当てられます。
- Network Admission Control（NAC）レイヤ 2 IP 検証 — この機能は、IEEE 802.1x ポートが例外リスト内のホストを含む MAC 認証バイパスを使用して認証されると有効になります。

## NAC レイヤ 2 IEEE 802.1x 検証の利用

Cisco IOS Release 12.2(25)SED 以降では、スイッチは NAC レイヤ 2 IEEE 802.1x 検証をサポートします。これは、デバイス ネットワーク アクセスを許可する前に、エンドポイント システムやクライアントのウイルス対策の状態や*態勢*をチェックします。NAC レイヤ 2 IEEE 802.1x 検証を使用すると、以下の作業を実行できます。

- Session-Timeout RADIUS アトリビュート（アトリビュート [27]）と Termination-Action RADIUS アトリビュート（アトリビュート [29]）を認証サーバからダウンロードします。
- Session-Timeout RADIUS アトリビュート（アトリビュート [27]）の値として再認証試行間の秒数を指定し、RADIUS サーバからクライアントのアクセス ポリシーを取得します。
- スイッチが Termination-Action RADIUS アトリビュート（アトリビュート [29]）を使用してクライアントを再認証する際のアクションを設定します。アクションの設定値が *DEFAULT* であるか、値が設定されていない場合、セッションは終了します。値が RADIUS 要求の場合、再認証プロセスが開始します。
- **show dot1x** 特権 EXEC コマンドを使用して、クライアントの態勢を表示する NAC ポスチャ トークンを表示します。
- ゲスト VLAN としてセカンダリ プライベート VLAN を設定します。

NAC レイヤ 2 IEEE 802.1x 検証の設定は、RADIUS サーバにポスチャ トークンを設定する必要があることを除いて、IEEE 802.1x ポートベース認証と似ています。NAC レイヤ 2 IEEE 802.1x 検証の設定に関する詳細については、「NAC レイヤ 2 IEEE 802.1x 検証の設定」（p.9-40）および「定期的な再認証の設定」（p.9-30）を参照してください。

NAC の詳細については、『*Network Admission Control Software Configuration Guide*』を参照してください。

## マルチドメイン認証の使用

このスイッチは、MDA をサポートしています。これにより、データ デバイスと（シスコまたはシスコ以外の）IP 電話のような音声 デバイスの両方が、独立して同一の IEEE 802.1x 対応スイッチ ポートを認証することができます。ポートは、データ ドメインと音声ドメインに分けられます。

MDA は、デバイス認証の順序を強制しません。しかし、最良の結果を出すには、MDA 対応ポートでは音声デバイスをデータ デバイスの前に認証することを推奨します。

MDA を設定するときには、次の注意事項に従ってください。

- MDA 用にスイッチ ポートを設定するには、「ホスト モードの設定」（p.9-29）を参照してください。
- ホスト モードがマルチドメインに設定される際に IP 電話の音声 VLAN を設定する必要があります。詳細は、第 15 章「音声 VLAN の設定」を参照してください。

**（注）** ダイナミック VLAN を使用して音声 VLAN を MDA 対応スイッチ ポートに割り当てる場合、音声デバイスで認証が失敗します。

- 音声デバイスを認証するには、値が device-traffic-class=voice の Cisco AV のペア アトリビュートを送信するように AAA サーバを設定する必要があります。この値がない場合、スイッチは音声デバイスをデータ デバイスとして扱います。
- ゲスト VLAN および制限付き VLAN 機能は、MDA 対応レポートのデータ デバイスにのみ適用されます。スイッチは、認証に失敗した音声デバイスをデータ デバイスとして扱います。
- 複数のデバイスでポートの音声またはデータ ドメインの認証を行おうとすると、errdisable になります。
- デバイスが認証されるまで、ポートでトラフィックが廃棄されます。シスコ製以外の IP 電話や音声デバイスがデータおよび音声 VLAN で許可されます。データ VLAN では、音声デバイスを DHCP サーバに接続して IP アドレスおよび音声 VLAN 情報を取得することができます音声デバイスが 音声 VLAN で送信を開始したあと、データ VLAN へのアクセスはブロックされます。
- データ VLAN とバインドしている音声デバイス MAC アドレスは、ポート セキュリティ MAC アドレス制限にカウントされません。
- データ デバイスに対してのみ、RADIUS サーバからのダイナミック VLAN 割り当てを使用することができます。
- MDA は、フォールバック メカニズムとして MAC 認証バイパスを使用して、IEEE 802.1x 認証をサポートしていないデバイスにスイッチポートを接続することができます。詳細については、「MAC 認証バイパス」（p.9-25）を参照してください。
- *データ*または*音声*デバイスがポートで検出されると、認証に成功するまでその MAC アドレスがブロックされます。認証に失敗した場合、MAC アドレスが 5 分間ブロックされたままになります。
- ポートが未認証中に 6 個以上のデバイスが*データ* VLAN で検出された場合や、複数の*音声*デバイスが音声 VLAN で検出された場合、ポートは errdisable になります。
- ポートのホスト モードがシングル ホストまたはマルチホストからマルチドメイン モードに変更される際に、認証済のデータ デバイスはポートで認証済のままになります。ただし、ポート音声 VLAN で許可されている Cisco IP Phone は自動的に削除され、そのポートで再認証される必要があります。
- ポートがシングルまたはマルチホスト モードからマルチドメイン モードに変更された後に、ゲスト VLAN や制限付き VLAN などのアクティブなフォールバック メカニズムは設定されたままになります。
- マルチドメイン モードからシングル ホストまたはマルチホスト モードにポートを切り替えると、ポートからすべての認証済デバイスが削除されます。
- データ ドメインがまず認証されてゲスト VLAN に配置された場合、IEEE 802.1x 非対応音声デバイスは認証をトリガするために音声 VLAN 上のパケットにタグを付ける必要があります。
- MDA 対応ポートでは、ユーザ単位 ACL を推奨しません。ユーザ単位 ACL ポリシーを有する認証済デバイスは、ポートの音声およびデータ VLAN の両方のトラフィックに影響を与える可能性があります。使用する場合、ポート上の 1 デバイスのみでユーザ単位 ACL が実行されます。

## Web 認証の使用

Web ブラウザを使用して、IEEE 802.1x 機能をサポートしないクライアントを認証することができます。

Web 認証のみを使用してポートを設定することが可能です。また、まず IEEE 802.1x 認証を試行してみて、クライアントが IEEE 802.1x 認証をサポートしていない場合は Web 認証を使用するようにポート設定することも可能です。

Web 認証には、2 種類の Cisco AV のペア アトリビュートが必要です。

- 最初のアトリビュート priv-lvl=15 は、常に *15* に設定しておく必要があります。これにより、スイッチにログインするユーザの権限レベルが設定されます。

- 次のアトリビュートが、Web　認証ホストに対して適用されるアクセス　リストです。構文は、IEEE 802.1x ユーザ単位 ACL と似ています。ただし、ip:inacl の代わりに、このアトリビュートは proxyacl で開始され、各エントリの source フィールドは any でなければなりません。（認証後、ACL が適用された時にクライアント IP アドレスが any フィールドを置き換えます。

  次に例を示します。

```
proxyacl# 10=permit ip any 10.0.0.0 255.0.0.0
proxyacl# 20=permit ip any 11.1.0.0 255.255.0.0
proxyacl# 30=permit udp any any eq syslog
proxyacl# 40=permit udp any any eq tftp
```

（注）　*proxyacl* エントリは、すべての許可済ネットワーク アクセスのタイプを決定します。

詳細については、「Web 認証の設定」（p.9-41）を参照してください。

# IEEE 802.1x 認証の設定

ここでは、次の設定情報について説明します。



## IEEE 802.1x 認証のデフォルト設定

表 9-2 に、IEEE 802.1x 認証のデフォルト設定を示します。

**表 9-2　IEEE 802.1x 認証のデフォルト設定**

| 機能 | デフォルト設定 |
|---|---|
| スイッチの IEEE 802.1x イネーブル ステート | ディセーブル |
| ポート単位の IEEE 802.1x イネーブル ステート | ディセーブル（force-authorized）<br>ポートはクライアントの IEEE 802.1x ベース認証を行わずに、通常のトラフィックを送受信します。 |
| Authentication, Authorization, Accounting（AAA; 認証、許可、アカウンティング） | ディセーブル |
| RADIUS サーバ<br>• IP アドレス<br>• UDP 認証ポート<br>• 鍵 | <br>• 指定なし<br>• 1812<br>• 指定なし |
| ホスト モード | シングル ホスト モード |
| 制御方向 | 双方向制御 |

表 9-2　IEEE 802.1x 認証のデフォルト設定（続き）

| 機能 | デフォルト設定 |
|---|---|
| 定期的な再認証 | ディセーブル |
| 再認証の間隔（秒） | 3600 秒 |
| 再認証回数 | 2 回（ポートが無許可ステートに変わる前に、スイッチが認証プロセスを再開する回数） |
| 待機時間 | 60 秒（スイッチがクライアントとの認証情報の交換に失敗したあと、待機状態を続ける秒数） |
| 再送信時間 | 30 秒（スイッチが EAP-Request/Identity フレームに対するクライアントからの応答を待ち、要求を再送信するまでの秒数） |
| 最大再送信回数 | 2 回（スイッチが認証プロセスを再開する前に、EAP-Request/Identity フレームを送信する回数） |
| クライアント タイムアウト時間 | 30 秒（認証サーバからの要求をクライアントにリレーするとき、スイッチが返答を待ち、クライアントに要求を再送信するまでの時間） |
| 認証サーバ タイムアウト時間 | 30 秒（クライアントからの応答を認証サーバにリレーするとき、スイッチが応答を待ち、応答をサーバに再送信するまでの時間。この値は設定変更ができません。） |
| 無活動タイムアウト | ディセーブル |
| ゲスト VLAN | 指定なし |
| アクセス不能認証バイパス | ディセーブル |
| 制限付き VLAN | 指定なし |
| 認証者（スイッチ）モード | 指定なし |
| MAC 認証バイパス | ディセーブル |

## IEEE 802.1x 認証設定時の注意事項

ここでは、次の機能における注意事項を説明します。

- IEEE 802.1x 認証（p.9-23）
- VLAN 割り当て、ゲスト VLAN、制限付き VLAN、アクセス不能認証バイパス（p.9-24）
- MAC 認証バイパス（p.9-25）

### IEEE 802.1x 認証

IEEE 802.1x 認証を設定する場合の注意事項は、次のとおりです。

- IEEE 802.1x 認証をイネーブルにすると、他のレイヤ 2 またはレイヤ 3 機能がイネーブルになる前に、ポートが認証されます。
- IEEE 802.1x 対応ポートを（たとえばアクセスからトランクに）変更しようとしても、エラーメッセージが表示され、ポート モードは変更されません。
- IEEE 802.1x 対応ポートが割り当てられている VLAN が変更された場合、この変更は透過的でスイッチには影響しません。たとえば、ポートが RADIUS サーバに割り当ててられた VLAN に割り当てられ、再認証後に別の VLAN に割り当てられた場合に、この変更が発生します。

  IEEE 802.1x ポートが割り当てられている VLAN がシャットダウン、ディセーブル、または削除される場合、ポートは無許可になります。たとえば、ポートが割り当てられたアクセス VLAN がシャットダウンまたは削除されたあと、ポートは無許可になります。

- IEEE 802.1x プロトコルは、レイヤ 2 スタティックアクセス ポート、音声 VLAN ポート、およびレイヤ 3 ルーテッド ポートでサポートされますが、次のポート タイプではサポートされません。
  - トランク ポート — トランク ポート上で IEEE 802.1x 認証をイネーブルにしようとすると、エラー メッセージが表示され、IEEE 802.1x 認証はイネーブルになりません。IEEE 802.1x 対応ポートをトランクに変更しようとしても、エラー メッセージが表示され、ポート モードは変更されません。
  - ダイナミック ポート — ダイナミック モードのポートは、ネイバとトランク ポートへの変更をネゴシエートする場合があります。ダイナミック ポートで IEEE 802.1x 認証をイネーブルにしようとすると、エラー メッセージが表示され、IEEE 802.1x 認証はイネーブルになりません。IEEE 802.1x 対応ポートをダイナミックに変更しようとしても、エラー メッセージが表示され、ポート モードは変更されません。
  - ダイナミック アクセス ポート — ダイナミック アクセス（VLAN Query Protocol [VQP]）ポートで IEEE 802.1x 認証をイネーブルにしようとすると、エラー メッセージが表示され、IEEE 802.1x 認証はイネーブルになりません。IEEE 802.1x 対応ポートを変更してダイナミック VLAN を割り当てようとしても、エラー メッセージが表示され、VLAN 設定は変更されません。
  - EtherChannel ポート — EtherChannel のアクティブ メンバーであるポート、またはこれからアクティブ メンバーにするポートを IEEE 802.1x ポートとして設定しないでください。EtherChannel ポートで IEEE 802.1x 認証をイネーブルにしようとすると、エラー メッセージが表示され、IEEE 802.1x 認証はイネーブルになりません。

  （注）　Cisco IOS Release 12.2(18)SE より前のソフトウェア リリースでは、これからアクティブになる EtherChannel ポート上で IEEE 802.1x 認証がイネーブルになった場合、そのポートは EtherChannel に参加しません。

  - Switched Port Analyzer（SPAN; スイッチド ポート アナライザ）および RSPAN 宛先ポート — SPAN または RSPAN 宛先ポートであるポート上で IEEE 802.1x 認証をイネーブルにできます。ただし、ポートを SPAN または RSPAN 宛先ポートとして削除するまでは、IEEE 802.1x 認証はディセーブルになります。SPAN または RSPAN 送信元ポートでは、IEEE 802.1x 認証をイネーブルにできます。
- スイッチ上で、**dot1x system-auth-control** グローバル コンフィギュレーション コマンドを入力して IEEE 802.1x 認証をグローバルにイネーブルにする前に、IEEE 802.1x 認証と EtherChannel が設定されているインターフェイスから、EtherChannel の設定を削除してください。

## VLAN 割り当て、ゲスト VLAN、制限付き VLAN、アクセス不能認証バイパス

VLAN 割り当て、ゲスト VLAN、制限付き VLAN、およびアクセス不能認証バイパス設定時の注意事項は、次のとおりです。

- IEEE 802.1x 認証をポート上でイネーブルにすると、音声 VLAN の機能を持つポート VLAN は設定できません。
- トランク ポート、ダイナミック ポート、または VMPS によるダイナミック アクセス ポート割り当ての場合、VLAN 割り当て機能を使用した IEEE 802.1x 認証はサポートされません。
- IEEE 802.1x 認証をプライベート VLAN ポートに設定できますが、ポート セキュリティ、音声 VLAN、ゲスト VLAN、制限付き VLAN、またはユーザ単位 ACL が付いた IEEE 802.1x 認証をプライベート VLAN ポートに設定できません。
- RSPAN VLAN、プライベート VLAN、音声 VLAN を除くあらゆる VLAN を IEEE 802.1x ゲスト VLAN として設定できます。ゲスト VLAN 機能は、内部 VLAN（ルーテッド ポート）またはトランク ポートではサポートされていません。アクセス ポート上でのみサポートされます。

- Dynamic Host Configuration Protocol（DHCP）クライアントが接続する IEEE 802.1x ポートにゲスト VLAN を設定したあとは、DHCP サーバからホスト IP アドレスが必要になる場合があります。クライアントの DHCP 処理がタイムアウトして、DHCP サーバからホスト IP アドレスを取得する前に、スイッチ上の IEEE 802.1x 認証プロセスを再開するための設定を変更することもできます。IEEE 802.1x 認証プロセスの設定を減らしてください（**dot1x timeout quiet-period** および **dot1x timeout tx-period** インターフェイス コンフィギュレーション コマンド）。設定を減らす量は、接続している IEEE 802.1x クライアント タイプによって異なります。
- アクセス不能認証バイパス機能を設定する際には、次の注意事項に従ってください。
  - この機能はシングル ホスト モードおよびマルチホスト モードの IEEE 802.1x ポートでサポートされます。
  - Windows XP を稼働しているクライアントに接続されたポートがクリティカル認証ステートの場合、Windows XP はインターフェイスが認証されないと報告する場合があります。
  - Windows XP クライアントに DHCP が設定されていて、DHCP サーバからの IP アドレスを持つ場合、クリティカル ポート上で EAP 成功メッセージを受信すると、DHCP 設定プロセスが再始動しない場合があります。
  - IEEE 802.1x ポート上では、アクセス不能認証バイパス機能および制限付き VLAN を設定できます。スイッチが制限付き VLAN 内でクリティカル ポートを再認証しようとし、すべての RADIUS サーバが利用不可能な場合、スイッチはポート ステートをクリティカル認証ステートに変更し、制限付き VLAN に残ります。
  - 同じスイッチ ポート上にアクセス不能バイパス機能とポート セキュリティを設定できます。
- RSPAN VLAN または音声 VLAN を除くあらゆる VLAN を、IEEE 802.1x 制限付き VLAN として設定できます。制限付き VLAN 機能は、内部 VLAN（ルーテッド ポート）またはトランク ポートではサポートされていません。アクセス ポート上でのみサポートされます。

### MAC 認証バイパス

MAC 認証バイパス設定時の注意事項は次のとおりです。

- 特に明記していないかぎり、MAC 認証バイパスの注意事項は IEEE 802.1x 認証のものと同じです。詳細については、「IEEE 802.1x 認証」（p.9-23）を参照してください。
- ポートが MAC アドレスで許可されたあとに、ポートから MAC 認証バイパスをディセーブルにしても、ポート ステートに影響はありません。
- ポートが無許可ステートでクライアント MAC アドレスが認証サーバ データベースにない場合、ポートは無許可ステートのままになります。ただし、クライアント MAC アドレスがデータベースに追加された場合、スイッチは MAC 認証バイパスを使用してポートを再認証できます。
- ポートが許可ステートである場合、再認証が発生するまでポートのステートは変わりません。
- Cisco IOS Release 12.2(35)SE 以降では、MAC 認証バイパスに接続されているものの非アクティブのホストのタイムアウト期間を設定することができます。範囲は 1 ～ 65535 秒です。タイムアウト値を設定する前にポート セキュリティをイネーブルにする必要があります。詳細については、「ポート セキュリティの設定」（p.24-10）を参照してください。

## 旧版のソフトウェア リリースからのアップグレード

Cisco IOS Release 12.2(25)SEE では、IEEE 802.1x 認証の実装が旧リリースから変更されています。IEEE 802.1x 認証がイネーブルの場合、PortFast に関する情報は設定には追加されず、この情報は実行コンフィギュレーションに表示されます。

```
dot1x pae authenticator
```

# IEEE 802.1x 認証の設定

IEEE 802.1x ポートベース認証を設定するには、AAA をイネーブルにして認証方式リストを指定する必要があります。方式リストは、ユーザ認証のためにクエリー送信を行う手順と認証方式を記述したものです。

ユーザ単位 ACL または VLAN 割り当てを可能にするには、AAA 許可をイネーブルにしてネットワーク関連のすべてのサービス要求に対してスイッチを設定する必要があります。

次に、IEEE 802.1x の AAA プロセスを示します。

**ステップ 1**　ユーザがスイッチのポートに接続します。

**ステップ 2**　認証が実行されます。

**ステップ 3**　RADIUS サーバ設定に基づいて、VLAN 割り当てが適宜イネーブルになります。

**ステップ 4**　スイッチが開始メッセージをアカウンティング サーバに送信します。

**ステップ 5**　必要に応じて、再認証が実行されます。

**ステップ 6**　スイッチが仮のアカウンティング アップデートを、再認証結果に基づいたアカウンティング サーバに送信します。

**ステップ 7**　ユーザがポートから切断します。

**ステップ 8**　スイッチが停止メッセージをアカウンティング サーバに送信します。

IEEE 802.1x ポートベース認証を設定するには、特権 EXEC モードで次の手順を実行します。

| | コマンド | 目的 |
|---|---|---|
| ステップ 1 | **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 2 | **aaa new-model** | AAA をイネーブルにします。 |
| ステップ 3 | **aaa authentication dot1x** {**default**} *method1* | IEEE 802.1x 認証方式リストを作成します。<br>**authentication** コマンドに名前付きリストが*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す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。<br>*method1* には、**group radius** キーワードを入力して、認証用のすべての RADIUS サーバ リストを使用できるようにします。<br>（注）　**group radius** キーワード以外にもコマンドラインのヘルプストリングに表示されますが、サポートされていません。 |
| ステップ 4 | **dot1x system-auth-control** | スイッチ上で IEEE 802.1x 認証をグローバルにイネーブルにします。 |

| | コマンド | 目的 |
|---|---|---|
| ステップ 5 | **aaa authorization network** {**default**} **group radius** | （任意）ユーザ単位 ACL や VLAN 割り当てなど、ネットワーク関連のすべてのサービス要求に対するユーザ RADIUS 許可をスイッチに設定します。<br><br>ユーザ単位 ACL を設定するには、シングル ホスト モードを設定する必要があります。この設定がデフォルトです。 |
| ステップ 6 | **radius-server host** *ip-address* | （任意）RADIUS サーバの IP アドレスを指定します。 |
| ステップ 7 | **radius-server key** *string* | （任意）RADIUS サーバ上で動作する RADIUS デーモンとスイッチの間で使用する認証および暗号鍵を指定します。 |
| ステップ 8 | **interface** *interface-id* | IEEE 802.1x 認証をイネーブルにするクライアントに接続しているポートを指定し、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。 |
| ステップ 9 | **switchport mode access** | （任意）ステップ 6 および 7 で RADIUS サーバを設定した場合のみ、ポートをアクセス モードに設定します。 |
| ステップ 10 | **dot1x port-control auto** | ポート上で IEEE 802.1x 認証をイネーブルにします。<br><br>機能の相互作用については、「IEEE 802.1x 認証設定時の注意事項」（p.9-23）を参照してください。 |
| ステップ 11 | **end** | 特権 EXEC モードに戻ります。 |
| ステップ 12 | **show dot1x** | 設定を確認します。 |
| ステップ 13 | **copy running-config startup-config** | （任意）コンフィギュレーション ファイルに設定を保存します。 |

## スイッチおよび RADIUS サーバ間の通信の設定

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識別します。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、サーバの同一 IP アドレス上にある複数の UDP ポートに RADIUS 要求を送信できるようになります。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（たとえば認証）を設定した場合、2 番めに設定されたホスト エントリは、最初に設定されたホスト 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。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。

スイッチ上に RADIUS サーバ パラメータを設定するには、特権 EXEC モードで次の手順を実行します。この手順は必須です。

| | コマンド | 目的 |
|---|---|---|
| ステップ 1 | **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 2 | **radius-server host** {*hostname* \| *ip-address*} **auth-port** *port-number* **key** *string* | RADIUS サーバ パラメータを設定します。<br><br>*hostname* \| *ip-address* には、リモート RADIUS サーバのホスト名または IP アドレスを指定します。<br><br>**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 1812 です。指定できる範囲は 0 ～ 65536 です。<br><br>**key** *string* には、スイッチと RADIUS サーバ上で動作する RADIUS デーモンとの間で使用する認証および暗号鍵を指定します。鍵は、RADIUS サーバで使用する暗号鍵に一致するテキスト ストリングでなければなりません。<br><br>（注） 鍵の先行スペースは無視されますが、途中および末尾のスペースは有効なので、鍵は必ず **radius-server host** コマンド構文の最後のアイテムとして設定してください。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。鍵は RADIUS デーモンで使用する暗号鍵に一致している必要があります。<br><br>複数の RADIUS サーバを使用する場合には、このコマンドを繰り返し入力します。 |
| ステップ 3 | **end** | 特権 EXEC モードに戻ります。 |
| ステップ 4 | **show running-config** | 設定を確認します。 |
| ステップ 5 | **copy running-config startup-config** | （任意）コンフィギュレーション ファイルに設定を保存します。 |

特定の RADIUS サーバを削除するには、**no radius-server host** {*hostname* | *ip-address*} 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。

次に、IP アドレス 172.120.39.46 のサーバを RADIUS サーバとして指定し、ポート 1612 を許可ポートとして使用し、暗号鍵を RADIUS サーバ上の鍵と同じ *rad123* に設定する例を示します。

```
Switch(config)# radius-server host 172.120.39.46 auth-port 1612 key rad123
```

すべての RADIUS サーバについて、タイムアウト、再送信回数、および暗号鍵値をグローバルに設定するには、**radius-server host** 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。これらのオプションをサーバ単位で設定するには、**radius-server timeout**、**radius-server retransmit**、および **radius-server key** 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。詳細については、「すべての RADIUS サーバの設定」（p.8-30）を参照してください。

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。これらの設定値としては、スイッチの IP アドレス、およびサーバとスイッチの双方で共有するキー ストリングがあります。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。

## ホスト モードの設定

IEEE 802.1x 認証済みポート上でシングル ホスト（クライアント）を許可するには、特権 EXEC モードで次の手順を実行します。**multi-domain** キーワードを使用して MDA を設定して、ホストと（シスコまたはシスコ以外の）IP 電話のような音声デバイスの両方が、同一スイッチ ポートで認証することができます。この手順は任意です。

| | コマンド | 目的 |
|---|---|---|
| ステップ 1 | **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 2 | radius-server vsa send authentication | VSA（vendor-specific attribute; ベンダー固有属性）を認識し使用するために、ネットワーク アクセス サーバを設定します。 |
| ステップ 3 | **interface** *interface-id* | 複数ホストが間接的に接続されているポートを指定し、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。 |
| ステップ 4 | **dot1x host-mode {single-host \| multi-host \| multi-domain}** | キーワードの意味は次のとおりです。<br>• **single-host —** IEEE 802.1x 許可ポートで複数のホスト（クライアント）の接続を許可します。<br>• **multi-host —** シングル ホストの認証後に IEEE 802.1x 許可ポートで複数のホスト（クライアント）の接続を許可します。<br>• **multidomain —** ホストと（シスコまたはシスコ以外の）IP 電話のような音声デバイスの両方を 1 つの IEEE 802.1x 認証済ポートで認証することができます。<br>**（注）** ホスト モードが **multi-domain** に設定される際に IP 電話の音声 VLAN を設定する必要があります。詳細は、第 15 章「音声 VLAN の設定」を参照してください。<br>指定するインターフェイスで、**dot1x port-control** インターフェイス コンフィギュレーション コマンドが **auto** に設定されていることを確認してください。 |
| ステップ 5 | **switchport voice vlan** *vlan-id* | （任意）音声 VLAN を設定します。 |
| ステップ 6 | **end** | 特権 EXEC モードに戻ります。 |
| ステップ 7 | **show dot1x interface** *interface-id* | 設定を確認します。 |
| ステップ 8 | **copy running-config startup-config** | （任意）コンフィギュレーション ファイルに設定を保存します。 |

ポート上で複数のホストをディセーブルにするには、**no dot1x host-mode multi-host** インターフェイス コンフィギュレーション コマンドを使用します。

次に、IEEE 802.1x 認証をイネーブルにして、複数のホストを許可する例を示します。

```
Switch(config)# interface gigabitethernet2/0/1

Switch(config-if)# dot1x port-control auto
Switch(config-if)# dot1x host-mode multi-host
Switch(config-if)# end
```

次に、MDA をイネーブルにしてポート上でホストと音声 デバイスを許可する例を示します。

```
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# dot1x port-control auto
Switch(config-if)# dot1x host-mode multi-domain
Switch(config-if)# switchport voice vlan 101
Switch(config-if)# end
```

## 定期的な再認証の設定

IEEE 802.1x クライアントの定期的な再認証をイネーブルにし、再認証の間隔を指定できます。再認証を行う間隔を指定しない場合、3600 秒おきに再認証が試みられます。

クライアントの定期的な再認証をイネーブルにし、再認証を行う間隔（秒）を設定するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

| | コマンド | 目的 |
|---|---|---|
| ステップ 1 | **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 2 | **interface** *interface-id* | 設定するポートを指定し、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。 |
| ステップ 3 | **dot1x reauthentication** | クライアントの定期的な再認証（デフォルトではディセーブル）をイネーブルにします。 |
| ステップ 4 | **dot1x timeout reauth-period** {*seconds* \| **server**} | 再認証の間隔（秒）を指定します。<br>キーワードの意味は次のとおりです。<br>• *seconds* — 秒数を 1 ～ 65535 の範囲で設定します。デフォルトは 3600 秒です。<br>• **server** — Session-Timeout RADIUS アトリビュート（アトリビュート [27]）および Terminate-Action RADIUS アトリビュート（アトリビュート [29]）の値に基づいて秒数を指定します。<br>このコマンドがスイッチの動作に影響するのは、定期的な再認証をイネーブルに設定した場合だけです。 |
| ステップ 5 | **end** | 特権 EXEC モードに戻ります。 |
| ステップ 6 | **show dot1x interface** *interface-id* | 設定を確認します。 |
| ステップ 7 | **copy running-config startup-config** | （任意）コンフィギュレーション ファイルに設定を保存します。 |

定期的な再認証をディセーブルにするには、**no dot1x reauthentication** インターフェイス コンフィギュレーション コマンドを使用します。再認証の間隔をデフォルトの秒数に戻すには、**no dot1x timeout reauth-period** インターフェイス コンフィギュレーション コマンドを使用します。

次に、定期的な再認証をイネーブルにし、再認証の間隔を 4000 秒に設定する例を示します。

```
Switch(config-if)# dot1x reauthentication
Switch(config-if)# dot1x timeout reauth-period 4000
```

## ポートに接続するクライアントの手動での再認証

**dot1x re-authenticate interface** *interface-id* 特権 EXEC コマンドを入力することにより、いつでも特定のポートに接続するクライアントを手動で再認証できます。この手順は任意です。定期的な再認証をイネーブルまたはディセーブルにする方法については、「定期的な再認証の設定」（p.9-30）を参照してください。

次に、ポートに接続するクライアントを手動で再認証する例を示します。

```
Switch# dot1x re-authenticate interface gigabitethernet0/1
```

## 待機時間の変更

スイッチはクライアントを認証できなかった場合に、所定の時間だけアイドル状態を続け、そのあと再び認証を試みます。**dot1x timeout quiet-period** インターフェイス コンフィギュレーション コマンドがその待ち時間を制御します。認証が失敗する理由としては、クライアントが無効なパスワードを提示した場合などが考えられます。デフォルトよりも小さい値を入力することによって、ユーザへの応答時間を短縮できます。

待機時間を変更するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

| | コマンド | 目的 |
|---|---|---|
| ステップ 1 | **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 2 | **interface** *interface-id* | 設定するポートを指定し、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。 |
| ステップ 3 | **dot1x timeout quiet-period** *seconds* | スイッチがクライアントとの認証情報の交換に失敗したあと、待機状態を続ける秒数を設定します。<br>指定できる範囲は 1 ～ 65535 秒です。デフォルトは 60 秒です。 |
| ステップ 4 | **end** | 特権 EXEC モードに戻ります。 |
| ステップ 5 | **show dot1x interface** *interface-id* | 設定を確認します。 |
| ステップ 6 | **copy running-config startup-config** | （任意）コンフィギュレーション ファイルに設定を保存します。 |

待機時間をデフォルトに戻すには、**no dot1x timeout quiet-period** インターフェイス コンフィギュレーション コマンドを使用します。

次に、スイッチの待機時間を 30 秒に設定する例を示します。

```
Switch(config-if)# dot1x timeout quiet-period 30
```

## スイッチからクライアントへの再送信時間の変更

クライアントはスイッチからの EAP-Request/Identity フレームに対し、EAP-Response/Identity フレームで応答します。スイッチがこの応答を受信できなかった場合、所定の時間（再送信時間）だけ待機し、そのあとフレームを再送信します。

（注）　このコマンドのデフォルト値は、リンクの信頼性が低い場合や、特定のクライアントおよび認証サーバの動作に問題がある場合など、異常な状況に対する調整を行う必要があるときに限って変更してください。

スイッチがクライアントからの通知を待機する時間を変更するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

| | コマンド | 目的 |
|---|---|---|
| ステップ 1 | **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 2 | **interface** *interface-id* | 設定するポートを指定し、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。 |
| ステップ 3 | **dot1x timeout tx-period** *seconds* | スイッチが EAP-Request/Identity フレームに対するクライアントからの応答を待ち、要求を再送信するまでの秒数を設定します。<br>指定できる範囲は 5 ～ 65535 秒です。デフォルトは 5 秒です。 |

| | コマンド | 目的 |
|---|---|---|
| ステップ 4 | **end** | 特権 EXEC モードに戻ります。 |
| ステップ 5 | **show dot1x interface** *interface-id* | 設定を確認します。 |
| ステップ 6 | **copy running-config startup-config** | （任意）コンフィギュレーション ファイルに設定を保存します。 |

再送信時間をデフォルトに戻すには、**no dot1x timeout tx-period** インターフェイス コンフィギュレーション コマンドを使用します。

次に、スイッチが EAP-Request/Identity フレームに対するクライアントからの応答を待ち、要求を再送信するまでの時間を 60 秒に設定する例を示します。

```
Switch(config-if)# dot1x timeout tx-period 60
```

## スイッチからクライアントへのフレーム再送信回数の設定

スイッチからクライアントへの再送信時間を変更できるだけでなく、（クライアントから応答が得られなかった場合に）スイッチが認証プロセスを再起動する前に、クライアントに EAP-Request/Identity フレームを送信する回数を変更できます。

（注）　このコマンドのデフォルト値は、リンクの信頼性が低い場合や、特定のクライアントおよび認証サーバの動作に問題がある場合など、異常な状況に対する調整を行う必要があるときに限って変更してください。

スイッチからクライアントへのフレーム再送信回数を設定するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

| | コマンド | 目的 |
|---|---|---|
| ステップ 1 | **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 2 | **interface** *interface-id* | 設定するポートを指定し、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。 |
| ステップ 3 | **dot1x max-reauth-req** *count* | スイッチが認証プロセスを再起動する前に、EAP-Request/Identity フレームを送信する回数を設定します。指定できる範囲は 1 ～ 10 です。デフォルトは 2 です。 |
| ステップ 4 | **end** | 特権 EXEC モードに戻ります。 |
| ステップ 5 | **show dot1x interface** *interface-id* | 設定を確認します。 |
| ステップ 6 | **copy running-config startup-config** | （任意）コンフィギュレーション ファイルに設定を保存します。 |

再送信回数をデフォルトに戻すには、**no dot1x max-req** インターフェイス コンフィギュレーション コマンドを使用します。

次に、スイッチが認証プロセスを再起動する前に、EAP-Request/Identity 要求を送信する回数を 5 に設定する例を示します。

```
Switch(config-if)# dot1x max-req 5
```

## 再認証回数の設定

ポートが無許可ステートに変わる前に、スイッチが認証プロセスを再開する回数を変更することもできます。

（注）　このコマンドのデフォルト値は、リンクの信頼性が低い場合や、特定のクライアントおよび認証サーバの動作に問題がある場合など、異常な状況に対する調整を行う必要があるときに限って変更してください。

再認証回数を設定するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

| | コマンド | 目的 |
|---|---|---|
| ステップ 1 | **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 2 | **interface** *interface-id* | 設定するポートを指定し、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。 |
| ステップ 3 | **dot1x max-reauth-req** *count* | ポートが無許可ステートに変わる前に、スイッチが認証プロセスを再開する回数を設定します。指定できる範囲は 0 ～ 10 です。デフォルトは 2 です。 |
| ステップ 4 | **end** | 特権 EXEC モードに戻ります。 |
| ステップ 5 | **show dot1x interface** *interface-id* | 設定を確認します。 |
| ステップ 6 | **copy running-config startup-config** | （任意）コンフィギュレーション ファイルに設定を保存します。 |

再認証回数をデフォルトに戻すには、**no dot1x max-reauth-req** インターフェイス コンフィギュレーション コマンドを使用します。

次に、ポートが無許可ステートに変わる前に、スイッチが認証プロセスを再開する回数として 4 を設定する例を示します。

```
Switch(config-if)# dot1x max-reauth-req 4
```

## IEEE 802.1x アカウンティングの設定

IEEE 802.1x アカウンティングを使用して、AAA システム アカウンティングをイネーブルにすると、ロギングのためにシステム リロード イベントをアカウンティング RADIUS サーバに送信できます。サーバは、アクティブな IEEE 802.1x セッションすべてが終了したものと判断します。

RADIUS は信頼性の低い UDP トランスポート プロトコルを使用するため、ネットワーク状態が良好でないと、アカウンティング メッセージが失われることがあります。設定した回数のアカウンティング要求の再送信後、スイッチが RADIUS サーバからアカウンティング応答メッセージを受信しない場合、次のメッセージが表示されます。

```
Accounting message %s for session %s failed to receive Accounting Response.
```

このストップ メッセージが正常に送信されない場合、次のメッセージが表示されます。

```
00:09:55: %RADIUS-3-NOACCOUNTINGRESPONSE: Accounting message Start for session
172.20.50.145 sam 11/06/03 07:01:16 11000002 failed to receive Accounting Response.
```

（注）　ロギングの開始、停止、仮のアップデート メッセージ、タイム スタンプなどのアカウンティング タスクを実行するように、RADIUS サーバを設定する必要があります。これらの機能をオンにするには、RADIUS サーバの Network Configuration タブの [Update/Watchdog packets from this AAA client] のロギングをイネーブルにします。次に、RADIUS サーバの System Configuration タブの [CVS RADIUS Accounting] をイネーブルにします。

AAA がスイッチでイネーブルになったあと、IEEE 802.1x アカウンティングを設定するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

| | コマンド | 目的 |
|---|---|---|
| ステップ 1 | **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 2 | **interface** *interface-id* | 設定するポートを指定し、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。 |
| ステップ 3 | **aaa accounting dot1x default start-stop group radius** | すべての RADIUS サーバのリストを使用して、IEEE 802.1x アカウンティングをイネーブルにします。 |
| ステップ 4 | **aaa accounting system default start-stop group radius** | （任意）システム アカウンティングをイネーブルにし（すべての RADIUS サーバのリストを使用）、スイッチがリロードするときにシステム アカウンティング リロード イベント メッセージを生成します。 |
| ステップ 5 | **end** | 特権 EXEC モードに戻ります。 |
| ステップ 6 | **show running-config** | 設定を確認します。 |
| ステップ 7 | **copy running-config startup-config** | （任意）コンフィギュレーション ファイルに設定を保存します。 |

アカウンティング応答メッセージを受信しない RADIUS メッセージ数を表示するには、**show radius statistics** 特権 EXEC コマンドを使用します。

次に、IEEE 802.1x アカウンティングを設定する例を示します。最初のコマンドは、アカウンティングの UDP ポートとして 1813 を指定して、RADIUS サーバを設定します。

```
Switch(config)# radius-server host 172.120.39.46 auth-port 1812 acct-port 1813 key
rad123
Switch(config)# aaa accounting dot1x default start-stop group radius
Switch(config)# aaa accounting system default start-stop group radius
```

## ゲスト VLAN の設定

サーバが EAP Request/Identity フレームに対する応答を受信しない場合、ゲスト VLAN を設定すると、IEEE 802.1x 対応でないクライアントはゲスト VLAN に配置されます。IEEE 802.1x 対応であっても、認証に失敗したクライアントは、ネットワークへのアクセスが許可されません。スイッチは、シングル ホスト モードまたはマルチ ホスト モードでゲスト VLAN をサポートします。

ゲスト VLAN を設定するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

| | コマンド | 目的 |
|---|---|---|
| ステップ 1 | **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 2 | **interface** *interface-id* | 設定するポートを指定し、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。サポートされるポートのタイプについては、「IEEE 802.1x 認証設定時の注意事項」（p.9-23）を参照してください。 |

| | コマンド | 目的 |
|---|---|---|
| ステップ 3 | **switchport mode access**<br>または<br>**switchport mode private-vlan host** | ポートをアクセス モードにします。<br>または<br>レイヤ 2 ポートをプライベート VLAN ホスト ポートとして設定します。 |
| ステップ 4 | **dot1x port-control auto** | ポート上で IEEE 802.1x 認証をイネーブルにします。 |
| ステップ 5 | **dot1x guest-vlan** *vlan-id* | アクティブ VLAN を IEEE 802.1x ゲスト VLAN として指定します。指定できる範囲は 1 ～ 4094 です。<br>内部 VLAN（ルーテッド ポート）、RSPAN VLAN、プライマリ プライベート VLAN、または音声 VLAN を除き、任意のアクティブ VLAN を IEEE 802.1x ゲスト VLAN として設定できます。 |
| ステップ 6 | **end** | 特権 EXEC モードに戻ります。 |
| ステップ 7 | **show dot1x interface** *interface-id* | 設定を確認します。 |
| ステップ 8 | **copy running-config startup-config** | （任意）コンフィギュレーション ファイルに設定を保存します。 |

ゲスト VLAN をディセーブルにして削除するには、**no dot1x guest-vlan** インターフェイス コンフィギュレーション コマンドを使用します。ポートは無許可ステートに戻ります。

次に、VLAN 2 を IEEE 802.1x ゲスト VLAN としてイネーブルにする例を示します。

```
Switch(config)# interface gigabitethernet0/2
Switch(config-if)# dot1x guest-vlan 2
```

次に、スイッチの待機時間として 3 を、要求の再送信前にクライアントからの EAP-Request/Identify フレーム応答を待機する時間（秒）を 15 に設定し、IEEE 802.1x ポートの DHCP クライアント接続時に、VLAN 2 を IEEE 802.1x ゲスト VLAN としてイネーブルにする例を示します。

```
Switch(config-if)# dot1x timeout quiet-period 3
Switch(config-if)# dot1x timeout tx-period 15
Switch(config-if)# dot1x guest-vlan 2
```

## 制限付き VLAN の設定

スイッチ上に制限付き VLAN を設定している、認証サーバが有効なユーザ名またはパスワードを受信できない場合と、IEEE 802.1x に準拠した場合クライアントは制限付き VLAN に移されます。スイッチは、シングル ホスト モードでのみ制限付き VLAN をサポートします。

制限付き VLAN を設定するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

| | コマンド | 目的 |
|---|---|---|
| ステップ 1 | **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 2 | **interface** *interface-id* | 設定するポートを指定し、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。サポートされるポートのタイプについては、「IEEE 802.1x 認証設定時の注意事項」（p.9-23）を参照してください。 |
| ステップ 3 | **switchport mode access**<br>または<br>**switchport mode private-vlan host** | ポートをアクセス モードにします。<br>または<br>レイヤ 2 ポートをプライベート VLAN ホスト ポートとして設定します。 |
| ステップ 4 | **dot1x port-control auto** | ポート上で IEEE 802.1x 認証をイネーブルにします。 |

| | コマンド | 目的 |
|---|---|---|
| ステップ 5 | **dot1x auth-fail vlan** *vlan-id* | アクティブな VLAN を、IEEE 802.1x 制限付き VLAN に指定します。指定できる範囲は 1 ～ 4094 です。<br><br>内部 VLAN（ルーテッド ポート）、RSPAN VLAN、プライマリ プライベート VLAN、または音声 VLAN を除き、任意のアクティブ VLAN を IEEE 802.1x 制限付き VLAN として設定できます。 |
| ステップ 6 | **end** | 特権 EXEC モードに戻ります。 |
| ステップ 7 | **show dot1x interface** *interface-id* | （任意）設定を確認します。 |
| ステップ 8 | **copy running-config startup-config** | （任意）コンフィギュレーション ファイルに設定を保存します。 |

制限付き VLAN をディセーブルにして削除するには、**no dot1x auth-fail vlan** インターフェイス コンフィギュレーション コマンドを使用します。ポートは無許可ステートに戻ります。

次に、*VLAN 2* を IEEE 802.1x 制限付き VLAN としてイネーブルにする例を示します。

```
Switch(config)# interface gigabitethernet0/2
Switch(config-if)# dot1x auth-fail vlan 2
```

ユーザに制限付き VLAN を割り当てる前に、**dot1x auth-fail max-attempts** インターフェイス コンフィギュレーション コマンドを使用して、認証試行回数を最大に設定できます。指定できる試行回数は 1 ～ 3 です。デフォルトは 3 回に設定されています。

認証試行回数を最大に設定するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

| | コマンド | 目的 |
|---|---|---|
| ステップ 1 | **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 2 | **interface** *interface-id* | 設定するポートを指定し、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。サポートされるポートのタイプについては、「IEEE 802.1x 認証設定時の注意事項」（p.9-23）を参照してください。 |
| ステップ 3 | **switchport mode access**<br><br>または<br><br>**switchport mode private-vlan host** | ポートをアクセス モードにします。<br><br>または<br><br>レイヤ 2 ポートをプライベート VLAN ホスト ポートとして設定します。 |
| ステップ 4 | **dot1x port-control auto** | ポート上で IEEE 802.1x 認証をイネーブルにします。 |
| ステップ 5 | **dot1x auth-fail vlan** *vlan-id* | アクティブな VLAN を、IEEE 802.1x 制限付き VLAN に指定します。指定できる範囲は 1 ～ 4094 です。<br><br>内部 VLAN（ルーテッド ポート）、RSPAN VLAN、プライマリ プライベート VLAN、または音声 VLAN を除き、任意のアクティブ VLAN を IEEE 802.1x 制限付き VLAN として設定できます。 |
| ステップ 6 | **dot1x auth-fail max-attempts** *max attempts* | ポートが制限付き VLAN に移行するための認証試行回数を指定します。指定できる範囲は 1 ～ 3 秒です。デフォルトは 3 です。 |
| ステップ 7 | **end** | 特権 EXEC モードに戻ります。 |
| ステップ 8 | **show dot1x interface** *interface-id* | （任意）設定を確認します。 |
| ステップ 9 | **copy running-config startup-config** | （任意）コンフィギュレーション ファイルに設定を保存します。 |

設定数をデフォルトに戻すには、**no dot1x auth-fail max-attempts** インターフェイス コンフィギュレーション コマンドを使用します。

次に、ポートを制限付き VLAN にするために、認証試行回数を *2* に設定する方法を示します。

```
Switch(config-if)# dot1x auth-fail max-attempts 2
```

## アクセス不能認証バイパス機能の設定

アクセス不能認証バイパス機能（クリティカル認証または AAA 失敗ポリシーとも呼ばれます）を設定できます。

ポートをクリティカル ポートとして設定し、アクセス不能認証バイパス機能をイネーブルにするには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

| | コマンド | 目的 |
|---|---|---|
| ステップ 1 | **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 2 | **radius-server dead-criteria time** *time* **tries** *tries* | （任意）RADIUS サーバが使用できない、または *dead* と見なされるときを判別するのに使われる条件を設定します。<br><br>指定できる *time* の範囲は 1 ～ 120 秒です。スイッチは、デフォルトの *seconds* 値を 10 ～ 60 秒の間で動的に決定します。<br><br>指定できる *tries* の範囲は 1 ～ 100 です。スイッチは *tries* のパラメータを動的に決定します。 |
| ステップ 3 | **radius-server deadtime** *minutes* | （任意）RADIUS サーバに要求が送信されない分数を設定します。指定できる範囲は 0 ～ 1440 分です（24 時間）。デフォルト値は 0 分です。 |
| ステップ 4 | **radius-server host** *ip-address* [**acct-port** *udp-port*] [**auth-port** *udp-port*] [**key** *string*] [**test username** *name* [**idle-time** *time*] [**ignore-acct-port**] [**ignore-auth-port**]] | （任意）次のキーワードを使用して RADIUS サーバ パラメータを設定します。<br><br>• **acct-port** *udp-port* — RADIUS アカウンティング サーバの UDP ポートを指定します。UDP ポート番号の範囲は 0 ～ 65536 です。デフォルトは 1646 です。<br>• **auth-port** *udp-port* — RADIUS 認証サーバの UDP ポートを指定します。UDP ポート番号の範囲は 0 ～ 65536 です。デフォルトは 1645 です。<br><br>（注） RADIUS アカウンティング サーバの UDP ポートと RADIUS 認証サーバの UDP ポートを非デフォルト値に設定します。<br><br>• **key** *string* — スイッチと RADIUS デーモンとの間のすべての RADIUS 通信で使用する認証および暗号鍵を指定します。<br><br>（注） **radius-server key** {**0** *string* \| **7** *string* \| *string*} 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も認証および暗号鍵を設定できます。<br><br>• **test username** *name* — RADIUS サーバ ステータスの自動テストをイネーブルにして、使用するユーザ名を指定します。<br>• **idle-time** *time* — スイッチがテスト パケットをサーバに送信したあとの間隔を分数で設定します。指定できる範囲は 1 ～ 35791 分です。デフォルトは 60 分（1 時間）です。<br>• **ignore-acct-port** — RADIUS サーバ アカウンティング ポートのテストをディセーブルにします。<br>• **ignore-auth-port** — RADIUS サーバ認証ポートのテストをディセーブルにします。 |

| | コマンド | 目的 |
|---|---|---|
| ステップ 5 | **dot1x critical** {**eapol** \| **recovery delay** *milliseconds*} | （任意）アクセス不能認証バイパスのパラメータを設定します。<br><br>**eapol** — スイッチがクリティカル ポートを正常に認証すると、スイッチが EAPOL 成功メッセージを送信するように指定します。<br><br>**recovery delay** *milliseconds* — 使用できない RADIUS サーバが使用できるようになったときに、スイッチがクリティカル ポートを再初期化するために待機する回復遅延期間を設定します。指定できる範囲は 1 ～ 10000 ミリ秒です。デフォルトは 1000 ミリ秒です（ポートは毎秒再初期化できます）。 |
| ステップ 6 | **interface** *interface-id* | 設定するポートを指定し、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。サポートされるポートのタイプについては、「IEEE 802.1x 認証設定時の注意事項」（p.9-23）を参照してください。 |
| ステップ 7 | **dot1x critical** [**recovery action reinitialize** \| **vlan** *vlan-id*] | アクセス不能認証バイパス機能をイネーブルにして、次のキーワードを使用して機能を設定します。<br><br>• **recovery action reinitialize** — 回復機能をイネーブルにして、認証サーバが使用可能なとき、回復動作中にポートを認証するように指定します。<br>• **vlan** *vlan-id* — スイッチがクリティカル ポートに割り当てるアクセス VLAN を指定します。指定できる範囲は 1 ～ 4094 です。 |
| ステップ 8 | **end** | 特権 EXEC モードに戻ります。 |
| ステップ 9 | **show dot1x** [**interface** *interface-id*] | （任意）設定を確認します。 |
| ステップ 10 | **copy running-config startup-config** | （任意）コンフィギュレーション ファイルに設定を保存します。 |

RADIUS サーバのデフォルト設定に戻すには、**no radius-server dead-criteria**、**no radius-server deadtime**、および **no radius-server host** 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。アクセス不能認証バイパスのデフォルト設定に戻すには、**no dot1x critical** {**eapol** | **recovery delay**} 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。アクセス不能認証バイパスをディセーブルにするには、**no dot1x critical** インターフェイス コンフィギュレーション コマンドを使用します。

次に、アクセス不能認証バイパス機能を設定する例を示します。

```
Switch(config)# radius-server dead-criteria time 30 tries 20
Switch(config)# radius-server deadtime 60
Switch(config)# radius-server host 1.1.1.2 acct-port 1550 auth-port 1560 key abc1234
test username user1 idle-time 30
Switch(config)# dot1x critical eapol
Switch(config)# dot1x critical recovery delay 2000
Switch(config)# interface gigabitethernet 0/1
Switch(config)# radius-server deadtime 60
Switch(config-if)# dot1x critical
Switch(config-if)# dot1x critical recovery action reinitialize
Switch(config-if)# dot1x critical vlan 20
Switch(config-if)# end
```

## WoL を使用した IEEE 802.1x 認証の設定

WoL を使用した IEEE 802.1x 認証をイネーブルにするには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

| | コマンド | 目的 |
|---|---|---|
| ステップ 1 | **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 2 | **interface** *interface-id* | 設定するポートを指定し、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。サポートされるポートのタイプについては、「IEEE 802.1x 認証設定時の注意事項」（p.9-23）を参照してください。 |
| ステップ 3 | **dot1x control-direction** {**both** \| **in**} | ポートで WoL を使用して IEEE 802.1x 認証をイネーブルにし、次のキーワードを使用してポートを双方向または単方向に設定します。<br>• **both** — ポートを双方向に設定します。ポートは、ホストとの間でパケットを送受信できません。デフォルトでは、ポートは双方向です。<br>• **in** — ポートを単方向に設定します。ポートはパケットをホストに送信できますが、ホストからパケットを受信できません。 |
| ステップ 4 | **end** | 特権 EXEC モードに戻ります。 |
| ステップ 5 | **show dot1x interface** *interface-id* | 設定を確認します。 |
| ステップ 6 | **copy running-config startup-config** | （任意）コンフィギュレーション ファイルに設定を保存します。 |

スイッチで WoL を使用した IEEE 802.1x 認証をディセーブルにするには、**no dot1x control-direction** インターフェイス コンフィギュレーション コマンドを使用します。

次に、WoL を使用した IEEE 802.1x 認証をイネーブルにして、ポートを双方向に設定する例を示します。

```
Switch(config-if)# dot1x control-direction both
```

## MAC 認証バイパスの設定

MAC 認証バイパスをイネーブルにするには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

| | コマンド | 目的 |
|---|---|---|
| ステップ 1 | **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 2 | **interface** *interface-id* | 設定するポートを指定し、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。サポートされるポートのタイプについては、「IEEE 802.1x 認証設定時の注意事項」（p.9-23）を参照してください。 |
| ステップ 3 | **dot1x port-control auto** | ポート上で IEEE 802.1x 認証をイネーブルにします。 |
| ステップ 4 | **dot1x mac-auth-bypass** [**eap** \| **timeout activity** {*value*}] | MAC 認証バイパスをイネーブルにします。<br>（任意）**eap** キーワードを使用して認証用の EAP を使用するようにスイッチを設定します。<br>（任意）**timeout activity** キーワードを使用して、未認証ステートに移行する前に接続されているホストを非アクティブにすることのできる秒数を設定します。指定できる範囲は 1 ～ 65535 です。<br>タイムアウト値を設定する前にポート セキュリティをイネーブルにする必要があります。詳細については、「ポート セキュリティの設定」（p.24-10）を参照してください。 |
| ステップ 5 | **end** | 特権 EXEC モードに戻ります。 |

| | コマンド | 目的 |
|---|---|---|
| ステップ 6 | **show dot1x interface** *interface-id* | 設定を確認します。 |
| ステップ 7 | **copy running-config startup-config** | （任意）コンフィギュレーション ファイルに設定を保存します。 |

MAC 認証バイパスをディセーブルにするには、**no dot1x mac-auth-bypass** インターフェイス コンフィギュレーション コマンドを使用します。

次に、MAC 認証バイパス機能をイネーブルにする例を示します。

```
Switch(config-if)# dot1x mac-auth-bypass
```

## NAC レイヤ 2 IEEE 802.1x 検証の設定

Cisco IOS Release 12.2(25)SED 以降では、NAC レイヤ 2 IEEE 802.1x 検証を設定できます。これは、RADIUS サーバを使用した IEEE 802.1x 認証とも呼ばれます。

NAC レイヤ 2 IEEE 802.1x 検証を設定するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

| | コマンド | 目的 |
|---|---|---|
| ステップ 1 | **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 2 | **interface** *interface-id* | 設定するポートを指定し、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。 |
| ステップ 3 | **dot1x guest-vlan** *vlan-id* | アクティブ VLAN を IEEE 802.1x ゲスト VLAN として指定します。指定できる範囲は 1 ～ 4094 です。<br>内部 VLAN（ルーテッド ポート）、RSPAN VLAN、音声 VLAN を除くあらゆるアクティブ VLAN を IEEE 802.1x ゲスト VLAN として設定できます。 |
| ステップ 4 | **dot1x reauthentication** | クライアントの定期的な再認証（デフォルトではディセーブル）をイネーブルにします。 |
| ステップ 5 | **dot1x timeout reauth-period** {*seconds* \| **server**} | 再認証の間隔（秒）を指定します。<br>キーワードの意味は次のとおりです。<br>• *seconds* — 秒数を 1 ～ 65535 の範囲で設定します。デフォルトは 3600 秒です。<br>• **server** — Session-Timeout RADIUS アトリビュート（アトリビュート [27]）および Terminate-Action RADIUS アトリビュート（アトリビュート [29]）の値に基づいて秒数を指定します。<br>このコマンドがスイッチの動作に影響するのは、定期的な再認証をイネーブルに設定した場合だけです。 |
| ステップ 6 | **end** | 特権 EXEC モードに戻ります。 |
| ステップ 7 | **show dot1x interface** *interface-id* | IEEE 802.1x 認証の設定を確認します。 |
| ステップ 8 | **copy running-config startup-config** | （任意）コンフィギュレーション ファイルに設定を保存します。 |

次に、NAC レイヤ 2 IEEE 802.1x 検証を設定する例を示します。

```
Switch# configure terminal
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# dot1x reauthentication
Switch(config-if)# dot1x timeout reauth-period server
```

## Web 認証の設定

Web 認証の設定後に AAA および RADIUS をスイッチに設定するには、特権 EXEC モードで次の手順を実行します。このステップにより、RADIUS 認証を使用して AAA がイネーブルになり、デバイス トラッキングがイネーブルになります。

| | コマンド | 目的 |
|---|---|---|
| ステップ 1 | **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 2 | **aaa new-model** | AAA をイネーブルにします。 |
| ステップ 3 | **aaa authentication login default 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 サーバを設定しておく必要があります。詳細は、第 8 章「スイッチ ベース認証の設定」を参照してください。<br><br>コンソールで、**aaa authentication login** コマンドを入力後にスイッチ コンソールにアクセスするために、ユーザ名とパスワードが要求されます。ユーザ名とパスワードを要求されたくない場合は、2 番目のログイン認証一覧を設定します。<br><br>`Switch# config t`<br>`Switch(config)# aaa authentication login line-console none`<br>`Switch(config)# line console 0`<br>`Switch(config-line)# login authentication line-console`<br>`Switch(config-line)# end` |
| ステップ 4 | **aaa authorization auth-proxy default group radius** | 認証プロキシ（auth-proxy）認証に RADIUS を使用します。 |
| ステップ 5 | **radius-server host key** *radius-key* | スイッチと RADIUS デーモンとの間のすべての RADIUS 通信で使用する認証および暗号鍵を指定します。 |
| ステップ 6 | **radius-server attribute 8 include-in-access-req** | アクセス要求またはアカウント要求パケットで Framed-IP-Address RADIUS アトリビュート（アトリビュート [8]）を送信するようにスイッチを設定します。 |
| ステップ 7 | **radius-server vsa send authentication** | VSA（vendor-specific attribute; ベンダー固有属性）を認識し使用するために、ネットワーク アクセス サーバを設定します。 |
| ステップ 8 | **ip device tracking** | IP デバイス トラッキング テーブルをイネーブルにします。<br><br>IP デバイス トラッキング テーブルをディセーブルにするには、**no ip device tracking** 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。 |
| ステップ 9 | **end** | 特権 EXEC モードに戻ります。 |

次に、AAA をイネーブルにし、RADIUS 認証を使用し、デバイス トラッキングをイネーブルにする例を示します。

```
Switch(config) configure terminal
Switch(config)# aaa new-model
Switch(config)# aaa authentication login default group radius
Switch(config)# aaa authorization auth-proxy default group radius
Switch(config)# radius-server host key key1
Switch(config)# radius-server attribute 8 include-in-access-req
Switch(config)# radius-server vsa send authentication
Switch(config)# ip device tracking
Switch(config) end
```

ポートで Web 認証を使用するように設定するには、特権 EXEC モードで次の手順を実行します。

| | コマンド | 目的 |
|---|---|---|
| ステップ 1 | **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 2 | **ip admission name** *rule* **proxy http** | Web 認証ルールを定義します。<br>（注）　Web 認証と NAC レイヤ 2 IP 検証に同じルールを使用することはできません。 |
| ステップ 3 | **interface** *interface-id* | 設定するポートを指定し、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。 |
| ステップ 4 | **switchport mode access** | ポートをアクセス モードにします。 |
| ステップ 5 | **ip access-group** *access-list* **in** | Web 認証前にネットワーク トラフィックに適用するデフォルトの Access Control List（ACL; アクセス コントロール リスト）を指定します。 |
| ステップ 6 | **ip admission** *rule* | IP 管理ルールをインターフェイスに適用します。 |
| ステップ 7 | **end** | 特権 EXEC モードに戻ります。 |
| ステップ 8 | **show running-config interface** *interface-id* | 設定を確認します。 |
| ステップ 9 | **copy running-config startup-config** | （任意）コンフィギュレーション ファイルに設定を保存します。 |

次に、スイッチ ポートで Web 認証のみを設定する例を示します。

```
Switch# configure terminal
Switch(config)# ip admission name rule1 proxy http
Switch(config)# interface gigabit1/0/1
Switch(config-if)# switchport mode access
Switch(config-if)# ip access-group policy1 in
Switch(config-if)# ip admission rule1
Switch(config-if)# end
```

フォールバック メソッドとしての Web 認証のある IEEE 802.1x 認証をスイッチ ポートに設定するには、特権 EXEC モードで次の手順を実行します。

| | コマンド | 目的 |
|---|---|---|
| ステップ 1 | **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 2 | **ip admission name** *rule* **proxy http** | Web 認証ルールを定義します。 |
| ステップ 3 | **fallback profile** *fallback-profile* | Web 認証を使用して IEEE 802.1x ポートでクライアントを認証することができるように、フォールバック プロファイルを定義します。 |
| ステップ 4 | **ip access-group** *policy* **in** | Web 認証前にネットワーク トラフィックに適用するデフォルトの ACL を指定します。 |
| ステップ 5 | **ip admission** *rule* | IP 管理ルールをプロファイルと関連付けして、Web 認証で接続するクライアントがこのルールを使用するように指定します。 |
| ステップ 6 | **end** | 特権 EXEC モードに戻ります。 |
| ステップ 7 | **interface** *interface-id* | 設定するポートを指定し、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。 |
| ステップ 8 | **switchport mode access** | ポートをアクセス モードにします。 |
| ステップ 9 | **dot1x port-control auto** | インターフェイス上で IEEE 802.1x 認証をイネーブルにします。 |

| | コマンド | 目的 |
|---|---|---|
| ステップ 10 | **dot1x fallback** *fallback-profile* | IEEE 802.1x サプリカントがポートで検出されてない場合に、Web 認証を使用してクライアントを認証するようにポートを設定します。次回 IEEE 802.1x フォールバックがインターフェイスで呼び出される際に、フォールバック プロファイルのグローバル コンフィギュレーションへの変更が有効になります。<br><br>（注）　ポートがマルチドメイン認証に設定されている場合、Web 認証を IEEE 802.1x のフォールバック メソッドとして使用することができません。 |
| ステップ 11 | **exit** | 特権 EXEC モードに戻ります。 |
| ステップ 12 | **show dot1x interface** *interface-id* | 設定を確認します。 |
| ステップ 13 | **copy running-config startup-config** | （任意）コンフィギュレーション ファイルに設定を保存します。 |

次に、フォールバック メソッドとしての Web 認証のある IEEE 802.1x 認証を設定する例を示します。

```
Switch(config) configure terminal
Switch(config)# ip admission name rule1 proxy http
Switch(config)# fallback profile fallback1
Switch(config-fallback-profile)# ip access-group default-policy in
Switch(config-fallback-profile)# ip admission rule1
Switch(config-fallback-profile)# exit
Switch(config)# interface gigabit1/0/1
Switch(config-if)# switchport mode access
Switch(config-if)# dot1x port-control auto
Switch(config-if)# dot1x fallback fallback1
Switch(config-if)# end
```

**ip admission name** および **dot1x fallback** コマンドの詳細については、このリリースに対応するコマンド リファレンスを参照してください。

## ポート上での IEEE 802.1x 認証のディセーブル化

IEEE 802.1x 認証をポートでディセーブルにするには、**no dot1x pae** インターフェイス コンフィギュレーション コマンドを使用します。

ポートで IEEE 802.1x 認証をディセーブルにするには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

| | コマンド | 目的 |
|---|---|---|
| ステップ 1 | **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 2 | **interface** *interface-id* | 設定するポートを指定し、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。 |
| ステップ 3 | **no dot1x pae** | ポート上で IEEE 802.1x 認証をディセーブルにします。 |
| ステップ 4 | **end** | 特権 EXEC モードに戻ります。 |
| ステップ 5 | **show dot1x interface** *interface-id* | 設定を確認します。 |
| ステップ 6 | **copy running-config startup-config** | （任意）コンフィギュレーション ファイルに設定を保存します。 |

IEEE 802.1x Port Access Entity（PAE; ポート アクセス エンティティ）認証者としてポートを設定するには、**dot1x pae authenticator** インターフェイス コンフィギュレーション コマンドを使用します。この設定では、ポートで IEEE 802.1x がイネーブルになりますが、ポートに接続されたクライアントは許可されません。

次に、IEEE 802.1x 認証をポートでディセーブルにする例を示します。

```
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# no dot1x pae authenticator
```

## IEEE 802.1x 認証設定のデフォルト値へのリセット

IEEE 802.1x 認証設定をデフォルト値に戻すには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

| | コマンド | 目的 |
|---|---|---|
| ステップ 1 | **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 2 | **interface** *interface-id* | 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、設定するポートを指定します。 |
| ステップ 3 | **dot1x default** | IEEE 802.1x パラメータをデフォルト値に戻します。 |
| ステップ 4 | **end** | 特権 EXEC モードに戻ります。 |
| ステップ 5 | **show dot1x interface** *interface-id* | 設定を確認します。 |
| ステップ 6 | **copy running-config startup-config** | （任意）コンフィギュレーション ファイルに設定を保存します。 |

# IEEE 802.1x の統計情報およびステータスの表示

すべてのポートに関する IEEE 802.1x 統計情報を表示するには、**show dot1x all statistics** 特権 EXEC コマンドを使用します。特定のポートに関する IEEE 802.1x 統計情報を表示するには、**show dot1x statistics interface** *interface-id* 特権 EXEC コマンドを使用します。

スイッチに関する IEEE 802.1x 管理および動作ステータスを表示するには、**show dot1x all** [**details** | **statistics** | **summary**] 特権 EXEC コマンドを使用します。特定のポートに関する IEEE 802.1x 管理および動作ステータスを表示するには、**show dot1x interface** *interface-id* 特権 EXEC コマンドを使用します。

出力フィールドの詳細については、このリリースに対応するコマンド リファレンスを参照してください。