CHAPTER 10

IEEE 802.1x ポートベースの認証の設定

この章では、Catalyst 3750 スイッチで IEEE 802.1x ポートベースの認証を設定する方法について説明します。IEEE 802.1x を使用すると、不正なデバイス（クライアント）がネットワークにアクセスするのを防止できます。特に明記しないかぎり、*スイッチ*という用語はスタンドアロン スイッチおよびスイッチ スタックを意味します。

（注） この章で使用されるコマンドの完全な構文および使用方法の詳細については、『*Cisco IOS Security Commmand Reference*』Release 12.2 の「RADIUS Commands」、およびこのリリースのコマンド 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 ポートベースの認証の概要

IEEE 802.1x 規格は、クライアント / サーバ ベースのアクセス制御と認証プロトコルについて定義し、適切に認証されていない場合、不正なクライアントが公的にアクセス可能なポートを介して LAN に接続するのを制限します。認証サーバは、スイッチ ポートに接続された各クライアントを認証してから、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。

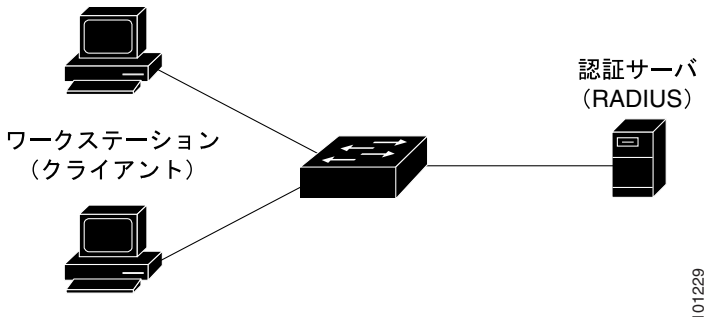
クライアントが認証されるまでは、IEEE 802.1x アクセス制御によって、クライアントに接続したポートを経由する Extensible Authentication Protocol over LAN（EAPOL）、Cisco Discovery Protocol（CDP）、および Spanning-Tree Protocol（STP; スパニング ツリー プロトコル）トラフィックだけを許可します。認証が成功すると、通常のトラフィックがポートを通過できます。

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 ポートベース認証を使用する場合、ネットワーク内のデバイスには図 10-1 のような特定の役割が割り当てられます。

図 10-1　IEEE 802.1x デバイスの役割



- *クライアント* — LAN およびスイッチへのアクセスを要求して、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 オペレーティング システムなど、IEEE 802.1x 準拠のクライアント ソフトウェアが稼働する必要があります（クライアントは、IEEE 802.1x 規格の *サプリカント*になります）。

（注）　Windows XP ネットワーク接続および IEEE 802.1x 認証の問題を解決するには、次の URL にアクセスして Microsoft Knowledge Base の項目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* — 実際にクライアントの認証を行います。認証サーバは、クライアントの ID を確認し、クライアントの LAN およびスイッチ サービスへのアクセスを許可する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機能するので、認証サービスはクライアントにトランスペアレントです。このリリースでサポートされている認証サーバは、Extensible Authentication Protocol（EAP）拡張機能を装備した 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 以上に対応しています。RADIUS は、RADIUS サーバと 1 つまたは複数の RADIUS クライアント間で安全な認証情報が交換されるクライアント / サーバ モデルで動作します。
- *スイッチ*（エッジ スイッチまたは無線アクセス 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的な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間の媒介（プロキシ）として機能し、クライアントに ID 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 RADIUS クライアントが組み込まれています。RADIUS クライアントは、EAP フレームのカプセル化 / カプセル化解除、および認証サーバとの相互作用の役割を果たします。

  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と、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 形式で再度カプセル化されます。EAP フレームはカプセル化の間は変更が行われず、認証サーバはネイティブのフレーム形式で EAP をサポートする必要があります。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、EAP フレームが残ります。これがイーサネット用にカプセル化されてクライアントに送信されます。

  媒介として機能できるデバイスには、Catalyst 3750、Catalyst 3560、Catalyst 3550、Catalyst 2970、Catalyst 2960、Catalyst 2955、Catalyst 2950、Catalyst 2940 スイッチ、または無線アクセス ポイントがあります。これらのデバイスは、RADIUS クライアントおよび IEEE 802.1x をサポートするソフトウェアを実行している必要があります。

認証の開始とメッセージ交換

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する場合、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されたときに認証を開始します。またはポートがアップおよび未認証のままであるかぎり、定期的に認証が行われます。スイッチは、クライアントに EAP 要求 / アイデンティティ フレームを送信して、クライアントの ID を要求します。フレームの受信後、クライアントは EAP 応答 / アイデンティティ フレームで応答します。

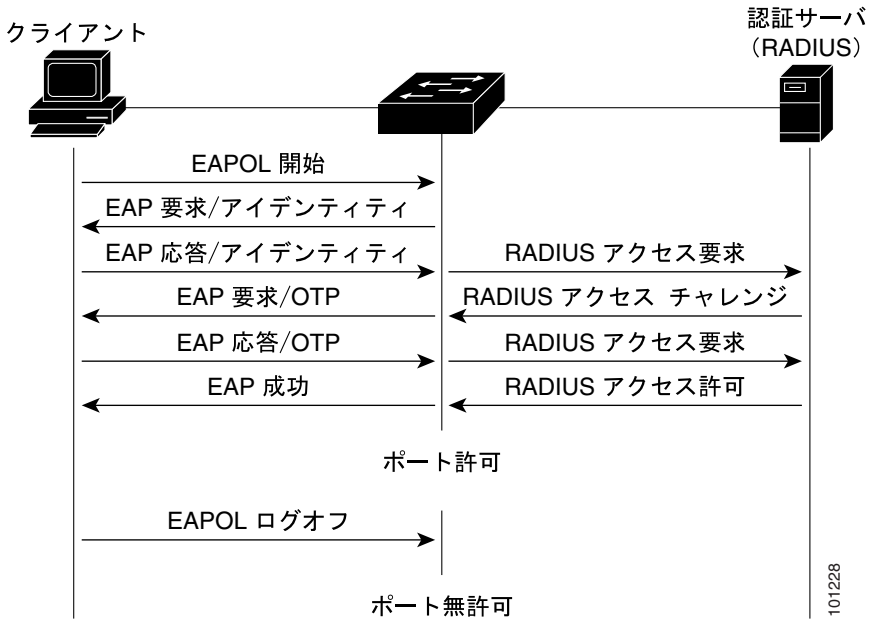
ただし、起動中にクライアントがスイッチから EAP 要求 / アイデンティティ フレームを受信しない場合は、クライアントは、EAPOL 開始フレームを送信して認証を開始できます。これにより、スイッチはクライアントのアイデンティティを要求するようになります。

（注）　ネットワーク アクセス デバイスで IEEE 802.1x がイネーブルになっていないかサポートされていない場合は、クライアントからの EAPOL フレームはすべて廃棄されます。認証の開始を 3 回試行してもクライアントが EAP 要求 / アイデンティティ フレームを受信しない場合は、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を送信します。許可ステートにあるポートは、事実上クライアントが正常に認証されたということです。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.10-4）を参照してください。

クライアントがそのアイデンティティを供給すると、スイッチは媒介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との間で EAP フレームを受け渡します。認証が成功すると、スイッチのポートは許可された状態になります。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.10-4）を参照してください。

特定の EAP フレーム交換は、使用される認証方式に依存します。図 10-2 に、RADIUS サーバで One Time Password（OTP; ワンタイム パスワード）認証方式を使用するクライアントによって開始されるメッセージ交換を示します。

図 10-2　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

スイッチ ポートのステートによって、スイッチはクライアントのネットワーク アクセスを許可できるかを判断します。ポートは、*無許可ステート*で開始します。このステートにある間は、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、CDP、STP パケットを除く入力トラフィックおよび出力トラフィックをすべて許可しません。クライアントが正常に認証されると、ポートは*許可ステート*に変更され、そのクライアントへのすべてのトラフィックは通常のフローが許可されます。ポートが音声 VLAN ポートとして設定されている場合、クライアントが正常に認証される前に、ポートは Voice over IP（VoIP）トラフィックおよび IEEE 802.1x プロトコル パケットを許可します。

IEEE 802.1x をサポートしないクライアントが無許可の IEEE 802.1x ポートに接続している場合は、スイッチはクライアントにアイデンティティを要求します。この場合、クライアントは要求に応答できないので、ポートは無許可ステートのままで、クライアントはネットワーク アクセスが許可されません。

対照的に、IEEE 802.1x 対応クライアントが IEEE 802.1x 規格を実行していないポートに接続している場合、クライアントは EAPOL 開始フレームを送信して認証プロセスを開始します。応答が得られなかった場合、クライアントは要求を一定の回数だけ送信します。応答が得られないので、クライアントはポートが許可ステートにあるものとしてフレームの送信を開始します。

ポートの許可ステートを制御するには、**dot1x port-control** インターフェイス コンフィギュレーション コマンドと以下のキーワードを使用します。

- **force-authorized —** IEEE 802.1x 認証をディセーブルにして、認証情報の交換を要求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 ベースの認証なしで通常のトラフィックを送受信します。これがデフォルト設定です。
- **force-unauthorized —** ポートを無許可ステートのままにし、クライアントが認証を試みてもすべて無視します。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て、ポートに無許可ステートで開始させ、EAPOL フレームだけがポート経由で送受信できるようにします。ポートのリンク ステートがダウンからアップに変更されるか、EAPOL 開始フレームを受信すると、認証プロセスが開始されます。スイッチは、クライアントのアイデンティティを要求し、クライアントと認証サーバ間で認証メッセージのリレーを開始します。スイッチはネットワークにアクセスしようとする各クライアントを、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一意に識別します。

クライアントが正常に認証されると（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のフレームはすべてそのポート経由で送受信を許可されます。認証が失敗した場合は、ポートは無許可ステートのままですが、認証を再試行できます。認証サーバにアクセスできない場合、スイッチは要求を再送信できます。指定された試行回数のあとでもサーバから応答が得られない場合は、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 EAPOL ログオフ メッセージを送信します。これにより、スイッチ ポートは無許可ステートに変更されます。

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

IEEE 802.1x アカウンティング

IEEE 802.1x 標準では、ネットワークへのユーザのアクセスを許可および認証する方法を定義します。ただし、ネットワーク使用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。代わりに、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設定する必要があります。

IEEE 802.1x アカウンティングのアトリビュートと値のペア

RADIUS サーバに送信された情報は、アトリビュートと値（AV）ペアという形式で表されます。AV ペアは、さまざまなアプリケーションにデータを提供します。たとえば課金アプリケーションでは、RADIUS パケットの Acct-Input-Octets アトリビュートまたは Acct-Output-Octets アトリビュートの情報が必要となることがあります。

AV ペアは、IEEE 802.1x アカウンティング用に設定されたスイッチによって自動的に送信されます。スイッチでは、次の 3 種類の RADIUS アカウンティング パケットが送信されます。

- START — 新しいユーザ セッションの開始時に送信
- INTERIM — 既存セッション中、アップデートのために送信
- STOP — セッションの終了時に送信

表 10-1 に、AV ペアおよび各ペアがスイッチによって送信されるか否かを示します。

表 10-1　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
Attribute[1]	User-Name	常に送信	常に送信	常に送信
Attribute[4]	NAS-IP-Address	常に送信	常に送信	常に送信
Attribute[5]	NAS-Port	常に送信	常に送信	常に送信
Attribute[8]	Framed-IP-Address	送信なし	一部送信[1]	一部送信[1]
Attribute[25]	Class	常に送信	常に送信	常に送信
Attribute[30]	Called-Station-ID	常に送信	常に送信	常に送信
Attribute[31]	Calling-Station-ID	常に送信	常に送信	常に送信
Attribute[40]	Acct-Status-Type	常に送信	常に送信	常に送信
Attribute[41]	Acct-Delay-Time	常に送信	常に送信	常に送信
Attribute[42]	Acct-Input-Octets	送信なし	送信なし	常に送信
Attribute[43]	Acct-Output-Octets	送信なし	送信なし	常に送信
Attribute[44]	Acct-Session-ID	常に送信	常に送信	常に送信
Attribute[45]	Acct-Authentic	常に送信	常に送信	常に送信
Attribute[46]	Acct-Session-Time	送信なし	送信なし	常に送信
Attribute[49]	Acct-Terminate-Cause	送信なし	送信なし	常に送信
Attribute[61]	NAS-Port-Type	常に送信	常に送信	常に送信

1. 有効な Dynamic Host Control Protocol（DHCP; 動的ホスト制御プロトコル）バインディングが、DHCP スヌーピング バインディング テーブルのホスト用に存在する場合に限って、Framed-IP-Address AV ペアは送信されます。

スイッチによって送信されている AV ペアを表示するには、**debug radius accounting** イネーブル EXEC コマンドを入力します。このコマンドの詳細については、次の URL の『*Cisco IOS Debug Command Reference*』Release 12.2 を参照してください。

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122sup/122debug

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。

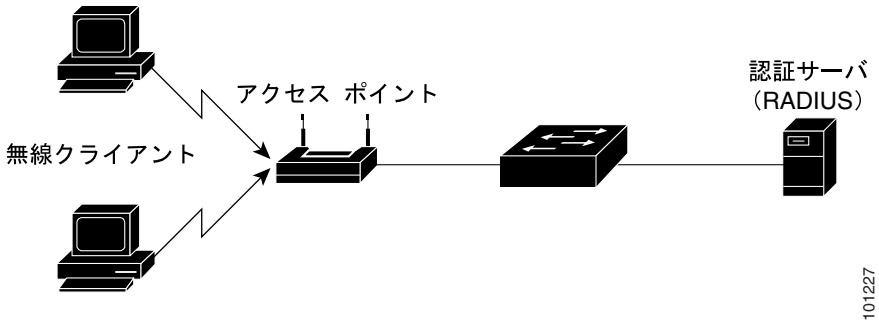
IEEE 802.1x ホスト モード

IEEE 802.1x ポートは、単一ホスト モードまたは複数ホスト モードに設定できます。単一ホスト モード（図 10-1 [p.10-2] を参照）では、IEEE 802.1x 対応のスイッチ ポートに接続できるクライアントは 1 台だけです。スイッチは、ポートのリンク ステートがアップに変化すると、EAPOL フレームを送信してクライアントを検出します。クライアントがログオフするか、別のクライアントに交換されると、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。

複数ホスト モードでは、単一の IEEE 802.1x 対応ポートに複数のホストを接続できます。図 10-3（p.10-7）に、無線 LAN における IEEE 802.1x ポートベースの認証を示します。このモードでは、接続クライアントのいずれか 1 つだけが許可されれば、すべてのクライアントがネットワーク アクセスを許可されます。ポートが無許可になると（再認証が失敗するか、EAPOL ログオフ メッセージを受信する）、スイッチは、接続しているすべてのクライアントに対してネットワーク アクセスを拒否します。このトポロジーでは、無線アクセス ポイントは、接続しているクライアントを認証する役割があり、スイッチに対してクライアントとしても機能します。

複数ホスト モードがイネーブルの場合、IEEE 802.1x をポートの認証に使用して、クライアントを含むすべての MAC アドレスへのネットワーク アクセスをポート セキュリティが管理します。

図 10-3　複数ホスト モードの例



IEEE 802.1x とポート セキュリティの使用方法

単一ホスト モードまたは複数ホスト モードのどちらかで、IEEE 802.1x ポートおよびポート セキュリティを設定できます（**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）。ポート上のポート セキュリティと IEEE 802.1x をイネーブルにすると、IEEE 802.1x がポートを認証し、ポート セキュリティがクライアントの MAC アドレスを含むすべての MAC アドレスについてネットワーク 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。

たとえば、スイッチにおいて、IEEE 802.1x とポート セキュリティの間には次のような相互作用があります。

- 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ければ、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ると、セキュア ホスト テーブル内のエントリが保証されます（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セキュリティ テーブルがいっぱいの場合は、セキュア違反が発生します。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 テーブルの位置は他のホストに取って代わられます。

最初の認証ホストによってセキュリティ違反が引き起こされた場合、ポートは errdisable となり、すぐにシャットダウンされます。

ポート セキュリティ違反モードは、セキュリティ違反の動作を判別します。詳細については、「セキュリティ違反」（p.25-11）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、IEEE 802.1x クライアントのアドレスをポート セキュリティ テーブルから手動で削除した場合は、**dot1x re-authenticate interface** *interface-id* イネーブル 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、ポートが無許可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 テーブル内のすべてのダイナミック エントリがクリアされます。ここで通常の認証が実行されます。
- ポートが管理上の理由からシャットダウンされる場合、ポートは無許可ステートになり、すべてのダイナミック エントリはセキュア ホスト テーブルから削除されます。
- ポート セキュリティと音声 VLAN は、単一ホストまたは複数ホスト モードのどちらかで、IEEE 802.1x ポートに同時に設定できます。ポート セキュリティは、Voice VLAN Identifier（VVID; 音声 VLAN ID）と Port VLAN Identifier（PVID; ポート VLAN ID）の両方に適用されます。

スイッチのポート セキュリティをイネーブルにする方法の詳細については、「ポート セキュリティの設定」（p.25-10）を参照してください。

IEEE 802.1x と音声 VLAN ポートの使用方法

音声 VLAN ポートは、2 つの VLAN ID に関連付けられた特殊なアクセス ポートです。

- IP Phone の入出音声トラフィックを搬送するための VVID。VVID は、ポートに接続されている 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の入出データ トラフィックを搬送するための PVID。PVID は、ポートのネイティブ VLAN です。

Cisco IOS Release 12.1(14)EA1 より前のリリースでは、単一ホスト モードのスイッチは単一ホストからのトラフィックのみを受け取り、音声トラフィックは受信できませんでした。複数ホスト モードでは、スイッチはクライアントがプライマリ VLAN 上で認証されるまで音声トラフィックを受け取れなかったため、IP Phone はユーザがログインするまで動作不能でした。

Cisco IOS Release 12.1(14)EA1 以上では、IP Phone は、ポートのステートに対する許可に関わらず、音声トラフィック用として VVID を使用します。これによって、IP Phone は IEEE 802.1x 認証とは独立して動作できます。

単一ホスト モードでは、音声 VLAN で許可されるのは IP Phone だけです。複数ホスト モードでは、PVID 上でサプリカントが認証されてから、追加のクライアントが音声 VLAN 上でトラフィックを送信できます。複数ホスト モードがイネーブルの場合、サプリカント認証は PVID および VVID の両方に影響します。

リンクが存在していれば音声 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 アドレスが明らかになります。Cisco IP Phone は、他のデバイスからの CDP メッセージをリレーしません。そのため、複数の IP Phone が直列で接続されても、スイッチは自身に直接接続された IP Phone しか認識しません。音声 VLAN ポートで IEEE 802.1x をイネーブルにすると、スイッチは 2 ホップ以上離れた認識されていない IP Phone からのパケットを廃棄します。

IEEE 802.1x をポートでイネーブルにすると、音声 VLAN と同じようにポート VLAN を設定できません。

（注）　音声 VLAN が設定されていて Cisco IP Phone が接続されているアクセス ポートで IEEE 802.1x をイネーブルにする場合、Cisco IP Phone とスイッチとの接続が最大 30 秒切断されます。

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。

IEEE 802.1x と VLAN 割り当ての使用方法

Cisco IOS Release 12.1(14)EA1 より古いリリースでは、IEEE 802.1x ポートが認証されると、RADIUS サーバがデータベースから許可済み VLAN の情報を返しても、そのポートは自身に設定されたアクセス VLAN に対して許可されました。アクセス VLAN は、アクセス ポートに割り当てられた VLAN であり、このポートとの間で送受信されたすべてのパケットは、この VLAN に属しています。

ただし、Cisco IOS Release 12.1(14)EA1 以上のリリースでは、スイッチは IEEE 802.1x と VLAN 割り当てをサポートしています。ポートの IEEE 802.1x 認証が成功すると、RADIUS サーバは、スイッチ ポートを設定するために VLAN 割り当てを送信します。RADIUS サーバのデータベースは、ユーザ名 /VLAN のマッピングを維持します。この対応では、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 を割り当てています。この機能を使用して、特定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 サーバを設定する場合、IEEE 802.1x と VLAN 割り当てには次の特性があります。

- RADIUS サーバが VLAN を割り当てていないか、または IEEE 802.1x 許可がディセーブルの場合、認証が成功したあとにポートはアクセス VLAN に設定されます。
- IEEE 802.1x 許可がイネーブルでも、RADIUS サーバからの VLAN 情報が有効でない場合には、ポートは無許可ステートに戻り、設定済みのアクセス VLAN 内に留まります。これにより、設定エラーによって不適切な VLAN 上にポートが突然現れることを防ぎます。

  設定エラーには、ルーテッド ポートへの VLAN の指定、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）の VLAN ID、あるいは音声 VLAN ID への割り当て試行、などがあります。
- IEEE 802.1x 許可がイネーブルで RADIUS サーバからのすべての情報が有効の場合、ポートは認証が成功した後、指定された VLAN に配置されます。
- IEEE 802.1x ポートで複数ホスト モードがイネーブルの場合は、全てのホストが最初に認証されたホストと同じ VLAN（RADIUS サーバによって指定された）に配置されます。
- IEEE 802.1x とポート セキュリティがポート上でイネーブルの場合は、そのポートは 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 がポートでディセーブルの場合は、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）、強制無許可（force unauthorized）、無許可、シャットダウンのいずれかのステートの場合、その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 に配置された場合、ポートのアクセス VLAN 設定への変更は反映されません。

VLAN 割り当て機能付きの IEEE 802.1x は、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）を使用したダイナミック アクセス ポート割り当てではサポートされていません。

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 をイネーブルにします。（VLAN 割り当て機能は、アクセス ポートに IEEE 802.1x が設定されると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戻さなければなりません。
  - [64] トンネル タイプ = VLAN
  - [65] トンネル メディア タイプ = 802
  - [81] トンネル プライベート グループ ID = VLAN 名または VLAN ID

  アトリビュート [64] は、値 *VLAN*（type 13）でなければなりません。アトリビュート [65] は、値 *802*（type 6）でなければなりません。アトリビュート [81] には、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 アトリビュート用にスイッチを設定する方法」（p.9-30）を参照してください。

IEEE 802.1x とゲスト VLAN の使用方法

スイッチ上の各 IEEE 802.1x ポートにゲスト VLAN を設定し、クライアントへのサービスを限定できます（たとえば、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 認証対応のシステムにアップグレードされている場合もあれば、Windows 98 システムなどの一部のホストは IEEE 802.1x に対応していない場合もあります。

IEEE 802.1x ポート上でゲスト VLAN をイネーブルにすると、スイッチが EAP 要求 / アイデンティティ フレームに対する応答を受信していない場合、またはクライアントが EAPOL パケットを送信していない場合に、スイッチがゲスト VLAN にクライアントを割り当てます。

Cisco IOS Release 12.2(25)SE1 より古いリリースでは、インターフェイスで EAPOL パケットが検出されたかどうかに関わらず、スイッチは EAPOL パケット履歴を維持せずに、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ていました。**dot1x guest-vlan supplicant** グローバル コンフィギュレーション コマンドを使用すると、このオプション動作をイネーブルにできます。

Cisco IOS Release 12.2(25)SE 以降のリリースでは、スイッチは EAPOL パケット履歴を維持します。リンクの存続時間中に EAPOL パケットがインターフェイスで検出されると、スイッチはインターフェイスに接続されているデバイスが IEEE 802.1x 対応のサプリカントであると判断し、インターフェイスはゲスト VLAN ステートに変更されません。インターフェイスのリンク ステータスがダウンになると、EAPOL 履歴は消去されます。インターフェイスで EAPOL パケットが検出されない場合は、インターフェイスはゲスト VLAN ステートに移行します。

（注）　インターフェイスがゲスト VLAN に移行したあとに EAPOL パケットが検出されると、インターフェイスは無許可ステートに戻り、802.1x 許可が再開されます。

スイッチ ポートがゲスト VLAN に移動された場合には、IEEE 802.1x 非対応クライアントにアクセスが許可されます。IEEE 802.1x 対応のクライアントが、ゲスト VLAN が設定されているポートと同じポートに結合すると、そのポートはユーザ設定済みのアクセス VLAN 内で無許可ステートに移行し、認証がやり直されます。

ゲスト VLAN は、単一ホストまたは複数ホスト モードの IEEE 802.1x ポートでサポートされています。

RSPAN VLAN、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。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。

詳細については、「ゲスト VLAN の設定」（p.10-26）を参照してください。

IEEE 802.1x と制限付き VLAN の使用方法

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 スタックまたはスイッチの各 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 IEEE 802.1x に準拠していて、認証プロセスに失敗したために他の VLAN にアクセスできません。制限付き VLAN を使用すると、ユーザは認証サーバ内に有効な証明書を持たなくても（一般に企業への訪問者）、限定されたサービスにアクセスできます。管理者は制限付き VLAN で使用可能なサービスを制御できます。

（注）　ゲスト VLAN と制限付き VLAN の両方に同一のサービスを提供する場合は、VLAN を両タイプ用に設定できます。

この機能を使用しない場合は、クライアントは認証の試行と失敗を何度も繰り返し、スイッチ ポートはスパニングツリー ブロッキング ステートのままになります。この機能を使用すると、指定された回数の認証試行（デフォルト値は 3 回）のあと、スイッチ ポートが制限付き VLAN になるように設定できます。

認証サーバはクライアントの認証失敗回数をカウントします。カウントが、設定されている認証試行の最大回数を超過すると、ポートは制限付き VLAN に移行します。失敗試行のカウントは、RADIUS サーバが *EAP failure* を返すかまたは EAP パケットのない空の応答を返すと、増分されます。ポートが制限付き VLAN に移行すると、失敗試行カウンタはリセットされます。

認証に失敗したユーザは、次の再認証試行まで制限付き VLAN に残ります。制限付き VLAN 内のポートは、設定された間隔（デフォルトは 60 秒）で再認証を試みます。再認証が失敗すると、ポートは制限付き VLAN のままとなります。再認証が成功すると、ポートは設定済み VLAN または RADIUS サーバから通知された VLAN に移行します。再認証はディセーブルにできます。ディセーブルにすると、ポートが *link down* または *EAP logoff* イベントを受信した場合にのみ認証プロセスが再開されます。クライアントがハブ経由で接続される可能性がある場合は、再認証をイネーブルにしておくことを推奨します。クライアントがハブから切り離されたときに、ポートは *link down* または *EAP logoff* イベントを受信できない可能性があります。

ポートが制限付き VLAN に移行したあとに、シミュレートされた EAP success メッセージがクライアントに送信されます。これにより、クライアントによる無期限の認証試行が抑制されます。一部のクライアント（Windows XP を実行するデバイスなど）は、EAP success がないと DHCP を実行できません。

制限付き VLAN は、シングルホスト モードの IEEE 802.1x ポートおよびレイヤ 2 ポートでのみサポートされます。

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 に設定できます。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 セキュリティと併用されます。ポートが許可されると、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 MAC アドレスを許可しない場合、またはセキュア アドレス カウントが最大に達している場合は、ポートは無許可になり、エラー ディセーブル状態となります。

ダイナミック ARP 検査、DHCP スヌーピング、および IP ソース ガードなどの、その他のポート セキュリティ機能は、制限付き VLAN 上に独立して設定できます。

詳細については、「制限付き VLAN の設定」（p.10-28）を参照してください。

IEEE 802.1x とアクセス不能認証バイパスの併用

Cisco IOS Release 12.2(25)SED 以降では、スイッチが設定済みの RADIUS サーバに到達できず、ホストが許可されない場合、*クリティカル* ポートに接続されたホストへのネットワーク アクセスを許可するよう、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*機能に対し、イネーブルになります。

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。サーバが利用可能な場合は、スイッチはホストの認証を行うことができます。ただし、すべての RADIUS サーバが利用不能な場合は、スイッチはホストへのネットワーク アクセスを許可し、ポートを認証ステートの特殊ケースである、クリティカル認証ステートに移行します。

アクセス不能認証バイパス機能の動作は、次のようにポートの許可ステートに依存します。

- クリティカル ポートに接続されたホストが認証を試行し、すべてのサーバが利用不能なときにポートが無許可の場合、スイッチは EAP success メッセージをホストに送信し、設定済みアクセス VLAN のポートをクリティカル認証ステートに移行させます。
- ポートが許可済みであり、再許可要求が発生した場合、スイッチは以前 RADIUS サーバによって割り当てられた可能性のある現行 VLAN 内のクリティカル ポートを、クリティカル認証ステートに移行させます。
- 認証交換中に RADIUS サーバが利用不能になった場合、認証交換がタイムアウトになり、スイッチは次回の認証試行の際にクリティカル ポートをクリティカル認証ステートに移行させます。

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 ポートが自動的に再認証されます。

最初のクリティカル ポートが設定されたあと、スイッチはサーバのステータス（*dead* または *alive*）を確認するために、RADIUS サーバに対して、server-detection リクエストの送信を定期的に開始します。スイッチは定期的にキープアライブ パケットをサーバに送信します。認証プロセス中に、RADIUS サーバが利用不能であるというエラー メッセージをスイッチが受け取ると、スイッチはサーバのステータスを確認するために即座にキープアライブ パケットを送信します。

スイッチ スタックでは、スタック マスターがキープアライブ パケットを送信して RADIUS サーバのステータスを確認します。RADIUS サーバのステータスが変化すると、スタック マスターはその情報をスタック メンバーに送信します。これにより、スタック メンバーはクリティカル ポートの再認証の際に RAIDUS サーバのステータスを確認できます。

新しいスタック マスターが選ばれると、スイッチ スタックと RADIUS サーバ間のリンクが変更することがあり、新しいスタック マスターは RADIUS サーバのステータスを更新するために、即座にキープアライブ パケットを送信します。サーバのステータスが dead から alive に変化すると、スイッチはクリティカル認証ステートの状態にあるすべてのスイッチ ポートを再認証します。

スタックにメンバーが追加されると、スタック マスターはそのメンバーにサーバ ステータスを送信します。

IEEE 802.1x と Wake-on-LAN の使用方法

IEEE 802.1x Wake-on-LAN（WoL）機能では、*マジック パケット*という特殊なイーサネット フレームをスイッチが受信すると、休止状態の PC に電源が入ります。管理者が電源切断されたシステムに接続する必要がある環境で、この機能を使用できます。

WoL を使用するホストが IEEE 802.1x ポートで接続されていて、ホストの電源が切断されると、IEEE 802.1x ポートは無許可になります。この状態の場合、ポートは EAPOL パケットの送受信しかできないため、WoL マジック パケットはホストに達しません。PC の電源が切断されると、PC は認証されず、スイッチ ポートは開きません。

スイッチで IEEE 802.1x と WoL を使用すると、スイッチは無許可 IEEE 802.1x ポートにパケットを送信します。この機能は、IEEE 802.1x 仕様で*単一方向制御ポート*と呼ばれています。

（注）　ポートで PortFast が有効になっていない場合、ポートは双方向状態になります。

単一方向状態

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として設定すると、ポートはスパニングツリー フォワーディング ステートに変更されます。

WoL を有効にすると、接続しているホストはスリーピング モードまたはパワーダウン状態になります。ホストは、ネットワーク内の他のデバイスとは、トラフィックの交換を行いません。ネットワークにトラフィックを送信できない単一方向ポートにホストを接続した場合、ホストはネットワーク内の他のホストからのみトラフィックを受信します。単一方向ポートが着信トラフィックを受信すると、ポートはデフォルトの双方向状態に戻り、スパニングツリー ブロッキング ステートに変更されます。ポートが初期状態に変更されると、EAPOL パケット以外のトラフィックは許可されません。ポートが双方向状態に戻ると、スイッチは 5 分間のタイマーをスタートします。タイマーが終了する前にポートが認証されないと、ポートは単一方向ポートになります。

双方向状態

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として設定すると、ポートは双方向でアクセス制御されます。この状態の場合、スイッチ ポートはパケットの送受信を行いません。

IEEE 802.1x とユーザ単位 ACL の使用方法

ユーザ単位の Access Control List（ACL; アクセス制御リスト）をイネーブルにして、IEEE 802.1x 認証ユーザが異なるレベルのネットワーク アクセスやサービスを使えるようにできます。RADIUS サーバは、IEEE 802.1x ポートに接続されているユーザを認証すると、ユーザ ID に基づき ACL アトリビュートを検索し、それらをスイッチへ送信します。スイッチは、ユーザ セッションの間、それらのアトリビュートを IEEE 802.1x ポートに適用します。スイッチは、セッションの終了後、認証が失敗した場合、またはリンクダウン状態の発生時に、ユーザ単位の ACL 設定を削除します。スイッチは、RADIUS 固有の ACL を実行コンフィギュレーションには保存しません。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。

同一スイッチ上で、ACL の設定およびポート ACL の入力を行えます。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。発信されるルーテッド パケットは、ルータ ACL によってフィルタリングされます。設定の矛盾を回避するには、RADIUS サーバに保存するユーザ プロファイルを慎重に計画しなければなりません。

RADIUS は、Vendor Specific Attribute（VSA）などのユーザ単位アトリビュートをサポートします。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。レイヤ 2 ポートの出力方向ではポート ACL をサポートしません。詳細については、第 32 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場合、拡張命名規則を使用して作成されます。ただし、フィルタ 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。

フィルタ 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、そのあとに入力フィルタリングか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。スイッチ上では Cisco IOS アクセス リストのサポートは限定されているため、フィルタ ID アトリビュートは番号が 1 ～ 199 および 1300 ～ 2699 までの IP ACL（IP 標準 ACL と IP 拡張 ACL）でのみサポートされています。

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。複数ホスト 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。

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 アトリビュート用にスイッチを設定する方法」（p.9-30）を参照してください。ACL の設定の詳細については、第 32 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 ACL を設定するには、以下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 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。
- IEEE 802.1x ポートを単一ホスト モードに設定します。

IEEE 802.1x とスイッチ スタック

スイッチがスイッチ スタックで追加または削除されても、RADIUS サーバとスタック間の IP 接続がそのまま残っているかぎりは、IEEE 802.1x 認証には影響はありません。このことは、スタック マスターがスイッチ スタックから削除された場合にも当てはまります。スタック マスターに障害が生じると、スタック メンバーが第 5 章「スイッチ スタックの管理」に記載された選択プロセスを使用して新たなスタック マスターとなり、IEEE 802.1x 認証プロセスが通常どおり継続される点に注意してください。

RADIUS サーバへの IP 接続が、サーバに接続されていたスイッチが削除された、またはそのスイッチに障害が発生したといった理由で切断された場合には、次のイベントが発生します。

- 既に認証済みで定期的な再認証がイネーブル化されていないポートは、認証ステートのままです。RADIUS サーバとのやり取りは必要ありません。
- 既に認証済みで、定期的な再認証がイネーブル化されているポートは（**dot1x re-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）、再認証時に認証プロセスに失敗します。ポートは、再認証プロセスで無許可ステートに戻ります。RADIUS サーバとのやり取りが必要となります。

  進行中の認証は、サーバ接続がないため即時に失敗します。

障害の発生したスイッチが再びアップし、スイッチ スタックに参加した場合は、起動時間と、認証が試行されるまでに RADIUS サーバへの接続が再確立されたかどうかによって、認証は失敗することもあればしないこともあります。

RADIUS サーバへの接続の切断を避けるには、冗長接続を確立しておく必要があります。たとえば、スタック マスターへの冗長接続とスタック メンバーへの別の冗長接続を確立しておけば、スタック マスターに障害が発生しても、スイッチ スタックは RADIUS サーバへの接続を維持できます。

IEEE 802.1x 認証の設定

ここでは、次の設定について説明します。

IEEE 802.1x のデフォルト設定

表 10-2 に、IEEE 802.1x のデフォルト設定を示します。

表 10-2　IEEE 802.1x のデフォルト設定

機能	デフォルト設定
AAA	ディセーブル
制御方向	双方向制御
RADIUS サーバ • IP アドレス • UDP 認証ポート • 鍵	 • 指定なし • 1812 • 指定なし
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） ポートは、クライアントの IEEE 802.1x ベースの認証なしで通常のトラフィックを送受信します。
定期的再認証	ディセーブル
再認証試行間隔	3600 秒
再認証回数	2 回（ポートが無許可ステートになるまで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（クライアントとの認証交換が失敗したあと、スイッチが待機ステートにとどまる秒数）

表 10-2　IEEE 802.1x のデフォルト設定（続き）

機能	デフォルト設定
再送信時間	30 秒（スイッチが、クライアントからの EAP 要求 / アイデンティティ フレームに対する応答を待ち、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までに EAP 要求 / アイデンティティ フレームを送信する回数）
ホスト モード	単一ホスト モード
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
クライアントのタイムアウト時間	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に、スイッチが応答を待ち、クライアントに要求を再送信するまでの時間）
認証サーバのタイムアウト時間	30 秒（クライアントの応答を認証サーバにリレーするときに、スイッチが応答を待ち、サーバに応答を送信するまでの時間。この値は設定変更不可能）

IEEE 802.1x 設定時の注意事項

IEEE 802.1x 認証の設定時の注意事項は次のとおりです。

- IEEE 802.1x がイネーブルに設定されていると、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、ポートは認証されます。
- 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、レイヤ 3 ルーテッド ポートでサポートされていますが、次のポート タイプではサポートされていません。
  - トランク ポート ― トランク ポートで IEEE 802.1x 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 はイネーブルになりません。IEEE 802.1x 対応ポートのモード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、近接ポートとネゴシエーションしてトランク ポートになる可能性があります。ダイナミック ポートで IEEE 802.1x 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 はイネーブルになりません。IEEE 802.1x 対応ポートのモード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 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 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 VLAN 割り当てに変更しようとすると、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 メンバーまたは未アクティブ メンバーであるポートは 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 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 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、EtherChannel の未アクティブのポートで IEEE 802.1x がイネーブルの場合、ポートが 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 Remote SPAN（RSPAN; リモート SPAN）宛先ポート ― SPAN または RSPAN 宛先ポートであるポートで IEEE 802.1x をイネーブルにできます。ただし、SPAN または RSPAN 宛先ポートとして削除するまでは、IEEE 802.1x 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 をイネーブルにできます。

- RSPAN VLAN、プライベート VLAN、または音声 VLAN を除き、任意の 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。
- 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 VLAN を IEEE 802.1x 制限付き VLAN に設定できます。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。
- IEEE 802.1x をポートでイネーブルにすると、音声 VLAN と同じようにポート VLAN を設定できません。
- VLAN 割り当て機能付きの IEEE 802.1x は、プライベート VLAN ポート、トランク ポート、ダイナミック ポート、または VMPS を使用したダイナミック アクセス ポート割り当てではサポートされていません。
- プライベート VLAN ポートで IEEE 802.1x を設定できます。ただし、プライベート VLAN ポート上で、IEEE 802.1x とポート 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 を設定しないでください。
- **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スイッチで IEEE 802.1x をグローバルにイネーブルにする前に、IEEE 802.1x および EtherChannel が設定されているインターフェイスから EtherChannel コンフィギュレーションを削除します。
- EAP-Transparent LAN Service（TLS）および EAP-MD5 を使用する IEEE 802.1x 認証用の Cisco Access Control Server（ACS）アプリケーションを実行しているデバイスを使用していて、スイッチが Cisco IOS Release 12.1(14)EA1 を実行している場合、デバイスで ACS バージョン 3.2.1 以降が動作していることを確認します。
- DHCP クライアントが接続されている IEEE 802.1x ポートにゲスト VLAN を設定したあと、DHCP サーバからホスト IP アドレスを取得する必要があります。クライアントでの DHCP プロセスがタイムアウトして DHCP サーバからホスト IP アドレスを取得しようとする前に、スイッチでの IEEE 802.1x 認証プロセスを再開するように設定を変更できます。IEEE 802.1x 認証プロセスに対する設定を減らします（**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）。設定の減少量は接続されている IEEE 802.1x クライアントのタイプに依存します。

アクセス不能認証バイパス機能をイネーブルにする場合は、次のガイドラインに従ってください。

　－ この機能は、シングルホスト モードの IEEE 802.1x ポートでのみサポートされます。ポートをクリティカル ポートに設定しようとした場合、またはホスト モードをマルチホスト モードに変更した場合は、次のメッセージが表示されます。

```
%Command rejected: Critical ports are only allowed in single-host mode
```

　－ クライアントが Windows XP を実行していて、クライアントが接続されているポートがクリティカル認証ステートにある場合、インターフェイスが認証されていないというメッセージが Windows XP によって表示される場合があります。

　－ Windows XP クライアントが DHCP を使用するように設定されていて、DHCP サーバから得た IP アドレスを使用している場合、クリティカル ポートで EAP success メッセージを受信しても、DHCP コンフィギュレーション プロセスが再開されないことがあります。

　－ IEEE 802.1x ポートにアクセス不能認証バイパス機能と制限付き VLAN を設定することができます。スイッチが制限付き VLAN 内のクリティカル ポートに対して再認証を試み、すべての RADIUS サーバが利用不能な場合、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 内に残ります。

　－ アクセス不能認証バイパス機能とポート セキュリティは、同一のスイッチ ポート上に設定できます。

旧ソフトウェア リリースからのアップグレード

Cisco IOS Release 12.1(14)EA1 では、IEEE 802.1x の実装はそれ以前のリリースとは異なっています。一部のグローバル コンフィギュレーション コマンドがインターフェイス コンフィギュレーション コマンドとなり、新たなコマンドが追加されました。

IEEE 802.1x が設定済みのスイッチを Cisco IOS Release 12.1(14)EA1 以上のリリースへアップグレードした場合は、コンフィギュレーション ファイルに新規コマンドが含まれないため、IEEE 802.1x は動作しません。アップグレードが完了後に、**dot1x system-auth-control** グローバルコンフィギュレーション コマンドを使用してグローバルに IEEE 802.1x をイネーブル化する必要があります。IEEE 802.1x が以前のリリースのインターフェイス上で複数ホスト モードで稼働していた場合は、必ず、**dot1x host-mode multi-host** インターフェイス コンフィギュレーション コマンドを使用してそれを再設定してください。

IEEE 802.1x 認証の設定

IEEE 802.1x ポートベースの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。

IEEE 802.1x AAA プロセスは、次のとおりです。

ステップ 1　ユーザは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　スイッチは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　スイッチは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　ユーザはポートから切断します。

ステップ 8　スイッチは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 ポートベースの認証を設定するには、イネーブル EXEC モードで次の手順を実行します。

	コマンド	説明
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。

	コマンド	説明
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。 **authentication** コマンドに名前付きリストが*指定されない*場合に使用される、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の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。 *method1* には、**group radius** キーワードを入力して、認証用のすべての RADIUS サーバのリストを使用します。 （注）　コマンドラインのヘルプ ストリングでは他のキーワードが表示されても、サポートされるのは **group radius** キーワードのみです。
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。
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。 （注）　ユーザ単位 ACL の場合は、単一ホスト モードを設定する必要があります。これはデフォルト設定です。
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）スイッチと RADIUS サーバ上で稼働する 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。
ステップ 8	**interface** *interface-id*	クライアントに接続されたポートの中で、IEEE 802.1x 認証をイネーブルにするものを指定し、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 とステップ 7 で RADIUS サーバを設定した場合は、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。 機能の相互作用の詳細については、「IEEE 802.1x 設定時の注意事項」（p.10-17）を参照してください。
ステップ 11	**end**	イネーブル 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。

スイッチと RADIUS サーバ間の通信を設定する方法

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、あるいは IP アドレスと特定の UDP ポート番号で識別します。IP アドレスと UDP ポート番号の組み合わせにより、一意の識別子が作成され、これにより、サーバ上の同一の IP アドレスの複数の UDP ポートに RADIUS 要求を送信できます。同一の RADIUS サーバ上の 2 つの異なるホスト エントリが同じサービス（たとえば、認証）を設定している場合、あとから設定されたホスト エントリは、最初のエントリのフェール オーバー バックアップとして機能します。RADIUS のホスト エントリは、設定された順序で試されます。

スイッチ上に RADIUS サーバ パラメータを設定するには、イネーブル 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	説明
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。 *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。 **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、指定できる範囲は 0 ～ 65536 です。 **key** *string* には、スイッチと RADIUS サーバ上で稼働する 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 サーバ上で使用する暗号鍵と一致する必要のある文字列です。 **（注）** 先行スペースは無視されますが、鍵の途中および末尾のスペースは使用されるため、鍵は必ず **radius-server host** コマンド構文の最後の項目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、鍵の一部として引用符を使用する場合を除いて、鍵を引用符で囲まないでください。この鍵は、RADIUS デーモン上で使用する暗号と一致する必要があります。 RADIUS サーバを複数使用する場合は、このコマンドを繰り返し入力してください。
ステップ 3	**end**	イネーブル 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。

次の例は、IP アドレスが 172.20.39.46 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 サーバ上の鍵と一致する *rad123* に設定します。

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

radius-server host グローバル コンフィギュレーション コマンドを使用すると、すべての RADIUS サーバに対してタイムアウト、再送信、および暗号鍵の値をグローバルに設定できます。サーバ単位でこれらのオプションを設定する場合は、**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 サーバに対する設定」（p.9-30）を参照してください。

さらに、RADIUS サーバでいくつかの設定を行う必要があります。これらの設定には、スイッチの IP アドレス、およびサーバとスイッチで共用するキー ストリングが含まれます。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。

RADIUS サーバによる IEEE 802.1x 認証の設定

Cisco IOS Release 12.2(25)SEC では、RADIUS サーバを使用して IEEE 802.1x 認証を設定することもできます。

RADIUS サーバを使用して IEEE 802.1x 認証を設定するには、イネーブル 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	説明
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。 内部 VLAN（ルーテッド ポート）、RSPAN VLAN、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 4	**dot1x reauthentication**	クライアントに対する定期的な再認証は、デフォルトではディセーブルになっていますが、これをイネーブルにします。
ステップ 5	**dot1x timeout reauth-period** {*seconds* | **server**}	再認証を試行する間隔（秒数）を設定します。 キーワードの意味は次のとおりです。 • *seconds* — 1 ～ 65535 の範囲で秒数を設定します。デフォルトは 3600 秒です。 • **server** — Session-Timeout RADIUS アトリビュート（Attribute[27]）の値として秒数を設定します。 定期的な再認証がイネーブルに設定されている場合のみ、このコマンドはスイッチの動作に影響します。
ステップ 6	**end**	イネーブル EXEC モードに戻ります。
ステップ 7	**show dot1x interface** *interface-id*	IEEE 802.1x 認証設定を確認します。
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。

次の例は、RADIUS サーバを使用して IEEE 802.1x を設定する方法を示しています。

```
Switch# configure terminal
Switch(config)# interface gigabitethernet2/0/1
Switch(config-if)# dot1x reauthentication
Switch(config-if)# dot1x timeout reauth-period server
```

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て、その発生間隔を指定できます。再認証をイネーブルにする間隔を指定しなかった場合は、再認証は 3600 秒ごとに行われます。

クライアントの定期的な再認証をイネーブルにして、再認証を試行する間隔（秒数）を設定するには、イネーブル 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	説明
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。

	コマンド	説明
ステップ 3	**dot1x reauthentication**	デフォルトではディセーブルに設定されている定期的な再認証をイネーブルにします。
ステップ 4	**dot1x timeout reauth-period** {*seconds* | **server**}	再認証を試行する間隔（秒数）を設定します。 キーワードの意味は次のとおりです。 • *seconds* — 1 ～ 65535 の範囲で秒数を設定します。デフォルトは 3600 秒です。 • **server** — Session-Timeout RADIUS アトリビュート（Attribute[27]）の値として秒数を設定します。スイッチで NAC レイヤ 2 IEEE 802.1x が使用されている場合は、このキーワードを使用できます。 定期的な再認証がイネーブルに設定されている場合のみ、このコマンドはスイッチの動作に影響します。
ステップ 5	**end**	イネーブル 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。デフォルトの再認証試行間隔（秒）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。

次の例では、定期的再認証をイネーブルにし、再認証を試行する間隔を 4000 秒に設定します。

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

ポートに接続されたクライアントの手動による再認証

dot1x re-authenticate interface *interface-id* イネーブル EXEC コマンドを使用すると、特定のポートに接続しているクライアントを手動でいつでも再認証できます。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場合は、「定期的な再認証の設定」（p.10-22）を参照してください。

次の例では、ポートに接続されているクライアントを手動で再認証する方法を示しています。

```
Switch# dot1x re-authenticate interface gigabitethernet2/0/1
```

待機時間の変更

スイッチがクライアントを認証できなかった場合は、スイッチは一定時間アイドル状態を続け、その後再試行します。**dot1x timeout quiet-period** インターフェイス コンフィギュレーション コマンドでアイドル時間を制御します。クライアントが無効なパスワードを提供したため、クライアントの認証失敗が起こる可能性があります。デフォルトより小さい数値を入力することで、ユーザに対する応答時間を短縮できます。

待機時間を変更するには、イネーブル 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	説明
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。

	コマンド	説明
ステップ 3	**dot1x timeout quiet-period** *seconds*	クライアントとの認証交換が失敗したあと、スイッチが待機ステートにある秒数を設定します。 指定できる範囲は 1 ～ 65535 秒で、デフォルトは 60 秒です。
ステップ 4	**end**	イネーブル 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。

デフォルトの待機時間に戻すには、**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。

次の例では、スイッチ上の待機時間を 30 秒に設定します。

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

スイッチとクライアント間の再送信時間の変更

クライアントは、スイッチからの EAP 要求 / アイデンティティ フレームに、EAP 応答 / アイデンティティ フレームで応答します。スイッチはこの応答を受信しなかった場合、一定時間（再送信時間）待機してから、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の変更は、信頼性のないリンクや、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など、異常な状況を調整する場合以外は行わないようにしてください。

スイッチがクライアントの通知を待機する時間を変更するには、イネーブル 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	説明
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*	スイッチがクライアントからの EAP 要求 / アイデンティティ フレームに対する応答を待ち、要求を再送信するまでの秒数を設定します。 指定できる範囲は 5 ～ 65535 秒で、デフォルトは 5 秒です。
ステップ 4	**end**	イネーブル EXEC モードに戻ります。
ステップ 5	**show dot1xinterface** *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。

デフォルトの再送信時間に戻すには、**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。

次の例では、スイッチがクライアントからの EAP 要求 / アイデンティティ フレームに対する応答を待ち、要求を再送信するまでの秒数を 60 秒に設定します。

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

スイッチとクライアント間のフレーム再送信回数の設定

スイッチとクライアント間の再送信時間の変更だけでなく、（応答を受信しなかった場合）認証プロセスを再開するまでに、スイッチがクライアントに EAP 要求 / アイデンティティ 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の変更は、信頼性のないリンクや、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など、異常な状況を調整する場合以外は行わないようにしてください。

スイッチとクライアント間のフレーム再送信回数を設定するには、イネーブル 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	説明
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、認証プロセスを再開するまでに EAP 要求 / アイデンティティ フレームをクライアントに送信する回数を設定します。指定できる範囲は 1 ～ 10 で、デフォルトは 2 です。
ステップ 4	**end**	イネーブル 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。

デフォルトの再送信回数に戻すには、**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。

次の例では、認証プロセスを再開するまでに、スイッチが EAP 要求 / アイデンティティ フレームを送信する回数を 5 に設定します。

```
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なるまでにスイッチが認証プロセスを再開する回数も変更できます。

（注）　このコマンドのデフォルト値の変更は、信頼性のないリンクや、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など、異常な状況を調整する場合以外は行わないようにしてください。

再認証回数を設定するには、イネーブル 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	説明
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。

	コマンド	説明
ステップ 3	**dot1x max-reauth-req** *count*	ポートが無許可ステートになるまで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、デフォルトは 2 です。
ステップ 4	**end**	イネーブル 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。

デフォルトの再認証回数に戻すには、**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。

次の例は、ポートが無許可ステートになるまでにスイッチが認証プロセスを再開する回数を 4 回に設定する方法を示します。

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

ホスト モードの設定

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 IEEE 802.1x 許可ポート上で、複数のホスト（クライアント）を許可するには、イネーブル 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	説明
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*	複数のホストを間接的に接続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 host-mode multi-host**	IEEE 802.1x 許可ポート上で、複数のホスト（クライアント）を許可します。 指定されたインターフェイスについて、**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ます。
ステップ 4	**end**	イネーブル 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。

ポート上の複数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。

次の例は、IEEE 802.1x をイネーブルにし、複数のホストを許可する方法を示します。

```
Switch(config)# interface gigabitethernet2/0/1
Switch(config-if)# dot1x port-control auto
Switch(config-if)# dot1x host-mode multi-host
```

ゲスト VLAN の設定

ゲスト VLAN を設定すると、サーバが EAP 要求 / アイデンティティ フレームへの応答を受信しなかった場合に、IEEE 802.1x 非対応のクライアントはゲスト VLAN に配置されます。IEEE 802.1x 対応だが、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は許可されません。スイッチは、単一ホスト モードまたは複数ホスト 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、イネーブル EXEC モードで次の手順を行います。この手順は任意です。

	コマンド	説明
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。サポートされているポート タイプについては、「IEEE 802.1x 設定時の注意事項」（p.10-17）を参照してください。
ステップ 3	**switchport mode access** または **switchport mode private-vlan host**	ポートをアクセス モードに設定します。 または 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。 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**	イネーブル 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 をディセーブル化し削除するには、**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。

次の例は、VLAN 2 を IEEE 802.1x ゲスト VLAN としてイネーブルにする方法を示します。

```
Switch(config)# interface gigabitethernet2/0/2
Switch(config-if)# dot1x guest-vlan 2
```

この例では、スイッチの待機時間を 3 に設定し、EAP 要求 / アイデンティティ フレームに対する応答を待ち、要求を再送信するまでの秒数を 15 に設定し、IEEE 802.1x ポートが DHCP クライアントに接続されている場合に VLAN 2 を IEEE 802.1x ゲスト VLAN としてイネーブルにする方法を示します。

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

dot1x guest-vlan supplicant グローバル コンフィギュレーション コマンドを使用すると、オプションのゲスト VLAN 動作をイネーブルにできます。これをイネーブルにすると、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の EAPOL パケット検出に関わらず、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す。

オプションのゲスト VLAN 動作をイネーブルにして、ゲスト VLAN を設定するには、イネーブル 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	説明
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	**dot1x guest-vlan supplicant**	スイッチ上でオプションのゲスト VLAN 動作をグローバルにイネーブルにします。
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。サポートされているポート タイプについては、「IEEE 802.1x 設定時の注意事項」（p.10-17）を参照してください。
ステップ 4	**switchport mode access** または **switchport mode private-vlan host**	ポートをアクセス モードに設定します。 または 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 5	**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 6	**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。 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 7	**end**	イネーブル EXEC モードに戻ります。
ステップ 8	**show dot1x 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。

オプションのゲスト VLAN 動作をディセーブルにするには、**no dot1x guest-vlan supplicant** グローバル コンフィギュレーション コマンドを使用します。ゲスト VLAN を削除するには、**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。ポートがゲスト VLAN 内で現行許可されている場合、ポートは無許可ステートに戻ります。

次に、オプションのゲスト VLAN 動作をイネーブルにし、VLAN 5 を IEEE 802.1x ゲスト VLAN として指定する例を示します。

```
Switch(config)# dot1x guest-vlan supplicant
Switch(config)# interface gigabitethernet2/0/1
Switch(config-if)# dot1x guest-vlan 5
```

制限付き VLAN の設定

スイッチ スタックまたはスイッチ上に制限付き VLAN を設定した場合、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と、IEEE 802.1x に準拠している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、イネーブル EXEC モードで次の手順を行います。この手順は任意です。

	コマンド	説明
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。サポートされているポート タイプについては、「IEEE 802.1x 設定時の注意事項」（p.10-17）を参照してください。

	コマンド	説明
ステップ 3	**switchport mode access** または **switchport mode private-vlan host**	ポートをアクセス モードに設定します。 または 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 VLAN を IEEE 802.1x 制限付き VLAN として指定します。指定できる範囲は 1 ～ 4094 です。 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**	イネーブル 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。

次の例は、*VLAN 2* を IEEE 802.1x 制限付き VLAN としてイネーブルにする方法を示します。

```
Switch(config)# interface gigabitethernet2/0/2
Switch(config-if)# dot1x auth-fail vlan 2
```

dot1x auth-fail max-attempts インターフェイス コンフィギュレーション コマンドを使用すると、ユーザが制限付き VLAN に割り当てられるまでに許可される認証試行の最大回数を設定できます。許可される認証試行回数の範囲は 1 ～ 3 で、デフォルトは 3 回です。

許可される認証試行の最大回数を設定するには、イネーブル 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	説明
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。サポートされているポート タイプについては、「IEEE 802.1x 設定時の注意事項」（p.10-17）を参照してください。
ステップ 3	**switchport mode access** または **switchport mode private-vlan host**	ポートをアクセス モードに設定します。 または 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 VLAN を IEEE 802.1x 制限付き VLAN として指定します。指定できる範囲は 1 ～ 4094 です。 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。

	コマンド	説明
ステップ 6	**dot1x auth-fail max-attempts** *max attempts*	ポートが制限付き VLAN に移動されるまでに許される認証試行の回数を指定します。指定できる範囲は 1 ～ 3 で、デフォルトは 3 です。
ステップ 7	**end**	イネーブル 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。

デフォルト値に戻すには、**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、ポートが制限付き VLAN に移されるまでに許可される認証試行の回数を *2* に設定する例を示します。

```
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

ポートをクリティカル ポートに設定し、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、イネーブル 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	説明
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。サポートされているポート タイプについては、「IEEE 802.1x 設定時の注意事項」（p.10-17）を参照してください。
ステップ 3	**dot1x critical**	アクセス不能認証バイパス機能をイネーブルにします。
ステップ 4	**end**	イネーブル EXEC モードに戻ります。
ステップ 5	**show dot1x [interface** *interface-id*]	（任意）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。

この機能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イネーブルにする例を示します。

```
Switch(config-if)# dot1x critical
```

IEEE 802.1x 設定をデフォルト値にリセットする方法

IEEE 802.1x 設定をデフォルト値にリセットするには、イネーブル 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	説明
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リセットします。
ステップ 4	**end**	イネーブル EXEC モードに戻ります。

	コマンド	説明
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 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、システムはロギングのためアカウンティング RADIUS サーバに送信するイベントをリロードできます。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 プロトコルを使用しているので、ネットワーク状態によりアカウンティング メッセージが失われる場合があります。設定した回数のアカウンティング要求の再送信を行ったあと、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、次のシステム メッセージが表示されます。

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

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、イネーブル 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	説明
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して）、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**	イネーブル 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** イネーブル 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
```

IEEE 802.1x 統計情報およびステータスの表示

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

スイッチについて IEEE 802.1x 管理および動作のステータスを表示するには、**show dot1x all** イネーブル EXEC コマンドを使用します。特定のポートの IEEE 802.1x 管理および動作のステータスを表示するには、**show dot1x interface** *interface-id* イネーブル EXEC コマンドを使用します。

表示されるフィールドの詳細については、このリリースのコマンド リファレンスを参照してください。