CHAPTER 8

IEEE 802.1x ポートベース認証の設定

この章では、Catalyst 3550 スイッチで IEEE（米国電気電子学会）802.1X ポートベース認証を設定して、不正なデバイス（クライアント）によるネットワークへのアクセスを防止する方法について説明します。

（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、このリリースのコマンド リファレンスおよび『*Cisco IOS Security Command Reference, Release 12.2*』の「RADIUS Commands」の項を参照してください。

この章の内容は、次のとおりです。

IEEE 802.1x ポートベース認証の概要

IEEE 802.1x 規格は、クライアント/サーバ ベースのアクセス コントロールと認証プロトコルについて規定しており、適切に認可されていない限り、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 に接続しないようにしています。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。

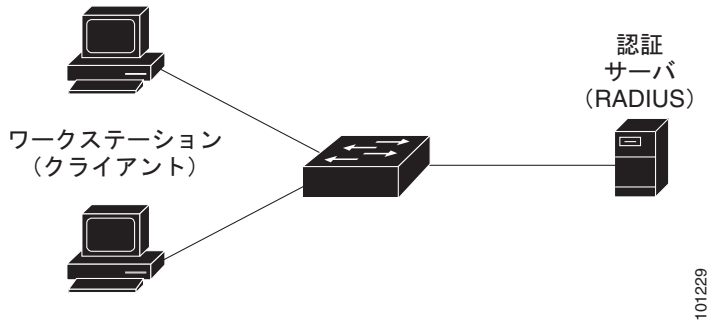
IEEE 802.1x アクセス コントロールでは、クライアントを認証するまでの間、そのクライアントが接続しているポート経由では Extensible Authentication Protocol over LAN（EAPOL）、Cisco Discovery Protocol（CDP）、およびスパニングツリー プロトコル（STP）トラフィックしか許可されません。認証に成功すると、通常のトラフィックはポートを通過できるようになります。

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、ネットワーク内のデバイスにそれぞれ固有の役割があります（図 8-1 を参照）。

図 8-1　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 システムで提供されるクライアントなど、IEEE 802.1x 準拠のクライアント ソフトウェアが稼働している必要があります（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 のネットワーク接続および IEEE 802.1x 認証の問題の解決方法については、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透過的に行われます。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、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デバイスは、Catalyst 3750、3560、3550、2970、2955、2950、2940 スイッチ、またはワイヤレス アクセス ポイントです。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。

認証の開始およびメッセージ交換

スイッチまたはクライアントのどちらからでも、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と、スイッチは、リンク ステートがダウンからアップに移行したときに認証を開始し、ポートがアップしていて認証されていない場合は定期的に認証を開始します。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。

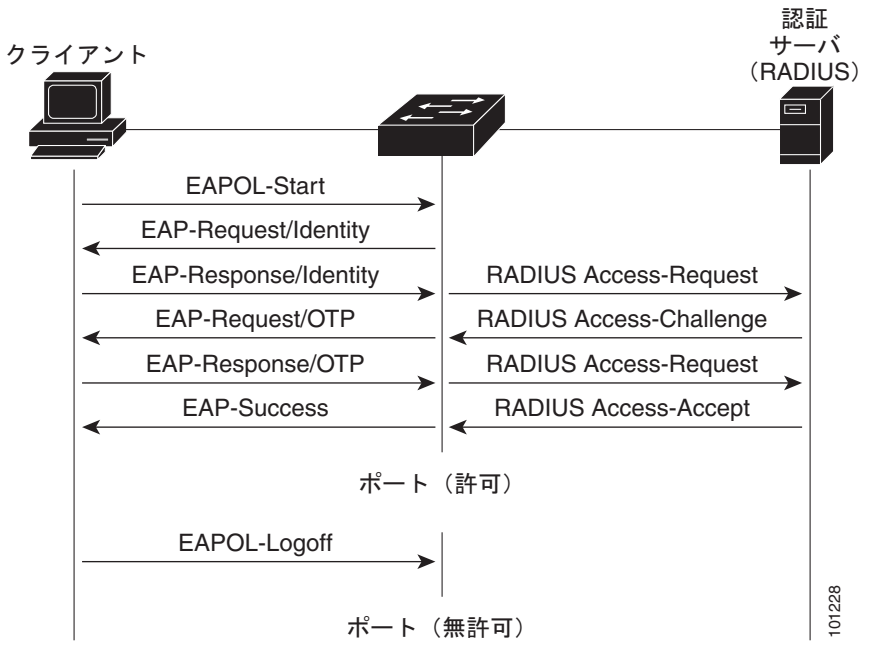
ただし、クライアントが起動時にスイッチからの EAP-Request/Identity フレームを受信しなかった場合、クライアントは EAPOL-Start フレームを送信して認証を開始できます。このフレームはスイッチに対し、クライアントの識別情報を要求するように指示します。

（注） ネットワーク アクセス デバイスで IEEE 802.1x がイネーブルになっていない、またはサポートされていない場合は、クライアントからの EAPOL フレームはドロップされます。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.8-4）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。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.8-4）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 8-2 に、クライアントが RADIUS サーバとの間でワンタイム パスワード（OTP）認証方式を使用する場合に行われるメッセージ交換を示します。

図 8-2　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、スイッチはネットワークへのクライアント アクセスを許可できます。ポートは最初、*無許可*ステートです。このステートにある間、音声 VLAN ポートとして設定されていないポートは、IEEE 802.1x、CDP、STP パケットを除くすべての入力トラフィックおよび出力トラフィックを許可しません。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 ポートとして設定されている場合、クライアントを正常に認証する前に、まず、このポートで VoIP トラフィックと IEEE 802.1x プロトコル パケットが許可されます。

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 ポートに接続する場合、スイッチはクライアントに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。

対照的に、IEEE 802.1x 対応クライアントが IEEE 802.1x 標準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-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。応答がないので、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移行させます。ポートはクライアントとの 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。スイッチはインターフェイス経由で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移行するか、または EAPOL-Start 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。ネットワークへのアクセスを試行する各クライアントは、クライアントの MAC アドレスを使用してスイッチにより一意に識別されます。

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全フレームがポート経由での送受信を許可されます。認証が失敗すると、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 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移行します。

ポートのリンク ステートがアップからダウンに移行した場合、または EAPOL ログオフ フレームを受信した場合、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、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トラッキングしません。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 アカウンティング属性値ペア

RADIUS サーバに送信された情報は、Attribute Value（AV; 属性値）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 属性の情報が必要です）。

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 8-1 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 8-1　アカウンティング AV ペア

属性番号	AV ペア名	START	INTERIM	STOP
属性 [1]	User-Name	常時送信	常時送信	常時送信
属性 [4]	NAS-IP-Address	常時送信	常時送信	常時送信
属性 [5]	NAS-Port	常時送信	常時送信	常時送信
属性 [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]
属性 [25]	クラス	常時送信	常時送信	常時送信
属性 [30]	Called-Station-ID	常時送信	常時送信	常時送信
属性 [31]	Calling-Station-ID	常時送信	常時送信	常時送信
属性 [40]	Acct-Status-Type	常時送信	常時送信	常時送信
属性 [41]	Acct-Delay-Time	常時送信	常時送信	常時送信
属性 [42]	Acct-Input-Octets	非送信	非送信	常時送信
属性 [43]	Acct-Output-Octets	非送信	非送信	常時送信
属性 [44]	Acct-Session-ID	常時送信	常時送信	常時送信
属性 [45]	Acct-Authentic	常時送信	常時送信	常時送信
属性 [46]	Acct-Session-Time	非送信	非送信	常時送信
属性 [49]	Acct-Terminate-Cause	非送信	非送信	常時送信
属性 [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 にある『*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 のホスト モード

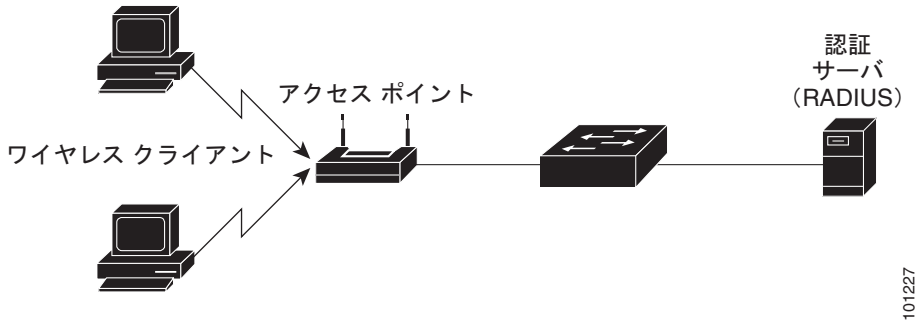
IEEE 802.1x ポートは、シングル ホスト モードまたはマルチホスト モードに設定できます。シングル ホスト モード（図 8-1（P.8-2）を参照）では、IEEE 802.1x 対応のスイッチ ポートに接続できるクライアントは 1 台だけです。スイッチは、ポートのリンク ステートがアップに変化したときに、EAPOL フレームを送信することでクライアントを検出します。クライアントがログオフしたとき、または別のクライアントに代わったときには、スイッチはポートのリンク ステートをダウンに変更し、ポートは無許可ステートに戻ります。

マルチホスト モードでは、1 つの IEEE 802.1x 対応ポートに複数のホストを接続できます。図 8-3（P.8-7）に、無線 LAN での 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 をポートの認証に使用し、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 8-3　　マルチホスト モードの例



ポート セキュリティを使用した IEEE 802.1x 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もあります)。ポートでポート セキュリティおよび IEEE 802.1x をイネーブルに設定すると、IEEE 802.1x 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または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でない場合、そのクライアントの 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がエージング アウトした場合に発生します。クライアントのアドレスがエージング アウトした場合、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。

  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.21-9）を参照してください。

- 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戻り、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。
- IEEE 802.1x クライアント 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する場合、**dot1x re-authenticate** 特権 EXEC コマンドを入力して、クライアントを再認証することをお勧めします。

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.21-7）を参照してください。

音声 VLAN ポートを使用した IEEE 802.1x 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。

シングル ホスト モードの音声 VLAN では、IP Phone だけが許可されます。マルチ ホスト モードでは、サプリカントが PVID で認証された後、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、いくつかの Cisco IP Phone が連続して接続されている場合、スイッチは直接接続している IP Phone だけを認識します。音声 VLAN ポートで IEEE 802.1x 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 からのパケットをドロップします。

IEEE 802.1x をポートでイネーブルにすると、音声 VLAN と同等であるポート VLAN を設定できません。

音声 VLAN の詳細については、第 13 章「音声 VLAN の設定」を参照してください。

VLAN 割り当てを使用した IEEE 802.1x の利用

VLAN 割り当てを使用して、特定のユーザによるネットワーク アクセスを制限できます。ポートの IEEE 802.1x 認証が成功すると、RADIUS サーバは VLAN 割り当てを送信し、スイッチ ポートを設定します。RADIUS サーバのデータベースは、ユーザ名 /VLAN マッピングを維持します。このマッピングでは、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。

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、認証が成功してからポートがアクセス VLAN に設定されます。
- IEEE 802.1x 認証がイネーブルだが、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 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 ポートへの VLAN の指定、誤った 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 への割り当ての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、ポートは認証のあとで指定した 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。
- 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）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 メンバーシップ ポリシー サーバ（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。

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。

- AAA 認証をイネーブルにします。
- IEEE 802.1x をイネーブルにする（VLAN 割り当て機能は、アクセス ポートに IEEE 802.1x を設定したときに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属性を割り当てます。RADIUS サーバは次の属性をスイッチに返す必要があります。
  - [64] Tunnel-Type = VLAN
  - [65] Tunnel-Medium-Type = IEEE 802
  - [81] Tunnel-Private-Group-ID = VLAN 名または VLAN ID

  属性 [64] は、値 *VLAN*（タイプ 13）でなければなりません。属性 [65] は、値 *IEEE 802*（タイプ 6）でなければなりません。属性 [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。

トンネル属性の例については、「ベンダー固有の RADIUS 属性を使用するスイッチ設定」（P.7-30）を参照してください。

ゲスト VLAN を使用した IEEE 802.1x 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。

認証サーバが EAPOL 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 よりも前のリリースでは、スイッチが EAPOL パケット履歴を保持していなかったため、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係なく、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、このオプションの動作をイネーブルにできます。

Cisco IOS Release 12.2(25)SE 以降では、スイッチは EAPOL パケット履歴を保持します。リンクの存続期間中に他の EAPOL パケットがインターフェイス上で検出された場合、ネットワーク アクセスは拒否されます。EAPOL 履歴は、リンクの消失時にリセットされます。

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。IEEE 802.1x 対応クライアントが、ゲスト VLAN を設定しているポートと同じポートに加入すると、そのポートはユーザ設定アクセス VLAN では無許可ステートに移行し、認証が再開されます。

ゲスト VLAN 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 ポート上でサポートされます。

RSPAN 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 の機能は、内部 VLAN（ルーテッド ポート）またはトランク ポート上ではサポートされません。サポートされるのはアクセス ポートだけです。

設定手順については、「ゲスト VLAN の設定」（P.8-22）を参照してください。

Wake-on-LAN を使用した IEEE 802.1x の利用

IEEE 802.1x 認証の Wake-on-LAN（WoL）機能を使用すると、*マジック パケット*と呼ばれる特定のイーサネット フレームの受信に基づいて、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。

IEEE 802.1x ポートを介して接続されたホストとともに WoL を使用する場合、ホストの電源がオフになると IEEE 802.1x ポートが無許可ポートになるという特有の問題が生じます。このステートでは、ポートは EAPOL パケットの受信と送信しか許可しないため、WoL マジック パケットはホストに到達できません。電源がオンにならなければ、コンピュータは認証されず、ポートは開かれません。

WoL 機能付きの IEEE 802.1x は、無許可の IEEE 802.1x ポートへのパケット送信を許可することで、この問題を解決します。この機能は、IEEE 802.1x 仕様では単一方向制御ポートとも呼ばれます。

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

単方向ステート

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ポートとして設定すると、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 がイネーブルになると、接続されたホストはスリープ モードまたは電源オフのステートになり、ホストはネットワーク上の他のデバイスを使用してトラフィックを交換しません。ホストがネットワークにトラフィックを送信できない単方向ポートに接続されている場合、ホストはネットワークの他の装置からのトラフィックだけを受信します。単一方向ポートが着信トラフィックを受信すると、ポートは双方向ステート（デフォルト）ステートに戻り、スパニングツリー ステートはブロッキング ステートに変わります。ポートが初期化ステートに変わると、EAPOL パケット以外のトラフィックは許可されなくなります。ポートが双方向ステートに戻ると、スイッチは 5 分間のタイマーを開始します。タイマーが期限切れになるまでに、ポートが認証されなければ、そのポートは単一方向ポートになります。

双方向ステート

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ポートとして設定すると、ポートは、両方向でアクセス コントロールされます。この場合、スイッチ ポートはパケットを送受信しません。

ユーザ単位 ACL を使用した IEEE 802.1x の利用

ユーザ単位のアクセス コントロール リスト（ACL）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 属性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、その属性を IEEE 802.1x ポートに適用します。セッションが終了すると、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 ACL 設定が削除されます。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。

スイッチ ポートでは、1 種類のユーザ単位 ACL のみを設定できます：ルータ ACL またはポート ACL。ルータ ACL は、レイヤ 3 インターフェイスに適用され、ポート ACL は、レイヤ 2 インターフェイスに適用されます。ポートがポート ベース ACL を使用して設定されている場合は、同じポートでルータ ベース ACL を設定する試みは拒否されます。ただし、ポートがルータ ベース ACL を使用して設定され、その後ポート ベース ACL を使用して設定されている場合、ポート ベース ACL はルータ ACL を上書きします。コンフィギュレーション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、ベンダー固有属性などのユーザ単位属性をサポートします。ベンダー固有属性（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、入力方向に限りサポートされます。

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コンフィギュレーションを定義します。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、Filter-Id 属性を使用する場合、標準 ACL を示すことができます。

Filter-Id 属性を使用して、すでにスイッチに設定されているインバウンドまたはアウトバウンド ACL を指定できます。属性には、ACL 番号と、その後ろに入力フィルタリングまたは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 属性は 1 ～ 199 および 1300 ～ 2699 の IP ACL（IP 標準 ACL および IP 拡張 ACL）に対してだけサポートされます。

1 ポートがサポートする IEEE 802.1x 認証ユーザは 1 ユーザだけです。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 属性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 ACSII 文字です。

ベンダー固有属性の例については、「ベンダー固有の RADIUS 属性を使用するスイッチ設定」（P.7-30）を参照してください。ACL の設定の詳細については、第 28 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、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する
- **network** キーワードを使用して AAA 認証をイネーブルにし、RADIUS サーバからインターフェイス設定を行えるようにする
- IEEE 802.1x をイネーブルにする
- RADIUS サーバにユーザ プロファイルと VSA を設定する
- シングルホスト モードの IEEE 802.1x ポートを設定する

IEEE 802.1x 認証の設定

ここでは、スイッチに IEEE 802.1x ポートベースの認証を設定する手順を説明します。

IEEE 802.1x のデフォルト設定

表 8-2 に、IEEE 802.1x のデフォルト設定を示します。

表 8-2　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
RADIUS サーバ • IP アドレス • UDP 認証ポート • キー	 • 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
インターフェイスごとの 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との 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。
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）

表 8-2　IEEE 802.1x のデフォルト設定 （続き）

機能	デフォルト設定
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後、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）
ホスト モード	シングル ホスト モード
ゲスト VLAN	指定なし
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。これは設定できません）。

IEEE 802.1x 設定時の注意事項

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 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、ポートが認証されます。
- 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、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、ネイバーとトランク 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 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に変更しようとしても、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：アクティブまたはアクティブでない EtherChannel メンバを 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 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(25)SE よりも前のソフトウェア リリースでは、まだアクティブになっていない EtherChannel のポートで IEEE 802.1x をイネーブルにしても、ポートは EtherChannel に加入しません。

  - スイッチド ポート アナライザ (SPAN) およびリモート SPAN（RSPAN）宛先ポート：SPAN 宛先、RSPAN 宛先、または RSPAN リフレクタ 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 宛先、RSPAN 宛先、または RSPAN リフレクタ ポートとしてポートを削除するまでは、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 をイネーブルにすることができます。

- RSPAN 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 の機能は、内部 VLAN（ルーテッド ポート）またはトランク ポート上ではサポートされません。サポートされるのはアクセス ポートだけです。
- IEEE 802.1x をポートでイネーブルにすると、音声 VLAN と同等であるポート VLAN を設定できません。
- VLAN 割り当て機能付きの IEEE 802.1x は、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。
- 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 をグローバルにイネーブルにする前に、IEEE 802.1x 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。
- EAP-Transparent LAN Service（TLS）および EAP-MD5 で IEEE 802.1x を認証する Cisco Access Control Server（ACS）アプリケーションが稼働するデバイスを使用し、スイッチが Cisco IOS Release 12.1(14)EA1 を実行している場合、デバイスが ACS バージョン 3.2.1 以降で稼働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 ポートのゲスト VLAN を設定した後、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。クライアント上の DHCP プロセスが時間切れとなり 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、スイッチ上の IEEE 802.1x 認証プロセスを再起動する設定を変更できます。IEEE 802.1x 認証プロセスの設定（IEEE 802.1x の待機時間およびスイッチ / クライアント間送信時間）を短くします。

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 12.1(14)EA1 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。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 コマンドになり、新しいコマンドが追加されました。

スイッチに IEEE 802.1x を設定してある場合、Cisco IOS Release 12.1(14)EA1 以降にアップグレードすると、コンフィギュレーション ファイルに新しいコマンドが含まれないため、IEEE 802.1x が機能しません。アップグレードの完了後に、必ず **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、IEEE 802.1x をグローバルにイネーブルにしてください。IEEE 802.1x が旧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、認証を設定しなおしてください。

IEEE 802.1x 認証のイネーブル化

IEEE 802.1x ポートベース認証をイネーブルにするには、認証、許可、アカウンティング（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 および VLAN 割り当てを行えるようにするには、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 ポートベースの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。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	**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。 **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。 *method1* には、**group radius** キーワードを入力して、すべての RADIUS サーバのリストが認証に使用されるようにします。 **（注）** 他のキーワードがコマンドラインのヘルプ ストリングに表示されますが、サポートされているのは **default** および **group radius** キーワードだけです。
ステップ 4	**dot1x system-auth-control**	スイッチで 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。 ユーザ単位 ACL を設定するには、シングルホスト モードをイネーブルにする必要があります。この設定は、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キーを指定します。
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	**swtichport 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**	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。 機能の相互作用については、「IEEE 802.1x 設定時の注意事項」（P.8-13）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**	入力内容を確認します。 表示された IEEE 802.1x Port Summary セクションの Status カラムを確認してください。*enabled* というステータスは、ポート制御値が、**auto** または **force-unauthorized** に設定されていることを意味します。
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。

AAA をディセーブルにするには、**no aaa new-model** グローバル コンフィギュレーション コマンドを使用します。IEEE 802.1x AAA 認証をディセーブルにするには、**no aaa authentication dot1x** {**default** | *list-name*} 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。IEEE 802.1x AAA 許可をディセーブルにするには、**no aaa authorization** 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。スイッチの IEEE 802.1x 認証をディセーブルにするには、**no dot1x system-auth-control** グローバル コンフィギュレーション コマンドを使用します。

次の例では、ポートの AAA と IEEE 802.1x をイネーブルにする方法を示します。

```
Switch# configure terminal
Switch(config)# aaa new-model
Switch(config)# aaa authentication dot1x default group radius
Switch(config)# dot1x system-auth-control
Switch(config)# interface fastethernet0/1
Switch(config-if)# switchport mode access
Switch(config-if)# dot1x port-control auto
Switch(config-if)# end
```

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 ポート番号で識別されます。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、同一 IP アドレスのサーバ上にある複数の 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*	スイッチ上で 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 です。 **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キーを指定します。キーは、RADIUS サーバで使用する暗号化キーに一致するテキスト ストリングでなければなりません。 **（注）** キー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、キーは必ず **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。キーにスペースを使用する場合は、引用符がキーの一部分である場合を除き、引用符でキーを囲まないでください。キーは RADIUS デーモンで使用する暗号に一致している必要があります。 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**	入力内容を確認します。
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、暗号キーを RADIUS サーバ上のキーと同じ *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
```

radius-server host グローバル コンフィギュレーション コマンドを使用して、タイムアウト、再送信回数、暗号化キーの値を、すべての RADIUS サーバにグローバルに設定できます。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.7-30）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。

RADIUS サーバを使用した IEEE 802.1x 認証の設定

Cisco IOS Release 12.2（25）SEC では、RADIUS サーバを使用した IEEE 802.1x 認証も設定できます。

IEEE 802.1x 認証を RADIUS サーバで設定するには、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。 RSPAN VLAN または音声 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**}	再認証の試行の間隔（秒）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**：セッションタイムアウト RADIUS 属性（属性 [27]）の値として秒数を設定します。 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。

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

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

定期的な再認証のイネーブル化

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。再認証の間隔を指定しなかった場合、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、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*	設定するインターフェイスを指定し、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**}	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**：セッションタイムアウト RADIUS 属性（属性 [27]）の値として秒数を設定します。スイッチが NAC レイヤ 2 IEEE 802.1x を使用する場合に、このキーワードを使用できます。 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*	入力内容を確認します。
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。再認証試行間隔をデフォルトの秒数に戻すには、**no dot1x timeout reauth-period** 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、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と、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、「定期的な再認証のイネーブル化」（P.8-18）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 fastethernet0/1
```

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、その後再び認証を試みます。このアイドル時間は、待機時間の値によって決定されます。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*	設定するインターフェイスを指定し、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。 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*	入力内容を確認します。
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、その後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下した場合や、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*	設定するインターフェイスを指定し、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	目的
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。 指定できる範囲は 15 ～ 65535 秒です。デフォルト値は 30 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*	入力内容を確認します。
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下した場合や、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*	設定するインターフェイスを指定し、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-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*	入力内容を確認します。
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下した場合や、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 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*	入力内容を確認します。
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。

次の例では、ポートが無許可ステートに移行する前に、スイッチが認証プロセスを再起動する回数を 4 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、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*	複数ホストが間接的に接続されているインターフェイスを指定し、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 許可ポートで複数のホスト（クライアント）の接続を許可します。 指定するインターフェイスでは、**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 4	**end**	特権 EXEC モードに戻ります。

	コマンド	目的
ステップ 5	**show dot1x interface** *interface-id*	入力内容を確認します。
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、ポートをイネーブルにし、複数のホストを許可する方法を示します。

```
Switch(config)# interface fastethernet0/1
Switch(config-if)# dot1x port-control auto
Switch(config-if)# dot1x host-mode multi-host
```

ゲスト VLAN の設定

サーバが EAPOL 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 対応のクライアントでも、認証できない場合は、ネットワークへのアクセスが認められません。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*	設定するインターフェイスを指定し、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。サポートされるインターフェイスのタイプについては、「IEEE 802.1x 設定時の注意事項」（P.8-13）を参照してください。
ステップ 3	**switchport mode access**	ポートをアクセス モードにします。
ステップ 4	**dot1x port-control auto**	ポートの 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、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 6	**end**	特権 EXEC モードに戻ります。
ステップ 7	**show dot1x interface** *interface-id*	入力内容を確認します。
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。

次の例では、ポート上で VLAN 9 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 fastethernet0/1
Switch(config-if)# dot1x guest-vlan 9
```

次の例では、スイッチの待機時間を 3 秒に設定し、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 15 に設定する方法、および IEEE 802.1x ポートが DHCP クライアントに接続されているときに 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 コマンドを使用して、オプションのゲスト VLAN の動作をイネーブルにできます。イネーブルにした場合、スイッチは EAPOL パケット履歴を保持せず、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係なく、認証に失敗したクライアントにもゲスト VLAN へのアクセスを許可します。

オプションのゲスト VLAN の動作をイネーブルにし、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	**dot1x guest-vlan supplicant**	スイッチでオプションのゲスト VLAN の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。サポートされるポートのタイプについては、「IEEE 802.1x 設定時の注意事項」（P.8-13）を参照してください。
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	**dot1x port-control auto**	ポートの 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、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 7	**end**	特権 EXEC モードに戻ります。
ステップ 8	**show dot1x interface** *interface-id*	入力内容を確認します。
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 の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。ポートは無許可ステートに戻ります。

次の例では、オプションのゲスト VLAN の動作をイネーブルにし、VLAN 5 を IEEE 802.1x ゲスト VLAN として指定する方法を示します。

```
Switch(config)# dot1x guest-vlan supplicant
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# dot1x guest-vlan 5
```

IEEE 802.1x 設定のデフォルト値へのリセット

IEEE 802.1x 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。

	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*	設定するインターフェイスを指定し、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 default**	設定可能な 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**	特権 EXEC モードに戻ります。
ステップ 5	**show dot1x interface** *interface-id*	入力内容を確認します。
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 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送信を行う手順と認証方式を記述したものです。

ソフトウェアは、リストの最初の方式を使用してユーザを認証します。この方式が応答しない場合、ソフトウェアは、方式リストの次の認証方式を選択します。このプロセスは、リスト内の認証方式による通信が成功するか、定義された方式をすべて試し終わるまで繰り返されます。このサイクルのいずれかの時点で認証が失敗した場合には、認証プロセスは中止され、その他の認証方式が試みられることはありません。

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 の認証、許可、およびアカウンティング 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* [*method2...*]	IEEE 802.1x 認証方式リストを作成します。 **authentication** コマンドにリストが*指定されていない*場合に使用するデフォルトのリストを作成するには、**default** キーワードの後ろにデフォルト状況で使用される方式を指定します。デフォルトの方式リストは、自動的にすべてのポートに適用されます。 次のキーワードのうち、少なくとも 1 つを指定します。 • **group radius**：すべての RADIUS サーバのリストを認証に使用します。 • **none**：認証を使用しません。クライアントは、クライアントが提供する情報を使用しないで、スイッチによって自動的に認証されます。
ステップ 4	**dot1x system-auth-control**	スイッチで 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 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。この設定は、デフォルトです。
ステップ 6	**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 7	**dot1x port-control auto**	ポートの IEEE 802.1x 認証をイネーブルにします。 機能の相互作用については、「IEEE 802.1x 設定時の注意事項」（P.8-13）を参照してください。
ステップ 8	**end**	特権 EXEC モードに戻ります。
ステップ 9	**show dot1x**	入力内容を確認します。
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。

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**	入力内容を確認します。
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。

次の例では、IEEE 802.1x アカウンティングを設定する方法を示します。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 の統計情報およびステータスの表示

すべてのインターフェイスに関する 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。特定のインターフェイスに関する 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。

スイッチの 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** 特権 EXEC コマンドを使用します。特定のインターフェイスに関する 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。