



IEEE 802.1X ポートベースの認証の設定

この章では、Catalyst 3550 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 認証により不正なデバイス（クライアント）がネットワークにアクセスすることを防止することができます。



(注)

この章で使用されるコマンドの構文および使用方法の詳細については、このリリースに対応するスイッチのコマンド リファレンス、および『*Cisco IOS Security Command Reference*』Release 12.2 の「RADIUS Commands」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 \(p.8-2\)](#)
- [IEEE 802.1X 認証の設定 \(p.8-19\)](#)
- [IEEE 802.1X 統計情報およびステータスの表示 \(p.8-40\)](#)

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かぎり、許可のない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 に接続するのを防ぎます。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) トラフィックだけが許可されます。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。

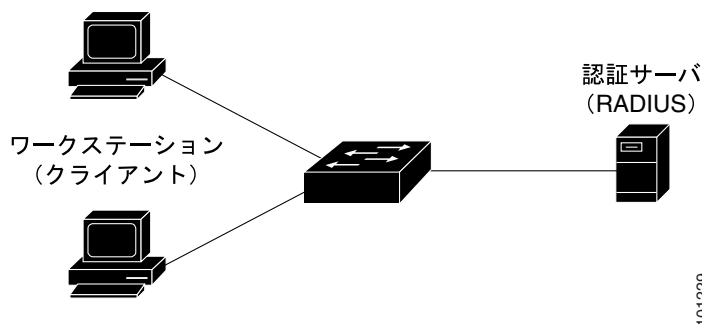
ここでは、IEEE 802.1X ポートベース認証について説明します。

- [デバイスの役割 \(p.8-2\)](#)
- [認証プロセス \(p.8-3\)](#)
- [認証の開始とメッセージ交換 \(p.8-5\)](#)
- [許可ステートおよび無許可ステートのポート \(p.8-7\)](#)
- [IEEE 802.1X ホスト モード \(p.8-8\)](#)
- [IEEE 802.1X アカウンティング \(p.8-8\)](#)
- [IEEE 802.1X アカウンティング AV のペア \(p.8-9\)](#)
- [IEEE 802.1X 認証と VLAN 割り当ての使用法 \(p.8-10\)](#)
- [IEEE 802.1X 認証とユーザ単位の ACL の使用法 \(p.8-11\)](#)
- [IEEE 802.1X 認証とゲスト VLAN の使用法 \(p.8-12\)](#)
- [IEEE 802.1X 認証と制限付き VLAN の使用法 \(p.8-13\)](#)
- [IEEE 802.1X 認証とアクセス不能認証バイパスの使用法 \(p.8-14\)](#)
- [IEEE 802.1X 認証と音声 VLAN ポートの使用法 \(p.8-15\)](#)
- [IEEE 802.1X 認証とポート セキュリティの使用法 \(p.8-15\)](#)
- [IEEE 802.1X 認証と Wake-on-LAN の使用法 \(p.8-16\)](#)
- [IEEE 802.1X 認証と MAC 認証バイパスの使用法 \(p.8-17\)](#)
- [NAC レイヤ 2 IEEE 802.1X 検証 \(p.8-18\)](#)

デバイスの役割

IEEE 802.1X ポートベース認証を使用すると、ネットワーク内のデバイスは [図 8-1](#) のような特定の役割が割り当てられます。

図 8-1 IEEE 802.1X デバイスの役割



101229

- **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は、Microsoft Windows XP 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 規格のサブリカントになりま
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 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** 実際には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、クライアントから 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。このリリースでは、認証サーバとして Extensible Authentication
Protocol (EAP) 拡張機能を備えた RADIUS セキュリティ システムのみサポートされています。
この認証サーバは、Cisco Secure Access Control Server バージョン 3.0 以降で使用可能です。
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
報を認証サーバで検証し、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およびカ
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されず、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。

媒介として機能するデバイスには、Catalyst 3750、Catalyst 3650、Catalyst 3550、Catalyst 2970、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 認証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。

認証プロセス

IEEE 802.1X ポートベース認証がイネーブルでクライアントが 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。

- クライアントの ID が有効で IEEE 802.1X 認証に成功した場合、スイッチがクライアントにネッ
トワーク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 (メディア アク
セス制御) 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
に使用できます。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、スイッチが
クライアントにネットワーク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、限定的なサービスを提供するゲスト VLAN が設定されていれば、スイ
ッチはクライアントにそのゲスト VLAN (仮想 LAN) 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、限定的なサービスを提供す
る制限付き VLAN が指定されている場合、スイッチはクライアントにその制限付き VLAN を
割り当てることができます。

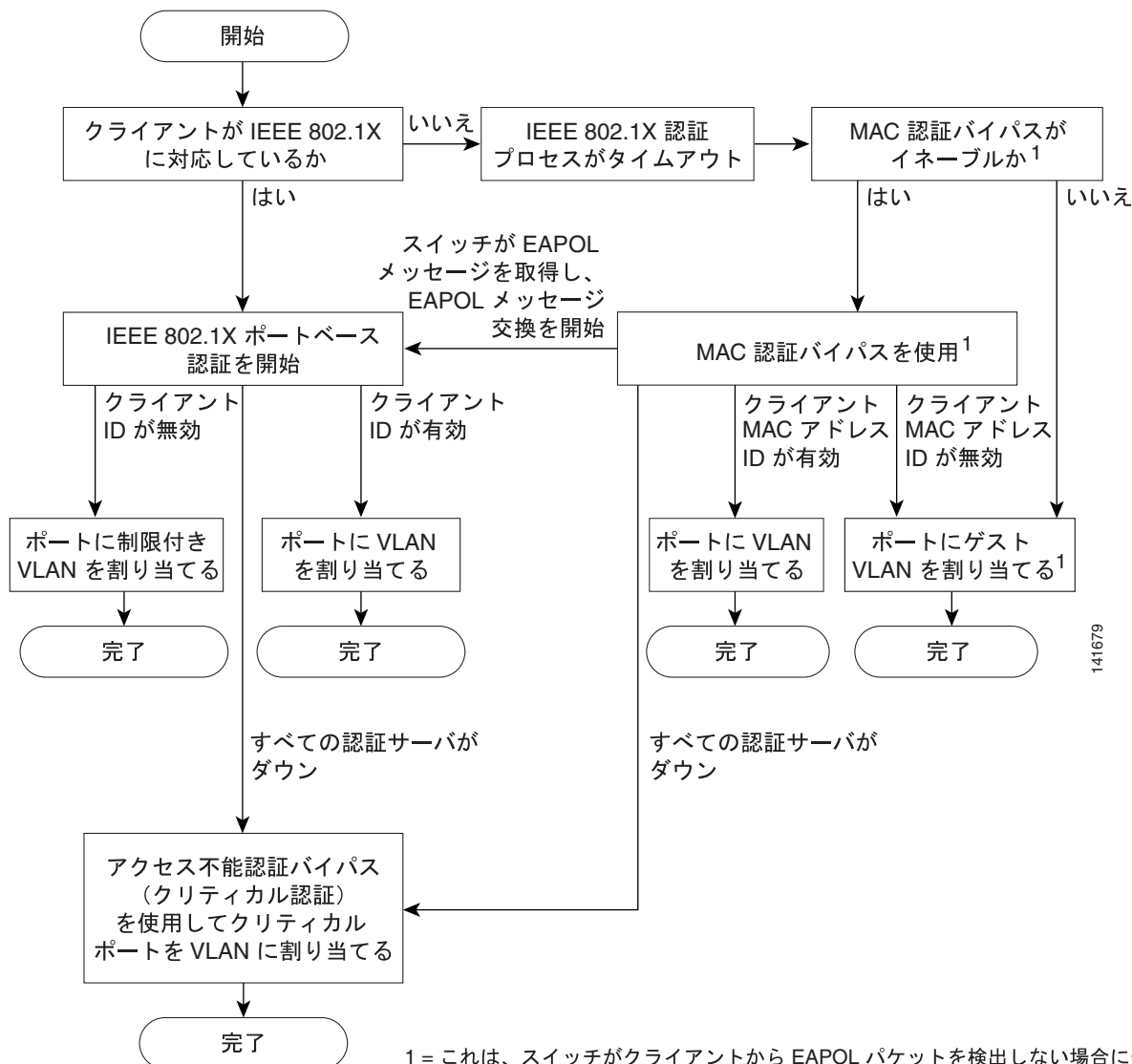
- RADIUS 認証サーバが使用できず（ダウンしていても）アクセス不能認証バイパスがイネーブルの場合、スイッチは、RADIUS 設定またはユーザ指定のアクセス VLAN にあるポートをクリティカル認証ステートにして、クライアントにネットワークのアクセスを許可します。



(注) アクセス不能認証バイパスは、クリティカル認証、または Authentication, Authorization, Accounting (AAA; 認証、許可、アカウントिंग) 失敗ポリシーとも呼ばれます。

図 8-2 に認証プロセスを示します。

図 8-2 認証フローチャート



スイッチは、次の状況のいずれかが発生した場合、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た場合。
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 サーバを使用して IEEE 802.1X 認証を設定したら、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、再認証を開始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、初期化または再認証に設定できます。初期化アクションが設定されると (アトリビュート値は *DEFAULT*) IEEE 802.1X セッションが終了し、再認証中に接続が切れます。再認証アクションが設定されると (アトリビュート値は RADIUS-Request)、再認証中にセッションは影響を受けません。
- `dot1x re-authenticate interface interface-id` イネーブル EXEC コマンドを入力することで、手動でクライアントを再認証できます。

認証の開始とメッセージ交換

IEEE 802.1X 認証中に、スイッチまたはクライアントが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移行したか、または定期的にポートがアップで未認証状態の間に、認証を開始します。スイッチは 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してアイデンティティを要求します。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。



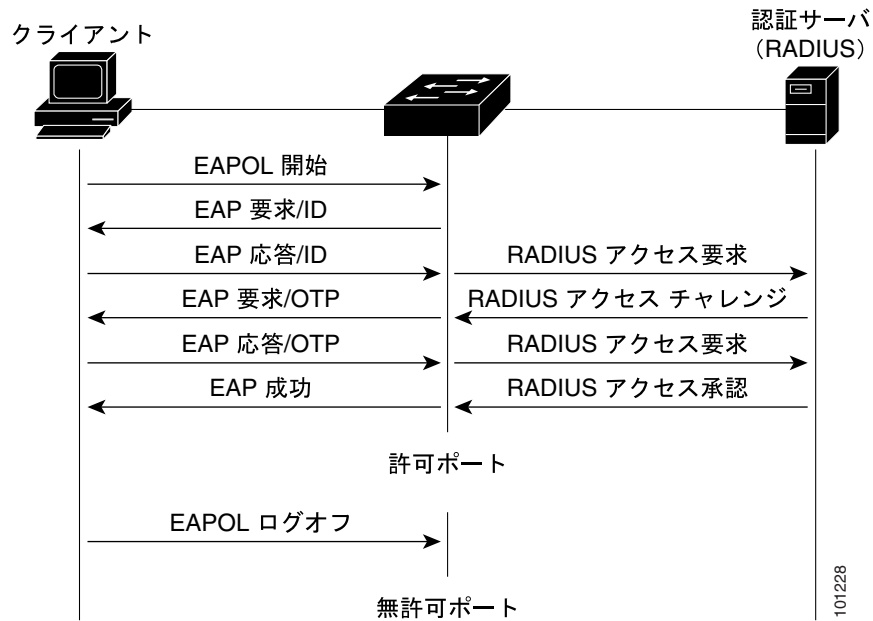
(注)

ネットワーク アクセス デバイスで IEEE 802.1X 認証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.8-7) 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。認証に失敗した場合、認証が再試行されるか、ポートは限定的なサービスを提供する VLAN に割り当てられるか、ネットワークアクセスが許可されません。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.8-7) 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 8-3 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。

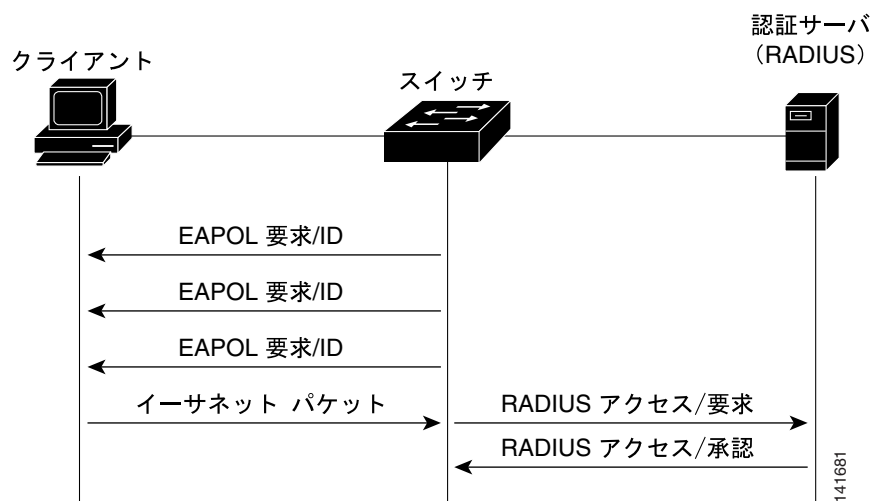
図 8-3 メッセージ交換



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のイーサネットパケットを検出すると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、この情報を RADIUS サーバに送信される RADIUS アクセス / 要求フレームに含めます。サーバがスイッチに RADIUS アクセス / 承認フレームを送信し（認証が成功し）、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 認証を使用して認証を開始します。

図 8-4 に、MAC 認証バイパス中のメッセージ交換を示します。

図 8-4 MAC 認証バイパス中のメッセージ交換



許可状態および無許可状態のポート

IEEE 802.1X 認証中は、スイッチ ポートの状態によって、スイッチがクライアントにネットワークのアクセスを許可します。ポートは、*無許可状態*で開始します。この状態にある間は、音声 VLAN ポートに設定されていないポートは、IEEE 802.1X 認証、CDP、および STP パケットを除いてすべての入力トラフィックおよび出力トラフィックが許可されていません。クライアントが正常に認証されると、ポートは*許可状態*に移行し、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 ポートに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 認証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、ポートは無許可状態のまま、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状態にあるものとしてフレームの送信を開始します。

ポートの許可状態を制御するには、`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状態に移行させます。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** ポートは無許可状態のままにし、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、インターフェイス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、ポートを無許可状態で開始させ、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移行するか、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 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（認証サーバから承認フレームを受信すると）、ポートが許可状態に変わり、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、ポートは無許可状態のままですが、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状態に移行します。

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は、ポートは無許可状態に戻ります。

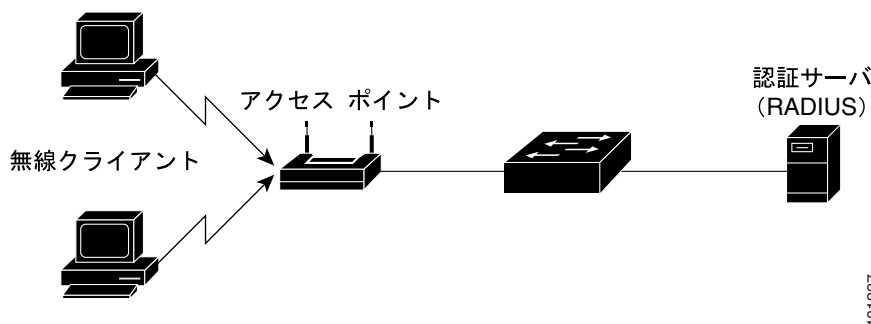
IEEE 802.1X ホスト モード

IEEE 802.1X ポートをシングル 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。クライアントが切断するか、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。

複数のホスト モードでは、複数のホストを単一 IEEE 802.1X 対応ポートに接続できます。図 8-5 (p.8-8) に、無線 LAN での 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。

複数のホスト モードがイネーブルの場合、IEEE 802.1X 認証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 8-5 複数のホスト モードの例



IEEE 802.1X アカウンティング

IEEE 802.1X 規格には、ネットワーク アクセスに対するユーザの許可と認証方法は定義されていますが、ネットワークの使用方法を監視するものではありません。IEEE 802.1X アカウンティングは、デフォルトでディセーブルに設定されています。IEEE 802.1X アカウンティングをイネーブルにして、IEEE 802.1X 対応ポートで次の内容をモニタできます。

- 正常なユーザ認証
- ユーザのログ オフ
- リンク ダウンの発生
- 正常な再認証の発生
- 再認証の失敗

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。その代わりに、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 AV のペア

RADIUS サーバに送信される情報は、Attribute-Value (AV) のペア形式で表示されます。AV ペアは異なる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は RADIUS パケットの Acct-Input-Octets または Acct-Output-Octets 属性にある情報を必要とする場合があります)。

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。次の 3 タイプの 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 セッションの開始時に送信されます。
- INTERIM セッションの継続中に更新用に送信されます。
- STOP セッション終了時に送信されます。

表 8-1 に、スイッチによって送信されたときの AV ペアを示します。

表 8-1 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	有効	有効	有効
アトリビュート [4]	NAS-IP-Address	有効	有効	有効
アトリビュート [5]	NAS-Port	有効	有効	有効
アトリビュート [8]	Framed-IP-Address	無効	以下の条件でのみ有効 ¹	以下の条件でのみ有効 ¹
アトリビュート [25]	Class	有効	有効	有効
アトリビュート [30]	Called-Station-ID	有効	有効	有効
アトリビュート [31]	Calling-Station-ID	有効	有効	有効
アトリビュート [40]	Acct-Status-Type	有効	有効	有効
アトリビュート [41]	Acct-Delay-Time	有効	有効	有効
アトリビュート [42]	Acct-Input-Octets	無効	無効	有効
アトリビュート [43]	Acct-Output-Octets	無効	無効	有効
アトリビュート [44]	Acct-Session-ID	有効	有効	有効
アトリビュート [45]	Acct-Authentic	有効	有効	有効
アトリビュート [46]	Acct-Session-Time	無効	無効	有効
アトリビュート [49]	Acct-Terminate-Cause	無効	無効	有効
アトリビュート [61]	NAS-Port-Type	有効	有効	有効

1. Framed-IP-Address の AV ペアは、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 テーブルのホストに存在する場合にのみ、送信されます。

`debug radius accounting` イネーブル EXEC コマンドを入力すると、スイッチによって送信される AV ペアを表示できます。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^F *IEEE 802.1X Remote Authentication Dial In User Service (RADIUS) Usage Guidelines* を参照してください。

IEEE 802.1X 認証と VLAN 割り当ての使用法

VLAN 割り当てを使用して、特定のユーザのネットワーク アクセスを制限できます。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、スイッチ ポートに接続されたクライアントのユーザ名に基づく VLAN を割り当てる、ユーザ名と VLAN のマッピングを維持します。

スイッチと RADIUS サーバを設定する際、IEEE 802.1X 認証と 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、ポートは認証が成功したあとにアクセス VLAN に設定されます。
- IEEE 802.1X 認証がイネーブルの場合でも、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 に保持されます。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止します。

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、存在しないかまたは内部(ルーテッド ポート)の VLAN ID、音声 VLAN ID への割り当て試行、などがあります。

- IEEE 802.1X 認証がイネーブルで RADIUS サーバからのすべての情報が有効の場合、ポートは認証後指定した VLAN に配置されます。
- IEEE 802.1X ポート上で複数のホスト 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して同じ VLAN (RADIUS サーバで指定された) 内に配置されます。
- IEEE 802.1X 認証およびポート セキュリティがポートでイネーブルの場合、ポートは RADIUS サーバで割り当てられた 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、強制無許可、無許可、またはシャットダウン ステートの場合は、設定済みのアクセス VLAN に配置されます。

IEEE 802.1X ポートが許可されて、RADIUS サーバで割り当てられた VLAN に配置される場合、ポート アクセス VLAN の設定変更は無効になります。

VLAN 割り当て機能を備えた IEEE 802.1X 認証は、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) を介したダイナミック アクセス ポートの割り当てではサポートされません。

VLAN 割り当てを設定するには、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。
- IEEE 802.1X 認証をイネーブルにします (アクセス ポートに 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 = IEEE 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 *IEEE 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.7-31) を参照してください。

IEEE 802.1X 認証とユーザ単位の 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なります。RADIUS サーバが IEEE 802.1X ポートに接続しているユーザを認証する場合、ユーザ ID に基づく ACL アトリビュートを取得し、スイッチに送信します。スイッチは、ユーザセッションの間このアトリビュートを IEEE 802.1X ポートに適用します。認証失敗、またはリンクダウン状態が発生した場合は、スイッチがセッション終了時にユーザ単位の ACL 設定を削除します。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。ポートが許可されない場合、スイッチはポートから ACL を削除します。

スイッチポートには、ユーザ単位の ACL を 1 タイプだけ設定できます。ルータ ACL またはポート ACL です。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。あるポートがポートベース ACL に設定されている場合、同じポートのルータベース ACL を設定しようとするとスイッチがこれを拒否します。ただし、あるポートがルータベース ACL に設定されていて、そのあとでポートベース ACL に設定される場合、ルータ ACL はポートベース ACL によって上書きされます。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) などのユーザ単位のアトリビュートをサポートします。これらの 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。ユーザ単位の 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、入力方向のみサポートされます。

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。サポートされるスイッチの Cisco IOS アクセスリストは制限されているため、フィルタ ID アトリビュートは、IP ACL 番号 1 ~ 199 および 1300 ~ 2699 でしかサポートされません (IP 標準および IP 拡張 ACL)。

1 つの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、ユーザ単位の ACL アトリビュートは関連ポートでディセーブルです。

ユーザ単位の ACL の最大サイズは、4000 ACSII 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.7-31) を参照してください。ACL 設定の詳細については、[第 29 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、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 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。
- IEEE 802.1X ポートを 1 つのホストモードに設定します。

IEEE 802.1X 認証とゲスト VLAN の使用方法

スイッチの各 IEEE 802.1X ポートにゲスト VLAN を設定することにより、クライアントに制限付きの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)。このようなクライアントは、IEEE 802.1X 認証用にシステムをアップグレードする場合があります。また、Windows 98 システムなど、IEEE 802.1X に対応していないホストもあります。

IEEE 802.1X ポートでゲスト VLAN がイネーブルの場合、スイッチが EAP 要求 /ID フレームへの応答を受信しない場合、または EAPOL パケットをクライアントが送信しない場合に、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 より前では、スイッチは EAPOL パケット履歴を保持せず、EAPOL パケットがインターフェイスで検出されていたかどうかにかかわらず、認証に失敗したクライアントにゲスト VLAN のアクセス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 コマンドを使用して、このオプションの動作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なくなりました。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 コマンドを入力することで、制限付き VLAN を使用して認証に失敗したクライアントにネットワーク アクセスを許可できます。

Cisco IOS Release 12.2(25)SE 以降、スイッチは EAPOL パケット履歴を保持するようになりました。リンクの存続中にインターフェイスで EAPOL パケットを検出すると、スイッチはそのインターフェイスに接続しているデバイスが 802.1X 対応のサブリカントで、インターフェイスがゲスト VLAN ステートに変更されないことを判断します。EAPOL 履歴は、インターフェイスリンク ステータスがダウンする場合にクリアされます。EAPOL パケットがインターフェイスで検出されない場合、インターフェイスはゲスト VLAN ステートに変更されます。



(注)

インターフェイスがゲスト VLAN に変更されたあとに EAPOL パケットが回線上で検出される場合、インターフェイスは無許可ステートに戻って、802.1X 認証が再開されます。

スイッチ ポートがゲスト VLAN に移行すると、アクセスを許可される IEEE 802.1X 非対応クライアント数に制限がなくなります。IEEE 802.1X 対応のクライアントが、ゲスト VLAN が設定されているのと同じポートに加入した場合、ポートはユーザ設定のアクセス VLAN で無許可ステートになり、認証が再開されます。

ゲスト VLAN は、IEEE 802.1X ポートでシングル ホスト モードおよびマルチ ホスト モードでサポートされます。

Remote SPAN (RSPAN) VLAN または音声 VLAN 以外であれば、いずれのアクティブな VLAN も、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ません。アクセス ポートでのみサポートされません。

スイッチでは、MAC authentication bypass キーワードは、Cisco IOS Release 12.2(25)SEE 以降でのみサポートされます。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、EAPOL メッセージ交換を待機している間に IEEE 802.1X 認証がタイムアウトした場合、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のイーサネット パケットを待ちます。スイッチは、認証サーバに MAC アドレスに基づくユーザ名とパスワードと共に RADIUS アクセス / 要求フレームを送信します。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、その VLAN にポートを割り当てます。詳細については、「IEEE 802.1X 認証と MAC 認証バイパスの使用方法」(p.8-17)を参照してください。

設定手順の詳細については、「ゲスト VLAN の設定」(p.8-31)を参照してください。

IEEE 802.1X 認証と制限付き VLAN の使用方法

スイッチの各 IEEE 802.1X ポートに制限付き VLAN を設定することにより、ゲスト VLAN にアクセスできないクライアントに制限付きのサービスを提供できます。これらのクライアントは IEEE 802.1X 準拠で、認証プロセスに失敗しているため別の VLAN にはアクセスできません。制限付き VLAN により、認証サーバに有効な証明書のないユーザ（通常は企業の訪問者）が制限付きのサービスにアクセスできます。管理者は、制限付き VLAN で利用できるサービスを制御できます。



(注)

ゲスト VLAN と制限付き VLAN のユーザに同じサービスを提供したい場合に、VLAN を両方のタイプに設定することができます。

この機能がないと、クライアントはいつまでも認証の試行と失敗を繰り返して、スイッチポートがスパンニングツリー ブロック ステートのままになります。この機能を使用すると、指定した数の認証試行（デフォルト値は 3 回）の後に、スイッチポートを制限付き VLAN に設定することができます。

認証者は、クライアントの認証試行失敗カウントを保持しています。このカウントが設定した最大認証試行数を超過すると、ポートが制限付き VLAN に移行します。失敗試行カウントは、RADIUS が EAP 失敗または EAP パケットを含まない空の応答で応答すると増加します。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、次の再認証試行が行われるまで制限付き VLAN 内に残ります。制限付き VLAN 内のポートは、指定した間隔（デフォルトでは 60 秒）で再認証を試行します。再認証に失敗すると、ポートは制限付き VLAN のままになります。再認証に成功すると、ポートは設定された VLAN または RADIUS サーバによって送信される VLAN のいずれかに移行します。再認証をディセーブルにできます。ディセーブルにする場合、認証プロセスを再び行う唯一の方法は、ポートがリンクダウンまたは EAP ログオフイベントを受信することです。クライアントがハブを介して接続している場合は、再認証をイネーブルのまま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断されると、ポートはリンクダウンまたは EAP ログオフイベントを受信しない場合があります。

ポートが制限付き VLAN に移行したあと、シミュレーションされた EAP 成功メッセージをクライアントに送信します。これにより、クライアントは認証を何回も試行する必要がなくなります。クライアントによっては（たとえば Windows XP を実行しているデバイス）、EAP の成功がない DHCP を実装できません。

制限付き VLAN は、シングル ホスト モードの IEEE 802.1X ポートまたはレイヤ 2 ポートでサポートされます。

RSPAN VLAN または音声 VLAN 以外であればいずれのアクティブな VLAN も、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、トランクポートではサポートされません。アクセスポート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、ポートセキュリティに MAC アドレスが提供されます。ポートセキュリティが MAC アドレスを許可しない場合、または最大セキュア アドレス カウントに達した場合、ポートは無許可になり、エラー ディセーブル ステートになります。

ダイナミック ARP 検査、DHCP スヌーピング、IP ソース ガードなどの他のポートセキュリティ機能を、制限付き VLAN に個別に設定することができます。

詳細については、「[制限付き VLAN の設定](#)」(p.8-32) を参照してください。

IEEE 802.1X 認証とアクセス不能認証バイパスの使用方法

Cisco IOS Release 12.2(25)SEE 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を認証できない場合、クリティカルポートに接続するホストへのネットワーク アクセスを許可するように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)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ているホストの認証を試行するたびに設定されている RADIUS サーバのステータスをチェックします。サーバが利用可能な場合、スイッチはホストを認証できます。ただし、すべての RADIUS サーバが利用できない場合、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、ポートをクリティカル認証ステートにします。これは、認証ステートの特殊なケースです。

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って左右されます。

- 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 設定によるアクセス 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。
- ポートがすでに許可されていて再認証が発生した場合、スイッチは現在の VLAN 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。この VLAN は、以前に RADIUS サーバによって割り当てられている場合があります。
- 認証交換中に RADIUS サーバが使用できなくなる場合、現在の交換がタイムアウトになり、次の認証試行の間スイッチが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。

ホストを認証できる RADIUS サーバが使用可能な場合は、クリティカル認証ステートになっている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作用します。
 - 少なくとも 1 つの RADIUS サーバが使用できる場合、スイッチが EAP 要求 /ID フレームへの応答を受信しないときまたは EAPOL パケットをクライアントが送信しないときに、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 設定によるアクセス 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に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にクライアントがクリティカルポートに接続されていて、そのクライアントが以前ゲスト VLAN に割り当てられていた場合、スイッチはそのポートをゲスト VLAN にとどめます。

- 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には影響しません。
- プライベート VLAN プライベート VLAN ホスト ポート上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 プライベート 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 設定によるアクセス VLAN またはユーザ指定のアクセス VLAN は音声 VLAN と別々にする必要があります。
- Remote Switched Port Analyzer (RSPAN; リモート スイッチド ポート アナライザ) RSPAN VLAN をアクセス不能認証バイパスの RADIUS 設定またはユーザ指定アクセス VLAN として指定しないでください。

IEEE 802.1X 認証と音声 VLAN ポートの使用方法

音声 VLAN ポートは、2 つの VLAN 識別子に関連付けられた特別なアクセス ポートです。

- IP Phone 間の音声トラフィックを搬送する Voice VLAN Identifier (VVID)。VVID は、ポートに接続している IP phone の設定に使用されます。
- 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間のデータトラフィックを搬送する Port VLAN Identifier (PVID)。PVID は、ポートのネイティブ VLAN です。

シングルホスト モードでは、IP Phone のみが音声 VLAN で許可されます。複数のホスト モードでは、要求元が PVID で認証されたあとに追加のクライアントが音声 VLAN にトラフィックを送信できます。複数のホスト モードがイネーブルの場合、要求元認証は、PVID および VVID の両方に影響します。

リンクがあると音声 VLAN ポートはアクティブになり、IP Phone からの最初の CDP メッセージのあとにデバイス MAC アドレスが表示されます。Cisco IP Phone は、ほかのデバイスからの CDP メッセージを転送しません。その結果、複数の Cisco IP Phone が連続して接続されている場合は、スイッチは直接接続されている Cisco IP Phone のみを認識します。IEEE 802.1X 認証が音声 VLAN ポート上でイネーブルの場合、スイッチは 2 ホップ以上離れて認識されない Cisco IP Phone からのパケットを廃棄します。

IEEE 802.1X 認証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。

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。

IEEE 802.1X 認証とポート セキュリティの使用方法

シングルホスト モードでもマルチホスト モードでも、IEEE 802.1X ポートでポート 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しなければなりません)。ポート上でポート セキュリティおよび IEEE 802.1X がイネーブルの場合、IEEE 802.1X 認証がポートを認証し、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 アドレスへのネットワーク 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 認証とポート 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、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。

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.22-10)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 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 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、ポートが未認証ステートに移行し、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、ポートは未認証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。
- IEEE 802.1X ポートでは、シングル ホスト モードでもマルチ ホスト モードでも、ポート セキュリティおよび音声 VLAN を同時に設定できます。ポート セキュリティは、VVID および PVID の両方に適用されます。

スイッチのポート セキュリティのイネーブル化については、「[ポート セキュリティの設定](#)」(p.22-9)を参照してください。

IEEE 802.1X 認証と Wake-on-LAN の使用方法

IEEE 802.1X の Wake-on-LAN (WoL) 機能を使用することにより、スイッチが *Magic Packet* と呼ばれる特定のイーサネット フレームを受信すると、休止状態の PC を起動できます。この機能は、管理者が電源が切られたシステムに接続する必要がある環境で使用できます。この機能は IEEE 802.1X 規格の *単一方向制御ポート*とも呼ばれます。

WoL を使用するホストが IEEE 802.1X ポートを通じて接続されていてホストの電源がオフになると、IEEE 802.1X ポートが無許可になります。ポートは、EAPOL パケットのみを送受信でき、WoL Magic Packet はホストに到達しません。PC の電源がオフになると、これは許可されず、スイッチポートが開きません。

スイッチが IEEE 802.1X 認証と WoL を併用する場合、スイッチはトラフィックを Magic Packet を含めて無許可 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の他のデバイスに送信できません。



(注) PortFast がポート上でイネーブルでない場合、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方向ポートとして設定する場合、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。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ポートとして設定する場合、ポートは両方向でアクセス制御されます。ポートは、ホストとの間でパケットの送受信を行いません。

IEEE 802.1X 認証と MAC 認証バイパスの使用方法

MAC 認証バイパス機能を使用してクライアント MAC アドレス (図 8-2 [p.8-4] を参照) に基づいてクライアントを認証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認証しようとします。

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のイーサネット パケットを待ちます。スイッチは、認証サーバに MAC アドレスに基づくユーザ名とパスワードと共に RADIUS アクセス / 要求フレームを送信します。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 が設定されていれば、スイッチはこの VLAN にポートを割り当てます。

リンクの存続中にインターフェイスで EAPOL パケットを検出すると、スイッチはそのインターフェイスに接続しているデバイスが IEEE 802.1X 対応のサブリカントで、(MAC 認証バイパスではなく) IEEE 802.1X 認証を使用してインターフェイスを許可していることを判断します。EAPOL 履歴は、インターフェイス リンク ステータスがダウンするとクリアされます。

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ていて IEEE 802.1X サブリカントを検出している場合、スイッチはそのポートに接続されているクライアントを無許可にしません。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は、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は、再認証できます。再認証プロセスは、IEEE 802.1X 認証を使用して認証されたクライアントのプロセスと同じです。再認証中に、ポートは前に割り当てられた VLAN に残ります。再認証に成功すると、ポートは同じ VLAN に保持されます。再認証に失敗した場合、ゲスト VLAN が設定されていれば、スイッチはその VLAN にポートを割り当てます。

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]) に基づいていて、Termination-Action RADIUS アトリビュート (アトリビュート [29]) アクションが初期化の場合 (アトリビュート値が DEFAULT)、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イネーブルで 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。これらの 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 クライアントに無効な MAC アドレス ID がある場合、ゲスト VLAN が設定されていれば、スイッチはこの 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 「IEEE 802.1X 認証とポート セキュリティの使用法」(p.8-15) を参照してください。
- 音声 VLAN 「IEEE 802.1X 認証と音声 VLAN ポートの使用法」(p.8-15) を参照してください。
- VMPS 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 に割り当てることができます。
- Network Admission Control (NAC; ネットワーク アドミッション制御) 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たあとに有効になります。

NAC レイヤ 2 IEEE 802.1X 検証

Cisco IOS Release 12.2(25) に 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条件やポスチャをチェックします。NAC レイヤ 2 IEEE 802.1X 検証を使用すると、以下の作業ができます。

- 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できます。
- 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の間隔を秒数で設定し、RADIUS サーバからクライアントに対するアクセス 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の再認証を試行する際のアクションを設定します。値が *DEFAULT* であるか、あるいは設定されていない場合、セッションが終了します。値が RADIUS 要求の場合、再認証プロセスが開始します。
- `show dot1x` イネーブル EXEC コマンドを使用して、クライアントのポスチャを示す 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 検証の設定の詳細については、「[NAC レイヤ 2 IEEE 802.1X 検証の設定](#)」(p.8-38) と「[定期的な再認証のイネーブル化](#)」(p.8-27) 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。

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 認証のデフォルト設定 (p.8-19)
- IEEE 802.1X 認証設定時の注意事項 (p.8-20)
- 旧ソフトウェアリリースからのアップグレード (p.8-22)
- IEEE 802.1X 認証の設定 (p.8-23) (必須)
- スイッチと RADIUS サーバ間通信を設定する方法 (p.8-25) (必須)
- ホスト モードの設定 (p.8-26) (任意)
- 定期的な再認証のイネーブル化 (p.8-27) (任意)
- 手動によるポート接続クライアントの再認証 (p.8-27) (任意)
- 待機時間の変更 (p.8-28) (任意)
- スイッチとクライアント間の再送信時間の変更 (p.8-28) (任意)
- 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 (p.8-29) (任意)
- 再認証回数の設定 (p.8-30) (任意)
- IEEE 802.1X アカウンティングの設定 (p.8-30) (任意)
- ゲスト VLAN の設定 (p.8-31) (任意)
- 制限付き VLAN の設定 (p.8-32) (任意)
- アクセス不能認証バイパス機能の設定 (p.8-34)
- WoL を使用した IEEE 802.1X 認証の設定 (p.8-36)
- MAC 認証バイパスの設定 (p.8-37)
- NAC レイヤ 2 IEEE 802.1X 検証の設定 (p.8-38)
- ポートでの IEEE 802.1X 認証のディセーブル化 (p.8-39)
- IEEE 802.1X 設定をデフォルト値にリセットする方法 (p.8-39) (任意)

IEEE 802.1X 認証のデフォルト設定

表 8-2 に、IEEE 802.1X 認証のデフォルト設定を示します。

表 8-2 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 イネーブル状態	ディセーブル
インターフェイス単位の IEEE 802.1X イネーブル状態	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。
AAA	ディセーブル
RADIUS サーバ	
<ul style="list-style-type: none"> • IP アドレス • UDP 認証ポート • 鍵 	<ul style="list-style-type: none"> • 指定なし • 1812 • 指定なし
ホスト モード	シングルのホスト モード
制御方向	双方向制御
定期的再認証	ディセーブル

表 8-2 IEEE 802.1X 認証のデフォルト設定 (続き)

機能	デフォルト設定
再認証試行間隔 (秒)	3600 秒
再認証回数	2 回 (ポートが無許可状態に変わる前にスイッチが認証プロセスを再起動する回数)
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、スイッチが待機状態にとどまる秒数)
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)
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、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、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)
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、これらの機能の設定時における注意事項を説明します。

- [IEEE 802.1X 認証 \(p.8-20\)](#)
- [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 \(p.8-21\)](#)
- [MAC 認証バイパス \(p.8-22\)](#)

IEEE 802.1X 認証

IEEE 802.1X 認証設定の注意事項は、次のとおりです。

- IEEE 802.1X 認証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、およびレイヤ 3 ルーテッド ポートでは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 認証をイネーブルにしようとする、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、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 認証をイネーブルにしようとする、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 対応ポートのモード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 認証をイネーブルにしようとする、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 VLAN 割り当てに変更しようとする、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にする予定の EtherChannel メンバーのポートを、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、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(25)SE より前のソフトウェア リリースでは、IEEE 802.1X 認証が EtherChannel の未アクティブ ポートでイネーブルになっている場合、ポートは EtherChannel に追加されません。

- 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 宛先ポート、RSPAN 宛先ポート、または RSPAN リフレクタ ポートで IEEE 802.1X 認証をイネーブルにできません。ただし、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。
- `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 認証をグローバルにイネーブルにする前に、IEEE 802.1X 認証および EtherChannel が設定されているインターフェイスから EtherChannel 設定を削除してください。
- EAP-Transparent LAN Services (TLS; 透過性 LAN サービス) および EAP-MD5 を使用した 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、さらにスイッチが Cisco IOS Release 12.1(14)EA1 を実行している場合、デバイスで実行している ACS のバージョンが 3.2.1 以降であることを確認してください。

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

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の設定時の注意事項は、次のとおりです。

- IEEE 802.1X 認証をポートでイネーブルにすると、音声 VLAN と同じポート VLAN を設定できません。
- トランク ポート、ダイナミック ポート、または VMPS を介したダイナミック アクセス ポート割り当ては、VLAN 割り当て機能を備えた IEEE 802.1X 認証をサポートしません。
- プライベート VLAN ポートで IEEE 802.1X 認証を設定できますが、プライベート VLAN ポート上で、ポート セキュリティ、音声 VLAN、ゲスト VLAN、制限付き VLAN、またはユーザ単位の ACL を使用する IEEE 802.1X 認証を設定しないでください。
- RSPAN VLAN または音声 VLAN 以外であれば、いずれの VLAN も、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ません。アクセス ポートでのみサポートされます。
- DHCP クライアントが接続されている IEEE 802.1X ポートに対してゲスト VLAN を設定したあと、ホスト IP アドレスを DHCP サーバから取得する必要があります。また、クライアントの DHCP プロセスがタイムアウトし、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、スイッチの IEEE 802.1X 認証プロセスを再起動するための設定を変更できます。IEEE 802.1X 認証プロセスの設定を減らします (`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)。設定を減らす量は、接続されている 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場合の注意事項は、次のとおりです。
 - この機能は、シングル ホスト モードとマルチホスト モードの IEEE 802.1X ポートでサポートされます。

- 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である場合、Windows XP はインターフェイスが認証されていないことをレポートすることがあります。
- Windows XP クライアントが DHCP 用に設定されていて、DHCP サーバから IP アドレスを取得している場合、クリティカル ポートの EAP 成功メッセージの受信が DHCP 設定プロセスを再開しない可能性があります。
- 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 を設定できます。スイッチが制限付き VLAN のクリティカル ポートを再認証しようとしてすべての RADIUS サーバが使用できない場合、スイッチはポートをクリティカル認証ステートにして、制限付き VLAN 内に残します。
- 同じスイッチ ポート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 以外であれば、いずれの VLAN も、IEEE 802.1X 認証の制限付き 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ません。アクセス ポート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限り、MAC 認証バイパスの注意事項は IEEE 802.1X 認証の注意事項と同じです。詳細については、「[IEEE 802.1X 認証](#)」(p.8-20) 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 MAC 認証バイパスをディセーブルにする場合、ポート ステートに影響しません。
- 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 データベースでない場合、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はこのステートのままになります。

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 認証に関する実装が旧リリースから変更されました。グローバル コンフィギュレーション コマンドの一部は、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、新しいコマンドも追加されました。

スイッチで IEEE 802.1X 認証が設定済みであり、Cisco IOS Release 12.1(14)EA1 以降にアップグレードする場合は、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ので、IEEE 802.1X 認証は動作しません。アップグレードの終了後、`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 認証をグローバルにイネーブルにする必要があります。IEEE 802.1X 認証が、旧リリースでインターフェイス上の複数のホスト モードで稼働していた場合、`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再設定する必要があります。

Cisco IOS Release 12.2(25)SEE では、IEEE 802.1X 認証に関する実装が旧リリースから変更されました。IEEE 802.1X 認証がイネーブルになる場合、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順番と認証方式を記述したものです。

ソフトウェアは方式リストの最初の方式を使用してユーザを認証します。この方式で応答に失敗した場合、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すまで続きます。このサイクルのいずれかの時点で認証が失敗すると、認証プロセスは停止し、他の認証方式が試行されることはありません。


ユーザ単位の 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。

これは、IEEE 802.1X AAA プロセスです。

-
- 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** VLAN 割り当てが RADIUS サーバ設定に基づいてイネーブルになります（該当する場合）。
 - ステップ 4** スイッチが開始メッセージをアカウントिंग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、再認証の結果に基づいて仮のアカウントिंग アップデートをアカウントिंग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トिंग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。この手順は必須です。

	コマンド	目的
ステップ 1	<code>configure terminal</code>	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	<code>aaa new-model</code>	AAA をイネーブルにします。

	コマンド	目的
ステップ 3	<code>aaa authentication dot1x {default} method1</code>	<p>IEEE 802.1X 認証方式リストを作成します。</p> <p>authentication コマンドで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。</p> <p><i>method1</i> 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。</p> <p> (注) 他のキーワードがコマンドラインのヘルプ スtring に表示されていても、default および group radius キーワードのみがサポートされています。</p>
ステップ 4	<code>dot1x system-auth-control</code>	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	<code>aaa authorization network {default} group radius</code>	<p>(任意) ユーザ単位の 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。</p> <p>ユーザ単位の 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。これがデフォルト設定です。</p>
ステップ 6	<code>radius-server host ip-address</code>	(任意) RADIUS サーバの IP アドレスを指定します。
ステップ 7	<code>radius-server key string</code>	(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化鍵を指定します。
ステップ 8	<code>interface interface-id</code>	IEEE 802.1X 認証をイネーブルにするクライアントに接続されたポートを指定して、インターフェイス コンフィギュレーション モードを開始します。
ステップ 9	<code>switchport mode access</code>	(任意) ステップ 6 および 7 で RADIUS サーバを設定した場合にのみ、ポートをアクセスモードに設定します。
ステップ 10	<code>dot1x port-control auto</code>	<p>インターフェイスで IEEE 802.1X 認証をイネーブルにします。</p> <p>設定の詳細については、「IEEE 802.1X 認証設定時の注意事項」(p.8-20) を参照してください。</p>
ステップ 11	<code>end</code>	イネーブル EXEC モードに戻ります。
ステップ 12	<code>show dot1x</code>	<p>設定を確認します。</p> <p>出力された IEEE 802.1X Port Summary セクションの Status カラムを調べてください。<i>enabled</i> 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。</p>
ステップ 13	<code>copy running-config startup-config</code>	(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。スイッチで 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。


次に、ポートで AAA および IEEE 802.1X をイネーブルにする例を示します。

```
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
```

スイッチと RADIUS サーバ間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、または 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	目的
ステップ 1	<code>configure terminal</code>	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	<code>radius-server host {hostname ip-address} auth-port port-number key string</code>	<p>スイッチに RADIUS サーバ パラメータを設定します。</p> <p><code>hostname ip-address</code> 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。</p> <p><code>auth-port port-number</code> には、認証要求の UDP 宛先ポートを指定します。デフォルト値は 1812 です。</p> <p><code>key string</code> には、スイッチと RADIUS サーバ上で稼働する RADIUS デモンとの間で使用する認証および暗号化鍵を指定します。鍵は、RADIUS サーバ上で使用する暗号化鍵と一致する必要のある文字列です。</p> <p> (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 <code>radius-server host</code> 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 デモン上で使用する暗号と一致する必要があります。</p> <p>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て入力してください。</p>
ステップ 3	<code>end</code>	イネーブル EXEC モードに戻ります。
ステップ 4	<code>show running-config</code>	設定を確認します。
ステップ 5	<code>copy running-config startup-config</code>	(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。

指定された 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、暗号化鍵を RADIUS サーバ上の鍵と一致する `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、および暗号化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.7-31) 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。この設定とは、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 テキスト ストリングです。詳細については、RADIUS サーバのマニュアルを参照してください。

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	目的
ステップ 1	<code>configure terminal</code>	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	<code>interface interface-id</code>	間接的に接続されている複数のホストに対して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	<code>dot1x host-mode multi-host</code>	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、 <code>dot1x port-control</code> インターフェイス コンフィギュレーション コマンドが <code>auto</code> に設定されていることを確認します。
ステップ 4	<code>end</code>	イネーブル EXEC モードに戻ります。
ステップ 5	<code>show dot1x interface interface-id</code>	設定を確認します。
ステップ 6	<code>copy running-config startup-config</code>	(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。

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

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

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て、その発生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)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	目的
ステップ 1	<code>configure terminal</code>	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	<code>interface interface-id</code>	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	<code>dot1x reauthentication</code>	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	<code>dot1x timeout reauth-period {seconds server}</code>	<p>キーワードの意味は次のとおりです。</p> <ul style="list-style-type: none"> <code>seconds</code> 指定できる範囲は 1 ~ 65535 秒です。デフォルトは 3600 秒です。 <code>server</code> 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。 <p>このコマンドがスイッチの動作に影響するのは、定期的な再認証がイネーブルに設定されている場合だけです。</p>
ステップ 5	<code>end</code>	イネーブル EXEC モードに戻ります。
ステップ 6	<code>show dot1x interface interface-id</code>	設定を確認します。
ステップ 7	<code>copy running-config startup-config</code>	(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を試行する間隔に戻すには、`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、再認証を試行する間隔を 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
```

手動によるポート接続クライアントの再認証

`dot1x re-authenticate interface interface-id` イネーブル EXEC コマンドを入力すると、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、「[定期的な再認証のイネーブル化](#)」(p.8-27)を参照してください。

次に、ポートに接続した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。アイドル時間は、quiet-period の値によって決まります。クライアントが無効なパスワードを指定したため、クライアントの認証に失敗す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	目的
ステップ 1	<code>configure terminal</code>	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	<code>interface interface-id</code>	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	<code>dot1x timeout quiet-period seconds</code>	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タスにな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	<code>end</code>	イネーブル EXEC モードに戻ります。
ステップ 5	<code>show dot1x interface interface-id</code>	設定を確認します。
ステップ 6	<code>copy running-config startup-config</code>	(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	目的
ステップ 1	<code>configure terminal</code>	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	<code>interface interface-id</code>	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	<code>dot1x timeout tx-period seconds</code>	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 15 ~ 65535 秒で、デフォルトは 30 秒です。
ステップ 4	<code>end</code>	イネーブル EXEC モードに戻ります。

	コマンド	目的
ステップ 5	<code>show dot1x interface interface-id</code>	設定を確認します。
ステップ 6	<code>copy running-config startup-config</code>	(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。

次に、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 秒に設定する例を示します。

```
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	目的
ステップ 1	<code>configure terminal</code>	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	<code>interface interface-id</code>	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	<code>dot1x max-req count</code>	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	<code>end</code>	イネーブル EXEC モードに戻ります。
ステップ 5	<code>show dot1x interface interface-id</code>	設定を確認します。
ステップ 6	<code>copy running-config startup-config</code>	(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。

次に、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 回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

ポートが無許可状態になる前にスイッチが認証プロセスを再起動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	目的
ステップ 1	<code>configure terminal</code>	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	<code>interface interface-id</code>	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	<code>dot1x max-reauth-req count</code>	ポートが無許可状態に変更する前にスイッチが認証プロセスを再起動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	<code>end</code>	イネーブル EXEC モードに戻ります。
ステップ 5	<code>show dot1x interface interface-id</code>	設定を確認します。
ステップ 6	<code>copy running-config startup-config</code>	(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。

次に、ポートが無許可状態にな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 アカウンティングによる AAA システムのアカウンティングをイネーブルにすると、システムがイベントをリロードしてアカウンティング RADIUS サーバに記録するために送信できるようになります。これにより、サーバはすべてのアクティブ IEEE 802.1X セッションがクローズされたと判断します。

RADIUS は信頼性のない UDP 転送プロトコルを使用しているため、ネットワークの状態が悪いとアカウンティングメッセージを損失する場合があります。アカウンティング要求の再送信を設定した回数行ったあとも、アカウンティングの応答メッセージをスイッチが RADIUS サーバから受信していない場合、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.
```

停止メッセージが正常に送信されないと、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) RADIUS サーバがアカウントリング タスク (ログインの開始、停止、中間アップデート メッセージ、タイム スタンプなど) を実行するように設定する必要があります。これらの機能を有効にするには、RADIUS サーバの Network Configuration タブにある [Update/Watchdog packets from this AAA client] のログインをイネーブルにしてください。次に、RADIUS サーバの System Configuration タブにある [CVS RADIUS Accounting] をイネーブルにしてください。

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	目的
ステップ 1	<code>configure terminal</code>	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	<code>interface interface-id</code>	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	<code>aaa accounting dot1x default start-stop group radius</code>	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	<code>aaa accounting system default start-stop group radius</code>	(任意) システムのアカウントリングをイネーブルにして (すべての RADIUS サーバのリストを使用)、スイッチのリロードのときに、システム アカウンティングのリロード イベント メッセージを生成します。
ステップ 5	<code>end</code>	イネーブル EXEC モードに戻ります。
ステップ 6	<code>show running-config</code>	設定を確認します。
ステップ 7	<code>copy running-config startup-config</code>	(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。

`show radius statistics` イネーブル EXEC コマンドを使用して、アカウントリング応答メッセージを受信していない RADIUS メッセージ数を表示します。

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、アカウントリング用の UDP ポートとして 1813 を指定し、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

ゲスト VLAN を設定する場合、サーバが EAPOL 要求 / アイデンティティ フレームへの応答を受信しなければ、IEEE 802.1X 未対応のクライアントはゲスト VLAN になります。IEEE 802.1X 対応のクライアントでも認証に失敗すれば、ネットワーク アクセスは許可されません。スイッチは、シングル ホスト モードでもマルチ ホスト モードでもゲスト VLAN をサポートします。



(注) スイッチ設定によっては、ゲスト VLAN へのクライアントの割り当てに数分かかる場合もあります。

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	目的
ステップ 1	<code>configure terminal</code>	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	<code>interface interface-id</code>	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 認証設定時の注意事項」(p.8-20) を参照してください。
ステップ 3	<code>switchport mode access</code>	ポートをアクセス モードに設定します。
ステップ 4	<code>dot1x port-control auto</code>	ポートで IEEE 802.1X 認証をイネーブルにします。
ステップ 5	<code>dot1x guest-vlan vlan-id</code>	IEEE 802.1X ゲスト VLAN として、アクティブな VLAN を指定します。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、または音声 VLAN 以外であれば、いずれのアクティブな VLAN も、IEEE 802.1X ゲスト VLAN として設定できます。
ステップ 6	<code>end</code>	イネーブル EXEC モードに戻ります。
ステップ 7	<code>show dot1x interface interface-id</code>	設定を確認します。
ステップ 8	<code>copy running-config startup-config</code>	(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場合は、`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、ポートで IEEE 802.1X ゲスト VLAN をイネーブルにする例を示します。

```
Switch(config)# interface fastethernet0/1
Switch(config-if)# dot1x guest-vlan 9
```

次に、スイッチの待機時間を 3 に設定して、スイッチが要求を再送信するまでクライアントからの EAP 要求 / アイデンティティ フレームの応答を待機する秒数を 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

スイッチに制限付き VLAN を設定すると、認証サーバが有効なユーザ名とパスワードを受信しなければ、IEEE 802.1X 準拠のクライアントは制限付き VLAN になります。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	目的
ステップ 1	<code>configure terminal</code>	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	<code>interface interface-id</code>	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.8-20) を参照してください。

	コマンド	目的
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 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	ポートで IEEE 802.1X 認証をイネーブルにします。
ステップ 5	dot1x guest-vlan <i>vlan-id</i>	IEEE 802.1X 制限付き VLAN として、アクティブな VLAN を指定します。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 以外であれば、いずれのアクティブな VLAN も、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 <i>interface-id</i>	(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場合は、`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、IEEE 802.1X 制限付き VLAN として VLAN 2 をイネーブルにする例を示します。

```
Switch(config)# interface gigabitethernet0/1
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 コマンドを使用して、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 回です。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	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 <i>interface-id</i>	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	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 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 <i>vlan-id</i>	IEEE 802.1X 制限付き VLAN として、アクティブ VLAN を指定します。指定できる範囲は 1 ~ 4094 です。 RSPAN VLAN または音声 VLAN 以外であればいずれのアクティブ VLAN も、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 <i>max attempts</i>	ポートが制限付き VLAN に移行するまで許可される認証試行回数を指定します。指定できる範囲は 1 ~ 3 回で、デフォルトは 3 回です。
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 <i>interface-id</i>	(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。

デフォルトの値に戻すには、`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 に移行するまで許可される認証試行回数を 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

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）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て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	目的
ステップ 1	<code>configure terminal</code>	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	<code>radius-server dead-criteria time <i>time</i> tries <i>tries</i></code>	(任意) RADIUS サーバが使用できないまたは停止中と見なされるときを決定するのに使われる条件を設定します。 指定できる <i>time</i> の範囲は 1 ~ 120 秒です。スイッチは、デフォルトの <i>seconds</i> 値を 10 ~ 60 秒の間で動的に決定します。 指定できる <i>tries</i> の範囲は 1 ~ 100 です。スイッチは、デフォルトの <i>tries</i> パラメータを 10 ~ 100 の間で動的に決定します。
ステップ 3	<code>radius-server deadtime <i>minutes</i></code>	(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 (24 時間) です。デフォルト値は 0 分です。

コマンド	目的
ステップ 4 <code>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]]</code>	<p>(任意) これら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。</p> <ul style="list-style-type: none"> • <code>acct-port udp-port</code> RADIUS アカウンティング サーバの UDP ポートを指定します。UDP ポートの範囲は 0 ~ 65536 です。デフォルト値は 1646 です。 • <code>auth-port udp-port</code> 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。デフォルト値は 1645 です。 <p> (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。</p> <ul style="list-style-type: none"> • <code>key string</code> スイッチと RADIUS デーモンとの間の RADIUS 通信で使用する認証および暗号化鍵を指定します。 <p> (注) <code>radius-server key {0 string 7 string string}</code> 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化鍵を設定できます。</p> <ul style="list-style-type: none"> • <code>test username name</code> RADIUS サーバステータスの自動テストをイネーブルにして、使用されるユーザ名を指定します。 • <code>idle-time time</code> 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。 • <code>ignore-acct-port</code> 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。 • <code>ignore-auth-port</code> RADIUS サーバ認証ポートのテストをディセーブルにします。
ステップ 5 <code>dot1x critical {eapol recovery delay milliseconds}</code>	<p>(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。</p> <p><code>eapol</code> スイッチがクリティカルポートの認証に成功したときにスイッチが EAPOL 成功メッセージを送信するように指定します。</p> <p><code>recovery delay milliseconds</code> 使用できなかった 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)。</p>
ステップ 6 <code>interface interface-id</code>	<p>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.8-20) を参照してください。</p>

	コマンド	目的
ステップ 7	<code>dot1x critical [recovery action reinitialize vlan <i>vlan-id</i>]</code>	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。 <ul style="list-style-type: none"> <code>recovery action reinitialize</code> 回復機能をイネーブルにして、回復アクションで、認証サーバが使用可能なときにポートを認証するように指定します。 <code>vlan <i>vlan-id</i></code> クリティカル ポートの割り当てが可能なアクセス VLAN スイッチを指定します。指定できる範囲は 1 ~ 4094 です。
ステップ 8	<code>end</code>	イネーブル EXEC モードに戻ります。
ステップ 9	<code>show dot1x interface <i>interface-id</i></code>	(任意) 設定を確認します。
ステップ 10	<code>copy running-config startup-config</code>	(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 サーバを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 fastethernet0/1
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

認証と WoL を使用した IEEE 802.1X 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	目的
ステップ 1	<code>configure terminal</code>	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	<code>interface <i>interface-id</i></code>	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.8-20)を参照してください。

	コマンド	目的
ステップ 3	<code>dot1x control-direction {both in}</code>	ポートで WoL を使用した IEEE 802.1X 認証をイネーブルにして、次のキーワードを使用して双方向または単一方向にポートを設定します。 <ul style="list-style-type: none"> 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の送受信を行なえません。デフォルトで、ポートは双方向です。 in ポートを単一方向に設定します。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	<code>end</code>	イネーブル EXEC モードに戻ります。
ステップ 5	<code>show dot1x interface interface-id</code>	設定を確認します。
ステップ 6	<code>copy running-config startup-config</code>	(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、ポートで WoL を使用した IEEE 802.1X 認証をイネーブル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、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	目的
ステップ 1	<code>configure terminal</code>	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	<code>interface interface-id</code>	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.8-20)を参照してください。
ステップ 3	<code>dot1x port-control auto</code>	ポートで IEEE 802.1X 認証をイネーブルにします。
ステップ 4	<code>dot1x mac-auth-bypass [eap]</code>	MAC 認証バイパスをイネーブルにします。 (任意) <code>eap</code> 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。
ステップ 5	<code>end</code>	イネーブル EXEC モードに戻ります。
ステップ 6	<code>show dot1x interface interface-id</code>	設定を確認します。
ステップ 7	<code>copy running-config startup-config</code>	(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設定する例を示します。

```
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、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	目的
ステップ 1	<code>configure terminal</code>	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	<code>interface interface-id</code>	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	<code>dot1x guest-vlan vlan-id</code>	IEEE 802.1X ゲスト VLAN として、アクティブ VLAN を指定します。指定できる範囲は 1 ~ 4094 です。 RSPAN VLAN または音声 VLAN 以外であればいずれのアクティブ VLAN も、IEEE 802.1X ゲスト VLAN として設定できます。
ステップ 4	<code>dot1x reauthentication</code>	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クライアントの再認証をイネーブルにします。
ステップ 5	<code>dot1x timeout reauth-period {seconds server}</code>	再認証を試行する間隔 (秒数) 設定します。 キーワードの意味は次のとおりです。 <ul style="list-style-type: none"> <code>seconds</code> 指定できる範囲は 1 ~ 65535 秒です。デフォルトは 3600 秒です。 <code>server</code> 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]) の値として秒数を指定します。 このコマンドがスイッチの動作に影響するのは、定期的な再認証がイネーブルに設定されている場合だけです。
ステップ 6	<code>end</code>	イネーブル EXEC モードに戻ります。
ステップ 7	<code>show dot1x interface interface-id</code>	IEEE 802.1X 認証設定を確認します。
ステップ 8	<code>copy running-config startup-config</code>	(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
```

ポートでの IEEE 802.1X 認証のディセーブル化

ポートで IEEE 802.1X 認証を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。

ポートでの IEEE 802.1X 認証をディセーブルにするには、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	目的
ステップ 1	<code>configure terminal</code>	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	<code>interface interface-id</code>	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	<code>no dot1x pae</code>	ポートで IEEE 802.1X 認証をディセーブルにします。
ステップ 4	<code>end</code>	イネーブル EXEC モードに戻ります。
ステップ 5	<code>show dot1x interface interface-id</code>	設定を確認します。
ステップ 6	<code>copy running-config startup-config</code>	(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。この場合、ポートで IEEE 802.1X がイネーブルになるものの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、ポートで IEEE 802.1X 認証をディセーブルにする例を示します。

```
Switch(config)# interface fastethernet0/1
Switch(config-if)# no dot1x pae authenticator
```

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。

	コマンド	目的
ステップ 1	<code>configure terminal</code>	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	<code>interface interface-id</code>	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	<code>dot1x default</code>	設定変更可能な 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	<code>end</code>	イネーブル EXEC モードに戻ります。
ステップ 5	<code>show dot1x interface interface-id</code>	設定を確認します。
ステップ 6	<code>copy running-config startup-config</code>	(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 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。特定のインターフェイスの 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。特定のインターフェイスの 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。