



## 802.1x ポートベースの認証の設定

---

この章では、Catalyst 3750 スイッチで IEEE 802.1x ポートベースの認証を設定する方法について説明します。LAN が、ホテル、空港、企業のロビーなどに拡張されると、安全とは言えない環境になりますが、802.1x を使用すれば、無許可のデバイス（クライアント）がネットワークへアクセスするのを防ぐことができます。特に明記しないかぎり、スイッチという用語はスタンドアロン スイッチおよびスイッチ スタックを意味します。



(注) この章で使用されるコマンドの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。

- [802.1x ポートベースの認証の概要 \(p.10-2\)](#)
- [802.1x 認証の設定 \(p.10-11\)](#)
- [802.1x 統計情報およびステータスの表示 \(p.10-21\)](#)

## 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、不正なクライアントが公的にアクセス可能なポートを介して LAN に接続するのを制限します。認証サーバは、スイッチ ポートに接続された各クライアントを認証してから、スイッチまたは LAN が提供するサービスを利用できるようにします。

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

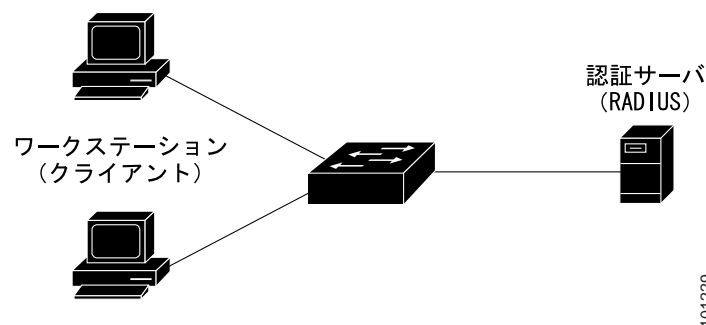
ここでは、802.1x ポートベース認証について説明します。

- デバイスの役割 (p.10-2)
- 認証の開始とメッセージ交換 (p.10-3)
- 許可ステートおよび無許可ステートのポート (p.10-4)
- サポート対象トポロジ (p.10-5)
- 802.1x とポート セキュリティの使用法 (p.10-6)
- 802.1x と音声 VLAN ポートの使用法 (p.10-6)
- 802.1x と VLAN 割り当ての使用法 (p.10-7)
- 802.1x とゲスト VLAN の使用法 (p.10-8)
- 802.1x とユーザ単位 ACL の使用法 (p.10-9)
- 802.1x とスイッチ スタック (p.10-10)

### デバイスの役割

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 10-1 のような特定の役割が割り当てられます。

図 10-1 802.1x デバイスの役割



- クライアント LAN およびスイッチへのアクセスを要求して、スイッチからの要求に応答するデバイス (ワークステーション)。ワークステーションでは、Microsoft Windows XP オペレーティング システムなど、802.1x 準拠のクライアント ソフトウェアが稼働する必要があります (クライアントは、IEEE 802.1x 規格の *supplicant* になります)。



(注) Windows XP ネットワーク接続および 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 Article を参照してください。  
<http://support.microsoft.com/support/kb/articles/Q303/5/97.ASP>

- **認証サーバ** 実際にクライアントの認証を行います。認証サーバは、クライアントの ID を確認し、クライアントの LAN およびスイッチ サービスへのアクセスを許可するかどうかをスイッチに通知します。スイッチはプロキシとして機能するので、認証サービスはクライアントにトランスペアレントです。このリリースでサポートされている認証サーバは、Extensible Authentication Protocol (EAP) 拡張機能を装備した 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 以上に対応しています。RADIUS は、RADIUS サーバと 1 つまたは複数の RADIUS クライアント間で安全な認証情報が交換されるクライアント / サーバ モデルで動作します。
- **スイッチ (エッジ スイッチまたは無線アクセス ポイント)** クライアントの認証ステータスに基づいてネットワークへの物理的なアクセスを制御します。スイッチは、クライアントと認証サーバとの間の媒介 (プロキシ) として機能し、クライアントに ID 情報を要求し、その情報を認証サーバで確認し、クライアントに応答をリレーします。スイッチには RADIUS クライアントが組み込まれています。RADIUS クライアントは、EAP フレームのカプセル化 / カプセル化解除、および認証サーバとの相互作用の役割を果たします。

スイッチが EAPOL フレームを受信して認証サーバにリレーすると、イーサネット ヘッダーが取り除かれ、残りの EAP フレームが RADIUS 形式で再度カプセル化されます。EAP フレームはカプセル化の間は変更や検査が行われず、認証サーバはネイティブのフレーム形式で EAP をサポートする必要があります。スイッチが認証サーバからフレームを受信すると、サーバのフレーム ヘッダーが削除され、EAP フレームが残ります。これがイーサネット用にカプセル化されてクライアントに送信されます。

媒介として機能できるデバイスには、Catalyst 3750、Catalyst 3560、Catalyst 3550、Catalyst 2970、Catalyst 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 802.1x をサポートするソフトウェアを実行している必要があります。

## 認証の開始とメッセージ交換

スイッチまたはクライアントは、認証を開始できます。**`dot1x port-control auto`** インターフェイス コンフィギュレーション コマンドを使用してポート上で認証をイネーブルにする場合、スイッチは、リンク ステートがダウンからアップに移行したときに、認証を開始する必要があります。次に 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してアイデンティティを要求します (一般に、スイッチは最初のアイデンティティ / 要求フレームを送信して、そのあとで 1 つまたは複数の認証情報の要求を送信します)。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。

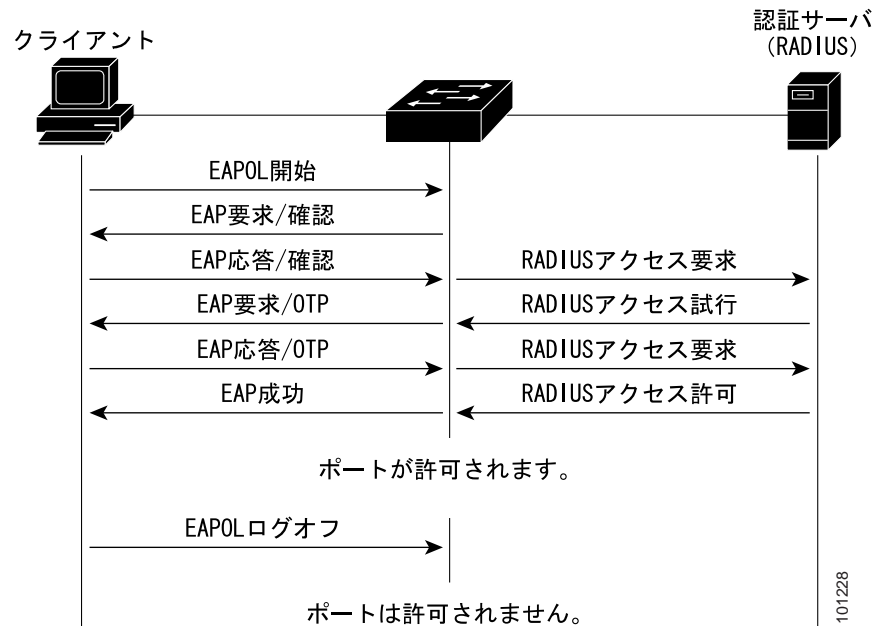


(注) ネットワーク アクセス デバイスで 802.1x がイネーブルになっていないかサポートされていない場合は、クライアントからの EAPOL フレームは廃棄されます。認証の開始を 3 回試行してもクライアントが EAP 要求 / アイデンティティ フレームを受信しない場合は、クライアントは、ポートが許可状態であるものとしてフレームを送信します。許可状態にあるポートは、事実上クライアントが正常に認証されたということです。詳細については、「許可状態および無許可状態のポート」(p.10-4) を参照してください。

クライアントがそのアイデンティティを供給すると、スイッチは媒介としての役割を開始し、認証が成功または失敗するまでクライアントと認証サーバとの間で EAP フレームを受け渡します。認証が成功すると、スイッチのポートは許可された状態になります。詳細については、「[許可ステートおよび無許可ステートのポート](#)」(p.10-4) を参照してください。

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

図 10-2 メッセージ交換



## 許可ステートおよび無許可ステートのポート

スイッチのポート ステートに応じて、スイッチはクライアントのネットワークへのアクセスを許可します。ポートは、*無許可*ステートで開始します。このステートにある間は、ポートは、802.1x、CDP、STP のプロトコル パケットを除くすべての入トラフィックおよび出トラフィックを許可しません。クライアントが正常に認証されると、ポートは*許可*ステートに移行し、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。

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

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

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

- **force-authorized** 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、クライアントの 802.1x ベースの認証なしで通常のトラフィックを送受信します。これがデフォルト設定です。

- **force-unauthorized** ポートを無許可状態のままにし、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、ポートを介してクライアントに認証サービスを提供できません。
- **auto** 802.1x 認証をイネーブルにして、ポートに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 Accept 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る後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。

## サポート対象トポロジー

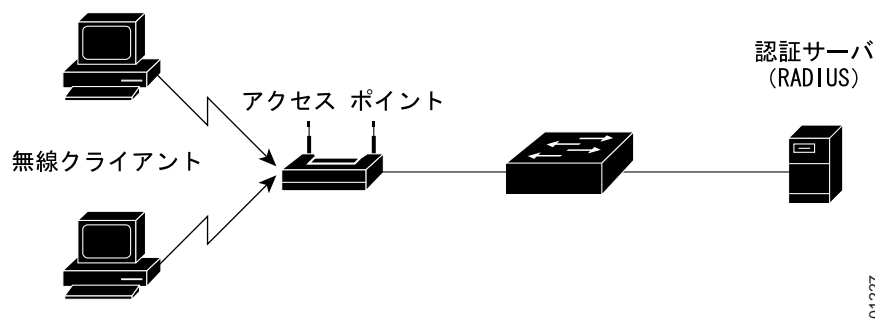
802.1x ポートベースの認証は、次の 2 つのトポロジーでサポートされています。

- ポイントツーポイント
- 無線 LAN

ポイントツーポイント（[図 10-1\[p.10-2\]](#)を参照）では、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、クライアントを検出します。クライアントがログオフするか、別のクライアントに交換されると、スイッチはポートのリンク ステートをダウンに変更し、ポートは無許可状態に戻ります。

[図 10-3](#) に、無線 LAN での 802.1x ポートベースの認証を示します。802.1x ポートは複数ホストポートとして設定されており、このポートは 1 つのクライアントが認証されるとすぐに許可状態になります。ポートが許可されると、そのポートに間接的に接続されている残りのホストはすべて、ネットワーク アクセスを許可されます。ポートが無許可になると（再認証が失敗するか、EAPOL ログオフ メッセージを受信する）、スイッチは、接続しているすべてのクライアントに対してネットワーク アクセスを拒否します。このトポロジーでは、無線アクセス ポイントは、接続しているクライアントを認証する役割があり、スイッチに対してクライアントとして機能します。

図 10-3 無線 LAN の例



## 802.1x とポート セキュリティの使用方法

単一ホストモードまたは複数ホストモードのどちらかで、802.1xポートおよびポートセキュリティを設定できます (*switchport port-security* インターフェイス コンフィギュレーション コマンドを使用してポートにポート セキュリティを設定しなければなりません)。ポート上のポート セキュリティと 802.1x をイネーブルにすると、802.1x がポートを認証し、ポート セキュリティがクライアントの MAC アドレスを含むすべての MAC アドレスについてネットワーク アクセスを管理します。この場合、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、802.1x とポート セキュリティの間には次のような相互作用があります。

- クライアントが認証され、ポート セキュリティ テーブルがいっぱいになっていない場合、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を保証されます (ポート セキュリティのスタティック エージングがイネーブルになっていない場合)。

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

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

ポート セキュリティ違反モードは、セキュリティ違反の動作を判別します。詳細については、「[セキュリティ違反](#)」(p.21-9) 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、802.1x クライアントのアドレスをポート セキュリティ テーブルから手動で削除した場合は、*dot1x re-authenticate interface interface-id* イネーブル EXEC コマンドを使用して 802.1x クライアントを再認証する必要があります。
- 802.1x クライアントがログオフすると、ポートが無許可状態に移行し、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、ポートは無許可状態になりすべてのダイナミック エントリはセキュア ホスト テーブルから削除されます。
- ポート セキュリティと音声 VLAN は、単一ホストまたは複数ホストモードのどちらかで、802.1x ポートに同時に設定できます。ポート セキュリティは、voice VLAN identifier (VVID; 音声 VLAN ID) と port VLAN identifier (PVID; ポート VLAN ID) の両方に適用されます。

スイッチのポート セキュリティをイネーブルにする方法の詳細については、「[ポート セキュリティの設定](#)」(p.21-8) を参照してください。

## 802.1x と音声 VLAN ポートの使用方法

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

- IP Phone の入出音声トラフィックを搬送するための VVID。VVID は、ポートに接続されている IP Phone を設定するために使用されます。
- IP Phone を通じてスイッチと接続しているワークステーションの入出データトラフィックを搬送するための PVID。PVID は、ポートのネイティブ VLAN です。

音声 VLAN に設定された各ポートに、PVID と VVID が関連付けられます。この設定によって、音声トラフィックとデータトラフィックを異なる VLAN に分離することができます。

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

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

単一ホストモードをイネーブルにすると、その VVID によって複数の IP Phone が許可されます。ただし、PVID では、1 つの 802.1x クライアントしか許可されません。複数ホストモードをイネーブルにする場合に 802.1x ユーザがプライマリ VLAN で認証されている場合、802.1x 認証がプライマリ VLAN で成功すれば音声 VLAN へ無制限にクライアントを追加できます。

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

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

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

## 802.1x と VLAN 割り当ての使用方法

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

ただし、Cisco IOS Release 12.1(14)EA1 以上では、スイッチは 802.1x と VLAN 割り当てをサポートしています。ポートの 802.1x 認証が成功すると、RADIUS サーバは、スイッチポートを設定するために VLAN 割り当てを送信します。RADIUS サーバのデータベースは、ユーザ名/VLAN の対応を維持します。この対応では、スイッチポートに接続するクライアントのユーザ名に基づいて VLAN を割り当てています。この機能を使用して、特定ユーザのネットワークアクセスを制限できます。

スイッチと RADIUS サーバを設定する場合、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 802.1x 許可がディセーブルの場合、認証が成功したあとにポートはアクセス VLAN に設定されます。
- 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を戻し、設定済みのアクセス VLAN 内に留まります。これにより、設定エラーによって不適切な VLAN 上にポートが突然現れることを防ぎます。

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

- 802.1x 許可がイネーブルで RADIUS サーバからのすべての情報が有効の場合、ポートは認証が成功したあと指定した VLAN に配置されます。
- 802.1x ポートで複数ホストモードがイネーブルの場合は、全てのホストが最初に認証されたホストと同じ VLAN（RADIUS サーバによって指定された）に配置されます。
- 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。

- 802.1x がポートでディセーブルの場合は、設定済みのアクセス VLAN に戻ります。

ポートが強制許可 (force authorized)、強制無許可 (force unauthorized)、無許可、シャットダウンのいずれかの状態の場合、そのポートは設定済みのアクセス VLAN に配置されます。

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 802.1x は、トランク ポート、ダイナミック ポート、または VLAN Membership Policy Server (VMPS) を使用したダイナミック アクセス ポート割り当てではサポートされていません。

VLAN 割り当てを設定するには、次の作業を実行する必要があります。

- **network** キーワードを使用して AAA 許可をイネーブルにし、RADIUS サーバからのインターフェイス設定を可能にします。
- 802.1x をイネーブルにします。(VLAN 割り当て機能は、アクセス ポートに 802.1x が設定されると自動的にイネーブルになります)
- RADIUS サーバにベンダー固有のトンネル アトリビュートを割り当てます。RADIUS サーバは次のアトリビュートをスイッチに戻さなければなりません。
  - [64] トンネル タイプ = VLAN
  - [65] トンネル メディア タイプ = 802
  - [81] トンネル プライベート グループ ID = VLAN 名または VLAN ID

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

トンネル アトリビュートの例については、「ベンダー固有の RADIUS アトリビュート用にスイッチを設定する方法」(p.9-29) を参照してください。

## 802.1x とゲスト VLAN の使用方法

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

認証サーバが EAPOL 要求 / アイデンティティ フレームへの応答を受信しなかった場合、802.1x 非対応のクライアントはポートのゲスト VLAN (設定されている場合) に配置されます。ただし、サーバは、ネットワークへの認証アクセスに失敗した 802.1x 対応のクライアントは許可しません。スイッチ ポートがゲスト VLAN に移動された場合には、無制限にホストにアクセスが許可されます。802.1x 対応のホストが、ゲスト VLAN が設定されているポートと同じポートに結合すると、そのポートはユーザ設定済みのアクセス VLAN 内で無許可状態に移行し、認証がやり直されます。

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

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

詳細については、「ゲスト VLAN の設定」(p.10-19) を参照してください。

## 802.1x とユーザ単位 ACL の使用方法

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

同じ Catalyst 3750 スイッチ上で、ACL の設定およびポート ACL の入力を行うことができます。ただし、ポート ACL はルータ ACL よりも優先されます。入力済みのポート ACL を VLAN に属するインターフェイスに適用する場合、ポート ACL は VLAN インターフェイスに適用する入力済みのルータ ACL よりも優先されます。ポート ACL が適用されたポート上で受信した着信パケットは、ポート ACL によってフィルタリングされます。その他のポートに着信したルーテッドパケットは、ルータ ACL によってフィルタリングされます。発信されるルーテッドパケットは、ルータ ACL によってフィルタリングされます。設定の矛盾を回避するには、RADIUS サーバに保存するユーザプロフィールを慎重に計画しなければなりません。

RADIUS は、Vendor Specific Attribute (VSA) などのユーザ単位アトリビュートをサポートします。これらの VSA は、オクテット スtring 形式で、認証プロセス中にスイッチに渡されます。ユーザ単位 ACL に使用される VSA は、入力方向では `inacl#<n>` で、出力方向では `outacl#<n>` です。MAC ACL は、入力方向でのみサポートされます。Catalyst 3750 スイッチは、入力方向でのみ VSA をサポートします。レイヤ 2 ポートの出力方向ではポート ACL をサポートしません。詳細については、[第 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。

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

フィルタ ID アトリビュートを使用して、すでにスイッチに設定されている着信または発信 ACL を指定できます。アトリビュートには、ACL 番号と、そのあとに入力フィルタリングか出力フィルタリングを示す `.in` または `.out` が含まれています。RADIUS サーバが `.in` または `.out` 構文を許可しない場合、アクセス リストはデフォルトで発信 ACL に適用されます。スイッチ上では Cisco IOS アクセス リストのサポートは限定されているため、フィルタ ID アトリビュートは番号が 1 ~ 199 および 1300 ~ 2699 までの IP ACL (IP 標準 ACL と IP 拡張 ACL) でのみサポートされています。

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

ユーザ単位 ACL の最大サイズは、4000 ASCII 文字です。

ベンダー固有のアトリビュートの例については、「[ベンダー固有の RADIUS アトリビュート用にスイッチを設定する方法](#)」(p.9-29) 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、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。
- 802.1x をイネーブルにします。
- RADIUS サーバにユーザプロフィールと VSA を設定します。
- 802.1x ポートを単一ホスト モードに設定します。

## 802.1x とスイッチ スタック

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

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

- すでに認証済みで定期的な再認証がイネーブル化されていないポートは、認証ステータスのままです。RADIUS サーバとのやり取りは必要ありません。
- すでに認証済みで、定期的な再認証がイネーブル化されているポートは (*dot1x re-authentication* グローバル コンフィギュレーション コマンドを使用して) 再認証時に認証プロセスに失敗します。ポートは、再認証プロセスで非認証ステータスに戻ります。RADIUS サーバとのやり取りが必要となります。

進行中の認証は、サーバ接続がないため即時に失敗します。

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

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

## 802.1x 認証の設定

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

- [802.1x のデフォルト設定 \(p.10-11\)](#)
- [802.1x 設定時の注意事項 \(p.10-12\)](#)
- [旧ソフトウェアリリースからのアップグレード \(p.10-13\)](#)
- [802.1x 認証の設定 \(p.10-13\)](#) (必須)
- [スイッチと RADIUS サーバ間通信を設定する方法 \(p.10-14\)](#) (必須)
- [定期的な再認証の設定 \(p.10-16\)](#) (任意)
- [手動によるポート接続クライアントの再認証 \(p.10-16\)](#) (任意)
- [待機時間の変更 \(p.10-16\)](#) (任意)
- [スイッチとクライアント間の再送信時間の変更 \(p.10-17\)](#) (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 \(p.10-18\)](#) (任意)
- [ホストモードの設定 \(p.10-18\)](#) (任意)
- [ゲスト VLAN の設定 \(p.10-19\)](#) (任意)
- [802.1x 設定をデフォルト値にリセットする方法 \(p.10-20\)](#) (任意)

## 802.1x のデフォルト設定

表 10-1 に、802.1x のデフォルト設定を示します。

表 10-1 802.1x 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	
<ul style="list-style-type: none"> <li>• IP アドレス</li> <li>• UDP 認証ポート</li> <li>• 鍵</li> </ul>	<ul style="list-style-type: none"> <li>• 指定なし</li> <li>• 1812</li> <li>• 指定なし</li> </ul>
スイッチの 802.1x イネーブル ステート	ディセーブル
ポート単位の 802.1x イネーブル ステート	ディセーブル (force-authorized)
	ポートは、クライアントの 802.1x ベースの認証なしで通常のトラフィックを送受信します。
定期的再認証	ディセーブル
再認証試行間隔	3600 秒
待機時間	60 秒 (クライアントとの認証交換が失敗したあと、スイッチが待機ステートにとどまる秒数)
再送信時間	30 秒 (スイッチが、クライアントからの EAP 要求 / アイデンティティ フレームに対する応答を待ち、要求を再送信するまでの秒数)
最大再送信回数	2 回 (スイッチが、認証プロセスを再開するまでに EAP 要求 / アイデンティティ フレームを送信する回数)
ホストモード	単一ホストモード
ゲスト VLAN	指定なし

表 10-1 802.1x のデフォルト設定 (続き)

機能	デフォルト設定
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)

## 802.1x 設定時の注意事項

802.1x 認証の設定時の注意事項は次のとおりです。

- 802.1x がイネーブルに設定されていると、他のレイヤ 2 またはレイヤ 3 機能がイネーブルになる前に、ポートは認証されません。
- 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 802.1x 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、802.1x はイネーブルになりません。802.1x 対応ポートのモードをトランクに変更しようとしても、エラーメッセージが表示され、ポートモードは変更されません。
  - ダイナミックポート ダイナミックモードのポートは、近接ポートとネゴシエーションしてトランクポートになる可能性があります。ダイナミックポートで 802.1x 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、802.1x はイネーブルになりません。802.1x 対応ポートのモードをダイナミックに変更しようとしても、エラーメッセージが表示され、ポートモードは変更されません。
  - ダイナミックアクセスポート ダイナミックアクセス (VLAN Query Protocol [VQP]) ポートで 802.1x 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、802.1x はイネーブルになりません。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 EtherChannel のアクティブメンバーであるポートは 802.1x ポートとして設定しないでください。EtherChannel のまだアクティブになっていないポートで 802.1x をイネーブルにしても、ポートは EtherChannel に加入しません。
  - Switched Port Analyzer (SPAN; スイッチドポートアナライザ) および Remote SPAN (RSPAN; リモート SPAN) 宛先ポート SPAN または RSPAN 宛先ポートであるポートで 802.1x をイネーブルにできます。ただし、SPAN または RSPAN 宛先ポートとして削除するまでは、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、802.1x をイネーブルにできません。
- RSPAN VLAN または音声 VLAN を除き、任意の VLAN を 802.1x ゲスト VLAN として設定できます。ゲスト VLAN 機能は、内部 VLAN (ルーテッドポート) またはトランクポートではサポートされていません。アクセスポート上でのみサポートされます。
- 802.1x をポートでイネーブルにすると、音声 VLAN と同じようにポート VLAN を設定できません。
- VLAN 割り当て機能付きの 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。

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

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

## 802.1x 認証の設定


802.1x ポートベースの認証をイネーブルにするには、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、1 番めにリストされた方式を使用して、ユーザを認証します。その方式が応答に失敗すると、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地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 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。

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	説明
ステップ 1	<b>configure terminal</b>	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	<b>aaa new-model</b>	AAA をイネーブルにします。
ステップ 3	<b>aaa authentication dot1x {default} method1 [method2...]</b>	802.1x 認証方式リストを作成します。  <b>authentication</b> コマンドに名前付きリストが指定されない場合に使用されるデフォルトのリストを作成するには、 <b>default</b> キーワードの後ろにデフォルトの状況で使用する方式を指定します。デフォルトの方式リストは、自動的にすべてのポートに適用されます。  次のキーワードを最低 1 つ入力します。 <ul style="list-style-type: none"> <li>• <b>group radius</b> 認証にすべての RADIUS サーバのリストを使用します。</li> <li>• <b>none</b> 認証を使用しません。スイッチは、クライアントから提供される情報を使用せずに、クライアントを自動的に認証します。</li> </ul>
ステップ 4	<b>dot1x system-auth-control</b>	スイッチ上で 802.1x 認証をグローバルにイネーブルにします。

	コマンド	説明
ステップ 5	<b>aaa authorization network { default } group radius</b>	(任意) ユーザ単位 ACL や VLAN 割り当てなど、ネットワーク関連のすべてのサービス要求に対するユーザ RADIUS 許可をスイッチに設定します。   (注) ユーザ単位 ACL の場合は、単一ホストモードを設定する必要があります。これはデフォルト設定です。
ステップ 6	<b>interface interface-id</b>	クライアントに接続されたポートの中で、802.1x 認証をイネーブルにするものを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 7	<b>dot1x port-control auto</b>	ポート上で 802.1x 認証をイネーブルにします。  機能の相互作用の詳細については、「 <a href="#">802.1x 設定時の注意事項</a> 」(p.10-12) を参照してください。
ステップ 8	<b>end</b>	イネーブル EXEC モードに戻ります。
ステップ 9	<b>show dot1x</b>	設定を確認します。
ステップ 10	<b>copy running-config startup-config</b>	(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。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。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。スイッチ上で 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、AAA および 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 gigabitethernet2/0/1
Switch(config)# 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、あるいは IP アドレスと特定の UDP ポート番号で識別します。IP アドレスと UDP ポート番号の組み合わせにより、一意の識別子が作成され、これにより、サーバ上の同一の IP アドレスの複数の UDP ポートに RADIUS 要求を送信できます。同一の RADIUS サーバ上の 2 つの異なるホストエントリが同じサービス (たとえば、認証) を設定している場合、あとから設定されたホストエントリは、最初のエントリのフェール オーバー バックアップとして機能します。RADIUS のホストエントリは、設定された順序で試されます。

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

	コマンド	説明
ステップ 1	<i>configure terminal</i>	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	<i>radius-server host {hostname   ip-address} auth-port port-number key string</i>	<p>RADIUS サーバパラメータを設定します。</p> <p><i>hostname   ip-address</i> 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><i>auth-port port-number</i> には、認証要求の UDP 宛先ポートを指定します。デフォルトは 1812 で、指定できる範囲は 0 ~ 65536 です。</p> <p><i>key string</i> には、スイッチと RADIUS サーバ上で稼働する RADIUS デーモンとの間で使用する認証および暗号化鍵を指定します。鍵は、RADIUS サーバ上で使用する暗号化鍵と一致する必要がある文字列です。</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 <i>radius-server host</i> コマンド構文の最後の項目として設定してください。鍵にスペースを使用する場合は、鍵の一部として引用符を使用する場合を除いて、鍵を引用符で囲まないでください。この鍵は、RADIUS デーモン上で使用する暗号と一致する必要があります。</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入力してください。</p>
ステップ 3	<i>end</i>	イネーブル EXEC モードに戻ります。
ステップ 4	<i>show running-config</i>	設定を確認します。
ステップ 5	<i>copy running-config startup-config</i>	(任意) コンフィギュレーション ファイルに設定を保存します。

特定の RADIUS サーバを削除するには、*no radius-server host {hostname | ip-address}* グローバル コンフィギュレーション コマンドを使用します。

次の例は、IP アドレスが 172.20.39.46 のサーバを RADIUS サーバとして指定し、ポート 1612 を許可ポートとして使用し、暗号化鍵を RADIUS サーバ上の鍵と *rad123* に設定します。

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

*radius-server host* グローバル コンフィギュレーション コマンドを使用すると、すべての RADIUS サーバに対してタイムアウト、再送信、および暗号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.9-29) 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 スtring 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。

## 定期的な再認証の設定

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）を設定するには、イネーブル EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	説明
ステップ 1	<b><i>configure terminal</i></b>	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	<b><i>interface interface-id</i></b>	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	<b><i>dot1x reauthentication</i></b>	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	<b><i>dot1x timeout reauth-period seconds</i></b>	再認証を試行する間隔（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 3600 秒です。  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 5	<b><i>end</i></b>	イネーブル EXEC モードに戻ります。
ステップ 6	<b><i>show dot1x interface interface-id</i></b>	設定を確認します。
ステップ 7	<b><i>copy running-config startup-config</i></b>	(任意) コンフィギュレーション ファイルに設定を保存します。

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

次の例では、定期的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 コマンドを使用すると、特定のポートに接続しているクライアントを手動でいつでも再認証できます。この手順は任意です。定期的な再認証をイネーブルまたはディセーブルにする場合は、「[定期的な再認証の設定](#)」(p.10-16) 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方法を示します。

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

## 待機時間の変更

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

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

	コマンド	説明
ステップ 1	<b><i>configure terminal</i></b>	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	<b><i>interface interface-id</i></b>	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	<b><i>dot1x timeout quiet-period seconds</i></b>	クライアントとの認証交換が失敗したあと、スイッチが待機ステートにある秒数を設定します。  指定できる範囲は 1 ~ 65535 秒で、デフォルトは 60 秒です。
ステップ 4	<b><i>end</i></b>	イネーブル EXEC モードに戻ります。
ステップ 5	<b><i>show dot1x interface interface-id</i></b>	設定を確認します。
ステップ 6	<b><i>copy running-config startup-config</i></b>	(任意) コンフィギュレーション ファイルに設定を保存します。

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

次の例では、スイッチ上の待機時間を 30 秒に設定します。

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

## スイッチとクライアント間の再送信時間の変更

クライアントは、スイッチからの EAP 要求 / アイデンティティ フレームに、EAP 応答 / アイデンティティ フレームで応答します。スイッチはこの応答を受信しなかった場合、一定時間 (再送信時間) 待機してから、フレームを再送信します。



(注) このコマンドのデフォルト値の変更は、信頼性のないリンクや、特定のクライアントおよび認証サーバの動作に問題があるなど、異常な状況を調整する場合以外は行わないようにしてください。

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

	コマンド	説明
ステップ 1	<b><i>configure terminal</i></b>	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	<b><i>interface interface-id</i></b>	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	<b><i>dot1x timeout tx-period seconds</i></b>	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 1 ~ 65535 秒で、デフォルトは 30 秒です。
ステップ 4	<b><i>end</i></b>	イネーブル EXEC モードに戻ります。
ステップ 5	<b><i>show dot1x interface interface-id</i></b>	設定を確認します。
ステップ 6	<b><i>copy running-config startup-config</i></b>	(任意) コンフィギュレーション ファイルに設定を保存します。

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

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

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

## スイッチとクライアント間のフレーム再送信回数の設定

スイッチとクライアント間の再送信時間の変更だけでなく、(応答を受信しなかった場合) 認証プロセスを再開するまでに、スイッチがクライアントに EAP 要求 / アイデンティティ フレームを送信する回数を変更できます。



(注) このコマンドのデフォルト値の変更は、信頼性のないリンクや、特定のクライアントおよび認証サーバの動作に問題があるなど、異常な状況を調整する場合以外は行わないようにしてください。

スイッチとクライアント間のフレーム再送信回数を設定するには、イネーブル EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	説明
ステップ 1	<b>configure terminal</b>	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	<b>interface interface-id</b>	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	<b>dot1x max-req count</b>	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	<b>end</b>	イネーブル EXEC モードに戻ります。
ステップ 5	<b>show dot1x interface interface-id</b>	設定を確認します。
ステップ 6	<b>copy running-config startup-config</b>	(任意) コンフィギュレーション ファイルに設定を保存します。

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

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

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

## ホスト モードの設定

802.1x ポートは、単一ホスト モードまたは複数ホスト モードに設定できます。単一ホスト モードでは、802.1x ポートで 1 台のホストだけが許可されます。ホストが認証されると、ポートは許可ステートになります。ホストがポートから切断されると、ポートは無許可ステートになります。認証済みのホスト以外のホストからのパケットは廃棄されます。

図 10-3 (p.10-5) のように、複数のホストを 1 つの 802.1x 対応ポートに接続できます。このモードでは、接続ホストのいずれか 1 つだけが許可されれば、すべてのホストがネットワーク アクセスを許可されます。ポートが無許可(再認証が失敗するか EAPOL ログオフ メッセージを受信した場合)になると、接続されたすべてのクライアントのネットワーク アクセスが拒否されます。

複数ホストモードがイネーブルの場合、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。

**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 802.1x 許可ポート上で、複数のホスト(クライアント)を許可するには、イネーブル EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	説明
ステップ 1	<b>configure terminal</b>	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	<b>interface interface-id</b>	複数のホストが間接的に接続されているポートを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	<b>dot1x host-mode multi-host</b>	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、 <b>dot1x port-control</b> インターフェイス コンフィギュレーション コマンドが <b>auto</b> に設定されていることを確認します。
ステップ 4	<b>end</b>	イネーブル EXEC モードに戻ります。
ステップ 5	<b>show dot1x interface interface-id</b>	設定を確認します。
ステップ 6	<b>copy running-config startup-config</b>	(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、802.1x をイネーブルにし、複数のホストを許可する方法を示します。

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

## ゲスト VLAN の設定

ゲスト VLAN を設定すると、サーバが EAPOL 要求 / アイデンティティ フレームへの応答を受信しなかった場合に、802.1x 非対応のクライアントはゲスト VLAN に配置されます。802.1x 対応だが、認証に失敗したクライアントは、ネットワークへのアクセスは許可されません。スイッチは、単一ホストモードまたは複数ホストモードでゲスト VLAN をサポートします。

ゲスト VLAN を設定するには、イネーブル EXEC モードで次の手順を行います。この手順は任意です。

	コマンド	説明
ステップ 1	<b><i>configure terminal</i></b>	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	<b><i>interface interface-id</i></b>	設定するポートを指定し、インターフェイス コンフィギュレーション モードを開始します。サポートされているポートタイプについては、「 <a href="#">802.1x 設定時の注意事項 (p.10-12)</a> 」を参照してください。
ステップ 3	<b><i>dot1x guest-vlan vlan-id</i></b>	アクティブ VLAN を 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、または音声 VLAN を除き、任意のアクティブ VLAN を 802.1x ゲスト VLAN として設定できます。
ステップ 4	<b><i>end</i></b>	イネーブル EXEC モードに戻ります。
ステップ 5	<b><i>show dot1x interface interface-id</i></b>	設定を確認します。
ステップ 6	<b><i>copy running-config startup-config</i></b>	(任意) コンフィギュレーション ファイルに設定を保存します。

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

次に、VLAN 2 を 802.1x ゲスト VLAN として設定する方法を示します。

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

## 802.1x 設定をデフォルト値にリセットする方法

802.1x 設定をデフォルト値にリセットするには、イネーブル EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	説明
ステップ 1	<b><i>configure terminal</i></b>	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	<b><i>interface interface-id</i></b>	インターフェイス コンフィギュレーション モードを開始し、設定するポートを指定します。
ステップ 3	<b><i>dot1x default</i></b>	設定変更可能な 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	<b><i>end</i></b>	イネーブル EXEC モードに戻ります。
ステップ 5	<b><i>show dot1x interface interface-id</i></b>	設定を確認します。
ステップ 6	<b><i>copy running-config startup-config</i></b>	(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。

## 802.1x 統計情報およびステータスの表示

すべてのポートの 802.1x 統計情報を表示するには、***show dot1x all statistics*** イネーブル EXEC コマンドを使用します。特定のポートの 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 802.1x 管理および動作のステータスを表示するには、***show dot1x all*** イネーブル EXEC コマンドを使用します。特定のポートの 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。

