CHAPTER 12

IEEE 802.1X ポートベースの認証の設定

IEEE 802.1X ポートベースの認証により、認証されていない装置（クライアント）がネットワークにアクセスするのを防止します。IE 3000 スイッチのコマンド リファレンスと、『Cisco IOS Security Command Reference, Release 12.2』の「RADIUS Commands」に、コマンドの構文と使用方法の情報があります。

この章の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.12-1）
- 「802.1X 認証の設定」（P.12-33）
- 「802.1X 統計情報およびステータスの表示」（P.12-67）

IEEE 802.1X ポートベースの認証の概要

この標準は、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を定義し、認可されていないクライアントが公にアクセス可能なポートを経由して LAN に接続するのを防ぎます。認証サーバは、スイッチ ポートに接続する各クライアントを認証したうえで、スイッチまたは LAN サービスを利用できるようにします。

IEEE 802.1X アクセス制御では、クライアントが認証されるまで、そのクライアントが接続しているポート経由では Extensible Authentication Protocol over LAN（EAPOL）、Cisco Discovery Protocol（CDP; シスコ検出プロトコル）、および Spanning Tree Protocol（STP; スパニング ツリー プロトコル）トラフィックしか許可されません。認証後は、通常のトラフィックがポート経由で送受信されます。

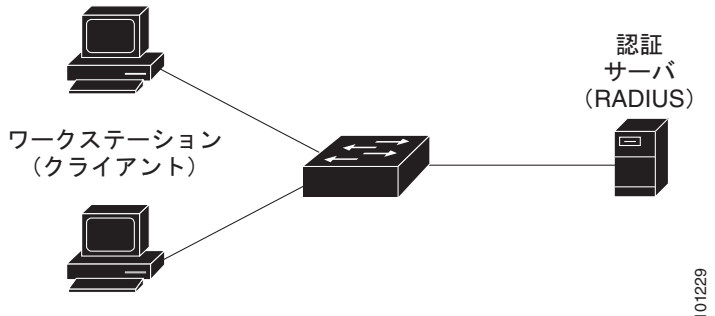
- 「装置の役割」（P.12-2）
- 「認証プロセス」（P.12-3）
- 「認証の開始およびメッセージ交換」（P.12-5）
- 「認証マネージャ」（P.12-7）
- 「認可ステートおよび無認可ステートのポート」（P.12-10）
- 「802.1X ホスト モード」（P.12-11）
- 「マルチドメイン認証」（P.12-12）
- 「802.1X マルチ認証モード」（P.12-13）
- 「MAC 移行」（P.12-13）
- 「MAC 置き換え」（P.12-14）
- 「802.1X アカウンティング」（P.12-15）
- 「802.1X アカウンティングの Attribute-Value ペア」（P.12-15）

- 「802.1X 準備状態チェック」（P.12-16）
- 「802.1X 認証と VLAN 割り当て」（P.12-16）
- 「802.1X 認証とユーザ単位 ACL の使用」（P.12-18）
- 「802.1X 認証とゲスト VLAN」（P.12-21）
- 「802.1X 認証と制限付き VLAN」（P.12-22）
- 「802.1X 認証とアクセス不能認証バイパス」（P.12-23）
- 「802.1X 認証と音声 VLAN ポート」（P.12-25）
- 「802.1X 認証とポート セキュリティ」（P.12-25）
- 「802.1X 認証と Wake-on-LAN」（P.12-26）
- 「802.1X 認証と MAC 認証バイパス」（P.12-27）
- 「802.1X ユーザ分散」（P.12-28）
- 「Network Admission Control レイヤ 2 802.1X 検証」（P.12-29）
- 「フレキシブルな認証順序付け」（P.12-29）
- 「Open1x 認証」（P.12-30）
- 「音声認識 802.1X セキュリティの使用」（P.12-30）
- 「802.1X サプリカント スイッチおよびオーセンティケータ スイッチと Network Edge Access Topology（NEAT; ネットワーク エッジ アクセス トポロジ）」（P.12-30）
- 「802.1X 認証とダウンロード可能 ACL およびリダイレクト URL」（P.12-19）
- 「IEEE 802.1X 認証と ACL および RADIUS Filter-Id 属性の使用」（P.12-32）
- 「共通セッション ID」（P.12-32）

装置の役割

802.1X ポートベースの認証での装置の役割：

図 12-1　802.1X 装置の役割



- *クライアント*：LAN およびスイッチ サービスへのアクセスを要求し、スイッチからの要求に応答する装置（ワークステーション）。ワークステーションでは、802.1X に準拠するクライアント ソフトウェア（Microsoft Windows XP オペレーティング システムで提供されるクライアント ソフトウェアなど）を実行している必要があります（クライアントは、802.1X 標準では*サプリカント*といいます）。

  （注）　Windows XP のネットワーク接続および 802.1X 認証の問題を解決するには、次の URL にあるマイクロソフト サポート技術情報の記事を参照してください。
  http://support.microsoft.com/support/kb/articles/Q303/5/97.ASP

- *認証サーバ*：クライアントの実際の認証を行います。認証サーバはクライアントの識別情報を確認し、そのクライアントに LAN およびスイッチ サービスへのアクセスを許可すべきかどうかをスイッチに通知します。スイッチはプロキシとして動作するので、認証サービスはクライアントに対してトランスペアレントに行われます。このリリースでは、Extensible Authentication Protocol（EAP）拡張機能を備えた RADIUS セキュリティ システムだけが認証サーバとしてサポートされています。この認証サーバは、Cisco Secure Access Control Server Version 3.0 以降で使用可能です。RADIUS はクライアント/サーバ モデルで動作し、RADIUS サーバと 1 つまたは複数の RADIUS クライアントとの間でセキュア認証情報を交換します。

- *スイッチ*（エッジ スイッチまたはワイヤレス アクセス ポイント）：クライアントの認証ステータスに基づいて、ネットワークへの物理アクセスを制御します。スイッチはクライアントと認証サーバの間の仲介装置（プロキシ）として動作し、クライアントに識別情報を要求し、その情報を認証サーバで確認し、クライアントに応答をリレーします。スイッチには、EAP フレームのカプセル化とカプセル化解除、および認証サーバとの対話を処理する、RADIUS クライアントが含まれています（スイッチは、802.1X 標準では*オーセンティケータ*です）。

  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際、イーサネット ヘッダーが取り除かれ、残りの EAP フレームが RADIUS フォーマットに再カプセル化されます。カプセル化では EAP フレームの変更は行われず、認証サーバはネイティブ フレーム フォーマット内の EAP をサポートする必要があります。スイッチが認証サーバからフレームを受信すると、サーバのフレーム ヘッダーが削除され、残りの EAP フレームがイーサネット用にカプセル化され、クライアントに送信されます。

  仲介装置として動作できる装置は、IE 3000、Catalyst 3750-E、Catalyst 3560-E、Catalyst 3750、Catalyst 3560、Catalyst 3550、Catalyst 2975、Catalyst 2970、Catalyst 2960、Catalyst 2955、Catalyst 2950、Catalyst 2940 の各スイッチや、ワイヤレス アクセス ポイントなどです。これらの装置では、RADIUS クライアントおよび 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

802.1X ポートベースの認証がイネーブルになっていて、クライアントが 802.1X に準拠するクライアント 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。

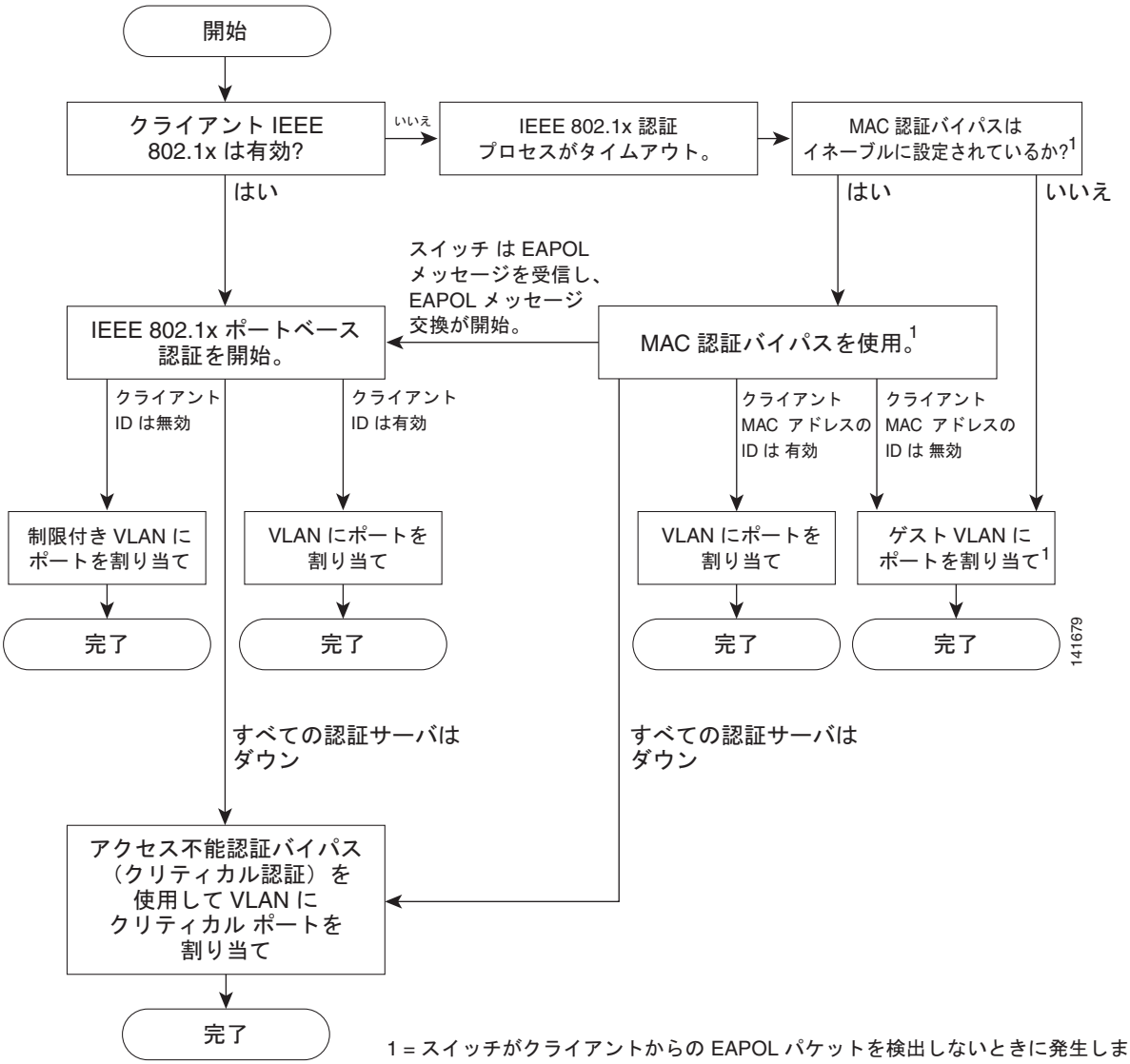
- クライアントの識別情報が有効で、802.1X 認証が成功した場合、スイッチはクライアントにネットワークへのアクセスを許可します。
- 802.1X 認証が EAPOL メッセージ交換を待機している間に時間切れとなり、Media Access Control（MAC; メディア アクセス制御）認証バイパスがイネーブルになっている場合、スイッチはクライアントの MAC アドレスを認証に使用できます。クライアントの MAC アドレスが有効で、認可が成功した場合、スイッチはクライアントにネットワークへのアクセスを許可します。クライアントの MAC が無効で、認可が失敗した場合、ゲスト VLAN が設定されていれば、スイッチは限られたサービスを提供するゲスト VLAN にクライアントを割り当てます。

- スイッチが 802.1X 対応のクライアントから無効な識別情報を取得し、制限付き VLAN が指定されている場合、スイッチは限られたサービスを提供する制限付き VLAN にクライアントを割り当てることができます。
- RADIUS 認証サーバが使用不可（ダウン）であり、アクセス不能認証バイパスがイネーブルになっている場合、スイッチは RADIUS 設定またはユーザ指定のアクセス VLAN でポートを critical-authentication ステートに置くことにより、ネットワークへのアクセスをクライアントに許可します。

（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、認可、アカウンティング）失敗ポリシーとも呼ばれます。

図 12-2 に認証プロセスを示します。

図 12-2　認証のフローチャート



1 = スイッチがクライアントからの EAPOL パケットを検出しないときに発生します。

スイッチは、次の状態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になっていて、再認証タイマーが期限切れになる。

  スイッチ固有の値を使用するか、RADIUS サーバの値に基づくように、再認証タイマーを設定できます。

  RADIUS サーバを使用する 802.1X 認証を設定したあと、スイッチは Session-Timeout RADIUS 属性（属性 [27]）および Termination-Action RADIUS 属性（属性 [29]）に基づいてタイマーを使用します。

  Session-Timeout RADIUS 属性（属性 [27]）は、再認証が行われるまでの時間を指定します。

  Termination-Action RADIUS 属性（属性 [29]）は、再認証中に実行するアクションを指定します。このアクションは、*Initialize* および *ReAuthenticate* です。*Initialize* アクションを設定した場合（属性値は *DEFAULT*）、802.1X セッションは終了し、接続は再認証中に失われます。*ReAuthenticate* アクションを設定した場合（属性値は RADIUS-Request）、セッションは再認証中に影響を受けません。

- **dot1x re-authenticate interface** *interface-id* 特権 EXEC コマンドを入力することにより、クライアントを手動で再認証する。

ポート上で Multidomain Authentication（MDA; マルチドメイン認証）がイネーブルになっている場合、このフローを使用できますが、音声認証に適用されるいくつかの例外があります。MDA の詳細については、「マルチドメイン認証」（P.12-12）を参照してください。

認証の開始およびメッセージ交換

802.1X 認証中に、スイッチまたはクライアントは認証を開始できます。**authentication port-control auto** または **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で認証をイネーブルにした場合、スイッチは、リンク ステートがダウンからアップに変化したときに、またはポートがアップのままで認証されていない限り定期的に、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識別情報を要求します。クライアントはフレームを受信すると、EAP 応答/アイデンティティ フレームで応答します。

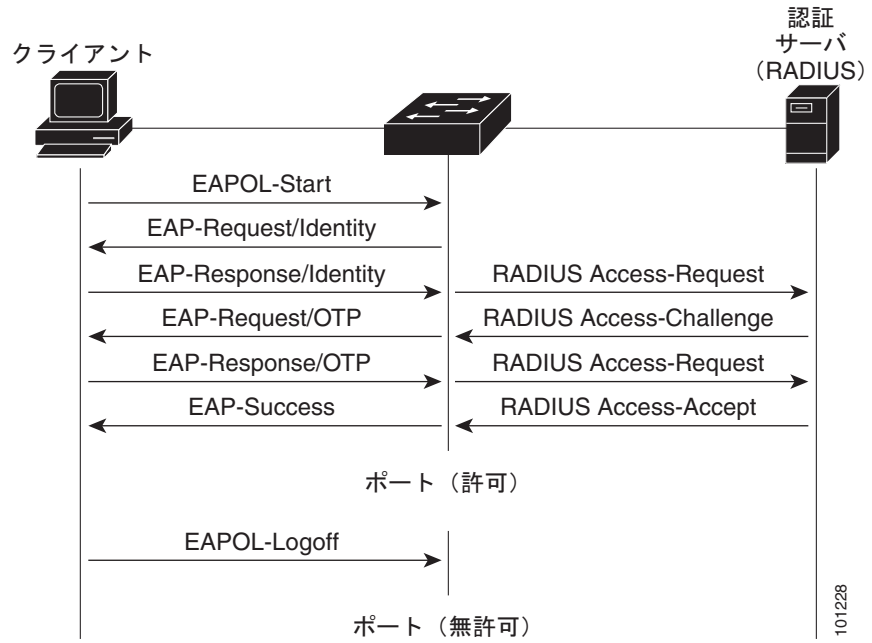
ただし、クライアントが起動時にスイッチから EAP 要求/アイデンティティ フレームを受信しなかった場合、クライアントは EAPOL 開始フレームを送信して認証を開始できます。このフレームはスイッチに対し、クライアントの識別情報を要求するように指示します。

（注）　ネットワーク アクセス装置で 802.1X 認証がイネーブルになっていない、またはサポートされていない場合には、クライアントからの EAPOL フレームはすべて廃棄されます。クライアントが認証の開始を 3 回試みても EAP 要求/アイデンティティ フレームを受信しなかった場合、クライアントはポートが認可ステートであるものとしてフレームを送信します。ポートが認可ステートであるということは、クライアントの認証が成功したことを実質的に意味します。詳細については、「認可ステートおよび無認可ステートのポート」（P.12-10）を参照してください。

クライアントが自らの識別情報を提示すると、スイッチは仲介装置としての役割を開始し、認証が成功または失敗するまで、クライアントと認証サーバの間で EAP フレームを送受信します。認証が成功すると、スイッチ ポートは認可ステートになります。認証が失敗した場合は、認証を再試行するか、限られたサービスを提供する VLAN にポートが割り当てられるか、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、「認可ステートおよび無認可ステートのポート」（P.12-10）を参照してください。

実際に行われる EAP フレーム交換は、使用する認証方式によって異なります。図 12-3 に、クライアントが RADIUS サーバとの間で One-Time-Password（OTP; ワンタイム パスワード）認証方式を使用する場合に行われるメッセージ交換を示します。

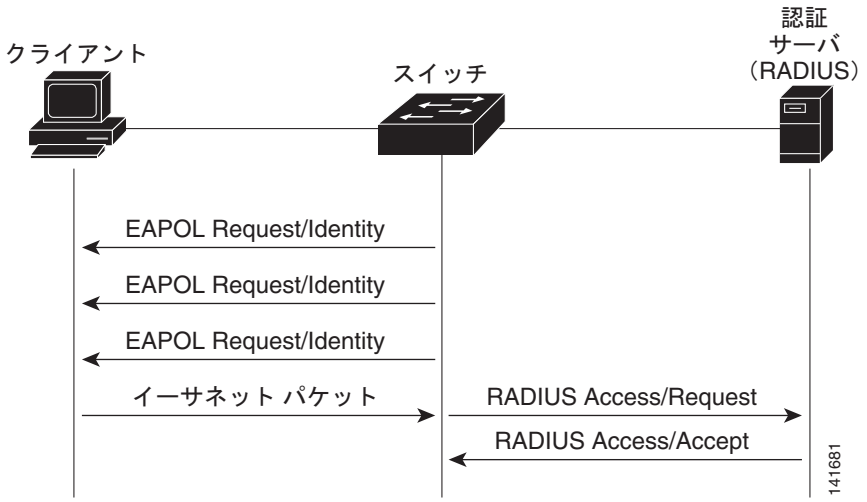
図 12-3　メッセージ交換



802.1X 認証が EAPOL メッセージ交換を待機している間に時間切れとなり、MAC 認証バイパスがイネーブルになっている場合、スイッチはクライアントからのイーサネット パケットを検出したときにクライアントを認可できます。スイッチは、クライアントの MAC アドレスを識別情報として使用し、この情報を RADIUS サーバに送信する RADIUS-access/request フレームに含めます。サーバがスイッチに RADIUS-access/accept フレームを送信したあと（認可が成功）、ポートは認可されます。認可が失敗し、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。スイッチがイーサネット パケットを待機しているときに EAPOL パケットを検出した場合、スイッチは MAC 認証バイパス プロセスを停止し、802.1X 認証を停止します。

図 12-4 に、MAC 認証バイパス中に行われるメッセージ交換を示します。

図 12-4　MAC 認証バイパス中のメッセージ交換



認証マネージャ

Cisco IOS Release 12.2(46)SE 以前では、このスイッチと Catalyst 6000 などの他のネットワーク装置で、CLI コマンドおよびメッセージなどの同じ認可方式を使用することはできませんでした。独立した認証設定を使用する必要がありました。Cisco IOS Release 12.2(50)SE 以降では、ネットワーク内のすべての Catalyst スイッチで同じ認可方式がサポートされます。

Cisco IOS Release 12.2(55)SE では、認証マネージャからの詳細なシステム メッセージのフィルタリングがサポートされます。詳細については、「認証マネージャの CLI コマンド」（P.12-9）を参照してください。

- 「ポートベースの認証方式」（P.12-7）
- 「ユーザ単位 ACL と Filter-Id」（P.12-8）
- 「認証マネージャの CLI コマンド」（P.12-9）

ポートベースの認証方式

表 12-1 に、次のホスト モードでサポートされる認証方式を示します。

- シングル ホスト：1 つのポートで 1 つのデータ ホストまたは音声ホスト（クライアント）だけを認証できます。
- マルチ ホスト：同じポートで複数のデータ ホストを認証できます（ポートがマルチホスト モードで無認可ステートになった場合、スイッチは接続されたすべてのクライアントへのネットワーク アクセスを拒否します）。
- マルチドメイン認証（MDA）：同じスイッチ ポートでデータ装置と音声装置の両方を認証できます。ポートは、データ ドメインと音声ドメインに分割されます。
- マルチ認証：データ VLAN で複数のホストを認証できます。音声 VLAN が設定されている場合、このモードでは VLAN で 1 つのクライアントが許可されます。

表 12-1　802.1X の機能

	モード			
認証方式	**シングル ホスト**	**マルチ ホスト**	**MDA[1]**	**マルチ認証[2]**
802.1X	VLAN 割り当て ユーザ単位 ACL Filter-ID 属性 ダウンロード可能 ACL[3] リダイレクト URL[3]	VLAN 割り当て ユーザ単位 ACL Filter-ID 属性 ダウンロード可能 ACL[4] リダイレクト URL[3]	VLAN 割り当て ユーザ単位 ACL[3] Filter-Id 属性[3] ダウンロード可能 ACL[3] リダイレクト URL[3]	ユーザ単位 ACL[3] Filter-Id 属性[3] ダウンロード可能 ACL[3] リダイレクト URL[3]
MAC 認証バイパス	VLAN 割り当て ユーザ単位 ACL Filter-ID 属性 ダウンロード可能 ACL[3] リダイレクト URL[3]	VLAN 割り当て ユーザ単位 ACL Filter-ID 属性 ダウンロード可能 ACL[3] リダイレクト URL[3]	VLAN 割り当て ユーザ単位 ACL[3] Filter-Id 属性[3] ダウンロード可能 ACL[3] リダイレクト URL[3]	ユーザ単位 ACL[3] Filter-Id 属性[3] ダウンロード可能 ACL[3] リダイレクト URL[3]
スタンドアロン Web 認証[4]	プロキシ ACL、Filter-Id 属性、ダウンロード可能 ACL[2]			

表 12-1　802.1X の機能 （続き）

認証方式	モード			
	シングル ホスト	マルチ ホスト	MDA[1]	マルチ認証[2]
NAC レイヤ 2 IP 検証	Filter-Id 属性[3] ダウンロード可能 ACL リダイレクト URL	Filter-Id 属性[3] ダウンロード可能 ACL リダイレクト URL	Filter-Id 属性[3] ダウンロード可能 ACL リダイレクト URL	Filter-Id 属性[3] ダウンロード可能 ACL[3] リダイレクト URL[3]
フォールバック方式としての Web 認証[5]	プロキシ ACL Filter-Id 属性[3] ダウンロード可能 ACL[3]	プロキシ ACL Filter-Id 属性[3] ダウンロード可能 ACL[3]	プロキシ ACL Filter-Id 属性[3] ダウンロード可能 ACL[3]	プロキシ ACL[3] Filter-Id 属性[3] ダウンロード可能 ACL[3]

1. MDA = マルチドメイン認証。
2. 「*multiauth*」とも呼ばれます。
3. Cisco IOS Release 12.2(50)SE 以降でサポートされます。
4. Cisco IOS Release 12.2(50)SE 以降でサポートされます。
5. 802.1X 認証をサポートしないクライアント用。

ユーザ単位 ACL と Filter-Id

Cisco IOS Release 12.2(50)SE よりも前のリリースでは、ユーザ単位 ACL と Filter-Id は、シングルホスト モードだけでサポートされていました。Cisco IOS Release 12.2(50) では、MDA 対応ポートおよびマルチ認証対応ポートに対するサポートが追加されました。12.2(52)SE 以降では、マルチ ホスト モードのポートに対するサポートが追加されました。

Cisco IOS Release 12.2(50)SE よりも前のリリースでは、スイッチで設定された ACL は、Catalyst 6000 スイッチなど、Cisco IOS ソフトウェアを実行する別の装置で設定された ACL と互換性がありませんでした。

Cisco IOS Release 12.2(50)SE 以降では、スイッチで設定された ACL は、Cisco IOS リリースを実行する他の装置と互換性があります。

（注） ACL で送信元として設定できるのは **any** だけです。

（注） マルチホスト モード用に設定されたすべての ACL では、ステートメントの送信元部分が *any* である必要があります（たとえば、**permit icmp** *any* **host 10.10.1.1**）。

定義されたすべての ACL の送信元ポートで *any* を指定する必要があります。それ以外の場合は、ACL を適用できず、認可は失敗します。シングル ホストは、下位互換性をサポートするための唯一の例外です。

MDA 対応ポートおよびマルチ認証ポートでは、複数のホストを認証できます。1 つのホストに適用された ACL ポリシーは、別のホストのトラフィックに影響を与えません。

マルチホスト ポートで 1 つのホストだけが認証され、他のホストは認証なしでネットワーク アクセスを取得する場合、送信元アドレスで *any* を指定することにより、最初のホストの ACL ポリシーを他の接続ホストに適用できます。

認証マネージャの CLI コマンド

認証マネージャのインターフェイス コンフィギュレーション コマンドは、802.1X、MAC 認証バイパス、Web 認証などのすべての認証方式を制御します。認証マネージャ コマンドは、接続したホストに適用される認証方式の優先順位と順序を決定します。

認証マネージャ コマンドは、ホスト モード、違反モード、認証タイマーなどの汎用的な認証機能を制御します。汎用の認証コマンドには、**authentication host-mode**、**authentication violation**、**authentication timer** などのインターフェイス コンフィギュレーション コマンドがあります。

802.1X に固有のコマンドは、**dot1x** というキーワードで始まります。たとえば、**authentication port-control auto** インターフェイス コンフィギュレーション コマンドは、インターフェイスでの認証をイネーブルにします。一方、**dot1x system-authentication control** グローバル コンフィギュレーション コマンドは、802.1X 認証をグローバルにだけイネーブルまたはディセーブルにします。

（注）　802.1X 認証をグローバルにディセーブルにした場合、Web 認証など、他の認証方式はそのポートでイネーブルのままになります。

認証マネージャ コマンドは、以前の 802.1X コマンドと同じ機能を提供します。

表 12-2　認証マネージャ コマンドと以前の 802.1X コマンド

Cisco IOS Release 12.2(50)SE 以降の認証マネージャ コマンド	Cisco IOS Release 12.2(46)SE 以前の相当する 802.1X コマンド	説明
authentication control-direction {both | in}	**dot1x control-direction {both | in}**	Wake-on-LAN（WoL）機能を含む認証をイネーブルにし、ポート制御を単一方向または双方向に設定します。
authentication event	**dot1x auth-fail vlan**	ポートで制限付き VLAN をイネーブルにします。
	dot1x critical (interface configuration)	アクセス不能認証バイパス機能をイネーブルにします。
	dot1x guest-vlan6	アクティブ VLAN をゲスト VLAN として指定します。
authentication fallback *fallback-profile*	**dot1x fallback** *fallback-profile*	認証をサポートしないクライアント用のフォールバック方式として Web 認証を使用するようにポートを設定します。
authentication host-mode [multi-auth | multi-domain | multi-host | single-host]	**dot1x host-mode {single-host | multi-host | multi-domain}**	認可ポート上で単一のホスト（クライアント）または複数のホストを許可します。
authentication order	**dot1x mac-auth-bypass**	使用する認証方式の順序を定義する柔軟性を提供します。
authentication periodic	**dot1x reauthentication**	クライアントの定期的な再認証をイネーブルにします。
authentication port-control {auto | force-authorized | force-un authorized}	**dot1x port-control {auto | force-authorized | force-unauthorized}**	ポートの認可ステートの手動制御をイネーブルにします。

表 12-2　認証マネージャ コマンドと以前の 802.1X コマンド （続き）

Cisco IOS Release 12.2(50)SE 以降の認証マネージャ コマンド	Cisco IOS Release 12.2(46)SE 以前の相当する 802.1X コマンド	説明
authentication timer	**dot1x timeout**	タイマーを設定します。
authentication violation {**protect** | **restrict** | **shutdown**}	**dot1x violation-mode** {**shutdown** | **restrict** | **protect**}	新しい装置がポートに接続した場合、または最大数の装置がポートに接続したあとに新しい装置がそのポートに接続した場合に発生する違反モードを設定します。

Cisco IOS Release 12.2(55)SE 以降、認証マネージャで生成された詳細なシステム メッセージをフィルタリングできるようになりました。フィルタリングされる内容は、通常、認証成功に関連しています。802.1X 認証および MAB 認証の詳細メッセージをフィルタリングすることもできます。認証方式ごとに異なるコマンドがあります。

- **no authentication logging verbose** グローバル コンフィギュレーション コマンドは、認証マネージャからの詳細メッセージをフィルタリングします。
- **no dot1x logging verbose** グローバル コンフィギュレーション コマンドは、802.1X 認証の詳細メッセージをフィルタリングします。
- **no mab logging verbose** グローバル コンフィギュレーション コマンドは、MAC Authentication Bypass（MAB; MAC 認証バイパス）の詳細メッセージをフィルタリングします。

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。

認可ステートおよび無認可ステートのポート

802.1X 認証中に、スイッチ ポートのステートに応じて、スイッチはクライアントにネットワークへのアクセスを許可できます。ポートは最初、*無認可*ステートです。このステートの間、音声 VLAN ポートとして設定されていないポートは、802.1X 認証、CDP、および STP のパケットを除くすべての入力トラフィックと出力トラフィックを禁止します。クライアントの認証が成功すると、ポートは*認可*ステートに変化し、クライアントのトラフィック送受信を通常どおりに許可します。ポートが音声 VLAN ポートとして設定されている場合、ポートはクライアントの認証が成功する前に、VoIP トラフィックおよび 802.1X プロトコル パケットを許可します。

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

一方、802.1X 対応のクライアントが、802.1X 標準を実行していないポートに接続すると、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。応答がなければ、クライアントは同じ要求を所定の回数だけ送信します。応答がないので、クライアントはポートが認可ステートであるものとしてフレーム送信を開始します。

authentication port-control または **dot1x port-control** インターフェイス コンフィギュレーション コマンドと次のキーワードを使用して、ポートの認可ステートを制御できます。

- **force-authorized**：802.1X 認証をディセーブルにし、認証情報の交換を必要とせずに、ポートを認可ステートに変化させます。ポートはクライアントの 802.1X ベース認証を行わずに、通常のトラフィックを送受信します。これは、デフォルト設定です。
- **force-unauthorized**：クライアントによる認証の試みをすべて無視し、ポートを無認可ステートのままにします。スイッチはポートを介してクライアントに認証サービスを提供できません。

- **auto**：802.1X 認証をイネーブルにします。ポートは最初、無認可ステートであり、ポート経由で送受信できるのは EAPOL フレームだけです。ポートのリンク ステートがダウンからアップに変化したとき、または EAPOL 開始フレームを受信したときに、認証プロセスが開始されます。スイッチは、クライアントの識別情報を要求し、クライアントと認証サーバとの間で認証メッセージのリレーを開始します。スイッチはクライアントの MAC アドレスを使用して、ネットワークへのアクセスを試みる各クライアントを一意に識別します。

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

クライアントはログオフするとき、EAPOL ログオフ メッセージを送信します。このメッセージにより、スイッチ ポートは無認可ステートに変化します。

ポートのリンク ステートがアップからダウンに変化した場合、または EAPOL ログオフ フレームを受信した場合に、ポートは無認可ステートに戻ります。

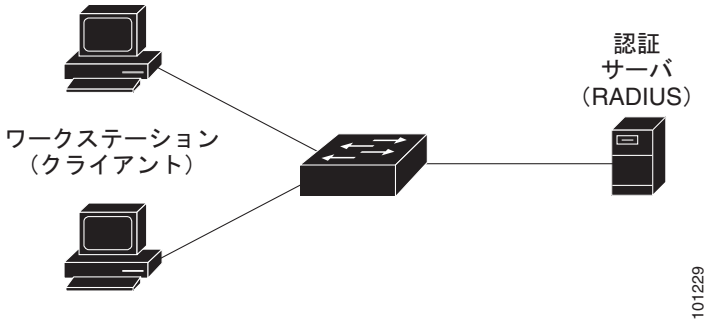
802.1X ホスト モード

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 12-1（P.12-2）を参照）では、1 つのクライアントだけを 802.1X 対応のスイッチ ポートに接続できます。スイッチは、ポートのリンク ステートがアップ ステートに変化したときに EAPOL フレームを送信することによりクライアントを検出します。クライアントがログオフした場合、または別のクライアントに代わった場合は、スイッチはポートのリンク ステートをダウンに変更し、ポートは無認可ステートに戻ります。

マルチホスト モードでは、単一の 802.1X 対応ポートに複数のホストを接続できます。図 12-5（P.12-11）に、ワイヤレス LAN における 802.1X ポートベースの認証を示します。このモードでは、すべてのクライアントにネットワーク アクセスを許可するために、接続されたホストのうちの 1 つを認証するだけで済みます。ポートが無認可ステートになった場合（再認証が失敗した場合、または EAPOL ログオフ メッセージを受信した場合）、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、ワイヤレス アクセス ポイントが接続先クライアントの認証を処理し、スイッチに対するクライアントとしての役割も果たします。

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

図 12-5　マルチ ホスト モードの例



スイッチはマルチドメイン認証（MDA）をサポートします。MDA により、データ装置と、IP Phone（シスコ製品またはシスコ以外の製品）などの音声装置の両方で、同じスイッチ ポートに接続することが可能になります。詳細については、「マルチドメイン認証」（P.12-12）を参照してください。

マルチドメイン認証

スイッチはマルチドメイン認証（MDA）をサポートします。MDA により、データ装置と、IP Phone（シスコ製品またはシスコ以外の製品）などの音声装置を、同じスイッチ ポートで認証できます。ポートは、データ ドメインと音声ドメインに分割されます。

MDA では、装置認証の順序は強制されません。ただし、最良の結果を得るために、MDA 対応ポートでは音声装置を認証してからデータ装置を認証することを推奨します。

MDA を設定するには、次の注意事項に従ってください。

- スイッチ ポートを MDA 用に設定するには、「ホスト モードの設定」（P.12-43）を参照してください。
- ホスト モードをマルチドメインに設定する場合、IP Phone 用に音声 VLAN を設定する必要があります。詳細については、第 16 章「VLAN の設定」を参照してください。
- 音声装置を認可するには、Cisco Attribute-Value（AV）ペア属性を値 `device-traffic-class=voice` で送信するように AAA サーバを設定する必要があります。この値がない場合、スイッチは音声装置をデータ装置として扱います。
- ゲスト VLAN 機能および制限付き VLAN 機能は、MDA 対応ポートのデータ装置にだけ適用されます。スイッチは、認可に失敗した音声装置をデータ装置として扱います。
- 複数の装置がポートの音声ドメインまたはデータ ドメインで認可を試みた場合、errdisable になります。
- 装置が認可されるまで、ポートはトラフィックを廃棄します。シスコ製品ではない IP Phone または音声装置は、データ VLAN および音声 VLAN への接続を許可されます。データ VLAN では、音声装置が Dynamic Host Configuration Protocol（DHCP）サーバに接続して IP アドレスを取得し、音声 VLAN 情報を入手できます。音声装置が音声 VLAN 上での送信を開始すると、データ VLAN へのアクセスはブロックされます。
- データ VLAN でバインドしている音声装置の MAC アドレスは、ポート セキュリティの MAC アドレス制限にカウントされません。
- MDA では、MAC 認証バイパスをフォールバック メカニズムとして使用して、スイッチ ポートに 802.1X 認証をサポートしない装置を接続させることができます。詳細については、「MAC 認証バイパス」（P.12-36）を参照してください。
- ポートで*データ*装置または*音声*装置が検出された場合、その装置の MAC アドレスは、認可が成功するまでブロックされます。認可が失敗した場合、MAC アドレスは 5 分間ブロックされたままになります。
- ポートが無認可ステートの間に*データ* VLAN で 6 つ以上の装置が検出された場合、または*音声* VLAN で 2 つ以上の音声装置が検出された場合、ポートは errdisable になります。
- ポートのホスト モードがシングルホスト モードまたはマルチホスト モードからマルチドメイン モードに変化した場合、認可されたデータ装置は、ポートで認可されたままになります。ただし、ポートの音声 VLAN 上の Cisco IP Phone は、自動的に削除され、そのポートで再認証する必要があります。
- ゲスト VLAN や制限付き VLAN などのアクティブなフォールバック メカニズムは、ポートがシングルホスト モードまたはマルチホスト モードからマルチドメイン モードに変化したあとも設定されたままになります。

- ポートのホスト モードをマルチドメイン モードからシングルホスト モードまたはマルチホスト モードに切り替えると、認可されたすべての装置がポートから削除されます。
- データ ドメインを最初に認可し、ゲスト VLAN に配置した場合、802.1X に対応していない音声装置は、音声 VLAN 上でパケットをタグ付けして認証を開始する必要があります。IP Phone では、タグ付けされたトラフィックを送信する必要はありません（802.1X 対応の IP Phone でも同じです）。
- MDA 対応ポートでユーザ単位 ACL を使用することは推奨できません。ユーザ単位 ACL ポリシーを持つ認可された装置は、ポートの音声 VLAN とデータ VLAN の両方のトラフィックに影響を与える可能性があります。ユーザ単位 ACL を強制するためにポートで使用できる装置は 1 つだけです。

詳細については、「ホスト モードの設定」（P.12-43）を参照してください。

802.1X マルチ認証モード

マルチ認証（multiauth）モードでは、データ VLAN 上で複数の認証済みクライアントを許可できます。各ホストは個別に認証されます。音声 VLAN が設定されている場合、このモードでは音声 VLAN 上でも 1 つのクライアントが許可されます（ポートが追加の音声クライアントを検出した場合、それらの音声クライアントはポートから破棄されますが、違反エラーは発生しません）。

ハブまたはアクセス ポイントが 802.1X 対応ポートに接続されている場合、接続されている各クライアントを認証する必要があります。

802.1X に対応していない装置に対し、MAC 認証バイパスまたは Web 認証をホスト単位の認証フォールバック方式として使用して、1 つのポートで異なるホストを異なる方式により認証することができます。

マルチ認証ポートで認証できるデータ ホストの数に制限はありません。ただし、音声 VLAN が設定されている場合、許可される音声装置は 1 つだけです。ホスト制限が定義されておらず、違反がトリガーされないので、第 2 の音声装置が確認された場合、その装置は自動的に破棄されますが、違反はトリガーされません。

音声 VLAN 上で MDA 機能を実現するために、マルチ認証モードでは、認証サーバから受信した Vendor-Specific Attribute（VSA; ベンダー固有属性）に応じて、認証された装置がデータ VLAN または音声 VLAN に割り当てられます。

（注） ポートがマルチ認証モードの場合、ゲスト VLAN および認証失敗 VLAN の各機能は、アクティブになりません。

クリティカル認証モードとクリティカル VLAN の詳細については、「802.1X 認証とアクセス不能認証バイパス」（P.12-23）を参照してください。

ポートでのマルチ認証モードの設定の詳細については、「ホスト モードの設定」（P.12-43）を参照してください。

MAC 移行

1 つのスイッチ ポートで MAC アドレスを認証しても、そのアドレスは、そのスイッチの別の認証マネージャ対応ポートでは許可されません。スイッチが同じ MAC アドレスを別の認証マネージャ対応ポートで検出した場合、そのアドレスは許可されません。

状況によっては、MAC アドレスを同じスイッチのあるポートから別のポートに移行する必要があります。たとえば、認証されたホストとスイッチ ポートの間に別の装置（ハブまたは IP Phone など）がある場合、そのホストを装置から接続解除し、同じスイッチの別のポートに直接接続することがあります。

装置が新しいポートで再認証されるように、MAC 移行をグローバルにイネーブルにすることができます。ホストが第 2 のポートに移行すると、最初のポートのセッションは削除され、新しいポートでホストが再認証されます。

MAC 移行は、すべてのホスト モードでサポートされます（認証されたホストは、ポートでイネーブルになっているホスト モードに関係なく、スイッチの任意のポートに移行できます）。

Cisco IOS Release 12.2(55)SE 以降、MAC 移行はポート セキュリティと共にすべてのホスト モードで設定できます。

あるポートから別のポートに MAC アドレスを移行すると、スイッチは元のポートでの認証済みセッションを終了し、新しいポートで新しい認証シーケンスを開始します。ポート セキュリティの動作は、MAC 移行を設定したときと同じです。

MAC 移行機能は、音声ホストとデータホストの両方に適用されます。

（注）　オープン認証モードでは、MAC アドレスは元のポートから新しいポートにすぐに移行され、新しいポートでの認証を必要としません。

詳細については、「MAC 移行のイネーブル化」（P.12-49）を参照してください。

MAC 置き換え

Cisco IOS Release 12.2(55)SE 以降、ホストが、別のホストが既に認証しているポートに接続を試行したときに発生する違反に対処するため、MAC 置き換え機能を設定できるようになりました。

（注）　マルチ認証モードでは違反がトリガーされないため、この機能はマルチ認証モードのポートには適用されません。マルチ ホスト モードでは最初のホストだけが認証を必要とするため、この機能はマルチ ホスト モードのポートには適用されません。

authentication violation インターフェイス コンフィギュレーション コマンドに **replace** キーワードを指定して設定した場合、マルチドメイン モードのポートでの認証プロセスは、次のようになります。

- 新しい MAC アドレスが既存の認証済み MAC アドレスのポートで受信されます。
- 認証マネージャが、ポート上の現行データ ホストの MAC アドレスを新しい MAC アドレスで置き換えます。
- 認証マネージャが新しい MAC アドレスの認証プロセスを開始します。
- 認証マネージャが、新しいホストが音声ホストであると判断した場合、元の音声ホストが削除されます。

ポートがオープン認証モードの場合、新しい MAC アドレスはすべて、MAC アドレス テーブルにすぐに追加されます。

詳細については、「MAC 置き換えのイネーブル化」（P.12-49）を参照してください。

802.1X アカウンティング

802.1X 標準は、ネットワーク アクセスに対するユーザの認可方法および認証方法を定義しますが、ネットワークの使用状況を追跡しません。802.1X アカウンティングは、デフォルトでディセーブルになっています。802.1X アカウンティングをイネーブルにすると、802.1X 対応ポートで次のアクティビティをモニタできます。

- ユーザ認証の成功
- ユーザのログオフ
- リンクダウンの発生
- 再認証の成功
- 再認証の失敗

スイッチは 802.1X アカウンティングの情報を記録しません。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されている必要があります。

802.1X アカウンティングの Attribute-Value ペア

RADIUS サーバに送信される情報は、Attribute-Value（AV）ペアの形式で表されます。これらの AV ペアは、さまざまなアプリケーションにデータを提供します（たとえば、課金アプリケーションでは、RADIUS パケットの Acct-Input-Octets 属性または Acct-Output-Octets 属性の情報が必要になることがあります）。

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

- START：新しいユーザ セッションの開始時に送信されます。
- INTERIM：既存のセッション中に更新のために送信されます。
- STOP：セッションの終了時に送信されます。

表 12-3 に、AV ペアと、それらのペアがスイッチによって送信されるタイミングを示します。

表 12-3　アカウンティングの AV ペア

属性番号	AV ペア名	START	INTERIM	STOP
属性 [1]	User-Name	常に送信	常に送信	常に送信
属性 [4]	NAS-IP-Address	常に送信	常に送信	常に送信
属性 [5]	NAS-Port	常に送信	常に送信	常に送信
属性 [8]	Framed-IP-Address	送信なし	一部送信[1]	一部送信[1]
属性 [25]	Class	常に送信	常に送信	常に送信
属性 [30]	Called-Station-ID	常に送信	常に送信	常に送信
属性 [31]	Calling-Station-ID	常に送信	常に送信	常に送信
属性 [40]	Acct-Status-Type	常に送信	常に送信	常に送信
属性 [41]	Acct-Delay-Time	常に送信	常に送信	常に送信
属性 [42]	Acct-Input-Octets	送信なし	常に送信	常に送信
属性 [43]	Acct-Output-Octets	送信なし	常に送信	常に送信
属性 [44]	Acct-Session-ID	常に送信	常に送信	常に送信

表 12-3　アカウンティングの AV ペア （続き）

属性番号	AV ペア名	START	INTERIM	STOP
属性 [45]	Acct-Authentic	常に送信	常に送信	常に送信
属性 [46]	Acct-Session-Time	送信なし	常に送信	常に送信
属性 [49]	Acct-Terminate-Cause	送信なし	送信なし	常に送信
属性 [61]	NAS-Port-Type	常に送信	常に送信	常に送信

1. Framed-IP-Address 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 テーブルに存在する場合にだけ送信されます。

スイッチによって送信されている AV ペアを表示するには、**debug radius accounting** 特権 EXEC コマンドを入力します。このコマンドの詳細については、『*Cisco IOS Debug Command Reference, Release 12.2*』を参照してください。
http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/products_command_reference_book09186a00800872ce.html

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

802.1X 準備状態チェック

802.1X 準備状態チェックでは、すべてのスイッチ ポートでの 802.1X アクティビティをモニタし、802.1X をサポートするポートに接続された装置に関する情報を表示します。この機能を使用して、スイッチ ポートに接続された装置が 802.1X に対応しているかどうかを判断できます。802.1X 機能をサポートしない装置に対しては、MAC 認証バイパスや Web 認証などの代替認証を使用します。

この機能は、クライアント上のサプリカントが NOTIFY EAP 通知パケットによるクエリーをサポートする場合にだけ機能します。クライアントは、802.1X のタイムアウト値以内に応答する必要があります。

スイッチを 802.1X 準備状態チェック用に設定する方法の詳細については、「802.1X 準備状態チェックの設定」（P.12-37）を参照してください。

802.1X 認証と VLAN 割り当て

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、ユーザ名と VLAN のマッピングを維持し、スイッチ ポートに接続しているクライアントのユーザ名に基づいて VLAN を割り当てます。この機能を使用して、特定のユーザのネットワーク アクセスを制限できます。

音声装置が認可され、RADIUS サーバが認可済みの VLAN を返した場合、ポート上の音声 VLAN は、割り当てられた音声 VLAN でパケットを送受信するように設定されます。マルチドメイン認証（MDA）対応ポートでは、音声 VLAN の割り当ては、データ VLAN の割り当てと同じように行われます。詳細については、「マルチドメイン認証」（P.12-12）を参照してください。

スイッチと RADIUS サーバで設定されている場合、802.1X 認証と VLAN 割り当てには次のような特徴があります。

- RADIUS サーバが VLAN を提供していないか、または 802.1X 認証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 で設定されます。アクセス VLAN とは、アクセス ポートに割り当てられた VLAN です。このポート上で送受信されるすべてのパケットは、この VLAN に属します。
- 802.1X 認証がイネーブルになっているが、RADIUS サーバからの VLAN 情報が有効ではない場合、認可は失敗し、設定された VLAN は使用されたままになります。これにより、設定エラーによってポートが不適切な VLAN に予期せず表示されるのを防ぎます。

  設定エラーには、ルーテッド ポートへの VLAN、形式に誤りのある VLAN ID、存在しないまたは内部の（ルーテッド ポート）VLAN ID、RSPAN VLAN、シャット ダウンまたは停止している VLAN の指定などがあります。マルチドメイン ホスト ポートの場合、設定エラーは、設定済みまたは割り当て済みの音声 VLAN ID と一致するデータ VLAN の割り当て（またはその逆）を試みることによって発生することもあります。
- 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、認可された装置は認証後に指定した VLAN に配置されます。
- 802.1X ポートでマルチホスト モードがイネーブルの場合、すべてのホストは最初に認証されたホストと同じ VLAN（RADIUS サーバによって指定されます）に配置されます。
- ポート セキュリティをイネーブルにしても、RADIUS サーバによって割り当てられた VLAN の動作に影響はありません。
- 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 と設定済みの音声 VLAN に戻ります。
- 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 アクセス VLAN 設定への変更は有効になりません。マルチドメイン ホストの場合、ポートが完全に認可されていれば、同じことが音声装置に当てはまります。ただし、次の例外があります。
  - 一方の装置の VLAN 設定変更により、他方の装置が設定済みまたは割り当て済みの VLAN と一致した場合、ポート上のすべての装置の認可は中止され、マルチドメイン ホスト モードは、データ装置が設定された VLAN と音声装置が設定された VLAN が一致しない有効な設定が復元されるまで無効になります。
  - 音声装置が認可され、ダウンロードされた音声 VLAN を使用している場合、音声 VLAN 設定を削除するか、設定値を *dot1p* または *untagged* に変更すると、音声装置は無認可になり、マルチドメイン ホスト モードはディセーブルになります。

ポートが強制認可、強制無認可、無認可、シャットダウンのいずれかのステートの場合、そのポートは設定済みのアクセス VLAN に配置されます。

VLAN 割り当て機能付きの 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 認可をイネーブルにし、RADIUS サーバからのインターフェイス コンフィギュレーションを許可します。
- 802.1X 認証をイネーブルにします（VLAN 割り当て機能は、アクセス ポートで 802.1X 認証を設定す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属性を割り当てます。RADIUS サーバは次の属性をスイッチに返す必要があります。
  - [64] Tunnel-Type = VLAN
  - [65] Tunnel-Medium-Type = 802

- [81] Tunnel-Private-Group-ID = VLAN 名、VLAN ID、または VLAN-Group
- [83] Tunnel-Preference

属性 [64] は、値 *VLAN*（type 13）を含んでいる必要があります。属性 [65] は、値 *802*（type 6）を含んでいる必要があります。属性 [81] 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。

トンネル属性の例については、「ベンダー固有の RADIUS 属性を使用するためのスイッチの設定」（P.11-34）を参照してください。

802.1X 認証とユーザ単位 ACL の使用

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 認証ユーザに異なるレベルのネットワーク アクセスおよびサービスを提供できます。RADIUS サーバは、802.1X ポートに接続したユーザを認証するときに、ユーザの識別情報に基づいて ACL 属性を取得し、それらをスイッチに送信します。スイッチは、ユーザ セッション中に、それらの属性を 802.1X ポートに適用します。スイッチは、セッションが終了したとき、認証が失敗したとき、またはリンクダウン状態が発生したときに、ユーザ単位 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。ポートが無認可の場合、スイッチはそのポートから ACL を削除します。

同じスイッチ上で、ルータ ACL と入力ポート ACL を設定できます。ただし、ポート ACL はルータ ACL よりも優先されます。VLAN に属するインターフェイスに入力ポート ACL を適用した場合、そのポート ACL は、VLAN インターフェイスに適用された入力ルータ ACL よりも優先されます。ポート ACL が適用されたポートで受信された着信パケットは、ポート ACL によってフィルタリングされます。他のポートで受信された着信のルーティング パケットは、ルータ ACL によってフィルタリングされます。発信のルーティング パケットは、ルータ ACL によってフィルタリングされます。設定の競合を回避するには、RADIUS サーバに格納されるユーザ プロファイルを慎重に計画する必要があります。

RADIUS は、ベンダー固有属性などのユーザ単位属性をサポートします。これらのベンダー固有属性（VSA）は、オクテット ストリング形式になっており、認証プロセス中にスイッチに渡されます。ユーザ単位 ACL に使用する VSA は、入力方向では `inacl#<n>`、出力方向では `outacl#<n>` です。MAC ACL は、入力方向だけでサポートされます。このスイッチは、入力方向でだけ 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 38 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 構文スタイルだけを使用して、RADIUS サーバに格納されるユーザ単位設定を定義します。RADIUS サーバから定義が渡される場合、それらの定義は、拡張命名規則を使用して作成されます。ただし、Filter-Id 属性を使用する場合、標準 ACL を示すことができます。

Filter-Id 属性を使用して、すでにスイッチで設定されている着信 ACL または発信 ACL を指定できます。属性には、ACL 番号と、そのあとに入力フィルタリングを示す *.in* または出力フィルタリングを示す *.out* が含まれています。RADIUS サーバが *.in* または *.out* の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 リストのサポートが制限されているので、Filter-Id 属性は番号が 1 ～ 199 および 1300 ～ 2699 の IP ACL（IP 標準 ACL と IP 拡張 ACL）だけでサポートされています。

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

ベンダー固有属性の例については、「ベンダー固有の RADIUS 属性を使用するためのスイッチの設定」（P.11-34）を参照してください。ACL の設定の詳細については、第 38 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。

（注）　ユーザ単位 ACL は、シングルホスト モードだけでサポートされます。

ユーザ単位 ACL を設定するには、次の作業を実行する必要があります。

- AAA 認証をイネーブルにします。
- **network** キーワードを使用して AAA 認可をイネーブルにし、RADIUS サーバからのインターフェイス コンフィギュレーションを許可します。
- 802.1X 認証をイネーブルにします。
- RADIUS サーバでユーザ プロファイルと VSA を設定します。
- 802.1X ポートをシングルホスト モード用に設定します。

設定の詳細については、「認証マネージャ」（P.12-7）を参照してください。

802.1X 認証とダウンロード可能 ACL およびリダイレクト URL

ホストの 802.1X 認証または MAC 認証バイパス中に、ACL をダウンロードし、URL を RADIUS サーバからスイッチにリダイレクトすることができます。また、Web 認証中に ACL をダウンロードすることもできます。

（注）　ダウンロード可能 ACL は、*dACL* とも呼ばれます。

複数のホストが認証され、ホストがシングル ホスト モード、MDA モード、またはマルチ認証モードである場合、スイッチは ACL の送信元アドレスをホスト IP アドレスに変更します。

802.1X 対応ポートに接続されているすべての装置に、ACL およびリダイレクト URL を適用できます。

802.1X 認証中に ACL がダウンロードされない場合、スイッチはスタティックなデフォルト ACL をホストへのポートに適用します。マルチ認証モードまたは MDA モードで設定されている音声 VLAN ポートでは、スイッチは認証ポリシーの一部として、電話にだけ ACL を適用します。

Cisco IOS Release 12.2(55)SE 以降、ポートにスタティックな ACL がない場合、動的な auth-default-ACL が作成され、dACL がダウンロードされて適用される前にポリシーが強制されます。

（注）　auth-default-ACL は、実行コンフィギュレーションには出現しません。

auth-default-ACL は、認証ポリシーが設定されているホストが 1 台以上、ポートで検出されたときに作成されます。auth-default-ACL は、最後の認証済みセッションが終了すると、ポートから削除されます。auth-default-ACL は、**ip access-list extended auth-default-acl** 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設定できます。

（注）　auth-default-ACL では、シングル ホスト モードでの Cisco Discovery Protocol（CDP）バイパスはサポートされません。CDP バイパスをサポートするには、インターフェイスにスタティックな ACL を設定する必要があります。

802.1X および MAB 認証方式では、*オープン*と*クローズド*の 2 つの認証方式がサポートされます。*クローズド*認証モードで、ポートにスタティックな ACL がない場合、次のようになります。

- auth-default-ACL が作成されます。
- ポリシーが強制されるまで、auth-default-ACL によって、DHCP トラフィックだけが許可されます。
- 最初のホストが認証を行うと、IP アドレス挿入なしで認証ポリシーが適用されます。

- 別のホストが検出されると、最初のホストのポリシーがリフレッシュされ、最初と後続のセッションのポリシーが IP アドレス挿入ありで強制されます。

*オープン*認証モードで、ポートにスタティックな ACL がない場合、以下のようになります。

- auth-default-ACL-OPEN が作成され、すべてのトラフィックを許可します。
- セキュリティ違反を防ぐために、ポリシーが IP アドレス挿入ありで強制されます。
- Web 認証は、auth-default-ACL-OPEN の対象です。

認証ポリシーがないホストのアクセスを制御するために、ディレクティブを設定できます。ディレクティブとしてサポートされる値は、*open* および *default* です。*open* ディレクティブを設定すると、すべてのトラフィックが許可されます。*default* ディレクティブでは、トラフィックは、ポートが提供するアクセスの対象になります。ディレクティブは、AAA サーバのユーザ プロファイルまたはスイッチで設定できます。AAA サーバでディレクティブを設定するには、**authz-directive =<open/default>** グローバル コマンドを使用します。スイッチでディレクティブを設定するには、**epm access-control open** 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。

（注） ディレクティブのデフォルト値は、*default* です。

設定済みの ACL がないポートで、ホストが Web 認証にフォールバックした場合は、次のようになります。

- ポートがオープン認証モードの場合、auth-default-ACL-OPEN が作成されます。
- ポートがクローズド認証モードの場合、auth-default-ACL が作成されます。

フォールバック ACL の Access Control Entry（ACE; アクセス コントロール エントリ）が、ユーザ単位のエントリに変換されます。構成済みのフォールバック プロファイルにフォールバック ACL が含まれていない場合、ホストは、ポートに関連付けられた auth-default-ACL の対象になります。

（注） Web 認証でカスタム ロゴを使用していて、これが外部サーバに格納されている場合、ポート ACL によって、認証前にこの外部サーバへのアクセスを許可する必要があります。外部サーバへの適切なアクセスを提供するには、スタティックなポート ACL を設定するか、auth-default-ACL を変更する必要があります。

リダイレクト URL 用の Cisco Secure ACS および Attribute-Value ペア

このスイッチは、次の *cisco-av-pair* VSA を使用します。

- url-redirect は、HTTP から HTTPS への URL です。
- url-redirect-acl は、スイッチの ACL 名または番号です。

スイッチは、CiscoSecure-Defined-ACL の属性と値のペアを使用して、エンド ポイント装置からの HTTP 要求または HTTPS 要求を代行受信します。次に、スイッチはクライアントの Web ブラウザを指定されたリダイレクト アドレスに転送します。Cisco Secure Access Control Server（ACS）の url-redirect の属性と値のペアには、Web ブラウザのリダイレクト先となる URL が含まれます。url-redirect-acl の属性と値のペアには、リダイレクトする HTTP トラフィックまたは HTTPS トラフィックを指定する ACL の名前または番号が含まれます。ACL 内の許可 ACE に一致するトラフィックはリダイレクトされます。

（注） URL リダイレクト ACL とデフォルト ポート ACL をスイッチで定義します。

リダイレクト URL が認証サーバ上でクライアントに対して設定されている場合、接続されているクライアントのスイッチ ポートのデフォルト ポート ACL も設定する必要があります。

ダウンロード可能 ACL 用の Cisco Secure ACS および Attribute-Value ペア

Cisco Secure ACS で RADIUS cisco-av-pair ベンダー固有属性（VSA）により CiscoSecure-Defined-ACL Attribute-Value ペアを設定できます。このペアは、#ACL#-IP-name-number 属性により、Cisco Secure ACS 上のダウンロード可能 ACL の名前を指定します。

- *name* は ACL 名です。
- *number* はバージョン番号です（たとえば、3f783768）。

ダウンロード可能 ACL が認証サーバ上でクライアントに対して設定されている場合、接続されているクライアントのスイッチ ポートのデフォルト ポート ACL も設定する必要があります。

スイッチでデフォルト ACL を設定している場合に、Cisco Secure ACS がホスト アクセス ポリシーをスイッチに送信すると、スイッチはスイッチ ポートに接続されたホストからのトラフィックに対し、このポリシーを適用します。ポリシーがトラフィックに適用されない場合は、スイッチはデフォルトの ACL を適用します。Cisco Secure ACS がスイッチにダウンロード可能 ACL を送信した場合、この ACL は、スイッチ ポートで設定されているデフォルト ACL よりも優先されます。ただし、スイッチが Cisco Secure ACS からホスト アクセス ポリシーを受信した場合に、デフォルト ACL が設定されていないと、認可の失敗が宣言されます。

設定の詳細については、「認証マネージャ」（P.12-7）および「802.1X 認証とダウンロード可能 ACL およびリダイレクト URL の設定」（P.12-61）を参照してください。

VLAN ID ベースの MAC 認証

ダウンロード可能な VLAN ではなく、スタティックな VLAN ID に基づいてホストを認証する場合は、VLAN ID ベースの MAC 認証を使用できます。スイッチでスタティックな VLAN ポリシーが設定されている場合、認証用に VLAN 情報が各ホストの MAC アドレスとともに Internet Authentication Service（IAS; インターネット認証サービス）（Microsoft）RADIUS サーバに送信されます。接続ポートで設定されている VLAN ID が、MAC 認証に使用されます。VLAN ID ベースの MAC 認証を ISA サーバとともに使用することで、固定数の VLAN をネットワーク内で使用できます。

この機能は、STP によりモニタおよび処理される VLAN の数も制限します。ネットワークは、固定 VLAN として管理できます。

（注）　この機能は、Cisco ACS Server ではサポートされていません（ACS サーバは、新しいホスト用に送信された VLAN ID を無視し、MAC アドレスに基づいた認証だけを行います）。

設定の詳細については、「VLAN ID ベースの MAC 認証の設定」（P.12-64）を参照してください。その他の設定は、「MAC 認証バイパスの設定」（P.12-57）で説明している MAC 認証バイパスに似ています。

802.1X 認証とゲスト VLAN

スイッチの各 802.1X ポートにゲスト VLAN を設定して、802.1X クライアントのダウンロードなどの限られたサービスをクライアントに提供できます。これらのクライアントは、802.1X 認証のためにシステムをアップグレードしている可能性があり、Windows 98 システムなどの一部のホストは、802.1X に対応していない可能性があります。

802.1X ポートでゲスト VLAN をイネーブルにすると、スイッチは EAP 要求/アイデンティティ フレームに対する応答を受信しないとき、または EAPOL パケットがクライアントによって送信されないときに、クライアントをゲスト VLAN に割り当てます。

スイッチは、EAPOL パケット履歴を保持します。リンクの存続時間中に EAPOL パケットがインターフェイスで検出された場合、スイッチは、そのインターフェイスに接続されている装置が 802.1X 対応サプリカントであると判断し、インターフェイスはゲスト VLAN ステートに変更されません。インターフェイスのリンク ステータスがダウンになった場合、EAPOL 履歴は消去されます。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。

装置がリンクの存続時間中に EAPOL パケットをスイッチに送信した場合、スイッチは認証に失敗したクライアントがゲスト VLAN にアクセスできないようにします。

スイッチが 802.1X 対応の音声装置を認可しようとしていて、AAA サーバが使用不可の場合、認可の試みは失敗しますが、EAPOL パケットが検出されたことは EAPOL 履歴に保存されます。AAA サーバが使用可能になると、スイッチは音声装置を認可します。ただし、スイッチは他の装置がゲスト VLAN にアクセスするのを許可しなくなります。この状態を避けるには、次のいずれかのコマンド シーケンスを使用します。

- **dot1x guest-vlan supplicant** グローバル コンフィギュレーション コマンドを入力して、ゲスト VLAN へのアクセスを許可します。
- **shutdown** インターフェイス コンフィギュレーション コマンドを入力し、さらに **no shutdown** インターフェイス コンフィギュレーション コマンドを入力してポートを再起動します。

（注） インターフェイスがゲスト VLAN に変更されたあとで EAPOL パケットが検出された場合、インターフェイスは無認可ステートに戻り、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、任意の数の 802.1X 非対応クライアントがアクセスを許可されます。802.1X 対応クライアントが、ゲスト VLAN が設定されているポートと同じポートに加わると、そのポートはユーザ設定アクセス VLAN で無認可ステートに移行し、認証が再開されます。

ゲスト VLAN は、シングルホスト モードまたはマルチホスト モードの 802.1X ポート上でサポートされます。

RSPAN VLAN、プライベート VLAN、または音声 VLAN 以外の任意のアクティブ VLAN を、802.1X のゲスト VLAN として設定できます。ゲスト VLAN の機能は、内部 VLAN（ルーテッド ポート）またはトランク ポート上ではサポートされません。サポートされるのはアクセス ポートだけです。

スイッチは、*MAC 認証バイパス*をサポートします。MAC 認証バイパスが 802.1X ポートでイネーブルになっている場合、EAPOL メッセージ交換の待機中に 802.1X 認証が時間切れになると、スイッチはクライアントの MAC アドレスに基づいてクライアントを認可できます。スイッチは、802.1X ポート上のクライアントを検出したあとで、クライアントからのイーサネット パケットを待機します。スイッチは、MAC アドレスに基づいたユーザ名およびパスワードを持つ RADIUS-access/request フレームを認証サーバに送信します。認証に成功すると、スイッチはクライアントにネットワークへのアクセスを許可します。認証に失敗すると、スイッチはポートにゲスト VLAN を割り当てます（指定されていない場合）。詳細については、「802.1X 認証と MAC 認証バイパス」（P.12-27）を参照してください。

詳細については、「ゲスト VLAN の設定」（P.12-51）を参照してください。

802.1X 認証と制限付き VLAN

スイッチ上の 802.1X ポートごとに制限付き VLAN（*認証失敗 VLAN* とも呼ばれます）を設定して、ゲスト VLAN にアクセスできないクライアントに限られたサービスを提供できます。これらのクライアントは、802.1X に準拠しており、認証プロセスに失敗するので別の VLAN にアクセスできません。制限付き VLAN により、認証サーバ内に有効なクレデンシャルがないユーザ（通常は企業への訪問者）が、一連の限られたサービスにアクセスできるようになります。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 の両方のタイプのユーザに同じサービスを提供する場合、1 つの VLAN をゲスト VLAN と制限付き VLAN の両方として設定できます。

この機能がなければ、クライアントは認証の試行と失敗を無制限に繰り返し、スイッチ ポートはスパニング ツリー ブロッキング ステートのままになります。この機能を使用すると、認証が指定回数（デフォルト値は 3 回）試行されたあとで、スイッチ ポートを制限付き VLAN に移行できます。

オーセンティケータが、クライアントの失敗した認証試行の回数をカウントします。このカウントが設定された最大認証試行回数を超えると、ポートは制限付き VLAN に移行します。失敗した試行のカウントは、RADIUS サーバが *EAP 失敗*または EAP パケットを含まない空の応答により応答した場合に増加します。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、次の再認証が試行されるまで制限付き VLAN に残ります。制限付き VLAN 内のポートは、設定された間隔（デフォルトは 60 秒）で再認証を試みます。再認証が失敗した場合、ポートは制限付き VLAN に残ります。再認証が成功した場合、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た VLAN に移行します。再認証はディセーブルにすることができます。その場合、再認証プロセスが再開されるのは、ポートが *リンクダウン*イベントまたは *EAP ログオフ*イベントを受信した場合だけです。クライアントがハブを介して接続する可能性がある場合は、再認証をイネーブルのままにすることを推奨します。クライアントがハブから接続解除されたときに、ポートは *リンクダウン*イベントまたは *EAP ログオフ*イベントを受信しない可能性があります。

ポートが制限付き VLAN に移行したあと、シミュレートされた EAP 成功メッセージがクライアントに送信されます。これにより、クライアントが認証を無制限に試みるのを防ぎます。一部のクライアント（たとえば、Windows XP を実行する装置）は、EAP 成功なしでは 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 802.1X ポートおよびレイヤ 2 ポートだけでサポートされます。

RSPAN VLAN、プライマリ プライベート VLAN、または音声 VLAN 以外の任意のアクティブ VLAN を、802.1X の制限付き VLAN として設定できます。制限付き VLAN の機能は、内部 VLAN（ルーテッド ポート）またはトランク ポート上ではサポートされません。サポートされるのはアクセス ポートだけです。

この機能は、ポート セキュリティと連動します。ポートが認可されるとすぐに、MAC アドレスがポート セキュリティに提供されます。ポート セキュリティで MAC アドレスが許可されない場合、またはセキュア アドレス カウントの最大数に達した場合、ポートは無認可ステートおよび errdisable になります。

ダイナミック Address Resolution Protocol（ARP; アドレス解決プロトコル）検査、DHCP スヌーピング、IP ソース ガードなどのその他のポート セキュリティ機能は、制限付き VLAN 上で個別に設定できます。

詳細については、「制限付き VLAN の設定」（P.12-52）を参照してください。

802.1X 認証とアクセス不能認証バイパス

スイッチが設定された RADIUS サーバに到達できず、新しいホストを認証できない場合は、*クリティカル認証*または *AAA 失敗ポリシー*とも呼ばれるアクセス不能認証バイパス機能を使用します。それらのホストを *クリティカル ポート*に接続するようにスイッチを設定できます。

新しいホストがクリティカル ポートへの接続を試みると、そのホストはユーザ指定のアクセス VLAN である *クリティカル VLAN* に移行します。管理者は、限られた認証をホストに与えます。

クリティカル ポートに接続されたホストを認証するとき、スイッチは設定された RADIUS サーバのステータスを確認します。サーバが使用可能な場合、スイッチはホストを認証できます。ただし、すべての RADIUS サーバが使用不可の場合、スイッチはネットワーク アクセスをホストに許可し、ポートを認証ステートの特別なケースである *critical-authentication* ステートに置きます。

マルチ認証ポートでのサポート

マルチ認証（multiauth）ポートでアクセス不能バイパスをサポートするには、**authentication event server dead action reinitialize vlan** *vlan-id* を使用します。新しいホストがクリティカル ポートへの接続を試みると、そのポートが再初期化され、接続しているすべてのホストがユーザ指定のアクセス VLAN に移行します。

authentication event server dead action reinitialize vlan *vlan-id* インターフェイス コンフィギュレーション コマンドは、すべてのホスト モードでサポートされます。

認証結果

アクセス不能認証バイパス機能の動作は、ポートの認可ステートによって異なります。

- クリティカル ポートに接続されたホストが認証を試行したときにポートが無認可で、すべてのサーバが使用不可の場合、スイッチはポートを RADIUS 設定またはユーザ指定のアクセス VLAN で critical-authentication ステートに置きます。
- ポートがすでに認可されていて、再認証が発生した場合、スイッチはクリティカル ポートを現在の VLAN で critical-authentication ステートに置きます。この VLAN は、RADIUS サーバによって事前に割り当てられたものである可能性があります。
- 認証交換中に RADIUS サーバが使用不可になった場合、現在の交換は時間切れとなり、スイッチは次回の認証試行時にクリティカル ポートを critical-authentication ステートに置きます。

RADIUS サーバが再び使用可能になったときにホストを再初期化し、それらのホストをクリティカル VLAN から移行するように、クリティカル ポートを設定できます。このように設定した場合、critical-authentication ステートのすべてのクリティカル ポートは、自動的に再認証されます。詳細については、このリリースのコマンド リファレンスと、「アクセス不能認証バイパス機能の設定」（P.12-54）を参照してください。

機能の相互作用

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 802.1X ポートでイネーブルになっている場合、これら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 サーバが使用可能な場合、スイッチは、EAP 要求/アイデンティティ フレームに対する応答を受信しないとき、または EAPOL パケットがクライアントによって送信されないときに、クライアントをゲスト VLAN に割り当てます。
  - すべての RADIUS サーバが使用不可であり、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、クリティカル ポートを RADIUS 設定またはユーザ指定のアクセス VLAN で critical-authentication ステートに置きます。
  - すべての RADIUS サーバが使用不可であり、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 が設定されていなければ、スイッチはクライアントをゲスト VLAN に割り当てない可能性があります。
  - すべての RADIUS サーバが使用不可であり、クライアントがクリティカル ポートに接続されていて事前にゲスト VLAN に割り当てられている場合、スイッチはそのポートをゲスト VLAN で維持します。
- 制限付き VLAN：ポートが制限付き VLAN ですでに認可されていて、RADIUS サーバが使用不可の場合、スイッチはクリティカル ポートを制限付き VLAN で critical-authentication ステートに置きます。
- 802.1X アカウンティング：RADIUS サーバが使用不可の場合、アカウンティングは影響を受けません。

- プライベート VLAN : プライベート VLAN ホスト ポートで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 である必要があります。
- 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 設定またはユーザ指定のアクセス VLAN と音声 VLAN は異なるものである必要があります。
- 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用の RADIUS 設定またはユーザ指定のアクセス VLAN として設定しないでください。

802.1X 認証と音声 VLAN ポート

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

IP Phone は、ポートの認可ステートに関係なく、音声トラフィックに VVID を使用します。これにより、IP Phone は 802.1X 認証とは独立して動作できます。

シングルホスト モードでは、IP Phone だけが音声 VLAN で許可されます。マルチホスト モードでは、サプリカントが PVID で認証されたあとに、追加のクライアントが音声 VLAN 上でトラフィックを送信できます。マルチホスト モードがイネーブルの場合、サプリカントの認証は、PVID と VVID に影響を与えます。

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装置の MAC アドレスが表示されます。Cisco IP Phone は、他の装置からの 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いても、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 認証がイネーブルになっている場合、スイッチは、2 ホップ以上離れた認識されていない IP Phone からのパケットを廃棄します。

ポートで 802.1X 認証がイネーブルになっている場合は、音声 VLAN と等価であるポート VLAN を設定できません。

（注）　音声 VLAN が設定されていて Cisco IP Phone が接続されているアクセス ポートで 802.1X 認証をイネーブルにした場合、Cisco IP Phone とスイッチの接続が最大 30 秒切断されます。

音声 VLAN の詳細については、第 18 章「音声 VLAN の設定」を参照してください。

802.1X 認証とポート セキュリティ

シングルホスト モードまたはマルチホスト モードのいずれかで、ポート セキュリティを含む 802.1X ポートを設定できます（**switchport port-security** インターフェイス コンフィギュレーション コマンドを使用して、ポートでポート セキュリティを設定する必要があります）。ポートでポート セキュリティおよび 802.1X 認証をイネーブルにすると、802.1X 認証によってポートが認証され、ポート セキュリティによってクライアントの MAC アドレスを含むすべての MAC アドレスについてのネットワーク アクセスが管理されます。そのあと、802.1X ポートを介してネットワークにアクセスできるクライアントの数またはグループを制限できます。

スイッチにおいて、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。すると、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、ポート セキュリティ用に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る場合を除きます）。

  クライアントが認証されても、ポート セキュリティ テーブルがいっぱいの場合は、セキュリティ違反が発生します。この状況は、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、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生じます。クライアントのアドレスの有効期限が切れた場合、そのクライアントのセキュア ホスト テーブル内の位置を、別のホストが使用できます。

  最初に認証されたホストによってセキュリティ違反が発生した場合、ポートは errdisable になり、すぐにシャットダウンされます。

  セキュリティ違反に対するアクションは、ポート セキュリティ違反モードによって決まります。詳細については、「セキュリティ違反」（P.29-10）を参照してください。

- 802.1X クライアントのアドレスを、**no switchport port-security mac-address** *mac-address* インターフェイス コンフィギュレーション コマンドを使用してポート セキュリティ テーブルから手動で削除した場合、**dot1x re-authenticate interface** *interface-id* 特権 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、ポートは無認証ステートに変わり、クライアントのエントリを含むセキュア ホスト テーブル内のすべてのダイナミック エントリが消去されます。続いて、通常の認証が実行されます。
- ポートを管理上の理由からシャットダウンした場合、ポートは無認証ステートになり、すべてのダイナミック エントリがセキュア 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、シングルホスト モードまたはマルチホスト モードの 802.1X ポートで同時に設定できます。ポート セキュリティは、音声 VLAN ID（VVID）とポート VLAN ID（PVID）の両方に適用されます。
- 新しい装置が 802.1X 対応ポートに接続したとき、または最大許可数の装置が認証されたときに、ポートをシャットダウンするか、Syslog エラーを生成するか、または新しい装置からのパケットを破棄するように、**authentication violation** または **dot1x violation-mode** インターフェイス コンフィギュレーション コマンドを設定できます。詳細については、「ポート単位で許可される装置の最大数」（P.12-37）およびこのリリースのコマンド リファレンスを参照してください。

スイッチでポート 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.29-9）を参照してください。

802.1X 認証と Wake-on-LAN

802.1X 認証と Wake-on-LAN（WoL）機能により、スイッチが *マジック パケット*と呼ばれる特殊なイーサネット フレームを受信したときに、休止状態の PC の電源をオンにできます。この機能は、電源がオフになっているシステムに管理者が接続する必要がある環境で使用できます。

WoL を使用するホストが 802.1X ポートを通じて接続されていて、そのホストの電源がオフになると、802.1X ポートは無認可ステートになります。ポートでは EAPOL パケットだけを送受信でき、WoL マジック パケットはホストに到達しません。PC の電源がオフになると、その PC は認可されず、スイッチ ポートは開きません。

スイッチで 802.1X 認証と WoL を使用する場合、スイッチはマジック パケットを含むトラフィックを無認可の 802.1X ポートに転送します。ポートが無認可ステートの間、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、ネットワーク内の他の装置にパケットを送信することはできません。

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

authentication control-direction in または **dot1x control-direction in** インターフェイス コンフィギュレーション コマンドを使用してポートを単一方向として設定すると、ポートはスパニング ツリー フォワーディング ステートに変更されます。ポートは、ホストにパケットを送信できますが、受信はできません。

authentication control-direction both または **dot1x control-direction both** インターフェイス コンフィギュレーション コマンドを使用してポートを双方向として設定すると、ポートは双方向でアクセス制御されます。ポートは、ホストとの間でパケットを送受信しません。

802.1X 認証と MAC 認証バイパス

MAC 認証バイパス機能を使用することで、クライアントの MAC アドレス（図 12-2（P.12-4）を参照）に基づいてクライアントを認可するようにスイッチを設定できます。たとえば、プリンタなどの装置に接続された 802.1X ポートでこの機能をイネーブルにできます。

クライアントからの EAPOL 応答を待機している間に 802.1X 認証が時間切れになった場合、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可しようと試みます。

802.1X ポートで MAC 認証バイパス機能がイネーブルになっている場合、スイッチは MAC アドレスをクライアントの識別情報として使用します。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。スイッチは、802.1X ポート上のクライアントを検出したあとで、クライアントからのイーサネット パケットを待機します。スイッチは、MAC アドレスに基づいたユーザ名およびパスワードを持つ RADIUS-access/request フレームを認証サーバに送信します。認証に成功すると、スイッチはクライアントにネットワークへのアクセスを許可します。認証に失敗すると、スイッチはポートをゲスト VLAN に割り当てます（設定されている場合）。

リンクの存続時間中に EAPOL パケットがインターフェイスで検出された場合、スイッチは、そのインターフェイスに接続されている装置が 802.1X 対応サプリカントであると判断し、（MAC 認証バイパスではなく）802.1X 認証を使用してインターフェイスを認可します。インターフェイスのリンク ステータスがダウンになった場合、EAPOL 履歴は消去されます。

スイッチが MAC 認証バイパスを使用してポートをすでに認可していて、802.1X サプリカントを検出した場合、スイッチはポートに接続されたクライアントを無認可にしません。再認証を行う場合、以前のセッションが Termination-Action RADIUS 属性値が DEFAULT であるために終了していれば、スイッチは 802.1X 認証を優先的な再認証プロセスとして使用します。

MAC 認証バイパスで認証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、802.1X で認証されたクライアントの再認証プロセスと同じです。再認証中に、ポートは以前に割り当てられた VLAN 内にとどまります。再認証に成功すると、スイッチはポートを同じ VLAN 内に維持します。再認証に失敗すると、スイッチはポートをゲスト VLAN に割り当てます（設定されている場合）。

再認証が Session-Timeout RADIUS 属性（属性 [27]）および Termination-Action RADIUS 属性（属性 [29]）に基づいていて、Termination-Action RADIUS 属性（属性 [29]）のアクションが *Initialize* の場合（属性値は *DEFAULT*）、MAC 認証バイパス セッションは終了し、再認証中に接続が失われます。MAC 認証バイパスがイネーブルになっていて、802.1X 認証が時間切れになった場合、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『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。

- 802.1X 認証：MAC 認証バイパスをイネーブルにできるのは、ポートで 802.1X 認証がイネーブルになっている場合だけです。
- ゲスト VLAN：クライアントの MAC アドレス識別情報が無効である場合、ゲスト VLAN が設定されていれば、スイッチはクライアントをゲスト VLAN に割り当てます。
- 制限付き VLAN：802.1X ポートに接続されたクライアントが MAC 認証バイパスで認証されている場合、この機能はサポートされません。
- ポート セキュリティ：「802.1X 認証とポート セキュリティ」（P.12-25）を参照してください。
- 音声 VLAN：「802.1X 認証と音声 VLAN ポート」（P.12-25）を参照してください。
- VLAN Membership Policy Server（VMPS; VLAN メンバーシップ ポリシー サーバ）：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）レイヤ 2 IP 検証：この機能は、例外リストのホストを含めて、802.1X ポートが MAC 認証バイパスで認証されたあとに有効になります。

設定の詳細については、「認証マネージャ」（P.12-7）を参照してください。

Cisco IOS Release 12.2(55)SE 以降では、詳細な MAB システム メッセージのフィルタリングがサポートされます。「認証マネージャの CLI コマンド」（P.12-9）を参照してください。

802.1X ユーザ分散

802.1X ユーザ分散を設定して、同じグループ名を持つユーザを複数の異なる VLAN に負荷分散させることができます。

VLAN は、RADIUS サーバによって提供されるか、スイッチの CLI を通じて VLAN グループ名の下に設定されます。

- ユーザに対して複数の VLAN 名を送信するように RADIUS サーバを設定します。ユーザへの応答の一部として複数の VLAN 名を送信できます。802.1X ユーザ分散では、特定の VLAN 内のすべてのユーザを追跡し、認可済みユーザを最もユーザが少ない VLAN に移動することでロード バランシングを実現します。
- ユーザに対して VLAN グループ名を送信するように RADIUS サーバを設定します。ユーザへの応答の一部として VLAN グループ名を送信できます。スイッチの CLI を使用して設定した VLAN グループ名の中から、選択した VLAN グループ名を検索できます。VLAN グループ名が見つかった場合、その VLAN グループ名の下の対応する VLAN が検索され、最もユーザが少ない VLAN が検索されます。その VLAN に対応する認可済みユーザを移動することで、ロード バランシングが実現されます。

（注） RADIUS サーバは、VLAN-ID、VLAN 名、または VLAN グループの任意の組み合わせで VLAN 情報を送信できます。

802.1X ユーザ分散の設定時の注意事項

- 少なくとも 1 つの VLAN が VLAN グループにマッピングされていることを確認します。
- 複数の VLAN を VLAN グループにマップできます。
- VLAN を追加または削除することで、VLAN グループを変更できます。

- 既存の VLAN を VLAN グループ名から消去した場合、VLAN の認証済みポートは消去されませんが、マッピングは既存の VLAN グループから削除されます。
- VLAN グループ名から最後の VLAN を消去すると、VLAN グループが消去されます。
- アクティブな VLAN が VLAN グループにマッピングされているときでも、VLAN グループを消去できます。VLAN グループを消去した場合、グループ内の任意の VLAN で認証済みステートであるポートまたはユーザは消去されませんが、VLAN グループへの VLAN マッピングは消去されます。

詳細については、「802.1X ユーザ分散の設定」（P.12-58）を参照してください。

Network Admission Control レイヤ 2 802.1X 検証

スイッチは、Network Admission Control（NAC）レイヤ 2 802.1X 検証をサポートします。この検証では、エンドポイント システムまたはクライアントにネットワーク アクセスを許可する前に、それらの装置のアンチウイルス状態または*ポスチャ*をチェックします。NAC レイヤ 2 802.1X 検証では、次の作業を実行できます。

- Session-Timeout RADIUS 属性（属性 [27]）および Termination-Action RADIUS 属性（属性 [29]）を認証サーバからダウンロードします。
- 再認証を試行する間隔の秒数を、Session-Timeout RADIUS 属性（属性 [27]）の値として設定し、クライアントに対するアクセス ポリシーを RADIUS サーバから取得します。
- Termination-Action RADIUS 属性（属性 [29]）を使用して、スイッチがクライアントの再認証を試みるときに実行するアクションを設定します。値が *DEFAULT* であるか、または設定されていない場合、セッションは終了します。値が RADIUS-Request の場合、再認証プロセスが開始されます。
- VLAN 番号または名前あるいは VLAN グループ名のリストを Tunnel Group Private ID（属性 [81]）の値として設定し、VLAN 番号または名前あるいは VLAN グループ名のプリファレンスを Tunnel Preference（属性 [83]）の値として設定します。Tunnel Preference を設定しない場合、最初の Tunnel Group Private ID（属性 [81]）属性がリストから取得されます。
- **show authentication** または **show dot1x** 特権 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。
- セカンダリ プライベート VLAN をゲスト VLAN として設定します。

NAC レイヤ 2 802.1X 検証の設定は、802.1X ポートベース認証の設定に似ていますが、RADIUS サーバでポスチャ トークンを設定する必要があります。NAC レイヤ 2 802.1X 検証の設定については、「NAC レイヤ 2 802.1X 検証の設定」（P.12-59）および「定期的再認証の設定」（P.12-44）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。

設定の詳細については、「認証マネージャ」（P.12-7）を参照してください。

フレキシブルな認証順序付け

フレキシブルな認証順序付け機能を使用して、ポートが新しいホストの認証に使用する方式の順序を設定できます。MAC 認証バイパスおよび 802.1X をプライマリ認証方式またはセカンダリ認証方式に設定し、これらの認証の一方または両方が失敗したときのフォールバック方式として Web 認証を設定することができます。詳細については、「フレキシブルな認証順序付けの設定」（P.12-64）を参照してください。

Open1x 認証

Open1x 認証により、装置を認証する前に装置のポートへのアクセスを許可することができます。オープン認証を設定した場合、ポート上の新しいホストは、スイッチへのトラフィックの送信だけを行うことができます。ホストが認証されると、RADIUS サーバで設定されたポリシーがそのホストに適用されます。

オープン認証は次のシナリオで設定できます。

- シングルホスト モードとオープン認証：認証の前後で、1 人のユーザだけがネットワーク アクセスを許可されます。
- MDA モードとオープン認証：音声ドメインの 1 人のユーザと、データ ドメインの 1 人のユーザだけが許可されます。
- マルチホスト モードとオープン認証：任意のホストがネットワークにアクセスできます。
- マルチ認証モードとオープン認証：MDA に似ていますが、複数のホストを認証できます。

詳細については、「ホスト モードの設定」（P.12-43）を参照してください。

音声認識 802.1X セキュリティの使用

データ VLAN であるか音声 VLAN であるかに関係なく、セキュリティ違反が発生した VLAN だけをディセーブルにするようにスイッチを設定するには、音声認識 802.1X セキュリティ機能を使用します。以前のリリースでは、データ クライアントの認証を試みたことによりセキュリティ違反が発生した場合、ポート全体がシャットダウンされ、接続が完全に失われました。

この機能は、PC が IP Phone に接続されている場合に使用できます。データ VLAN でセキュリティ違反が見つかった場合、データ VLAN だけがシャットダウンされます。音声 VLAN のトラフィックは、中断せずに継続されます。

音声認識 802.1X セキュリティの設定については、「音声認識 802.1X セキュリティの設定」（P.12-38）を参照してください。

802.1X サプリカント スイッチおよびオーセンティケータ スイッチと Network Edge Access Topology（NEAT; ネットワーク エッジ アクセス トポロジ）

ネットワーク エッジ アクセス トポロジ（NEAT）機能は、配線クローゼットの外部の領域（会議室など）に ID を拡張します。これにより、任意のタイプの装置をポートで認可できます。

- 802.1X スイッチ サプリカント：802.1X サプリカント機能を使用することで、スイッチを別のスイッチへのサプリカントとして機能するように設定できます。この設定は、たとえば、スイッチが配線クローゼットの外部にあり、トランク ポートを通じてアップストリーム スイッチに接続されているシナリオで役立ちます。802.1X スイッチ サプリカント機能を使用して設定されたスイッチは、セキュアな接続のために、アップストリーム スイッチとの間で認証を行います。

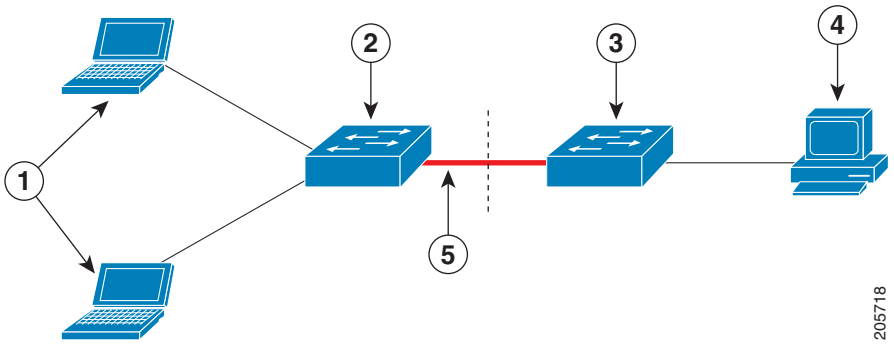
  サプリカント スイッチの認証が成功すると、ポート モードがアクセスからトランクに変更されます。
- オーセンティケータ スイッチでアクセス VLAN が設定されている場合、そのアクセス VLAN は、認証が成功したあとにトランク ポートのネイティブ VLAN になります。

1 つまたは複数のサプリカント スイッチに接続するオーセンティケータ スイッチ インターフェイスで、MDA モードまたはマルチ認証モードをイネーブルにすることができます。マルチホスト モードは、オーセンティケータ スイッチ インターフェイスでサポートされません。

ネットワーク エッジ アクセス トポロジ（NEAT）がすべてのホスト モードで動作するようにするには、サプリカント スイッチで **dot1x supplicant force-multicast** 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。

- ホスト認証：認可されたホスト（サプリカントによりスイッチに接続しているもの）からのトラフィックだけがネットワーク上で許可されるようにします。スイッチは、図 12-6 に示すように、Client Information Signalling Protocol（CISP）を使用して、サプリカント スイッチに接続している MAC アドレスをオーセンティケータ スイッチに送信します。
- 自動イネーブル化：オーセンティケータ スイッチでトランク設定を自動的にイネーブルにし、サプリカント スイッチから送信される複数の VLAN からのユーザ トラフィックを許可します。ACS で、cisco-av-pair を *device-traffic-class=switch* として設定します（この設定は *group* 設定または *user* 設定で行うことができます）。

図 12-6　CISP を使用するオーセンティケータ スイッチとサプリカント スイッチ



1	ワークステーション（クライアント）	**2**	サプリカント スイッチ（配線クローゼットの外部）
3	オーセンティケータ スイッチ	**4**	Access Control Server（ACS）
5	トランク ポート		

注意事項

- 他の認証ポートと同じ設定で NEAT ポートを設定できます。サプリカント スイッチの認証時に、ポート モードは、スイッチのベンダー固有属性（VSA）に基づいて *アクセス*から *トランク*に変更されます（device-traffic-class=switch）。
- VSA は、オーセンティケータ スイッチのポート モードをアクセスからトランクに変更し、802.1X トランク カプセル化とアクセス VLAN をイネーブルにします（ネイティブ トランク VLAN に変換する場合）。VSA は、サプリカントのポート設定を変更しません。
- ホスト モードを変更し、かつオーセンティケータ スイッチ ポートに標準ポート設定を適用するには、スイッチ VSA ではなく、Auto Smartports ユーザ定義マクロを使用することもできます。これにより、オーセンティケータ スイッチ ポート上のサポートされていない設定を削除し、ポート モードを *アクセス*から *トランク*に変更できます。詳細については、第 15 章「SmartPort マクロの設定」を参照してください。

詳細については、「オーセンティケータおよびサプリカント スイッチと NEAT の設定」（P.12-60）を参照してください。

IEEE 802.1X 認証と ACL および RADIUS Filter-Id 属性の使用

スイッチは、入力ポートに適用された IP 標準および IP 拡張ポート アクセス制御リスト（ACL）をサポートします。

- ユーザが設定する ACL
- Access Control Server（ACS）からの ACL

シングルホスト モードの IEEE 802.1X ポートは、ACS からの ACL を使用して、異なるレベルのサービスを IEEE 802.1X 認証済みユーザに提供します。RADIUS サーバは、このタイプのユーザおよびポートを認証すると、ユーザの識別情報に基づいて ACL 属性をスイッチに送信します。スイッチは、ユーザ セッション中に、それらの属性をポートに適用します。セッションが終了した場合、認証が失敗した場合、またはリンクが失敗した場合、ポートは無認可ステートになり、スイッチは ACL をポートから削除します。

ACS からの IP 標準ポート ACL および IP 拡張ポート ACL だけが Filter-Id 属性をサポートします。Filter-Id 属性は、ACL の名前または番号を指定します。Filter-id 属性では、方向（着信または発信）と、ユーザまたはユーザが属するグループも指定できます。

- ユーザの Filter-Id 属性は、グループの Filter-Id 属性よりも優先されます。
- ACS からの Filter-Id 属性がすでに設定されている ACL を指定する場合、その ACL はユーザ設定の ACL よりも優先されます。
- RADIUS サーバが複数の Filter-Id 属性を送信した場合、最後の属性だけが適用されます。

Filter-Id 属性がスイッチで定義されていない場合、認証は失敗し、ポートは無認可ステートに戻ります。

共通セッション ID

認証マネージャでは、使用する認証方式に関係なく、1 つのセッション ID（共通セッション ID と呼ばれます）をクライアントに対して使用します。この ID は、show コマンドや Management Information Base（MIB; 管理情報ベース）など、すべてのレポート目的に使用されます。セッション ID は、すべてのセッション単位 Syslog メッセージとともに表示されます。

セッション ID には次のものが含まれます。

- Network Access Device（NAD; ネットワーク アクセス装置）の IP アドレス
- 単調に増加する一意の 32 ビット整数
- セッション開始時間スタンプ（32 ビット整数）

次に、**show authentication** コマンドの出力に表示されるセッション ID の例を示します。この例のセッション ID は、160000050000000B288508E5 です。

```
Switch# show authentication sessions

Interface  MAC Address     Method   Domain   Status         Session ID
Fa4/0/4    0000.0000.0203  mab      DATA     Authz Success  160000050000000B288508E5
```

次に、Syslog 出力に表示されるセッション ID の例を示します。この例のセッション ID も、160000050000000B288508E5 です。

```
1w0d: %AUTHMGR-5-START: Starting 'mab' for client (0000.0000.0203) on Interface Fa4/0/4
AuditSessionID 160000050000000B288508E5
1w0d: %MAB-5-SUCCESS: Authentication successful for client (0000.0000.0203) on Interface
Fa4/0/4 AuditSessionID 160000050000000B288508E5
1w0d: %AUTHMGR-7-RESULT: Authentication result 'success' from 'mab' for client
(0000.0000.0203) on Interface Fa4/0/4 AuditSessionID 160000050000000B288508E5
```

セッション ID は、NAD、AAA サーバ、およびその他のレポート解析アプリケーションでクライアントを識別するために使用されます。ID は自動的に表示されます。したがって設定作業は不要です。

802.1X 認証の設定

- 「802.1X 認証のデフォルト設定」（P.12-34）
- 「802.1X 認証の設定時の注意事項」（P.12-35）
- 「802.1X 準備状態チェックの設定」（P.12-37）（任意）
- 「音声認識 802.1X セキュリティの設定」（P.12-38）（任意）
- 「802.1X 違反モードの設定」（P.12-39）（任意）
- 「スイッチと RADIUS サーバ間の通信の設定」（P.12-42）（必須）
- 「ホスト モードの設定」（P.12-43）（任意）
- 「定期的再認証の設定」（P.12-44）（任意）
- 「ポートに接続されたクライアントの手動再認証」（P.12-45）（任意）
- 「待機時間の変更」（P.12-46）（任意）
- 「スイッチとクライアント間の再送信時間の変更」（P.12-46）（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.12-47）（任意）
- 「再認証回数の設定」（P.12-48）（任意）
- 「802.1X アカウンティングの設定」（P.12-50）（任意）
- 「MAC 移行のイネーブル化」（P.12-49）（任意）
- 「MAC 置き換えのイネーブル化」（P.12-49）（任意）
- 「ゲスト VLAN の設定」（P.12-51）（任意）
- 「制限付き VLAN の設定」（P.12-52）（任意）
- 「アクセス不能認証バイパス機能の設定」（P.12-54）（任意）
- 「802.1X 認証と WoL の設定」（P.12-56）（任意）
- 「MAC 認証バイパスの設定」（P.12-57）（任意）
- 「NAC レイヤ 2 802.1X 検証の設定」（P.12-59）（任意）
- 「オーセンティケータおよびサプリカント スイッチと NEAT の設定」（P.12-60）
- 「802.1X 認証とダウンロード可能 ACL およびリダイレクト URL の設定」（P.12-61）
- 「フレキシブルな認証順序付けの設定」（P.12-64）
- 「ポートでの 802.1X 認証のディセーブル化」（P.12-66）（任意）
- 「802.1X 認証設定のデフォルト値へのリセット」（P.12-66）（任意）

802.1X 認証のデフォルト設定

表 12-4 に、802.1X 認証のデフォルト設定を示します。

表 12-4　802.1X 認証のデフォルト設定

機能	デフォルト設定
スイッチの 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 ベース認証を行わずに、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 • IP アドレス • UDP 認証ポート • キー	 • 指定なし。 • 1812。 • 指定なし。
ホスト モード	シングルホスト モード。
制御方向	双方向制御。
定期的再認証	ディセーブル。
再認証の試行間隔（秒）	3600 秒。
再認証回数	2 回（ポートが無認可ステートに移行する前に、スイッチが認証プロセスを再開する回数）。
待機時間	60 秒（スイッチがクライアントとの認証情報の交換に失敗したあと、待機状態を続ける秒数）。
再送信時間	30 秒（スイッチが要求を再送信する前に、EAP 要求/アイデンティティ フレームに対するクライアントからの応答を待機する秒数）。
最大再送信回数	2 回（スイッチが認証プロセスを再開する前に、EAP 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 タイムアウト時間	30 秒（認証サーバからの要求をクライアントにリレーするときに、スイッチが要求をクライアントに再送信する前に応答を待機する時間）。
認証サーバ タイムアウト時間	30 秒（クライアントからの応答を認証サーバにリレーするとき、スイッチが応答をサーバに再送信する前に、応答を待機する時間）。 このタイムアウト時間を変更するには、**authentication timer server** または **dot1x timeout server-timeout** 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。
無活動タイムアウト	ディセーブル。
ゲスト VLAN	指定なし。
アクセス不能認証バイパス	ディセーブル。
制限付き VLAN	指定なし。
オーセンティケータ（スイッチ）モード	指定なし。
MAC 認証バイパス	ディセーブル。
音声認識セキュリティ	ディセーブル。

802.1X 認証の設定時の注意事項

- 「802.1X 認証」（P.12-35）
- 「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.12-36）
- 「MAC 認証バイパス」（P.12-36）
- 「ポート単位で許可される装置の最大数」（P.12-37）

802.1X 認証

- 802.1X 認証をイネーブルにすると、ポートが認証されてから、他のレイヤ 2 機能またはレイヤ 3 機能がイネーブルになります。
- 802.1X 対応ポートのモードを変更しようとしても（たとえば、アクセスからトランク）、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。
- 802.1X 対応ポートが割り当てられている VLAN が変更された場合、この変更はトランスペアレントであり、スイッチに影響を与えません。たとえば、この変更は、ポートが RADIUS サーバによって割り当てられた VLAN に割り当てられていて、再認証後に異なる VLAN に割り当てられた場合に発生します。

  802.1X ポートが割り当てられている VLAN がシャットダウンするか、ディセーブルになるか、または削除された場合、ポートは無認可ステートになります。たとえば、ポートが割り当てられているアクセス VLAN がシャットダウンされるか、または削除されると、ポートは無認可になります。
- 802.1X プロトコルは、レイヤ 2 のスタティック 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ますが、次のポート タイプではサポートされません。
  - トランク ポート：トランク ポートで 802.1X 認証をイネーブルにしようとすると、エラー メッセージが表示され、802.1X 認証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、ネイバーとトランク ポートへの変更をネゴシエートする場合があります。ダイナミック ポートで 802.1X 認証をイネーブルにしようとすると、エラー メッセージが表示され、802.1X 認証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 認証をイネーブルにしようとすると、エラー メッセージが表示され、802.1X 認証はイネーブルになりません。802.1X 対応ポートを変更してダイナミック VLAN を割り当てようとしても、エラー メッセージが表示され、VLAN 設定は変更されません。
  - EtherChannel　ポート：アクティブまたはまだアクティブでない　EtherChannel　メンバーを 802.1X ポートとして設定しないでください。EtherChannel ポートで 802.1X 認証をイネーブルにしようとすると、エラー メッセージが表示され、802.1X 認証はイネーブルになりません。
  - 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 認証をイネーブルにすることができます。ただし、そのポートが SPAN または RSPAN 宛先ポートとして削除されるまで、802.1X 認証はディセーブルのままです。SPAN または RSPAN 送信元ポートでは 802.1X 認証をイネーブルにすることができます。
- **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 802.1X 認証をスイッチでグローバルにイネーブルにする前に、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 設定を削除します。
- Cisco IOS Release 12.2(55)SE 以降では、802.1X 認証に関連するシステム メッセージのフィルタリングがサポートされます。「認証マネージャの CLI コマンド」（P.12-9）を参照してください。

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

- ポートで 802.1X 認証がイネーブルになっている場合は、音声 VLAN と等価であるポート VLAN を設定できません。
- VLAN 割り当て機能付きの 802.1X 認証は、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。
- プライベート VLAN ポートで 802.1X 認証を設定することは可能ですが、プライベート VLAN ポートでポート 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 ACL とともに 802.1X 認証を設定しないでください。
- RSPAN VLAN、プライベート VLAN、または音声 VLAN 以外の任意の VLAN を、802.1X のゲスト VLAN として設定できます。ゲスト VLAN の機能は、内部 VLAN（ルーテッド ポート）またはトランク ポート上ではサポートされません。サポートされるのはアクセス ポートだけです。
- DHCP クライアントが接続されている 802.1X ポートのゲスト VLAN を設定したあと、DHCP サーバからホスト IP アドレスを取得することが必要な場合があります。クライアント上の DHCP プロセスが時間切れとなり DHCP サーバからホスト IP アドレスを取得する前に、スイッチ上の 802.1X 認証プロセスを再開するための設定を変更できます。802.1X 認証プロセスの設定を減らします（**authentication timer inactivity**（または **dot1x timeout quiet-period**）および **authentication timer reauthentication**（または **dot1x timeout tx-period**）インターフェイス コンフィギュレーション コマンド）。設定の減少量は、接続された 802.1X クライアントの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ときは、次の注意事項に従ってください。
  - この機能は、シングルホスト モードおよびマルチホスト モードの 802.1X ポートでサポートされています。
  - クライアントが Windows XP を実行し、クライアントが接続されているポートが critical-authentication 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と報告することがあります。
  - Windows XP クライアントで DHCP が設定され、DHCP サーバからの IP アドレスがある場合、クリティカル ポートで EAP 認証成功メッセージを受信しても DHCP 設定プロセスを再初期化しません。
  - アクセス不能認証バイパス機能および制限付き VLAN を 802.1X ポートで設定できます。スイッチが制限付き VLAN でクリティカル ポートの再認証を試行し、すべての RADIUS サーバが使用不可の場合、スイッチはポートのステートを critical-authentication ステートに変更し、制限付き VLAN にとどまります。
  - アクセス不能認証バイパス機能とポート セキュリティは、同じスイッチ ポートに設定できます。
- RSPAN VLAN または音声 VLAN 以外の任意の VLAN を、802.1X の制限付き VLAN として設定できます。制限付き VLAN の機能は、内部 VLAN（ルーテッド ポート）またはトランク ポート上ではサポートされません。サポートされるのはアクセス ポートだけです。

MAC 認証バイパス

- 特に言及しない限り、MAC 認証バイパスの注意事項は、802.1X 認証の注意事項と同じです。詳細については、「802.1X 認証」（P.12-35）を参照してください。
- ポートが MAC アドレスで認証されたあとで、ポートから MAC 認証バイパスをディセーブルにした場合、ポート ステートに影響はありません。
- ポートが未許可ステートであり、クライアント MAC アドレスが認証サーバ データベースにない場合、ポートは未許可ステートのままです。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ると、スイッチは MAC 認証バイパス機能を使用してポートを再認証できます。

- ポートが認証ステートにない場合、再認証が行われるまでポートはこのステートを維持します。
- MAC 認証バイパスによって接続されたが非アクティブであるホストのタイムアウト時間を設定できます。指定できる範囲は 1 ～ 65535 秒です。タイムアウト値を設定する前に、ポート セキュリティをイネーブルにする必要があります。詳細については、「ポート セキュリティの設定」（P.29-9）を参照してください。

ポート単位で許可される装置の最大数

これは、802.1X 対応ポートで許可される装置の最大数です。

- シングルホスト モードでは、アクセス VLAN で 1 つの装置だけが許可されます。ポートが音声 VLAN でも設定されている場合、無制限の数の Cisco IP Phone が音声 VLAN を通じてトラフィックを送受信できます。
- マルチドメイン認証（MDA）モードでは、アクセス VLAN で 1 つの装置が許可され、音声 VLAN で 1 つの IP Phone が許可されます。
- マルチホスト モードでは、1 つの 802.1X サプリカントだけがポートで許可されますが、無制限の数の非 802.1X ホストがアクセス VLAN で許可されます。音声 VLAN では無制限の数の装置が許可されます。

802.1X 準備状態チェックの設定

802.1X 準備状態チェックでは、すべてのスイッチ ポートでの 802.1X アクティビティをモニタし、802.1X をサポートするポートに接続された装置に関する情報を表示します。この機能を使用して、スイッチ ポートに接続された装置が 802.1X に対応しているかどうかを判断できます。

802.1X 準備状態チェックは、802.1X 用に設定できるすべてのポートで許可されます。準備状態チェックは、**dot1x force-unauthorized** として設定されているポートでは使用できません。

スイッチで準備状態チェックをイネーブルにするには、次の注意事項に従ってください。

- 準備状態チェックは、通常はスイッチで 802.1X をイネーブルにする前に使用します。
- インターフェイスを指定せずに **dot1x test eapol-capable** 特権 EXEC コマンドを使用した場合、スイッチ スタックのすべてのポートがテストされます。
- 802.1X 対応ポートで **dot1x test eapol-capable** コマンドを設定し、リンクがアップになった場合、ポートは 802.1X 機能に関するクエリーを接続済みクライアントに送信します。クライアントが通知パケットで応答した場合、そのクライアントは 802.1X に対応しています。クライアントがタイムアウト時間内に応答した場合、Syslog メッセージが生成されます。クライアントがクエリーに応答しない場合、そのクライアントは 802.1X に対応していません。Syslog メッセージは生成されません。
- 準備状態チェックは、複数のホストを処理するポート（たとえば、IP Phone に接続されている PC）で送信できます。タイマー時間内に準備状態チェックに応答した各クライアントに対して、Syslog メッセージが生成されます。

スイッチで 802.1X 準備状態チェックをイネーブルにするには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**dot1x test eapol-capable** [**interface** *interface-id*]	スイッチで 802.1X 準備状態チェックをイネーブルにします。 （任意）*interface-id* には、802.1X 準備状態をチェックするポートを指定します。 **（注）** オプションの **interface** キーワードを省略した場合、スイッチのすべてのインターフェイスがテストされます。
ステップ 2	**configure terminal**	（任意）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 3	**dot1x test timeout** *timeout*	（任意）EAPOL 応答の待機に使用するタイムアウトを設定します。指定できる範囲は 1 ～ 65535 秒です。デフォルト値は 10 秒です。
ステップ 4	**end**	（任意）特権 EXEC モードに戻ります。
ステップ 5	**show running-config**	（任意）変更したタイムアウト値を確認します。

次に、スイッチで準備状態チェックをイネーブルにしてポートにクエリーを送信する例を示します。この例は、クエリー先のポートから受信した応答も示しており、接続している装置が 802.1X 対応であることを確認しています。

```
switch# dot1x test eapol-capable interface gigabitethernet1/2

DOT1X_PORT_EAPOL_CAPABLE:DOT1X: MAC 00-01-02-4b-f1-a3 on gigabitethernet1/2 is EAPOL
capable
```

音声認識 802.1X セキュリティの設定

データ VLAN であるか音声 VLAN であるかに関係なく、セキュリティ違反が発生した VLAN だけをディセーブルにするには、スイッチで音声認識 802.1X セキュリティ機能を使用します。この機能は、PC が IP Phone に接続されている IP Phone 配置で使用できます。データ VLAN でセキュリティ違反が見つかった場合、データ VLAN だけがシャットダウンされます。音声 VLAN 上のトラフィックは、中断されずにスイッチを通過します。

スイッチで音声認識 802.1X 音声セキュリティを設定するには、次の注意事項に従ってください。

- 音声認識 802.1X セキュリティをイネーブルにするには、**errdisable detect cause security-violation shutdown vlan** グローバル コンフィギュレーション コマンドを入力します。音声認識 802.1X セキュリティをディセーブルにするには、このコマンドの **no** バージョンを入力します。このコマンドは、スイッチのすべての 802.1X 設定ポートに適用されます。

（注） **shutdown vlan** キーワードを含めない場合、errdisable ステートになったときにポート全体がシャットダウンされます。

- **errdisable recovery cause security-violation** 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 errdisable ステート回復を設定した場合、ポートは自動的に再びイネーブルになります。errdisable ステート回復をポートに設定していない場合は、**shutdown** および **no-shutdown** 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再びイネーブルにします。
- 個別の VLAN を再びイネーブルにするには、**clear errdisable interface** *interface-id* **vlan** [*vlan-list*] 特権 EXEC コマンドを使用します。範囲を指定しない場合、ポートのすべての VLAN がイネーブルになります。

音声認識 802.1X セキュリティをイネーブルにするには、特権 EXEC モードで次の手順を実行します。

	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	**errdisable detect cause security-violation shutdown vlan**	セキュリティ違反エラーが発生した任意の VLAN をシャットダウンします。 **（注）** **shutdown vlan** キーワードを含めない場合、ポート全体が errdisable ステートになり、シャットダウンします。
ステップ 3	**errdisable recovery cause security-violation**	（任意）VLAN 単位の自動エラー回復をイネーブルにします。
ステップ 4	**clear errdisable interface** *interface-id* **vlan** [*vlan-list*]	（任意）errdisable になっている個別の VLAN を再びイネーブルにします。 • *interface-id* には、個別の VLAN を再びイネーブルにするポートを指定します。 • （任意）*vlan-list* には、再びイネーブルにする VLAN のリストを指定します。*vlan-list* を指定しない場合は、すべての VLAN が再びイネーブルになります。
ステップ 5	**shutdown** **no-shutdown**	（任意）errdisable の VLAN を再びイネーブルにし、すべての errdisable 表示を消去します。
ステップ 6	**end**	特権 EXEC モードに戻ります。
ステップ 7	**show errdisable detect**	設定を確認します。
ステップ 8	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

次に、セキュリティ違反エラーが発生した任意の VLAN をシャットダウンするようにスイッチを設定する例を示します。

```
Switch(config)# errdisable detect cause security-violation shutdown vlan
```

次に、ギガビット イーサネット 0/2 ポートで errdisable になっているすべての VLAN を再びイネーブルにする例を示します。

```
Switch# clear errdisable interface gigabitethernet0/2 vlan
```

設定を確認するには、**show errdisable detect** 特権 EXEC コマンドを入力します。

802.1X 違反モードの設定

次の場合にポートをシャットダウンするか、Syslog エラーを生成するか、または新しい装置からのパケットを破棄するように、802.1X ポートを設定できます。

- 装置が 802.1X 対応ポートに接続したとき
- 最大許可数の装置がポートで認証されたとき

スイッチのセキュリティ違反アクションを設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**aaa new-model**	AAA をイネーブルにします。

	コマンド	目的
ステップ 3	**aaa authentication dot1x** {**default**} *method1*	802.1X 認証方式リストを作成します。 **authentication** コマンドに名前付きリストが*指定されていない*場合に使用するデフォルトのリストを作成するには、**default** キーワードの後ろにデフォルト状況で使用される方式を指定します。デフォルトの方式リストは、自動的にすべてのポートに適用されます。 *method1* には、**group radius** キーワードを入力して、認証用のすべての RADIUS サーバのリストを使用します。 **（注）** 他のキーワードがコマンドラインのヘルプ ストリングに表示されますが、サポートされているのは **group radius** キーワードだけです。
ステップ 4	**interface** *interface-id*	クライアントに接続された、802.1X 認証をイネーブルに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 5	**switchport mode access**	ポートをアクセス モードに設定します。
ステップ 6	**authentication violation shutdown** | **restrict** | **protect** | **replace**} または **dot1x violation-mode** {**shutdown** | **restrict** | **protect**}	違反モードを設定します。キーワードの意味は次のとおりです。 • **shutdown**：ポートを errdisable にします。 • **restrict**：Syslog エラーを生成します。 • **protect**：ポートにトラフィックを送信する任意の新しい装置からのパケットを廃棄します。 • **replace**：現行セッションを削除し、新しいホストで認証します。
ステップ 7	**end**	特権 EXEC モードに戻ります。
ステップ 8	**show authentication** または **show dot1x**	設定を確認します。
ステップ 9	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

802.1X 認証の設定

802.1X ポートベース認証を設定するには、認証、認可、アカウンティング（AAA）をイネーブルにし、認証方式リストを指定する必要があります。方式リストは、ユーザ認証のためクエリー送信を行う手順と認証方式を記述したものです。

ユーザ単位 ACL または VLAN 割り当てを許可するには、AAA 認可をイネーブルにして、すべてのネットワーク関連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 AAA プロセスを次に示します。

ステップ 1　ユーザがスイッチのポートに接続します。

ステップ 2　認証が実行されます。

ステップ 3　RADIUS サーバの設定に基づいて、VLAN 割り当てが必要に応じてイネーブルにされます。

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

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　再認証の結果に基づいて、スイッチがアカウンティング サーバに中間アカウンティング更新を送信します。

ステップ 7　ユーザがポートから接続解除します。

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

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

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**aaa new-model**	AAA をイネーブルにします。
ステップ 3	**aaa authentication dot1x** {**default**} *method1*	802.1X 認証方式リストを作成します。 **authentication** コマンドに名前付きリストが*指定されていない*場合に使用するデフォルトのリストを作成するには、**default** キーワードの後ろにデフォルト状況で使用する方式を指定します。デフォルトの方式リストは、自動的にすべてのポートに適用されます。 *method1* には、**group radius** キーワードを入力して、認証用のすべての RADIUS サーバのリストを使用します。 **（注）**　他のキーワードがコマンドラインのヘルプ ストリングに表示されますが、サポートされているのは **group radius** キーワードだけです。
ステップ 4	**dot1x system-auth-control**	スイッチで 802.1X 認証をグローバルにイネーブルにします。
ステップ 5	**aaa authorization network** {**default**} **group radius**	（任意）ユーザ単位 ACL または VLAN 割り当てなどのすべてのネットワーク関連サービス要求に対してユーザ RADIUS 認可を使用するようにスイッチを設定します。 ユーザ単位 ACL に対しては、シングルホスト モードを設定する必要があります。この設定は、デフォルトです。
ステップ 6	**radius-server host** *ip-address*	（任意）RADIUS サーバの IP アドレスを指定します。
ステップ 7	**radius-server key** *string*	（任意）スイッチと RADIUS サーバ上で動作する RADIUS デーモンとの間で使用する認証キーおよび暗号キーを指定します。
ステップ 8	**interface** *interface-id*	クライアントに接続された、802.1X 認証をイネーブルに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 9	**switchport mode access**	（任意）ステップ 6 および 7 で RADIUS サーバを設定した場合だけ、ポートをアクセス モードに設定します。
ステップ 10	**authentication port-control auto** または **dot1x port-control auto**	ポートで 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、「802.1X 認証の設定時の注意事項」（P.12-35）を参照してください。
ステップ 11	**end**	特権 EXEC モードに戻ります。
ステップ 12	**show authentication** または **show dot1x**	設定を確認します。
ステップ 13	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

スイッチと RADIUS サーバ間の通信の設定

RADIUS セキュリティ サーバは、ホスト名または IP アドレス、ホスト名と特定の UDP ポート番号、または IP アドレスと特定の UDP ポート番号によって識別されます。IP アドレスと UDP ポート番号の組み合わせによって、一意の ID が作成され、同じ IP アドレスのサーバ上にある複数の UDP ポートに RADIUS 要求を送信できるようになります。同じ RADIUS サーバ上の異なる 2 つのホスト エントリに同じサービス（認証など）を設定した場合、2 番めに設定されたホスト エントリは、最初に設定されたホスト エントリのフェールオーバー バックアップとして動作します。RADIUS ホスト エントリは、設定した順序に従って試行されます。

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

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**radius-server host** {*hostname* | *ip-address*} **auth-port** *port-number* **key** *string*	RADIUS サーバ パラメータを設定します。 *hostname* | *ip-address* には、リモート RADIUS サーバのホスト名または IP アドレスを指定します。 **auth-port** *port-number* には、認証要求の UDP 宛先ポートを指定します。デフォルト値は 1812 です。指定できる範囲は 0 ～ 65536 です。 **key** *string* には、スイッチと RADIUS サーバ上で動作する RADIUS デーモンとの間で使用する認証キーおよび暗号キーを指定します。key は文字列であり、RADIUS サーバで使用されている暗号キーと一致する必要があります。 **（注）** キーは、**radius-server host** コマンド構文の末尾で設定してください。これは、先頭のスペースは無視されるが、キーの文字列内または末尾のスペースは使用されるためです。キーにスペースを使用する場合は、引用符がキーの一部分である場合を除き、引用符でキーを囲まないでください。キーは RADIUS デーモンで使用する暗号に一致している必要があります。 複数の RADIUS サーバを使用する場合は、このコマンドを再度入力します。
ステップ 3	**end**	特権 EXEC モードに戻ります。
ステップ 4	**show running-config**	設定を確認します。
ステップ 5	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

指定した RADIUS サーバを消去するには、**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 を認可ポートとして使用し、暗号キーを *rad123* に設定して、RADIUS サーバ上でキーを一致させる例を示します。

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

radius-server host グローバル コンフィギュレーション コマンドを使用して、タイムアウト、再送信回数、暗号キーの値を、すべての RADIUS サーバにグローバルに設定できます。これらのオプションをサーバ単位で設定するには、**radius-server timeout**、**radius-server retransmit**、および **radius-server key** グローバル コンフィギュレーション コマンドを使用します。詳細については、「すべての RADIUS サーバに対する設定」（P.11-34）を参照してください。

RADIUS サーバ上でも、いくつかの値を設定する必要があります。これらの設定値としては、スイッチの IP アドレス、およびサーバとスイッチの両方で共有されるキー文字列があります。詳細については、RADIUS サーバのマニュアルを参照してください。

ホスト モードの設定

802.1X 認可ポートで単一のホスト（クライアント）または複数のホストを許可するには、特権 EXEC モードで次の手順を実行します。マルチドメイン認証（MDA）を設定して、同じスイッチ ポートでホストと IP Phone（シスコ製品またはシスコ以外の製品）などの音声装置の両方を認証できるようにするには、**multi-domain** キーワードを使用します。

この手順は任意です。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**radius-server vsa send authentication**	ベンダー固有属性（VSA）を認識および使用するようにネットワーク アクセス サーバを設定します。
ステップ 3	**interface** *interface-id*	複数のホストが間接的に接続されるポートを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	**authentication host-mode** [**multi-auth** | **multi-domain** | **multi-host** | **single-host**] または **dot1x host-mode** {**single-host** | **multi-host** | **multi-domain**}	キーワードの意味は次のとおりです。 • **multi-auth** : 音声 VLAN 上で 1 つのクライアントを許可し、データ VLAN 上で複数の認証済みクライアントを許可します。各ホストは個別に認証されます。 （注）　**multi-auth** キーワードは、**authentication host-mode** コマンドだけで使用できます。 • **multi-host** : 単一のホストが認証されたあと、802.1X 認可ポートで複数のホストを許可します。 • **multi-domain** : ホストと、IP Phone（シスコ製品またはシスコ以外の製品）などの音声装置の両方を、802.1X 認可ポートで認証できるようにします。 （注）　ホスト モードを **multi-domain** に設定する場合、IP Phone 用に音声 VLAN を設定する必要があります。詳細については、第 18 章「音声 VLAN の設定」を参照してください。 • **single-host** : 802.1X 認可ポートでシングル ホスト（クライアント）を許可します。 指定するインターフェイスで、**authentication port-control** または **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 セットが **auto** に設定されていることを確認してください。
ステップ 5	**switchport voice vlan** *vlan-id*	（任意）音声 VLAN を設定します。
ステップ 6	**end**	特権 EXEC モードに戻ります。

	コマンド	目的
ステップ 7	**show authentication interface** *interface-id* または **show dot1x interface** *interface-id*	設定を確認します。
ステップ 8	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

ポートで複数のホストをディセーブルにするには、**no authentication host-mode** または **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 認証をイネーブルにし、複数のホストを許可する例を示します。

```
Switch(config)# interface gigabitethernet1/2
Switch(config-if)# dot1x port-control auto
Switch(config-if)# dot1x host-mode multi-host
Switch(config-if)# end
```

次に、MDA をイネーブルにし、ホストと音声装置の両方をポートで許可する例を示します。

```
Switch(config)# interface gigabitethernet1/2
Switch(config-if)# dot1x port-control auto
Switch(config-if)# dot1x host-mode multi-domain
Switch(config-if)# switchport voice vlan 101
Switch(config-if)# end
```

定期的再認証の設定

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

クライアントの定期的な再認証をイネーブルにし、再認証の試行間隔を秒数で指定するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id*	設定するポートを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	**authentication periodic** または **dot1x reauthentication**	クライアントの定期的な再認証をイネーブルにします。デフォルトではディセーブルです。

	コマンド	目的
ステップ 4	**authentication timer** {{[**inactivity** | **reauthenticate**]} {**restart** *value*}} または **dot1x timeout reauth-period** {*seconds* | **server**}	再認証の間隔（秒）を指定します。 **authentication timer** キーワードには次の意味があります。 • **inactivity**：クライアントからのアクティビティがない場合に、クライアントを無認可にするまでの間隔（秒単位） • **reauthenticate**：自動再認証の試行を開始するまでの時間（秒単位） • **restart** *value*：無認可ポートの認証を試行するまでの間隔（秒単位） **dot1x timeout reauth-period** キーワードには次の意味があります。 • *seconds*：1 ～ 65535 の範囲で秒数を指定します。デフォルトは 3600 秒です。 • **server**：Session-Timeout RADIUS 属性（属性 [27]）および Termination-Action RADIUS 属性（属性 [29]）の値に基づいて、秒数を設定します。 このコマンドがスイッチの動作に影響するのは、定期的な再認証をイネーブルに設定した場合だけです。
ステップ 5	**end**	特権 EXEC モードに戻ります。
ステップ 6	**show authentication** *interface-id* または **show dot1x interface** *interface-id*	設定を確認します。
ステップ 7	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

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

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

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

ポートに接続されたクライアントの手動再認証

dot1x re-authenticate interface *interface-id* 特権 EXEC コマンドを入力することにより、特定のポートに接続されたクライアントをいつでも手動で再認証できます。この手順は任意です。定期的な再認証をイネーブルまたはディセーブルにするには、「定期的再認証の設定」（P.12-44）を参照してください。

次に、ポートに接続され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 gigabitethernet1/2
```

待機時間の変更

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

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

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

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 フレームに対し、EAP 応答/アイデンティティ フレームで応答します。この応答を受信しない場合、スイッチは所定の時間（再送信時間）だけ待機し、そのあとフレームを再送信します。

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

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

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id*	設定するポートを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	**dot1x timeout tx-period** *seconds*	スイッチが要求を再送信する前に、EAP 要求/アイデンティティ フレームに対するクライアントからの応答を待機する秒数を設定します。 指定できる範囲は 1 ～ 65535 です。デフォルト値は 5 秒です。
ステップ 4	**end**	特権 EXEC モードに戻ります。
ステップ 5	**show authentication** *interface-id* または **show dot1x interface** *interface-id*	設定を確認します。
ステップ 6	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

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、スイッチが要求を再送信する前に、EAP 要求/アイデンティティ フレームに対するクライアントからの応答を待機する時間を 60 秒に設定する例を示します。

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

スイッチとクライアント間のフレーム再送信回数の設定

応答が受信されない場合に、スイッチが認証プロセスを再開する前にクライアントに 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は、リンクの信頼性が低下した場合や、特定のクライアントおよび認証サーバの動作に問題がある場合など、異常な状況に対する調整を行う必要があるときに限って変更してください。

スイッチ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、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id*	設定するポートを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	**dot1x max-reauth-req** *count*	スイッチが認証プロセスを再開する前に、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 です。デフォルト値は 2 です。
ステップ 4	**end**	特権 EXEC モードに戻ります。

	コマンド	目的
ステップ 5	**show authentication interface** *interface-id* または **show dot1x interface** *interface-id*	設定を確認します。
ステップ 6	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

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、スイッチが認証プロセスを再起動する前に、EAP 要求/アイデンティティ要求を送信する回数を 5 に設定する例を示します。

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

再認証回数の設定

ポートが無認可ステートに移行する前に、スイッチが認証プロセスを再開する回数も変更できます。

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

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

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id*	設定するポートを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	**dot1x max-reauth-req** *count*	ポートが無認可ステートに移行する前に、スイッチが認証プロセスを再開する回数を設定します。指定できる範囲は 0 ～ 10 です。デフォルト値は 2 です。
ステップ 4	**end**	特権 EXEC モードに戻ります。
ステップ 5	**show authentication interface** *interface-id* または **show dot1x interface** *interface-id*	設定を確認します。
ステップ 6	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

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

次の例では、ポートが無許可ステートに移行する前に、スイッチが認証プロセスを再起動する回数を 4 に設定する方法を示します。

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

MAC 移行のイネーブル化

MAC 移行により、認証済みホストをスイッチ上のあるポートから別のポートに移行できます。

スイッチで MAC 移行をグローバルにイネーブルにするには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**authentication mac-move permit**	スイッチ上で MAC 移行をイネーブルに設定します。
ステップ 3	**end**	特権 EXEC モードに戻ります。
ステップ 4	**show running-config**	（任意）設定を確認します。
ステップ 5	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

次に、スイッチで MAC 移行をグローバルにイネーブルにする例を示します。

```
Switch(config)# authentication mac-move permit
```

MAC 置き換えのイネーブル化

MAC 置き換えによって、ホストがポート上の認証済みホストを置き換えることができます。

インターフェイス上で MAC 置き換えをイネーブルにするには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id*	設定するポートを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	**authentication violation** {**protect** | **replace** | **restrict** | **shutdown**}	インターフェイスで MAC 置き換えをイネーブルにするには、**replace** キーワードを使用します。ポートは、現行セッションを削除し、新しいホストで認証を開始します。 その他のキーワードには、次の効果があります。 • **protect**：ポートは、システム メッセージを生成せずに、予期しない MAC アドレスのパケットをドロップします。 • **restrict**：CPU によって違反パケットがドロップされ、システム メッセージが生成されます。 • **shutdown**：予期しない MAC アドレスを受信すると、ポートがエラー ディセーブル状態になります。
ステップ 4	**end**	特権 EXEC モードに戻ります。
ステップ 5	**show running-config**	設定を確認します。
ステップ 6	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

次の例では、インターフェイス上で MAC 置き換えをイネーブルにする方法を示します。

```
Switch(config)# interface gigabitethernet2/0/2
Switch(config-if)# authentication violation replace
```

802.1X アカウンティングの設定

AAA システム アカウンティングと 802.1X アカウンティングをイネーブルにすると、ロギング用にシステム リロード イベントをアカウンティング RADIUS サーバに送信できます。これにより、サーバはすべてのアクティブ 802.1X セッションが閉じていることを推測できます。

RADIUS では信頼性の低い UDP トランスポート プロトコルを使用するので、ネットワークの状態が悪いと、アカウンティング メッセージが消失する可能性があります。設定可能なアカウンティング要求の再送信回数を超えてもスイッチが RADIUS サーバからアカウンティング応答メッセージを受信しない場合、次のシステム メッセージが表示されます。

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

停止メッセージが正常に送信されない場合、次のメッセージが表示されます。

```
00:09:55: %RADIUS-4-RADIUS_DEAD: RADIUS server 172.20.246.201:1645,1646 is not responding.
```

（注） 開始メッセージ、停止メッセージ、中間更新メッセージ、およびタイム スタンプのロギングなどのアカウンティング作業を実行するように RADIUS サーバを設定する必要があります。これらの機能をオンにするには、RADIUS サーバの [Network Configuration] タブで、[Update/Watchdog packets from this AAA client] のロギングをイネーブルにします。次に、RADIUS サーバの [System Configuration] タブで、[CVS RADIUS Accounting] をイネーブルにします。

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

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

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

次に、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、RADIUS サーバを設定し、アカウンティング用の UDP ポートとして 1813 を指定します。

```
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 を設定すると、サーバが EAP 要求/アイデンティティ フレームに対する応答を受信しない場合に、802.1X に対応していないクライアントがゲスト VLAN に置かれます。802.1X に対応しているが、認証に失敗したクライアントには、ネットワーク アクセスが許可されません。スイッチは、シングルホスト モードまたはマルチホスト モードでゲスト VLAN をサポートします。

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

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id*	設定するポートを指定し、インターフェイス コンフィギュレーション モードを開始します。サポートされているポート タイプについては、「802.1X 認証の設定時の注意事項」（P.12-35）を参照してください。
ステップ 3	**switchport mode access** または **switchport mode private-vlan host**	ポートをアクセス モードに設定します。 または レイヤ 2 ポートをプライベート VLAN ホスト ポートとして設定します。
ステップ 4	**authentication port-control auto** または **dot1x port-control auto**	ポートで 802.1X 認証をイネーブルにします。
ステップ 5	**dot1x guest-vlan** *vlan-id*	アクティブ VLAN を 802.1X ゲスト VLAN として指定します。指定できる範囲は 1 ～ 4094 です。 内部 VLAN（ルーテッド ポート）、RSPAN VLAN、プライマリ プライベート VLAN、または音声 VLAN 以外の任意のアクティブ VLAN を、802.1X ゲスト VLAN として設定できます。
ステップ 6	**end**	特権 EXEC モードに戻ります。
ステップ 7	**show authentication** *interface-id* または **show dot1x interface** *interface-id*	設定を確認します。
ステップ 8	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

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

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

```
Switch(config)# interface gigabitethernet1/2
Switch(config-if)# dot1x guest-vlan 2
```

次に、スイッチの待機時間を 3 秒に設定し、スイッチが要求を再送信する前に EAP 要求/アイデンティティ フレームに対するクライアントからの応答を待機する秒数を 15 秒に設定し、802.1X ポートが DHCP クライアントに接続されているときに VLAN 2 を 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

スイッチで制限付き VLAN を設定すると、認証サーバが有効なユーザ名およびパスワードを受信しない場合に、802.1X に準拠するクライアントが制限付き VLAN に移行します。スイッチは、シングルホスト モードでだけ制限付き VLAN をサポートします。

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

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id*	設定するポートを指定し、インターフェイス コンフィギュレーション モードを開始します。サポートされているポート タイプについては、「802.1X 認証の設定時の注意事項」（P.12-35）を参照してください。
ステップ 3	**switchport mode access** または **switchport mode private-vlan host**	ポートをアクセス モードに設定します。 または レイヤ 2 ポートをプライベート VLAN ホスト ポートとして設定します。
ステップ 4	**authentication port-control auto** または **dot1x port-control auto**	ポートで 802.1X 認証をイネーブルにします。
ステップ 5	**authentication event fail action authorize** *vlan-id*	アクティブ VLAN を 802.1X 制限付き VLAN として指定します。指定できる範囲は 1 ～ 4094 です。 内部 VLAN（ルーテッド ポート）、RSPAN VLAN、プライマリ プライベート VLAN、または音声 VLAN 以外の任意のアクティブ VLAN を、802.1X 制限付き VLAN として設定できます。
ステップ 6	**end**	特権 EXEC モードに戻ります。
ステップ 7	**show authentication** *interface-id* または **show dot1x interface** *interface-id*	（任意）設定を確認します。
ステップ 8	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

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

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

```
Switch(config)# interface gigabitethernet1/2
Switch(config-if)# dot1x auth-fail vlan 2
```

dot1x auth-fail max-attempts インターフェイス コンフィギュレーション コマンドを使用して、ユーザが制限付き VLAN に割り当てられる前に許可される最大認証試行回数を設定できます。許容可能な認証試行回数の範囲は 1 ～ 3 回です。デフォルト値は 3 回です。

認証試行の最大許容回数を設定するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id*	設定するポートを指定し、インターフェイス コンフィギュレーション モードを開始します。サポートされているポート タイプについては、「802.1X 認証の設定時の注意事項」（P.12-35）を参照してください。
ステップ 3	**switchport mode access** または **switchport mode private-vlan host**	ポートをアクセス モードに設定します。 または レイヤ 2 ポートをプライベート VLAN ホスト ポートとして設定します。
ステップ 4	**authentication port-control auto** または **dot1x port-control auto**	ポートで 802.1X 認証をイネーブルにします。
ステップ 5	**dot1x auth-fail vlan** *vlan-id*	アクティブ VLAN を 802.1X 制限付き VLAN として指定します。指定できる範囲は 1 ～ 4094 です。 内部 VLAN（ルーテッド ポート）、RSPAN VLAN、プライマリ プライベート VLAN、または音声 VLAN 以外の任意のアクティブ VLAN を、802.1X 制限付き VLAN として設定できます。
ステップ 6	**dot1x auth-fail max-attempts** *max attempts*	ポートが制限付き VLAN に移行する前に許可する認証試行の回数を指定します。指定できる範囲は 1 ～ 3 です。デフォルト値は 3 です。
ステップ 7	**end**	特権 EXEC モードに戻ります。
ステップ 8	**show authentication** *interface-id* または **show dot1x interface** *interface-id*	（任意）設定を確認します。
ステップ 9	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

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

次に、ポートが制限付き VLAN に移行する前に許可される認証試行の回数を *2* 回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

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

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

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**radius-server dead-criteria time** *time* **tries** *tries*	（任意）RADIUS サーバが使用不可または*停止状態*であると判断するために使用する条件を設定します。 *time* の範囲は 1 ～ 120 秒です。スイッチは、10 ～ 60 秒のデフォルトの *seconds* 値をダイナミックに決定します。 *tries* の範囲は 1 ～ 100 です。スイッチは、10 ～ 100 のデフォルトの *tries* パラメータをダイナミックに決定します。
ステップ 3	**radius-server deadtime** *minutes*	（任意）RADIUS サーバに要求が送信されない分数を設定します。指定できる範囲は 0 ～ 1440 分（24 時間）です。デフォルト値は 0 分です。
ステップ 4	**radius-server host** *ip-address* [**acct-port** *udp-port*] [**auth-port** *udp-port*] [**test username** *name* [**idle-time** *time*] [**ignore-acct-port**] [**ignore-auth-port**]] [**key** *string*]	（任意）次のキーワードを使用して RADIUS サーバのパラメータを設定します。 • **acct-port** *udp-port :* RADIUS アカウンティング サーバ用の 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 1646 です。 • **auth-port** *udp-port :* RADIUS 認証サーバ用の 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。 **（注）** RADIUS アカウンティング サーバ用の UDP ポートと、RADIUS 認証サーバ用の UDP ポートは、デフォルト以外の値に設定する必要があります。 • **test username** *name* : RADIUS サーバ ステータスの自動テストをイネーブルにし、使用するユーザ名を指定します。 • **idle-time** *time :* スイッチがサーバにテスト パケットを送信したあとの間隔を分単位で設定します。設定できる範囲は 1 ～ 35791 分です。デフォルト値は 60 分（1 時間）です。 • **ignore-acct-port** *:* RADIUS サーバのアカウンティング ポートのテストをディセーブルにします。 • **ignore-auth-port** *:* RADIUS サーバの認証ポートのテストをディセーブルにします。 • **key** *string :* スイッチと RADIUS デーモンの間のすべての RADIUS 通信のための認証キーおよび暗号キーを指定します。 **（注）** キーは、**radius-server host** コマンド構文の末尾で設定してください。これは、先頭のスペースは無視されるが、キーの文字列内または末尾のスペースは使用されるためです。キーにスペースを使用する場合は、引用符がキーの一部分である場合を除き、引用符でキーを囲まないでください。キーは RADIUS デーモンで使用する暗号に一致している必要があります。 **radius-server key** {**0** *string* | **7** *string* | *string*} グローバル コンフィギュレーション コマンドを使用して、認証キーおよび暗号キーを設定することもできます。

	コマンド	目的
ステップ 5	**dot1x critical** {**eapol** | **recovery delay** *milliseconds*}	（任意）アクセス不能認証バイパス用のパラメータを設定します。 **eapol**：スイッチがクリティカル ポートを正常に認証したときに EAPOL-Success メッセージを送信するように指定します。 **recovery delay** *milliseconds*：使用不可の RADIUS サーバが使用可能になったときにスイッチがクリティカル ポートの再初期化を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。デフォルト値は 1000 ミリ秒です（ポートを 1 秒おきに再初期化できます）。
ステップ 6	**interface** *interface-id*	設定するポートを指定し、インターフェイス コンフィギュレーション モードを開始します。サポートされているポート タイプについては、「802.1X 認証の設定時の注意事項」（P.12-35）を参照してください。
ステップ 7	**authentication event server dead action [authorize | reinitialize] vlan** *vlan-id*	RADIUS サーバに到達できない場合にポート上のホストを移行するには、次のキーワードを使用します。 • **authorize**：認証を試みるすべての新しいホストを、ユーザ指定のクリティカル VLAN に移行します。 • **reinitialize**：ポート上のすべての認可済みホストをユーザ指定のクリティカル VLAN に移行します。
ステップ 8	**dot1x critical** [**recovery action reinitialize** | **vlan** *vlan-id*]	アクセス不能認証バイパス機能をイネーブルにし、次のキーワードを使用してこの機能を設定します。 • **recovery action reinitialize**：回復機能をイネーブルにし、認証サーバが使用可能の場合に回復アクションによりポートを認証するよう指定します。 • **vlan** *vlan-id*：スイッチがクリティカル ポートを割り当てることができるアクセス VLAN を指定します。指定できる範囲は 1 ～ 4094 です。
ステップ 9	**end**	特権 EXEC モードに戻ります。
ステップ 10	**show authentication interface** *interface-id* または **show dot1x interface** *interface-id*	（任意）設定を確認します。
ステップ 11	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

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

次に、アクセス不能認証バイパス機能を設定する例を示します。

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

802.1X 認証と WoL の設定

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

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id*	設定するポートを指定し、インターフェイス コンフィギュレーション モードを開始します。サポートされているポート タイプについては、「802.1X 認証の設定時の注意事項」（P.12-35）を参照してください。
ステップ 3	**authentication control-direction {both | in}** または **dot1x control-direction {both | in}**	ポートで 802.1X 認証と WoL をイネーブルにし、次のキーワードを使用してポートを双方向または単一方向に設定します。 • **both**：ポートを双方向に設定します。ポートは、ホストにパケットを送受信できません。デフォルトでは、ポートは双方向です。 • **in**：ポートを単一方向に設定します。ポートは、ホストにパケットを送信できますが、受信はできません。
ステップ 4	**end**	特権 EXEC モードに戻ります。
ステップ 5	**show authentication interface** *interface-id* または **show dot1x interface** *interface-id*	設定を確認します。
ステップ 6	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

802.1X 認証と WoL をディセーブルにするには、**no authentication control-direction** または **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、802.1X 認証と WoL をイネーブルにし、ポートを双方向に設定する例を示します。

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

または

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

MAC 認証バイパスの設定

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

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id*	設定するポートを指定し、インターフェイス コンフィギュレーション モードを開始します。サポートされているポート タイプについては、「802.1X 認証の設定時の注意事項」（P.12-35）を参照してください。
ステップ 3	**authentication port-control auto** または **dot1x port-control auto**	ポートで 802.1X 認証をイネーブルにします。
ステップ 4	**dot1x mac-auth-bypass** [**eap** | **timeout activity** {*value*}]	MAC 認証バイパスをイネーブルにします。 （任意）認可に EAP を使用するようにスイッチを設定するには、**eap** キーワードを使用します。 （任意）接続されているホストを無認可ステートにする前に非アクティブにできる秒数を設定するには、**timeout activity** キーワードを使用します。指定できる範囲は 1 ～ 65535 です。 タイムアウト値を設定する前に、ポート セキュリティをイネーブルにする必要があります。詳細については、「ポート セキュリティの設定」（P.29-9）を参照してください。
ステップ 5	**end**	特権 EXEC モードに戻ります。
ステップ 6	**show authentication** *interface-id* または **show dot1x interface** *interface-id*	設定を確認します。
ステップ 7	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

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 認証バイパスをイネーブルにする方法を示します。

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

802.1X ユーザ分散の設定

VLAN グループを設定し、その VLAN グループに VLAN をマッピングするには、グローバル コンフィギュレーションで次の手順を実行します。

	コマンド	目的
ステップ 1	**vlan group** *vlan-group-name* ***vlan-list*** *vlan-list*	VLAN グループを設定し、そのグループに 1 つの VLAN または VLAN の範囲をマッピングします。
ステップ 2	**show vlan group all** *vlan-group-name*	設定を確認します。
ステップ 3	**no vlan group** ***vlan-group-name*** **vlan-list** *vlan-list*	VLAN グループ設定または VLAN グループ設定の要素を消去します。

次に、VLAN グループを設定し、そのグループに VLAN をマッピングし、VLAN グループ設定および指定した VLAN へのマッピングを確認する例を示します。

```
switch(config)# vlan group eng-dept vlan-list 10

switch(config)# show vlan group group-name eng-dept
Group Name                      Vlans Mapped
--------------                  --------------
eng-dept                        10
switch# show dot1x vlan-group all
Group Name                      Vlans Mapped
--------------                  --------------
eng-dept                        10
hr-dept                         20
```

次に、既存の VLAN グループに VLAN を追加し、VLAN が追加されたことを確認する例を示します。

```
switch(config)# vlan group eng-dept vlan-list 30
switch(config)# show vlan group eng-dept
Group Name                      Vlans Mapped
--------------                  --------------
eng-dept                        10,30
```

次に、VLAN グループから VLAN を削除する例を示します。

```
switch# no vlan group eng-dept vlan-list 10
```

次に、VLAN グループからすべての VLAN を消去したときに、VLAN グループを消去する例を示します。

```
switch(config)# no vlan group eng-dept vlan-list 30
Vlan 30 is successfully cleared from vlan group eng-dept.

switch(config)# show vlan group group-name eng-dept
```

次に、すべての VLAN グループを消去する例を示します。

```
switch(config)# no vlan group end-dept vlan-list all
switch(config)# show vlan-group all
```

これらのコマンドの詳細については、『*Cisco IOS Security Command Reference*』を参照してください。

NAC レイヤ 2 802.1X 検証の設定

NAC レイヤ 2 802.1X 検証を設定できます。この機能は、RADIUS サーバによる 802.1X 認証とも呼ばれます。

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

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id*	設定するポートを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	**dot1x guest-vlan** *vlan-id*	アクティブ VLAN を 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 以外の任意のアクティブ VLAN を、802.1X ゲスト VLAN として設定できます。
ステップ 4	**authentication periodic** または **dot1x reauthentication**	クライアントの定期的な再認証をイネーブルにします。デフォルトではディセーブルです。
ステップ 5	**dot1x timeout reauth-period** {*seconds* | **server**}	再認証の間隔（秒）を指定します。 キーワードの意味は次のとおりです。 • *seconds*：1 ～ 65535 の秒数を設定します。デフォルト値は 3600 秒です。 • **server**：Session-Timeout RADIUS 属性（属性 [27]）および Termination-Action RADIUS 属性（属性 [29]）の値に基づいて、秒数を設定します。 このコマンドがスイッチの動作に影響するのは、定期的な再認証をイネーブルに設定した場合だけです。
ステップ 6	**end**	特権 EXEC モードに戻ります。
ステップ 7	**show authentication interface** *interface-id* または **show dot1x interface** *interface-id*	802.1X 認証の設定を確認します。
ステップ 8	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

次に、NAC レイヤ 2 802.1X 検証を設定する例を示します。

```
Switch# configure terminal
Switch(config)# interface gigabitethernet1/1
Switch(config-if)# dot1x reauthentication
Switch(config-if)# dot1x timeout reauth-period server
```

オーセンティケータおよびサプリカント スイッチと NEAT の設定

この機能を設定するには、配線クローゼットの外部にある 1 つのスイッチをサプリカントとして設定し、オーセンティケータ スイッチに接続する必要があります。

概要については、「802.1X サプリカント スイッチおよびオーセンティケータ スイッチと Network Edge Access Topology（NEAT; ネットワーク エッジ アクセス トポロジ）」（P.12-30）を参照してください。

（注）　ACS で *cisco-av-pairs* を *device-traffic-class=switch* として設定する必要があります。これにより、サプリカントが正常に認証されたあとにインターフェイスがトランクとして設定されます。

スイッチをオーセンティケータとして設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**cisp enable**	CISP をイネーブルにします。
ステップ 3	**interface** *interface-id*	設定するポートを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	**switchport mode access**	ポート モードを **access** に設定します。
ステップ 5	**authentication port-control auto**	ポート認証モードを自動に設定します。
ステップ 6	**dot1x pae authenticator**	インターフェイスを Port Access Entity（PAE; ポート アクセス エンティティ）オーセンティケータとして設定します。
ステップ 7	**spanning-tree portfast**	1 つのワークステーションまたはサーバに接続されたアクセス ポートで PortFast をイネーブルにします。
ステップ 8	**end**	特権 EXEC モードに戻ります。
ステップ 9	**show running-config interface** *interface-id*	設定を確認します。
ステップ 10	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

次に、スイッチを 802.1X オーセンティケータとして設定する例を示します。

```
Switch# configure terminal
Switch(config)# cisp enable
Switch(config)# interface gigabitethernet1/1
Switch(config-if)# switchport mode access
Switch(config-if)# authentication port-control auto
Switch(config-if)# dot1x pae authenticator
Switch(config-if)# spanning-tree portfast trunk
```

スイッチをサプリカントとして設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**cisp enable**	CISP をイネーブルにします。
ステップ 3	**dot1x credentials** *profile*	802.1X クレデンシャル プロファイルを作成します。このクレデンシャル プロファイルは、サプリカントとして設定されたポートに割り当てる必要があります。
ステップ 4	**username** *suppswitch*	ユーザ名を作成します。

	コマンド	目的
ステップ 5	**password** *password*	新しいユーザ名用のパスワードを作成します。
ステップ 6	**dot1x supplicant force-multicast**	スイッチに対し、ユニキャスト パケットまたはマルチキャスト パケットを受信したときにマルチキャスト EAPOL パケット*だけ*を送信するように強制します。 これにより、すべてのホスト モードのサプリカント スイッチで NEAT を動作させることも可能になります。
ステップ 7	**interface** *interface-id*	設定するポートを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 8	**switchport trunk encapsulation dot1q**	ポートをトランク モードに設定します。
ステップ 9	**switchport mode trunk**	インターフェイスを VLAN トランク ポートとして設定します。
ステップ 10	**dot1x pae supplicant**	インターフェイスをポート アクセス エンティティ（PAE）サプリカントとして設定します。
ステップ 11	**dot1x credentials** *profile-name*	802.1X クレデンシャル プロファイルをインターフェイスに割り当てます。
ステップ 12	**end**	特権 EXEC モードに戻ります。
ステップ 13	**show running-config interface** *interface-id*	設定を確認します。
ステップ 14	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

次の例では、スイッチをサプリカントとして設定する方法を示します。

```
Switch# configure terminal
Switch(config)# cisp enable
Switch(config)# dot1x credentials test
Switch(config)# username suppswitch
Switch(config)# password myswitch
Switch(config)# dot1x supplicant force-multicast
Switch(config)# interface gigabitethernet1/1
Switch(config-if)# switchport trunk encapsulation dot1q
Switch(config-if)# switchport mode trunk
Switch(config-if)# dot1x pae supplicant
Switch(config-if)# dot1x credentials test
Switch(config-if)# end
```

Smartports マクロでの NEAT の設定

スイッチ VSA の代わりに Smartports ユーザ定義マクロを使用してオーセンティケータ スイッチを設定することもできます。詳細については、第 15 章「SmartPort マクロの設定」を参照してください。

802.1X 認証とダウンロード可能 ACL およびリダイレクト URL の設定

スイッチでの 802.1X 認証の設定に加えて、ACS を設定する必要があります。詳細については、Cisco Secure ACS の各種コンフィギュレーション ガイドを参照してください。

（注） ダウンロード可能 ACL をスイッチにダウンロードする前に、ACS 上でダウンロード可能 ACL を設定する必要があります。

ポートでの認証後に、**show ip access-list** 特権 EXEC コマンドを使用してポート上のダウンロード可能 ACL を表示できます。

ダウンロード可能 ACL の設定

ポリシーは、クライアントが認証され、クライアントの IP アドレスが IP 装置追跡テーブルに追加されたあとに有効になります。次に、スイッチはダウンロード可能 ACL をポートに適用します。

特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ip device tracking**	IP 装置追跡テーブルを設定します。
ステップ 3	**aaa new-model**	AAA をイネーブルにします。
ステップ 4	**aaa authorization network default group radius**	認可方式をローカルに設定します。認可方式を削除するには、**no aaa authorization network default group radius** コマンドを使用します。
ステップ 5	**radius-server vsa send authentication**	RADIUS VSA 送信認証を設定します。
ステップ 6	**interface** *interface-id*	設定するポートを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 7	**ip access-group** *acl-id* **in**	input 方向のポートでデフォルト ACL を設定します。 **（注）**　*acl-id* は、アクセス リストの名前または番号です。
ステップ 8	**show running-config interface** *interface-id*	設定を確認します。
ステップ 9	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

ダウンロード可能ポリシーの設定

特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**access-list** *access-list-number* **deny source** *source-wildcard* **log**	送信元アドレスとワイルドカードを使用して、デフォルトのポート ACL を定義します。 access-list-number 値は、1 ～ 99 または 1300 ～ 1999 の範囲の 10 進数値です。 **deny** または **permit** を入力して、条件が一致した場合にアクセスを拒否するのか許可するのかを指定します。 *source* 値は、パケットを送信するネットワークまたはホストの送信元アドレスであり、次のようなものになります。 • ドット付き 10 進表記による 32 ビット長の値。 • source、および source-wildcard 値 0.0.0.0 255.255.255.255 の略を意味するキーワード any。source-wildcard 値を入力する必要はありません。 • source および source-wildcard 値 source 0.0.0.0 の略を意味するキーワード host。 （任意）source-wildcard を使用して、ワイルドカード ビットを送信元アドレスに適用します。 （任意）log を入力すると、エントリと一致するパケットの詳細を示すロギング メッセージがコンソールに送信されます。
ステップ 3	**interface** *interface-id*	インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	**ip access-group** *acl-id* **in**	input 方向のポートでデフォルト ACL を設定します。 **（注）**　*acl-id* は、アクセス リストの名前または番号です。
ステップ 5	**exit**	グローバル コンフィギュレーション モードに戻ります。
ステップ 6	**aaa new-model**	AAA をイネーブルにします。
ステップ 7	**aaa authorization network default group radius**	認可方式をローカルに設定します。認可方式を削除するには、**no aaa authorization network default group radius** コマンドを使用します。
ステップ 8	**ip device tracking**	IP 装置追跡テーブルをイネーブルにします。 IP 装置追跡テーブルをディセーブルにするには、**no ip device tracking** グローバル コンフィギュレーション コマンドを使用します。
ステップ 9	**ip device tracking probe** [**count** | **interval** | **use-svi**]	（任意）IP 装置追跡テーブルを設定します。 • **count** *count*：スイッチが ARP プローブを送信する回数を設定します。指定できる範囲は 1 ～ 5 です。デフォルト値は 3 です。 • **interval** *interval*：スイッチが ARP プローブを再送信する前に、応答を待機する秒数を設定します。指定できる範囲は 30 ～ 300 秒です。デフォルト値は 30 秒です。 • **use-svi**：Switch Virtual Interface（SVI; スイッチ仮想インターフェイス）IP アドレスを ARP プローブの送信元として使用します。
ステップ 10	**radius-server vsa send authentication**	ベンダー固有属性を認識および使用するようにネットワーク アクセス サーバを設定します。 **（注）**　ダウンロード可能 ACL が動作可能である必要があります。
ステップ 11	**end**	特権 EXEC モードに戻ります。

	コマンド	目的
ステップ 12	**show ip device tracking all**	IP 装置追跡テーブル内の各エントリの情報を表示します。
ステップ 13	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

次に、ダウンロード可能ポリシー用にスイッチを設定する例を示します。

```
Switch# config terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# aaa new-model
Switch(config)# aaa authorization network default group radius
Switch(config)# ip device tracking
Switch(config)# ip access-list extended default_acl
Switch(config-ext-nacl)# permit ip any any
Switch(config-ext-nacl)# exit
Switch(config)# radius-server vsa send authentication
Switch(config)# interface gigabitethernet1/1
Switch(config-if)# ip access-group default_acl in
Switch(config-if)# exit
```

VLAN ID ベースの MAC 認証の設定

特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**mab request format attribute 32 vlan access-vlan**	VLAN ID ベースの MAC 認証をイネーブルにします。
ステップ 3	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

VLAN ID ベースの MAC 認証のステータスを確認する show コマンドはありません。**debug radius accounting** 特権 EXEC コマンドを使用すると、RADIUS 属性 32 を確認できます。このコマンドの詳細については、『*Cisco IOS Debug Command Reference, Release 12.2*』を参照してください。
http://www.cisco.com/en/US/docs/ios/debug/command/reference/db_q1.html#wp1123741

次に、スイッチで VLAN ID ベースの MAC 認証をグローバルにイネーブルにする例を示します。

```
Switch# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# mab request format attribute 32 vlan access-vlan
Switch(config-if)# exit
```

フレキシブルな認証順序付けの設定

特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id*	設定するポートを指定し、インターフェイス コンフィギュレーション モードを開始します。

	コマンド	目的
ステップ 3	**authentication order** [**dot1x** | **mab**] | {**webauth**}	（任意）ポートで使用する認証方式の順序を設定します。
ステップ 4	**authentication priority** [**dot1x** | **mab**] | {**webauth**}	（任意）認証方式をポート プライオリティ リストに追加します。
ステップ 5	**show authentication**	（任意）設定を確認します。
ステップ 6	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

次に、ポートが最初に 802.1X 認証を試行し、次に Web 認証をフォールバック方式として試行するように設定する例を示します。

```
Switch# configure terminal
Switch(config)# interface gigabitethernet1/1
Switch(config)# authentication order dot1x webauth
```

Open1x の設定

特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id*	設定するポートを指定し、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	**authentication control-direction** {**both** | **in**}	（任意）ポート制御を単一方向または双方向に設定します。
ステップ 4	**authentication fallback** *name*	（任意）802.1X 認証をサポートしないクライアント用のフォールバック方式として Web 認証を使用するようにポートを設定します。
ステップ 5	**authentication host-mode** [**multi-auth** | **multi-domain** | **multi-host** | **single-host**]	（任意）ポートで認可マネージャ モードを設定します。
ステップ 6	**authentication open**	（任意）ポートでオープン アクセスをイネーブルまたはディセーブルにします。
ステップ 7	**authentication order** [**dot1x** | **mab**] | {**webauth**}	（任意）ポートで使用する認証方式の順序を設定します。
ステップ 8	**authentication periodic**	（任意）ポートで再認証をイネーブルまたはディセーブルにします。
ステップ 9	**authentication port-control** {**auto** | **force-authorized** | **force-un authorized**}	（任意）ポートの認可ステートの手動制御をイネーブルにします。
ステップ 10	**show authentication**	（任意）設定を確認します。
ステップ 11	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

次に、ポートで Open1x を設定する例を示します。

```
Switch# configure terminal
Switch(config)# interface gigabitethernet1/1
Switch(config)# authentication control-direction both
Switch(config)# au ten tic at ion fallback profile1
Switch(config)# authentication host-mode multi-auth
Switch(config)# authentication open
Switch(config)# authentication order dot1x webauth
Switch(config)# authentication periodic
Switch(config)# authentication port-control auto
```

ポートでの 802.1X 認証のディセーブル化

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

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id*	設定するポートを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	**no dot1x pae**	ポートで 802.1X 認証をディセーブルにします。
ステップ 4	**end**	特権 EXEC モードに戻ります。
ステップ 5	**show authentication** *interface-id* または **show dot1x interface** *interface-id*	設定を確認します。
ステップ 6	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

ポートを 802.1X ポート アクセス エンティティ（PAE）オーセンティケータとして設定し、ポートで 802.1X をイネーブルにしてポートに接続したクライアントが許可されないようにするには、**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。

次に、ポートで 802.1X 認証をディセーブルにする例を示します。

```
Switch(config)# interface gigabitethernet1/1
Switch(config-if)# no dot1x pae authenticator
```

802.1X 認証設定のデフォルト値へのリセット

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

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id*	インターフェイス コンフィギュレーション モードを開始し、設定するポートを指定します。
ステップ 3	**dot1x default**	802.1X パラメータをデフォルト値にリセットします。
ステップ 4	**end**	特権 EXEC モードに戻ります。
ステップ 5	**show authentication interface** *interface-id* または **show dot1x interface** *interface-id*	設定を確認します。
ステップ 6	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

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** 特権 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* 特権 EXEC コマンドを使用します。

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

Cisco IOS Release 12.2(55)SE 以降、**no dot1x logging verbose** 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、詳細な 802.1X 認証メッセージをフィルタリングできるようになりました。「認証マネージャの CLI コマンド」（P.12-9）を参照してください。

これらの出力に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。