CHAPTER 9

IEEE 802.1X ポートベース認証の設定

IEEE 802.1X ポートベース認証は、不正なデバイス（クライアント）によるネットワーク アクセスを防止します。

Catalyst 3560 スイッチ コマンド リファレンスと『Cisco IOS Security Command Reference, Release 12.2』の「RADIUS Commands」のセクションに、コマンドの構文および使用方法の詳細が記載されています。

スイッチは、Cisco TrustSec の Security Group Tag（SGT）Exchange Protocol（SXP）もサポートします。この機能では、Security Group Access Control List（SGACL; セキュリティ グループ アクセス コントロール リスト）がサポートされます。これは IP アドレスではなく、デバイスのグループに対する ACL ポリシーを定義します。SXP 制御プロトコルを使用すると、ハードウェアのアップグレードなしに SGT によるパケットのタグ付けを行うことができます。SXP 制御プロトコルは Cisco TrustSec ドメイン エッジのアクセス レイヤ デバイスと Cisco TrustSec ドメイン内のディストリビューション レイヤ デバイス間で実行されます。Catalyst 3750-X および 3560-X スイッチは、Cisco TrustSec ネットワーク内でアクセス レイヤ スイッチとして動作します。

Cisco TrustSec の詳細については、次の URL にある『*Cisco TrustSec Switch Configuration Guide*』を参照してください。
http://www.cisco.com/en/US/docs/switches/lan/trustsec/configuration/guide/trustsec.html

SXP のセクションでは、Catalyst 3560 スイッチでサポートされる機能を定義します。

この章で説明する内容は、次のとおりです。

IEEE 802.1X ポートベース認証の概要

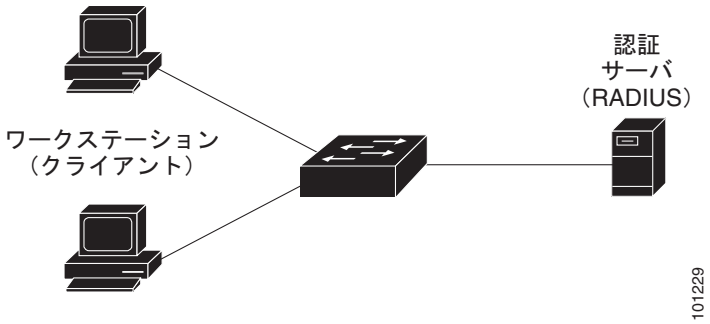
この規格では、不正なクライアントがアクセス可能なポートから LAN に接続しないように規制する、クライアント/サーバ型のアクセス制御および認証プロトコルを定めています。認証サーバがスイッチ ポートに接続する各クライアントを認証したうえで、スイッチまたは LAN サービスを利用できるようにします。

IEEE 802.1X アクセス制御では、クライアントを認証するまでの間、そのクライアントが接続しているポート経由では Extensible Authentication Protocol over LAN（EAPOL）、Cisco Discovery Protocol（CDP）、および 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、通常のトラフィックがポート経由で送受信されます。

デバイスの役割

802.1X ポートベース認証でのデバイスの役割

図 9-1　802.1X におけるデバイスの役割



- *クライアント*：LAN およびスイッチ サービスへのアクセスを要求し、スイッチからの要求に応答するデバイス（ワークステーション）。ワークステーションでは、Microsoft Windows XP OS（オペレーティング システム）に付属しているような 802.1X 準拠のクライアント ソフトウェアを実行する必要があります（クライアントは、802.1X 規格では*サプリカント*といいます）。

（注） Windows XP のネットワーク接続と 802.1x 認証の問題を解決するには、次の URL にある「Microsoft Knowledge Base」を参照してください。
http://support.microsoft.com/support/kb/articles/Q303/5/97.ASP

- *認証サーバ*：クライアントの実際の認証を行います。認証サーバはクライアントの識別情報を確認し、そのクライアントに LAN およびスイッチ サービスへのアクセスを許可すべきかどうかをスイッチに通知します。スイッチはプロキシとして動作するので、認証サービスはクライアントに対して透過的に行われます。今回のリリースでサポートされる認証サーバは、Extensible Authentication Protocol（EAP）拡張機能を備えた Remote Authentication Dial-In User Service（RADIUS）セキュリティ システムだけです。これは Cisco Secure Access Control Server バージョン 3.0 以降で利用できます。RADIUS はクライアント/サーバ モデルで動作し、RADIUS サーバと 1 つまたは複数の RADIUS クライアントとの間でセキュア認証情報を交換します。
- *スイッチ*（エッジ スイッチまたはワイヤレス アクセス ポイント）：クライアントの認証ステータスに基づいて、ネットワークへの物理アクセスを制御します。スイッチはクライアントと認証サーバとの仲介デバイス（プロキシ）として動作し、クライアントに識別情報を要求し、その情報を認証サーバで確認し、クライアントに応答をリレーします。スイッチには、EAP フレームのカプセル化とカプセル化解除、および認証サーバとの対話を処理する RADIUS クライアントが含まれています（スイッチは、802.1X 規格では*オーセンティケータ*といいます）。

  スイッチが EAPOL フレームを受信して認証サーバにリレーする場合、イーサネット ヘッダーが取り除かれ、残りの EAP フレームが RADIUS フォーマットに再カプセル化されます。カプセル化では EAP フレームの変更は行われないため、認証サーバはネイティブ フレーム フォーマットの EAP をサポートしなければなりません。スイッチが認証サーバからフレームを受信すると、サーバのフレーム ヘッダーが削除され、残りの EAP フレームがイーサネット用にカプセル化され、クライアントに送信されます。

  仲介デバイスとして動作できるものには、Catalyst 3750-E、Catalyst 3560-E、Catalyst 3750、Catalyst 3560、Catalyst 3550、Catalyst 2975、Catalyst 2970、Catalyst 2960、Catalyst 2955、Catalyst 2950、Catalyst 2940、またはワイヤレス アクセス ポイントがあります。これらのデバイスでは、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

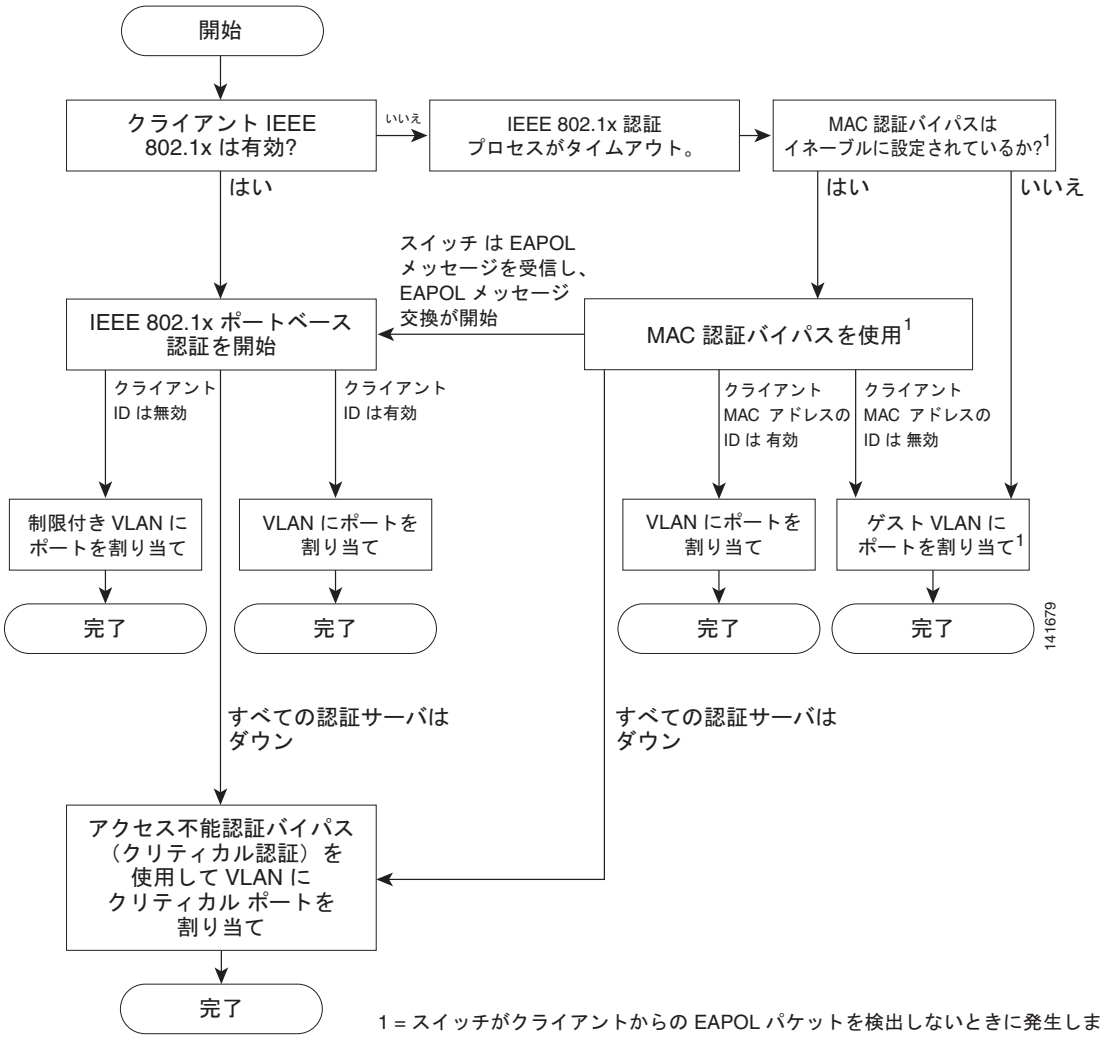
802.1X ポートベース認証がイネーブルであり、クライアントが 802.1X 準拠のクライアント ソフトウェアをサポートしている場合、次のイベントが発生します。

- クライアント ID が有効で 802.1X 認証に成功した場合、スイッチはクライアントにネットワークへのアクセスを許可します。
- EAPOL メッセージ交換の待機中に 802.1X 認証がタイムアウトし、MAC 認証バイパスがイネーブルの場合、スイッチはクライアント MAC アドレスを認証用に使用します。このクライアント MAC アドレスが有効で認証に成功した場合、スイッチ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 MAC アドレスが無効で認証に失敗した場合、ゲスト VLAN が設定されていれば、スイッチはクライアントに限定的なサービスを提供するゲスト VLAN を割り当てます。
- スイッチが 802.1X 対応クライアントから無効な ID を取得し、制限付き VLAN が指定されている場合、スイッチはクライアントに限定的なサービスを提供する制限付き VLAN を割り当てることができます。
- RADIUS 認証サーバが使用できず（ダウンしていて）アクセスできない認証バイパスがイネーブルの場合、スイッチは、RADIUS 設定 VLAN またはユーザ指定アクセス VLAN で、ポートをクリティカル認証ステートにして、クライアントにネットワークのアクセスを許可します。

（注） アクセスできない認証バイパスは、クリティカル認証、または Authentication, Authorization, Accounting（AAA; 認証、許可、アカウンティング）失敗ポリシーとも呼ばれます。

図 9-2 に、認証プロセスを示します。

図 9-2　認証フローチャート



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。

次の状況のいずれかが発生すると、スイッチはクライアントを再認証します。

- 定期的な再認証がイネーブルで、再認証タイマーの期限が切れている場合。

  スイッチ固有の値を使用するか、RADIUS サーバからの値に基づいて再認証タイマーを設定できます。

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

  Session-Timeout RADIUS アトリビュート（アトリビュート [27]）は、再認証が発生するまでの時間を指定します。

  Termination-Action RADIUS アトリビュート（アトリビュート [29]）は、再認証中に行うアクションを指定します。アクションは *Initialize* および *ReAuthenticate* に設定できます。*Initialize* アクションが設定されていると（アトリビュートの値は *DEFAULT*）、802.1X セッションが終了し、再認証中に接続が切断されます。*ReAuthenticate* アクションが設定されていると（アトリビュートの値は RADIUS-Request）、再認証中にセッションは影響を受けません。

- クライアントを手動で再認証するには、**dot1x re-authenticate interface** *interface-id* 特権 EXEC コマンドを入力します。

Multidomain Authentication（MDA; マルチ ドメイン認証）がポートでイネーブルの場合、音声認証に適用可能ないくつかの例外とともにこのフローを使用することができます。MDA の詳細については、「マルチドメイン認証」（P.9-13）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上で認証をイネーブルにした場合、スイッチはポートのリンク ステートがダウンからアップに変更した時点で、またはポートが認証されてないままアップの状態であるかぎり定期的に認証を開始します。スイッチはクライアントに EAP-Request/Identity フレームを送信し、その ID を要求します。クライアントはフレームを受信すると、EAP-Response/Identity フレームで応答します。

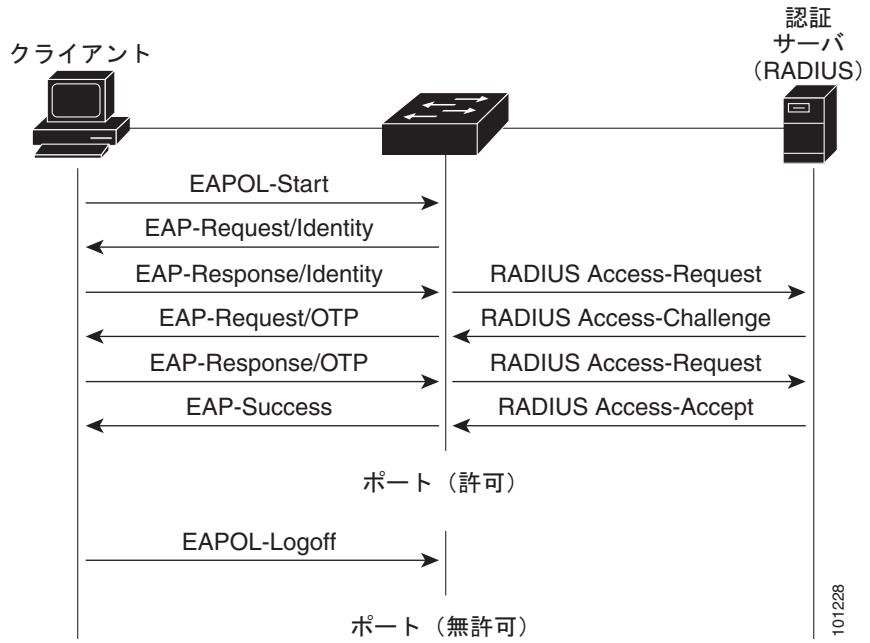
ただし、クライアントが起動時にスイッチからの EAP-Request/Identity フレームを受信しなかった場合、クライアントは EAPOL-Start フレームを送信して認証を開始できます。このフレームはスイッチに対し、クライアントの識別情報を要求するように指示します。

（注） ネットワーク アクセス デバイスで 802.1X 認証がイネーブルに設定されていない、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-Request/Identity フレームを受信しなかった場合、クライアントはポートが許可ステートであるものとしてフレームを送信します。ポートが許可ステートであるということは、クライアントの認証が成功したことを実質的に意味します。詳細については、「許可ステートおよび無許可ステートのポート」（P.9-11）を参照してください。

クライアントが自らの識別情報を提示すると、スイッチは仲介デバイスとしての役割を開始し、認証が成功または失敗するまで、クライアントと認証サーバの間で EAP フレームを送受信します。認証が成功すると、スイッチ ポートは許可ステートになります。認証に失敗した場合、認証が再試行されるか、ポートが限定的なサービスを提供する VLAN に割り当てられるか、あるいはネットワーク アクセスが許可されないかのいずれかになります。詳細については、「許可ステートおよび無許可ステートのポート」（P.9-11）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 9-3 に、クライアントが RADIUS サーバとの間で OTP（ワンタイム パスワード）認証方式を使用する際に行われるメッセージ交換を示します。

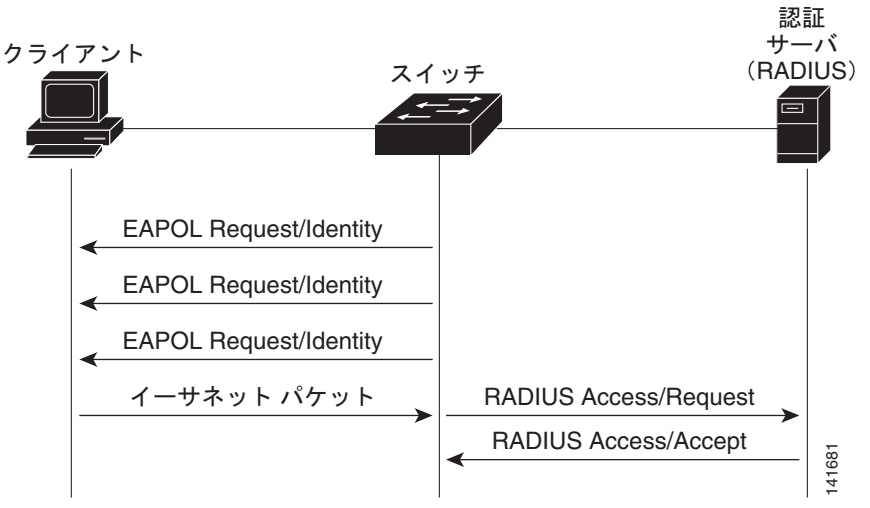
図 9-3　メッセージ交換



EAPOL メッセージ交換の待機中に 802.1X 認証がタイムアウトし、MAC 認証バイパスがイネーブルの場合、スイッチはクライアントからイーサネット パケットを検出するとそのクライアントを認証できます。スイッチは、クライアントの MAC アドレスを ID として使用し、RADIUS サーバに送信される RADIUS アクセス / 要求フレームにこの情報を保存します。サーバがスイッチに RADIUS アクセス / 承認フレームを送信（認証が成功）すると、ポートが許可されます。認証に失敗してゲスト VLAN が指定されている場合、スイッチはポートをゲスト VLAN に割り当てます。イーサネット パケットの待機中にスイッチが EAPOL パケットを検出すると、スイッチは MAC 認証バイパス プロセスを停止して、802.1X 認証を停止します。

図 9-4 に、MAC 認証バイパス中のメッセージ交換を示します。

図 9-4　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 などのその他のネットワーク デバイスで CLI コマンドやメッセージを含め、同じ認証方式を使うことができませんでした。個別の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 スイッチで同じ認証方式をサポートします。

Cisco IOS Release 12.2(55)SE は、認証マネージャからの冗長なシステム メッセージのフィルタリングをサポートします。詳細については、「認証マネージャ CLI コマンド」（P.9-10）を参照してください。

ポートベース認証方式

表 9-1 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 つのポート上で 1 つのデータ ホストまたは音声ホスト（クライアント）だけが認証されます。
- マルチ ホスト：同じポート上で複数のデータ ホストを認証できます（マルチ ホスト モードでポートが無許可になると、スイッチはそのポートに接続された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）。
- マルチドメイン認証（MDA）：データ デバイスと音声デバイスの両方を同じスイッチ ポート上で認証できます。ポートは、データ ドメインと音声ドメインに分けられます。
- マルチ認証：データ VLAN で複数のホストを認証できます。このモードで音声 VLAN が設定されている場合は、さらに 1 つのクライアントが VLAN で許可されます。

表 9-1　802.1x 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 アトリビュート ダウンロード ACL[3] リダイレクト URL [3]	VLAN 割り当て ユーザ単位 ACL Filter-ID アトリビュート ダウンロード ACL[4] リダイレクト URL [3]	VLAN 割り当て ユーザ単位 ACL[3] Filter-ID アトリビュート[3] ダウンロード ACL[3] リダイレクト URL [3]	ユーザ単位 ACL[3] Filter-ID アトリビュート[3] ダウンロード 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 アトリビュート ダウンロード ACL[3] リダイレクト URL [3]	VLAN 割り当て ユーザ単位 ACL Filter-ID アトリビュート ダウンロード ACL[3] リダイレクト URL [3]	VLAN 割り当て ユーザ単位 ACL[3] Filter-ID アトリビュート[3] ダウンロード ACL[3] リダイレクト URL [3]	ユーザ単位 ACL[3] Filter-ID アトリビュート[3] ダウンロード 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 アトリビュート、ダウンロード ACL[2]			

表 9-1　802.1x 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 アトリビュート[3] ダウンロード ACL リダイレクト URL	Filter-ID アトリビュート[3] ダウンロード ACL リダイレクト URL	Filter-ID アトリビュート[3] ダウンロード ACL リダイレクト URL	Filter-ID アトリビュート[3] ダウンロード ACL[3] リダイレクト URL [3]
フォールバック メソッドとしての Web 認証[5]	プロキシ ACL Filter-ID アトリビュート[3] ダウンロード ACL[3]	プロキシ ACL Filter-ID アトリビュート[3] ダウンロード ACL[3]	プロキシ ACL Filter-ID アトリビュート[3] ダウンロード ACL[3]	プロキシ ACL[3] Filter-ID アトリビュート[3] ダウンロード 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 認証をサポートしてい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 以前のリリースでは、ユーザ単位 ACL および 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 およびマルチ認証対応ポートのサポートが追加されました。12.2(52)SE 以降、マルチホスト モードの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、スイッチに設定された ACL は、Catalyst 6000 スイッチなどの Cisco IOS ソフトウェアを実行する別のデバイスに設定された ACL と互換性がありません。

Cisco IOS Release 12.2(50)SE 以降では、スイッチに設定された ACL は Cisco IOS リリースを実行する他のデバイスと互換性があります。

（注） ACL には送信元として **any** に限り設定できます。

（注） マルチホスト モードに設定された ACL は、ステートメントの送信元ポートに *any* を指定する必要があります（例：**permit icmp** *any* **host 10.10.1.1**）。

ACL を定義する場合は必ず、送信元ポートに *any* を指定する必要があります。それ以外を指定すると ACL を適用できず、認証に失敗します。シングル ホストだけは例外で、下位互換性がありません。

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。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は影響しません。

送信元アドレスに *any* を指定することで、マルチホスト ポートでホストが 1 つだけ認証され、他のホストが無許可でネットワーク アクセスを取得している場合、最初のホストの ACL ポリシーをその他のホストにも適用できます。

認証マネージャ 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、接続されたホストに適用される認証方式のプライオリティ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一般認証機能を制御します。一般認証コマンドには、**authentication host-mode**、**authentication violation**、および **authentication timer** 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 固有のコマンドは **dot1x** 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認証をイネーブルにします。ただし、**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 認証がグローバルにディセーブルにされた場合、Web 認証などの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 9-2　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 以前の同等の 802.1X コマンド	説明
authentication control-direction {**both** | **in**}	**dot1x control-direction** {**both** | **in**}	Wake-on-LAN（WoL）機能を持つ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**	ポート上で制限付き VLAN をイネーブルにします。
	dot1x critical（インターフェイス コンフィギュレーション）	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*	認証をサポートしていないクライアント用に、フォールバック メソッドとして 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**}	認証済みポート上で、シングル ホスト（クライアント）またはマルチ 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柔軟に定義できるようにします。
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}**	ポートの認証ステートの手動制御をイネーブルにします。

表 9-2　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 以前の同等の 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**}	ポートに新しいデバイスが接続するか、最大数のデバイスがポートに接続された後に、そのポートに新しいデバイスが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 以降のリリースでは、認証マネージャで生成された冗長なシステム メッセージをフィルタリングできます。通常、フィルタリングされた内容は、認証の成功と関係しています。802.1x 認証および MAB 認証の冗長な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用意されています。

- **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冗長な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 認証の冗長な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）の冗長な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。

許可ステートおよび無許可ステートのポート

802.1X 認証中に、スイッチのポート ステートによって、スイッチはネットワークへのクライアント アクセスを許可します。ポートは最初、*無許可*ステートです。このステートでは、音声 VLAN（仮想 LAN）ポートとして設定されていないポートは 802.1X 認証、CDP、および STP パケットを除くすべての入力および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*許可*ステートに変更し、クライアントのトラフィック送受信を通常どおりに許可します。ポートが音声 VLAN として設定されている場合、VoIP トラフィックおよび 802.1X プロトコル パケットが許可されたあとクライアントが正常に認証されます。

802.1X をサポートしていないクライアントが、無許可ステートの 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許可ステートとなり、クライアントはネットワーク アクセスを許可されません。

反対に、802.1X 対応のクライアントが、802.1X 標準が実行していないポートに接続すると、クライアントは EAPOL-Start フレームを送信して認証プロセスを開始します。応答がなければ、クライアントは同じ要求を所定の回数だけ送信します。また、応答がない場合は、クライアントはポートが許可ステートであるものとしてフレーム送信を開始します。

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 コマンドおよび次のキーワードを使用して、ポートの許可ステートを制御できます。

- **force-authorized**：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、ポートを許可ステートに変更します。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。これがデフォルトの設定です。
- **force-unauthorized**：クライアントからの認証の試みをすべて無視し、ポートを無許可ステートのままにします。スイッチは、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、無許可ステートであり、ポート経由で送受信できるのは EAPOL フレームだけです。ポートのリンク ステートがダウンからアップに変更したとき、または EAPOL-Start 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（メディア アクセス コントロール）アドレスを使用して、ネットワーク 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）、ポートが許可ステートに変わり、認証されたクライアントからのすべてのフレームがポート経由での送受信を許可されます。認証に失敗すると、ポートは無許可ステートのままですが、認証を再試行することはできます。認証サーバに到達できない場合、スイッチは要求を再送信します。所定の回数だけ試行してもサーバから応答が得られない場合には、認証が失敗し、ネットワーク アクセスは許可されません。

クライアントはログオフするとき、EAPOL-Logoff メッセージを送信します。このメッセージによって、スイッチ ポートが無許可ステートになります。

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

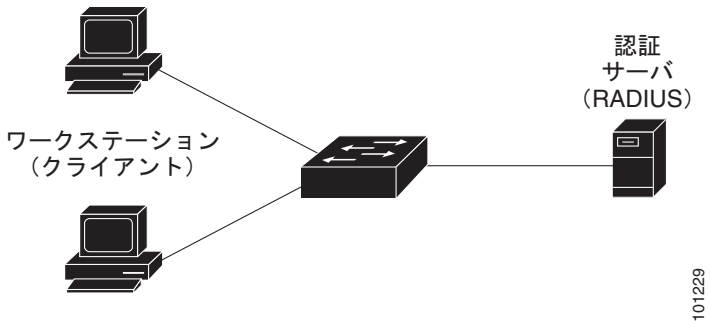
802.1X のホスト モード

802.1X ポートは、シングルホスト モードまたはマルチホスト モードで設定できます。シングルホスト モード（図 9-1（P.9-3）を参照）では、802.1X 対応のスイッチ ポートに接続できるのはクライアント 1 つだけです。スイッチは、ポートのリンク ステートがアップに変化したときに、EAPOL フレームを送信することでクライアントを検出します。クライアントがログオフしたとき、または別のクライアントに代わったときには、スイッチはポートのリンク ステートをダウンに変更し、ポートは無許可ステートに戻ります。

マルチホスト モードでは、複数のホストを単一の 802.1X 対応ポートに接続できます。図 9-5（P.9-12）に、ワイヤレス LAN における 802.1X ポートベース認証を示します。このモードでは、接続されたクライアントのうち 1 つが許可されれば、クライアントすべてのネットワーク アクセスが許可されます。ポートが無許可ステートになると（再認証が失敗するか、または EAPOL-Logoff メッセージを受信した場合）、スイッチは接続しているクライアントのネットワーク アクセスをすべて禁止します。このトポロジでは、ワイヤレス アクセス ポイントが接続しているクライアントの認証を処理し、スイッチに対してクライアントとしての役割を果たします。

マルチホスト モードがイネーブルの場合、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 9-5　マルチホスト モードの例



このスイッチは、MDA をサポートしています。これにより、データ デバイスと（シスコまたはシスコ以外の）IP 電話のような音声 デバイスの両方が、同一の 802.1X 対応スイッチ ポートに接続することができます。詳細については、「マルチドメイン認証」（P.9-13）を参照してください。

マルチドメイン認証

このスイッチは、MDA をサポートしています。これにより、データ デバイスと（シスコまたはシスコ以外の）IP 電話のような音声 デバイスの両方が、独立して同一の 802.1X 対応スイッチ ポートを認証することができます。ポートは、データ ドメインと音声ドメインに分けられます。

MDA は、デバイス認証の順序を強制しません。しかし、最良の結果を出すには、MDA 対応ポートでは音声デバイスをデータ デバイスの前に認証することを推奨します。

MDA を設定するときには、次の注意事項に従ってください。

- MDA 用にスイッチ ポートを設定するには、「ホスト モードの設定」（P.9-45）を参照してください。
- ホスト モードがマルチドメインに設定される際に IP 電話の音声 VLAN を設定する必要があります。詳細については、第 13 章「VLAN の設定」を参照してください。
- Cisco IOS Release 12.2(40)SE 以降のリリースでは、MDA 対応ポートでの音声 VLAN 割り当てをサポートしています。

（注） ダイナミック VLAN を使用して音声 VLAN を Cisco IOS Release 12.2(37)SE の動作する MDA 対応スイッチ ポートに割り当てると、音声デバイスで認証が失敗します。

- 音声デバイスを許可するには、`device-traffic-class=voice` という値を持ったシスコ アトリビュート値（AV）ペア アトリビュートを送信するように、AAA サーバを設定する必要があります。この値がない場合、スイッチは音声デバイスをデータ デバイスとして扱います。
- ゲスト VLAN および制限付き VLAN 機能は、MDA 対応レポートのデータ デバイスに限り適用されます。スイッチは、認証に失敗した音声デバイスをデータ デバイスとして扱います。
- 複数のデバイスでポートの音声またはデータ ドメインの認証を行おうとすると、errdisable になります。
- デバイスが認証されるまで、ポートでトラフィックが廃棄されます。シスコ製以外の IP 電話や音声デバイスがデータおよび音声 VLAN で許可されます。データ VLAN では、音声デバイスを DHCP サーバに接続して IP アドレスおよび音声 VLAN 情報を取得することができます 音声デバイスが 音声 VLAN で送信を開始したあと、データ VLAN へのアクセスはブロックされます。
- データ VLAN とバインドしている音声デバイス MAC アドレスは、ポート セキュリティ MAC アドレス制限にカウントされません。
- MDA は、フォールバック メカニズムとして MAC 認証バイパスを使用して、802.1X 認証をサポートしていないデバイスにスイッチポートを接続することができます。詳細については、「MAC 認証バイパス」（P.9-38）を参照してください。
- *データ*または*音声*デバイスがポートで検出されると、認証に成功するまでその MAC アドレスがブロックされます。認証に失敗した場合、MAC アドレスが 5 分間ブロックされたままになります。
- ポートが未認証中に 6 つ以上のデバイスが*データ* VLAN で検出された場合や、複数の*音声*デバイスが音声 VLAN で検出された場合、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またはマルチホストからマルチドメイン モードに変更される際に、認証済のデータ デバイスはポートで認証済のままになります。ただし、ポート音声 VLAN 上の Cisco IP Phone は自動的に削除され、そのポートで再認証される必要があります。

- ポートがシングルホストまたはマルチホスト モードからマルチドメイン モードに変更されたあとに、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 メカニズムは設定されたままになります。
- マルチドメイン モードからシングルホストまたはマルチホスト モードにポートを切り替えると、ポートからすべての認証済デバイスが削除されます。
- データ ドメインがまず認証されてゲスト VLAN に配置された場合、802.1X 非対応音声デバイスは認証をトリガするために音声 VLAN 上のパケットにタグを付ける必要があります。電話機からタグ付きトラフィックを送信する必要はありません（802.1x 対応電話機でも同様です）。
- MDA 対応ポートでは、ユーザ単位 ACL を推奨しません。ユーザ単位 ACL ポリシーを使用した認証済デバイスは、ポートの音声およびデータ 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 を適用する場合、ポートで使用できるデバイスは 1 つだけです。

詳細については、「ホスト モードの設定」（P.9-45）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します。各ホストは個別に認証されます。このモードで音声 VLAN が設定されている場合は、さらに 1 つのクライアントが VLAN で許可されます（ポートが追加の音声クライアントを検出すると、それらはポートから廃棄されますが違反は発生しません）。

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、接続された各クライアントの認証が必要です。

802.1X 非対応デバイスの場合、個々のホスト認証のフォールバック メソッドとして、MAC 認証バイパスまたは Web 認証を使用して、単一のポート上でさまざまな方法によってさまざまなホストを認証できます。

マルチ認証ポートで認証できるデータ ホストの数には制限はありません。ただし、音声 VLAN が設定されている場合、許可される音声デバイスは 1 つだけです。このホストの制限には違反のトリガが定義されていないため、2 番目の音声が検出されても違反をトリガせず、何も通知せずにその音声は廃棄されます。

音声 VLAN 上の MDA 機能をサポートするため、マルチ認証モードでは認証サーバから受信した VSA に応じて、認証済みデバイスをデータ VLAN または音声 VLAN に割り当てます。

（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 機能はアクティブになりません。

クリティカルな認証モードおよびクリティカルな 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.9-25）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.9-45）を参照してください。

Cisco IOS Release 12.2(55)SE 以降のリリースでは、RADIUS サーバにより提供される VLAN を次の条件でマルチ認証モードで割り当てることができます。

- ホストがポートで最初に許可されたホストであり、RADIUS サーバが VLAN 情報を提供している。
- 後続のホストが、動作 VLAN に一致する VLAN を使用して許可される。
- ホストは VLAN が割り当てられていないポートで許可され、後続のホストでは VLAN 割り当てが設定されていないか、VLAN 情報が動作 VLAN と一致している。

- ポートで最初に許可されたホストにはグループ VLAN が割り当てられ、後続のホストでは VLAN 割り当てが設定されていないか、グループ VLAN がポート上のグループ VLAN と一致している。後続のホストが、最初のホストと同じ VLAN グループの VLAN を使用する必要がある。VLAN リストが使用されている場合、すべてのホストは VLAN リストで指定された条件に従う。
- マルチ認証ポート上で、1 つの音声 VLAN 割り当てのみがサポートされている。
- VLAN がポート上のホストに割り当てられると、後続のホストは一致する VLAN 情報を持つ必要があり、この情報がなければポートへのアクセスを拒否される。
- ゲスト VLAN または認証失敗 VLAN をマルチ認証モードに設定できない。
- クリティカル認証 VLAN の動作が、マルチ認証モード用に変更されない。ホストが認証を試みたときにサーバに到達できない場合、許可されたすべてのホストは、設定された VLAN で再初期化される。

MAC の移動

あるスイッチ ポートで MAC アドレスが認証されると、そのアドレスは同じスイッチの別の 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すると、そのアドレスは許可されなくなります。

同じスイッチ上のポート間で MAC アドレスを移動する必要が生じる場合があります。たとえば、認証済みのホストとスイッチ ポート間に別のデバイス（ハブ、IP Phone など）が存在し、そのデバイスからホストの接続を解除し、同じスイッチ上の別のポートに直接接続する必要が生じる場合があります。

MAC の移動をグローバルにイネーブルにすると、デバイスを新しいポート上で認証できるようになります。ホストが 2 番目のポートに移動すると、最初のポート上のセッションが削除され、新しいポート上でホストが再認証されます。

MAC の移動はすべてのホスト モードでサポートされています（ポート上でイネーブルになっているホスト モードに関わらず、認証済みのホストをスイッチの任意のポートに移動できます）。

Cisco IOS Release 12.2(55)SE 以降のリリースでは、MAC 移動は、ポートのセキュリティとともに、すべてのホスト モードで設定できるようになりました。

あるポートから別のポートに MAC アドレスが移動すると、スイッチは元のポートで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。ポートのセキュリティの動作は、MAC 移動を設定するときと変わりません。

MAC 移動の機能は、音声およびデータ 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、新しいポートでの許可を必要とせずに、元のポートから新しいポートへただちに移動します。

詳細については、「MAC 移動のイネーブル化」（P.9-50）を参照してください。

MAC 置換

Cisco IOS Release 12.2(55)SE 以降のリリースでは、MAC 置換機能を設定して、事前に別のホストが認証されたポートにホストが接続を試みるときに発生する違反に対処できるようになりました。

（注）　違反はマルチ認証モードでは発生しないため、マルチ認証モードのポートにこの機能は適用されません。マルチホスト モードで認証が必要なのは最初のホストだけなので、この機能はこのモードのポートには適用されません。

replace キーワードを指定して **authentication violation** インターフェイス コンフィギュレーション コマンドを設定すると、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。

- 既存の認証済み MAC アドレスを使用するポートで新しい MAC アドレスが受信されます。
- 認証マネージャは、ポート上の現在のデータ 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。
- 認証マネージャは、新しい MAC アドレスに対する認証プロセスを開始します。
- 認証マネージャによって新しいホストが音声ホストであると判断された場合、元の音声ホストは削除されます。

ポートがオープン認証モードになっている場合、MAC アドレスはただちに MAC アドレス テーブルに追加されます。

詳細については、「MAC 置換のイネーブル化」（P.9-50）を参照してください。

802.1X アカウンティング

802.1X 標準では、ユーザの認証およびユーザのネットワーク アクセスに対する許可方法を定義しています。ただし、ネットワークの使用法についてはトラッキングしません。802.1X アカウンティングは、デフォルトでディセーブルです。802.1X アカウンティングをイネーブルにすると、次のアクティビティを 802.1X 対応のポート上でモニタできます。

- 正常にユーザを認証します。
- ユーザがログ オフします。
- リンクダウンが発生します。
- 再認証が正常に行われます。
- 再認証が失敗します。

スイッチは 802.1X アカウンティング情報を記録しません。その代わり、スイッチはこの情報を RADIUS サーバに送信します。RADIUS サーバは、アカウンティング メッセージを記録するように設定する必要があります。

802.1X アカウンティング アトリビュート値（AV）ペア

RADIUS サーバに送信された情報は、アトリビュート値（AV）ペアの形式で表示されます。これらの AV ペアのデータは、各種アプリケーションによって使用されます（たとえば課金アプリケーションの場合、RADIUS パケットの Acct-Input-Octets または Acct-Output-Octets アトリビュートの情報が必要です）。

AV ペアは、802.1X アカウンティングが設定されているスイッチによって自動的に送信されます。次の種類の RADIUS アカウンティング パケットがスイッチによって送信されます。

- START：新規ユーザ セッションが始まると送信されます。
- INTERIM：既存のセッションが更新されると送信されます。
- STOP：セッションが終了すると送信されます。

次の表 9-3 に、AV ペアおよびスイッチによって送信される AV ペアの条件を示します。

表 9-3　アカウンティング AV ペア

アトリビュート番号	AV ペア名	START	INTERIM	STOP
アトリビュート [1]	User-Name	常時送信	常時送信	常時送信
アトリビュート [4]	NAS-IP-Address	常時送信	常時送信	常時送信
アトリビュート [5]	NAS-Port	常時送信	常時送信	常時送信
アトリビュート [8]	Framed-IP-Address	非送信	条件に応じて送信[1]	条件に応じて送信[1]
アトリビュート [25]	クラス	常時送信	常時送信	常時送信
アトリビュート [30]	Called-Station-ID	常時送信	常時送信	常時送信
アトリビュート [31]	Calling-Station-ID	常時送信	常時送信	常時送信
アトリビュート [40]	Acct-Status-Type	常時送信	常時送信	常時送信
アトリビュート [41]	Acct-Delay-Time	常時送信	常時送信	常時送信
アトリビュート [42]	Acct-Input-Octets	非送信	常時送信	常時送信
アトリビュート [43]	Acct-Output-Octets	非送信	常時送信	常時送信
アトリビュート [44]	Acct-Session-ID	常時送信	常時送信	常時送信
アトリビュート [45]	Acct-Authentic	常時送信	常時送信	常時送信
アトリビュート [46]	Acct-Session-Time	非送信	常時送信	常時送信
アトリビュート [49]	Acct-Terminate-Cause	非送信	非送信	常時送信
アトリビュート [61]	NAS-Port-Type	常時送信	常時送信	常時送信

1. ホストに対して有効な Dynamic Host Control Protocol（DHCP）バインディングが DHCP スヌーピング バインディング テーブルに存在している場合にだけ、Framed-IP-Address の AV ペアは送信されます。

スイッチによって送信された AV ペアは、**debug radius accounting** 特権 EXEC コマンドを入力することで表示できます。このコマンドの詳細については、『*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 準備チェック

802.1X 準備チェックは、すべてのスイッチ ポート上で 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デバイス情報を表示します。この機能を使用すると、スイッチ ポートに接続したデバイスが 802.1X に対応しているかどうかを判断できます。802.1X 機能をサポートしていないデバイスについては、MAC 認証バイパスまたは Web 認証などの認証を変更できます。

この機能は、クライアントのサプリカントが NOTIFY EAP 通知パケットのクエリーをサポートしている場合にだけ有効です。クライアントは 802.1X タイムアウト値内に応答する必要があります。

802.1X 準備チェックに関するスイッチ設定の詳細については、「802.1X 準備チェックの設定」（P.9-39）を参照してください。

VLAN 割り当てを使用した 802.1X 認証

RADIUS サーバは VLAN 割り当てを送信し、スイッチ ポートを設定します。RADIUS サーバ 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 ポートに接続す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。

音声デバイス認証は、Cisco IOS Release 12.2(37)SE のマルチドメイン ホスト モードでサポートされています。Cisco IOS Release 12.2(40)SE 以降、音声デバイスが許可されており、RADIUS サーバが許可された VLAN を返した場合、割り当てられた音声 VLAN 上でパケットを送受信するようにポート上の音声 VLAN が設定されます。音声 VLAN 割り当ては、マルチドメイン認証（MDA）対応ポート上でデータ VLAN 割り当てと同じように動作します。詳細については、「マルチドメイン認証」（P.9-13）を参照してください。

スイッチと RADIUS サーバ上で設定された場合、VLAN 割り当てを使用した 802.1X 認証には次の特性があります。

- RADIUS サーバから VLAN が提供されない場合、または 802.1X 認証がディセーブルの場合、認証が成功するとポートはアクセス VLAN に設定されます。アクセス VLAN 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パケットはすべてこの VLAN に所属します。
- 802.1X 認証がイネーブルで、RADIUS サーバからの VLAN 情報が有効でない場合、認証に失敗して、設定済の VLAN が引き続き使用されます。これにより、設定エラーによって不適切な VLAN に予期せぬポートが現れることを防ぎます。

  設定エラーには、ルーテッド ポートの VLAN、間違った VLAN ID、存在しないまたは内部（ルーテッド ポート）VLAN ID、RSPAN VLAN、シャットダウンまたは一時停止している 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、設定エラーには、設定済または割り当て済 VLAN ID と一致するデータ VLAN の割り当て試行（またはその逆）のために発生するものもあります。
- 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、許可されたデバイスは認証後、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 サーバにより指定）に配置されます。
- ポート セキュリティをイネーブル化しても、RADIUS サーバが割り当てられた VLAN の動作には影響しません。
- 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 に配置されると、そのポートのアクセス 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、ポートが完全にこれらの例外で許可されている場合、同じことが音声デバイスに適用されます。
  - あるデバイスで VLAN 設定を変更したことにより、他のデバイスに設定済または割り当て済の VLAN と一致した場合、ポート上の全デバイスの認証が中断して、データおよび音声デバイスに設定済の VLAN が一致しなくなるような有効な設定が復元されるまで、マルチドメイン ホスト モードがディセーブルになります。
  - 音声デバイスが許可されて、ダウンロードされた音声 VLAN を使用している場合、音声 VLAN 設定を削除したり設定値を *dot1p* または *untagged* に修正したりすると、音声デバイスが未許可になり、マルチドメイン ホスト モードがディセーブルになります。

ポートが、強制許可（force-authorized）ステート、強制無許可（force-unauthorized）ステート、無許可ステート、またはシャットダウン ステートの場合、ポートは設定済みのアクセス VLAN に配置されます。

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 メンバシップ ポリシー サーバ）によるダイナミック アクセス ポート割り当ての場合、VLAN 割り当て機能を使用した 802.1X 認証はサポートされません。

VLAN 割り当てを設定するには、次の作業を実行する必要があります。

- **network** キーワードを使用して AAA 許可をイネーブルにし、RADIUS サーバからのインターフェイス設定を可能にします。
- 802.1X 認証をイネーブルにします（アクセス ポートで 802.1X 認証を設定すると、VLAN 割り当て機能は自動的にイネーブルになります）。
- RADIUS サーバにベンダー固有のトンネル アトリビュートを割り当てます。RADIUS サーバは次のアトリビュートをスイッチに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 グループ
  - [83] Tunnel-Preference

  アトリビュート [64] は、値 *VLAN*（タイプ 13）でなければなりません。アトリビュート [65] は、値 *802*（タイプ 6）でなければなりません。アトリビュート [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 アトリビュートの例については、「ベンダー固有の RADIUS アトリビュートを使用するスイッチ設定」（P.8-35）を参照してください。

ユーザ単位 ACL を使用した 802.1X 認証の利用

ユーザ単位の Access Control List（ACL; アクセス コントロール リスト）をイネーブルにして、802.1X 認証ユーザに対して異なるレベルのネットワーク アクセスおよびサービスを提供します。RADIUS サーバが 802.1X ポートに接続されたユーザを認証すると、ユーザ ID に基づいて ACL アトリビュートを取得してスイッチに送信します。スイッチは、ユーザ セッションの期間中、そのアトリビュートを 802.1X 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、またはリンクダウン状態になった場合には、スイッチはユーザ単位の ACL を削除します。スイッチは、RADIUS 指定の ACL を実行コンフィギュレーションに保存しません。ポートが無許可の場合、スイッチはそのポートから ACL を削除します。

同じスイッチ上で、ルータ ACL の設定およびポート ACL の入力を行うことができます。ただし、ポート ACL はルータ ACL よりも優先されます。入力済みのポート ACL を VLAN に属するインターフェイスに適用する場合、ポート ACL は VLAN インターフェイスに適用する入力済みのルータ ACL よりも優先されます。ポート ACL が適用されたポート上で受信した着信パケットは、ポート ACL によってフィルタリングされます。その他のポートに着信したルーテッド パケットは、ルータ ACL によってフィルタリングされます。発信するルーテッド パケットは、ルータ ACL によってフィルタリングされます。設定の矛盾を避けるために、RADIUS サーバに格納するユーザ プロファイルを慎重に計画します。

RADIUS は、ベンダー固有のアトリビュートなどのユーザ単位アトリビュートをサポートします。これらのベンダー固有のアトリビュート（VSA）は、オクテット ストリング形式で、認証プロセス中にスイッチに渡されます。ユーザ単位 ACL に使用される VSA は、入力方向では `inacl#<n>` で、出力方向では `outacl#<n>` です。MAC ACL は、入力方向でだけサポートされます。スイッチは、入力方向でだけ VSA をサポートします。このスイッチでは、レイヤ 2 ポートで出力方向のポート ACL はサポートされません。詳細については、第 33 章「ACL によるネットワーク セキュリティの設定」を参照してください。

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

Filter-Id アトリビュートを使用して、すでにスイッチに設定されている着信または発信 ACL を指定できます。アトリビュートには、ACL 番号と、その後ろに入力フィルタリング、出力フィルタリングを示す *.in* または *.out* が含まれています。RADIUS サーバが *.in* または *.out* 構文を許可しない場合、アクセス リストはデフォルトで発信 ACL に適用されます。スイッチでの Cisco IOS のアクセス リストに関するサポートが制限されているため、Filter-ID アトリビュートは 1 ～ 199 および 1300 ～ 2699 の IP ACL（IP 標準 ACL および IP 拡張 ACL）に対してだけサポートされます。

ユーザ単位 ACL の最大サイズは 4000 ASCII 文字ですが、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。

ベンダー固有のアトリビュートの例については、「ベンダー固有の RADIUS アトリビュートを使用するスイッチ設定」（P.8-35）を参照してください。ACL の設定の詳細については、第 33 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 モードでだけサポートされています。

ユーザ単位の 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 許可をイネーブルにし、RADIUS サーバからのインターフェイス設定を可能にします。
- 802.1X 認証をイネーブルにします。
- RADIUS サーバにユーザ プロファイルと VSA を設定します。
- シングルホスト モードの 802.1X ポートを設定します。

設定の詳細については、「認証マネージャ」（P.9-8）を参照してください。

ダウンロード ACL およびリダイレクト URL を使用した 802.1X 認証

ホストの 802.1X 認証または MAC 認証バイパス時に、RADIUS サーバから、ACL と リダイレクト URL をスイッチにダウンロードできます。Web 認証時にも ACL をダウンロードできます。

（注）　ダウンロード ACL は *dACL* とも呼ばれます。

複数のホストが認証され、それらのホストがシングル 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デバイスに ACL およびリダイレクト URL を適用できます。

802.1X 認証時に ACL がダウンロードされない場合、スイッチはホストへのポートにスタティック デフォルト ACL を適用します。マルチ認証モードまたは MDA モードで設定された音声 VLAN ポートでは、スイッチは ACL を認証ポリシーの一部として電話にだけ適用します。

Cisco IOS Release 12.2(55)SE 以降のリリースでは、ポート上にスタティック ACL がない場合、ダイナミックな認証デフォルト 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実施されます。

（注）　認証デフォルト ACL は、実行コンフィギュレーションでは表示されません。

認証デフォルト ACL は、ポートで許可ポリシーを持つホストが 1 つ以上検出されると作成されます。認証デフォルト ACL は、最後の認証セッションが終了すると削除されます。認証デフォルト 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）　認証デフォルト ACL は、シングル ホスト モードの Cisco Discovery Protocol（CDP; シスコ検出プロトコル）バイパスをサポートしていません。CDP バイパスをサポートするには、インターフェイス上のスタティック 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*および*クローズ*の 2 つの認証方式がサポートされます。*クローズ*認証モードのポートにスタティック ACL がない場合、次のようになります。

- 認証デフォルト ACL が作成されます。
- 認証デフォルト ACL は、ポリシーが実施されるまで DHCP トラフィックのみを許可します。
- 最初のホスト認証では、許可ポリシーは IP アドレスを挿入せずに適用されます。
- 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、最初のセッションと後続セッションのポリシーが IP アドレスを挿入して実施されます。

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

- 認証デフォルト ACL-OPEN が作成され、すべてのトラフィックが許可されます。
- セキュリティ違反を防ぐために、IP アドレスを挿入してポリシーが実施されます。
- Web 認証は、認証デフォルト ACL-OPEN に従います。

許可ポリシーのないホストへのアクセスを制御するために、ディレクティブを設定することができます。サポートされているディレクティブの値は、*open* と *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* ディレクティブは、ポートから提供されるアクセスにトラフィックを従わせます。ディレクティブは、AAA サーバ上のユーザ プロファイル、またはスイッチ上のいずれかで設定できます。AAA サーバ上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。スイッチ上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。

設定された ACL なしでポート上の Web 認証にホストがフォールバックする場合は、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、認証デフォルト ACL-OPEN が作成されます。
- ポートがクローズ認証モードの場合、認証デフォルト 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）は、ユーザ単位のエントリに変換されます。設定されたフォールバック 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認証デフォルト ACL に従います。

（注）　Web 認証でカスタム ロゴを使用し、それを外部サーバに格納する場合、認証の前にポートの ACL で外部サーバへのアクセスを許可する必要があります。外部サーバに適切なアクセスを提供するには、スタティック ポート ACL を設定するか、認証デフォルト ACL を変更する必要があります。

リダイレクト URL の Cisco Secure ACS とアトリビュート値ペア

スイッチは次の *cisco-av-pair* VSA を使用します。

- url-redirect は HTTP から HTTPS URL です。
- url-redirect-acl はスイッチ ACL 名または数字です。

スイッチは、CiscoSecure-Defined-ACL アトリビュート値ペアを使用して、エンドポイント デバイスからの HTTP または HTTPS リクエストを代行受信します。次に、スイッチはクライアント 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 ACS の url-redirect アトリビュート値ペアには、Web ブラウザがリダイレクトされる URL が含まれます。url-redirect-acl アトリビュート値ペアには、リダイレクトする HTTP 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 の許可（permit）ACE に一致するトラフィックがリダイレクトされます。

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

リダイレクト URL が認証サーバのクライアントに設定される場合、接続され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。

Cisco Secure ACS とダウンロード ACL のアトリビュート値ペア

RADIUS の cisco-av-pair Vendor-Specific Attribute（VSA; ベンダー固有アトリビュート）を使用すると、Cisco Secure ACS で CiscoSecure-Defined-ACL Attribute-Value（AV; アトリビュート値）ペアを設定できます。このペアは、#ACL#-IP-name-number アトリビュートで、Cisco Secure ACS のダウンロード 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（3f783768 など）です。

認証サーバで、クライアントのダウンロード ACL が設定されている場合、接続されているクライアント スイッチ ポートのデフォルト ポート ACL も設定されている必要があります。

スイッチにデフォルト ACL が設定されており、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 ポートに接続されているホストからのトラフィックに、ポリシーが適用されます。ポリシーが適用されない場合、スイッチはデフォルト ACL を適用します。Cisco Secure ACS がスイッチにダウンロード ACL を送信すると、この ACL がスイッチ ポートに設定されているデフォルト ACL より優先されます。ただし、スイッチが Cisco Secure ACS からホスト アクセス ポリシーを受信しても、デフォルトの ACL が設定されていない場合、認証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.9-8）および「ダウンロード ACL とリダイレクト URL を使用した 802.1X 認証の設定」（P.9-63）を参照してください。

VLAN ID に基づく MAC 認証

ダウンロード可能 VLAN ではなくスタティック VLAN ID に基づいてホストを認証する場合、VLAN ID に基づく MAC 認証を使用できます。スイッチにスタティック VLAN ポリシーを設定している場合、認証のために各ホストの MAC アドレスと VLAN 情報が IAS（Microsoft）RADIUS サーバに送信されます。接続されたポートに設定された VLAN ID が MAC 認証に使用されます。IAS サーバで VLAN ID に基づく MAC 認証を使用すると、ネットワーク内で所定の数の VLAN を使用できます。

この機能では、STP によってモニタおよび処理される VLAN の数も制限されます。ネットワークを固定された VLAN として管理できます。

（注）　この機能は Cisco ACS サーバではサポートされていません（ACS サーバは新しいホストの送信元 VLAN ID を無視し、MAC アドレスだけに基づいて認証します）。

設定情報については、「VLAN ID に基づく MAC 認証の設定」（P.9-66）を参照してください。その他の設定は、MAC 認証バイパスと同様です。「MAC 認証バイパスの設定」（P.9-59）を参照してください。

ゲスト VLAN を使用した 802.1X 認証

スイッチ上の各 802.1X ポートにゲスト VLAN を設定し、クライアントに対して限定的なサービスを提供できます（802.1X クライアントのダウンロードなど）。これらのクライアントは 802.1X 認証用にシステムをアップグレードできる場合がありますが、一部のホスト（Windows 98 システムなど）は 802.1X 対応ではありません。

スイッチが EAP Request/Identity フレームに対する応答を受信していない場合、または EAPOL パケットがクライアントによって送信されない場合に、802.1X ポート上でゲスト VLAN をイネーブルにすると、スイッチはクライアントにゲスト VLAN を割り当てます。

スイッチは EAPOL パケット履歴を維持します。EAPOL パケットがリンクの存続時間中に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デバイスが 802.1X 対応のものであると判断します。インターフェイスはゲスト VLAN ステートにはなりません。インターフェイスのリンク ステータスがダウンした場合、EAPOL 履歴はクリアされます。EAPOL パケットがインターフェイスで検出されない場合、そのインターフェイスはゲスト VLAN のステートになります。

リンクの存続時間中にデバイスがスイッチに EAPOL パケットを送信した場合、スイッチはゲスト VLAN への認証アクセスに失敗したクライアントを許可しません。

スイッチが 802.1X 対応の音声デバイスを認証するときに AAA が使用できない場合、認証は失敗しますが EAPOL パケットの検出は EAPOL 履歴に保存されます。その後 AAA サーバが使用できるようになれば、スイッチはその音声デバイスを認証します。ただし、スイッチは他のデバイスがゲスト VLAN へアクセスすることを許可しなくなります。この状態を回避するには、次のコマンドのいずれかを使用してください。

- **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、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 コマンドに続けて **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、ポートを再起動します。

（注）　インターフェイスがゲスト VLAN に変わってから EAPOL パケットが検出された場合、無許可ステートに戻って 802.1X 認証を再起動します。

スイッチ ポートがゲスト VLAN に変わると、802.1X 非対応クライアントはすべてアクセスを許可されます。ゲスト VLAN が設定されているポートに 802.1X 対応クライアントが加入すると、ポートは、ユーザ設定によるアクセス VLAN で無許可ステートになり、認証が再起動されます。

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

RSPAN VLAN、プライベート VLAN、音声 VLAN を除いて、アクティブ VLAN を 802.1X ゲスト VLAN として設定できます。ゲスト VLAN 機能は、内部 VLAN（ルーテッド ポート）またはトランク ポートではサポートされていません。アクセス ポート上でだけサポートされます。

スイッチは *MAC 認証バイパス*をサポートしています。MAC 認証バイパスが 802.1X ポートでイネーブルの場合、スイッチは、802.1X 認証のタイムアウト時に EAPOL メッセージ交換を待機している間、クライアント MAC アドレスに基づいてクライアントを許可できます。802.1X ポートでクライアントを検出したあと、スイッチはクライアントからイーサネット パケットを待ちます。スイッチは MAC アドレスに基づいて、ユーザ名とパスワードとともに RADIUS アクセス/要求フレームを認証サーバに送信します。認証に成功した場合、スイッチはクライアントにネットワークへのアクセスを許可します。認証に失敗した場合、ゲスト VLAN が指定されていれば、スイッチはポートをゲスト VLAN に割り当てます。詳細については、「MAC 認証バイパスを使用した 802.1X 認証の利用」（P.9-28）を参照してください。

詳細については、「ゲスト VLAN の設定」（P.9-52）を参照してください。

制限付き VLAN を使用した 802.1x 認証

ゲスト VLAN にアクセスできないクライアント向けに、限定されたサービスを提供するために、スイッチの各 802.1X ポートに対して制限付き VLAN（*認証失敗 VLAN* と呼ばれることもあります）を設定できます。これらのクライアントは、認証プロセスに失敗したため他の VLAN にアクセスできない 802.1X 対応クライアントです。制限付き VLAN を使用すると、認証サーバの有効な資格情報を持たないユーザ（通常、企業にアクセスするユーザ）に、サービスを制限したアクセスを提供できます。管理者は制限付き VLAN のサービスを制御できます。

（注）　両方のタイプのユーザに同じサービスを提供する場合、ゲスト VLAN と制限付き VLAN の両方を同じに設定できます。

この機能がないと、クライアントは認証失敗を永遠に繰り返すことになるため、スイッチ ポートがスパニング ツリーのブロッキング ステートから変わることができなくなります。制限付き VLAN の機能を使用することで、クライアントの認証試行回数を指定し（デフォルト値は 3 回）、一定回数後にスイッチ ポートを制限付き VLAN の状態に移行させることができます。

認証サーバはクライアントの認証試行回数をカウントします。このカウントが設定した認証試行回数を超えると、ポートが制限付き VLAN の状態に変わります。失敗した試行回数は、RADIUS サーバが *EAP failure* で応答したときや、EAP パケットなしの空の応答を返したときからカウントされます。ポートが制限付き VLAN に変わったら、このカウント数はリセットされます。

認証に失敗したユーザの VLAN は、もう一度認証を実行するまで制限された状態が続きます。制限付き VLAN 内のポートは設定された間隔に従って再認証を試みます（デフォルトは 60 秒）。再認証に失敗している間は、ポートの VLAN は制限された状態が続きます。再認証に成功した場合、ポートは設定された VLAN もしくは 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もできますが、ディセーブルにすると、*link down* または *EAP logoff* イベントを受信しないかぎり、ポートの認証プロセスを再起動できません。クライアントがハブを介して接続している場合、再認証機能はイネーブルにしておくことを推奨します。クライアントの接続をハブから切り離すと、ポートに *link down* や *EAP logoff* イベントが送信されない場合があります。

ポートが制限付き VLAN に移行すると、EAP 成功の擬似メッセージがクライアントに送信されます。このメッセージによって、繰り返し実行している再認証を停止させることができます。クライアントによっては（Windows XP が実行しているデバイスなど）、EAP なしで DHCP を実装できません。

制限付き VLAN は、レイヤ 2 ポートにある 802.1X ポート上でシングルホスト モードの場合だけサポートされます。

RSPAN VLAN、プライマリ プライベート VLAN、音声 VLAN を除いて、アクティブ VLAN を 802.1X 制限付き VLAN として設定できます。制限付き VLAN 機能は、内部 VLAN（ルーテッド ポート）またはトランク ポートではサポートされていません。アクセス ポート上でだけサポートされます。

この機能はポート セキュリティと連動します。ポートが認証されると、すぐに MAC アドレスがポート セキュリティに提供されます。ポート セキュリティがその MAC アドレスを許可しない場合、またはセキュア アドレス カウントが最大数に達している場合、ポートは無許可になり、errdisable ステートに移行します。

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、および IP 送信元ガードのような他のポート セキュリティ機能は、制限付き VLAN に対して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.9-53）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、アクセス不能認証バイパス機能（*クリティカル認証*または *AAA 失敗ポリシーとも呼ばれる*）を使用します。これらのホストを*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 ポートに接続しようとすると、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* に移されます。管理者は、制限された認証をそれらのホストに提供します。

スイッチがクリティカル 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。利用可能なサーバが 1 つあれば、スイッチはホストを認証できます。ただし、すべての RADIUS サーバが利用不可能な場合は、スイッチはホストへのネットワーク アクセスを許可して、ポートを認証ステートの特別なケースである*クリティカル認証*ステートにします。

マルチ認証ポートのサポート

マルチ認証（multiauth）ポートでアクセス不能認証バイパスをサポートするには、**authentication event server dead action reinitialize vlan** *vlan-id* を実行します。新しいホストがクリティカル ポートに接続しようとすると、ポートは再初期化され、接続されているすべてのホストがユーザ指定のアクセス VLAN に移されます。

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ています。

認証結果

アクセス不能認証バイパス機能の動作は、ポートの許可ステートにより異なります。

- クリティカル ポートに接続されているホストが認証しようとする際にポートが無許可ですべてのサーバが利用できない場合、スイッチは RADIUS 設定済み VLAN またはユーザ指定のアクセス VLAN にあるポートをクリティカル認証ステートにします。
- ポートが許可済みで、再認証が行われた場合、スイッチは現在の VLAN（事前に RADIUS サーバにより割り当てられた）でクリティカル ポートをクリティカル認証ステートにします。
- 認証交換中に RADIUS サーバが利用不可能となった場合、現在の交換はタイム アウトとなり、スイッチは次の認証試行の間にクリティカル ポートをクリティカル認証ステートとします。

RADIUS サーバが復旧したときにホストを再初期化してクリティカル VLAN から移動させるように、クリティカル ポートを設定できます。このように設定すると、すべてのクリティカル認証ステートのクリティカル ポートが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 リファレンスおよび「アクセス不能認証バイパス機能の設定」（P.9-55）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、次の機能と相互に作用します。

- 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の場合、この機能は次のように相互に作用します。
  - スイッチが EAP Request/Identity フレームへの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、少なくとも 1 つの RADIUS サーバが使用できれば、スイッチはクライアントにゲスト VLAN を割り当てます。
  - すべての RADIUS サーバが使用できず、クライアントがクリティカル ポートに接続されている場合、スイッチはクライアントを認証して、クリティカル ポートを RADIUS 認証済み VLAN またはユーザ指定のアクセス VLAN でクリティカル認証ステートにします。
  - すべての RADIUS サーバが使用できず、クライアントがクリティカル ポートに接続されていない場合、ゲスト VLAN が設定されていても、スイッチはクライアントにゲスト VLAN を割り当てられません。
  - すべての RADIUS サーバが使用できず、クライアントがクリティカル ポートに接続されていて、すでにゲスト VLAN が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 に保持します。
- 制限付き VLAN : ポートがすでに制限付き VLAN で許可されていて RADIUS サーバが使用できない場合、スイッチはクリティカル ポートを制限付き VLAN でクリティカル認証ステートにします。
- 802.1X アカウンティング : RADIUS サーバが使用できない場合、アカウンティング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 ポートにアクセス不能認証バイパスを設定できます。アクセス VLAN は、セカンダリ VLAN でなければなりません。
- 音声 VLAN : アクセス不能認証バイパスは音声 VLAN と互換性がありますが、RADIUS 設定済み VLAN またはユーザ指定のアクセス VLAN は、音声 VLAN と異なっていなければなりません。
- Remote Switched Port Analyzer（RSPAN）: アクセス不能認証バイパスの RADIUS 設定またはユーザ指定のアクセス VLAN として RSPAN VLAN を指定しないでください。

音声 VLAN ポートを使用した 802.1X 認証

音声 VLAN ポートは特殊なアクセス ポートで、次の 2 つの VLAN ID が対応付けられています。

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

ポートの許可ステートにかかわらず、IP Phone は音声トラフィックに対して 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、追加のクライアントがトラフィックを音声 VLAN 上で送信できます。マルチホスト モードがイネーブルの場合、サプリカント認証は PVID と VVID の両方に影響します。

リンクがあるとき、音声 VLAN ポートはアクティブになり、IP Phone からの最初の CDP メッセージを受け取るとデバイスの MAC アドレスが表示されます。Cisco IP Phone は、他のデバイスから受け取った CDP メッセージをリレーしません。その結果、複数の IP Phone が直列に接続されている場合、

スイッチは直接接続されている 1 台の IP Phone だけを認識します。音声 VLAN ポートで 802.1X 認証がイネーブルの場合、スイッチは 2 ホップ以上離れた認識されない IP Phone からのパケットをドロップします。

802.1X 認証をポート上でイネーブルにすると、音声 VLAN の機能を持つポート VLAN は設定できません。

IP 電話がシングル ホスト モードで 802.1x 対応のスイッチ ポートに接続されている場合、スイッチは認証を行わずに電話ネットワーク アクセスを承認します。ポートで Multidomain Authentication（MDA）を使用して、データ デバイスと IP 電話などの音声デバイスの両方を認証することを推奨します。

（注）　音声 VLAN が設定され、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 のスイッチへの接続が最大 30 秒間失われます。

音声 VLAN の詳細については、第 12 章「音声 VLAN の設定」を参照してください。

ポート セキュリティを使用した 802.1X 認証

シングルホスト モードまたはマルチホスト モードのどちらでもポート セキュリティを備えた 802.1X ポートを設定できます（**switchport port-security** インターフェイス コンフィギュレーション コマンドを使用してポートにポート セキュリティを設定する必要があります）。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設定すると、802.1X 認証はそのポートを認証し、ポート セキュリティはそのクライアントを含むすべての MAC アドレスに対するネットワーク アクセスを管理します。この場合、802.1X ポートを介してネットワークへアクセスできるクライアントの数とグループを制限できます。

次に、スイッチ上での 802.1X 認証とポート セキュリティ間における相互関係の例を示します。

- クライアントが認証され、ポート セキュリティ テーブルがいっぱいになっていない場合、クライアントの MAC アドレスがセキュア ホストのポート セキュリティ リストに追加されます。追加されると、ポートが通常どおりアクティブになります。

  クライアントが認証されて、ポート セキュリティが手動で設定された場合、セキュア ホスト テーブル内のエントリは保証されます（ポート セキュリティのスタティック エージングがイネーブルになっていない場合）。

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

  最初に認証されたホストが原因でセキュリティ違反が発生すると、ポートは errdisable ステートになり、ただちにシャットダウンします。

  セキュリティ違反発生時の動作は、ポート セキュリティ違反モードによって決まります。詳細については、「セキュリティ違反」（P.23-10）を参照してください。

- **no switchport port-security mac-address** *mac-address* インターフェイス コンフィギュレーション コマンドを使用して、ポート セキュリティ テーブルから 802.1X クライアント アドレスを手動で削除する場合、**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、ポートが未認証ステートに変更され、クライアントのエントリを含むセキュア ホスト テーブル内のダイナミック エントリがすべてクリアされます。ここで通常の認証が実行されます。

- ポートが管理上のシャットダウン状態になると、ポートは未認証ステートになり、ダイナミック エントリはすべてセキュア ホスト テーブルから削除されます。
- シングルホスト モードまたはマルチホスト モードのいずれの場合でも、802.1X ポート上でポート セキュリティと音声 VLAN を同時に設定できます。ポート セキュリティは、Voice VLAN Identifier（VVID）および Port VLAN Identifier（PVID）の両方に適用されます。
- **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 コマンドを設定することで、ポートが 802.1X 対応のポートに接続しているか、許可できるデバイスの最大数が認証されている場合に、ポートはシャットダウン、Syslog エラーの生成、または新規デバイスからのパケットの廃棄を実行できます。詳細については、「ポートごとに許可できるデバイスの最大数」（P.9-38）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。

スイッチ上でポート セキュリティをイネーブルにする手順については、「ポート セキュリティの設定」（P.23-9）を参照してください。

WoL 機能を使用した 802.1X 認証

802.1X 認証の Wake-on-LAN（WoL）機能を使用すると、スイッチに *マジック パケット*と呼ばれる特定のイーサネット フレームを受信させて、休止状態の PC を起動させることができます。この機能は、管理者が休止状態のシステムへ接続しなければならない場合に役立ちます。

WoL を使用するホストが 802.1X ポートを通じて接続され、ホストの電源がオフになると、802.1X ポートは無許可になります。無許可になったポートは EAPOL パケットしか送受信できないため、WoL マジック パケットはホストに届きません。さらに PC が休止状態になると、PC が認証されなくなるため、スイッチ ポートは閉じたままになります。

スイッチが WoL 機能を有効にした 802.1X 認証を使用している場合、スイッチはマジック パケットを含むトラフィックを無許可の 802.1X ポートに転送します。ポートが無許可の間、スイッチは EAPOL パケット以外の入力トラフィックをブロックし続けます。ホストはパケットを受信できますが、パケットをネットワーク内にある他のデバイスに送信できません。

（注）　PortFast がポートでイネーブルになっていないと、その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に設定すると、そのポートはスパニング ツリー フォワーディング ステートに変わります。ポートはパケットをホストに送信できますが、ホストからパケットを受信できません。

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に設定すると、そのポートのアクセスが双方向で制御されます。ポートは、ホストとの間でパケットを送受信しません。

MAC 認証バイパスを使用した 802.1X 認証の利用

MAC 認証バイパス機能を使用し、クライアント MAC アドレス（図 9-2（P.9-5）を参照）に基づいてクライアントを許可するようにスイッチを設定できます。たとえば、プリンタなどのデバイスに接続された 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 応答の待機中に 802.1X 認証がタイムアウトした場合、スイッチは MAC 認証バイパスを使用してクライアントを許可しようとします。

MAC 認証バイパス機能が 802.1X ポートでイネーブルの場合、スイッチはクライアント ID として MAC アドレスを使用します。認証サーバには、ネットワーク アクセスを許可されたクライアント MAC アドレスのデータベースがあります。802.1X ポートでクライアントを検出したあと、スイッチはクライアントからイーサネット パケットを待ちます。スイッチは MAC アドレスに基づいて、ユーザ名とパスワードとともに RADIUS アクセス / 要求フレームを認証サーバに送信します。認証に成功した場合、スイッチはクライアントにネットワークへのアクセスを許可します。許可が失敗した場合、ゲスト VLAN が設定されていれば、スイッチはポートをゲスト VLAN に割り当てます。

リンクの存続時間中にインターフェイスで EAPOL パケットが検出された場合、スイッチはそのインターフェイスに接続されているデバイスが 802.1X 対応サプリカントであると判断し、インターフェイスを許可するために（MAC 認証バイパスではなく）802.1X 認証を使用します。インターフェイスのリンク ステータスがダウンした場合、EAPOL 履歴はクリアされます。

スイッチがすでに MAC 認証バイパスを使用してポートを許可し、802.1X サプリカントを検出している場合、スイッチはポートに接続されているクライアントを許可します。再認証が発生するときに、Termination-Action RADIUS アトリビュート値が DEFAULT であるために前のセッションが終了した場合、スイッチは優先再認証プロセスとして 802.1X 認証を使用します。

MAC 認証バイパスを使用して許可されたクライアントを再認証できます。再認証プロセスは、802.1X を使用して認証されたクライアントに対するプロセスと同じです。再認証中は、ポートは前に割り当てられた VLAN のままです。再認証に成功すると、スイッチはポートを同じ VLAN に保持します。再認証に失敗した場合、ゲスト VLAN が設定されていれば、スイッチはポートをゲスト VLAN に割り当てます。

再認証が Session-Timeout RADIUS アトリビュート（アトリビュート [27]）と Termination-Action RADIUS アトリビュート（アトリビュート [29]）に基づいており、Termination-Action RADIUS アトリビュート（アトリビュート [29]）のアクションが *Initialize（初期化）* される場合（アトリビュート値が *DEFALUT*）、MAC 認証バイパス セッションが終了して、再認証中に接続が切断されます。MAC 認証バイパス機能が 802.1X 認証がタイムアウトした場合、スイッチは MAC 認証バイパス機能を使用して再認証を開始します。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、次の機能と相互に作用します。

- 802.1X 認証：802.1X 認証がポートでイネーブルの場合にだけ MAC 認証バイパスをイネーブルにできます。
- ゲスト VLAN：クライアントの MAC アドレス ID が無効な場合、ゲスト VLAN が設定されていれば、スイッチは VLAN にクライアントを割り当てます。
- 制限付き VLAN：802.1X ポートに接続されているクライアントが MAC 認証バイパスで認証されている場合には、この機能はサポートされません。
- ポート セキュリティ：「ポート セキュリティを使用した 802.1X 認証」（P.9-27）を参照してください。
- 音声 VLAN：「音声 VLAN ポートを使用した 802.1X 認証」（P.9-26）を参照してください。
- VLAN Membership Policy Server（VMPS; VLAN メンバシップ 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 に割り当てられます。
- Network Admission Control（NAC）レイヤ 2 IP 検証：この機能は、802.1X ポートが例外リスト内のホストを含む MAC 認証バイパスを使用して認証されると有効になります。

設定の詳細については、「認証マネージャ」（P.9-8）を参照してください。

Cisco IOS Release 12.2(55)SE 以降では、冗長 MAB システム メッセージのフィルタリングをサポートします。「認証マネージャ CLI コマンド」（P.9-10）を参照してください。

802.1x ユーザ分散

複数の異なる VLAN で同じグループ名を持つユーザのロードバランシングを行う場合、802.1x ユーザ分散を設定できます。

VLAN は RADIUS サーバが提供するか、またはスイッチの CLI を通じて特定の VLAN グループ名を使用して設定されます。

- 1 人の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。ユーザへの応答に複数の VLAN 名を設定して送信できます。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、認証されたユーザを最も負荷の小さい VLAN に移動することで、ロード バランシングを実現します。
- ユーザの VLAN グループ名を送信するように、RADIUS サーバを設定します。ユーザへの応答に VLAN グループ名を設定して送信できます。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、選択された 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ら、最も負荷の小さい VLAN を特定するために VLAN グループ名に対応する VLAN が検索されます。対応する認証済みのユーザをその VLAN に移動することで、ロード バランシングを実現します。

（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

- VLAN グループに少なくとも 1 つの VLAN がマッピングされていることを確認してください。
- VLAN グループには複数の VLAN をマッピングできます。
- VLAN を追加または削除して、VLAN グループを変更できます。
- 既存の VLAN を VLAN グループ名からクリアすると、その VLAN で認証されたポートは削除されませんが、マッピングは既存の VLAN グループからクリアされます。
- VLAN グループ名から最後の VLAN をクリアすると、その VLAN グループはクリアされます。
- VLAN グループにアクティブな VLAN がマッピングされていても、VLAN グループをクリアできます。VLAN グループをクリアすると、グループ内の VLAN で認証ステートのポートまたはユーザはクリアされませんが、VLAN グループへの VLAN のマッピングはクリアされます。

詳細については、「802.1x ユーザ分散の設定」（P.9-60）を参照してください。

NAC レイヤ 2 802.1X 検証

スイッチは NAC レイヤ 2 完了 802.1X 検証をサポートします。これは、デバイス ネットワーク アクセスを許可する前に、エンドポイント システムやクライアントのウイルス対策の状態や*ポスチャ*をチェックします。NAC レイヤ 2 802.1X 検証を使用すると、以下の作業を実行できます。

- Session-Timeout RADIUS アトリビュート（アトリビュート [27]）と Termination-Action RADIUS アトリビュート（アトリビュート [29]）を認証サーバからダウンロードします。
- Session-Timeout RADIUS アトリビュート（アトリビュート [27]）の値として再認証試行間の秒数を指定し、RADIUS サーバからクライアントのアクセス ポリシーを取得します。
- スイッチが Termination-Action RADIUS アトリビュート（アトリビュート [29]）を使用してクライアントを再認証する際のアクションを設定します。アクションの設定 値が *DEFAULT* であるか、値が設定されていない場合、セッションは終了します。値が RADIUS 要求の場合、再認証プロセスが開始します。

- Tunnel-Private-Group-ID（アトリビュート [81]）の値として VLAN 番号または名前、あるいは VLAN グループ名のリストを設定し、Tunnel-Preference（アトリビュート [83]）の値として 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設定します。Tunnel-Preference を設定していない場合、最初の Tunnel-Private-Group-ID（アトリビュート [81]）アトリビュートがこのリストから選択されます。
- **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表示する NAC ポスチャ トークンを表示します。
- ゲスト VLAN としてセカンダリ プライベート VLAN を設定します。

NAC レイヤ 2 802.1X 検証の設定は、RADIUS サーバにポスチャ トークンを設定する必要があることを除いて、802.1X ポートベース認証と似ています。NAC レイヤ 2 802.1X 検証の設定に関する詳細については、「NAC レイヤ 2 802.1X 検証の設定」（P.9-61）および「定期的な再認証の設定」（P.9-46）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.9-8）を参照してください。

柔軟な認証順序

柔軟な認証順序を使用して、ポートが新しいホストを認証する方式の順番を設定することができます。MAC 認証バイパスと 802.1X をプライマリまたはセカンダリ認証方式にし、それらのどちらか、または両方の試みが失敗した場合に、Web 認証をフォールバック メソッドにすることができます。詳細については、「柔軟な認証順序の設定」（P.9-66）を参照してください。

Open1x 認証

Open1x 認証は、デバイスが認証される前に、デバイスのポートへのアクセスを許可します。Open 認証が設定されている場合、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ができます。ホストの認証後、RADIUS サーバに設定されているポリシーがホストに適用されます。

Open 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 Open 認証 : 認証の前後で、1 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 Open 認証 : 音声ドメイン内の 1 ユーザとデータ ドメイン内の 1 ユーザだけが許可されます。
- マルチホスト モードと Open 認証 : すべて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 Open 認証 : 複数のホストを認証できることを除いて、MDA と同じです。

詳細については、「ホスト モードの設定」（P.9-45）を参照してください。

音声認識 802.1X セキュリティの使用法

音声認識 802.1X セキュリティ機能を使用すると、データまたは音声 VLAN に関わらず、セキュリティ違反が発生した VLAN だけをスイッチの設定でディセーブルにできます。以前のリリースで、データ クライアントの認証の試みで、セキュリティ違反が発生すると、ポート全体がシャットダウンしていたため、接続が完全に失われていました。

この機能は、PC が IP Phone に接続されている場合に役立ちます。データ VLAN でセキュリティ違反が検出されると、データ VLAN だけがシャットダウンします。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.9-40）を参照してください。

Network Edge Access Topology（NEAT）を使用した 802.1x サプリカント スイッチと認証スイッチ

Network Edge Access Topology（NEAT; ネットワーク エッジ アクセス トポロジ）機能は、ID を ワイヤリング クローゼットの外部の領域（会議室など）に拡大します。この機能により、あらゆる種類のデバイスをポート上で認証できます。

- 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して、スイッチを別のスイッチへのサプリカントとして動作するように設定できます。この設定は、たとえば、スイッチがワイヤリング クローゼットの外部にあり、トランク ポートを経由してアップストリーム スイッチに接続されている場合などのシナリオで役立ちます。802.1X スイッチ サプリカント機能で設定されているスイッチは、セキュアな接続のため、アップストリーム スイッチによって認証します。

  サプリカント スイッチが正常に認証すると、ポート モードがアクセスからトランクに変わります。

- 認証者スイッチでアクセス VLAN が設定されている場合、認証の成功後にアクセス VLAN がトランク ポートのネイティブ VLAN になります。

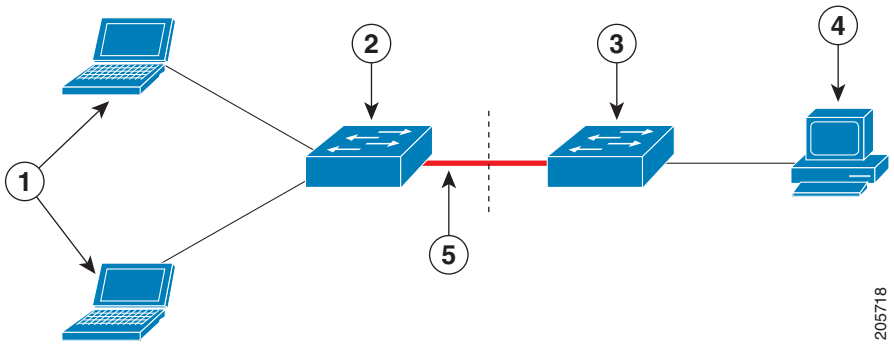
複数のサプリカント スイッチに接続する認証者スイッチ インターフェイスでは MDA または multiauth モードをイネーブルにできます。認証者スイッチ インターフェイスではマルチホスト モードはサポートされていません。

すべてのホスト モードで NEAT を機能させるには、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 コマンドを実行します。

- ホスト認証：ネットワークで認証済みホスト（サプリカントを備えたスイッチに接続する）からのトラフィックだけが許可されるようにします。スイッチは図 9-6 に示すように、Client Information Signalling Protocol（CISP; クライアント情報シグナリング プロトコル）を使用して、サプリカント スイッチに接続する MAC アドレスを認証者スイッチに送信します。

- 自動イネーブル：認証者スイッチのトランク設定を自動的にイネーブルにし、複数の VLAN からのユーザ トラフィックの、サプリカントスイッチからの着信を許可します。ACS で cisco-av-pair を *device-traffic-class=switch* として設定します（これは、*group* または *user* 設定の下で設定できます）。

図 9-6　CISP を使用した認証者およびサプリカント 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（ワイヤリング クローゼット外）
3	認証者スイッチ	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を使用して NEAT ポートを設定できます。サプリカント スイッチが認証するときは、スイッチの Vendor-Specific Attribute（VSA; ベンダー固有アトリビュート）に基づいて、ポート モードが *アクセス*から *トランク*に変わります（device-traffic-class=switch）。
- いずれかがネイティブ トランク VLAN に変換される場合、VSA は認証者スイッチ ポートをアクセス モードからトランク モードに変更し、802.1x トランク カプセル化およびアクセス VLAN をイネーブルにします。VSA はサプリカント上のポート設定は変更しません
- ホスト モードを変更して、認証者スイッチ ポートの標準ポート コンフィギュレーションを適用するには、スイッチ VSA ではなく、Auto SmartPort 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、サポートされていない設定を認証者スイッチ ポートから削除し、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、『*AutoSmartports Configuration Guide*』を参照してください。

詳細については、「NEAT を使用した認証者スイッチおよびサプリカント スイッチの設定」（P.9-62）を参照してください。

ACL および RADIUS Filter-Id アトリビュートを使用した IEEE 802.1x 認証の使用

スイッチは、IP 標準および IP 拡張の両方のポート Access Control List（ACL; アクセス コントロール リスト）の入力ポートへの適用をサポートしています。

- ユーザが設定する ACL
- ACS の ACL

シングルホスト モードの IEEE 802.1x ポートは ACS の ACL を使用し、IEEE 802.1x 認証ユーザにさまざまなレベルのサービスを提供します。RADIUS サーバはこのような種類のユーザおよびポートを認証すると、ユーザ ID に基づく ACL アトリビュートをスイッチに送信します。スイッチは、ユーザ セッションの期間中、そのアトリビュート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、またはリンクで障害が発生した場合は、ポートは無許可になり、スイッチはポートから ACL を削除します。

ACS からの IP 標準および IP 拡張ポート ACL だけが Filter-ID アトリビュートをサポートしています。Filter-ID アトリビュートは ACL の名前または番号を指定します。また、方向（入力または出力）、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 アトリビュートは、グループの Filter-ID アトリビュートよりも優先されます。
- ACS からの Filter-ID アトリビュートで設定済みの ACL に対して指定する場合、ユーザが設定した ACL よりも ACS からの指定が優先されます。
- RADIUS サーバが複数の Filter-ID アトリビュートを送信すると、最後のアトリビュートだけが適用されます。

スイッチで Filter-ID アトリビュートが定義されていない場合、認証に失敗し、ポートは無許可ステートに戻ります。

共通セッション ID

認証マネージャは、使用された認証方式が何であれ、クライアントの単一のセッション ID（共通セッション ID）を使用します。この ID は、show コマンドや MIB など、すべてのレポートに使用されます。このセッション ID は、セッションごとのすべての syslog メッセージに表示されます。

このセッション ID には、次の要素が含まれています。

- ネットワーク アクセス デバイス（NAD）の IP アドレス
- 単調増加する一意の 32 ビット整数
- セッション開始時のタイムスタンプ（32 ビット整数）

次に、**show authentication** コマンドの出力にセッション ID が表示される例を示します。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 の出力に表示されたセッション 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
```

このセッション ID は、NAD、AAA サーバ、およびその他のレポート分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。設定は必要ありません。

802.1X 認証の設定

ここでは、次の設定情報について説明します。

- 「802.1X 認証のデフォルト設定」（P.9-35）
- 「802.1X 認証設定時の注意事項」（P.9-36）
- 「802.1X 準備チェックの設定」（P.9-39）（任意）
- 「音声認識 802.1X セキュリティの設定」（P.9-40）（任意）
- 「802.1X 違反モードの設定」（P.9-41）（任意）
- 「スイッチおよび RADIUS サーバ間の通信の設定」（P.9-43）（必須）
- 「ホスト モードの設定」（P.9-45）（任意）
- 「定期的な再認証の設定」（P.9-46）（任意）
- 「ポートに接続するクライアントの手動での再認証」（P.9-47）（任意）
- 「待機時間の変更」（P.9-47）（任意）
- 「スイッチからクライアントへの再送信時間の変更」（P.9-48）（任意）
- 「スイッチからクライアントへのフレーム再送信回数の設定」（P.9-48）（任意）
- 「再認証回数の設定」（P.9-49）（任意）

- 「802.1X アカウンティングの設定」（P.9-51）（任意）
- 「MAC 移動のイネーブル化」（P.9-50）（任意）
- 「MAC 置換のイネーブル化」（P.9-50）（任意）
- 「ゲスト VLAN の設定」（P.9-52）（任意）
- 「制限付き VLAN の設定」（P.9-53）（任意）
- 「アクセス不能認証バイパス機能の設定」（P.9-55）（任意）
- 「WoL を使用した 802.1X 認証の設定」（P.9-58）（任意）
- 「MAC 認証バイパスの設定」（P.9-59）（任意）
- 「NAC レイヤ 2 802.1X 検証の設定」（P.9-61）（任意）
- 「NEAT を使用した認証者スイッチおよびサプリカント スイッチの設定」（P.9-62）
- 「ダウンロード ACL とリダイレクト URL を使用した 802.1X 認証の設定」（P.9-63）
- 「柔軟な認証順序の設定」（P.9-66）
- 「ポート上での 802.1X 認証のディセーブル化」（P.9-67）（任意）
- 「802.1X 認証設定のデフォルト値へのリセット」（P.9-68）（任意）

802.1X 認証のデフォルト設定

表 9-4 に、802.1X 認証のデフォルト設定を示します。

表 9-4　802.1X 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。
Authentication, Authorization, Accounting（AAA; 認証、許可、アカウンティング）	ディセーブル。
RADIUS サーバ • IP アドレス • UDP 認証ポート • 鍵	 • 指定なし。 • 1812 • 指定なし。
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。
定期的な再認証	ディセーブル。
再認証の間隔（秒）	3600 秒。
再認証回数	2 回（ポートが無許可ステートに変わる前に、スイッチが認証プロセスを再開する回数）。
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）。

表 9-4　802.1X 認証のデフォルト設定 （続き）

機能	デフォルト設定
再送信時間	30 秒（スイッチが EAP-Request/Identity フレームに対するクライアントからの応答を待ち、要求を再送信するまでの秒数）。
最大再送信回数	2 回（スイッチが認証プロセスを再開する前に、EAP-Request/Identity フレームを送信する回数）。
クライアント タイムアウト時間	30 秒（認証サーバからの要求をクライアントにリレーするとき、スイッチが返答を待ち、クライアントに要求を再送信するまでの時間）。
認証サーバ タイムアウト時間	30 秒（クライアントからの応答を認証サーバにリレーするとき、スイッチが応答を待ち、応答をサーバに再送信するまでの時間）。 タイムアウト期間は **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 コマンドを使用して変更できます。
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。
認証者（スイッチ）モード	指定なし。
MAC 認証バイパス	ディセーブル。
音声認識セキュリティ	ディセーブル。

802.1X 認証設定時の注意事項

ここでは、次の機能における注意事項を説明します。

- 「802.1X 認証」（P.9-36）
- 「VLAN 割り当て、ゲスト VLAN、制限付き VLAN、アクセス不能認証バイパス」（P.9-37）
- 「MAC 認証バイパス」（P.9-38）
- 「ポートごとに許可できるデバイスの最大数」（P.9-38）

802.1X 認証

- 802.1X 認証をイネーブルにすると、他のレイヤ 2 またはレイヤ 3 機能がイネーブルになる前に、ポートが認証されます。
- 802.1X 対応ポートを（たとえばアクセスからトランクに）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。
- 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、この変更は透過的でスイッチには影響しません。たとえば、ポートが RADIUS サーバに割り当ててられた VLAN に割り当てられ、再認証後に別の VLAN に割り当てられた場合に、この変更が発生します。

  802.1X ポートが割り当てられている VLAN がシャットダウン、ディセーブル、または削除される場合、ポートは無許可になります。たとえば、ポートが割り当てられたアクセス VLAN がシャットダウンまたは削除されたあと、ポートは無許可になります。
- 802.1X プロトコルは、レイヤ 2 スタティックアクセス ポート、音声 VLAN ポート、およびレイヤ 3 ルーテッド ポートで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 ポート上で 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：EtherChannel のアクティブ メンバーであるポート、またはこれからアクティブ メンバーにするポートを 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 RSPAN 宛先ポート：SPAN または RSPAN 宛先ポートであるポート上で 802.1X 認証をイネーブルにできます。ただし、ポートを SPAN または RSPAN 宛先ポートとして削除するまでは、802.1X 認証はディセーブルになります。SPAN または RSPAN 送信元ポートでは、802.1X 認証をイネーブルにできます。

- スイッチ上で、**dot1x system-auth-control** グローバル コンフィギュレーション コマンドを入力して 802.1X 認証をグローバルにイネーブルにする前に、802.1X 認証と EtherChannel が設定されているインターフェイスから、EtherChannel の設定を削除してください。
- Cisco IOS Release 12.2(55)SE 以降のリリースでは、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ています。「認証マネージャ CLI コマンド」（P.9-10）を参照してください。

VLAN 割り当て、ゲスト VLAN、制限付き VLAN、アクセス不能認証バイパス

- 802.1X 認証をポート上でイネーブルにすると、音声 VLAN の機能を持つポート VLAN は設定できません。
- トランク ポート、ダイナミック ポート、または VMPS によるダイナミック アクセス ポート割り当ての場合、VLAN 割り当て機能を使用した 802.1X 認証はサポートされません。
- 802.1X 認証をプライベート VLAN ポートに設定できますが、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 が付いた 802.1X 認証をプライベート VLAN ポートに設定できません。
- RSPAN VLAN、プライベート VLAN、音声 VLAN を除くあらゆる VLAN を 802.1X ゲスト VLAN として設定できます。ゲスト VLAN 機能は、内部 VLAN（ルーテッド ポート）またはトランク ポートではサポートされていません。アクセス ポート上でだけサポートされます。
- Dynamic Host Configuration Protocol（DHCP）クライアントが接続する 802.1X ポートにゲスト VLAN を設定したあとは、DHCP サーバからホスト IP アドレスが必要になる場合があります。クライアントの DHCP 処理がタイムアウトして、DHCP サーバからホスト IP アドレスを取得する前に、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することもできます。802.1X 認証プロセスの設定を減らしてください（**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）。設定を減らす量は、接続している 802.1X クライアント タイプによって異なります。

- アクセス不能認証バイパス機能を設定する際には、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ます。
  - Windows XP を実行しているクライアントに接続されたポートがクリティカル認証ステートの場合、Windows XP はインターフェイスが認証されないと報告する場合があります。
  - Windows XP クライアントに DHCP が設定されていて、DHCP サーバからの IP アドレスを持つ場合、クリティカル ポート上で EAP 成功メッセージを受信すると、DHCP 設定プロセスが再始動しない場合があります。
  - 802.1X ポート上では、アクセス不能認証バイパス機能および制限付き VLAN を設定できます。スイッチが制限付き VLAN 内でクリティカル ポートを再認証しようとし、すべての RADIUS サーバが利用不可能な場合、スイッチはポート ステートをクリティカル認証ステートに変更し、制限付き VLAN に残ります。
  - 同じスイッチ ポート上にアクセス不能バイパス機能とポート セキュリティを設定できます。
- RSPAN VLAN または音声 VLAN を除くあらゆる VLAN を、802.1X 制限付き VLAN として設定できます。制限付き VLAN 機能は、内部 VLAN（ルーテッド ポート）またはトランク ポートではサポートされていません。アクセス ポート上でだけサポートされます。

MAC 認証バイパス

- 特に明記していないかぎり、MAC 認証バイパスの注意事項は 802.1X 認証のものと同じです。詳細については、「802.1X 認証」（P.9-36）を参照してください。
- ポートが MAC アドレスで許可されたあとに、ポートから MAC 認証バイパスをディセーブルにしても、ポート ステートに影響はありません。
- ポートが無許可ステートでクライアント MAC アドレスが認証サーバ データベースにない場合、ポートは無許可ステートのままになります。ただし、クライアント MAC アドレスがデータベースに追加された場合、スイッチは MAC 認証バイパスを使用してポートを再認証できます。
- ポートが許可ステートである場合、再認証が発生するまでポートのステートは変わりません。
- MAC 認証バイパスによって接続されているが、非アクティブのホストのタイムアウト期間を設定することができます。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.23-9）を参照してください。

ポートごとに許可できるデバイスの最大数

802.1X 対応ポートで許可できるデバイスの最大数は、次のとおりです。

- シングルホスト モードでは、1 つのデバイスだけがアクセス VLAN で許可されます。ポートも音声 VLAN で設定されていた場合、音声 VLAN で送受信される Cisco IP Phone は無制限です。
- MultiDomain Authentication（MDA）モードでは、1 つのデバイスだけがアクセス VLAN に許可されます。また、1 つの IP Phone が音声 VLAN に許可されます。
- 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。ただし、非 802.1X ホストはアクセス VLAN で無制限に許可されます。また、デバイスも音声 VLAN で無制限に許可されます。

802.1X 準備チェックの設定

802.1X 準備チェックは、すべてのスイッチ ポート上で 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デバイス情報を表示します。この機能を使用すると、スイッチ ポートに接続したデバイスが 802.1X に対応しているかどうかを判断できます。

802.1X 準備チェックは、802.1X を設定できるすべてのポートに許可されています。**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。

スイッチで準備チェックをイネーブルにするには、次の事項に注意してください。

- 通常、準備チェックは 802.1X がスイッチでイネーブルになる前に使用します。
- インターフェイスを指定せずに **dot1x test eapol-capable** 特権 EXEC コマンドを使用している場合、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 対応のポートに **dot1x test eapol-capable** コマンドを設定してリンクをアップした場合、ポートは 802.1X 機能に関して接続クライアントにクエリーを送信します。クライアントが通知パケットに応答した場合、802.1X に対応していることになります。クライアントがタイムアウト期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かった場合、そのクライアントは 802.1X に対応していません。そのため、Syslog メッセージも生成されません。
- 準備チェックは、複数のホストを扱うポートにも送信できます（例：IP Phone に接続した PC）。準備チェクに対してタイムアウト期間内に応答したクライアントごとに Syslog メッセージが生成されます。

スイッチ上で 802.1X 準備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*]	スイッチ上で 802.1X 準備チェックをイネーブルにします。 （任意）*interface-id* には、802.1X 準備チェックを行うポートを指定します。 **（注）** **interface** キーワードを省略した場合、スイッチ上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 1	**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 2	**dot1x test timeout** *timeout*	（任意）EAPOL 応答を待機するタイムアウト時間を設定します。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 3	**end**	（任意）特権 EXEC モードに戻ります。
ステップ 4	**show running-config**	（任意）変更したタイムアウト値を確認します。

次に、ポートにクエリーを実行するスイッチ上で準備チェックをイネーブルにする方法を示します。また、クエリーを送信したポートから受信した応答も示します。これにより、接続したデバイスが 802.1X に対応しているかどうか確認できます。

```
switch# dot1x test eapol-capable interface gigabitethernet0/13

DOT1X_PORT_EAPOL_CAPABLE:DOT1X: MAC 00-01-02-4b-f1-a3 on gigabitethernet0/13 is EAPOL
capable
```

音声認識 802.1X セキュリティの設定

音声認識 802.1X セキュリティ機能を使用すると、データまたは音声 VLAN に関わらず、セキュリティ違反が発生した VLAN だけをスイッチでディセーブルにできます。この機能は、PC が IP Phone に接続されている IP Phone 環境に役立ちます。データ VLAN でセキュリティ違反が検出されてもシャットダウン対象はそのデータ VLAN だけです。音声 VLAN のトラフィックは中断せずにスイッチを通過できます。

スイッチに音声認識 802.1X セキュリティを設定する場合、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 コマンドを入力してイネーブルにします。音声認識 802.1X セキュリティをディセーブルにする場合は、このコマンドの **no** バージョンを使用します。このコマンドはスイッチで 802.1X を設定したすべてのポートに適用されます。

（注）　**shutdown vlan** キーワードを指定しない場合、errdisable ステートになった際にポート全体がシャットダウンします。

- **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 errdisabled 回復を設定した場合、ポートは自動的に再度イネーブルになります。errdisable 回復がポートに設定されていない場合、**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、もう一度イネーブルにします。
- **clear errdisable interface** *interface-id* **vlan** [*vlan-list*] 特権 EXEC コマンドを使用すれば、VLAN ごとに再度イネーブルにできます。範囲を指定しない場合、ポート上のすべての 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**	セキュリティ違反が発生したすべての VLAN をシャットダウンします。 （注）　**shutdown vlan** キーワードを指定しない場合、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 ごと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 ステートの個々の VLAN を再度イネーブルにします。 • *interface-id* には、再度イネーブルにする各 VLAN ポートを指定します。 • （任意）*vlan-list* には、再度イネーブルにする VLAN のリストを指定します。*vlan-list* が指定されていない場合、すべての VLAN が再度イネーブルになります。
ステップ 5	**shutdown** **no-shutdown**	（任意）errdisable ステートの VLAN を再度イネーブルにし、すべての errdisable 状態を回復します。
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）コンフィギュレーション ファイルに設定を保存します。

次に、セキュリティ違反が発生したすべての VLAN をシャットダウンするようにスイッチを設定する方法を示します。

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

次に、ポート ギガビット イーサネット 0/2 で errdisable ステートだったすべての VLAN を再度イネーブルにする方法を示します。

```
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

802.1X ポートを設定することで、シャットダウン、Syslog エラーの生成、または新規デバイスからのパケットの廃棄を実行できます。実行するための条件は次のとおりです。

- デバイスが 802.1x 対応のポートに接続した
- 許可するデバイスの最大数がポートで認証された

スイッチ上に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。
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、デフォルト状況で使用することになっている方法に続いて **default** キーワードを使用します。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 リストを使用できるようにします。 （注）　**group radius** キーワード以外にもコマンドラインのヘルプ ストリングに表示されますが、サポートされていません。
ステップ 4	**interface** *interface-id*	802.1X 認証をイネーブルにするクライアントに接続しているポートを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 5	**switchport mode access**	ポートをアクセス モードにします。
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 ステートにします。 • **restrict**：Syslog エラーを生成します。 • **protect**：そのポートへトラフィックを送信する新規デバイスからのパケットをドロップします。 • **replace**：現在の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。

	コマンド	目的
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）コンフィギュレーション ファイルに設定を保存します。

802.1X 認証の設定

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

ユーザ単位 ACL または VLAN 割り当てを可能にするには、AAA 許可をイネーブルにしてネットワーク関連のすべてのサービス要求に対してスイッチを設定する必要があります。

次に、802.1X の AAA プロセスを示します。

ステップ 1　ユーザがスイッチのポートに接続します。

ステップ 2　認証が実行されます。

ステップ 3　RADIUS サーバ設定に基づいて、VLAN 割り当てが適宜イネーブルになります。

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

ステップ 5　必要に応じて、再認証が実行されます。

ステップ 6　スイッチが仮のアカウンティング アップデートを、再認証結果に基づいたアカウンティング サーバに送信します。

ステップ 7　ユーザがポートから切断します。

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

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、デフォルト状況で使用することになっている方法に続いて **default** キーワードを使用します。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 リストを使用できるようにします。 **（注）**　**group radius** キーワード以外にもコマンドラインのヘルプ ストリングに表示されますが、サポートされていません。
ステップ 4	**dot1x system-auth-control**	スイッチ上で 802.1X 認証をグローバルにイネーブルにします。

	コマンド	目的
ステップ 5	**aaa authorization network** {**default**} **group radius**	（任意）ユーザ単位 ACL や VLAN 割り当てなど、ネットワーク関連のすべてのサービス要求に対するユーザ RADIUS 許可をスイッチに設定します。 ユーザ単位 ACL を設定するには、シングルホスト モードを設定する必要があります。この設定がデフォルトです。
ステップ 6	**radius-server host** *ip-address*	（任意）RADIUS サーバの IP アドレスを指定します。
ステップ 7	**radius-server key** *string*	（任意）RADIUS サーバ上で動作する RADIUS デーモンとスイッチの間で使用する認証および暗号鍵を指定します。
ステップ 8	**interface** *interface-id*	802.1X 認証をイネーブルにするクライアントに接続しているポートを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 9	**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**	ポート上で 802.1X 認証をイネーブルにします。 機能の相互作用については、「802.1X 認証設定時の注意事項」（P.9-36）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）コンフィギュレーション ファイルに設定を保存します。

スイッチおよび RADIUS サーバ間の通信の設定

RADIUS セキュリティ サーバは、ホスト名または IP アドレス、ホスト名と特定の UDP ポート番号、または IP アドレスと特定の UDP ポート番号によって識別します。IP アドレスと UDP ポート番号の組み合わせによって、一意の ID が作成され、サーバの同一 IP アドレス上にある複数の UDP ポートに RADIUS 要求を送信できるようになります。同じ RADIUS サーバ上の異なる 2 つのホスト エントリに同じサービス（たとえば認証）を設定した場合、2 番めに設定されたホスト エントリは、最初に設定されたホスト エントリのフェールオーバー バックアップとして動作します。RADIUS ホスト エントリは、設定した順序に従って試行されます。

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

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**radius-server host** {*hostname* | *ip-address*} **auth-port** *port-number* **key** *string*	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および暗号鍵を指定します。鍵は、RADIUS サーバで使用する暗号鍵に一致するテキスト ストリングでなければなりません。 **（注）** 鍵の先行スペースは無視されますが、途中および末尾のスペースは有効なので、鍵は必ず **radius-server host** コマンド構文の最後の項目として設定してください。鍵にスペースを使用する場合は、引用符が鍵の一部分である場合を除き、引用符で鍵を囲まないでください。鍵は RADIUS デーモンで使用する暗号鍵に一致している必要があります。 複数の RADIUS サーバを使用する場合には、このコマンドを繰り返し入力します。
ステップ 3	**end**	特権 EXEC モードに戻ります。
ステップ 4	**show running-config**	設定を確認します。
ステップ 5	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

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

次に、IP アドレス 172.120.39.46 のサーバを RADIUS サーバとして指定し、ポート 1612 を許可ポートとして使用し、暗号鍵を RADIUS サーバ上の鍵と同じ *rad123* に設定する例を示します。

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

すべての RADIUS サーバについて、タイムアウト、再送信回数、および暗号鍵値をグローバルに設定するには、**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。これらのオプションをサーバ単位で設定するには、**radius-server timeout**、**radius-server retransmit**、および **radius-server key** グローバル コンフィギュレーション コマンドを使用します。詳細については、「すべての RADIUS サーバの設定」（P.8-35）を参照してください。

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

ホスト モードの設定

802.1X 認証済みポート上でシングルホスト（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。**multi-domain** キーワードを使用して MDA を設定して、ホストと（シスコまたはシスコ以外の）IP 電話のような音声デバイスの両方を、同一スイッチ ポートで認証することができます。

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**	ベンダー固有アトリビュート（VSA）を認識し使用するために、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*	複数ホストが間接的に接続されているポートを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 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、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** コマンドでだけ使用できます。 • **multi-host**：シングル ホストの認証後に 802.1X 許可ポートで複数のホスト（クライアント）の接続を許可します。 • **multi-domain**：ホストと（シスコまたはシスコ以外の）IP 電話のような音声デバイスの両方を 1 つの 802.1X 認証済ポートで認証することができます。 （注）　ホスト モードが **multi-domain** に設定される際に IP 電話の音声 VLAN を設定する必要があります。詳細については、第 12 章「音声 VLAN の設定」を参照してください。 • **single-host**：802.1X 許可ポートで複数のホスト（クライアント）の接続を許可します。 指定するインターフェイスで、**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。
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）コンフィギュレーション ファイルに設定を保存します。

ポート上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て、複数のホストを許可する例を示します。

```
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# dot1x port-control auto
Switch(config-if)# dot1x host-mode multi-host
Switch(config-if)# end
```

次に、MDA をイネーブルにしてポート上でホストと音声 デバイスを許可する例を示します。

```
Switch(config)# interface gigabitethernet0/1
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
```

定期的な再認証の設定

802.1X クライアントの定期的な再認証をイネーブルにし、再認証の間隔を指定できます。再認証を行う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、再認証を行う間隔（秒）を設定するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id*	設定するポートを指定し、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（デフォルトではディセーブル）をイネーブルにします。
ステップ 4	**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** キーワードの意味は次のとおりです。 • **inactivity**：クライアントからのアクティビティがなく、無許可とするまでの期間（秒）。 • **reauthenticate**：自動認証試行が開始されるまでの期間（秒）。 • **restart *value***：無許可ポートを認証するための試行が行われるまでの期間（秒）。 **dot1x timeout reauth-period** キーワードの意味は次のとおりです。 • *seconds*：秒数を 1 ～ 65535 の範囲で設定します。デフォルトは 3600 秒です。 • **server**：Session-Timeout RADIUS アトリビュート（アトリビュート [27]）および Terminate-Action RADIUS アトリビュート（アトリビュート [29]）の値に基づいて秒数を指定します。 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。

	コマンド	目的
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）コンフィギュレーション ファイルに設定を保存します。

定期的な再認証をディセーブルにするには、**no 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、再認証の間隔を 4000 秒に設定する例を示します。

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

ポートに接続するクライアントの手動での再認証

dot1x re-authenticate interface *interface-id* 特権 EXEC コマンドを入力すると、いつでも特定のポートに接続するクライアントを手動で再認証できます。この手順は任意です。定期的な再認証をイネーブルまたはディセーブルにする方法については、「定期的な再認証の設定」（P.9-46）を参照してください。

次に、ポートに接続するクライアントを手動で再認証する例を示します。

```
Switch# dot1x re-authenticate interface gigabitethernet0/1
```

待機時間の変更

スイッチはクライアントを認証できなかった場合に、所定の時間だけアイドル状態を続け、その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 コマンドがその待ち時間を制御します。クライアント認証が失敗する理由としては、クライアントが無効なパスワードを提示した場合などが考えられます。デフォルトよりも小さい値を入力することによって、ユーザへの応答時間を短縮できます。

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

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id*	設定するポートを指定し、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 秒です。デフォルトは 60 秒です。
ステップ 4	**end**	特権 EXEC モードに戻ります。
ステップ 5	**show 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）コンフィギュレーション ファイルに設定を保存します。

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

次に、スイッチの待機時間を 30 秒に設定する例を示します。

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

スイッチからクライアントへの再送信時間の変更

クライアントはスイッチからの EAP-Request/Identity フレームに対し、EAP-Response/Identity フレームで応答します。スイッチがこの応答を受信できなかった場合、所定の時間（再送信時間）だけ待機し、その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い場合や、特定のクライアントおよび認証サーバの動作に問題がある場合など、異常な状況に対する調整を行う必要があるときに限って変更してください。

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

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id*	設定するポートを指定し、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 EAP-Request/Identity フレームに対するクライアントからの応答を待ち、要求を再送信するまでの秒数を設定します。 指定できる範囲は 1 ～ 65535 秒です。デフォルトは 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）コンフィギュレーション ファイルに設定を保存します。

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

次に、スイッチが EAP-Request/Identity フレームに対するクライアントからの応答を待ち、要求を再送信するまでの時間を 60 秒に設定する例を示します。

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

スイッチからクライアントへのフレーム再送信回数の設定

（クライアントから応答が得られなかった場合に）スイッチが認証プロセスを再起動する前に、クライアントに EAP-Request/Identity フレームを送信する回数を変更できます。

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

スイッチからクライアントへのフレーム再送信回数を設定するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id*	設定するポートを指定し、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起動する前に、EAP-Request/Identity フレームを送信する回数を設定します。指定できる範囲は 1 ～ 10 です。デフォルトは 2 です。
ステップ 4	**end**	特権 EXEC モードに戻ります。
ステップ 5	**show 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）コンフィギュレーション ファイルに設定を保存します。

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

次に、スイッチが認証プロセスを再起動する前に、EAP-Request/Identity 要求を送信する回数を 5 に設定する例を示します。

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

再認証回数の設定

ポートが無許可ステートに変わる前に、スイッチが認証プロセスを再開する回数を変更することもできます。

（注）　このコマンドのデフォルト値は、リンクの信頼性が低い場合や、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。

	コマンド	目的
ステップ 3	**dot1x max-reauth-req** *count*	ポートが無許可ステートに変わる前に、スイッチが認証プロセスを再開する回数を設定します。指定できる範囲は 0 ～ 10 です。デフォルトは 2 です。
ステップ 4	**end**	特権 EXEC モードに戻ります。
ステップ 5	**show 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）コンフィギュレーション ファイルに設定を保存します。

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

次に、ポートが無許可ステートに変わる前に、スイッチが認証プロセスを再開する回数として 4 を設定する例を示します。

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

MAC 移動のイネーブル化

MAC 移動により、認証済みのホストをスイッチ上のポート間で移動できます。

スイッチ上での MAC 移動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**	スイッチで MAC の移動をイネーブルにします。
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）コンフィギュレーション ファイルに設定を保存します。

次に、スイッチ上で MAC 移動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 置換のイネーブル化

MAC 置換を使用すると、ホストはポート上の認証ホストを置換できます。

インターフェイス上で MAC 置換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**}	インターフェイス上で MAC 置換をイネーブルにするには、**replace** キーワードを使用します。ポートが現在のセッションを削除し、新しいホストを使用して認証を開始します。 他のキーワードは、次のような機能があります。 • **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 を使用するパケットをドロップします。 • **restrict** : 違反パケットが CPU によってドロップされ、システム メッセージが生成されます。 • **shutdown** : ポートは、予期しない MAC アドレスを受信すると errdisable 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）コンフィギュレーション ファイルに設定を保存します。

次に、インターフェイス上で MAC 置換をイネーブルにする例を示します。

```
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

802.1X アカウンティングを使用して、AAA システム アカウンティングをイネーブルにすると、ロギングのためにシステム リロード イベントをアカウンティング RADIUS サーバに送信できます。サーバは、アクティブな 802.1X セッションすべてが終了したものと判断します。

RADIUS は信頼性の低い UDP トランスポート プロトコルを使用するため、ネットワーク状態が良好でないと、アカウンティング メッセージが失われることがあります。設定した回数のアカウンティング要求の再送信後、スイッチが RADIUS サーバからアカウンティング応答メッセージを受信しない場合、次のメッセージが表示されます。

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

このストップ メッセージが正常に送信されない場合、次のメッセージが表示されます。

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

（注）　ロギングの開始、停止、仮のアップデート メッセージ、タイム スタンプなどのアカウンティング タスクを実行するように、RADIUS サーバを設定する必要があります。これらの機能をオンにするには、RADIUS サーバの Network Configuration タブの [Update/Watchdog packets from this AAA client] のロギングをイネーブルにします。次に、RADIUS サーバの System Configuration タブの [CVS RADIUS Accounting] をイネーブルにします。

AAA がスイッチでイネーブルになったあと、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）システム アカウンティングをイネーブルにし（すべての RADIUS サーバのリストを使用）、スイッチがリロードするときにシステム アカウンティング リロード イベント メッセージを生成します。
ステップ 5	**end**	特権 EXEC モードに戻ります。
ステップ 6	**show running-config**	設定を確認します。
ステップ 7	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

アカウンティング応答メッセージを受信しない RADIUS メッセージ数を表示するには、**show radius statistics** 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、アカウンティングの UDP ポートとして 1813 を指定して、RADIUS サーバを設定します。

```
Switch(config)# radius-server host 172.120.39.46 auth-port 1812 acct-port 1813 key rad123
Switch(config)# aaa accounting dot1x default start-stop group radius
Switch(config)# aaa accounting system default start-stop group radius
```

ゲスト VLAN の設定

サーバが EAP Request/Identity フレームに対する応答を受信しない場合、ゲスト VLAN を設定すると、802.1X 対応でないクライアントはゲスト VLAN に配置されます。802.1X 対応であっても、認証に失敗したクライアントは、ネットワークへのアクセスが許可されません。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。サポートされるポートのタイプについては、「802.1X 認証設定時の注意事項」（P.9-36）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**	ポート上で 802.1X 認証をイネーブルにします。

	コマンド	目的
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 を除き、任意のアクティブ VLAN を 802.1X ゲスト VLAN として設定できます。
ステップ 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）コンフィギュレーション ファイルに設定を保存します。

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

次に、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 gigabitethernet0/2
Switch(config-if)# dot1x guest-vlan 2
```

次に、スイッチの待機時間として 3 を、要求の再送信前にクライアントからの EAP-Request/Identify フレーム応答を待機する時間（秒）を 15 に設定し、802.1X ポートの DHCP クライアント接続時に、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

スイッチ上に制限付き VLAN を設定している、認証サーバが有効なユーザ名またはパスワードを受信できない場合と、802.1X に準拠した場合クライアントは制限付き VLAN に移されます。スイッチは、シングルホスト モードでだけ制限付き 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。サポートされるポートのタイプについては、「802.1X 認証設定時の注意事項」（P.9-36）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**	ポート上で 802.1X 認証をイネーブルにします。

	コマンド	目的
ステップ 5	**authentication event fail action authorize** *vlan-id*	アクティブな VLAN を、802.1X 制限付き VLAN に指定します。指定できる範囲は 1 ～ 4094 です。 内部 VLAN（ルーテッド ポート）、RSPAN VLAN、プライマリ プライベート VLAN、または音声 VLAN を除き、任意のアクティブ VLAN を 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）コンフィギュレーション ファイルに設定を保存します。

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

次に、*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-if)# dot1x auth-fail vlan 2
```

ユーザに制限付き VLAN を割り当てる前に、**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、認証試行回数を最大に設定できます。指定できる認証試行回数は 1 ～ 3 回です。デフォルトは 3 回に設定されています。

認証試行回数を最大に設定するには、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。サポートされるポートのタイプについては、「802.1X 認証設定時の注意事項」（P.9-36）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**	ポート上で 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*	アクティブな VLAN を、802.1X 制限付き VLAN に指定します。指定できる範囲は 1 ～ 4094 です。 内部 VLAN（ルーテッド ポート）、RSPAN VLAN、プライマリ プライベート VLAN、または音声 VLAN を除き、任意のアクティブ VLAN を 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 に移行するための認証試行回数を指定します。指定できる範囲は 1 ～ 3 です。デフォルトは 3 です。
ステップ 7	**end**	特権 EXEC モードに戻ります。

	コマンド	目的
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）コンフィギュレーション ファイルに設定を保存します。

設定数をデフォルトに戻すには、**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、ポートを制限付き VLAN にするために、認証試行回数を *2* に設定する方法を示します。

```
Switch(config-if)# dot1x auth-fail max-attempts 2
```

アクセス不能認証バイパス機能の設定

アクセス不能認証バイパス機能（クリティカル認証または AAA 失敗ポリシーとも呼ばれます）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 サーバが使用できない、または *dead* と見なされるときを判別するのに使われる条件を設定します。 指定できる *time* の範囲は 1 ～ 120 秒です。スイッチは、デフォルトの *seconds* 値を 10 ～ 60 秒の間で動的に決定します。 指定できる *tries* の範囲は 1 ～ 100 です。スイッチは、デフォルトの *tries* パラメータを 10 ～ 100 の間で動的に決定します。
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 分です（24 時間）。デフォルト値は 0 分です。

	コマンド	目的
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 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 サーバの UDP ポートと RADIUS 認証サーバの UDP ポートを非デフォルト値に設定します。 • **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て、使用するユーザ名を指定します。 • **idle-time** *time* : スイッチがテスト パケットをサーバに送信したあとの間隔を分数で設定します。指定できる範囲は 1 ～ 35791 分です。デフォルトは 60 分（1 時間）です。 • **ignore-acct-port** : RADIUS サーバ アカウンティング ポートのテストをディセーブルにします。 • **ignore-auth-port** : RADIUS サーバ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 デーモンとの間のすべての RADIUS 通信で使用する認証および暗号鍵を指定します。 **（注）** 鍵の先行スペースは無視されますが、途中および末尾のスペースは有効なので、鍵は必ず **radius-server host** コマンド構文の最後の項目として設定してください。鍵にスペースを使用する場合は、引用符が鍵の一部分である場合を除き、引用符で鍵を囲まないでください。鍵は RADIUS デーモンで使用する暗号鍵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も認証および暗号鍵を設定できます。
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すると、スイッチが EAPOL 成功メッセージを送信するように指定します。 **recovery delay** *milliseconds* : 使用できない RADIUS サーバが使用できるようになったときに、スイッチがクリティカル ポートを再初期化するために待機する回復遅延期間を設定します。指定できる範囲は 1 ～ 10000 ミリ秒です。デフォルトは 1000 ミリ秒です（ポートは毎秒再初期化できます）。
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。サポートされるポートのタイプについては、「802.1X 認証設定時の注意事項」（P.9-36）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 サーバが到達不能の場合にポート上のホストを移動するには、次のキーワードを使用します。 • **authorize** : 認証しようとしている新しいホストをすべて、ユーザ指定のクリティカル VLAN に移動します。 • **reinitialize** : ポート上のすべての認証済みホストをユーザ指定のクリティカル VLAN に移動します。

	コマンド	目的
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て、次のキーワードを使用して機能を設定します。 • **recovery action reinitialize**：回復機能をイネーブルにして、認証サーバが使用可能なとき、回復動作中にポートを認証するように指定します。 • **vlan** *vlan-id*：スイッチがクリティカル ポートに割り当てるアクセス 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）コンフィギュレーション ファイルに設定を保存します。

RADIUS サーバ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 gigabitethernet0/2
Switch(config)# radius-server deadtime 60
Switch(config-if)# dot1x critical
Switch(config-if)# dot1x critical recovery action reinitialize
Switch(config-if)# dot1x critical vlan 20
Switch(config-if)# end
```

WoL を使用した 802.1X 認証の設定

WoL を使用した 802.1X 認証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。サポートされるポートのタイプについては、「802.1X 認証設定時の注意事項」（P.9-36）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 WoL を使用して 802.1X 認証をイネーブルにし、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、ホストとの間で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**：ポートを単方向に設定します。ポートはパケットをホストに送信できますが、ホストからパケットを受信できません。
ステップ 4	**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）コンフィギュレーション ファイルに設定を保存します。

スイッチで WoL を使用した 802.1X 認証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、WoL を使用した 802.1X 認証をイネーブルにして、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。サポートされるポートのタイプについては、「802.1X 認証設定時の注意事項」（P.9-36）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**	ポート上で 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）**eap** キーワードを使用して認証用の EAP を使用するようにスイッチを設定します。 （任意）**timeout activity** キーワードを使用して、未認証ステートに移行する前に接続されているホストを非アクティブにすることのできる秒数を設定します。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.23-9）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）コンフィギュレーション ファイルに設定を保存します。

MAC 認証バイパスをディセーブルにするには、**no dot1x mac-auth-bypass** インターフェイス コンフィギュレーション コマンドを使用します。

次に、MAC 認証バイパス機能をイネーブルにする例を示します。

```
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 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	**vlan group** *vlan-group-name* ***vlan-list*** *vlan-list*	VLAN グループを設定し、1 つの VLAN または一連の VLAN をそのグループにマッピングします。
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クリアします。

次に、VLAN グループを設定し、VLAN をそのグループにマッピングし、VLAN グループの設定および特定の 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 が削除され、VLAN グループが削除される例を示します。

```
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 グループをクリアする例を示します。

```
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。これは、RADIUS サーバを使用した 802.1X 認証とも呼ばれます。

NAC レイヤ 2 802.1X 検証を設定するには、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、音声 VLAN を除くあらゆるアクティブ 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（デフォルトではディセーブル）をイネーブルにします。
ステップ 5	**dot1x timeout reauth-period** {*seconds* | **server**}	再認証の間隔（秒）を指定します。 キーワードの意味は次のとおりです。 • *seconds*：秒数を 1 ～ 65535 の範囲で設定します。デフォルト値は 3600 秒です。 • **server**：Session-Timeout RADIUS アトリビュート（アトリビュート [27]）および Terminate-Action RADIUS アトリビュート（アトリビュート [29]）の値に基づいて秒数を指定します。 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）コンフィギュレーション ファイルに設定を保存します。

次に、NAC レイヤ 2 802.1X 検証を設定する例を示します。

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

NEAT を使用した認証者スイッチおよびサプリカント スイッチの設定

この機能を設定するには、ワイヤリング クローゼット外の 1 つのスイッチをサプリカントとして設定し、認証者スイッチに接続する必要があります。

概要については、「Network Edge Access Topology（NEAT）を使用した 802.1x サプリカント スイッチと認証スイッチ」（P.9-32）を参照してください。

（注）　ACS で *cisco-av-pairs* を *device-traffic-class=switch* と設定する必要があります。これはサプリカントが正常に認証された後に、インターフェイスをトランクとして設定します。

スイッチを認証者に設定するには、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 auto 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）として設定します。
ステップ 7	**spanning-tree portfast**	単一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 ポート上で 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）コンフィギュレーション ファイルに設定を保存します。

次に、スイッチを 802.1X 認証者に設定する例を示します。

```
Switch# configure terminal
Switch(config)# cisp enable
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に設定するには、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 資格情報プロファイルを作成します。これをサプリカントに設定するポートに付加する必要があります。
ステップ 4	**username** *suppswitch*	ユーザ名を作成します。
ステップ 5	**password** *password*	新しいユーザ名のパスワードを作成します。

	コマンド	目的
ステップ 6	**dot1x supplicant force-multicast**	スイッチがユニキャストまたはマルチキャスト パケットを受信したときに、スイッチが強制的にマルチキャスト EAPOL パケット*だけ*を送信するように設定します。 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 を機能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 PAE サプリカントに設定します。
ステップ 11	**dot1x credentials** *profile-name*	802.1X 資格情報プロファイルをインターフェイスに付加します。
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）コンフィギュレーション ファイルに設定を保存します。

次に、サプリカントとしてスイッチを設定する例を示します。

```
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-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
```

Auto SmartPort マクロを使用した NEAT の設定

スイッチ VSA ではなく Auto SmartPort ユーザ定義マクロを使用して、認証者スイッチを設定することもできます。詳細については、『*Auto Smartports Configuration Guide*』を参照してください。

ダウンロード ACL とリダイレクト URL を使用した 802.1X 認証の設定

スイッチに 802.1X 認証を設定するだけでなく、ACS を設定する必要があります。詳細については、Cisco Secure ACS 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 ACL をスイッチにダウンロードする前に、ACS でダウンロード 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、ポートのダウンロードされた ACL を表示できます。

ダウンロード ACL の設定

ポリシーは、クライアントが認証され、IP デバイス トラッキング テーブルにクライアント IP アドレスが追加された後に有効になります。その後、スイッチはダウンロード 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 デバイス トラッキング 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**	認証方式をローカルに設定します。認証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 send 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**	ポートのデフォルトの ACL を入力方向に設定します。 **（注）**　*acl-id* はアクセス リスト名または番号です。
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）コンフィギュレーション ファイルに設定を保存します。

ダウンロードポリシーの設定

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**	送信元アドレスおよびワイルドカードを使用して、デフォルト ポート ACL を定義します。 access-list-number は、1 ～ 99 または 1300 ～ 1999 の 10 進数です。 **deny** または **permit** を入力し、条件と一致した場合にアクセスを拒否するか、許可するかを指定します。 *source* は次のような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す。 • ドット付き 10 進表記で 32 ビットの値。 • 0.0.0.0 255.255.255.255 という source および source-wildcard 値の省略形を表すキーワード any。source-wildcard 値の入力は不要です。 • source 0.0.0.0 という source および source-wildcard の省略形を表すキーワード host。 （任意）source-wildcard ワイルドカード ビットを source に適用します。 （任意）log を指定すると、エントリと一致するパケットに関するログ通知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。

	コマンド	目的
ステップ 4	**ip access-group** *acl-id* **in**	ポートのデフォルトの ACL を入力方向に設定します。 **（注）**　*acl-id* はアクセス リスト名または番号です。
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**	認証方式をローカルに設定します。認証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 デバイス トラッキング テーブルをイネーブルにします。 IP デバイス トラッキング 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 デバイス トラッキング 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までに応答を待機する時間（秒単位）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）の 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**	ベンダー固有アトリビュートを認識し使用するために、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 ACL が動作している必要があります。
ステップ 11	**end**	特権 EXEC モードに戻ります。
ステップ 12	**show ip device tracking all**	IP デバイス トラッキング テーブルのエントリに関する情報を表示します。
ステップ 13	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

次の例で、ダウンロードポリシー用にスイッチを設定する方法を示します。

```
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 gigabitethernet0/1
Switch(config-if)# ip access-group default_acl in
Switch(config-if)# exit
```

VLAN ID に基づく 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 に基づく 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）コンフィギュレーション ファイルに設定を保存します。

VLAN ID に基づく MAC 認証のステータスを確認できる show コマンドはありません。RADIUS アトリビュート 32 を確認するには、**debug radius accounting** 特権 EXEC コマンドを実行します。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/docs/ios/debug/command/reference/db_q1.html#wp1123741

次に、スイッチで VLAN ID に基づく 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
```

柔軟な認証順序の設定

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 order** [**dot1x** | **mab**] | {**webauth**}	（任意）ポートで使用する認証方式の順番を設定します。
ステップ 4	**authentication priority** [**dot1x** | **mab**] | {**webauth**}	（任意）ポート プライオリティ リストに認証方式を追加します。
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）コンフィギュレーション ファイルに設定を保存します。

次の例で、ポートがまず 802.1X 認証を試み、次にフォールバック メソッドとして、Web 認証を試みるように設定する方法を示します。

```
Switch# configure terminal
Switch(config)# interface gigabitethernet0/1
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}**	（オプション）ポートを単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に、フォールバック メソッドとして 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）ポートの認証マネージャ モードを設定します。
ステップ 6	**authentication open**	（任意）ポートのオープン 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番を設定します。
ステップ 8	**authentication periodic**	（任意）ポートの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）ポート認証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）コンフィギュレーション ファイルに設定を保存します。

次の例で、ポートに Open1x を設定する方法を示します。

```
Switch# configure terminal
Switch(config)# interface gigabitethernet0/1
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
```

ポート上での 802.1X 認証のディセーブル化

802.1X 認証をポートで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。

	コマンド	目的
ステップ 3	**no dot1x pae**	ポート上で 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）コンフィギュレーション ファイルに設定を保存します。

802.1X Port Access Entity（PAE; ポート アクセス エンティティ）認証者としてポートを設定するには、**dot1x pae authenticator** インターフェイス コンフィギュレーション コマンドを使用します。この設定では、ポートで 802.1X がイネーブルになりますが、ポートに接続されたクライアントは許可されません。

次に、802.1X 認証をポートでディセーブルにする例を示します。

```
Switch(config)# interface gigabitethernet0/1
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戻すには、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戻します。
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）コンフィギュレーション ファイルに設定を保存します。

802.1X の統計情報およびステータスの表示

すべてのポートに関する 802.1X 統計情報を表示するには、**show dot1x all statistics** EXEC コマンドを使用します。特定のポートに関する 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。

スイッチに関する 802.1X 管理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。特定のポートに関する 802.1X 管理および動作ステータスを表示するには、**show dot1x interface** *interface-id* 特権 EXEC コマンドを使用します。

Cisco IOS Release 12.2(55)SE 以降では、**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、冗長な 802.1x 認証メッセージをフィルタリングできます。「認証マネージャ CLI コマンド」（P.9-10）を参照してください。

出力フィールドの詳細については、このリリースに対応するコマンド リファレンスを参照してください。