CHAPTER 35

ポート セキュリティの設定

この章では、Catalyst 4500 シリーズ スイッチ上で、ポート セキュリティを設定する方法について説明します。Catalyst 4500 シリーズ スイッチのポート セキュリティの概要と、アクセス、音声、トランク、プライベート VLAN など各種ポートの設定について説明します。

この章の内容は、次のとおりです。

（注） この章のスイッチ コマンドの構文および使用方法の詳細については、『*Catalyst 4500 Series Switch Cisco IOS Command Reference*』および次の URL の関連マニュアルを参照してください。

http://www.cisco.com/en/US/products/ps6350/index.html

コマンド リスト

この表には、主にポート セキュリティで共通に使用されるコマンドを示します。

コマンド	目的	ナビゲーション
errdisable recovery cause psecure-violation	セキュア ポートの errdisable ステートを解除します。	「違反処理」（P.35-6）
errdisable recovery interval	指定した errdisable 理由から回復する時間をカスタマイズします。	「違反処理」（P.35-6）
port-security mac-address	それぞれの VLAN にセキュアなすべての MAC アドレスを設定します。	「セキュア MAC アドレス」（P.35-3）

コマンド	目的	ナビゲーション
port-security maximum	インターフェイスに MAC アドレスの最大数を設定します。	「アクセス ポート上のポート セキュリティの設定」（P.35-7）
private-vlan association add	セカンダリ VLAN とプライマリ VLAN のアソシエーションを作成します。	「独立 PVLAN ホスト ポートでのポート セキュリティの例」（P.35-15）
private-vlan isolated	VLAN を PVLAN として指定します。	「独立プライベート VLAN ホスト ポートでのポート セキュリティの設定」（P.35-14）
private-vlan primary	VLAN をプライマリ プライベート VLAN として指定します。	「独立プライベート VLAN ホスト ポートでのポート セキュリティの設定」（P.35-14）
switchport mode private-vlan host	有効な PVLAN トランクのアソシエーションを持つポートが、アクティブ ホストの PVLAN トランク ポートになるように指定します。	「独立プライベート VLAN ホスト ポートでのポート セキュリティの設定」（P.35-14）
switchport private-vlan host-association	独立ホスト ポート上でホスト アソシエーションを定義します。	「独立プライベート VLAN ホスト ポートでのポート セキュリティの設定」（P.35-14）
switchport private-vlan mapping	無差別ポートに対して PVLAN を定義します。	「独立プライベート VLAN ホスト ポートでのポート セキュリティの設定」（P.35-14）
switchport port-security	ポート セキュリティをイネーブルにします。	「アクセス ポート上のポート セキュリティの設定」（P.35-7）
switchport port-security aging static	MAC アドレスのスタティック エージングを設定します。	「セキュア MAC アドレスのエージング」（P.35-5）
switchport port-security aging time	ポートに対してエージング タイムを指定します。	「例 3：エージング タイマーの設定」（P.35-11）
switchport port-security limit rate invalid-source-mac	不良パケットに対してレート制限を設定します。	「例 7：不良パケットに対するレート制限の設定」（P.35-13）
switchport port-security mac-address	インターフェイスに対してセキュア MAC アドレスを設定します。	「例 5：セキュア MAC アドレスの設定」（P.35-11）
switchport port-security mac-address *<mac_address>* **sticky**	インターフェイスに対してスティッキ MAC アドレスを指定します。	「アクセス ポート上のポート セキュリティの設定」（P.35-7）
switchport port-security mac-address sticky	スティッキ ポート セキュリティをイネーブルにします。	「ポートのスティッキ アドレス」（P.35-5）
no switchport port-security mac-address sticky	スティッキ セキュア MAC アドレスをダイナミック MAC セキュア アドレスに変換します。	「アクセス ポート上のポート セキュリティの設定」（P.35-7）
switchport port-security maximum	インターフェイスに対して最大セキュア MAC アドレス数を設定します。	「例 1：最大セキュア アドレス数の設定」（P.35-10）
switchport port-security violation	違反モードを設定します。	「例 2：違反モードの設定」（P.35-10）

コマンド	目的	ナビゲーション
no switchport port-security violation	違反モードを設定します。	「アクセス ポート上のポート セキュリティの設定」（P.35-7）
switchport trunk encapsulation dot1q	カプセル化モードを dot1q に設定します。	「例 1：すべての VLAN での最大セキュア MAC アドレス制限の設定」（P.35-18）

ポート セキュリティの概要

ポート セキュリティを使用すると、ポート上で MAC アドレス（*セキュア MAC アドレス*）の数を制限し、未認証 MAC アドレスによるアクセスを防ぐことができます。また、指定したポートにセキュア MAC アドレスの最大数を設定することもできます（トランク ポートの VLAN に対しても任意で設定できます）。セキュア ポートが最大数を超えるとセキュリティ違反がトリガーされ、そのポートに設定された違反処理モードに基づいて違反アクションが実行されます。

そのポートの最大セキュア MAC アドレス数を 1 に設定すると、そのセキュア ポートに接続された装置だけがそのポートにアクセスできるようになります。

ポート上でセキュア MAC アドレスがセキュアな場合、その MAC アドレスはその VLAN 以外のポートでは受信されません。他の VLAN のポートに送信すると、パケットは通知されないままハードウェアでドロップされます。インターフェイスまたはポート カウンタを使用する場合は別として、ドロップされたことを知らせるログ メッセージが表示されることはありません。これにより違反がトリガーされることに注意する必要があります。このようなパケットはハードウェアでドロップする方が効率的であり、CPU に余分な負荷がかかることはありません。

ポート セキュリティには次のような特性があります。

- セキュア MAC アドレスをエージング アウトできます。サポートされているエージングは、非アクティブと絶対の 2 種類です。
- スティッキ機能をサポートします。この機能により、ポート上のセキュア MAC アドレスがスイッチのリブートとリンク フラップを通じて保持されます。
- アクセス、音声、トランク、EtherChannel、プライベート VLAN ポートなど、さまざまな種類のポート上で設定できます。

ここでは、次の内容について説明します。

- 「セキュア MAC アドレス」（P.35-3）
- 「セキュア MAC アドレスの最大数」（P.35-4）
- 「セキュア MAC アドレスのエージング」（P.35-5）
- 「ポートのスティッキ アドレス」（P.35-5）
- 「違反処理」（P.35-6）

セキュア MAC アドレス

ポート セキュリティは、次のタイプのセキュア MAC アドレスをサポートします。

- ダイナミックまたは学習済み：セキュア ポートのホストからパケットを受信すると、ダイナミック セキュア MAC アドレスが学習されます。このタイプは、ユーザの MAC アドレスが固定されていない場合（たとえばラップトップ コンピュータの場合）に使用できます。

- スタティックまたは設定済み：ユーザは、CLI または SNMP を通じてスタティック セキュア MAC アドレスを設定します。このタイプは、MAC アドレスが固定されている場合（たとえば PC の場合）に使用します。
- スティッキ：スティッキ アドレスはダイナミック セキュア MAC アドレスと同じように学習されますが、スタティック セキュア MAC アドレスと同じようにスイッチの再起動やリンク フラップを通じて継続されます。このタイプは、固定 MAC アドレスが多数あって手動で MAC アドレスを設定しない場合（たとえば 100 台の PC がそれぞれのポートでセキュアになっている場合）に使用します。

ポートのセキュア MAC アドレスが最大数を超過しているときにスタティック セキュア MAC アドレスを設定しようとすると、設定が拒否されエラー メッセージが表示されます。ポートのセキュア MAC アドレスが最大数を超過しているときにダイナミック セキュア MAC アドレスが新しく追加されると、違反処理がトリガーされます。

ダイナミック セキュア MAC アドレスをクリアするには、**clear port-security** コマンドを使用します。スティッキ セキュア MAC アドレスとスタティック セキュア MAC アドレスを同時にクリアするには、**switchport port-security mac-address** コマンドの **no** 形式を使用します。

セキュア MAC アドレスの最大数

セキュア ポートの MAC アドレスは、デフォルトで 1 つです。このデフォルト値は、1 ～ 3,000 の任意の値に変更できます。上限の 3,000 を指定すると、各ポートに MAC アドレスが 1 つ設定され、さらにシステムのポート全体で 3,000 の MAC アドレスが設定されます。

ポートに最大セキュア MAC アドレス数を設定すると、セキュア アドレスを次のいずれかの方法でアドレス テーブルに含めることができます。

- セキュア MAC アドレスを設定するには、**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 コマンドを使用します。
- トランクポートの VLAN 範囲にすべてのセキュア MAC アドレスを設定するには、**port-security mac-address** VLAN 範囲コンフィギュレーション コマンドを使用します。
- 接続されているデバイスの MAC アドレスで、ポートがセキュア MAC アドレスをダイナミックに設定するようにすることができます。
- いくつかのアドレスを手動で設定し、残りは動的に設定されるようにすることも可能です。

（注） ポートのリンクがダウンした場合、そのポート上のダイナミック セキュア アドレスはすべてセキュアではなくなります。

- MAC アドレスをスティッキに設定できます。MAC アドレスは動的に学習されるか、または手動で設定され、アドレス テーブル内に格納され、実行コンフィギュレーションに追加されます。これらのアドレスをコンフィギュレーション ファイルに保存した後は、スイッチを再起動しても、インターフェイスはこれらのアドレスを動的に再学習する必要がありません。スティッキ セキュア アドレスを手動で設定することは可能ですが、推奨しません。

（注） トランク ポートでは、セキュア MAC アドレスの最大数をポートとポート VLAN の両方に設定できます。ポートの最大数をポート VLAN の最大数以上にすることはできますが、ポート VLAN の最大数よりも小さくすることはできません。ポートの最大数がいずれかのポート VLAN の最大数よりも小さい場合（VLAN 10 の最大数を 3 に設定し、「スイッチ ポートの最大数」を設定しない場合（デフォルトは 1））、VLAN 10 のダイナミック アドレスが 2 つになるとポートはシャットダウンします（「ポートセキュリティに関する注意事項および制約事項」（P.32）を参照）。ポート VLAN の最大数により、指定

した VLAN の指定したポートに最大数が設定されます。指定した VLAN で最大数を超過し、ポートの最大数は超過していない場合でも、ポートはシャットダウンします。ポートのいずれか 1 つの VLAN が違反した場合でも、ポート全体がシャットダウンします。

セキュア MAC アドレスのエージング

スイッチが 3,000 件より多くの入力アドレスを受信する場合、セキュア MAC アドレスをエージングさせることができます。

（注）　スティッキ アドレスのエージングはサポートされません。

デフォルトでは、ポートセキュリティはセキュア MAC アドレスをエージング アウトしません。学習された MAC アドレスは、スイッチが再起動するかリンクがダウンするまでポートに残ります（スティッキ機能がイネーブルでない限り）。ただしポート セキュリティでは、絶対モードまたは非アクティビティ モードおよびエージング間隔（1 ～ n、分単位）に基づいてエージングを設定できます。

- 絶対モード：n と n+1 の間のエージング
- 非アクティビティ モード：n+1 と n+2 の間のエージング

この機能を使用すると、既存のセキュア MAC アドレスを手動で削除しなくても、ポートのセキュア アドレス数を制限しながら、セキュア ポート上の PC の取り外しを削除および追加ができます。

switchport port-security aging static コマンドを使用してスタティック エージングを明示的に設定しない限り、ポートでエージングが設定されていてもスタティック アドレスがエージングすることはありません。

（注）　エージングは 1 分ごとに増加します。

ポートのスティッキ アドレス

スティッキ ポート セキュリティをイネーブルにすると、ダイナミック MAC アドレスをスティッキ セキュア MAC アドレスに変換し、それらを実行コンフィギュレーションに追加するように、インターフェイスを設定できます。この作業は、ユーザが他のポートに移動しないことがわかっている場合や各ポートに MAC アドレスを静的に設定しない場合に行います。

（注）　別のシャーシを使用する場合は、別の MAC アドレスが必要です。

スティッキ ポート セキュリティをイネーブルにするには、**switchport port-security mac-address sticky** コマンドを入力します。このコマンドを入力すると、インターフェイスはスティッキ ラーニングがイネーブルになる前に学習したものを含め、すべてのダイナミック セキュア MAC アドレスをスティッキ セキュア MAC アドレスに変換します。

スティッキ セキュア MAC アドレスは、コンフィギュレーション ファイル（スイッチが再起動されるたびに使用されるスタートアップ コンフィギュレーション）に、自動的には反映されません。コンフィギュレーション ファイルに実行コンフィギュレーション ファイルをユーザが保存した場合は、スイッチを再起動するときに、インターフェイスはこれらのアドレスを再学習する必要がありません。この設定は保存しないと失われます。

スティッキ ポート セキュリティをディセーブルにした場合、スティッキ セキュア MAC アドレスはダイナミック セキュア アドレスに変換され、実行コンフィギュレーションから削除されます。

最大数のセキュア MAC アドレスが設定されると、それらはアドレス テーブルに保存されます。接続デバイスがポートに唯一アクセスできるようにする場合は、接続デバイスの MAC アドレスを設定し、最大アドレス数を 1 に設定します（デフォルト設定）。

ポートに対する最大数のセキュア MAC アドレスがアドレス テーブルに追加されている場合に、アドレス テーブルにない MAC アドレスを持つワークステーションがインターフェイスにアクセスしようとすると、セキュリティ違反が発生します。

違反処理

ポートのセキュア MAC アドレス数がそのポートで許容されている最大セキュア MAC アドレス数を超過した場合、セキュリティ違反がトリガーされます。

（注） あるポートでセキュアなホストが別のポートで認識された場合は、セキュア違反はトリガーされません。Catalyst 4500 シリーズ スイッチはハードウェア上で、そのようなパケットを新しいポートで自動的にドロップし、CPU に余分な負荷をかけません。

次のいずれかの違反モードをインターフェイスに設定できます。違反に対する応答に基づいています。

- restrict（制限）：ポート セキュリティ違反によりデータが制限され（つまり、ソフトウェアでパケットがドロップされ）、セキュリティ違反カウンタが増加し、SNMP 通知が生成されます。このモードは、セキュア ポートのサービスやアクセスを中断しないために設定します。

  SNMP トラップが生成される頻度は、**snmp-server enable traps port-security trap-rate** コマンドで制御できます。デフォルト値（「0」）の場合、SNMP トラップはセキュリティ違反が発生するたびに生成されます。

- shutdown（シャットダウン）：ポート セキュリティ違反が発生すると、インターフェイスがただちにシャットダウンします。このモードは非常にセキュアな環境で使用します。セキュアではない MAC アドレスがソフトウェアで拒否されることを回避し、サービスが中断しても問題ではない場合です。

  errdisable recovery cause psecure-violation グローバル コンフィギュレーション コマンドを設定すると、セキュア ポートが errdisable ステートの場合に実行してこのステートを自動的に解除できます。また、**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 コマンドを入力すると、手動で再びイネーブルにできます これは、デフォルトのモードです。

  また、**errdisable recovery interval** *interval* コマンドを入力して、指定したエラー ディセーブル理由から回復する時間（デフォルトは 300 秒）をカスタマイズすることも可能です。

無効なパケット操作

デバイスが無効なパケットを送信すると思われる場合（トラフィック ジェネレータ、スニッファ、不良な NIC など）、セキュア ポート上で無効な送信元 MAC アドレス パケットのレート制限を行えます。ポート セキュリティにより、すべてゼロの MAC アドレスを持つパケットと、マルチキャストまたはブロードキャスト送信元 MAC アドレスを持つパケットは、無効なパケットと見なされます。これらのパケットのレート制限を選択し、レートを超過した場合はポートに対する違反処理をトリガーできます。

アクセス ポート上のポート セキュリティ

ここでは、ポート セキュリティを設定する手順について説明します。

（注） アクセス モードに設定されたレイヤ 2 ポート チャネル インターフェイスのポート セキュリティはイネーブルにできます。EtherChannel のポート セキュリティ設定は、物理メンバ ポートの設定とは別に保持されます。

アクセス ポート上のポート セキュリティの設定

ポートで許容されたステーションの MAC アドレスを制限および識別することにより、ポートのトラフィックを制限するには、次の作業を行います。

	コマンド	目的
ステップ 1	`Switch(config)# interface interface_id` `interface port-channel port_channel_number`	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、設定するインターフェイスを指定します。 **（注）** レイヤ 2 ポート チャネル論理インターフェイスを指定できます。
ステップ 2	`Switch(config-if)# switchport mode access`	インターフェイス モードを設定します。 **（注）** デフォルト モード（dynamic desirable）のインターフェイスは、セキュア ポートとして設定できません。
ステップ 3	`Switch(config-if)# [no] switchport port-security`	インターフェイス上でポート セキュリティをイネーブルにします。 インターフェイスをセキュア ポートでないデフォルトの状態に戻すには、**no switchport port-security** コマンドを使用します。
ステップ 4	`Switch(config-if)# [no] switchport port-security maximum value`	（任意）インターフェイスの最大セキュア MAC アドレス数を設定します。指定できる範囲は 1 ～ 3072 です。デフォルト値は 1 です。 インターフェイスをデフォルトのセキュア MAC アドレス数に戻すには、no **switchport port-security maximum** *value* を使用します。

	コマンド	目的 （続き）
ステップ 5	`Switch(config-if)# switchport port-security [aging {static | time aging_time | type {absolute | inactivity}]`	ポート上のすべてのセキュア アドレスに対して、エージング タイムとエージング タイプを設定します。 この機能を使用すると、既存のセキュア MAC アドレスを手動で削除しなくても、ポートのセキュア アドレス数を制限しながら、セキュア ポート上の PC の取り外しおよび追加ができます。 **static** キーワードは、このポートに静的に設定されたセキュア アドレスのエージングをイネーブルにします。 **time** *aging_tim* キーワードは、このポートのエージング タイムを指定します。*aging_time* の有効範囲は 0 ～ 1,440 分です。時間が 0 の場合、このポートのエージングはディセーブルになります。 **type** キーワードは、エージング タイプを **absolute** または **inactive** に設定します。 • **absolute**：このポートのすべてのセキュア アドレスは指定した時間（分）が経過したあとに期限切れとなり、セキュア アドレス リストから削除されます。 • **inactive**：指定された時間内にセキュア送信元アドレスからのデータ トラフィックがない場合のみ、このポートのセキュア アドレスが期限切れとなります。 ポート上のすべてのセキュア アドレスに対してポート セキュリティ エージングをディセーブルにするには、**no switchport port-security aging time** 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。
ステップ 6	`Switch(config-if)# [no] switchport port-security violation {restrict | shutdown}`	（任意）違反モードを設定します。セキュリティ違反が発生した場合に、次のいずれかのアクションを実行します。 • **restrict**：ポート セキュリティ違反によりデータが制限され、セキュリティ違反カウンタが増加して、SNMP トラップ通知が送信されます。 • **shutdown**：セキュリティ違反が発生すると、インターフェイスが errdisable になります。 **（注）** セキュア ポートが errdisable ステートの場合、**errdisable recovery cause psecure-violation** 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このステートを解除したり、**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 コマンドを入力して手動で再びイネーブルにしたりできます。 違反モードをデフォルト状態（shutdown モード）に戻すには、**no switchport port-security violation shutdown** コマンドを使用します。
ステップ 7	`Switch(config-if)# switchport port-security limit rate invalid-source-mac packets_per_sec`	不良パケットに対してレート制限を設定します。 デフォルトは 10 pps です。

	コマンド	目的 （続き）
ステップ 8	`Switch(config-if)# [no] switchport port-security mac-address mac_address`	（任意）インターフェイスのセキュア MAC アドレスを入力します。このコマンドを使用するとセキュア MAC アドレスが設定できます。設定したセキュア MAC アドレスが最大数より少ない場合、残りの MAC アドレスは動的に学習されます。 MAC アドレスをアドレス テーブルから削除するには、**no switchport port-security mac-address** *mac_address* コマンドを使用します。 **（注）** このコマンドは、アクセス、PVLAN ホスト、および PVLAN 無差別モードに対してのみ適用できます。PVLAN、トランク、または通常のトランク モードの詳細については、「トランク ポートのポート セキュリティ」（P.35-16）を参照してください。
ステップ 9	`Switch(config-if)# [no] switchport port-security mac-address sticky`	（任意）インターフェイスでスティッキー ラーニングをイネーブルにします。 インターフェイス上でスティッキ ラーニングをディセーブルにするには、**no switchport port-security mac-address sticky** コマンドを使用します。インターフェイスがスティッキー セキュア MAC アドレスをダイナミック セキュア アドレスに変換します。
ステップ 10	`Switch(config-if)# [no] switchport port-security mac-address mac_address sticky [vlan [voice | access]]`	インターフェイスにスティッキ MAC アドレスを指定します。 **vlan** キーワードを指定すると、指定した VLAN の MAC アドレスがスティッキになります。 アドレス テーブルからスティッキ セキュア MAC アドレスを削除するには、**no switchport port-security mac-address** *mac_address* **sticky** コマンドを使用します。スティッキ アドレスをダイナミック アドレスに変換するには、**no switchport port-security mac-address sticky** コマンドを使用します。 **（注）** このコマンドは、アクセス、PVLAN ホスト、および PVLAN 無差別モードに対してのみ適用できます。PVLAN、トランク、または通常のトランク モードの詳細については、「トランク ポートのポート セキュリティ」（P.35-16）を参照してください。
ステップ 11	`Switch(config-if)# end`	特権 EXEC モードに戻ります。
ステップ 12	`Switch# show port-security address interface interface_id` `Switch# show port-security address`	入力を確認します。

（注） ダイナミックに学習されたポート セキュリティ MAC アドレスを CAM テーブルから削除するには、**clear port-security dynamic** コマンドを使用します。**address** キーワードを指定すると、セキュア MAC アドレスを削除できます。**interface** キーワードを指定すると、各種のインターフェイス上の

（ポート チャネル インターフェイスを含む）すべてのセキュア アドレスを削除できるようになります。**VLAN** キーワードにより、VLAN 単位 / ポート単位でポート セキュリティ MAC アドレスをクリアできます。

例

ここでは、次の例を示します。

例 1：最大セキュア アドレス数の設定

次に、ファスト イーサネット インターフェイス 3/12 でポート セキュリティをイネーブルにし、セキュア アドレスの最大数を 5 に設定する例を示します。違反モードはデフォルトで、セキュア MAC アドレスは設定されていません。

```
Switch# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# interface fastethernet 3/12
Switch(config-if)# switchport mode access
Switch(config-if)# switchport port-security
Switch(config-if)# switchport port-security maximum 5
Switch(config-if)# switchport port-security mac-address sticky
Switch(config-if)# end
Switch# show port-security interface fastethernet 3/12
Port Security              : Enabled
Port Status                : Secure-up
Violation Mode             : Shutdown
Aging Time                 : 0 mins
Aging Type                 : Absolute
SecureStatic Address Aging : Enabled
Maximum MAC Addresses      : 5
Total MAC Addresses        : 0
Configured MAC Addresses   : 0
Sticky MAC Addresses       : 0
Last Source Address:Vlan   : 0000.0000.0000:0
Security Violation Count   : 0
```

例 2：違反モードの設定

この例では、ファスト イーサネット インターフェイス 3/12 の違反モードを restrict に設定する例を示します。

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# interface fastethernet 3/12
```

```
Switch(config-if)# switchport port-security violation restrict
Switch(config-if)# end
Switch#
```

レート制限を使用することによって SNMP トラップをイネーブルにし、制限モードによるポートセキュリティ違反を検出します。次に、1 秒間に 5 回のポート セキュリティのトラップを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)# snmp-server enable traps port-security trap-rate 5
Switch(config)# end
Switch#
```

例 3：エージング タイマーの設定

次に、ファスト イーサネット インターフェイス 5/1 のセキュア アドレスのエージング タイムを 2 時間（120 分）に設定する例を示します。

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# interface fastethernet 5/1
Switch(config-if)# switchport port-security aging time 120
Switch(config-if)# end
Switch#
```

次に、エージング タイムを 2 分に設定する例を示します。

```
Switch(config-if)# switchport port-security aging time 2
```

上記のコマンドを確認するには、**show port-security interface** コマンドを使用します。

例 4：エージング タイマーのタイプの設定

次に、インターフェイス ファスト イーサネット 3/5 のセキュア アドレスでエージング タイム タイプを inactivity に設定する例を示します。

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# interface fastethernet 3/5
Switch(config-if)# switch port-security aging type inactivity
Switch(config-if)# end
Switch# show port-security interface fastethernet 3/5
Port Security              : Enabled
Port Status                : Secure-up
Violation Mode             : Shutdown
Aging Time                 : 0 mins
Aging Type                 : Inactivity
SecureStatic Address Aging : Disabled
Maximum MAC Addresses      : 1
Total MAC Addresses        : 0
Configured MAC Addresses   : 0
Sticky MAC Addresses       : 0
Last Source Address:Vlan   : 0000.0000.0000:0
Security Violation Count   : 0
```

例 5：セキュア MAC アドレスの設定

次に、ファスト イーサネット インターフェイス 5/1 にセキュア MAC アドレスを設定し、設定を確認する例を示します。

```
Switch# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# interface fastethernet 5/1
Switch(config-if)# switchport mode access
Switch(config-if)# switchport port-security
Switch(config-if)# switchport port-security maximum 10
Switch(config-if)# switchport port-security mac-address 0000.0000.0003 (Static secure MAC)
Switch(config-if)# end
Switch#show port address
Secure Mac Address Table
------------------------------------------------------------------------
Vlan    Mac Address       Type                      Ports   Remaining Age
                                                              (mins)
----    -----------       ----                      -----   -------------
   1    0000.0000.0003    SecureConfigured          Fa5/1         -

------------------------------------------------------------------------
Total Addresses in System (excluding one mac per port)     : 2
Max Addresses limit in System (excluding one mac per port) : 3072
```

例 6：スティッキ ポート セキュリティの設定

次に、ファスト イーサネット インターフェイス 5/1 にスティッキ MAC アドレスを設定し、設定を確認する例を示します。

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# interface fa5/1
Switch(config-if)# switchport mode access
Switch(config-if)# switchport port-security
Switch(config-if)# switchport port-security mac-address sticky
Switch(config-if)# switchport port-security maximum 5
Switch(config-if)# end
```

（注） ポートにトラフィックを送信すると、ポートにスティッキ セキュア アドレスが設定されます。

```
Switch# show port-security address
          Secure Mac Address Table
------------------------------------------------------------------------
Vlan    Mac Address       Type                      Ports   Remaining Age
                                                              (mins)
----    -----------       ----                      -----   -------------
   1    0000.0000.0001    SecureSticky              Fa5/1         -
   1    0000.0000.0002    SecureSticky              Fa5/1         -
   1    0000.0000.0003    SecureSticky              Fa5/1         -
------------------------------------------------------------------------
Total Addresses in System (excluding one mac per port)     : 2
Max Addresses limit in System (excluding one mac per port) : 3072
Switch# show running-config interface fastEthernet 5/1
Building configuration...

Current configuration : 344 bytes
!
interface FastEthernet5/1
 switchport mode access
 switchport port-security
 switchport port-security maximum 5
 switchport port-security mac-address sticky
 switchport port-security mac-address sticky 0000.0000.0001
 switchport port-security mac-address sticky 0000.0000.0002
 switchport port-security mac-address sticky 0000.0000.0003
```

```
end

Switch#
```

例 7：不良パケットに対するレート制限の設定

次に、ファスト イーサネット インターフェイス 5/1 の無効な送信元パケットにレート制限を設定する例を示します。

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# interface fastethernet 5/1
Switch(config-if)# switchport port-security limit rate invalid-source-mac 100
Switch(config-if)# end
Switch#
```

次に、ファスト イーサネット インターフェイス 5/1 の無効な送信元パケットにレート制限を設定する例を示します。

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# interface fastethernet 5/1
Switch(config-if)# switchport port-security limit rate invalid-source-mac none
Switch(config-if)# end
Switch#
```

例 8：ダイナミック セキュア MAC アドレスの削除

次に、ダイナミック セキュア MAC アドレスを削除する例を示します。

```
Switch# clear port-security dynamic address 0000.0001.0001
```

次に、インターフェイス fa 2/1 のすべてのダイナミック セキュア MAC アドレスを削除する例を示します。

```
Switch# clear port-security dynamic interface fa2/1
```

次に、システムのすべてのダイナミック セキュア MAC アドレスを削除する例を示します。

```
Switch# clear port-security dynamic
```

プライベート VLAN ポートのポート セキュリティ

PVLAN ポート上でポート セキュリティを設定すると、PVLAN 機能を利用しながら MAC アドレスの数を制限することができます。

（注） ここでは、アクセス ポートで説明したものと同じ設定モデルを使用します。

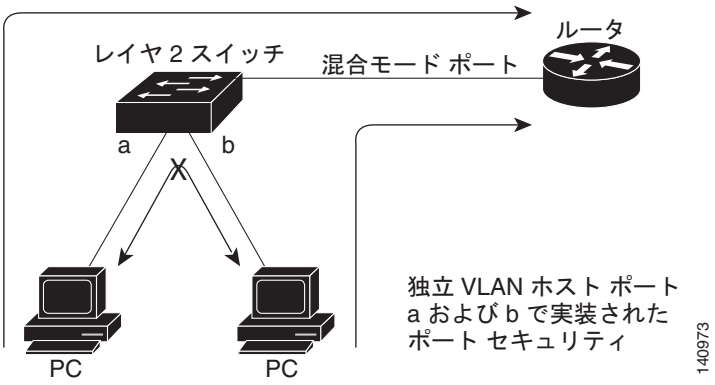
ここでは、ホストと無差別ポート上でトランク ポート セキュリティを設定する方法を説明します。

- 「独立プライベート VLAN ホスト ポートでのポート セキュリティの設定」（P.35-14）
- 「独立 PVLAN ホスト ポートでのポート セキュリティの例」（P.35-15）
- 「PVLAN 無差別ポートでのポート セキュリティの設定」（P.35-15）
- 「PVLAN 無差別モード ポートでのポート セキュリティの例」（P.35-16）

独立プライベート VLAN ホスト ポートでのポート セキュリティの設定

図 35-1 に、PVLAN ホスト ポートに実装されている代表的なポート セキュリティのトポロジを示します。このトポロジでは、スイッチのポート a で接続する PC は、無差別ポートで接続するルータだけと通信できます。ポート a で接続する PC はポート b で接続する PC とは通信できません。

図 35-1　独立 PVLAN ホスト ポートのポート セキュリティ



（注） PVLAN 上の独立 PVLAN ホスト ポートでセキュアなダイナミック アドレスはセカンダリ VLAN 上でセキュアであり、プライマリ VLAN 上ではセキュアではありません。

独立 PVLAN ホスト ポート上でポート セキュリティを設定するには、次の作業を実行します。

	コマンド	目的
ステップ 1	`Switch# 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	`Switch(config)# vlan sec_vlan_id`	セカンダリ VLAN を指定します。
ステップ 3	`Switch(config-vlan)# private-vlan isolated`	PVLAN モードを isolated に設定します。
ステップ 4	`Switch(config-vlan)# 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 5	`Switch(config)# vlan pri_vlan_id`	プライマリ VLAN を指定します。
ステップ 6	`Switch(config-vlan)# private-vlan primary`	VLAN をプライマリ PVLAN として指定します。
ステップ 7	`Switch(config-vlan)# private-vlan association add sec_vlan_id`	セカンダリ VLAN とプライマリ VLAN のアソシエーションを作成します。
ステップ 8	`Switch(config-vlan)# 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 9	`Switch(config)# 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、設定する物理インターフェイスを指定します。
ステップ 10	`Switch(config-if)# switchport mode private-vlan host`	有効な PVLAN トランクのアソシエーションを持つポートが、アクティブ ホストの PVLAN トランク ポートになるように指定します。
ステップ 11	`Switch(config-if)# switchport private-vlan host-association primary_vlan secondary_vlan`	独立ホスト ポート上でホスト アソシエーションを設定します。
ステップ 12	`Switch(config-if)# [no] switchport port-security`	インターフェイス上でポート セキュリティをイネーブルにします。

	コマンド	目的 （続き）
ステップ 13	Switch(config-if)# **end**	特権 EXEC モードに戻ります。
ステップ 14	Switch# **show port-security address interface** *interface_id* Switch# **show port-security address**	入力を確認します。

独立 PVLAN ホスト ポートでのポート セキュリティの例

次に、独立 PVLAN ホスト ポートであるファスト イーサネット インターフェイス 3/12 上でポート セキュリティを設定する例を示します。

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# vlan 6
Switch(config-vlan)# private-vlan isolated
Switch(config-vlan)# exit
Switch(config)# vlan 3
Switch(config-vlan)# private-vlan primary
Switch(config-vlan)# private-vlan association add 6
Switch(config-vlan)# exit
Switch(config)# interface fastethernet 3/12
Switch(config-if)# switchport mode private-vlan host
Switch(config-if)# switchport private-vlan association host 3 6
Switch(config-if)# switchport port-security
Switch(config-if)# end
```

PVLAN 無差別ポートでのポート セキュリティの設定

独立 PVLAN 無差別ポート上でポート セキュリティを設定するには、次の作業を実行します。

	コマンド	目的
ステップ 1	Switch# **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	Switch(config)# **vlan** *sec_vlan_id*	VLAN を設定します。
ステップ 3	Switch(config-vlan)# **private-vlan isolated**	PVLAN モードを isolated に設定します。
ステップ 4	Switch(config-vlan)# **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 5	Switch(config)# **vlan** *pri_vlan_id*	VLAN を設定します。
ステップ 6	Switch(config-vlan)# **private-vlan primary**	VLAN をプライマリ PVLAN として指定します。
ステップ 7	Switch(config-vlan)# **private-vlan association add** *sec_vlan_id*	セカンダリ VLAN とプライマリ VLAN のアソシエーションを作成します。
ステップ 8	Switch(config-vlan)# **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 9	Switch(config)# **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、設定する物理インターフェイスを指定します。
ステップ 10	Switch(config-if)# **switchport mode private-vlan promiscuous**	有効な PVLAN マッピングのあるポートがアクティブ無差別ポートになるように指定します。
ステップ 11	Switch(config-if)# **switchport private-vlan mapping** *primary_vlan secondary_vlan*	無差別ポートに対して PVLAN を設定します。
ステップ 12	Switch(config-if)# **switchport port-security**	インターフェイス上でポート セキュリティをイネーブルにします。

	コマンド	目的 （続き）
ステップ 13	`Switch(config-if)# end`	特権 EXEC モードに戻ります。
ステップ 14	`Switch# show port-security address interface interface_id` `Switch# show port-security address`	入力を確認します。

PVLAN 無差別モード ポートでのポート セキュリティの例

次に、PVLAN 無差別ポートであるファスト イーサネット インターフェイス 3/12 上でポート セキュリティを設定する例を示します。

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# vlan 6
Switch(config-vlan)# private-vlan isolated
Switch(config-vlan)# exit
Switch(config)# vlan 3
Switch(config-vlan)# private-vlan primary
Switch(config-vlan)# private-vlan association add 6
Switch(config-vlan)# exit
Switch(config)# interface fastethernet 3/12
Switch(config-if)# switchport mode private-vlan promiscuous
Switch(config-if)# switchport mode private-vlan mapping 3 6
Switch(config-if)# switchport port-security
Switch(config-if)# end
```

トランク ポートのポート セキュリティ

メトロ集約のトランク ポート上にポート セキュリティを設定すると、VLAN ごとに MAC アドレスの数を制限することができます。トランク ポート セキュリティにより、ポート セキュリティがトランク ポートにまで拡張されます。許容される MAC アドレスまたは MAC アドレスの最大数は、トランク ポート上の個々の VLAN ごとに制限されます。トランク ポート セキュリティにより、サービス プロバイダーはそのトランク ポートの VLAN に指定されたものとは異なる MAC アドレスを持つステーションからのアクセスをブロックできるようになります。また、トランク ポート セキュリティは PVLAN のトランク ポートでもサポートされます。

（注）　アクセス モードに設定されたレイヤ 2 ポート チャネル インターフェイスのポート セキュリティはイネーブルにできます。EtherChannel のポート セキュリティ設定は、物理メンバ ポートの設定とは別に保持されます。

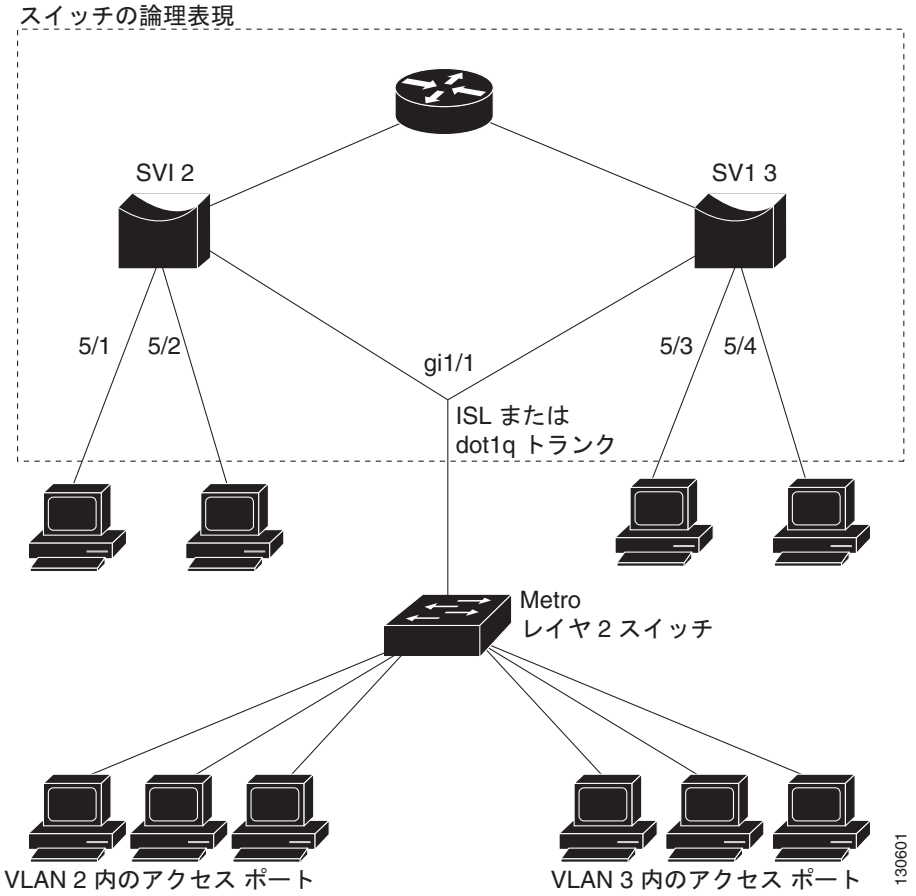
ここでは、トランク ポート セキュリティを設定する方法について説明します。

- 「トランク ポート セキュリティの設定」（P.35-17）
- 「トランク ポート セキュリティの例」（P.35-18）
- 「トランク ポート セキュリティの注意事項および制約事項」（P.35-20）

トランク ポート セキュリティの設定

Catalyst 4500 シリーズ スイッチの 802.1q または ISL トランクがネイバー レイヤ 2 スイッチに接続されている場合は、トランク ポート セキュリティが使用されます。たとえば、メトロ集約ネットワーク（図 35-2）で使用されます。

図 35-2　　トランク ポート セキュリティ



さまざまなポート セキュリティ関連パラメータをポート単位/VLAN 単位で設定できます。

（注） ポート セキュリティ パラメータを設定する手順はアクセス ポートの場合と似ています。トランク ポートの場合は、これらの手順に加えて次のポート単位/VLAN 単位設定を行います。

ポート セキュリティ関連パラメータを VLAN 単位/ポート単位で設定するには、次の作業を行います。

	コマンド	目的
ステップ 1	`Switch(config)# interface interface_id` `interface port-channel port_channel_number`	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、設定するインターフェイスを指定します。 **（注）** レイヤ 2 ポート チャネル論理インターフェイスを指定できます。
ステップ 2	`Switch(config-if)# switchport trunk encapsulation dot1q`	トランク カプセル化形式を 802.1Q に設定します。
ステップ 3	`Switch(config-if)# switchport mode trunk`	インターフェイス モードを設定します。 **（注）** デフォルト モード（dynamic desirable）のインターフェイスは、セキュア ポートとして設定できません。
ステップ 4	`Switch(config-if)# switchport port-security maximum value vlan`	最大 MAC アドレス制限が明示的に設定されていない VLAN ごとに、最大セキュア MAC アドレス数を設定します（「セキュア MAC アドレスの最大数」（P.35-4）を参照）。
ステップ 5	`Switch(config-if)# vlan-range range`	VLAN 範囲サブモードを開始します。 **（注）** 単一または複数の VLAN を指定できます。
ステップ 6	`Switch(config-if-vlan-range)#` `port-security maximum value`	最大セキュア MAC アドレス数を VLAN ごとに設定します。
ステップ 7	`Switch(config-if-vlan-range)#` `no port-security maximum`	すべての VLAN の最大セキュア MAC アドレス数の設定を削除します。そのあと、ポートに設定された最大値がすべての VLAN で使用されます。
ステップ 8	`Switch(config-if-vlan-range)# [no] port-security mac-address mac_address`	VLAN 範囲にセキュア MAC アドレスを設定します。
ステップ 9	`Switch(config-if-vlan-range)# [no] port-security mac-address sticky mac_address`	VLAN 範囲にスティッキ MAC アドレスを設定します。
ステップ 10	`Switch(config-if-vlan-range)# end`	インターフェイス コンフィギュレーション モードに戻ります。
ステップ 11	`Switch(config-if)# end`	特権 EXEC モードに戻ります。

トランク ポート セキュリティの例

ここでは、次の例を示します。

- 「例 1：すべての VLAN での最大セキュア MAC アドレス制限の設定」（P.35-18）
- 「例 2：特定の VLAN での最大セキュア MAC アドレス制限の設定」（P.35-19）
- 「例 3：VLAN 範囲でのセキュア MAC アドレスの設定」（P.35-19）

例 1：すべての VLAN での最大セキュア MAC アドレス制限の設定

次に、すべての VLAN のインターフェイス g1/1 上でセキュア MAC アドレスおよび最大セキュア MAC アドレス制限を設定する例を示します。

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
```

```
Switch(config)# interface g1/1
Switch(config-if)# switchport trunk encapsulation dot1q
Switch(config-if)# sw mode trunk
Switch(config-if)# switchport port-security
Switch(config-if)# switchport port-security maximum 3

Switch# show port-security in gi1/1 vlan
Default maximum: 3
VLAN  Maximum    Current
    1          3          0
    2          3          0
    3          3          0
    4          3          0
    5          3          0
    6          3          0
Switch#

Switch# show running interface gi1/1
Building configuration...

Current configuration : 161 bytes
!
interface GigabitEthernet1/1
 switchport trunk encapsulation dot1q
 switchport mode trunk
 switchport port-security
 switchport port-security maximum 3 vlan
end
```

例 2：特定の VLAN での最大セキュア MAC アドレス制限の設定

次に、特定の VLAN または VLAN 範囲のインターフェイス g1/1 にセキュア MAC アドレスを設定する例を示します。

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# interface g1/1
Switch(config-if)# switchport trunk encapsulation dot1q
Switch(config-if)# sw mode trunk
Switch(config-if)# switchport port-security
Switch(config-if)# vlan-range 2-6
Switch(config-if-vlan-range)# port-security maximum 3
Switch(config-if)# exit

Switch# show port-security interface g1/1 vlan
Default maximum: not set, using 3072
VLAN  Maximum    Current
   2          3          0
   3          3          0
   4          3          0
   5          3          0
   6          3          0
Switch#
```

例 3：VLAN 範囲でのセキュア MAC アドレスの設定

次に、インターフェイス g1/1 上の VLAN でセキュア MAC アドレスを設定する例を示します。

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# interface g1/1
Switch(config-if)# switchport trunk encapsulation dot1q
```

```
Switch(config-if)# sw mode trunk
Switch(config-if)# switchport port-security
Switch(config-if)# switchport port-security mac-address sticky
Switch(config-if)# vlan-range 2-6
Switch(config-if-vlan-range)# port-security mac-address 1.1.1
Switch(config-if-vlan-range)# port-security mac-address sticky 1.1.2
Switch(config-if-vlan-range)# port-security mac-address sticky 1.1.3
Switch(config-if-vlan-range)# exit
Switch# show port-security interface g1/1 address vlan 2-4
          Secure Mac Address Table
------------------------------------------------------------------------
Vlan    Mac Address       Type                       Ports   Remaining Age
                                                                (mins)
----    -----------       ----                       -----   -------------
  2    0001.0001.0001    SecureConfigured         Gi1/1        -
  2    0001.0001.0002    SecureSticky             Gi1/1        -
  2    0001.0001.0003    SecureSticky             Gi1/1        -
  3    0001.0001.0001    SecureConfigured         Gi1/1        -
  3    0001.0001.0002    SecureSticky             Gi1/1        -
  3    0001.0001.0003    SecureSticky             Gi1/1        -
  4    0001.0001.0001    SecureConfigured         Gi1/1        -
  4    0001.0001.0002    SecureSticky             Gi1/1        -
  4    0001.0001.0003    SecureSticky             Gi1/1        -
------------------------------------------------------------------------
Total Addresses: 9

Switch#
```

トランク ポート セキュリティの注意事項および制約事項

ポート単位/VLAN 単位でポート セキュリティ関連パラメータを設定する場合は、次の注意事項に従ってください。

- セキュア MAC アドレスは、通常のトランク ポートで許容されていない VLAN では設定できません。
- PVLAN トランク上のプライマリ VLAN の設定はできません。CLI は拒否され、エラー メッセージが表示されます。
- ポート上の特定の VLAN で最大値が設定されていない場合（直接的または間接的）、この VLAN にはポートに設定された最大値が使用されます。この場合、この VLAN 上のセキュア アドレスの最大数はポートに設定された最大値に制限されます。

  各 VLAN は、ポートで設定された値よりも大きい最大数を設定できます。また、すべての VLAN に設定される最大値の合計は、ポートに設定される最大値を上回ることができます。いずれの場合でも、各 VLAN のセキュア MAC アドレス数は、VLAN の設定最大値とポートの設定最大値の小さい方の数に制限されます。また、すべての VLAN のポートでのセキュア アドレス数は、ポートに設定された最大数を超えることはできません。
- PVLAN のトランク ポートでは、設定が実行される VLAN は、PVLAN トランクの許容 VLAN リストか、またはアソシエーション ペアのセカンダリ VLAN リスト内にある必要があります（この条件が満たされていない場合、CLI は拒否されます）。PVLAN トランク上の許容 VLAN リストでは、PVLAN トランクで許可されたすべての通常の VLAN の VLAN ID が保持されます。
- PVLAN トランクからアソシエーション ペアを削除すると、ペアのセカンダリ VLAN に関連付けられたすべてのスタティックおよびスティッキ アドレスが実行コンフィギュレーションから削除されます。セカンダリ VLAN に関連付けられているダイナミック アドレスはシステムから削除されます。

同様に、許容された PVLAN トランクのリストから VLAN を削除すると、その VLAN に関連付けられているアドレスが削除されます。

（注）　通常の VLAN または PVLAN のトランク ポートでは、VLAN が許容 VLAN リストから削除されると、その VLAN に関連付けられたすべてのアドレスが削除されます。

ポート モードの変更

一般的にポート モードが変更されると、そのポートに関連付けられたすべてのダイナミック アドレスは削除されます。すべてのスタティックまたはスティッキ アドレス、およびネイティブ VLAN で設定されたその他のポート セキュリティ パラメータは、新しいモードのポートのネイティブ VLAN に移動されます。非ネイティブ VLAN のすべてのアドレスは削除されます。

ネイティブ VLAN とは、次のポート タイプの VLAN です。

ポート タイプ	ネイティブ VLAN
アクセス	アクセス VLAN
トランク	ネイティブ VLAN
独立	セカンダリ VLAN（ホスト アソシエーションから）
無差別	プライマリ VLAN（マッピングから）
PVLAN トランク	PVLAN トランク ネイティブ VLAN
802.1Q トンネル	アクセス VLAN

たとえば、モードがアクセスから PVLAN トランクに変わると、アクセス ポートのアクセス VLAN に設定されているすべてのスタティックおよびスティッキ アドレスは、PVLAN トランク ポートの PVLAN ネイティブ VLAN に移動します。その他のアドレスはすべて削除されます。

同様に、PVLAN トランク モードからアクセス モードに変わると、PVLAN ネイティブ VLAN に設定されているすべてのスタティックおよびスティッキ アドレスは、アクセス ポートのアクセス VLAN に移動します。その他のアドレスはすべて削除されます。

ポートがトランクから PVLAN トランクに変わる場合は、許容されている PVLAN トランクのリストにその VLAN がある場合、または PVLAN トランクで関連付けられているセカンダリ VLAN にある場合は、トランクの VLAN に関連付けられているアドレスはそのまま残ります。VLAN がいずれにもない場合は、実行コンフィギュレーションからアドレスが削除されます。

ポートが PVLAN トランクからトランクに変わる場合は、アドレスに関連付けられている VLAN がトランクの許容 VLAN リストにあれば、スタティックまたはスティッキ アドレスはそのまま残ります。VLAN が許容されているリストにない場合、実行コンフィギュレーションからアドレスが削除されます。

音声ポート上のポート セキュリティ

ポートにデータ VLAN（PC 用）と音声 VLAN（Cisco IP Phone 用）が設定されている場合、IP テレフォニー環境にポート セキュリティを設定できます。

ここでは、音声ポート上にポート セキュリティを設定する方法について説明します。

- 「音声ポート上のポート セキュリティの設定」（P.35-22）

- 「音声ポート セキュリティの例」（P.35-24）
- 「音声ポート セキュリティの注意事項および制約事項」（P.35-26）

音声ポート上のポート セキュリティの設定

音声ポート上でポート セキュリティを設定するには、次の作業を実行します。

	コマンド	目的
ステップ 1	`Switch(config)# 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、設定する物理インターフェイスを指定します。
ステップ 2	`Switch(config-if)# switchport mode access`	インターフェイス モードを設定します。 （注）　デフォルト モード（dynamic desirable）のインターフェイスは、セキュア ポートとして設定できません。
ステップ 3	`Switch(config-if)# [no] switchport port-security`	インターフェイス上でポート セキュリティをイネーブルにします。 インターフェイスをセキュア ポートでないデフォルトの状態に戻すには、**no switchport port-security** コマンドを使用します。
ステップ 4	`Switch(config-if)# [no] switchport port-security violation {restrict | shutdown}`	（任意）違反モードを設定します。セキュリティ違反が発生した場合に、次のいずれかのアクションを実行します。 • **restrict**：ポート セキュリティ違反によりデータが制限され、セキュリティ違反カウンタが増加して、SNMP トラップ通知が送信されます。 • **shutdown**：セキュリティ違反が発生すると、インターフェイスが errdisable になります。 （注）　セキュア ポートが errdisable ステートの場合、**errdisable recovery cause psecure-violation** 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このステートを解除したり、**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 コマンドを入力して手動で再びイネーブルにしたりできます。 違反モードをデフォルト状態（shutdown モード）に戻すには、**no switchport port-security violation shutdown** コマンドを使用します。
ステップ 5	`Switch(config-if)# switchport port-security limit rate invalid-source-mac packets_per_sec`	不良パケットに対してレート制限を設定します。 デフォルトは 10 pps です。

	コマンド	目的 （続き）
ステップ 6	`Switch(config-if)# [no] switchport port-security mac-address mac_address [vlan {voice | access}]`	（任意）インターフェイスのセキュア MAC アドレスを指定します。 **vlan** キーワードを指定すると、指定した VLAN にアドレスが設定されます。 • **voice**：音声 VLAN に MAC アドレスが設定されます。 • **access**：アクセス VLAN に MAC アドレスが設定されます。 このコマンドを使用するとセキュア MAC アドレスが設定できます。設定したセキュア MAC アドレスが最大数より少ない場合、残りの MAC アドレスは動的に学習されます。 MAC アドレスをアドレス テーブルから削除するには、**no switchport port-security mac-address** *mac_address* コマンドを使用します。 **（注）** このコマンドは、アクセス、PVLAN ホスト、および PVLAN 無差別モードに対してのみ適用できます。PVLAN、トランク、または通常のトランク モードの詳細については、「トランク ポートのポート セキュリティ」（P.35-16）を参照してください。
ステップ 7	`Switch(config-if)# [no] switchport port-security mac-address sticky`	（任意）インターフェイスでスティッキー ラーニングをイネーブルにします。 インターフェイス上でスティッキ ラーニングをディセーブルにするには、**no switchport port-security mac-address sticky** コマンドを使用します。インターフェイスがスティッキー セキュア MAC アドレスをダイナミック セキュア アドレスに変換します。

	コマンド	目的 （続き）
ステップ 8	`Switch(config-if)# [no] switchport port-security mac-address mac_address sticky [vlan {voice | access}]`	インターフェイスにスティッキ MAC アドレスを指定します。 **vlan** キーワードを指定すると、指定した VLAN の MAC アドレスがスティッキになります。 • **voice**：音声 VLAN の MAC アドレスがスティッキになります。 • **access**：アクセス VLAN の MAC アドレスがスティッキになります。 アドレス テーブルからスティッキ セキュア MAC アドレスを削除するには、**no switchport port-security mac-address** *mac_address* **sticky** コマンドを使用します。スティッキ アドレスをダイナミック アドレスに変換するには、**no switchport port-security mac-address sticky** コマンドを使用します。 **（注）** このコマンドは、アクセス、PVLAN ホスト、および PVLAN 無差別モードに対してのみ適用できます。PVLAN、トランク、または通常のトランク モードの詳細については、「トランク ポートのポート セキュリティ」（P.35-16）を参照してください。
ステップ 9	`Switch(config-if)# end`	特権 EXEC モードに戻ります。
ステップ 10	`Switch# show port-security address interface interface_id` `Switch# show port-security address`	入力を確認します。

（注） ダイナミックに学習されたポート セキュリティ MAC アドレスを CAM テーブルから削除するには、**clear port-security dynamic** コマンドを使用します。**address** キーワードを指定すると、セキュア MAC アドレスを削除できます。**interface** キーワードを指定すると、インターフェイス上の（ポート チャネル インターフェイスを含む）すべてのセキュア アドレスを削除できます。**VLAN** キーワードにより、VLAN 単位/ポート単位でポート セキュリティ MAC アドレスをクリアできます。

音声ポート セキュリティの例

ここでは、次の例を示します。

- 「例 1：音声 VLAN およびデータ VLAN への最大 MAC アドレスの設定」（P.35-24）
- 「例 2：音声 VLAN およびデータ VLAN へのスティッキ MAC アドレスの設定」（P.35-25）

例 1：音声 VLAN およびデータ VLAN への最大 MAC アドレスの設定

次の例では、ファスト イーサネット インターフェイス 5/1 上で Cisco IP Phone などの音声 VLAN に最大 1 つの MAC アドレスを指定し、PC などのデータ VLAN に 1 つの MAC アドレスを指定して、その設定を確認する方法を示します。

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
```

```
Switch(config)# interface fa5/1
Switch(config-if)# switchport mode access
Switch(config-if)# switchport port-security
Switch(config-if)# switchport port-security mac-address sticky
Switch(config-if)# switchport port-security maximum 1 vlan voice
Switch(config-if)# switchport port-security maximum 1 vlan access
Switch(config-if)# end
```

（注）　ポートにトラフィックを送信すると、ポートにスティッキ セキュア アドレスが設定されます。

```
Switch# show port-security address
          Secure Mac Address Table
------------------------------------------------------------------------
Vlan    Mac Address       Type                      Ports   Remaining Age
                                                              (mins)
----    -----------       ----                      -----   -------------
   1    0000.0000.0001    SecureSticky              Fa5/1         -
   3    0000.0000.0004    SecureSticky              Fa5/1         -
------------------------------------------------------------------------
Total Addresses in System (excluding one mac per port)     : 1
Max Addresses limit in System (excluding one mac per port) : 3072

Switch# show running-config interface fastEthernet 5/1
Building configuration...

Current configuration : 344 bytes
!
interface FastEthernet5/1
 switchport mode access
 switchport voice vlan 3
 switchport port-security
 switchport port-security maximum 1 vlan voice
 switchport port-security maximum 1 vlan access
 switchport port-security mac-address sticky
 switchport port-security mac-address sticky 0000.0000.0001
 switchport port-security mac-address sticky 0000.0000.0004 vlan voice
end

Switch#
```

例 2：音声 VLAN およびデータ VLAN へのスティッキ MAC アドレスの設定

次に、インターフェイス fa5/1 上で音声 VLAN およびデータ VLAN に対してスティッキ MAC アドレスを設定する例を示します。

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# interface fa5/1
Switch(config-if)# switchport mode access
Switch(config-if)# switchport port-security
Switch(config-if)# switchport port-security mac-address sticky 0000.0000.obob vlan voice
Switch(config-if)# switchport port-security mac-address sticky 0000.0000.0005 vlan access
Switch(config-if)# end
```

（注）　ポートにトラフィックを送信すると、ポートにスティッキ セキュア アドレスが設定されます。

```
Switch# show port-security address
          Secure Mac Address Table
------------------------------------------------------------------------
Vlan    Mac Address       Type                      Ports   Remaining Age
                                                              (mins)
----    -----------       ----                      -----   -------------
   1    0000.0000.0001    SecureSticky              Fa5/1        -
   1    0000.0000.0002    SecureSticky              Fa5/1        -
   1    0000.0000.0003    SecureSticky              Fa5/1        -
   3    0000.0000.0004    SecureSticky              Fa5/1        -
   1    0000.0000.0005    SecureSticky              Fa5/1        -
   3    0000.0000.0b0b    SecureSticky              Fa5/1        -
------------------------------------------------------------------------
Total Addresses in System (excluding one mac per port)     : 5
Max Addresses limit in System (excluding one mac per port) : 3072

Switch# show running-config interface fastEthernet 5/1
Building configuration...

Current configuration : 344 bytes
!
interface FastEthernet5/1
 switchport mode access
 switchport voice vlan 3
 switchport port-security
 switchport port-security maximum 5 vlan voice
 switchport port-security mac-address sticky
 switchport port-security mac-address sticky 0000.0000.0001
 switchport port-security mac-address sticky 0000.0000.0002
 switchport port-security mac-address sticky 0000.0000.0003
 switchport port-security mac-address sticky 0000.0000.0004 vlan voice
 switchport port-security mac-address sticky 0000.0000.0005
 switchport port-security mac-address sticky 0000.0000.0b0b vlan voice
end

Switch#
```

音声ポート セキュリティの注意事項および制約事項

音声ポートに実装されたポート セキュリティの動作は、アクセス ポート上のポート セキュリティと同じです。

- 音声ポートにスティッキ ポート セキュリティを設定できます。音声ポートのスティッキ ポート セキュリティがイネーブルの場合、データ VLAN および音声 VLAN 上でセキュアなアドレスはスティッキ アドレスとしてセキュアです。
- 最大セキュア アドレスは VLAN 単位で設定できます。最大数は、データ VLAN または音声 VLAN のいずれかに設定できます。また、アクセス ポートの場合と同様、ポート単位でも設定できます。
- ポート セキュリティ MAC アドレスは、データ VLAN または音声 VLAN 上で VLAN 単位で設定できます。
- Cisco IOS Release 12.2(31)SG よりも前のリリースでは、IP Phone と PC をサポートするために 3 つの MAC アドレスが最大パラメータとして必要でした。Cisco IOS Release 12.2(31)SG 以降のリリースでは、最大数パラメータは 2（IP Phone と PC に 1 つずつ）に設定する必要があります。

ポート セキュリティ設定の表示

show port-security コマンドを使用すると、インターフェイスまたはスイッチのポート セキュリティ設定が表示されます。

トラフィック制御情報を表示するには、次の作業を 1 つまたは複数行います。

コマンド	目的
`Switch# show interface status err-disable`	errdisable となったインターフェイスを、ディセーブルの理由とともに表示します。
`Switch# show port-security [interface interface_id | interface port_channel port_channel_number]`	スイッチまたは指定されたインターフェイスのポート セキュリティ設定を、各インターフェイスで許容されるセキュア MAC アドレスの最大数、インターフェイスのセキュア MAC アドレスの数、発生したセキュリティ違反の数、違反モードを含めて表示します。 ポート チャネル論理インターフェイスを指定することができます。
`Switch# show port-security [interface interface_id | interface port_channel port_channel_number] address`	すべてのスイッチ インターフェイスまたは指定されたインターフェイスに設定されたすべてのセキュア MAC アドレス、および各アドレスのエージング情報を表示します。
`Switch# show port-security [interface interface_id | interface port_channel port_channel_number] vlan vlan_list`	特定の VLAN リストおよび特定のインターフェイス上で、許容される最大セキュア MAC アドレス数および現在のセキュア MAC アドレス数を表示します。
`Switch# show port-security [interface interface_id | interface port_channel port_channel_number] [address [vlan vlan_list]]`	特定の VLAN リストおよび特定のインターフェイスで設定されたすべてのセキュア MAC アドレスを表示します。

例

ここでは、次の例を示します。

- 「例 1：スイッチ全体のセキュリティ設定の表示」（P.35-28）
- 「例 2：インターフェイスのセキュリティ設定の表示」（P.35-28）
- 「例 3：スイッチ全体のすべてのセキュア アドレスの表示」（P.35-28）
- 「例 4：インターフェイス上の最大 MAC アドレス数の表示」（P.35-29）
- 「例 5：VLAN 範囲に対するインターフェイス上のセキュリティ設定の表示」（P.35-29）
- 「例 6：インターフェイスのセキュア MAC アドレスおよびエージング情報の表示」（P.35-29）
- 「例 7：インターフェイスの VLAN 範囲でのセキュア MAC アドレスの表示」（P.35-30）

例 1：スイッチ全体のセキュリティ設定の表示

次に、スイッチ全体のポート セキュリティの設定を表示する例を示します。

```
Switch# show port-security
Secure Port  MaxSecureAddr  CurrentAddr  SecurityViolation  Security Action
               (Count)       (Count)          (Count)
-----------------------------------------------------------------------------
      Fa3/1              2            2                  0         Restrict
      Fa3/2              2            2                  0         Restrict
      Fa3/3              2            2                  0         Shutdown
      Fa3/4              2            2                  0         Shutdown
      Fa3/5              2            2                  0         Shutdown
      Fa3/6              2            2                  0         Shutdown
      Fa3/7              2            2                  0         Shutdown
      Fa3/8              2            2                  0         Shutdown
     Fa3/10              1            0                  0         Shutdown
     Fa3/11              1            0                  0         Shutdown
     Fa3/12              1            0                  0         Restrict
     Fa3/13              1            0                  0         Shutdown
     Fa3/14              1            0                  0         Shutdown
     Fa3/15              1            0                  0         Shutdown
     Fa3/16              1            0                  0         Shutdown
        Po2              3            0                  0         Shutdown
-----------------------------------------------------------------------------
Total Addresses in System (excluding one mac per port)     :8
Max Addresses limit in System (excluding one mac per port) :3072
Global SNMP trap control for port-security                 :20 (traps per second)
```

例 2：インターフェイスのセキュリティ設定の表示

次に、ファスト イーサネット インターフェイス 5/1 のポート セキュリティの設定を表示する例を示します。

```
Switch# show port-security interface fastethernet 5/1
Port Security              : Enabled
Port Status                : Secure-up
Violation Mode             : Shutdown
Aging Time                 : 0 mins
Aging Type                 : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses      : 1
Total MAC Addresses        : 1
Configured MAC Addresses   : 0
Sticky MAC Addresses       : 1
Last Source Address:Vlan   : 0000.0001.001a:1
Security Violation Count   : 0
```

例 3：スイッチ全体のすべてのセキュア アドレスの表示

次に、スイッチのすべてのインターフェイスで設定されたすべてのセキュア MAC アドレスを表示する例を示します。

```
Switch# show port-security address
          Secure Mac Address Table
------------------------------------------------------------------------
Vlan    Mac Address       Type                Ports   Remaining Age
                                                        (mins)
----    -----------       ----                -----   -------------
   1    0000.0001.0000    SecureConfigured    Fa3/1       15 (I)
   1    0000.0001.0001    SecureConfigured    Fa3/1       14 (I)
   1    0000.0001.0100    SecureConfigured    Fa3/2        -
   1    0000.0001.0101    SecureConfigured    Fa3/2        -
```

```
   1    0000.0001.0200    SecureConfigured    Fa3/3        -
   1    0000.0001.0201    SecureConfigured    Fa3/3        -
   1    0000.0001.0300    SecureConfigured    Fa3/4        -
   1    0000.0001.0301    SecureConfigured    Fa3/4        -
   1    0000.0001.1000    SecureDynamic    Fa3/5        -
   1    0000.0001.1001    SecureDynamic    Fa3/5        -
   1    0000.0001.1100    SecureDynamic    Fa3/6        -
   1    0000.0001.1101    SecureDynamic    Fa3/6        -
   1    0000.0001.1200    SecureSticky    Fa3/7        -
   1    0000.0001.1201    SecureSticky    Fa3/7        -
   1    0000.0001.1300    SecureSticky    Fa3/8        -
   1    0000.0001.1301    SecureSticky    Fa3/8        -
   1    0000.0001.2000    SecureSticky    Po2        -
------------------------------------------------------------------
Total Addresses in System (excluding one mac per port)     :8
Max Addresses limit in System (excluding one mac per port) :3072
```

例 4：インターフェイス上の最大 MAC アドレス数の表示

次に、インターフェイス g1/1 上で許容される最大セキュア MAC アドレス数および現在のセキュア MAC アドレス数を表示する例を示します。

```
Switch# show port-security interface g1/1 vlan
Default maximum: 22
VLAN  Maximum    Current
2         22          3
3         22          3
4         22          3
5         22          1
6         22          2
```

例 5：VLAN 範囲に対するインターフェイス上のセキュリティ設定の表示

次に、VLAN 2 および VLAN 3 のインターフェイス g1/1 上のポート セキュリティの設定を表示する例を示します。

```
Switch# show port-security interface g1/1 vlan 2-3
Default maximum: 22
VLAN  Maximum    Current
    2         22          3
    3         22          3
```

例 6：インターフェイスのセキュア MAC アドレスおよびエージング情報の表示

次に、ギガビット イーサネット インターフェイス 1/1 上で設定されたすべてのセキュア MAC アドレスおよび各アドレスのエージング情報を表示する例を示します。

```
Switch# show port-security interface g1/1 address

          Secure Mac Address Table
------------------------------------------------------------------------
Vlan    Mac Address       Type                    Ports   Remaining Age(mins)
----    -----------                ----                        -----   -------------
   2    0001.0001.0001    SecureConfigured        Gi1/1       -
   2    0001.0001.0002    SecureSticky               Gi1/1        -
   2    0001.0001.0003    SecureSticky               Gi1/1        -
   3    0001.0001.0001    SecureConfigured        Gi1/1       -
   3    0001.0001.0002    SecureSticky               Gi1/1        -
   3    0001.0001.0003    SecureSticky               Gi1/1        -
```

```
   4    0001.0001.0001    SecureConfigured         Gi1/1        -
   4    0001.0001.0002    SecureSticky             Gi1/1        -
   4    0001.0001.0003    SecureSticky             Gi1/1        -
   5    0001.0001.0001    SecureConfigured         Gi1/1        -
   6    0001.0001.0001    SecureConfigured         Gi1/1        -
   6    0001.0001.0002    SecureConfigured         Gi1/1        -
-----------------------------------------------------------------------
Total Addresses: 12
```

例 7：インターフェイスの VLAN 範囲でのセキュア MAC アドレスの表示

次に、ギガビット イーサネット インターフェイス 1/1 の VLAN 2 および VLAN 3 上で設定されたすべてのセキュア MAC アドレスおよび各アドレスのエージング情報を表示する例を示します。

```
Switch# show port-security interface g1/1 address vlan 2-3

          Secure Mac Address Table
-----------------------------------------------------------------------
Vlan    Mac Address       Type                      Ports   Remaining Age(mins)
----    -----------       ----                      -----   -------------
   2    0001.0001.0001    SecureConfigured          Gi1/1        -
   2    0001.0001.0002    SecureSticky              Gi1/1        -
   2    0001.0001.0003    SecureSticky              Gi1/1        -
   3    0001.0001.0001    SecureConfigured          Gi1/1        -
   3    0001.0001.0002    SecureSticky              Gi1/1        -
   3    0001.0001.0003    SecureSticky              Gi1/1        -
-----------------------------------------------------------------------
Total Addresses: 12
Switch#
```

他の機能/環境でのポート セキュリティの設定

ここでは、次の内容について説明します。

DHCP および IP ソース ガード

DHCP および IP ソース ガードを使用してポート セキュリティを設定し、セキュアではない MAC アドレスによる IP スプーフィングを防ぐことができます。IP ソース ガードは次の 2 つのレベルの IP トラフィック フィルタリングをサポートします。

- 送信元 IP アドレス フィルタリング
- 送信元 IP および MAC アドレス フィルタリング

IP ソース ガードをソース IP および MAC アドレス フィルタリングで使用する場合、送信元 IP アドレスに基づいてトラフィックをフィルタリングする場合はプライベート ACL（アクセス コントロール リスト）が、送信元 MAC アドレスに基づいてトラフィックをフィルタリングする場合はポート セキュリティが使用されます。このため、このモードではアクセス ポートのポート セキュリティをイネーブルにする必要があります。

両方の機能がイネーブルの場合の制約事項は次のとおりです。

- DHCP パケットは、ポート セキュリティのダイナミック学習の対象になりません。
- 複数の IP クライアントが 1 つのアクセス ポートに接続されている場合、ポート セキュリティでは各クライアントの送信元 IP アドレスと MAC アドレスを正確にバインディングすることはできません。

  たとえば、クライアントが次の IP/MAC アドレスのアクセス ポートに存在するとします。

  - クライアント 1 : MAC1 <---> IP1
  - クライアント 2 : MAC2 <---> IP2

  この場合、トラフィックの送信元 MAC アドレスと IP アドレス トラフィックの組み合わせは、次のいずれも許容されます。

  - MAC1 <---> IP1、有効
  - MAC2 <---> IP2、有効
  - MAC1 <---> IP2、無効
  - MAC2 <---> IP1、無効

  送信元 IP/MAC アドレス バインディングが正しい IP トラフィックだけが許可され、ポート セキュリティはこのトラフィックの MAC アドレスをダイナミックに学習します。バインディングされていない送信元アドレスの IP トラフィックは、ポート セキュリティによって無効なパケットとして処理され、ドロップされます。DoS 攻撃（サービス拒絶攻撃）を防ぐには、無効な送信元 MAC アドレスに対してポート セキュリティ レート制限を設定する必要があります。

802.1X 認証

MAC スプーフィングを防ぐために、802.1X 認証を使用したポート セキュリティを設定できます。802.1X は、通常の VLAN トランクおよび PVLAN トランクではサポートされません。アクセス ポート、および PVLAN ホストまたは無差別ポートでは、ポート セキュリティと 802.1X を同時に設定できます。両方とも設定する場合、ホストが 802.1X 認証されたあとでポート セキュリティによってホストの MAC アドレスをセキュアにする必要があります。802.1X とポート セキュリティの両方がホストを承認する必要があります。一方がホストを認証しない場合、セキュリティ違反がトリガーされます。セキュリティ違反の種類は、ポートを拒否する機能がどちらであるかによって異なります。ホストが 802.1X では許可されても（たとえばポートがマルチ ホスト モードであるため）ポート セキュリティでは許可されない場合、ポートセキュリティ違反アクションがトリガーされます。ホストがポート セキュリティでは許可されても 802.1X では拒否される場合（たとえば、ホストがシングル ホスト モード ポートでは未許可であるため）、802.1X セキュリティ違反アクションがトリガーされます。

（注） 802.1X、ポートセキュリティ、および VVID は、すべて同じポートに設定できます。

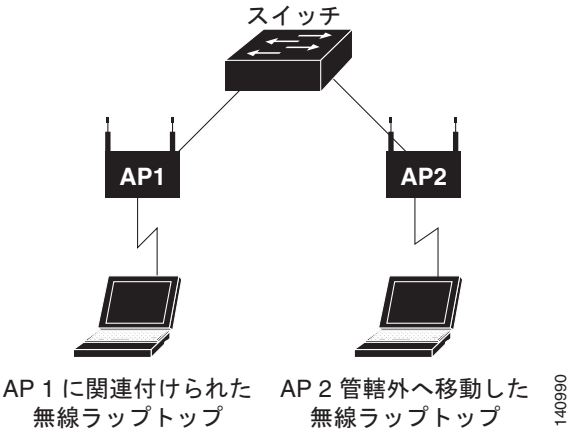
802.1X とポート セキュリティの相互作用の詳細については、次を参照してください。
「ポート セキュリティを使用した 802.1X 認証の利用」（P.14）。

ワイヤレス環境でのポート セキュリティの設定

アクセス ポイントをセキュア ポートに接続する場合、ユーザのスタティック MAC アドレスを設定しないでください。MAC アドレスは 1 つのアクセス ポイントから別のアクセス ポイントに移動することがあり、両方のアクセス ポイントが同じスイッチに接続されるとセキュリティ違反になります。

図 35-3 に、ワイヤレス環境でのポート セキュリティの代表的なトポロジを示します。

図 35-3　　ワイヤレス環境でのポート セキュリティ



レイヤ 2 EtherChannel でのポート セキュリティの設定

（注）　Supervisor Engine 6-E は、この機能をサポートしていません。

ポート セキュリティは、トランク モードまたはアクセス モードのいずれかの EtherChannel でイネーブルにできます （設定手順については、「アクセス ポート上のポート セキュリティ」（P.35-7）および「トランク ポートのポート セキュリティ」（P.35-16）を参照してください）。トランキング モードで設定するときは、MAC アドレスの制限が、VLAN 単位でポート チャネル全体に適用されます。

一般的に、次の点に注意してください。

- レイヤ 2 EtherChannel でのポート セキュリティはアクセス モードまたはトランク モード上でだけ有効で、物理メンバ ポートでの設定からは独立しています。
- 少なくともメンバ ポートが 1 つセキュアであれば、チャネル インターフェイスのポート セキュリティはディセーブルにできず、CLI によって拒否されます。
- セキュア ポートは非セキュア EtherChannel に加入できません。CLI によって拒否されます。
- EtherChannel でのポート セキュリティは、PAgP モードと LACP モードの両方でサポートされています。レイヤ 3 EtherChannel には適用されません。

ポートセキュリティに関する注意事項および制約事項

ポート セキュリティを設定するときには、次の注意事項に従ってください。

- セキュア ポートをスイッチド ポート アナライザ（SPAN）の宛先ポートにすることはできません。
- インターフェイスのセキュア ポートおよびスタティック MAC アドレス設定は、相互に排他的です。

- インターフェイスの最大セキュア アドレス値を入力したときに、新しい値がそれまでの値より大きいと、それまで設定されていた値が新しい値によって上書きされます。新しい値が前回の値より小さく、インターフェイスで設定されているセキュア アドレス数が新しい値より大きい場合、コマンドは拒否されます。
- トランク ポートでトランク ポート セキュリティを設定しているときは、プロトコル パケット（CDP や BPDU）を考慮する必要はありません。これらは学習されることも、セキュアにされることもありません。
- スティッキ セキュア MAC アドレスのポート セキュリティ エージングはイネーブルにできません。
- ポート セキュリティを使用して MAC スプーフィングを制限するには、802.1X 認証をイネーブルにする必要があります。
- ダイナミック ポートにはポート セキュリティを設定できません。ポート セキュリティをイネーブルにする前にモードをアクセスに変更する必要があります。
- EtherChannel のポート セキュリティがイネーブルの場合、802.1X はイネーブルにすることはできません。
- セキュア EtherChannel は PVLAN モードでは動作しません。