



CHAPTER 48

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 (PVLAN) など各種ポートの設定について説明します。

この章で説明する内容は、次のとおりです。

- 「ポート セキュリティ コマンド」 (P.48-2)
- 「ポート セキュリティの概要」 (P.48-3)
- 「アクセス ポート上のポート セキュリティの設定」 (P.48-7)
- 「PVLAN ポート上のポート セキュリティの設定」 (P.48-14)
- 「トランク ポート上のポート セキュリティの設定」 (P.48-17)
- 「音声ポート上のポート セキュリティの設定」 (P.48-22)
- 「ポート セキュリティ設定の表示」 (P.48-28)
- 「他の機能/環境でのポート セキュリティの設定」 (P.48-31)
- 「ポート セキュリティ設定の注意事項および制約事項」 (P.48-33)



(注)

この章で使用するスイッチ コマンドの構文および使用方法の詳細については、次の URL で『Cisco Catalyst 4500 Series Switch Command Reference』と関連資料を参照してください。

<http://www.cisco.com/en/US/products/hw/switches/ps4324/index.html>

『Catalyst 4500 Series Switch Command Reference』に掲載されていないコマンドについては、より詳細な Cisco IOS ライブラリを参照してください。次の URL で『Cisco IOS Command Reference』と関連資料を参照してください。

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

ポートセキュリティコマンド

この表には、主にポートセキュリティでよく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
<code>errdisable recovery cause psecure-violation</code>	セキュアポートの <code>errdisable</code> ステータスを解除します。	「違反処理」(P.48-6)
<code>errdisable recovery interval</code>	指定した <code>errdisable</code> 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.48-6)
<code>port-security mac-address</code>	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.48-4)
<code>port-security maximum</code>	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.48-7)
<code>private-vlan association add</code>	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.48-16)
<code>private-vlan isolated</code>	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.48-14)
<code>private-vlan primary</code>	VLAN をプライマリ 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.48-14)
<code>switchport mode private-vlan host</code>	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.48-14)
<code>switchport private-vlan host-association</code>	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.48-14)
<code>switchport private-vlan mapping</code>	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.48-14)
<code>switchport port-security</code>	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.48-7)
<code>switchport port-security aging static</code>	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.48-5)
<code>switchport port-security aging time</code>	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.48-11)
<code>switchport port-security limit rate invalid-source-mac</code>	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.48-13)
<code>switchport port-security mac-address</code>	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.48-12)
<code>switchport port-security mac-address mac_address sticky</code>	インターフェイスに対してスティック 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.48-7)
<code>switchport port-security mac-address sticky</code>	スティックポートセキュリティをイネーブルにします。	「ポートのスティックアドレス」(P.48-5)

コマンド	目的	ナビゲーション
<code>no switchport port-security mac-address sticky</code>	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.48-7)
<code>switchport port-security maximum</code>	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.48-11)
<code>switchport port-security violation</code>	違反モードを設定します。	「例 2 : 違反モードの設定」(P.48-11)
<code>no switchport port-security violation</code>	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.48-7)
<code>switchport trunk encapsulation dot1q</code>	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.48-19)

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。
- スティック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.48-4)
- 「セキュア MAC アドレスの最大数」(P.48-4)
- 「セキュア MAC アドレスのエージング」(P.48-5)
- 「ポートのスティッキ アドレス」(P.48-5)
- 「違反処理」(P.48-6)

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 アドレスなどのように学習されますが、スタティックセキュア MAC アドレスなどのように、スイッチのリブートおよびリンクフラップを通じて維持されます。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、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せん。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せんが、ポート VLAN の最大数よりも少な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（たとえば、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設定の注意事項および制約事項」（P.33）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) スティック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（スティック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。

ポートのスティックアドレス

スティック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クセキュア 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。

スティック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ク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クセキュア 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。
- **shutdown vlan** (シャットダウン VLAN) : 各 VLAN に対するセキュリティ違反モードを設定する場合に使用します。このモードで違反が発生すると、ポート全体ではなく、問題になっている VLAN が **errdisable** になります。

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。これがデフォルトのモードです。ポートが VLAN 単位で **errdisable** モードの場合、**clear errdisable interface name vlan range** コマンドを使用すると、ポート上の VLAN を再度イネーブルにすることもできます。

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います。

ポートセキュリティ機能は次のパケットを「無効なフレーム」と見なします。

- すべてゼロである送信元または宛先 MAC アドレスを持つパケット
- マルチキャストまたはブロードキャストの送信元 MAC アドレスを持つパケット
- 同じ VLAN 内の別のセキュア インターフェイスでモニタされるセキュア インターフェイスで学習されたかまたは設定されているアドレスからのパケット

これらのパケットのレート制限を選択できます。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の設定

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。

- 「アクセス ポート上のポートセキュリティの設定」(P.48-7)
- 「アクセス ポートでのポートセキュリティの例」(P.48-10)



(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せん。EtherChannel のポートセキュリティ設定は、メンバ ポートの設定に依存しません。

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 auto) 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。

コマンド	目的
ステップ 4 Switch(config-if)# [no] switchport port-security maximum value	<p>(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。</p> <p>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。</p>
ステップ 5 Switch(config-if)# switchport port-security [aging {static time aging_time type {absolute inactivity}}	<p>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。</p> <p>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。</p> <p>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。</p> <p>time aging_time 値は、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 ~ 1440 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。</p> <p>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。</p> <ul style="list-style-type: none"> • 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。 <p>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。</p>

コマンド	目的
ステップ6 Switch(config-if)# [no] switchport port-security violation {restrict shutdown shutdown vlan}	<p>(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。</p> <ul style="list-style-type: none"> • 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。 • shutdown vlan : 各 VLAN に対するセキュリティ違反モードを設定する場合に使用します。このモードでは違反が発生した際に、ポート全体ではなく、対象の VLAN が errdisable になります。 <p>(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。</p> <p>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。</p>
ステップ7 Switch(config-if)# switchport port-security limit rate invalid-source-mac <i>packets_per_sec</i>	<p>不良パケットに対してレート制限を設定します。</p> <p>デフォルトは 10 pps です。</p>
ステップ8 Switch(config-if)# [no] switchport port-security mac-address <i>mac_address</i>	<p>(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。</p> <p>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 <i>mac_address</i> コマンドを使用します。</p> <p>(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 ポート上のポートセキュリティの設定」(P.48-17) を参照してください。</p>
ステップ9 Switch(config-if)# [no] switchport port-security mac-address sticky	<p>(任意) インターフェイス上でスティッキ ラーニングをイネーブルにします。</p> <p>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 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。</p>

コマンド	目的
ステップ 10 Switch(config-if)# [no] switchport port-security mac-address mac_address sticky [vlan [voice access]]	<p>インターフェイスにスティック MAC アドレスを指定します。</p> <p>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クになります。</p> <p>アドレステーブルからスティックセキュア 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。スティック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。</p> <p>(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、「トランクポート上のポートセキュリティの設定」(P.48-17)を参照してください。</p>
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)

動的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。

アクセスポートでの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：最大セキュアアドレス数の設定](#)」(P.48-11)
- 「[例 2：違反モードの設定](#)」(P.48-11)
- 「[例 3：エージングタイマーの設定](#)」(P.48-11)
- 「[例 4：エージングタイマーのタイプの設定](#)」(P.48-12)
- 「[例 5：セキュア MAC アドレスの設定](#)」(P.48-12)
- 「[例 6：スティックポートセキュリティの設定](#)」(P.48-13)
- 「[例 7：不良パケットに対するレート制限の設定](#)」(P.48-13)
- 「[例 8：ダイナミックセキュア MAC アドレスの削除](#)」(P.48-14)

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 : スティック 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 にスティック 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、ポートにスティック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
```

PVLAN ポート上のポートセキュリティの設定

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一設定モデルを使用します。

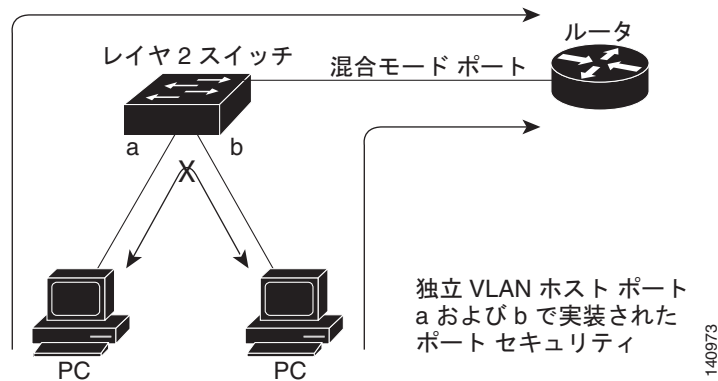
ここでは、ホストと無差別ポート上でトランクポートセキュリティを設定する方法を説明します。

- 「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.48-14)
- 「独立 PVLAN ホストポートでのポートセキュリティの例」(P.48-16)
- 「PVLAN 無差別ポートでのポートセキュリティの設定」(P.48-16)
- 「PVLAN 無差別モードポートでのポートセキュリティの例」(P.48-17)

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 48-1 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、スイッチの無差別ポートを使用して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 48-1 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# <code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ2 Switch(config)# <code>vlan sec_vlan_id</code>	セカンダリ VLAN を指定します。
ステップ3 Switch(config-vlan)# <code>private-vlan isolated</code>	PVLAN モードを <code>isolated</code> に設定します。
ステップ4 Switch(config-vlan)# <code>exit</code>	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)# <code>vlan pri_vlan_id</code>	プライマリ VLAN を指定します。
ステップ6 Switch(config-vlan)# <code>private-vlan primary</code>	VLAN をプライマリ PVLAN として指定します。
ステップ7 Switch(config-vlan)# <code>private-vlan association add sec_vlan_id</code>	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)# <code>exit</code>	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)# <code>interface interface_id</code>	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)# <code>switchport mode private-vlan host</code>	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)# <code>switchport private-vlan host-association primary_vlan secondary_vlan</code>	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)# <code>[no] switchport port-security</code>	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。
ステップ13 Switch(config-if)# <code>end</code>	特権 EXEC モードに戻ります。
ステップ14 Switch# <code>show port-security address interface interface_id</code> Switch# <code>show port-security address</code>	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。
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 ポート上のポートセキュリティの設定

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ー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。

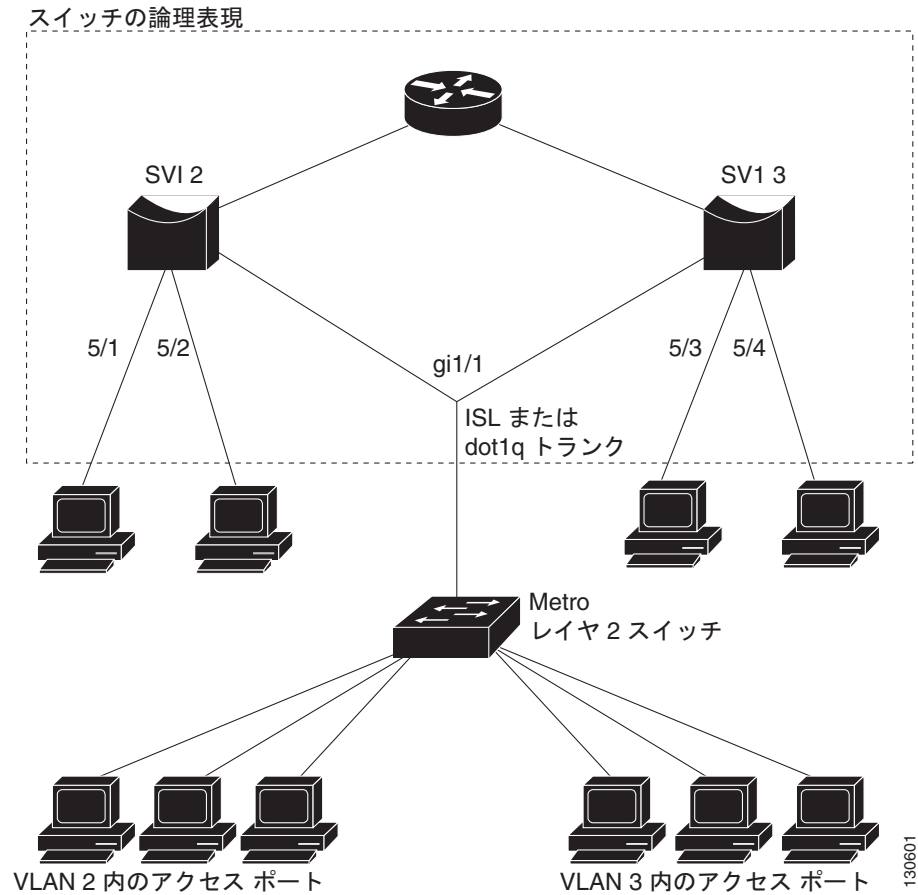
ここでは、トランク ポートセキュリティを設定する方法について説明します。

- 「トランク ポートセキュリティの設定」(P.48-17)
- 「トランク ポートセキュリティの例」(P.48-19)
- 「トランク ポートセキュリティ設定の注意事項および制約事項」(P.48-21)

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 48-2) で使用されます。

図 48-2 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 <i>interface_id</i> interface <i>port-channel port_channel_number</i>	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 チャン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 auto) 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。

	コマンド	目的
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.48-4)を参照してください。
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 範囲にスティッキー 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.48-19)
- 「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.48-20)
- 「例 3 : VLAN 範囲でのセキュア MAC アドレスの設定」(P.48-20)

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 g1/1 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#
```

■ トランク ポート上のポートセキュリティの設定

```
Switch# show running interface g1/1
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 セキュリティ設定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、次の注意事項および制約事項を考慮してください。

- 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ク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 がある場合は、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の設定

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 Phone 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.48-23)
- 「音声ポートセキュリティの例」 (P.48-25)
- 「音声ポートセキュリティ設定の注意事項および制約事項」 (P.48-27)

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 <i>interface_id</i>	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 auto) 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。 <ul style="list-style-type: none"> • 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の状態 (シャットダウン 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 <i>packets_per_sec</i>	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
ステップ6 Switch(config-if)# [no] switchport port-security mac-address mac_address [vlan {voice access}]	<p>(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。</p> <p>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。</p> <ul style="list-style-type: none"> • 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。 <p>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。</p> <p>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。</p> <p>(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 ポート上のポートセキュリティの設定」(P.48-17) を参照してください。</p>
ステップ7 Switch(config-if)# [no] switchport port-security mac-address sticky	<p>(任意) インターフェイス上でスティック ラーニングをイネーブルにします。</p> <p>インターフェイス上でスティック 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ク 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。</p>

コマンド	目的
ステップ8 Switch(config-if)# [no] switchport port-security mac-address mac_address sticky [vlan {voice access}]	<p>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。</p> <p>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。</p> <ul style="list-style-type: none"> • 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。 <p>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。</p> <p>(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せん。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 ポート上のポートセキュリティの設定」(P.48-17) を参照してください。</p>
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 (ポートチャンネル 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。



(注) ポートセキュリティを設定した各インターフェイスは、デフォルトで 1 つの MAC アドレスを受け入れます。ポートセキュリティでは、ポート レベルのポートセキュリティ設定が VLAN レベルのポートセキュリティ設定よりも優先されます。1 つの MAC アドレスをそれぞれ音声 VLAN およびデータ VLAN で許可するために、最大 2 アドレス以上にポートを設定します。

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.48-26)
- 「[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.48-26)

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 と PC などのデータ VLAN に MAC アドレスをそれぞれ最大 1 つ設定して、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 maximum 2
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 3072
 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 maximum 3072
```

```
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 3072
 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設定の注意事項および制約事項



(注) 音声ポートに実装されたポートセキュリティの機能は、アクセスポート上のポートセキュリティと同じです。

音声ポートセキュリティを使用（または設定）するときは、次の注意事項および制約事項を考慮してください。

- 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# <code>show interface status err-disable</code>	<code>errdisable</code> 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# <code>show port-security [interface interface_id interface port_channel port_channel_number]</code>	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# <code>show port-security [interface interface_id interface port_channel port_channel_number] address</code>	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# <code>show port-security [interface interface_id interface port_channel port_channel_number] vlan vlan_list</code>	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# <code>show port-security [interface interface_id interface port_channel port_channel_number] [address [vlan vlan_list]]</code>	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。

セキュリティ設定の例

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.48-29)
- 「例 2 : インターフェイスのセキュリティ設定の表示」 (P.48-29)
- 「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.48-29)
- 「例 4 : インターフェイス上の最大 MAC アドレス数の表示」 (P.48-30)
- 「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.48-30)
- 「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.48-30)

- 「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.48-31)

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)
```

■ ポートセキュリティ設定の表示

```

-----
      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、各アドレスのエージング情報とともにギガビットイーサネットインターフェイス 1/1 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 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、各アドレスのエージング情報とともにギガビットイーサネットインターフェイス 1/1 および VLAN 2 と 3 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 interface gi1/1 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](#)」(P.48-31)
- 「[802.1X 認証](#)」(P.48-32)
- 「[ワイヤレス環境でのポートセキュリティの設定](#)」(P.48-33)

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、これらのクライアントは次の IP アドレスと MAC アドレスを持つアクセス ポートに存在します。

- クライアント 1 : MAC1 <---> IP1
- クライアント 2:MAC2 <---> IP2e b ここで示すように送信元 MAC アドレスと IP アドレストラフィックの任意の組み合わせが許可されます。
- 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処理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 セキュリティ違反処理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。

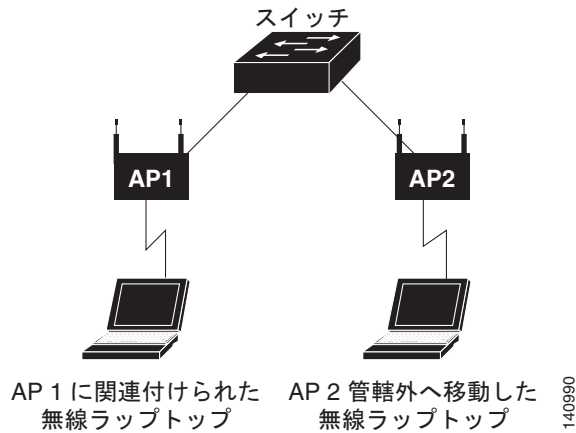
802.1X とポートセキュリティの相互作用の詳細については、「ポートセキュリティを使用した 802.1X 認証の利用」(P.19) を参照してください。

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 48-3 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 48-3 ワイヤレス環境でのポートセキュリティ



ポートセキュリティ設定の注意事項および制約事項

ポートセキュリティを使用（または設定）するときは、次の注意事項および制約事項を考慮してください。

- ポートセキュリティが PACL の「拒否」とともにポート上で設定されると、CPU は特定のポートから拒否された PACL パケットのいずれも表示せず、また拒否されたパケットの送信元 MAC アドレスを学習することはありません。したがって、ポートセキュリティ機能は、このようなパケットを認識しません。
- 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するときは、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。
- スティックセキュア 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 でのポートセキュリティはサポートされていません。

