



## CHAPTER 24

# ポートベースのトラフィック制御の設定

この章では、スイッチにポートベースのトラフィック制御機能を設定する方法について説明します。



(注)

この章で使用するコマンドの構文および使用方法の詳細については、このリリースに対応するコマンドリファレンスを参照してください。

この章で説明する内容は、次のとおりです。

- 「ストーム制御の設定」(P.24-1)
- 「保護ポートの設定」(P.24-6)
- 「ポートブロッキングの設定」(P.24-8)
- 「ポートセキュリティの設定」(P.24-9)
- 「ポートベースのトラフィック制御の設定」(P.24-21)

## ストーム制御の設定

ここでは、次の概念および設定情報について説明します。

- 「ストーム制御の概要」(P.24-1)
- 「ストーム制御のデフォルト設定」(P.24-3)
- 「ストーム制御およびしきい値レベルの設定」(P.24-3)
- 「スモールフレーム着信レートの設定」(P.24-5)

## ストーム制御の概要

ストーム制御は、物理インターフェイスの1つで発生したブロードキャスト、マルチキャスト、またはユニキャストストームによってLAN上のトラフィックが混乱することを防ぎます。LANストームは、LANにパケットがフラッディングした場合に発生します。その結果、トラフィックが極端に増えてネットワークパフォーマンスが低下します。ストームは、プロトコルスタック実装でのエラー、ネットワーク設定の誤り、およびDenial-of-Service (DoS; サービス拒絶) 攻撃を行うユーザにより引き起こされる可能性があります。

ストーム制御（またはトラフィック抑制）はインターフェイスからスイッチングバスへ流れるパケットを監視し、そのパケットがユニキャスト、マルチキャスト、ブロードキャストのいずれであるかを判別します。スイッチは、1秒のタイムインターバル内に受信される、指定されたタイプのパケット数をカウントして、事前に定義された抑制レベルのしきい値と比較します。

ストーム制御は、次のうちのいずれかをトラフィック アクティビティの測定方法に使用します。

- 帯域幅（ブロードキャスト、マルチキャスト、またはユニキャスト トラフィックが使用できるポートの総帯域幅の割合）
- ブロードキャスト、マルチキャスト、またはユニキャスト パケットが受信される、1 秒あたりのパケット単位のトラフィック レート
- ブロードキャスト、マルチキャスト、またはユニキャスト パケットが受信される、1 秒あたりのビット単位のトラフィック レート
- スモール フレーム用の 1 秒あたりのパケット単位でのトラフィック レート。この機能は、グローバルにイネーブルです。スモール フレームのしきい値は、インターフェイスごとに設定されます（Cisco IOS リリース 12.2(44)SE 以降）。

上記の方法のいずれを使用しても、しきい値に到達すると、ポートはトラフィックをブロックします。トラフィック レートが下限しきい値（指定されている場合）を下回らない限り、ポートはブロックされたままになり、その後、通常の転送が再開されます。下限抑制レベルが指定されていない場合、トラフィック レートが上限抑制レベルを下回らない限り、スイッチはすべてのトラフィックをブロックします。一般に、そのレベルが高ければ高いほど、ブロードキャスト ストームに対する保護効果は薄くなります。

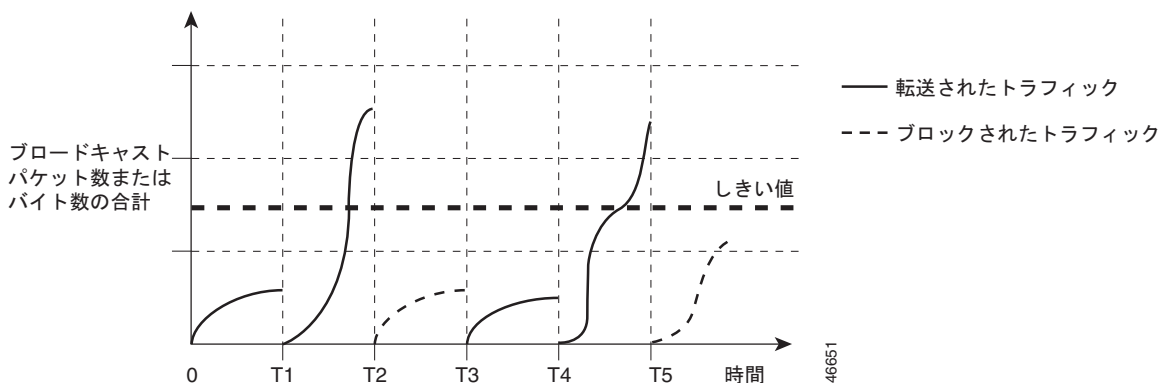


(注)

マルチキャスト トラフィックのストーム制御しきい値に達した場合、ブリッジプロトコル データ ユニット (BPDU) および Cisco Discovery Protocol (CDP) フレームなどのコントロール トラフィック以外のマルチキャスト トラフィックすべてがブロックされます。ただし、スイッチは、ルーティング アップデートと通常のマルチキャスト データ トラフィックとを区別しないため、両方のトラフィックがブロックされます。

図 24-1 のグラフは、一定時間におけるインターフェイス上のブロードキャスト トラフィック パターンを示しています。この例は、マルチキャストおよびユニキャスト トラフィックにも当てはまります。この例では、T1 から T2、T4 から T5 のタイム インターバルで、転送するブロードキャスト トラフィックが設定されたしきい値を上回っています。指定のトラフィック量がしきい値を上回ると、次のインターバルで、そのタイプのトラフィックがすべてドロップされます。したがって、T2 と T5 の後のインターバルの間、ブロードキャスト トラフィックがブロックされます。その次のインターバル（たとえば、T3）では、しきい値を上回らない限り、ブロードキャスト トラフィックが再び転送されます。

図 24-1 ブロードキャスト ストーム制御の例



ストーム制御抑制レベルと 1 秒のタイム インターバルの組み合わせにより、ストーム制御アルゴリズムの動作を制御します。しきい値が高いほど、通過するパケット数が多くなります。しきい値が 100% であれば、トラフィックに対する制限はありません。値を 0.0 にすると、そのポート上ではすべてのブロードキャスト、マルチキャスト、またはユニキャスト トラフィックがブロックされます。



(注) パケットは均一の間隔で着信するのではないため、トラフィック アクティビティを測定する 1 秒のタイム インターバルを設けることによって、ストーム制御の動作に影響を与える可能性があります。

各トラフィック タイプのしきい値を設定するには、**storm-control** 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。

## ストーム制御のデフォルト設定

デフォルトでは、スイッチ インターフェイスでユニキャスト、ブロードキャスト、およびマルチキャスト ストーム制御はディセーブルです (抑制レベルは 100% です)。

## ストーム制御およびしきい値レベルの設定

ポートにストーム制御を設定し、特定のトラフィック タイプで使用するしきい値レベルを入力します。ただし、ハードウェアの制約とともに、さまざまなサイズのパケットをどのように数えるかという問題があるため、しきい値の割合はあくまでも近似値です。着信トラフィックを形成するパケットのサイズによって、実際に適用されるしきい値は設定されたレベルに対して、数パーセントの差異が生じる可能性があります。



(注) ストーム制御は、物理インターフェイスでサポートされています。また、EtherChannel でもストーム制御を設定できます。ストーム制御を EtherChannel で設定する場合、ストーム制御設定は EtherChannel 物理インターフェイスに伝播します。

ストーム制御およびしきい値レベルを設定するには、特権 EXEC モードで次の手順を行います。

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

コマンド	目的
<b>ステップ 3</b> <code>storm-control {broadcast   multicast   unicast} level {level [level-low]   bps bps [bps-low]   pps pps [pps-low]}</code>	<p>ブロードキャスト、マルチキャスト、またはユニキャストストーム制御を設定します。デフォルトでは、ストーム制御はディセーブルに設定されています。</p> <p>キーワードの意味は次のとおりです。</p> <ul style="list-style-type: none"> <li>• <i>level</i> には、ブロードキャスト、マルチキャスト、またはユニキャストトラフィックの上限しきい値レベルを帯域幅のパーセンテージで指定します (小数点第 2 位まで)。上限しきい値に到達すると、ポートはトラフィックをブロックします。指定できる範囲は 0.00 ~ 100.00 です。</li> <li>• (任意) <i>level-low</i> には、下限しきい値レベルを帯域幅のパーセンテージで指定します (小数点第 2 位まで)。この値は、上限抑制値より小さいまたは等しい必要があります。トラフィックがこのレベルを下回っていれば、ポートはトラフィックを転送します。下限抑制レベルを設定しない場合、上限抑制レベルの値に設定されます。指定できる範囲は 0.00 ~ 100.00 です。</li> </ul> <p>しきい値を最大値 (100%) に設定すると、トラフィックの制限はなくなります。しきい値に 0.0 を設定すると、そのポート上のすべてのブロードキャスト、マルチキャスト、またはユニキャストトラフィックがブロックされます。</p> <ul style="list-style-type: none"> <li>• <i>bps bps</i> には、ブロードキャスト、マルチキャスト、またはユニキャストトラフィックの上限しきい値レベルをビット/秒で指定します (小数点第 1 位まで)。上限しきい値に到達すると、ポートはトラフィックをブロックします。指定できる範囲は 0.0 ~ 10000000000.0 です。</li> <li>• (任意) <i>bps-low</i> には、下限しきい値レベルをビット/秒で指定します (小数点第 1 位まで)。この値は上限しきい値レベル以下の値である必要があります。トラフィックがこのレベルを下回っていれば、ポートはトラフィックを転送します。指定できる範囲は 0.0 ~ 10000000000.0 です。</li> <li>• <i>pps pps</i> には、ブロードキャスト、マルチキャスト、またはユニキャストトラフィックの上限しきい値レベルをパケット/秒で指定します (小数点第 1 位まで)。上限しきい値に到達すると、ポートはトラフィックをブロックします。指定できる範囲は 0.0 ~ 10000000000.0 です。</li> <li>• (任意) <i>pps-low</i> には、下限しきい値レベルをパケット/秒で指定します (小数点第 1 位まで)。この値は上限しきい値レベル以下の値である必要があります。トラフィックがこのレベルを下回っていれば、ポートはトラフィックを転送します。指定できる範囲は 0.0 ~ 10000000000.0 です。</li> </ul> <p>BPS および PPS の設定には、しきい値の数値を大きく設定できるように、サフィックスに測定記号 (k、m、g) を使用できます。</p>

コマンド	目的
ステップ 4 <b>storm-control action {shutdown   trap}</b>	ストームが検出された場合に実行するアクションを指定します。デフォルトではトラフィックにフィルタリングを実行し、トラップは送信しない設定です。 <ul style="list-style-type: none"> <li>ストーム中、ポートを <b>error-disable</b> の状態にするには、<b>shutdown</b> キーワードを選択します。</li> <li>ストームが検出された場合、SNMP トラップを生成するには、<b>trap</b> キーワードを選択します。</li> </ul>
ステップ 5 <b>end</b>	特権 EXEC モードに戻ります。
ステップ 6 <b>show storm-control [interface-id] [broadcast   multicast   unicast]</b>	指定したトラフィック タイプについて、インターフェイスで設定したストーム制御抑制レベルを確認します。トラフィック タイプを入力しなかった場合は、ブロードキャスト ストーム制御の設定が表示されます。
ステップ 7 <b>copy running-config startup-config</b>	(任意) コンフィギュレーション ファイルに設定を保存します。

ストーム制御をディセーブルにするには、**no storm-control {broadcast | multicast | unicast} level** インターフェイス コンフィギュレーション コマンドを使用します。

次に、ポート上で、上限抑制レベルを 87%、下限抑制レベルを 65% に設定し、ユニキャスト ストーム制御をイネーブルにする例を示します。

```
Switch# configure terminal
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# storm-control unicast level 87 65
```

次に、ポート上で、ブロードキャスト アドレスのストーム制御を 20% のレベルでイネーブルにする例を示します。ブロードキャスト トラフィックが、トラフィック ストーム制御インターバル内にポートで使用できる総帯域幅のうち、設定された 20% のレベルを超えた場合、トラフィック ストーム制御インターバルが終わるまで、スイッチはすべてのブロードキャスト トラフィックをドロップします。

```
Switch# configure terminal
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# storm-control broadcast level 20
```

## スモール フレーム着信レートの設定

67 バイト未満の着信 VLAN タグ付きパケットは、スモール フレームと見なされます。これらのフレームはスイッチにより転送されますが、スイッチのストーム制御カウンタは増分されません。Cisco IOS リリース 12.2(44)SE 以降は、スモール フレームが指定のレート（しきい値）で着信した場合、ポートが **errdisable** となるように設定できます。

スイッチでスモール フレームの着信機能をグローバルにイネーブルにし、次に各インターフェイス上でパケットのスモール フレームしきい値を設定します。最小サイズよりも小さく、指定のレート（しきい値）で着信したパケットは（ポートが **errdisable** となるため）、ドロップされます。

**errdisable recovery cause small-frame** グローバル コンフィギュレーション コマンドを入力すると、ポートは指定された時間の後、再度イネーブルになります（**errdisable recovery** グローバル コンフィギュレーション コマンドにより、回復時間を指定できます）。

各インターフェイスのしきい値レベルを設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	<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	<code>errdisable detect cause small-frame</code>	スイッチでスモールフレーム レート着信機能をイネーブルにします。
ステップ 3	<code>errdisable recovery interval interval</code>	(任意) 指定された <code>errdisable</code> ステートから回復する時間を指定します。
ステップ 4	<code>errdisable recovery cause small-frame</code>	(任意) スモール フレームの着信により <code>errdisable</code> となったポートが、自動的に再度イネーブルになる回復時間を設定します。
ステップ 5	<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、設定するインターフェイスを指定します。
ステップ 6	<code>small violation-rate pps</code>	インターフェイスが着信パケットをドロップし、ポートを <code>errdisable</code> とするしきい値レートを設定します。指定できる範囲は、1 ~ 10,000 パケット/秒 (pps) です。
ステップ 7	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 8	<code>show interfaces interface-id</code>	設定を確認します。
ステップ 9	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

次に、スモールフレーム着信レート機能をイネーブルにし、ポートの回復時間を設定して、ポートが `errdisable` となるしきい値を設定する例を示します。

```
Switch# configure terminal
Switch# errdisable detect cause small-frame
Switch# errdisable recovery cause small-frame
Switch(config)# interface fastethernet0/1
Switch(config-if)# small-frame violation rate 10000
Switch(config-if)# end
```

## 保護ポートの設定

アプリケーションによっては、あるネイバーが生成したトラフィックが別のネイバーにわからないように、同一スイッチ上のポート間でレイヤ 2 トラフィックが転送されないように設定する必要があります。このような環境では、保護ポートを使用すると、スイッチ上のポート間でユニキャスト、ブロードキャスト、またはマルチキャスト トラフィックの交換が確実になくなります。

保護ポートには、次の機能があります。

- 保護ポートは、同様に保護ポートである他のポートに、トラフィック (ユニキャスト、マルチキャスト、またはブロードキャスト) をすべて転送するわけではありません。データ トラフィックはレイヤ 2 の保護ポート間で転送されません。PIM パケットなどは CPU で処理されてソフトウェアで転送されるため、PIM パケットなどの制御トラフィックのみが転送されます。保護ポート間を通過するすべてのデータ トラフィックはレイヤ 3 装置を介して転送されなければなりません。
- 保護ポートと非保護ポート間の転送動作は、通常どおりに進みます。

ここでは、次の設定情報について説明します。

- 「保護ポートのデフォルト設定」 (P.24-7)
- 「保護ポートの設定時の注意事項」 (P.24-7)
- 「保護ポートの設定」 (P.24-7)

## 保護ポートのデフォルト設定

デフォルトでは、保護ポートは定義されません。

## 保護ポートの設定時の注意事項

保護ポートは、物理インターフェイス（たとえば、GigabitEthernet ポート 1）または EtherChannel グループ（たとえば、ポート チャネル 5）のいずれにも設定できます。ポート チャネルで保護ポートをイネーブルにした場合は、そのポート チャネル グループ内のすべてのポートでイネーブルになります。

プライベート VLAN ポートを保護ポートとして設定しないでください。保護ポートをプライベート VLAN ポートとして設定しないでください。プライベート VLAN の独立ポートは、他の独立ポートやコミュニティ ポートにトラフィックを転送しません。プライベート VLAN の詳細については、[第 15 章「プライベート VLAN の設定」](#)を参照してください。

## 保護ポートの設定

ポートを保護ポートとして定義するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	<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	<code>interface interface-id</code>	設定するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	<code>switchport protected</code>	インターフェイスを保護ポートに設定します。
ステップ 4	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 5	<code>show interfaces interface-id switchport</code>	設定を確認します。
ステップ 6	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

保護ポートをディセーブルにするには、`no switchport protected` インターフェイス コンフィギュレーション コマンドを使用します。

次の例では、ポートを保護ポートとして設定する方法を示します。

```
Switch# configure terminal
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# switchport protected
Switch(config-if)# end
```

## ポートブロッキングの設定

デフォルトでは、スイッチは未知の宛先 MAC アドレスが指定されたパケットをすべてのポートからフラッディングします。未知のユニキャストおよびマルチキャストトラフィックが保護ポートに転送されると、セキュリティ上、問題になる可能性があります。未知のユニキャストおよびマルチキャストトラフィックがあるポートから別のポートに転送されないようにするために、(保護または非保護)ポートをブロックし、未知のユニキャストまたはマルチキャストパケットが他のポートにフラッディングされないようにします。



(注)

マルチキャストトラフィックでは、ポートブロッキング機能によって、純粋なレイヤ 2 パケットだけがブロックされます。ヘッダー内に IPv4 または IPv6 情報を含んでいるマルチキャストパケットはブロックされません。

ここでは、次の設定情報について説明します。

- 「ポートブロッキングのデフォルト設定」(P.24-8)
- 「インターフェイスでのフラッディングトラフィックのブロック」(P.24-8)

## ポートブロッキングのデフォルト設定

デフォルトでは、ポートから未知のマルチキャストおよびユニキャストトラフィックのフラッディングがブロックされず、すべてのポートにこのようなパケットがフラッディングされます。

## インターフェイスでのフラッディングトラフィックのブロック



(注)

このインターフェイスには、物理インターフェイスグループまたは EtherChannel グループを指定できます。特定のポートチャンネルのマルチキャストまたはユニキャストトラフィックをブロックすると、ポートチャンネルグループのすべてのポートでブロックされます。

ユニキャストパケットおよびレイヤ 2 マルチキャストパケットのフラッディングをインターフェイスでディセーブルにするには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	<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	<code>interface interface-id</code>	設定するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	<code>switchport block multicast</code>	ポートからの未知のマルチキャストの転送をブロックします。 (注) 純粋なレイヤ 2 マルチキャストトラフィックだけがブロックされます。ヘッダー内に IPv4 または IPv6 情報を含んでいるマルチキャストパケットはブロックされません。
ステップ 4	<code>switchport block unicast</code>	ポートからの未知のユニキャストの転送をブロックします。
ステップ 5	<code>end</code>	特権 EXEC モードに戻ります。



	コマンド	目的
ステップ 6	<code>show interfaces interface-id switchport</code>	設定を確認します。
ステップ 7	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

ポート上でトラフィックがブロックされずに、通常の転送が行われるデフォルトの状態にインターフェイスに戻すには、`no switchport block {multicast | unicast}` インターフェイス コンフィギュレーション コマンドを使用します。

次に、ポート上でユニキャストおよびレイヤ 2 マルチキャスト フラッドイングをブロックする例を示します。

```
Switch# configure terminal
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# switchport block multicast
Switch(config-if)# switchport block unicast
Switch(config-if)# end
```

## ポートセキュリティの設定

ポートセキュリティ機能を使用すると、ポートへのアクセスを許可するステーションの MAC アドレスを制限および識別して、インターフェイスへの入力を制限できます。セキュア ポートにセキュア MAC アドレスを割り当てると、ポートは定義されたアドレス グループ以外の送信元アドレスを持つパケットを転送しません。セキュア MAC アドレス数を 1 つに制限し、単一のセキュア MAC アドレスを割り当てると、そのポートに接続されたワークステーションに、ポートの帯域幅全体が保証されます。

セキュア ポートとしてポートを設定し、セキュア MAC アドレスが最大数に達した場合、ポートにアクセスを試みるステーションの MAC アドレスが識別されたセキュア MAC アドレスのいずれとも一致しないため、セキュリティ違反が発生します。また、あるセキュア ポート上でセキュア MAC アドレスが設定または学習されているステーションが、別のセキュア ポートにアクセスしようとしたときにも、違反のフラグが立てられます。

ここでは、次の概念および設定情報について説明します。

- 「ポートセキュリティの概要」 (P.24-9)
- 「ポートセキュリティのデフォルト設定」 (P.24-12)
- 「ポートセキュリティの設定時の注意事項」 (P.24-12)
- 「ポートセキュリティのイネーブル化および設定」 (P.24-13)
- 「ポートセキュリティ エージングのイネーブル化および設定」 (P.24-18)
- 「ポートセキュリティおよびプライベート VLAN」 (P.24-20)

## ポートセキュリティの概要

ここでは、次の概要について説明します。

- 「セキュア MAC アドレス」 (P.24-10)
- 「セキュリティ違反」 (P.24-10)

## セキュア MAC アドレス

ポートで許可されるセキュアアドレスの最大数を設定するには、**switchport port-security maximum value** 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。



(注)

最大値をインターフェイス上ですでに設定されているセキュアアドレスの数より小さい値に設定しようとすると、コマンドが拒否されます。

スイッチは、次のセキュア MAC アドレス タイプをサポートします。

- **スタティック セキュア MAC アドレス** : **switchport port-security mac-address mac-address** インターフェイス コンフィギュレーション コマンドを使用して手動で設定され、アドレス テーブルに保存されたのち、スイッチの実行コンフィギュレーションに追加されます。
- **ダイナミック セキュア MAC アドレス** : ダイナミックに設定されてアドレス テーブルに限り保存され、スイッチの再起動時に削除されます。
- **スティッキセキュア MAC アドレス** : ダイナミックに学習することも、手動で設定することもできます。アドレス テーブルに保存され、実行コンフィギュレーションに追加されます。このアドレスがコンフィギュレーション ファイルに保存されていると、スイッチの再起動時にインターフェイスはこれらをダイナミックに再設定する必要がありません。

スティッキ ラーニング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 アドレスに変換して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。スティッキ ラーニングをイネーブルにするには、**switchport port-security mac-address sticky** 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。すべてのスティッキ セキュア MAC アドレスは実行コンフィギュレーションに追加されます。

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。スティッキ セキュア MAC アドレスをコンフィギュレーション ファイルに保存すると、スイッチの再起動時にインターフェイスはこれらを再び学習する必要がありません。スティッキ セキュア アドレスが保存されていない場合は、アドレスは失われます。

スティッキ ラーニング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。

スイッチに設定できるセキュア MAC アドレスの最大数は、システムで許可されている MAC アドレスの最大数によって決まります。この数字はアクティブな Switch Database Management (SDM) テンプレートによって決められます。第 6 章「SDM テンプレートの設定」を参照してください。この値は、使用可能な MAC アドレス (その他のレイヤ 2 機能やインターフェイスに設定されたその他のセキュア MAC アドレスで使用される MAC アドレスを含む) の総数です。

## セキュリティ違反

次のいずれかの状況が発生すると、セキュリティ違反になります。

- 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状態で、アドレス テーブルに未登録の MAC アドレスを持つステーションがインターフェイスにアクセスしようとした場合。
- あるセキュア インターフェイスで学習または設定されたアドレスが、同一 VLAN 内の別のセキュア インターフェイスで使用された場合。

違反が発生した場合の対処に基づいて、次の 3 種類の違反モードのいずれかにインターフェイスを設定できます。

- **protect** (保護) : セキュア MAC アドレスの数がポートで許可されている最大限度に達すると、最大値を下回るまで十分な数のセキュア MAC アドレスを削除するか、許可アドレス数を増やさない限り、未知の送信元アドレスを持つパケットはドロップされます。セキュリティ違反が起こっても、ユーザには通知されません。



**(注)** トランク ポートに **protect** 違反モードを設定することは推奨しません。保護モードでは、ポートが最大制限に達していなくても VLAN が保護モードの最大制限に達すると、ラーニングがディセーブルになります。

- **restrict** (制限) : セキュア MAC アドレスの数がポートで許可されている最大限度に達すると、最大値を下回るまで十分な数のセキュア MAC アドレスを削除するか、許可アドレス数を増やさない限り、未知の送信元アドレスを持つパケットはドロップされます。このモードでは、セキュリティ違反が発生したことが通知されます。SNMP トラップが送信されます。また、Syslog メッセージがロギングされ、違反カウンタが増加します。
- **shutdown** (シャットダウン) : ポートセキュリティ違反により、インターフェイスが **errdisable** になり、ただちにシャットダウンされます。その後、ポートの LED が消灯します。SNMP トラップが送信されます。また、Syslog メッセージがロギングされ、違反カウンタが増加します。セキュア ポートが **errdisable** ステートの場合は、**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するか、**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できます (デフォルトのモードです)。
- **shutdown vlan** : VLAN ごとにセキュリティ違反モードを設定するために使用します。このモードでは、違反が発生すると、ポート全体ではなく VLAN が **errdisable** になります。

表 24-1 に、ポートセキュリティをインターフェイスに設定した場合の違反モードおよび対処について示します。

表 24-1 セキュリティ違反モードの処置

違反モード	トラフィックの転送 <sup>1</sup>	SNMP トラップの送信	Syslog メッセージの送信	エラーメッセージの表示 <sup>2</sup>	違反カウンタの増加	ポートのシャットダウン
protect	不可	不可	不可	不可	不可	不可
restrict	不可	可	可	不可	可	不可
shutdown	不可	可	可	不可	可	可
shutdown vlan	不可	可	可	不可	可	不可 <sup>3</sup>

1. 十分な数のセキュア MAC アドレスを削除するまで未知の送信元アドレスを持つパケットがドロップされます。
2. セキュリティ違反を引き起こすアドレスを手動で設定した場合、スイッチがエラーメッセージを返します。
3. 違反が発生した VLAN だけをシャットダウンします。

## ポートセキュリティのデフォルト設定

表 24-2 に、インターフェイスに対するポートセキュリティのデフォルト設定を示します。

表 24-2 ポートセキュリティのデフォルト設定

機能	デフォルト設定
ポートセキュリティ	ポート上でディセーブル
スティッキアドレスラーニング	ディセーブル
各ポートのセキュア MAC アドレス最大数	1
違反モード	shutdown (シャットダウン)。セキュア MAC アドレスが最大数を上回ると、ポートがシャットダウンします。
ポートセキュリティ エージング	ディセーブル。エージング タイムは 0 スタティック。エージングはディセーブル タイプは absolute

## ポートセキュリティの設定時の注意事項

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。

- ポートセキュリティを設定できるのは、スタティック アクセス ポートまたはトランク ポートに限られます。セキュア ポートをダイナミック アクセス ポートにできません。
- 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。
- セキュア ポートを Gigabit EtherChannel ポート グループに含めることはできません。



(注) 音声 VLAN はアクセス ポートだけでサポートされており、設定可能であってもトランク ポートではサポートされていません。

- 音声 VLAN も設定されているインターフェイスでポートセキュリティをイネーブルにする際には、ポート上で許可されるセキュアアドレスの最大数を 2 に設定します。ポートを Cisco IP Phone に接続している場合、IP Phone には 1 つの MAC アドレスが必要になります。Cisco IP Phone のアドレスは音声 VLAN 上で学習されますが、アクセス VLAN 上では学習されません。1 台の PC を Cisco IP Phone に接続する場合、MAC アドレスの追加は必要ありません。複数の PC を Cisco IP Phone に接続する場合、各 PC と IP Phone に 1 つずつ使用できるように、十分な数のセキュアアドレスを設定する必要があります。
- トランク ポートにポートセキュリティが設定され、トランク ポートが、データトラフィック用にアクセス VLAN、音声トラフィック用に音声 VLAN に割り当てられている場合は、**switchport voice** および **switchport priority extend** 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も無効です。

接続装置が同じ MAC アドレスを使用してアクセス VLAN の IP アドレス、音声 VLAN の IP アドレスの順に要求すると、アクセス VLAN だけに IP アドレスが割り当てられます。

- 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。新しい値が古い値より小さく、インターフェイスで設定されていたセキュア アドレス数も新しい値より大きい場合、コマンドは拒否されます。
- スイッチはスティッキ セキュア MAC アドレスのポート セキュリティ エージングはサポートしていません。

表 24-3 に、ポート セキュリティと他のポートベース機能との互換性が要約されています。

表 24-3 ポート セキュリティと他のポートベース機能との互換性

ポートのタイプまたはポート上の機能	ポート セキュリティとの互換性
DTP <sup>1</sup> ポート <sup>2</sup>	不可
トランク ポート	可
ダイナミック アクセス ポート <sup>3</sup>	不可
ルーテッド ポート	不可
SPAN 送信元ポート	可
SPAN 宛先ポート	不可
EtherChannel	不可
トンネリング ポート	可
保護ポート	可
IEEE 802.1x ポート	可
音声 VLAN ポート <sup>4</sup>	可
プライベート VLAN ポート	不可
IP ソース ガード	可
ダイナミック Address Resolution Protocol (ARP; アドレス解決プロトコル) インспекション	可
Flex Link	可

1. DTP = Dynamic Trunking Protocol (ダイナミック トランキング プロトコル)
2. **switchport mode dynamic** インターフェイス コンフィギュレーション コマンドで設定されたポート
3. **switchport access vlan dynamic** インターフェイス コンフィギュレーション コマンドで設定された VLAN Query Protocol (VQP)
4. ポートのセキュア アドレスの最大許容数を、アクセス VLAN のセキュア アドレスの最大許容数に 2 を足した数に設定する必要があります。

## ポート セキュリティのイネーブル化および設定

ポートへのアクセスを許可するステーションの MAC アドレスを制限および識別することによって、インターフェイスへの入力を制限するには、特権 EXEC モードで次の手順を実行します。

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

	コマンド	目的
ステップ 3	<code>switchport mode {access   trunk}</code>	インターフェイス スイッチポート モードを <code>access</code> または <code>trunk</code> に設定します。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 4	<code>switchport voice vlan <i>vlan-id</i></code>	ポート上で音声 VLAN をイネーブルにします。 <i>vlan-id</i> : 音声トラフィックに VLAN を使用するよう指定します。
ステップ 5	<code>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 6	<code>switchport port-security [maximum value [vlan {<i>vlan-list</i>   {access   voice}}]]</code>	<p>(任意) インターフェイスに対するセキュア MAC アドレスの最大数を設定します。スイッチに設定できるセキュア MAC アドレスの最大数は、システムで許可されている MAC アドレスの最大数によって決まります。この値は、アクティブな Switch Database Management (SDM) テンプレートによって設定されます。第 6 章「スイッチ SDM テンプレートの設定」を参照してください。この値は、使用可能な MAC アドレス (その他のレイヤ 2 機能やインターフェイスに設定されたその他のセキュア MAC アドレスで使用される MAC アドレスを含む) の総数です。</p> <p>(任意) <b>vlan</b> : VLAN ごとに最大値を設定します。</p> <p><b>vlan</b> キーワードを入力後、次のいずれかのオプションを入力します。</p> <ul style="list-style-type: none"> <li><b>vlan-list</b> : トランク ポートで、VLAN 範囲 (ハイフンで区切る) または一連の VLAN (カンマで区切る) に関する VLAN 単位の最大値を設定できます。VLAN を指定しない場合、VLAN ごとの最大値が使用されます。</li> <li><b>access</b> : アクセス ポートで、VLAN をアクセス VLAN として指定します。</li> <li><b>voice</b> : アクセス ポートで、VLAN を音声 VLAN として指定します。</li> </ul> <p>(注) <b>voice</b> キーワードは、音声 VLAN がポートに設定されてそのポートがアクセス VLAN でない場合に限り利用可能です。インターフェイスに音声 VLAN が設定されている場合、セキュア MAC アドレスの最大数を 2 に設定します。</p>

コマンド	目的
<b>ステップ 7</b> <code>switchport port-security violation {protect   restrict   shutdown   shutdown vlan}</code>	<p>(任意) 違反モード、つまりセキュリティ違反が検出されたときの対応を、次のいずれかに設定します。</p> <ul style="list-style-type: none"> <li> <b>protect</b> (保護) : ポートセキュア MAC アドレスの数がポートで許可されている最大限度に達すると、最大値を下回るまで十分な数のセキュア MAC アドレスを削除するか、または許可アドレス数を増やさない限り、未知の送信元アドレスを持つパケットはドロップされます。セキュリティ違反が起こっても、ユーザには通知されません。 </li> </ul> <p>(注) トランク ポート上に保護モードを設定することは推奨できません。保護モードでは、ポートが最大制限に達していなくても VLAN が保護モードの最大制限に達すると、ラーニングがディセーブルになります。</p> <ul style="list-style-type: none"> <li> <b>restrict</b> : セキュア MAC アドレスの数がポートで許可されている最大限度に達すると、十分な数のセキュア MAC アドレスを削除するか、または許可アドレス数を増やさない限り、未知の送信元アドレスを持つパケットはドロップされます。SNMP トラップが送信されます。また、Syslog メッセージがロギングされ、違反カウンタが増加します。 </li> <li> <b>shutdown</b> (シャットダウン) : 違反が発生すると、インターフェイスが <code>errdisable</code> になり、ポートの LED が消灯します。SNMP トラップが送信されます。また、Syslog メッセージがロギングされ、違反カウンタが増加します。 </li> <li> <b>shutdown vlan</b> : VLAN ごとにセキュリティ違反モードを設定するために使用します。このモードでは、違反が発生すると、ポート全体ではなく VLAN が <code>errdisable</code> になります。 </li> </ul> <p>(注) セキュア ポートが <code>errdisable</code> ステートになっている場合は、<code>errdisable recovery cause psecure-violation</code> 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、このステートから回復できます。<code>shutdown</code> および <code>no shutdown</code> 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か、<code>clear errdisable interface vlan</code> 特権 EXEC コマンドを使用して、ポートを手動で再びイネーブルにできます。</p>

コマンド	目的
ステップ 8 <b>switchport port-security</b> <b>[mac-address mac-address [vlan</b> <b>{vlan-id   {access   voice}}]</b>	<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、最大数のセキュア MAC アドレスを入力できます。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 アドレスはダイナミックに学習されます。</p> <p>(注) このコマンドの入力後にスティック ラーニングをイネーブルにすると、ダイナミックに学習されたセキュア アドレスがスティック セキュア MAC アドレスに変換されて実行コンフィギュレーションに追加されます。</p> <p>(任意) <b>vlan</b> : VLAN ごとに最大値を設定します。</p> <p><b>vlan</b> キーワードを入力後、次のいずれかのオプションを入力します。</p> <ul style="list-style-type: none"> <li>• (任意) <b>vlan-id</b> : トランク ポートでは、VLAN ID および MAC アドレスを指定できます。VLAN ID を指定しない場合は、ネイティブ VLAN が使用されます。</li> <li>• <b>access</b> : アクセス ポートで、VLAN をアクセス VLAN として指定します。</li> <li>• <b>voice</b> : アクセス ポートで、VLAN を音声 VLAN として指定します。</li> </ul> <p>(注) <b>voice</b> キーワードは、音声 VLAN がポートに設定されてそのポートがアクセス VLAN でない場合に限り利用可能です。インターフェイスに音声 VLAN が設定されている場合、セキュア MAC アドレスの最大数を 2 に設定します。</p>
ステップ 9 <b>switchport port-security</b> <b>mac-address sticky</b>	<p>(任意) インターフェイスでスティック ラーニングをイネーブルにします。</p>
ステップ 10 <b>switchport port-security</b> <b>mac-address sticky [mac-address  </b> <b>vlan {vlan-id   {access   voice}}]</b>	<p>(任意) スティック セキュア MAC アドレスを入力し、必要な回数だけコマンドを繰り返します。設定したセキュア MAC アドレスの数が最大数より少ない場合、残りの MAC アドレスはダイナミックに学習されてスティック セキュア MAC アドレスに変換され、実行コンフィギュレーションに追加されます。</p> <p>(注) このコマンドの入力前にスティック ラーニングをイネーブルにしないと、エラー メッセージが表示されてスティック セキュア MAC アドレスを入力できません。</p> <p>(任意) <b>vlan</b> : VLAN ごとに最大値を設定します。</p> <p><b>vlan</b> キーワードを入力後、次のいずれかのオプションを入力します。</p> <ul style="list-style-type: none"> <li>• (任意) <b>vlan-id</b> : トランク ポートでは、VLAN ID および MAC アドレスを指定できます。VLAN ID を指定しない場合は、ネイティブ VLAN が使用されます。</li> <li>• <b>access</b> : アクセス ポートで、VLAN をアクセス VLAN として指定します。</li> <li>• <b>voice</b> : アクセス ポートで、VLAN を音声 VLAN として指定します。</li> </ul> <p>(注) <b>voice</b> キーワードは、音声 VLAN がポートに設定されてそのポートがアクセス VLAN でない場合に限り利用可能です。</p>
ステップ 11 <b>end</b>	<p>特権 EXEC モードに戻ります。</p>



	コマンド	目的
ステップ 12	<b>show port-security</b>	設定を確認します。
ステップ 13	<b>copy running-config startup-config</b>	(任意) コンフィギュレーション ファイルに設定を保存します。

セキュア ポートではないデフォルトの状態にインターフェイスを戻す場合は、**no switchport port-security** インターフェイス コンフィギュレーション コマンドを使用します。スティッキ ラーニングがイネーブルの状態でのこのコマンドを入力すると、スティッキ セキュア アドレスが実行コンフィギュレーションの一部に残りますが、アドレス テーブルからは削除されます。ここですべてのアドレスがダイナミックに学習されます。

インターフェイスのセキュア MAC アドレス数をデフォルトに戻す場合は、**no switchport port-security maximum value** 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。違反モードをデフォルト状態 (shutdown モード) に戻す場合は、**no switchport port-security violation {protocol | restrict}** 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。

インターフェイスでスティッキ ラーニングをディセーブルにするには、**no switchport port-security mac-address sticky** 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。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。ただし、スティッキ MAC アドレスによる設定を保存した場合、**no switchport port-security mac-address sticky** コマンドの入力後に設定をもう一度保存しないと、スイッチの再起動時にスティッキ アドレスが復元されます。

MAC アドレス テーブルからすべてのセキュア アドレスを削除するか、スイッチまたはインターフェイス上の特定タイプ (設定済み、ダイナミック、スティッキ) のすべてのセキュア アドレスを削除するには、**clear port-security {all | configured | dynamic | sticky}** 特権 EXEC コマンドを使用します。

アドレス テーブルから特定のセキュア MAC アドレスを削除するには、**no switchport port-security mac-address mac-address** インターフェイス コンフィギュレーション コマンドを使用します。インターフェイス上のすべてのダイナミック セキュア 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** インターフェイス コンフィギュレーション コマンドの後に、(インターフェイスでポート セキュリティを再びイネーブルにするために) **switchport port-security** コマンドを入力します。**no switchport port-security** コマンドを入力する前に、**no switchport port-security mac-address sticky** インターフェイス コンフィギュレーション コマンドを使用してスティッキ セキュア MAC アドレスをダイナミック セキュア MAC アドレスに変換した場合、手動で設定されたものを除き、インターフェイス上のすべてのセキュア アドレスが削除されます。

設定済みのセキュア MAC アドレスをアドレス テーブルから明確に削除する場合、**no switchport port-security mac-address mac-address** インターフェイス コンフィギュレーション コマンドを使用しなければなりません。

次の例では、ポートでポート 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 50 に設定する方法を示します。違反モードはデフォルトであり、スタティック セキュア MAC アドレスは設定されず、スティッキ ラーニングはイネーブルにされます。

```
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# switchport mode access
Switch(config-if)# switchport port-security
Switch(config-if)# switchport port-security maximum 50
Switch(config-if)# switchport port-security mac-address sticky
```

次に、ポートに VLAN 3 のスタティック セキュア MAC アドレスを設定する例を示します。

```
Switch(config)# interface gigabitethernet0/11
Switch(config-if)# switchport mode trunk
Switch(config-if)# switchport port-security
Switch(config-if)# switchport port-security mac-address 0000.02000.0004 vlan 3
```

次に、ポート上でスティックポートセキュリティをイネーブルにし、データ VLAN および音声 VLAN の MAC アドレスを手動で設定し、セキュアアドレスの最大合計数を 20（データ VLAN 用に 10、音声 VLAN 用に 10）に設定する例を示します。

```
Switch(config)# interface gigabitethernet1/0/1
Switch(config-if)# switchport access vlan 21
Switch(config-if)# switchport mode access
Switch(config-if)# switchport voice vlan 22
Switch(config-if)# switchport port-security
Switch(config-if)# switchport port-security maximum 20
Switch(config-if)# switchport port-security violation restrict
Switch(config-if)# switchport port-security mac-address sticky
Switch(config-if)# switchport port-security mac-address sticky 0000.0000.0002
Switch(config-if)# switchport port-security mac-address 0000.0000.0003
Switch(config-if)# switchport port-security mac-address sticky 0000.0000.0001 vlan voice
Switch(config-if)# switchport port-security mac-address 0000.0000.0004 vlan voice
Switch(config-if)# switchport port-security maximum 10 vlan access
Switch(config-if)# switchport port-security maximum 10 vlan voice
```

## ポートセキュリティ エージングのイネーブル化および設定

ポート上のすべてのセキュアアドレスにエージングタイムを設定するには、ポートセキュリティ エージングを使用します。ポートごとに 2 つのタイプのエージングがサポートされています。

- **absolute** : 指定されたエージングタイムの経過後に、ポート上のセキュアアドレスが削除されます。
- **inactivity** : 指定されたエージングタイムの間、セキュアアドレスが非アクティブであった場合に限り、ポート上のセキュアアドレスが削除されます。

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、セキュアポート上のデバイスを削除および追加し、なおかつポート上のセキュアアドレス数を制限できます。セキュアアドレスのエージングは、ポート単位でイネーブルまたはディセーブルにできます。

ポートセキュリティ エージングを設定するには、特権 EXEC モードで次の手順を実行します。

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

コマンド	目的
ステップ 3 <b>switchport port-security aging {static   time time   type {absolute   inactivity}}</b>	<p>セキュア ポートのスタティック エージングをイネーブ爾またはディセーブルにします。またはエージング タイムやタイプを設定します。</p> <p>(注) スイッチは、スタティックセキュア アドレスのポートセキュリティ エージングをサポートしていません。</p> <p>このポートに、スタティック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爾にする場合は、<b>static</b> を入力します。</p> <p><i>time</i> には、このポートのエージング タイムを指定します。指定できる範囲は、0 ~ 1440 分です。</p> <p><b>type</b> には、次のキーワードのいずれか 1 つを選択します。</p> <ul style="list-style-type: none"> <li>• <b>absolute</b> : エージング タイプを絶対エージングとして設定します。このポートのセキュア アドレスはすべて、指定した時間 (分単位) が経過するとエージングアウトし、セキュア アドレス リストから削除されます。</li> <li>• <b>inactivity</b> : エージング タイプを非アクティブ エージングとして設定します。指定された 期間中にセキュア 送信元アドレスからのデータ トラフィックがない場合に限り、このポートのセキュア アドレスがエージングアウトします。</li> </ul>
ステップ 4 <b>end</b>	特権 EXEC モードに戻ります。
ステップ 5 <b>show port-security [interface interface-id] [address]</b>	設定を確認します。
ステップ 6 <b>copy running-config startup-config</b>	(任意) コンフィギュレーション ファイルに設定を保存します。

ポート上のすべてのセキュア 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。スタティックに設定されたセキュア アドレスに対してだけエージングをディセーブルにするには、**no switchport port-security aging static** インターフェイス コンフィギュレーション コマンドを使用します。

次に、ポート上でセキュア アドレスのエージング タイムを 2 時間に設定する例を示します。

```
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# switchport port-security aging time 120
```

次に、このインターフェイスに設定されたセキュア アドレスに対して、エージングをイネーブ爾にし、非アクティブ エージング タイプのエージング 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
Switch(config-if)# switchport port-security aging type inactivity
Switch(config-if)# switchport port-security aging static
```

上記のコマンドを確認するには、**show port-security interface interface-id** 特権 EXEC コマンドを入力します。

## ポートセキュリティおよびプライベート VLAN

管理者はポートセキュリティを使用して、ポートで学習する MAC アドレスの数を制限したり、ポートで学習可能な MAC アドレスを指定したりできます。

PVLAN ホストおよび混合モード ポート上でポートセキュリティを設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	<b>configure terminal</b>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<b>interface interface-id</b>	設定するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	<b>switchport mode private-vlan {host   promiscuous}</b>	インターフェイスでプライベート VLAN をイネーブルにします。
ステップ 4	<b>switchport port-security</b>	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 5	<b>end</b>	特権 EXEC モードに戻ります。
ステップ 6	<b>show port-security [interface interface-id] [address]</b>	設定を確認します。
ステップ 7	<b>copy running-config startup-config</b>	(任意) コンフィギュレーション ファイルに設定を保存します。

```
Switch(config)# interface GigabitEthernet 0/8
Switch(config-if)# switchport private-vlan mapping 2061 2201-2206,3101
Switch(config-if)# switchport mode private-vlan promiscuous
Switch(config-if)# switchport port-security maximum 288
Switch(config-if)# switchport port-security
Switch(config-if)# switchport port-security violation restrict
```



(注)

ポートセキュリティとプライベート VLAN の両方が設定されたポートを、セキュア PVLAN ポートと呼びます。セキュア PVLAN ポートでセキュア アドレスを学習すると、同一のプライマリ VLAN に属する他のセキュア PVLAN ポートで同じセキュア アドレスを学習できません。ただし、非セキュア PVLAN ポートで学習したアドレスは、同一プライマリ VLAN に属するセキュア PVLAN ポートで学習できます。

ホスト ポートで学習したセキュア アドレスは、関連するプライマリ VLAN で自動的に複製されます。同様に、混合ポートで学習したセキュア アドレスは、すべての関連するセカンダリ VLAN で自動的に複製されます。ユーザがスタティック アドレス (mac-address-table static コマンドを使用) をセキュア ポートに設定できません。

## ポートベースのトラフィック制御の設定

**show interfaces *interface-id* switchport** 特権 EXEC コマンドを使用すると、(他の特性の中から) インターフェイス トラフィックの抑制および制御の設定が表示されます。**show storm-control** および **show port-security** 特権 EXEC コマンドを使用すると、それぞれストーム制御とポート セキュリティ設定が表示されます。

トラフィックの制御情報を表示するには、表 24-4 の特権 EXEC コマンドを 1 つ以上使用します。

表 24-4      トラフィック制御ステータスおよび設定を表示するためのコマンド

コマンド	目的
<b>show interfaces [<i>interface-id</i>] switchport</b>	すべてのスイッチング (非ルーティング) ポートまたは指定されたポートの管理ステータスまたは動作ステータスを、ポート ブロックングおよびポート保護の設定を含めて表示します。
<b>show storm-control [<i>interface-id</i>] [broadcast   multicast   unicast]</b>	すべての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ているストーム制御抑制レベルを、指定されたトラフィックタイプについて、またはブロードキャストトラフィック (トラフィックタイプが入力されていない場合) について表示します。
<b>show port-security [interface <i>interface-id</i>]</b>	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 アドレスの最大許容数、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。
<b>show port-security [interface <i>interface-id</i>] address</b>	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。
<b>show port-security interface <i>interface-id</i> vlan</b>	指定されたインターフェイスに VLAN 単位で設定されているセキュア MAC アドレスの数を表示します。

