CHAPTER 26

# ポート単位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。特に明記しない限り、*スイッチ*という用語は、スタンドアロン スイッチおよびスイッチ スタックを指します。

（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

ここでは、次の概念と設定情報について説明します。

# 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。プロトコルスタックの実装エラー、ネットワーク構成の間違い、またはユーザによって引き起こされる DoS 攻撃もストームの原因になります。

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 バスを通過するパケットをモニタし、パケットがユニキャスト、マルチキャスト、または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 秒間に受け取った特定のタイプのパケットの数をカウントして、事前に定義された抑制レベルのしきい値とその測定結果を比較します。

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。

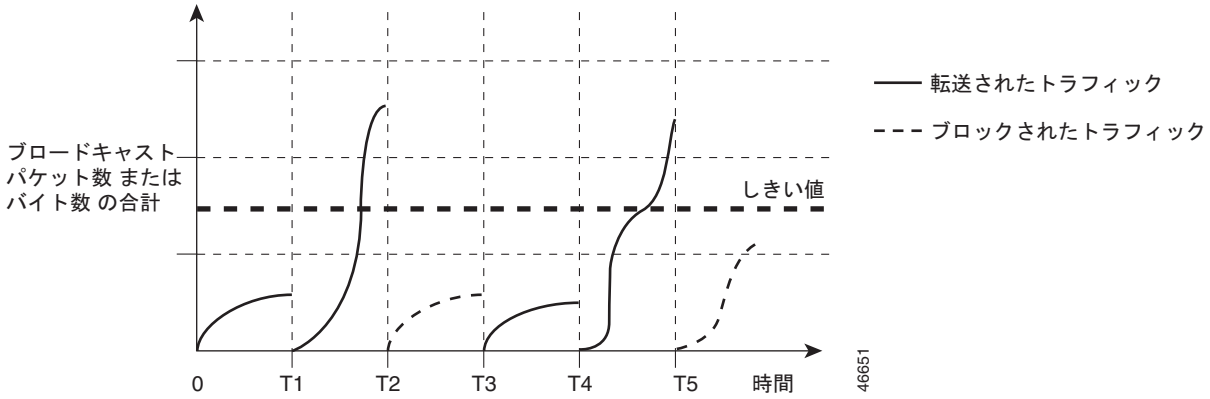
- 帯域幅（ブロードキャスト、マルチキャスト、またはユニキャスト トラフィックが使用できるポートの総帯域幅の割合）。
- 秒単位で受信するパケット（ブロードキャスト、マルチキャスト、またはユニキャスト）のトラフィック レート
- 小さいフレームのトラフィック レートの秒単位のパケット数。この機能は、グローバルにイネーブルです。小さいフレームのしきい値は、各インターフェイスで設定されます。（Cisco IOS Release 12.2(44)SE 以降）。

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）フレーム、Cisco Discovery Protocol（CDP）フレームのような制御トラフィック以外のマルチキャスト トラフィックはすべてブロックされます。ただし、スイッチでは OSPF のようなルーティング アップデートと、正規のマルチキャスト データ トラフィックは区別されないため、両方のトラフィック タイプがブロックされます。

図 26-1 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 26-1　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 秒間のインターバルを組み合わせて、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、通過でき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）　パケットは一定の間隔で届くわけではないので、トラフィック アクティビティを測定する 1 秒間のインターバルがストーム制御の動作を左右す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、ユニキャスト、ブロードキャスト、およびマルチキャスト ストーム制御はスイッチ インターフェイス上でディセーブルになります。したがって、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ので、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 % 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。

ストーム制御と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 | **configure terminal** | グローバル コンフィギュレーション モードを開始します。 |
| ステップ 2 | **interface** *interface-id* | 設定する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 | **storm-control** {**broadcast** \| **multicast** \| **unicast**} **level** {*level* [*level-low*] \| **bps** *bps* [*bps-low*] \| **pps** *pps* [*pps-low*]} | 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。<br>キーワードの意味は次のとおりです。<br>• *level* 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。<br>• （任意）*level-low* 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か、または等しくなければなりません。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。<br>しきい値に最大値（100%）を指定した場合、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。<br>• **bps** *bps* 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。<br>• （任意）*bps-low* 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。<br>• **pps** *pps* 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。<br>• （任意）*pps-low* 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。<br>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 など）を使用できます。 |

| | コマンド | 目的 |
|---|---|---|
| ステップ 4 | **storm-control action** {**shutdown** \| **trap**} | 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。<br>• ストーム中、ポートを errdisable の状態にするには、**shutdown** キーワードを選択します。<br>• ストームが検出された場合、SNMP（簡易ネットワーク管理プロトコル）トラップを生成するには、**trap** キーワードを選択します。 |
| ステップ 5 | **end** | 特権 EXEC モードに戻ります。 |
| ステップ 6 | **show storm-control** [*interface-id*] [**broadcast** \| **multicast** \| **unicast**] | 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 | **copy running-config startup-config** | （任意）コンフィギュレーション ファイルに設定を保存します。 |

ス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方法を示します。

```
Switch# configure terminal
Switch(config)# interface gigabitethernet1/0/1
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 gigabitethernet1/0/1
Switch(config-if)# storm-control broadcast level 20
```

# スモール フレーム到着レートの設定

67 バイト未満の着信 VLAN タグ付きパケットは、*小さいフレーム*と見なされます。このパケットはスイッチにより転送されますが、スイッチ ストーム制御カウンタを増加させません。Cisco IOS Release 12.2(44)SE 以降では、小さいフレームが指定されたレート（しきい値）で到着した場合は、ポートがディセーブルになるように設定できます。

スイッチ上の小さいフレームの着信機能をグローバルにイネーブルにして、各インターフェイスのパケットの小さいフレームのしきい値を設定します。最小サイズよりも小さく、指定されたレート（しきい値）で着信するパケットは、ポートがディセーブルにされた後はドロップされます。

**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、指定された時間後にポートが再び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 コマンドを使用して、リカバリ時間を指定します）。

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 | **configure terminal** | グローバル コンフィギュレーション モードを開始します。 |
| ステップ 2 | **errdisable detect cause small-frame** | スイッチ上の小さいフレームの着信レート機能をイネーブルにします。 |
| ステップ 3 | **errdisable recovery interval** *interval* | （任意）指定された errdisable ステートから回復する時間を指定します。 |
| ステップ 4 | **errdisable recovery cause small-frame** | （任意）小さいフレームの着信によりポートが errdisable になった後、そのポートを自動的に再イネーブルにするリカバリ時間を設定します。 |
| ステップ 5 | **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、設定するインターフェイスを指定します。 |
| ステップ 6 | **small violation-rate** *pps* | インターフェイスが着信パケットをドロップしてポートを errdisable にするようにしきい値レートを設定します。範囲は、1 ～ 10,000 Packets Per Second（pps; パケット / 秒）です。 |
| ステップ 7 | **end** | 特権 EXEC モードに戻ります。 |
| ステップ 8 | **show interfaces** *interface-id* | 設定を確認します。 |
| ステップ 9 | **copy running-config startup-config** | （任意）コンフィギュレーション ファイルに設定を保存します。 |

次に、小さいフレームの着信レート機能をイネーブルにし、ポートのリカバリ時間を設定し、ポートを errdisable にす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 gigabitethernet1/0/1
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、同様に保護ポートになっている他のポートに対して、ユニキャスト、マルチキャスト、またはブロードキャスト トラフィックを転送しません。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、このような制御トラフィックだけが転送されます。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 デバイス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。

スイッチ スタックは論理的には 1 つのスイッチを表しているため、レイヤ 2 トラフィックは、スタック内の同一スイッチか異なるスイッチかにかかわらず、スイッチ スタックの保護ポート間では転送されません。

ここでは、次の設定について説明します。



# 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。

# 保護ポート設定時の注意事項

保護ポートは、物理インターフェイス（GigabitEthernet ポート 1 など）または EtherChannel グループ（port-channel 5 など）に設定できます。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 16 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 | **configure terminal** | グローバル コンフィギュレーション モードを開始します。 |
| ステップ 2 | **interface** *interface-id* | 設定する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 | **switchport protected** | 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 | **end** | 特権 EXEC モードに戻ります。 |
| ステップ 5 | **show interfaces** *interface-id* **switchport** | 設定を確認します。 |
| ステップ 6 | **copy running-config startup-config** | （任意）コンフィギュレーション ファイルに設定を保存します。 |

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。

次に、保護ポートとしてポートを設定する例を示します。

```
Switch# configure terminal
Switch(config)# interface gigabitethernet1/0/1
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 ブロッキング機能は純粋なレイヤ 2 パケットだけをブロックします。ヘッダーに IPv4 または IPv6 の情報を含むマルチキャスト 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.26-8）
- 「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キング」（P.26-8）

## 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キング

（注）　インターフェイスは物理インターフェイスまたは EtherChannel グループのいずれも可能です。ポート チャ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 パケットのインターフェイスからのフラッディングをディセーブルにするには、特権 EXEC モードで次の手順を実行します。

| | コマンド | 目的 |
|---|---|---|
| ステップ 1 | **configure terminal** | グローバル コンフィギュレーション モードを開始します。 |
| ステップ 2 | **interface** *interface-id* | 設定する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 | **switchport block multicast** | 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。<br>（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。ヘッダーに IPv4 または IPv6 の情報を含むマルチキャスト パケットはブロックされません。 |
| ステップ 4 | **switchport block unicast** | 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 | **end** | 特権 EXEC モードに戻ります。 |
| ステップ 6 | **show interfaces** *interface-id* **switchport** | 設定を確認します。 |
| ステップ 7 | **copy running-config startup-config** | （任意）コンフィギュレーション ファイルに設定を保存します。 |

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を戻すには、**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、ポート上のユニキャストおよびレイヤ 2 マルチキャスト フラッディングをブロックする例を示します。

```
Switch# configure terminal
Switch(config)# interface gigabitethernet1/0/1
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、アップリンク 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、アップリンク 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 ポートとしてアップリンク 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、次の概念と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.26-9）
- 「ポート セキュリティのデフォルト設定」（P.26-12）
- 「ポート セキュリティの設定時の注意事項」（P.26-12）
- 「ポート セキュリティのイネーブル化および設定」（P.26-14）
- 「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.26-18）
- 「ポート セキュリティとスイッチ スタック」（P.26-19）
- 「ポート セキュリティおよびプライベート VLAN」（P.26-20）


## 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.26-9）
- 「セキュリティ違反」（P.26-10）


### セキュア MAC アドレス

アップリンク 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：動的に設定されてアドレス テーブルにのみ保存され、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：動的に学習することも、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動的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、自動的には反映されません。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 アドレスを保存しない場合、アドレスは失われます。

スティッキ ラーニングがディセーブルの場合、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。

スイッチまたはスイッチ スタック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 8 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）の総数を表します。

## 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かぎり、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、ポートが最大数に達していなくても VLAN が保護モードの最大数に達すると、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かぎり、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。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 error-disabled になり、ただちにシャットダウンされます。そのあと、ポートの LED が消灯します。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。これは、デフォルトのモードです。
- shutdown vlan（VLAN シャットダウン）：VLAN 単位で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 26-1 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 26-1　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[1] | 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[2] | 違反カウンタの増加 | ポートのシャットダウン |
|---|---|---|---|---|---|---|
| protect | No | No | No | No | No | No |
| restrict | No | Yes | Yes | No | Yes | No |
| shutdown | No | No | No | No | Yes | Yes |
| shutdown vlan | No | No | Yes | No | Yes | No[3] |

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 のみ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 26-2 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 26-2　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。 |
| ポートあたりのセキュア MAC アドレスの最大数 | 1 |
| 違反モード | 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。<br>スタティック エージングはディセーブル。<br>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 ポートにすることはできません。
- セキュア ポートを Switched Port Analyzer（SPAN; スイッチド ポート アナライザ）の宛先ポートにすることはできません。
- セキュア ポートは、ギガビット EtherChannel ポート グループに属することができません。

**（注）** 音声 VLAN はアクセス ポートでのみ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。

- セキュア ポートは、プライベート VLAN ポートにできません。
- 音声 VLAN が設定された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する場合は、ポートの最大セキュア アドレス許容数を 2 に設定します。ポートを Cisco IP Phone に接続する場合は、IP Phone に MAC アドレスが 1 つ必要です。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 ポートがポート セキュリティで設定され、データ トラフィックのアクセス VLAN および音声トラフィックのアクセス 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効果はありません。

  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 だけが IP アドレスに割り当てられます。

- ポート セキュリティを設定する場合は、最初に **switchport port-security maximum** 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許可する MAC アドレスの合計数を指定し、次に許可するアクセス VLAN（**switchport port-security vlan access** インターフェイス コンフィギュレーション コマンド）の数および音声 VLAN（**switchport port-security vlan voice** インターフェイス コンフィギュレーション コマンド）の数を設定します。最初に合計数を指定しなかった場合は、システムによってデフォルト設定（1 つの MAC アドレス）が返されます。
- 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。
- 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 エージングをサポートしていません。

表 26-3 に、他のポートベース機能と互換性のあるポート セキュリティについてまとめます。

**表 26-3　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 タイプまたはポートの機能 | ポート セキュリティとの互換性 |
|---|---|
| DTP [1] ポート[2] | No |
| トランク ポート | Yes |
| ダイナミック アクセス ポート[3] | No |
| ルーテッド ポート | No |
| Switched Port Analyzer（SPAN; スイッチド ポート アナライザ）送信元ポート | Yes |
| SPAN 宛先ポート | No |
| EtherChannel | No |
| トンネリング ポート | Yes |
| 保護ポート | Yes |
| IEEE 802.1x ポート | Yes |
| 音声 VLAN ポート[4] | Yes |
| プライベート VLAN ポート | No |
| IP ソース ガード | Yes |
| ダイナミック アドレス解決プロトコル（ARP）インスペクション | Yes |
| Flex Link | Yes |

1. DTP = Dynamic Trunking Protocol
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）ポート。
4. ポートに最大限可能なセキュアなアドレスを設定します（アクセス VLAN で可能なセキュアなアドレスの最大数に 2 を加えた数）。

# 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 | **configure terminal** | グローバル コンフィギュレーション モードを開始します。 |
| ステップ 2 | **interface** *interface-id* | 設定する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 | **switchport mode** {**access** \| **trunk**} | インターフェイス スイッチポート モードを access または trunk 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 | **switchport voice vlan** *vlan-id* | ポート上で音声 VLAN をイネーブルにします。<br>*vlan-id*：音声トラフィックに使用する VLAN を指定します。 |
| ステップ 5 | **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 6 | **switchport port-security** [**maximum** ***value*** [**vlan** {*vlan-list* \| {**access** \| **voice**}}]] | （任意）**maximum**：ポート上のセキュア MAC アドレスの最大数を指定します。デフォルトでは、1 つの MAC アドレスのみ許可されます。<br>スイッチまたはスイッチ スタック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 SDM テンプレートによって決まります。第 8 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）の総数を表します。<br>（任意）**vlan**：VLAN 単位の最大値を設定します。<br>**vlan** 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。<br>• *vlan-list*：トランク ポート上で、ハイフンで区切った範囲の VLAN、またはカンマで区切った一連の VLAN における、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。<br>• **access**：アクセス ポート上で、アクセス VLAN として VLAN を指定します。<br>• **voice**：アクセス ポート上で、音声 VLAN として VLAN を指定します。<br>**（注）** **voice** キーワードは、音声 VLAN がポートに設定されていて、さらにそのポートがアクセス VLAN でない場合のみ有効です。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。 |

| | コマンド | 目的 |
|---|---|---|
| ステップ 7 | **switchport port-security violation** {**protect** \| **restrict** \| **shutdown** \| **shutdown vlan**} | （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。<br>• **protect**（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。<br>（注）　トランク ポートに protect モードを設定することは推奨しません。保護モードでは、ポートが最大数に達していなくても VLAN が保護モードの最大数に達すると、ラーニングがディセーブルになります。<br>• **restrict**：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。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。<br>• **shutdown**（シャットダウン）：違反が発生すると、インターフェイスが error-disabled 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。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。<br>• **shutdown vlan**：VLAN 単位で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。<br>（注）　セキュア ポートが errdisable ステートになった場合は、**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します。手動で再びイネーブルにするには、**shutdown** および **no shutdown** インターフェイス コンフィギュレーション コマンドを入力するか、**clear errdisable interface vlan** 特権 EXEC コマンドを入力します。 |

| | コマンド | 目的 |
|---|---|---|
| ステップ 8 | **switchport port-security** [**mac-address** *mac-address* [**vlan** {*vlan-id* \| {**access** \| **voice**}}] | （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 アドレスは動的に学習されます。<br>**（注）** このコマンドの入力後にスティッキ ラーニングをイネーブルにすると、動的に学習されたセキュア アドレスがスティッキ 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。<br>（任意）**vlan**：VLAN 単位の最大値を設定します。<br>**vlan** 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。<br>• *vlan-id*：トランク ポートで、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、ネイティブ VLAN が使用されます。<br>• **access**：アクセス ポート上で、アクセス VLAN として VLAN を指定します。<br>• **voice**：アクセス ポート上で、音声 VLAN として VLAN を指定します。<br>**（注）** **voice** キーワードは、音声 VLAN がポートに設定されていて、さらにそのポートがアクセス VLAN でない場合のみ有効です。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。 |
| ステップ 9 | **switchport port-security mac-address sticky** | （任意）インターフェイスでスティッキ ラーニングをイネーブルにします。 |
| ステップ 10 | **switchport port-security mac-address sticky** [*mac-address* \| **vlan** {*vlan-id* \| {**access** \| ***voice***}}] | （任意）スティッキ 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 アドレスは動的に学習されてスティッキ 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。<br>**（注）** このコマンドの入力前にスティッキ 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キ セキュア MAC アドレスを入力できません。<br>（任意）**vlan**：VLAN 単位の最大値を設定します。<br>**vlan** 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。<br>• *vlan-id*：トランク ポートで、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、ネイティブ VLAN が使用されます。<br>• **access**：アクセス ポート上で、アクセス VLAN として VLAN を指定します。<br>• **voice**：アクセス ポート上で、音声 VLAN として VLAN を指定します。<br>**（注）** **voice** キーワードは、音声 VLAN がポートに設定されていて、さらにそのポートがアクセス VLAN でない場合のみ有効です。 |
| ステップ 11 | **end** | 特権 EXEC モードに戻ります。 |
| ステップ 12 | **show port-security** | 設定を確認します。 |
| ステップ 13 | **copy running-config startup-config** | （任意）コンフィギュレーション ファイルに設定を保存します。 |

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動的に学習されます。

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には、**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）に戻すには、**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 テーブルからスイッチまたはインターフェイス上のセキュア アドレスすべてまたは特定（設定、ダイナミック、スティッキ）のセキュア アドレスすべてを削除するには、**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** コマンドを使用する前に、**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ー 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 コマンドを使用する必要があります。

次に、ポート上でポート 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 に設定する例を示します。違反モードはデフォルトです。スタティック セキュア MAC アドレスは設定せず、スティッキ ラーニングはイネーブルです。

```
Switch(config)# interface gigabitethernet1/0/1
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、ポートの VLAN 3 上にスタティック セキュア MAC アドレスを設定する例を示します。

```
Switch(config)# interface gigabitethernet1/0/2
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、ポートのスティッキ ポート セキュリティをイネーブルにする例を示します。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 アドレスの総数を 20 に設定します（データ VLAN に 10、音声 VLAN に 10 を割り当てます）。

```
Switch(config)# interface tengigabitethernet1/0/1
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 | **configure terminal** | グローバル コンフィギュレーション モードを開始します。 |
| ステップ 2 | **interface** *interface-id* | 設定する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 | **switchport port-security aging** {**static** \| **time** *time* \| **type** {**absolute** \| **inactivity**}} | セキュア ポートのスタティック エージングをイネーブル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。<br>**（注）** スイッチは、スティッキ 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。<br>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ルにする場合は、**static** を入力します。<br>*time* 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。<br>**type** には、次のキーワードのいずれか 1 つを選択します。<br>• **absolute**：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）が経過すると期限切れになり、セキュア アドレス リストから削除されます。<br>• **inactivity**：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 time 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 アドレスが期限切れになります。 |
| ステップ 4 | **end** | 特権 EXEC モードに戻ります。 |
| ステップ 5 | **show port-security** [**interface** *interface-id*] [**address**] | 設定を確認します。 |
| ステップ 6 | **copy running-config startup-config** | （任意）コンフィギュレーション ファイルに設定を保存します。 |

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。静的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、ポート上のセキュア 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 gigabitethernet1/0/1
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ルにし、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 セキュリティとスイッチ スタック

スタックに新規に加入したスイッチは、設定済みのセキュア アドレスを取得します。他のスタック メンバーから新しいスタック メンバーに、ダイナミック セキュア アドレスがすべてダウンロードされます。

スイッチ（スタック マスターまたはスタック メンバのいずれか）がスタックから離れると、その他のスタック メンバに通知が行き、そのスイッチが設定または学習したセキュア MAC アドレスがセキュア MAC アドレス テーブルから削除されます。スイッチ スタックの詳細については、第 7 章「スイッチ スタックの管理」を参照してください。

# ポート セキュリティおよびプライベート VLAN

ポート セキュリティにより、管理者はポートで学習する MAC アドレス数を制限したり、ポートで学習する MAC アドレスを定義したりできます。

PVLAN ホストおよび無差別ポートでポート 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 | **configure terminal** | グローバル コンフィギュレーション モードを開始します。 |
| ステップ 2 | **interface** *interface-id* | 設定する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 | **switchport mode private-vlan** {**host** \| **promiscuous**} | 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 | **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 5 | **end** | 特権 EXEC モードに戻ります。 |
| ステップ 6 | **show port-security** [**interface** *interface-id*] [**address**] | 入力内容を確認します。 |
| ステップ 7 | **copy running-config startup-config** | （任意）コンフィギュレーション ファイルに設定を保存します。 |

次に、PVLAN ホストおよび無差別ポートでポート セキュリティを設定する例を示します。

```
Switch(config)# interface gigabitethernet 1/0/8
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 の両方が設定されているポートには、セキュア PVLAN ポートのラベル付けが可能です。セキュア アドレスがセキュア PVLAN ポートで学習されるとき、同じセキュア アドレスは、同じプライマリ VLAN に属する別のセキュア PVLAN ポートでは学習できません。ただし、非セキュア PVLAN ポートで学習されたアドレスは、同じプライマリ VLAN に属するセキュア PVLAN ポートで学習できます。

ホスト ポートで学習されるセキュア アドレスは、関連プライマリ VLAN で自動的に複製され、また同様に、無差別ポートで学習されるセキュア アドレスは、すべての関連セカンダリ VLAN で自動的に複製されます。静的アドレス（mac-address-table static コマンドを使用）は、ユーザがセキュア ポートで設定することはできません。

# プロトコル ストーム保護の設定



## プロトコル ストーム保護の概要

スイッチが Address Resolution Protocol（ARP; アドレス解決プロトコル）または制御パケットでフラッドされると、CPU の高い使用率により CPU のオーバーロードが発生する可能性があります。これらの問題は、次のように発生します。

- プロトコル制御パケットが受信されず、ネイバーの隣接がドロップされるため、ルーティング プロトコルがフラップする場合があります。
- Spanning Tree Protocol（STP; スパニングツリー プロトコル）Bridge Protocol Data Unit（BPDU; ブリッジ プロトコル データ ユニット）が送受信されないため、STP が再収束します。
- CLI が遅くなるか応答しなくなります。

プロトコル ストーム保護を使用すると、パケットのフロー レートの上限しきい値を指定して、制御パケットが送信されるレートを制御できます。サポートされるプロトコルは、ARP、ARP スヌーピング、Dynamic Host Configuration Protocol（DHCP）v4、DHCP スヌーピング、インターネット グループ管理プロトコル（IGMP）、および IGMP スヌーピングです。

パケットのレートが定義されたしきい値を超えると、スイッチは指定されたポートに着信したすべてのトラフィックを 30 秒間ドロップします。パケット レートが再度計測され、必要な場合はプロトコル ストーム保護が再度適用されます。

より強力な保護が必要な場合は、仮想ポートを手動で errdisable にし、その仮想ポートのすべての着信トラフィックをブロックできます。また、手動で仮想ポートをイネーブルにしたり、仮想ポートの自動再イネーブル化の時間間隔を設定することもできます。

（注）　超過したパケットは、2 つ以下の仮想ポートにおいてドロップされます。
仮想ポートの errdisable は、EtherChannel および Flexlink インターフェイスではサポートされません。

## デフォルトのプロトコル ストーム保護の設定

プロトコル ストーム保護はデフォルトでディセーブルです。これがイネーブルになると、仮想ポートの自動リカバリがデフォルトでディセーブルになります。

# プロトコル ストーム保護のイネーブル化

プロトコル ストーム保護を設定するには、特権 EXEC モードで次の手順を実行します。

| | コマンド | 目的 |
|---|---|---|
| ステップ 1 | **configure terminal** | グローバル コンフィギュレーション モードを開始します。 |
| ステップ 2 | **psp** {**arp** \| **dhcp** \| **igmp**} **pps** *value* | ARP、IGMP、または DHCP に対してプロトコル ストーム保護を設定します。<br>*value* には、1 秒あたりのパケット数のしきい値を指定します。トラフィックがこの値を超えると、プロトコル ストーム保護が適用されます。範囲は毎秒 5 ～ 50 パケットです。 |
| ステップ 3 | **errdisable detect cause psp** | （任意）プロトコル ストーム保護の errdisable 検出をイネーブルにします。この機能がイネーブルになると、仮想ポートが errdisable になります。この機能がディセーブルになると、そのポートは、ポートを errdisable にせずに超過したパケットをドロップします。 |
| ステップ 4 | **errdisable recovery interval** *time* | （任意）errdisable の仮想ポートの自動リカバリ時間を秒単位で設定します。仮想ポートが errdisable の場合、この時間を過ぎるとスイッチは自動的にリカバリします。指定できる範囲は 30 ～ 86400 秒です。 |
| ステップ 5 | **end** | 特権 EXEC モードに戻ります。 |
| ステップ 6 | **show psp config** {**arp** \| **dhcp** \| **igmp**} | 設定を確認します。 |

次の例では、DHCP の着信 DHCP トラフィックが毎秒 35 パケットを超えた場合に、トラフィックをドロップするようプロトコル ストーム保護を設定する方法を示します。

```
Switch# configure terminal
Switch(config)# psp dhcp pps 35
```

特定のプロトコルで、プロトコル ストーム保護をディセーブルにするには、**no psp** {**arp** | **dhcp** | **igmp**} 特権 EXEC コマンドを使用します。

プロトコル ストーム保護の errdisable 検出をディセーブルにするには、**no errdisable detect cause psp** グローバル コンフィギュレーション コマンドを使用します。

手動で errdisable 仮想ポートを再度イネーブルにするには、**errdisable recovery cause psp** グローバル コンフィギュレーション コマンドを使用します。

errdisable ポートの自動リカバリをディセーブルにするには、**no errdisable recovery cause psp** グローバル コンフィギュレーション コマンドを使用します。

プロトコル ストーム保護が設定されている場合、ドロップされたパケットの数がカウンタに記録されます。このカウンタを表示するには、**show psp statistics** [**arp** | **igmp** | **dhcp**] 特権 EXEC コマンドを使用します。あるプロトコルのカウンタをクリアするには、**clear psp counter** [**arp** | **igmp** | **dhcp**] コマンドを使用します。

# ポート単位のトラフィック制御設定の表示

**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、ストーム制御およびポート セキュリティの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 26-4 の特権 EXEC コマンドを 1 つまたは複数使用します。

**表 26-4　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 |
|---|---|
| **show interfaces** [*interface-id*] **switchport** | 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 ブロッキングおよびポート保護の設定を含めて表示します。 |
| **show storm-control** [*interface-id*] [**broadcast** \| **multicast** \| **unicast**] | 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。 |
| **show port-security** [**interface** *interface-id*] | 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。 |
| **show port-security** [**interface** *interface-id*] **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。 |
| **show port-security interface** *interface-id* **vlan** | 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。 |