CHAPTER 21

# ポート単位のトラフィック制御の設定

この章では、Catalyst 3550 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。

この章の内容は、次のとおりです。



## ストーム制御の設定

ここでは、ストーム制御の設定および手順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。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、またはサービス拒絶（DoS）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。

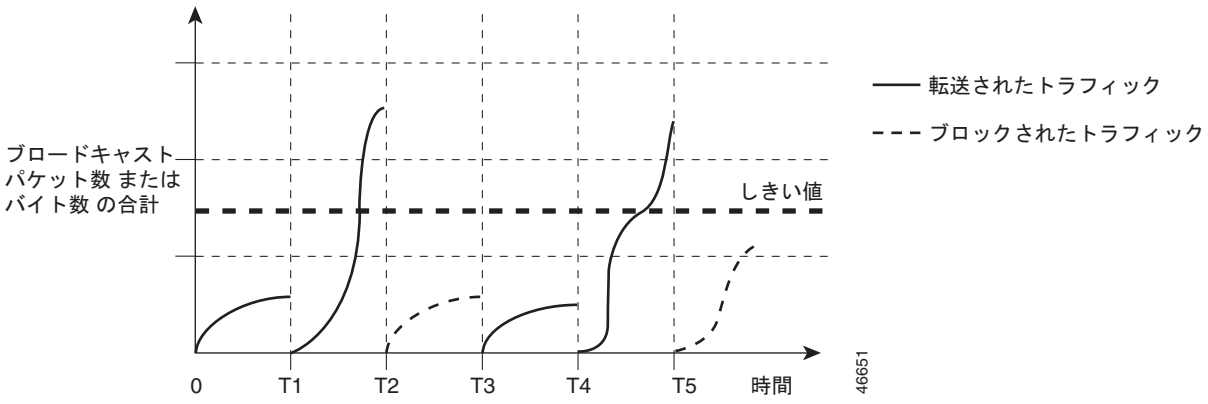
- 帯域幅（ブロードキャスト、マルチキャスト、またはユニキャスト トラフィックが使用できるポートの総帯域幅の割合）。
- ブロードキャスト、マルチキャスト、またはユニキャスト パケットが受信される、1 秒あたりのパケット単位のトラフィック レート（Cisco IOS Release 12.1(22)EA1 以降）

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 トラフィックのレートが、設定したしきい値を超えると、レベルがしきい値未満に低下するまで、すべての着信トラフィック（ブロードキャスト、マルチキャスト、およびユニキャスト）はドロップされます。スパニングツリー パケットだけが転送されます。ブロードキャストおよびユニキャストのしきい値を超えると、しきい値を超過したトラフィックのタイプについてのみトラフィックがブロックされます。

図 21-1 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 21-1　　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。

**（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。

（注）　Cisco IOS Release 12.1(8)EA1 よりも前は、**switchport broadcast**、**switchport multicast**、および **switchport unicast** インターフェイス コンフィギュレーション コマンドを使用してストーム制御しきい値を設定します。これらのコマンドは使用されなくなり、**storm-control** インターフェイス コンフィギュレーション コマンドに置き換えられました。

# 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（トラフィックに対して課せられた制限はありません）。

# 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 タイプが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だけでサポートされています。これは、コマンドが CLI で利用できる場合でも、EtherChannel ポート チャネルまたはポート チャネルのメンバである物理インターフェイスではサポートされていません。

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* | 設定する物理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 | **storm-control** {**broadcast** \| **multicast** \| **unicast**} **level** {*level* [*level-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>• **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>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。 |
| 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 fastethernet0/1
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 fastethernet0/1
Switch(config-if)# storm-control broadcast level 20
```

# 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。
- 保護ポートは、IEEE 802.1Q トランクでサポートされます。

デフォルトでは、保護ポートは定義されません。

**（注）** 保護ポート機能とフォールバック ブリッジングとの併用はできません。フォールバック ブリッジングがイネーブルである場合、スイッチ上の 1 つの保護ポートから、別の VLAN 内にある同じスイッチ上の別の保護ポートにパケットが転送される可能性があります。

**（注）** MAC アドレスが期限切れ、またはスイッチによって学習されなかったために、保護されていないポートからの不明のユニキャストまたはマルチキャスト トラフィックが保護されたポートにフラッディングすることがあります。そのような場合に、ユニキャストまたはマルチキャスト トラフィックがポートにフラッディングされないことを保証するには、**switchport block unicast** および **switchport block multicast** 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。

物理インターフェイスまたは EtherChannel グループで保護ポートを設定できます。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。

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** | 入力内容を確認します。 |
| 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 fastethernet0/1
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、スイッチは不明の宛先 MAC アドレスを持つパケットをすべてのポートに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。

不明のユニキャストまたはマルチキャスト トラフィックがポート間で転送されないようにするために、不明のユニキャストまたはマルチキャスト パケットをブロックするよう、ポート（保護または非保護）を設定できます。

（注）　ユニキャストまたはマルチキャスト トラフィックのブロックは、保護ポート上で自動的にイネーブルにはなりません。明示的に設定する必要があります。

## 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。

マルチキャストおよびユニキャスト 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 | **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** | ポートへの不明マルチキャストの転送をブロックします。 |
| ステップ 4 | **switchport block unicast** | ポートへの不明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** | 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。 |

トラフィックがブロックされ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 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 gigabitethernet0/1
Switch(config-if)# switchport block multicast
Switch(config-if)# switchport block unicast
Switch(config-if)# end
```

## ポート上での通常の転送の再開

ポート上で通常の転送を復元するには、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 | **no switchport block multicast** | ポートへの不明マルチキャストのフラッディングをイネーブルにします。 |
| ステップ 4 | **no switchport block unicast** | ポートへの不明ユニキャストのフラッディング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 interfaces** *interface-id* **switchport** | 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。 |

# 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。

ここでは、次の情報について説明します。



# ポート セキュリティの概要

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

次のタイプのセキュア MAC アドレスを設定できます。

- 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：動的に学習されてアドレス 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。
- スティッキー 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場合は、スイッチを再起動しても、インターフェイスはダイナミックにこれらのアドレスを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もできますが、推奨しません。

*スティッキー 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ー 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。

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。この設定は保存しないと失われます。

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。

セキュア ポートまたは VLAN で使用可能な MAC アドレスの最大数は、アクティブな Switch Database Management（SDM）テンプレートによって決まります。SDM テンプレートの設定の詳細については、「ユーザ選択機能のためのシステム リソースの最適化」（P.6-28）を参照してください。

## 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：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。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 ポートで **protect** モードをイネーブルにすることは推奨しません。**protect** 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：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。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。具体的には、SNMP トラップが送信され、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：このモードでは、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はただちに errdisable になり、ポート LED がオフになります。また、SNMP トラップも送信され、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。これは、デフォルトのモードです。

表 21-1 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 21-1　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 | Yes | Yes | No | Yes | Yes |

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。

# デフォルトのポート セキュリティ設定

表 21-2 にインターフェイス用のデフォルトのポート セキュリティ設定を示します。

**表 21-2　デフォルトのポート セキュリティ設定**

| 機能 | デフォルト設定 |
|---|---|
| ポート セキュリティ | ディセーブル |
| セキュア MAC アドレスの最大数 | 1 |
| 違反モード | shutdown |
| スティッキー アドレス ラーニング | ディセーブル |
| 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 。イネーブルにした場合、デフォルトの **type** は **absolute** です。 |

# 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、トランク ポート、または IEEE 802.1Q トンネル ポートにかぎられます。
- 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 ポートは、Fast EtherChannel やギガビット EtherChannel ポート グループに属すことができません。

（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。

- 音声 VLAN も設定している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、ポートで許容されるセキュア アドレスの最大数を、アクセス VLAN におけるセキュア アドレスの最大数に 2 を足した数に設定する必要があります。ポートを Cisco IP Phone に接続する場合は、IP Phone に最大 2 つの MAC アドレスが必要です。IP Phone アドレスは音声 VLAN 上で学習されますが、アクセス VLAN 上で学習される場合もあります。PC を IP Phone に接続するには、さらに MAC アドレスが必要になります。
- 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 21-3 に、ポート セキュリティと、ポートに設定されたその他の機能との互換性について、概要を示します。

**表 21-3　ポート セキュリティと、その他の Catalyst 3550 の機能との互換性**

| ポートのタイプ | 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 |
| SPAN 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 |
| 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**} | アクセスまたはトランクとしてインターフェイス スイッチポート モードを設定します。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。 |

| | コマンド | 目的 |
|---|---|---|
| ステップ 6 | **switchport port-security** [**maximum** *value* [**vlan** {*vlan-list* \| {**access** \| **voice**}}]] | （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。使用可能なアドレスの最大数は、アクティブな Switch Database Management（SDM）テンプレートによって決まります。デフォルトは 1 です。<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。 |
| ステップ 7 | **switchport port-security violation** {**protect** \| **restrict** \| **shutdown**} | （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。protect 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>**（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 コマンドを使用することにより、ステートを変更することができます。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ことにより、手動でポートをイネーブルに戻すこともできます。 |

| | 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ー 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ー 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。 |
| 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ー 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）スティッキー 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ー 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ー 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ー 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。 |
| 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** | 入力内容を確認します。 |
| 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。スティッキー 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、スティッキー 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** {**protect** | **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ー 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ー セキュア MAC アドレスをダイナミック セキュア アドレスに変換します。

スタティック セキュア MAC アドレスをアドレス テーブルから削除するには、**clear port-security configured address** *mac-address* 特権 EXEC コマンドを使用します。インターフェイスまたは VLAN 上にあるすべてのスタティック セキュア MAC アドレスを削除するには、**clear port-security configured interface** *interface-id* 特権 EXEC コマンドを使用します。

ダイナミック セキュア MAC アドレスをアドレス テーブルから削除するには、**clear port-security dynamic address** *mac-address* 特権 EXEC コマンドを使用します。インターフェイスまたは VLAN 上にあるすべてのダイナミック アドレスを削除するには、**clear port-security dynamic interface** *interface-id* 特権 EXEC コマンドを使用します。

スティッキ セキュア MAC アドレスをアドレス テーブルから削除するには、**clear port-security sticky address** *mac-address* 特権 EXEC コマンドを使用します。インターフェイスまたは VLAN 上にあるすべてのスティッキ アドレスを削除するには、**clear port-security sticky interface** *interface-id* 特権 EXEC コマンドを使用します。

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、スティッキー ラーニングはイネーブルです。

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# interface fastethernet0/1
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
Switch(config-if)# end
```

次に、ポートにスタティック セキュア MAC アドレスを設定し、スティッキ ラーニング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)# interface fastethernet0/2
Switch(config-if)# switchport mode access
Switch(config-if)# switchport port-security
Switch(config-if)# switchport port-security mac-address 0000.02000.0004
Switch(config-if)# switchport port-security mac-address sticky
Switch(config-if)# end
```

次に、ポートの VLAN 5 に対して最大 8 個のセキュア MAC アドレスを設定する例を示します。

```
Switch(config-if)# switchport port-security maximum 8 vlan 5
Switch(config-if)# end
```

次に、ポートの VLAN 5 に対して最大 8 個のセキュア MAC アドレスを設定する例を示します。

```
Switch(config-if)# switchport port-security maximum 8 vlan 5
Switch(config-if)# end
```

次に、ポートのスティッキー 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 FastEthernet1/0/1
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
```

次に、ポートの VLAN 5 に対して最大 8 個のセキュア MAC アドレスを設定する例を示します。

```
Switch(config-if)# switchport port-security maximum 8 vlan 5
Switch(config-if)# end
```

# 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 セキュリティ エージングを使用すると、ポート上のスタティックおよびダイナミック セキュア アドレスにエージング タイムを設定できます。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 PC 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。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* | ポート セキュリティ エージングをイネーブルにするポートを指定し、インターフェイス コンフィギュレーション モードを開始します。<br>**（注）** スイッチは、スティッキー 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。 |
| 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>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。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。<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。このポートのすべてのセキュア アドレスは、指定された時間（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。<br>**（注）** 絶対エージング時間は、システム タイマーの進行状況によっては、1 分の差が出る場合があります。<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**] | 入力内容を確認します。 |
| 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 fastethernet0/1
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、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 21-4 の特権 EXEC コマンドを 1 つまたは複数使用します。

**表 21-4　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** | 各 VLAN のセキュア MAC アドレスの最大許容数と、VLAN のセキュア MAC アドレス数を表示します。 |