



# ポートベース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)

ここで使用されるコマンドの構文および使用方法の詳細については、このリリースのコマンド 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 \(p.22-2\)](#)
- [保護ポートの設定 \(p.22-6\)](#)
- [ポート ブロッキングの設定 \(p.22-7\)](#)
- [ポート セキュリティの設定 \(p.22-9\)](#)
- [ポートベースのトラフィック制御設定の表示 \(p.22-20\)](#)

## 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 \(p.22-2\)](#)
- [ストーム制御のデフォルト設定 \(p.22-3\)](#)
- [ストーム制御およびスレッシュホールド レベルの設定 \(p.22-3\)](#)

### ストーム制御の概要

ストーム制御は、LAN 上のトラフィックが、いずれかの物理インターフェイス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のストームによって影響されないようにします。LAN ストームは、パケットが LAN にフラディングした場合に発生するもので、過剰なトラフィックが生成され、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、ネットワーク構成でのエラー、またはユーザによる DoS 攻撃が、ストームの原因となります。

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 バスへ流れるパケットをモニタし、その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 秒間で受信された指定タイプのパケット数をカウントし、あらかじめ定義された抑制レベル スレッシュホールドと計測値を比較します。

ストーム制御は、トラフィック アクティビティを測定するために次のいずれかの方法を使用します。

- **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、ポートの利用可能な総帯域幅に対する割合
- **トラフィック速度** 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たときの 1 秒あたりのパケット数 (Cisco IOS Release 12.1(22)EA1 以降)

いずれの方法も、上限のスレッシュホールドに到達するとポートがトラフィックをブロックします。トラフィックの速度が下限スレッシュホールド(指定されている場合)を下回るまでポートはブロックされたままになり、下回ると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、スイッチはトラフィックの速度が上限抑制レベルを下回るまですべてのトラフィックをブロックします。一般的に、スレッシュホールドのレベルが高くなると、ブロードキャスト ストームに対する保護の効果が薄くなります。

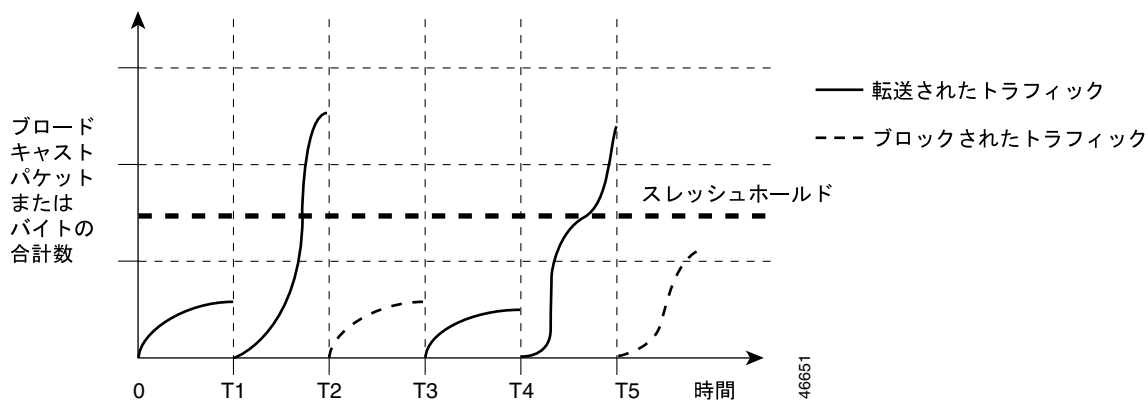


(注)

マルチキャスト トラフィックの速度が、設定されているスレッシュホールドを上回ると、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、スレッシュホールド レベルを下回るまで廃棄され、スパニングツリー パケットのみが転送されます。ブロードキャストおよびユニキャストがスレッシュホールドを上回った場合、スレッシュホールドを上回ったトラフィック タイプのみがブロックされます。

図 22-1 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 トラフィックにも適用できます。この例では、転送されているブロードキャスト トラフィックが、タイム インターバル T1 ~ T2 間および T4 ~ T5 間で設定されたスレッシュホールドを上回っています。特定のトラフィックの量がスレッシュホールドを上回ると、そのタイプのすべてのトラフィックは次の一定時間にわたり、廃棄されます。したがって、ブロードキャスト トラフィックは T2 および T5 のあとのインターバルではブロックされています。次のタイム インターバル(たとえば T3)では、ブロードキャスト トラフィックがスレッシュホールドを上回らなければ、再度転送されます。

図 22-1 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。スレッシュホールドが高いほど、通過できるパケットが多くなります。



(注) パケットは均一の間隔で着信するわけではないため、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 タイプのスレッシュホールドの値を設定するには、`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) IOS 12.1(8)EA1 より前のリリースでは、ストーム制御スレッシュホールドの設定には、`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いましたが、上記のコマンドは現在では廃止され、`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ています。

## 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のストーム制御はスイッチでディセーブルになっています。つまり抑制レベルは 100% であり、トラフィックには制限がありません。

## ストーム制御およびスレッシュホールド レベルの設定

ポートにストーム制御を設定して特定のタイプのトラフィックに使用するスレッシュホールド レベルを入力します。

ただし、ハードウェアの制約や、さまざまなサイズのパケットがカウントされる動作のため、スレッシュホールドの割合には誤差が生じます。着信トラフィックを構成するパケットのサイズによっては、実際のスレッシュホールドは、数パーセント程度、設定されたレベルと異なる場合があります。

## ■ ストーム制御の設定



(注) ストーム制御がサポートされるのは物理インターフェイスに限られます。EtherChannel ポートチャンネルやポートチャンネルのメンバーである物理インターフェイスでは、CLI (コマンドラインインターフェイス) でコマンドが利用できても、サポートはされません。

ストーム制御とスレッシュホールドレベルを設定するには、イネーブル 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。
ステップ 3	<code>storm-control {broadcast   multicast   unicast} level {level [level-low]   pps pps [pps-low]}</code>	<p>ブロードキャスト、マルチキャスト、およびユニキャスト ストーム制御を設定します。デフォルトで、ストーム制御はディセーブルです。</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><code>level</code> 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スレッシュホールドを帯域幅のパーセント (小数点以下 2 桁まで) で指定します。上限のスレッシュホールドに到達するとポートが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) <code>level-low</code> には、下限スレッシュホールドを帯域幅のパーセント (小数点以下 2 桁まで) で指定します。この値は上限抑制値以下でなければなりません。トラフィックがこのレベルより下回った場合に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、上限抑制レベルに設定されます。指定できる範囲は 0.00 ~ 100.00 です。</li> </ul> <p>スレッシュホールドの最大値 (100%) を設定した場合、トラフィックの制限がなくなります。スレッシュホールドを 0.00 に設定した場合、そのポートのすべてのブロードキャスト、マルチキャスト、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><code>pps pps</code> には、ブロードキャスト、マルチキャスト、ユニキャスト トラフィックの上限スレッシュホールド レベルを、1 秒あたりのパケット数 (小数点以下 1 桁まで) で指定します。上限のスレッシュホールドに到達するとポートが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) <code>pps-low</code> には、下限スレッシュホールド レベルを、1 秒あたりのパケット数 (小数点以下 1 桁まで) で指定します。これは上限スレッシュホールド以下に設定できます。トラフィックがこのレベルより下回った場合に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>PPS 設定の場合、数字の大きなスレッシュホールドに k、m、g などの接尾辞を使用できます。</p>
ステップ 4	<code>storm-control action {shutdown   trap}</code>	<p>ストームが検出された場合に取る処置を指定します。デフォルトは、トラフィックをフィルタリングし、トラップを送信しません。</p> <ul style="list-style-type: none"> <li>ストーム中にポートをエラー ディセーブルにするには、<code>shutdown</code> キーワードを選択します。</li> <li>ストームが検出されたときに SNMP トラップを生成するには、<code>trap</code> キーワードを選択します。</li> </ul>
ステップ 5	<code>end</code>	イネーブル EXEC モードに戻ります。

	コマンド	目的
ステップ 6	<code>show storm-control [interface-id] [broadcast   multicast   unicast]</code>	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に設定したストーム制御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 ストーム制御設定が表示されません。
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。

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

```
Switch# configure terminal
Switch(config)# interface fastethernet0/1
Switch(config-if)# storm-control unicast level 87 65
```

次に、ポートでブロードキャスト アドレス ストーム制御をイネーブルにし、レベルを 20% 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のポートの使用可能な総帯域幅の設定レベルの 20% を超えた場合、スイッチはトラフィック ストーム制御インターバルが終了するまでブロードキャスト トラフィックをすべて廃棄します。

```
Switch# configure terminal
Switch(config)# interface fastethernet0/1
Switch(config-if)# storm-control broadcast level 20
```

## 保護ポートの設定

一部のアプリケーションでは、同一スイッチのポート間でトラフィックが転送されないようにすることにより、あるネイバによって生成されたトラフィックを別のネイバが認識しないように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れば、スイッチ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は行われません。

保護ポートには次のような機能があります。

- 保護ポートは、ほかの保護ポートにいかなるトラフィック（ユニキャスト、マルチキャスト、またはブロードキャスト）も転送しません。レイヤ 2 では、保護ポート間にデータトラフィックを転送できません。PIM パケットのような制御トラフィックのパケットは CPU で処理されてからソフトウェアで転送されるため、これら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 デバイスを經由して転送する必要があります。
- 保護ポート / 非保護ポート間の転送動作は、通常どおり行われます。
- IEEE 802.1Q トランクでは、保護ポートがサポートされています。

デフォルトでは、保護ポートは定義されていません。



(注)

保護ポート機能は代替ブリッジングと併用できません。代替ブリッジングがイネーブルである場合、スイッチの 1 つの保護ポートから、別の VLAN（仮想 LAN）内にある同じスイッチ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（メディア アクセス制御）アドレスが期限切れになったことや、スイッチによって学習されなかったことが原因で、非保護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ポートにフラッディングされることがあります。このような場合、保護ポートへのユニキャストまたはマルチキャストトラフィックのフラッディングを防止するには、`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 グループに保護ポートを設定できます。ポート チャンネルについて保護ポートをイネーブルにすると、ポート チャンネル グループ内の全ポートが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、イネーブル 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として設定します。
ステップ 4	<code>end</code>	イネーブル 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、宛先 MAC アドレスが不明のパケットは、すべてのポートにフラッディングされます。不明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、セキュリティ上の問題が発生することがあります。

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、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にポート（保護ポートまたは非保護ポート）を設定できます。



(注) 保護ポートでは、ユニキャストやマルチキャストトラフィックのブロックは自動的にイネーブルになりません。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ク



(注) インターフェイスは物理インターフェイスまたは EtherChannel グループを指定できます。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。

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、イネーブル 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	<code>switchport block unicast</code>	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	<code>end</code>	イネーブル EXEC モードに戻ります。
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。

インターフェイスをトラフィックがブロックされないデフォルトの状態に戻すには、`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。

## ■ ポートブロッキングの設定

次に、ポートでユニキャストおよびマルチキャスト フラ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
```

## ポートでの通常の転送の再開

ポート上で通常の転送を再開するには、イネーブル 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>no switchport block multicast</code>	ポートへの不明マルチキャストのフラディングをイネーブルにします。
ステップ 4	<code>no switchport block unicast</code>	ポートへの不明ユニキャストのフラディングをイネーブルにします。
ステップ 5	<code>end</code>	イネーブル EXEC モードに戻ります。
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が許可されたステーションの 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、次の内容について説明します。

- [ポートセキュリティの概要 \(p.22-9\)](#)
- [ポートセキュリティのデフォルト設定 \(p.22-11\)](#)
- [ポートセキュリティ設定時の注意事項 \(p.22-11\)](#)
- [ポートセキュリティのイネーブル化と設定 \(p.22-12\)](#)
- [ポートセキュリティエージングのイネーブル化と設定 \(p.22-18\)](#)

### 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 \(p.22-9\)](#)
- [セキュリティ違反 \(p.22-10\)](#)

### セキュア MAC アドレス

スイッチでは、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を使用して手動で設定されます。これらはアドレステーブルに格納され、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** ダイナミックに学習されます。これらはアドレステーブル内のみ格納され、スイッチが再起動するときに削除されます。
- **固定 (sticky) セキュア MAC アドレス** ダイナミックに学習または手動で設定されます。これらは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。これらのアドレスがコンフィギュレーションファイルに保存されている場合は、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な学習を再度行う必要はありません。固定セキュアアドレスは手動で設定できますが、この方法は推奨しません。

*固定学習をイネーブルにすると、ダイナミック MAC アドレスを固定セキュア 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。固定学習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すべてのダイナミックセキュア MAC アドレス (固定学習がイネーブルになる前にダイナミックに学習されたアドレスを含む) を、固定セキュア MAC アドレスに変換します。*

固定セキュア MAC アドレスは、コンフィギュレーションファイル (スイッチの再起動時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、自動的に格納されません。コンフィギュレーションファイルに固定セキュア MAC アドレスが保存されている場合は、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。設定は保存しないと失われます。

固定学習がディセーブルの場合、固定セキュア 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て動作中のコンフィギュレーションから削除されます。

## ■ ポートセキュリティの設定

セキュア ポートまたは VLAN 上の使用できる 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定されます。SDM テンプレートの設定については、「ユーザが選択した機能に対するシステム 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

セキュリティ違反とは、次のいずれかの状況が発生したときです。

- セキュア MAC アドレスが最大数までアドレス テーブルに追加され、アドレス テーブルにない 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認識された場合。

違反発生時の対処方法に関して、次の 3 つ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に許容された限界に達した場合、十分な数のセキュア MAC アドレスを削除するまで、不明の送信元アドレスを持つパケットは廃棄されます。セキュリティ違反の発生は通知されません。



(注) トランク ポート上の **protect** モードをイネーブルにしないでください。ポートがその最大制限値に達していない場合でも、いずれかの VLAN が最大制限値に達すると、**protect** モードにより学習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に許容された限界に達した場合、十分な数のセキュア MAC アドレスを削除するか、または許容されるアドレスの最大数を増やすまで、不明の送信元アドレスを持つパケットは廃棄されます。セキュリティ違反の発生は通知されません。具体的には、SNMP トラップが送信され、Syslog メッセージが記録され、違反カウンタが増加します。
- **shutdown** このモードでは、ポートのセキュリティ違反が発生すると、インターフェイスが即座にエラーディセーブルになり、ポート LED がオフになります。また、SNMP トラップを送信し、Syslog メッセージを記録し、違反カウンタが増加します。セキュア ポートがエラー ディセーブル 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。デフォルトはこのモードに設定されています。

表 22-1 に、インターフェイスにポート セキュリティを設定した場合の、違反モードおよび動作を示します。

表 22-1 セキュリティ違反モードの動作

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	なし	なし	なし	なし	なし	なし
restrict	なし	あり	あり	なし	あり	なし
shutdown	なし	あり	あり	なし	あり	あり

1. 十分な数のセキュア MAC アドレスを削除するまで、送信元アドレスが不明のパケットは廃棄されます。
2. セキュリティ違反の原因となるアドレスを手動で設定すると、スイッチはエラー メッセージを返します。

## ポートセキュリティのデフォルト設定

表 22-2 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 22-2 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	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
固定アドレス学習	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 です。イネーブルの場合、デフォルトの type は absolute になります。

## ポートセキュリティ設定時の注意事項

ポートセキュリティの設定時は、次の注意事項に従ってください。

- ポートセキュリティは、スタティックアドレスポート、トランクポート、または IEEE 802.1Q トンネルポート上でのみ設定できます。
- セキュアポートは、ダイナミックアクセスポートにできません。
- セキュアポートは、Switched Port Analyzer (SPAN; スイッチドポートアナライザ) の宛先ポートにできません。
- セキュアポートは、Fast EtherChannel や Gigabit EtherChannel ポートグループに属することができません。



(注) 音声 VLAN がサポートされるのは、アクセスポートのみです。設定で許可されている場合でも、トランクポートではサポートされません。

- 音声 VLAN と共に設定され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、ポート上に設定可能な最大セキュアアドレスを 2 に設定します。ポートが Cisco IP Phone に接続されている場合、IP Phone には 1 つの MAC (メディアアクセス制御) アドレスが必要になります。Cisco IP Phone アドレスは音声 VLAN 上で学習されますが、アクセス VLAN 上では学習されません。1 つの PC を Cisco IP Phone に接続する場合、追加の MAC アドレスは不要です。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。
- インターフェイスのセキュアアドレスの最大値として入力した値が古い値よりも大きい場合、新しい値が古い設定値よりも優先されます。新しい値が古い値よりも小さく、インターフェイスに設定されたセキュアアドレス数が新しい値を超えている場合、コマンドは拒否されます。
- スイッチでは、固定セキュア 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ません。

表 22-3 は、ポートセキュリティとポートに設定されている他の機能との互換性を要約したものです。

表 22-3 ポートセキュリティと Catalyst 3550 の他の機能との互換性


ポートのタイプ	ポートセキュリティとの互換性
DTP <sup>1</sup> ポート <sup>2</sup>	なし
トランク ポート	あり
ダイナミック アクセス ポート <sup>3</sup>	なし
ルーテッド ポート	なし
SPAN 送信元ポート	あり
SPAN 宛先ポート	なし
EtherChannel	なし
トンネリング ポート	あり
保護ポート	あり
IEEE 802.1X ポート	あり
音声 VLAN ポート <sup>4</sup>	あり
IP ソース ガード	あり
ダイナミック Address Resolution Protocol ( ARP; アドレス解決プロトコル) 検査	あり
Flex Link	あり



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 コマンドが設定されたポート
3. `switchport access vlan dynamic` インターフェイス コンフィギュレーション コマンドを設定した VLAN Query Protocol (VQP) ポート
4. ポート上で許可されるセキュアアドレスの最大数を 2 にして、さらにアクセス VLAN に許可されているセキュアアドレスの最大数を加える必要があります。



## ポートセキュリティのイネーブル化と設定

ポートへのアクセスが許可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方法でインターフェイスへの入力を制限するには、イネーブル 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 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 ( <code>dynamic auto</code> ) 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 vlan-id</code>	ポートで音声 VLAN をイネーブルにします。  <i>vlan-id</i> 音声トラフィックに使用する VLAN を指定します。
ステップ 5	<code>switchport port-security</code>	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します。

コマンド	目的
<b>ステップ 6</b> <code>switchport port-security [maximum value [vlan {vlan-list / {access / voice}}]]</code>	<p>(任意) インターフェイスについてセキュア MAC アドレスの最大数を設定します。使用できるアドレスの最大数は、アクティブな SDM テンプレートにより決定されます。デフォルト値は 1 です。インターフェイスが音声 VLAN 用に設定されている場合、最大 2 つのセキュア MAC アドレスを設定します。</p> <p>(任意) <code>vlan</code> VLAN 単位の最大値を設定します。</p> <p><code>vlan</code> キーワードを入力したあと、次のオプションを 1 つ入力します。</p> <ul style="list-style-type: none"> <li><code>vlan-list</code> トランク ポートで、ハイフンで区切られた VLAN 範囲、またはカンマで区切られた一連の VLAN 上の VLAN 単位の最大値を設定できます。VLAN が指定されていない場合は、VLAN 単位の最大値が使用されます。</li> <li><code>access</code> アクセス ポートで、VLAN をアクセス VLAN として設定します。</li> <li><code>voice</code> アクセス ポートで、VLAN を音声 VLAN として設定します。</li> </ul> <p> <b>(注)</b> <code>voice</code> キーワードは、音声 VLAN がポートに設定され、そのポートがアクセス VLAN でない場合のみ、使用できません。</p>

コマンド	目的
<b>ステップ 7</b> <code>switchport port-security violation {protect   restrict   shutdown}</code>	<p>(任意) 違反モード、セキュリティ違反検出時の対処方法を次のいずれかで設定します。</p> <ul style="list-style-type: none"> <li> <b>protect</b> ポートセキュア MAC アドレスの数がポートに許容された最大限度に達した場合、十分な数のセキュア MAC アドレスを削除して最大値以下にする、またはアドレスの最大許容数を増やすまで、不明の送信元アドレスを持つパケットは廃棄されます。セキュリティ違反の発生は通知されません。 </li> </ul> <p> <b>(注)</b> トランク ポートに <code>protect</code> モードを設定しないでください。ポートがその最大制限値に達していない場合でも、いずれかの VLAN が最大制限値に達すると、<code>protect</code> モードにより学習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に許容された限界に達した場合、十分な数のセキュア MAC アドレスを削除する、または許容されるアドレスの最大数を増やすまで、不明の送信元アドレスを持つパケットは廃棄されます。SNMP トラップが送信され、Syslog メッセージが記録され、違反カウンタが増加します。 </li> <li> <b>shutdown</b> 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エラーディセーブル状態になって、ポート LED が消灯します。SNMP トラップが送信され、Syslog メッセージが記録され、違反カウンタが増加します。 </li> </ul> <p> <b>(注)</b> セキュア ポートがエラーディセーブル状態になった場合は、<code>errdisable recovery cause psecure-violation</code> グローバル コンフィギュレーション コマンドを使用することにより、状態を変更できます。また、<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。</p>

コマンド	目的
<b>ステップ 8</b> <code>switchport port-security [mac-address mac-address [vlan {vlan-id / {access / voice}}]]</code>	<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してセキュア MAC アドレスの最大数を入力できます。最大数より少ないセキュア MAC アドレス数を設定すると、残りの MAC アドレスはダイナミックに学習されます。</p> <p> <b>(注)</b> このコマンドを入力したあとに固定学習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 アドレスが固定セキュア 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) <code>vlan</code> VLAN 単位の最大値を設定します。</p> <p><code>vlan</code> キーワードを入力したあと、次のオプションを 1 つ入力します。</p> <ul style="list-style-type: none"> <li>• <code>vlan-id</code> トランク ポートで、VLAN ID と MAC アドレスを指定できます。VLAN ID が指定されていない場合は、ネイティブ VLAN が使用されます。</li> <li>• <code>access</code> アクセス ポートで、VLAN をアクセス VLAN として設定します。</li> <li>• <code>voice</code> アクセス ポートで、VLAN を音声 VLAN として設定します。</li> </ul> <p> <b>(注)</b> <code>voice</code> キーワードは、音声 VLAN がポートに設定され、そのポートがアクセス VLAN でない場合のみ、使用できます。</p>
<b>ステップ 9</b> <code>switchport port-security mac-address sticky</code>	<p>(任意) インターフェイスで固定学習をイネーブルにします。</p>

## ■ ポートセキュリティの設定

ステップ	コマンド	目的
ステップ 10	<pre>switchport port-security mac-address sticky [mac-address   vlan {vlan-id / {access / voice}}]</pre>	<p>(任意) 固定セキュア MAC アドレスを入力します。必要に応じて、このコマンドを繰り返し入力します。セキュア MAC アドレス数を最大値より少なく設定する場合、残りの MAC アドレスはダイナミックに学習され、固定セキュア 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) このコマンドを入力する前に固定学習をイネーブルにしておかないと、エラーメッセージが表示され、固定セキュア MAC アドレスを入力できません。</p> <p>(任意) vlan VLAN 単位の最大値を設定します。</p> <p>vlan キーワードを入力したあと、次のオプションを 1 つ入力します。</p> <ul style="list-style-type: none"> <li>• <i>vlan-id</i> トランクポートで、VLAN ID と MAC アドレスを指定できます。VLAN ID が指定されていない場合は、ネイティブ VLAN が使用されます。</li> <li>• <i>access</i> アクセスポートで、VLAN をアクセス VLAN として設定します。</li> <li>• <i>voice</i> アクセスポートで、VLAN を音声 VLAN として設定します。</li> </ul> <p> (注) <i>voice</i> キーワードは、音声 VLAN がポートに設定され、そのポートがアクセス VLAN でない場合のみ、使用できません。</p>
ステップ 11	end	イネーブル 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。

インターフェイスをデフォルトの非セキュアポートに戻すには、**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。固定学習がイネーブルの場合にこのコマンドを入力すると、固定学習アドレスは実行コンフィギュレーション内に残りますが、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の 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。

固定学習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 コマンドを実行します。インターフェイスは固定セキュア 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。

アドレステーブルからスタティック セキュア MAC アドレスを削除するには、**clear port-security configured address mac-address** イネーブル EXEC コマンドを使用します。インターフェイスまたは VLAN 上の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** イネーブル EXEC コマンドを使用します。

アドレス テーブルからダイナミック セキュア MAC アドレスを削除するには、`clear port-security dynamic address mac-address` イネーブル EXEC コマンドを使用します。インターフェイスまたは VLAN 上の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` イネーブル EXEC コマンドを使用します。

アドレス テーブルから固定セキュア MAC アドレスを削除するには、`clear port-security sticky address mac-address` イネーブル EXEC コマンドを使用します。インターフェイスまたは VLAN 上のすべての固定アドレスを削除するには、`clear port-security sticky interface interface-id` イネーブル EXEC コマンドを使用します。

次に、ポートで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設定、スタティック セキュア MAC アドレスは設定なし、固定学習はイネーブルにします。

```
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、固定学習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 で、セキュア MAC アドレスの最大数を 8 に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、ポート上で固定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 に MAC アドレスを手動で設定し、セキュア アドレスの最大数の合計を 20 に設定する例を示します (うち 10 はデータ VLAN、10 は音声 VLAN 用です)。

```
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
```



## ポートセキュリティ エージングのイネーブル化と設定

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 種類のエージングがサポートされています。

- **absolute** ポートのセキュア アドレスは、指定のエージング タイムの経過後、削除されます。
- **inactivity** ポートのセキュア アドレスが削除されるのは、指定したエージング タイムの間、そのセキュア アドレスが非アクティブであった場合だけです。

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 ポートで PC の削除や追加を実行でき、ポートのセキュア アドレスの数を制限することもできます。また、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についても、ポート単位でイネーブルまたはディセーブルに設定できます。

ポートセキュリティのエージング タイムを設定するには、イネーブル 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>	ポートセキュリティの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。   (注) スイッチでは、固定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ません。
ステップ 3	<code>switchport port-security aging {static   time time   type {absolute   inactivity}}</code>	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するか、またはエージング タイムやタイプを設定します。  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、 <code>static</code> を入力します。  <code>time</code> 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。この値を 0 に設定すると、このポートのエージングはディセーブルになります。  <code>type</code> には、次のキーワードのいずれかを 1 つ選択します。 <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に設定します。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。</li> </ul>  (注) 絶対エージング タイムは、システム タイマーの順序に従って 1 分単位で異なる可能性があります。  <ul style="list-style-type: none"> <li>• <b>inactivity</b> エージングのタイプを非活動エージングに設定します。このポートのセキュア アドレスが期限切れになるのは、指定した時間中にセキュア ソース アドレスからのデータ トラフィックを受信しなかった場合だけです。</li> </ul>
ステップ 4	<code>end</code>	イネーブル EXEC モードに戻ります。
ステップ 5	<code>show port-security [interface interface-id] [address]</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。

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、非活動エージング タイプに対するエージング タイムを 2 分に設定して、このインターフェイス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
```

設定したコマンドを確認するには、`show port-security interface interface-id` イネーブル EXEC コマンドを入力します。

## ポートベースのトラフィック制御設定の表示

`show interfaces interface-id switchport` イネーブル EXEC コマンドを使用すると、(各種の特性の中から) インターフェイスのトラフィック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` イネーブル 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。

トラフィック制御情報を表示するには、表 22-4 に示す 1 つまたは複数のイネーブル EXEC コマンドを使用します。

表 22-4 トラフィック制御のステータスと設定表示用のコマンド

コマンド	目的
<code>show interfaces [interface-id] switchport</code>	すべてのスイッチング (非ルーティング) ポートまたは指定したポートについて、管理ステータスまたは動作ステータスを表示します (ポートブロッキング、ポート保護設定など)。
<code>show storm-control [interface-id] [broadcast   multicast   unicast]</code>	すべてのインターフェイスまたは指定したインターフェイスについて、指定したトラフィックタイプ (指定されていない場合はブロードキャストトラフィック) のストーム制御抑制レベルを表示します。
<code>show port-security [interface interface-id]</code>	スイッチまたは指定したインターフェイスのポートのセキュリティ設定を表示します。各インターフェイスのセキュア MAC アドレスの最大数、インターフェイスのセキュア MAC アドレス数、発生したセキュリティ違反数、違反モードなどが含まれます。
<code>show port-security [interface interface-id] address</code>	すべてのスイッチ インターフェイスまたは指定したインターフェイスについて、設定されたすべてのセキュア MAC アドレスと、各アドレスのエージング情報を表示します。
<code>show port-security [interface interface-id] vlan</code>	各 VLAN のセキュア MAC アドレスの最大許容数および VLAN 上のセキュア MAC アドレス数を表示します。