



# ポートベースのトラフィック制御の設定

この章では、Catalyst 3750 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。特に明記しないかぎり、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 スタックを意味します。



(注) この章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 \(p.21-2\)](#)
- [保護ポートの設定 \(p.21-6\)](#)
- [ポートブロッキングの設定 \(p.21-7\)](#)
- [ポートセキュリティの設定 \(p.21-8\)](#)
- [ポートベースのトラフィック制御設定の表示 \(p.21-17\)](#)

## 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 \(p.21-2\)](#)
- [ストーム制御のデフォルト設定 \(p.21-3\)](#)
- [ストーム制御のイネーブル化 \(p.21-3\)](#)

### ストーム制御の概要

ストーム制御は、LAN 上のスイッチ ポートが、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混乱しないようにします。LAN ストームは、パケットが LAN にフラッ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み出され、ネットワーク パフォーマンスが低下します。プロトコル スタックの実装やネットワーク構成でのエラーが、ストームの原因となります。

ストーム制御 (トラフィック抑制) は、一定時間にわたる着信トラフィック統計情報をモニタし、あらかじめ定義された抑制スレッシュホールドと計測値を比較します。このスレッシュホールドは、ポートで利用可能な総帯域幅に対する割合を表します。スイッチは、ブロードキャスト、マルチキャスト、およびユニキャスト トラフィックのストーム制御スレッシュホールドを個別にサポートします。あるトラフィック タイプがスレッシュホールドに達すると、着信トラフィックがスレッシュホールド レベルを下回るまで、そのタイプのトラフィックは抑制されます。



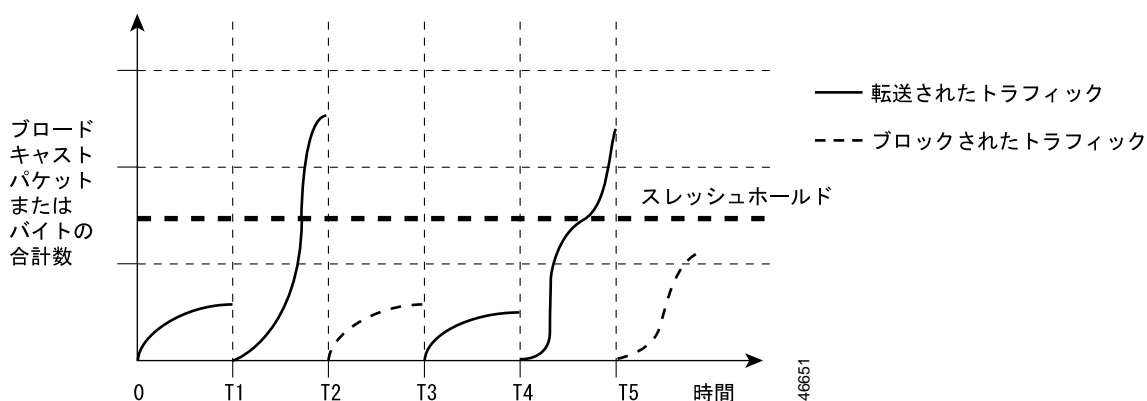
(注)

マルチキャスト トラフィックのストーム制御スレッシュホールドに達すると、Bridge Protocol Data Unit (BPDU; ブリッジ プロトコル データ ユニット) や Cisco Discovery Protocol (CDP) フレームなどの制御トラフィックを除いて、すべてのマルチキャスト トラフィックがブロックされます。ただし、スイッチでは Open Shortest Path First (OSPF) などの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。

ストーム制御がイネーブルの場合、スイッチ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、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、受信したユニキャスト、マルチキャスト、またはブロードキャストの数を 200 ミリ秒以内のタイム インターバルでモニタし、あるタイプのトラフィックがスレッシュホールドに達すると、そのタイプのトラフィックを廃棄します。このスレッシュホールドは、ブロードキャスト (マルチキャストまたはユニキャスト) トラフィックが利用可能な総帯域幅に対する割合として指定します。

[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 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 200 ミリ秒のタイム 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。スレッシュホールドの値が 100% であれば、トラフィックに対する制限はありません。値が 0.0 であれば、ポート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すべてブロックされます。



(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 200 ミリ秒のタイム 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。

スイッチは、ポートのトラフィックを引き続きモニタし、利用率がスレッシュホールド レベルを下回ると、廃棄されていたトラフィック タイプの転送を再開します。

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) 抑制レベルを設定するための **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 コマンドは、CLI (コマンドライン インターフェイス) オンライン ヘルプに表示されていますが、使用できません。上記のコマンドは廃止され、**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、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)。

## ストーム制御のイネーブル化

インターフェイスのストーム制御をイネーブルにして、利用可能な総帯域幅のうち、特定タイプのトラフィックに使用する割合を入力します。100% と入力するとすべてのトラフィックが許可されます。ただし、ハードウェアの制約や、さまざまなサイズの packets 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。



(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 チャネルでは、CLI でコマンドが利用できても、サポートはされません。

特定タイプのストーム制御をイネーブルにするには、イネーブル EXEC モードで次の手順を実行します。

	コマンド	説明
ステップ 1	<b><i>configure terminal</i></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><i>interface interface-id</i></b>	インターフェイス コンフィギュレーション モードを開始し、設定する物理インターフェイスのタイプおよび番号を入力します。
ステップ 3	<b><i>storm-control broadcast level level [.level]</i></b>	インターフェイスのブロードキャスト トラフィック抑制レベルを総帯域幅に対する割合として指定します。指定できるレベルの範囲は 1 ~ 100 です。オプションで、レベルの小数部を 0 ~ 99 の範囲で指定できます。スレッシュホールド値が 100% であれば、ブロードキャスト トラフィックに対する制限はありません。0.0 の値は、ポートのすべてのブロードキャスト トラフィックがブロックされるということです。
ステップ 4	<b><i>storm-control multicast level level [.level]</i></b>	インターフェイスのマルチキャスト トラフィック抑制レベルを総帯域幅に対する割合として指定します。指定できるレベルの範囲は 1 ~ 100 です。オプションで、レベルの小数部を 0 ~ 99 の範囲で指定できます。スレッシュホールド値が 100% であれば、マルチキャスト トラフィックに対する制限はありません。0.0 の値は、ポートのすべてのマルチキャスト トラフィックがブロックされるということです。
ステップ 5	<b><i>storm-control unicast level level [.level]</i></b>	インターフェイスのユニキャスト トラフィック抑制レベルを総帯域幅に対する割合として指定します。指定できるレベルの範囲は 1 ~ 100 です。オプションで、レベルの小数部を 0 ~ 99 の範囲で指定できます。スレッシュホールド値が 100% であれば、ユニキャスト トラフィックに対する制限はありません。0.0 の値は、ポートのすべてのユニキャスト トラフィックがブロックされるということです。
ステップ 6	<b><i>end</i></b>	イネーブル EXEC モードに戻ります。
ステップ 7	<b><i>show storm-control [interface-id] [broadcast   multicast   unicast]</i></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す。
ステップ 8	<b><i>copy running-config startup-config</i></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 level***、***no storm-control multicast level***、または ***no storm-control 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、ポート上でマルチキャスト ストーム制御レベルを 70.5% に設定し、その設定を確認する方法を示します。

```
Switch# configure terminal
Switch(config)# interface gigabitethernet2/0/1
Switch(config-if)# storm-control multicast level 70.5
Switch(config-if)# end
Switch# show storm-control gigabitethernet2/0/1 multicast
Interface  Filter State    Level    Current
-----  -
Gi2/0/1   Forwarding  70.50%  0.00%
```

次に、ポート上でマルチキャスト ストーム制御をディセーブルにする方法を示します。

```
Switch# configure terminal
Switch(config)# interface gigabitethernet2/0/1
Switch(config-if)# no storm-control multicast level
Switch(config-if)# end
```

## 保護ポートの設定

一部のアプリケーションでは、同一スイッチ上のポート間でトラフィックがレイヤ 2 で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、他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。データトラフィックは、レイヤ 2 の保護ポートの間では転送できません。PIM パケットは CPU によって処理されソフトウェアで転送されるので、制御トラフィック（PIM パケットなど）のみが転送されます。したがって、保護ポート間を通過するすべてのトラフィックは、レイヤ 3 デバイスを経由して転送する必要があります。
- 保護ポートと非保護ポート間の転送動作は、通常どおり行われます。

スイッチスタックは単一の論理スイッチを表すため、スイッチスタック内の保護ポート間では、これらのポートがスタック内の同じスイッチ上にあるか、異なるスイッチ上にあるかに関係なく、レイヤ 2 トラフィックは転送されません。

## 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ていません。

## 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（ギガビットイーサネットポート 1 など）または EtherChannel グループ（port-channel 5 など）のいずれにも設定できます。特定の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で保護ポートがイネーブルになります。

## 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、イネーブル EXEC モードで次の手順を実行します。

	コマンド	説明
ステップ 1	<b><i>configure terminal</i></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><i>interface interface-id</i></b>	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のタイプと番号を入力します（例： <i>gigabitethernet1/0/1</i> ）。
ステップ 3	<b><i>switchport protected</i></b>	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	<b><i>end</i></b>	イネーブル EXEC モードに戻ります。
ステップ 5	<b><i>show interfaces interface-id switchport</i></b>	設定を確認します。
ステップ 6	<b><i>copy running-config startup-config</i></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。

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、宛先 MAC アドレスが不明のパケットは、すべてのポートから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が他のポートにフラッディングされないようにポート（保護ポートまたは非保護ポート）をブロックできます。

### ポート ブロッキングのデフォルト設定

デフォルトでは、ポートから送信される不明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はブロックされません。これらのトラフィックは、すべてのポートに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) インターフェイスは物理インターフェイスまたは EtherChannel グループに設定できます。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。

インターフェイスから送信される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	説明
ステップ 1	<b><i>configure terminal</i></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><i>interface interface-id</i></b>	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のタイプおよび番号を入力します。
ステップ 3	<b><i>switchport block multicast</i></b>	ポートから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	<b><i>switchport block unicast</i></b>	ポートから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	<b><i>end</i></b>	イネーブル EXEC モードに戻ります。
ステップ 6	<b><i>show interfaces interface-id switchport</i></b>	設定を確認します。
ステップ 7	<b><i>copy running-config startup-config</i></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。

トラフィックがブロックされず、ポート上で標準転送が行われるデフォルト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 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、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。セキュア MAC アドレスを 1 つに制限し、1 つだけ割り当てると、そのポートに接続されたワークステーションでは、ポートの全帯域幅が保証されます。

セキュア ポートとして設定されたポートのセキュア MAC アドレスが最大数に達した場合に、ポートにアクセスしようとするステーションの MAC アドレスが、識別されたどのセキュア MAC アドレスとも異なるときは、セキュリティ違反が発生します。また、あるセキュア ポートで設定または学習されたセキュア MAC アドレスを持つステーションが別のセキュア ポートにアクセスしようすると、違反のフラグが立てられます。

ここでは、ポートセキュリティの設定および手順について説明します。

- [ポートセキュリティの概要 \(p.21-8\)](#)
- [ポートセキュリティのデフォルト設定 \(p.21-10\)](#)
- [設定時の注意事項 \(p.21-10\)](#)
- [ポートセキュリティのイネーブル化と設定 \(p.21-11\)](#)
- [ポートセキュリティ エージングのイネーブル化と設定 \(p.21-14\)](#)
- [ポートセキュリティおよびスイッチ スタック \(p.21-16\)](#)

## 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 \(p.21-8\)](#)
- [セキュリティ違反 \(p.21-9\)](#)

## セキュア MAC アドレス

1 つの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) インターフェイスにすでに設定されているセキュア アドレス数よりも小さい値を最大値に設定しようとする、コマンドは拒否されます。

スイッチは、次のタイプのセキュア MAC アドレスをサポートします。

- **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** 動的に設定されます。これらはアドレス テーブルにのみ格納され、スイッチが再起動するときに削除されます。
- **固定セキュア MAC アドレス** 動的に学習されるか、または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、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、スイッチを再起動するときに、インターフェイスがアドレスを動的に再設定する必要はありません。

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することができます。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動的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。すべての固定セキュア MAC アドレスが、実行コンフィギュレーションに追加されます。

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はありません。固定セキュア アドレスは、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、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 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「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

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限度以下にするか、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 ポートには `protect` 違反モードを設定しないでください。保護モードを使用すると、ポートが最大限度に達していない場合でも、VLAN が最大限度に達すると、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限度以下にするか、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。このモードでは、セキュリティ違反が起こった場合、ユーザに通知されます。SNMP トラップが送信され、Syslog メッセージが記録されて、違反カウンタが増加します。
- **shutdown** 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 **errdisable** ステートになって、ただちにシャットダウンし、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て、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変更することができます。また、**shutdown** および **no shut down** 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、ポートを手動で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 21-1 に、違反モード、およびポートセキュリティのインターフェイスを設定した場合の動作を示します。

表 21-1 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. 送信元アドレスが不明なパケットは、十分な数のセキュア MAC アドレスが削除されるまで、廃棄されます。

2. 手動で設定したアドレスがセキュリティ違反の原因となる場合には、エラー メッセージが表示されます。

## ポートセキュリティのデフォルト設定

表 21-2 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 21-2 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	ポートでディセーブル
固定アドレス学習	ディセーブル
ポート単位のセキュア MAC アドレスの最大数	1
違反モード	shutdown。セキュア MAC アドレスの最大数を超過すると、ポートはシャットダウンします。
ポートセキュリティのエージング	ディセーブルエージング タイムは 0 です。 スタティック エージングはディセーブルです。 タイプは absolute です。

## 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。
- 音声 VLAN では、スタティックセキュア MAC アドレスまたは固定セキュア MAC アドレスを設定できません。





(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。



- 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、さらに音声 VLAN を使用するようにも設定する場合は、ポートで許可されるセキュアアドレスの最大数を、アクセス VLAN で許可されているセキュアアドレスの最大数に 2 を加えた値に設定する必要があります。ポートが Cisco IP Phone に接続されている場合は、IP Phone に MAC アドレスが最大で 2 つ必要です。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。
- アクセス VLAN 上でいずれかのタイプのポートセキュリティがイネーブルの場合は、音声 VLAN 上でダイナミックポートセキュリティが自動的にイネーブルになります。VLAN 単位でポートセキュリティを設定することはできません。
- 固定セキュアポートとして設定されたセキュアポートに音声 VLAN が設定されている場合、音声 VLAN のすべてのアドレスはダイナミックセキュアアドレスとして学習されます。また、ポートが属するアクセス VLAN で認識されるすべてのアドレスは、固定セキュアアドレスとして学習されます。
- 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は、新しい値が古い設定値よりも優先します。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。

## 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	説明
ステップ 1	<b><i>configure terminal</i></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><i>interface interface-id</i></b>	インターフェイス コンフィギュレーション モードを開始し、設定する物理インターフェイスを入力します。
ステップ 3	<b><i>switchport mode {access / trunk}</i></b>	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	<b><i>switchport port-security</i></b>	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	説明
ステップ 5	<b>switchport port-security maximum value</b> [vlan [vlan-list]]	<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。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「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。</p> <p>(任意) トランク ポートの場合は、VLAN にセキュア MAC アドレスの最大数を設定できます。vlan キーワードを入力しない場合は、デフォルト値が使用されます。</p> <ul style="list-style-type: none"> <li>• <b>vlan</b> VLAN 単位の最大値を設定します。</li> <li>• <b>vlan vlan-list</b> 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します。指定されない VLAN については、VLAN 単位の最大値が使用されます。</li> </ul>
ステップ 6	<b>switchport port-security violation</b> {protect / restrict / shutdown}	<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> セキュア MAC アドレスの数がポートの最大許容値に達した場合、十分な数のセキュア MAC アドレスを削除して最大限度以下にするか、または使用可能な最大アドレス数を増加させるまで、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 ポートには protect モードを設定しないでください。保護モードを使用すると、ポートが最大限度に達していない場合でも、VLAN が最大限度に達すると、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の許容限度に達した場合、十分な数のセキュア MAC アドレスを削除するか、またはアドレスの最大許容数を増加させるまで、不明の送信元アドレスを持つパケットは廃棄されます。SNMP トラップが送信され、Syslog メッセージが記録されて、違反カウンタが増加します。</li> <li>• <b>shutdown</b> セキュリティ違反が発生すると、インターフェイスが errdisable ステートになり、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て、違反カウンタが増加します。</li> </ul> <p> (注) セキュア ポートが errdisable ステートになった場合は、<b>errdisable recovery cause psecure-violation</b> 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、<b>shutdown</b> および <b>no shut down</b> 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	説明
ステップ 7	<b><i>switchport port-security mac-address mac-address [vlan vlan-id]</i></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 アドレスは動的に学習されます。</p> <p>(任意) 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 を指定しないと、ネイティブ VLAN が使用されます。</p> <p> (注) 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、動的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>
ステップ 8	<b><i>switchport port-security mac-address sticky</i></b>	(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。
ステップ 9	<b><i>switchport port-security mac-address sticky mac-address</i></b>	<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。設定したセキュア MAC アドレス数が最大値より小さい場合、残りの MAC アドレスは動的に学習され、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>
ステップ 10	<b><i>end</i></b>	イネーブル EXEC モードに戻ります。
ステップ 11	<b><i>show port-security</i></b>	設定を確認します。
ステップ 12	<b><i>copy running-config startup-config</i></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。

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の 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。

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。ただし、固定 MAC アドレスを含む設定がすでに保存されている場合は、***no switchport port-security mac-address sticky*** コマンドを入力したあとに再び設定を保存する必要があります。保存しない場合スイッチを再起動すると固定アドレスが復元されます。

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。

アドレステーブルから特定のインターフェイスに関するダイナミックセキュアアドレスを削除するには、**no switchport port-security** インターフェイス コンフィギュレーション コマンドのあとに、**switchport port-security** コマンドを入力して、インターフェイスのポートセキュリティをイネーブルに戻します。**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、固定セキュア MAC アドレスをダイナミックセキュア MAC アドレスに変換してから、**no switchport port-security** コマンドを入力すると、手動で設定されたセキュアアドレスを除き、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。

**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 コマンドを使用して、アドレステーブルから設定済みのセキュア MAC アドレスを削除する必要があります。

次に、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(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 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
```

## 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、ポート上の全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、セキュアポートでデバイスの削除や追加を実行でき、しかもポートのセキュアアドレスの数を制限することができます。また、セキュアアドレスのエージングをポート単位でイネーブルまたはディセーブルに設定することができます。

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	説明
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>	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について、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	説明
ステップ 3	<b>switchport port-security aging</b> { <i>static</i> / <i>time time</i>   <i>type</i> { <i>absolute</i> / <i>inactivity</i> } }	<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。</p> <p> (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。</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ルにする場合は、<b>static</b> を入力します。</p> <p><b>time</b> 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。</p> <p><b>type</b> には、次のキーワードのいずれかを 1 つ選択します。</p> <ul style="list-style-type: none"> <li>• <b>absolute</b> エージングタイプを absolute 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> <li>• <b>inactivity</b> エージングのタイプを inactivity 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送信元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	<b>end</b>	イネーブル EXEC モードに戻ります。
ステップ 5	<b>show port-security</b> [ <i>interface interface-id</i> ] [ <i>address</i> ]	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 アドレスのエージングをイネーブルにし、エージング タイプを inactivity に、エージング タイムを 2 分に設定する例を示します。

```
Switch(config-if)# switchport port-security aging time 2
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。

## ポートセキュリティおよびスイッチ 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 メンバーのいずれか)がスタックから脱退すると、残りのスタック メンバーに通知されて、そのスイッチによって設定または学習されたセキュア 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 5 章「スイッチ スタックの管理」](#)を参照してください。

## 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、(各種の特性とともに) 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 interfaces counters** イネーブル EXEC コマンドを使用すると、廃棄されたパケット数が表示されます。**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 21-3 に示すイネーブル EXEC コマンドを 1 つまたは複数使用します。

表 21-3 トラフィック制御のステータスおよび設定表示用のコマンド

コマンド	説明
<b>show interfaces [interface-id] 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)。
<b>show storm-control [interface-id] [broadcast   multicast   unicast]</b>	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。
<b>show interfaces [interface-id] counters broadcast</b>	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、廃棄されたパケットの数を示す、ストーム制御ブロードキャスト抑制廃棄カウンタを表示します。
<b>show interfaces [interface-id] counters multicast</b>	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、廃棄されたパケットの数を示す、ストーム制御マルチキャスト抑制廃棄カウンタを表示します。
<b>show interfaces [interface-id] counters unicast</b>	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、廃棄されたパケットの数を示す、ストーム制御ユニキャスト抑制廃棄カウンタを表示します。
<b>show port-security [interface interface-id]</b>	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。
<b>show port-security [interface interface-id] address</b>	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。
<b>show port-security interface interface-id vlan</b>	指定したインターフェイスの VLAN ごとに設定されたセキュア MAC アドレス数を表示します。

