



## ポート単位のトラフィック制御の設定

- [ポートベースのトラフィック制御の概要 \(1 ページ\)](#)
- [機能情報の確認 \(2 ページ\)](#)
- [ストーム制御に関する情報 \(2 ページ\)](#)
- [ストーム制御の設定方法 \(4 ページ\)](#)
- [保護ポートに関する情報 \(9 ページ\)](#)
- [保護ポートの設定方法 \(10 ページ\)](#)
- [保護ポートの監視 \(12 ページ\)](#)
- [ポートブロッキングに関する情報 \(12 ページ\)](#)
- [ポートブロッキングの設定方法 \(12 ページ\)](#)
- [ポートブロッキングの監視 \(14 ページ\)](#)
- [ポートセキュリティの前提条件 \(14 ページ\)](#)
- [ポートセキュリティの制約事項 \(14 ページ\)](#)
- [ポートセキュリティの概要 \(15 ページ\)](#)
- [ポートセキュリティの設定方法 \(21 ページ\)](#)
- [ポートセキュリティの設定例 \(45 ページ\)](#)

## ポートベースのトラフィック制御の概要

ポートベースのトラフィック制御は、特定トラフィック状態に応じてポートレベルでパケットをフィルタまたはブロックするために使用する Cisco Catalyst スイッチ上のレイヤ 2 機能の組み合わせです。次のポートベースのトラフィック制御機能が、このガイドの記述対象の Cisco IOS リリースでサポートされます。

- Storm Control
- 保護ポート
- ポートブロッキング
- ポートセキュリティ
- プロトコルストームプロテクション

## 機能情報の確認

ご使用のソフトウェアリリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報および警告については、使用するプラットフォームおよびソフトウェアリリースの Bug Search Tool およびリリース ノートを参照してください。このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このモジュールの最後にある機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator には、<http://www.cisco.com/go/cfn> からアクセスします。Cisco.com のアカウントは必要ありません。

## ストーム制御に関する情報

### Storm Control

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 コントロール（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。

## トラフィック アクティビティの測定方法

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
- 秒単位で受信するビット（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。

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

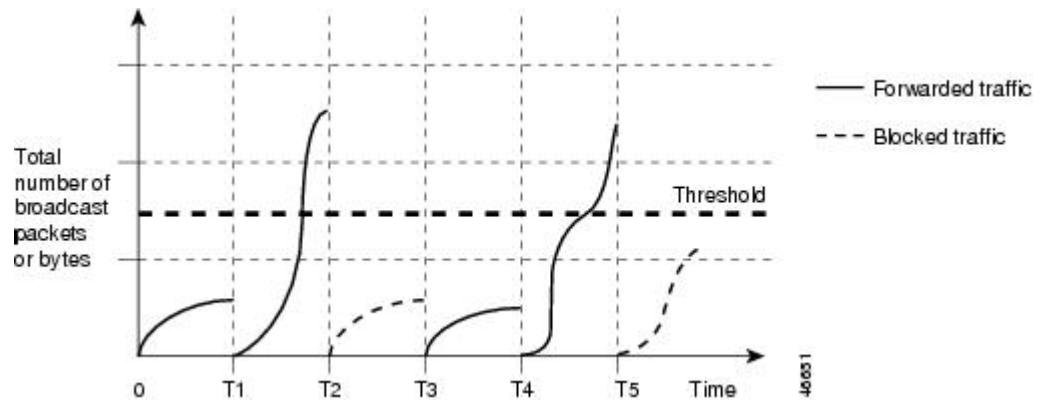


- (注) マルチキャストトラフィックのストーム制御しきい値に達した場合、ブリッジプロトコルデータユニット (BPDU) および Cisco Discovery Protocol (CDP) フレームなどの制御トラフィック以外のマルチキャストトラフィックはすべてブロックされます。ただし、スイッチでは Open Shortest Path First (OSPF) などのルーティングアップデートと、正規のマルチキャストデータトラフィックは区別されないため、両方のトラフィックタイプがブロックされます。

## トラフィックパターン

図 1: ブロードキャストストーム制御の例

次の例は、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。



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。

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ると、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。

## ストーム制御の設定方法

### 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 packets 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 packets 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、次の手順を実行します。

#### 始める前に

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。

#### 手順

	コマンドまたはアクション	目的
ステップ 1	<b>enable</b> 例： Device> <b>enable</b>	特権 EXEC モードをイネーブルにします。 <ul style="list-style-type: none"> <li>パスワードを入力します（要求された場合）。</li> </ul>

	コマンドまたはアクション	目的
ステップ 2	<b>configureterminal</b> 例 : Device# <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 3	<b>interface interface-id</b> 例 : Device(config)# <b>interface gigabitethernet1/0/1</b>	設定するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	<b>storm-control {broadcast   multicast   unicast} level {level [level-low]   bps bps [bps-low]   pps pps [pps-low]}</b> 例 : Device(config-if)# <b>storm-control unicast level 87 65</b>	<p>ブロードキャスト、マルチキャスト、またはユニキャスト ストーム制御を設定します。デフォルトでは、ストーム制御はディセーブルに設定されています。</p> <p>キーワードの意味は次のとおりです。</p> <ul style="list-style-type: none"> <li>• <b>level</b> には、ブロードキャスト、マルチキャスト、またはユニキャストトラフィックの上限しきい値レベルを帯域幅のパーセンテージで指定します (小数点第2位まで)。上限しきい値に到達すると、ポートはトラフィックをブロックします。指定できる範囲は 0.00 ~ 100.00 です。</li> <li>• (任意) <b>level-low</b> 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。</li> </ul> <p>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。</p>

	コマンドまたはアクション	目的
		<ul style="list-style-type: none"> <li>• <b>bps</b> <i>bps</i> には、ブロードキャスト、マルチキャスト、またはユニキャストトラフィックの上限しきい値レベルをビット/秒で指定します（小数点第1位まで）。上限しきい値に到達すると、ポートはトラフィックをブロックします。指定できる範囲は 0.0 ~ 10000000000.0 です。</li> <li>• (任意) <i>bps-low</i> には、下限しきい値レベルをビット/秒で指定します（小数点第1位まで）。この値は上限しきい値レベル以下の値である必要があります。トラフィックがこのレベルを下回っていれば、ポートはトラフィックを転送します。指定できる範囲は 0.0 ~ 10000000000.0 です。</li> <li>• <b>pps</b> <i>pps</i> には、ブロードキャスト、マルチキャスト、またはユニキャストトラフィックの上限しきい値レベルをパケット/秒で指定します（小数点第1位まで）。上限しきい値に到達すると、ポートはトラフィックをブロックします。指定できる範囲は 0.0 ~ 10000000000.0 です。</li> <li>• (任意) <i>pps-low</i> には、下限しきい値レベルをパケット/秒で指定します（小数点第1位まで）。この値は上限しきい値レベル以下の値である必要があります。トラフィックがこのレベルを下回っていれば、ポートはトラフィックを転送します。指定できる範囲は <b>0.0</b> ~ 10000000000.0 です。</li> </ul> <p>BPS および PPS の設定には、しきい値の数値を大きく設定できるように、サフィックスに測定記号 (k、m、g など) を使用できます。</p>
ステップ 5	<b>storm-control action {shutdown   trap}</b> 例 :	ストーム検出時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

	コマンドまたはアクション	目的
	Device (config-if) # <b>storm-control action trap</b>	<p>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。</p> <ul style="list-style-type: none"> <li>• ストーム中、ポートを <b>error-disable</b> の状態にするには、<b>shutdown</b> キーワードを選択します。</li> <li>• ストームが検出された場合、SNMP（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、<b>trap</b> キーワードを選択します。</li> </ul>
ステップ 6	<b>end</b> 例： Device (config-if) # <b>end</b>	特権 EXEC モードに戻ります。
ステップ 7	<b>show storm-control [interface-id] [broadcast   multicast   unicast]</b> 例： Device# <b>show storm-control gigabitethernet1/0/1 unicast</b>	指定したトラフィックタイプについて、インターフェイスで設定したストーム制御抑制レベルを確認します。トラフィックタイプを入力しなかった場合は、ブロードキャストストーム制御の設定が表示されます。
ステップ 8	<b>copy running-config startup-config</b> 例： Device# <b>copy running-config startup-config</b>	(任意) コンフィギュレーションファイルに設定を保存します。

## スモール 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。

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。

## 手順

	コマンドまたはアクション	目的
ステップ 1	<b>enable</b> 例：  Device> <b>enable</b>	特権 EXEC モードをイネーブルにします。  • パスワードを入力します（要求された場合）。
ステップ 2	<b>configureterminal</b> 例：  Device# <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 3	<b>errdisable detect cause small-frame</b> 例：  Device(config)# <b>errdisable detect cause small-frame</b>	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 4	<b>errdisable recovery interval</b> 間隔 例：  Device(config)# <b>errdisable recovery interval 60</b>	（任意）指定された <b>errdisable</b> ステートから回復する時間を指定します。
ステップ 5	<b>errdisable recovery cause small-frame</b> 例：  Device(config)# <b>errdisable recovery cause small-frame</b>	（任意）小さいフレームの着信によりポートが <b>errdisable</b> 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。
ステップ 6	<b>interface interface-id</b> 例：  Device(config)# <b>interface gigabitethernet1/0/2</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を指定します。



	コマンドまたはアクション	目的
ステップ 7	<b>small-frame violation-rate pps</b> 例：  Device(config-if)# <b>small-frame violation rate 10000</b>	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 パケット/秒 (pps) です。
ステップ 8	<b>end</b> 例：  Device(config)# <b>end</b>	特権 EXEC モードに戻ります。
ステップ 9	<b>show interfaces interface-id</b> 例：  Device# <b>show interfaces gigabitethernet1/0/2</b>	設定を確認します。
ステップ 10	<b>show running-config</b> 例：  Device# <b>show running-config</b>	入力を確認します。
ステップ 11	<b>copy running-config startup-config</b> 例：  Device# <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。

## 保護ポートに関する情報

### 保護ポート

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。

## 保護ポートのデフォルト設定

デフォルトでは、保護ポートは定義されません。

## 保護ポートのガイドライン

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。ポートチャンネルで保護ポートをイネーブルにした場合は、そのポートチャン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。

## 保護ポートの設定方法

### 保護ポートの設定

始める前に

保護ポートは事前定義されていません。これは設定する必要があるタスクです。

手順

	コマンドまたはアクション	目的
ステップ 1	<b>enable</b> 例：  Device> <b>enable</b>	特権 EXEC モードをイネーブルにします。  • パスワードを入力します（要求された場合）。
ステップ 2	<b>configureterminal</b> 例：	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。

	コマンドまたはアクション	目的
	Device# <code>configure terminal</code>	
ステップ 3	<b>interface <i>interface-id</i></b> 例 :  Device(config)# <b>interface</b> <b>gigabitethernet1/0/1</b>	設定するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	<b>switchport protected</b> 例 :  Device(config-if)# <b>switchport protected</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 5	<b>end</b> 例 :  Device(config)# <b>end</b>	特権 EXEC モードに戻ります。
ステップ 6	<b>show interfaces <i>interface-id</i> switchport</b> 例 :  Device# <b>show interfaces</b> <b>gigabitethernet1/0/1 switchport</b>	入力を確認します。
ステップ 7	<b>show running-config</b> 例 :  Device# <b>show running-config</b>	入力を確認します。
ステップ 8	<b>copy running-config startup-config</b> 例 :  Device# <b>copy running-config</b> <b>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。

## 保護ポートの監視

表 1: 保護ポートの設定を表示するコマンド

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。

## ポートブロッキングに関する情報

### ポートブロッキング

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。

## ポートブロッキングの設定方法

### 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

#### 始める前に

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。

## 手順

	コマンドまたはアクション	目的
ステップ 1	<b>enable</b> 例：  Device> <b>enable</b>	特権 EXEC モードをイネーブルにします。  • パスワードを入力します（要求された場合）。
ステップ 2	<b>configureterminal</b> 例：  Device# <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 3	<b>interface interface-id</b> 例：  Device(config)# <b>interface gigabitethernet1/0/1</b>	設定するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	<b>switchport block multicast</b> 例：  Device(config-if)# <b>switchport block multicast</b>	ポートからの未知のマルチキャストの転送をブロックします。  (注) 純粋なレイヤ 2 マルチキャストトラフィックだけがブロックされます。ヘッダーに 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 5	<b>switchport block unicast</b> 例：  Device(config-if)# <b>switchport block unicast</b>	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 6	<b>end</b> 例：  Device(config)# <b>end</b>	特権 EXEC モードに戻ります。
ステップ 7	<b>show interfaces interface-id switchport</b> 例：  Device# <b>show interfaces</b>	入力を確認します。

	コマンドまたはアクション	目的
	<code>gigabitethernet1/0/1 switchport</code>	
ステップ 8	<b>show running-config</b> 例：  Device# <code>show running-config</code>	入力を確認します。
ステップ 9	<b>copy running-config startup-config</b> 例：  Device# <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。

## ポートブロッキングの監視

表 2: ポートブロッキングの設定を表示するコマンド

コマンド	目的
<b>show interfaces</b> <i>[interface-id]</i> <b>switchport</b>	すべてのスイッチング (非ルーティング) ポートまたは指定されたポートの管理ステータスまたは動作ステータスを、ポートブロッキングおよびポート保護の設定を含めて表示します。

## ポートセキュリティの前提条件



- (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、コマンドが拒否されます。

## ポートセキュリティの制約事項

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。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。

## ポートセキュリティの概要

### ポートセキュリティ

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

セキュアポートとしてポートを設定し、セキュアMACアドレスが最大数に達した場合、ポートにアクセスを試みるステーションのMACアドレスが識別されたセキュアMACアドレスのいずれとも一致しないので、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。

#### 関連トピック

[ポートセキュリティのイネーブル化および設定](#) (21 ページ)

[ポートセキュリティの設定例](#) (45 ページ)

### セキュアMACアドレスのタイプ

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。

### スティッキーセキュアMACアドレス

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。インターフェイスはスティッキー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ーセキュア MAC アドレスに変換します。すべてのスティッキーセキュア 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。

スティッキーセキュア MAC アドレスは、コンフィギュレーションファイル（スイッチが再起動されるたびに使用されるスタートアップコンフィギュレーション）に、自動的に反映されません。スティッキーセキュア 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。スティッキーセキュア アドレスを保存しない場合、アドレスは失われます。

スティッキーラーニングがディセーブルの場合、スティッキーセキュア 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 **error-disabled** 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 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。

次の表に、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 3: セキュリティ違反モードの処置

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

- <sup>1</sup> 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。
- <sup>2</sup> 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。
- <sup>3</sup> 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 エージング

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。

## 関連トピック

[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](#) (27 ページ)

## 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（アクティブスイッチまたはスタックメンバーのいずれか）がスタックから離れると、その他のスタックメンバーに通知が行き、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。

## デフォルトのポートセキュリティ設定

表 4: 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	ポート上でディセーブル
スティッキー 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	shutdown。セキュア MAC アドレスが最大数を上回ると、ポートがシャットダウンします。
ポートセキュリティ エージング	ディセーブルエージング タイムは 0 スタティック エージングはディセーブル タイプは absolute

## ポートセキュリティの設定時の注意事項

- ポートセキュリティを設定できるのは、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。



(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 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 に接続する場合は、MAC アドレスの追加は必要ありません。複数の PC を Cisco IP Phone に接続する場合は、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。

- 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。

次の表に、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 5: 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 <sup>4</sup> ポート <sup>5</sup>	なし
トランク ポート	Yes
ダイナミックアクセス ポート <sup>6</sup>	なし
ルーテッド ポート	なし
SPAN 送信元ポート	Yes
SPAN 宛先ポート	No
EtherChannel	Yes
トンネリング ポート	Yes

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
保護ポート	Yes
IEEE 802.1x ポート	Yes
音声 VLAN ポート <sup>7</sup>	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

<sup>4</sup> DTP = Dynamic Trunking Protocol

<sup>5</sup> **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。

<sup>6</sup> **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る Vlan Query Protocol (VQP) ポート。

<sup>7</sup> 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)。

## ポートベースのトラフィック制御の概要

ポートベースのトラフィック制御は、特定トラフィック状態に応じてポート レベルでパケットをフィルタまたはブロックするために使用する Cisco Catalyst スイッチ上のレイヤ 2 機能の組み合わせです。次のポートベースのトラフィック制御機能が、このガイドの記述対象の Cisco IOS リリースでサポートされます。

- Storm Control
- 保護ポート
- ポート ブロッキング
- ポート セキュリティ
- プロトコル ストーム プロテクション

# ポートセキュリティの設定方法

## ポートセキュリティのイネーブル化および設定

### 始める前に

このタスクは、ポートにアクセスできるステーションの 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約します。

### 手順

	コマンドまたはアクション	目的
ステップ 1	<b>enable</b> 例：  Device> <b>enable</b>	特権 EXEC モードをイネーブルにします。  • パスワードを入力します（要求された場合）。
ステップ 2	<b>configureterminal</b> 例：  Device# <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 3	<b>interface interface-id</b> 例：  Device(config)# <b>interface gigabitethernet1/0/1</b>	設定するインターフェイスを指定し、インターフェイス コンフィギュレーションモードを開始します。
ステップ 4	<b>switchport mode {access   trunk}</b> 例：  Device(config-if)# <b>switchport mode access</b>	インターフェイススイッチポートモードを <b>access</b> または <b>trunk</b> 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 5	<b>switchport voice vlan vlan-id</b> 例：  Device(config-if)# <b>switchport voice vlan 22</b>	ポート上で音声 VLAN をイネーブルにします。  vlan-id : 音声トラフィックに使用する VLAN を指定します。

	コマンドまたはアクション	目的
ステップ 6	<b>switchport port-security</b> 例 : Device(config-if) # <b>switchport port-security</b>	インターフェイス上でポートセキュリティをイネーブルにします。
ステップ 7	<b>switchport port-security [maximum value [vlan {vlan-list   {access   voice}}]]</b> 例 : Device(config-if) # <b>switchport port-security maximum 20</b>	<p>(任意) インターフェイスの最大セキュア MAC アドレス数を設定します。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。この値は、アクティブな SDM テンプレートによって決まります。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) <b>vlan</b> : VLAN 当たりの最大値を設定します。</p> <p><b>vlan</b> キーワードを入力後、次のいずれかのオプションを入力します。</p> <ul style="list-style-type: none"> <li>• <b>vlan-list</b> : トランクポート上で、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。</li> <li>• <b>access</b> : アクセスポート上で、アクセス VLAN として VLAN を指定します。</li> <li>• <b>voice</b> : アクセスポート上で、音声 VLAN として VLAN を指定します。</li> </ul>

	コマンドまたはアクション	目的
		<p>(注) <b>voice</b> 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。</p>
<p>ステップ 8</p>	<p><b>switchport port-security violation {protect   restrict   shutdown   shutdown vlan}</b></p> <p>例 :</p> <pre>Device (config-if) # switchport port-security violation restrict</pre>	<p>(任意) 違反モードを設定します。セキュリティ違反が発生した場合に、次のいずれかのアクションを実行します。</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で許可されている最大限度に達すると、最大値を下回るまで十分な数のセキュア MAC アドレスを削除するか、許可アドレス数を増やさない限り、未知の送信元アドレスを持つパケットはドロップされます。セキュリティ違反が起こっても、ユーザには通知されません。</li> </ul> <p>(注) トランクポート上に保護モードを設定することは推奨できません。保護モードでは、ポートが最大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。</p> <ul style="list-style-type: none"> <li>• <b>restrict</b> : セキュア MAC アドレス数がポートで許可されている最大数に到達した場合、不明な送信元アドレスのパケットはドロップされます。セキュア MAC アドレス数を上限よりも少なくするか、許容できるアドレスの最大数を増やさない限り、この状態が続きます。</li> </ul>

	コマンドまたはアクション	目的
		<p>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。</p> <ul style="list-style-type: none"> <li>• <b>shutdown</b> : 違反が発生すると、イ ンターフェイスが <b>error-disabled</b> 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。</li> <li>• <b>shutdown vlan</b> : 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 <b>errdisable</b> にな ります。</li> </ul> <p>(注) セキュア ポートが <b>error-disabled</b> ステートの 場合は、<b>errdisable recovery cause psecure-violation</b> グロー バル コンフィギュレー ションコマンドを入力し て、このステートから回 復させることができま す。手動で再びイネー ブルにするには、<b>shutdown</b> および <b>no shutdown</b> イン ターフェイス コンフィ ギュレーションコマンド を入力するか、<b>clear errdisable interface vlan</b> 特権 EXEC コマンドを入 力します。</p>
ステップ 9	<p><b>switchport port-security [mac-address mac-address [vlan {vlan-id   {access   voice}}]</b></p> <p>例 :</p> <p>Device(config-if)# <b>switchport</b></p>	<p>(任意) インターフェイスのセキュア MAC アドレスを入力します。このコ マンドを使用すると、最大数のセキュア MAC アドレスを入力できます。設定し たセキュア MAC アドレスが最大数よ</p>



	コマンドまたはアクション	目的
	<pre>port-security mac-address 00:A0:C7:12:C9:25 vlan 3 voice</pre>	<p>り少ない場合、残りの MAC アドレスは動的に学習されます。</p> <p>(注) このコマンドの入力後にスティッキー 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。</p> <p>(任意) <b>vlan</b> : VLAN 当たりの最大値を設定します。</p> <p><b>vlan</b> キーワードを入力後、次のいずれかのオプションを入力します。</p> <ul style="list-style-type: none"> <li>• <b>vlan-id</b> : 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。</li> <li>• <b>access</b> : アクセスポート上で、アクセス VLAN として VLAN を指定します。</li> <li>• <b>voice</b> : アクセスポート上で、音声 VLAN として VLAN を指定します。</li> </ul> <p>(注) <b>voice</b> キーワードは、音声 VLAN がポートに設定されていて、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。</p>
<p>ステップ 10</p>	<pre>switchport port-security mac-address sticky</pre> <p>例 :</p>	<p>(任意) インターフェイス上でスティッキーラーニングをイネーブルにします。</p>

	コマンドまたはアクション	目的
	<pre>Device(config-if)# switchport port-security mac-address sticky</pre>	
ステップ 11	<p><b>switchport port-security mac-address sticky</b> [<i>mac-address</i>   <b>vlan</b> {<i>vlan-id</i>   {<b>access</b>   <b>voice</b>}}]</p> <p>例 :</p> <pre>Device(config-if)# switchport port-security mac-address sticky 00:A0:C7:12:C9:25 vlan voice</pre>	<p>(任意) スティックキーセキュア 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。</p> <p>(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。</p> <p>(任意) <b>vlan</b> : VLAN 当たりの最大値を設定します。</p> <p><b>vlan</b> キーワードを入力後、次のいずれかのオプションを入力します。</p> <ul style="list-style-type: none"> <li>• <b>vlan-id</b> : 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。VLANID を指定しない場合、ネイティブ VLAN が使用されます。</li> <li>• <b>access</b> : アクセスポート上で、アクセス VLAN として VLAN を指定します。</li> <li>• <b>voice</b> : アクセスポート上で、音声 VLAN として VLAN を指定します。</li> </ul> <p>(注) <b>voice</b> キーワードは、音声 VLAN がポートに設定されていて、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。</p>

	コマンドまたはアクション	目的
ステップ 12	<b>end</b> 例： Device (config) # <b>end</b>	特権 EXEC モードに戻ります。
ステップ 13	<b>show port-security</b> 例： Device# <b>show port-security</b>	入力を確認します。
ステップ 14	<b>show running-config</b> 例： Device# <b>show running-config</b>	入力を確認します。
ステップ 15	<b>copy running-config startup-config</b> 例： Device# <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。

関連トピック

[ポートセキュリティ](#)

[ポートセキュリティ \(15 ページ\)](#)

[ポートセキュリティの設定例 \(45 ページ\)](#)

## 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

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。

手順

	コマンドまたはアクション	目的
ステップ 1	<b>enable</b> 例： Device> <b>enable</b>	特権 EXEC モードをイネーブルにします。  • パスワードを入力します (要求された場合)。

	コマンドまたはアクション	目的
ステップ 2	<b>configureterminal</b> 例 :  Device# <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 3	<b>interface interface-id</b> 例 :  Device(config)# <b>interface gigabitethernet1/0/1</b>	設定するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	<b>switchport port-security aging {static   time time   type {absolute   inactivity}}</b> 例 :  Device(config-if)# <b>switchport port-security aging time 120</b>	<p>セキュア ポートのスタティック エージングをイネーブ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。</p> <p>(注) スイッチは、ステイッキー 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。</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。有効な範囲は、0～1440 分です。</p> <p><b>type</b> には、次のキーワードのいずれか 1 つを選択します。</p> <ul style="list-style-type: none"> <li>• <b>absolute</b> : (任意) 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。</li> <li>• <b>inactivity</b> : (任意) 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 <b>time</b> 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</li> </ul>

	コマンドまたはアクション	目的
		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 5	<b>end</b> 例：  Device (config) # <b>end</b>	特権 EXEC モードに戻ります。
ステップ 6	<b>show port-security [interface interface-id] [address]</b> 例：  Device# <b>show port-security interface gigabitethernet1/0/1</b>	入力を確認します。
ステップ 7	<b>show running-config</b> 例：  Device# <b>show running-config</b>	入力を確認します。
ステップ 8	<b>copy running-config startup-config</b> 例：  Device# <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。

#### 関連トピック

[ポートセキュリティ エージング](#) (17 ページ)

## 機能情報の確認

ご使用のソフトウェアリリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報および警告については、使用するプラットフォームおよびソフトウェア リリースの [Bug Search Tool](#) およびリリース ノートを参照してください。このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このモジュールの最後にある機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、[Cisco Feature Navigator](#) を使用します。Cisco Feature Navigator には、<http://www.cisco.com/go/cfn> からアクセスします。Cisco.com のアカウントは必要ありません。

## ストーム制御に関する情報

### Storm Control

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。

ストームコントロール（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。

### トラフィック アクティビティの測定方法

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
- 秒単位で受信するビット（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。

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

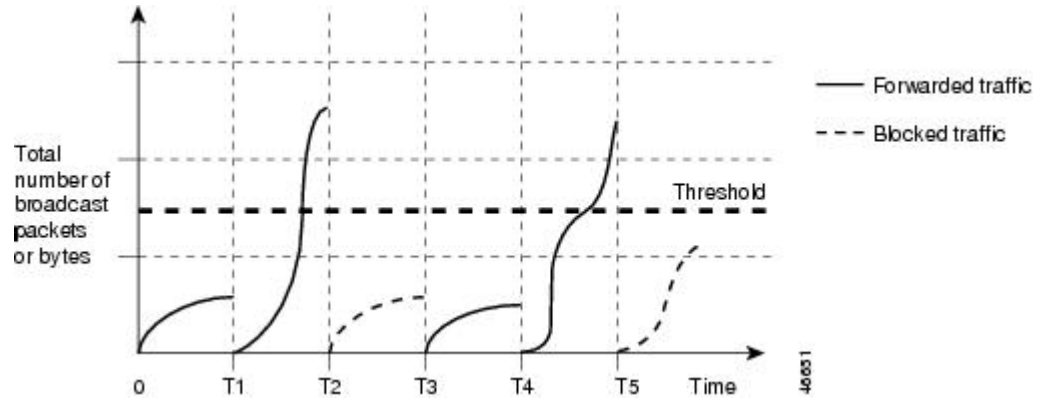


- (注) マルチキャストトラフィックのストーム制御しきい値に達した場合、ブリッジプロトコルデータ ユニット (BPDU) および Cisco Discovery Protocol (CDP) フレームなどの制御トラフィック以外のマルチキャストトラフィックはすべてブロックされます。ただし、スイッチでは Open Shortest Path First (OSPF) などのルーティング アップデートと、正規のマルチキャスト データトラフィックは区別されないため、両方のトラフィック タイプがブロックされます。

## トラフィック パターン

図 2: ブロードキャストストーム制御の例

次の例は、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。



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。

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ると、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。

## ストーム制御の設定方法

### 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 packets 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 packets 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、次の手順を実行します。

#### 始める前に

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。

#### 手順

	コマンドまたはアクション	目的
ステップ 1	<b>enable</b> 例：  Device> <b>enable</b>	特権 EXEC モードをイネーブルにします。  • パスワードを入力します（要求された場合）。
ステップ 2	<b>configureterminal</b> 例：  Device# <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 3	<b>interface interface-id</b> 例：  Device(config)# <b>interface gigabitethernet1/0/1</b>	設定するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	<b>storm-control {broadcast   multicast   unicast} level {level [level-low]   bps bps [bps-low]   pps pps [pps-low]}</b> 例：  Device(config-if)# <b>storm-control unicast level 87 65</b>	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。 キーワードの意味は次のとおりです。  • <i>level</i> には、ブロードキャスト、マルチキャスト、またはユニキャスト



	コマンドまたはアクション	目的
		<p>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。</p> <ul style="list-style-type: none"> <li>•（任意）<i>level-low</i>には、下限しきい値レベルを帯域幅のパーセンテージで指定します（小数点第2位まで）。この値は上限抑制値より小さいか、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。</li> </ul> <p>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。</p> <ul style="list-style-type: none"> <li>• <b>bps bps</b>には、ブロードキャスト、マルチキャスト、またはユニキャストトラフィックの上限しきい値レベルをビット/秒で指定します（小数点第1位まで）。上限しきい値に到達すると、ポートはトラフィックをブロックします。指定できる範囲は 0.0 ～ 10000000000.0 です。</li> <li>•（任意）<i>bps-low</i>には、下限しきい値レベルをビット/秒で指定します（小数点第1位まで）。この値は上限しきい値レベル以下の値である必要があります。トラフィックがこのレベルを下回っていれば、ポートはトラフィックを転送します。指定できる範囲は 0.0 ～ 10000000000.0 です。</li> </ul>

	コマンドまたはアクション	目的
		<ul style="list-style-type: none"> <li>• <b>pps pps</b> には、ブロードキャスト、マルチキャスト、またはユニキャストトラフィックの上限しきい値レベルをパケット/秒で指定します（小数点第1位まで）。上限しきい値に到達すると、ポートはトラフィックをブロックします。指定できる範囲は 0.0 ~ 10000000000.0 です。</li> <li>• (任意) <b>pps-low</b> 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 <b>0.0</b> ~ 10000000000.0 です。</li> </ul> <p>BPS および PPS の設定には、しきい値の数値を大きく設定できるように、サフィックスに測定記号 (k、m、g など) を使用できます。</p>
ステップ 5	<b>storm-control action {shutdown   trap}</b> 例 : <pre>Device(config-if)# storm-control action trap</pre>	<p>ストーム検出時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。</p> <ul style="list-style-type: none"> <li>• ストーム中、ポートを <b>error-disable</b> の状態にするには、<b>shutdown</b> キーワードを選択します。</li> <li>• ストームが検出された場合、SNMP（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、<b>trap</b> キーワードを選択します。</li> </ul>
ステップ 6	<b>end</b> 例 : <pre>Device(config-if)# end</pre>	特権 EXEC モードに戻ります。

	コマンドまたはアクション	目的
ステップ 7	<b>show storm-control [interface-id] [broadcast   multicast   unicast]</b> 例 : Device# <b>show storm-control gigabitethernet1/0/1 unicast</b>	指定したトラフィックタイプについて、インターフェイスで設定したストーム制御抑制レベルを確認します。トラフィックタイプを入力しなかった場合は、ブロードキャストストーム制御の設定が表示されます。
ステップ 8	<b>copy running-config startup-config</b> 例 : Device# <b>copy running-config startup-config</b>	(任意) コンフィギュレーションファイルに設定を保存します。

## スモール 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。

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。

### 手順

	コマンドまたはアクション	目的
ステップ 1	<b>enable</b> 例 : Device> <b>enable</b>	特権 EXEC モードをイネーブルにします。 <ul style="list-style-type: none"> <li>パスワードを入力します（要求された場合）。</li> </ul>
ステップ 2	<b>configureterminal</b> 例 : Device# <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 3	<b>errdisable detect cause small-frame</b> 例 : Device(config)# <b>errdisable detect cause small-frame</b>	スwitch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。

	コマンドまたはアクション	目的
ステップ 4	<b>errdisable recovery interval</b> 間隔 例 :  Device(config)# <b>errdisable recovery interval 60</b>	(任意) 指定された <b>errdisable</b> ステートから回復する時間を指定します。
ステップ 5	<b>errdisable recovery cause small-frame</b> 例 :  Device(config)# <b>errdisable recovery cause small-frame</b>	(任意) 小さいフレームの着信によりポートが <b>errdisable</b> 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、 <b>EtherChannel</b> でもストーム制御を設定できます。ストーム制御を <b>EtherChannel</b> で設定する場合、ストーム制御設定は <b>EtherChannel</b> 物理インターフェイスに伝播します。
ステップ 6	<b>interface interface-id</b> 例 :  Device(config)# <b>interface gigabitethernet1/0/2</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を指定します。
ステップ 7	<b>small-frame violation-rate pps</b> 例 :  Device(config-if)# <b>small-frame violation rate 10000</b>	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 <b>errdisable</b> 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 パケット/秒 (pps) です。
ステップ 8	<b>end</b> 例 :  Device(config)# <b>end</b>	特権 EXEC モードに戻ります。
ステップ 9	<b>show interfaces interface-id</b> 例 :  Device# <b>show interfaces gigabitethernet1/0/2</b>	設定を確認します。

	コマンドまたはアクション	目的
ステップ 10	<b>show running-config</b> 例 : Device# <b>show running-config</b>	入力を確認します。
ステップ 11	<b>copy running-config startup-config</b> 例 : Device# <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。

## 機能情報の確認

ご使用のソフトウェアリリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報および警告については、使用するプラットフォームおよびソフトウェア リリースの **Bug Search Tool** およびリリース ノートを参照してください。このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このモジュールの最後にある機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、**Cisco Feature Navigator** を使用します。Cisco Feature Navigator には、<http://www.cisco.com/go/cfn> からアクセスします。Cisco.com のアカウントは必要ありません。

## 保護ポートに関する情報

### 保護ポート

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。

## 保護ポートのデフォルト設定

デフォルトでは、保護ポートは定義されません。

## 保護ポートのガイドライン

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 チャン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 チャンネル グループ内のすべてのポートでイネーブルになります。

## 保護ポートの設定方法

### 保護ポートの設定

始める前に

保護ポートは事前定義されていません。これは設定する必要があるタスクです。

手順

	コマンドまたはアクション	目的
ステップ 1	<b>enable</b> 例：  Device> <b>enable</b>	特権 EXEC モードをイネーブルにします。  • パスワードを入力します（要求された場合）。
ステップ 2	<b>configureterminal</b> 例：  Device# <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 3	<b>interface interface-id</b> 例：  Device(config)# <b>interface gigabitethernet1/0/1</b>	設定するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	<b>switchport protected</b> 例：	インターフェイスを保護ポートとして設定します。

	コマンドまたはアクション	目的
	Device (config-if) # <b>switchport protected</b>	
ステップ 5	<b>end</b> 例 : Device (config) # <b>end</b>	特権 EXEC モードに戻ります。
ステップ 6	<b>show interfaces interface-id switchport</b> 例 : Device# <b>show interfaces gigabitethernet1/0/1 switchport</b>	入力を確認します。
ステップ 7	<b>show running-config</b> 例 : Device# <b>show running-config</b>	入力を確認します。
ステップ 8	<b>copy running-config startup-config</b> 例 : Device# <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。

## 保護ポートの監視

表 6: 保護ポートの設定を表示するコマンド

コマンド	目的
<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。

## 次の作業

.

## その他の参考資料

### エラー メッセージ デコーダ

説明	リンク
このリリースのシステムエラーメッセージを調査し解決するために、エラー メッセージ デコーダ ツールを使用します。	<a href="https://www.cisco.com/cgi-bin/Support/Errordecoder/index.cgi">https://www.cisco.com/cgi-bin/Support/Errordecoder/index.cgi</a>

### MIB

MIB	MIB のリンク
本リリースでサポートするすべての MIB	選択したプラットフォーム、Cisco IOS リリース、およびフィチャセットに関する MIB を探してダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 <a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a>

### シスコのテクニカル サポート

説明	Link
<p>シスコのサポート Web サイトでは、シスコの製品やテクノロジーに関するトラブルシューティングにお役立ていただけるように、マニュアルやツールをはじめとする豊富なオンラインリソースを提供しています。</p> <p>お使いの製品のセキュリティ情報や技術情報を入手するために、Cisco Notification Service (Field Notice からアクセス)、Cisco Technical Services Newsletter、Really Simple Syndication (RSS) フィードなどの各種サービスに加入できます。</p> <p>シスコのサポート Web サイトのツールにアクセスする際は、Cisco.com のユーザ ID およびパスワードが必要です。</p>	<a href="http://www.cisco.com/support">http://www.cisco.com/support</a>

## 機能情報

リリース	機能情報
Cisco IOS XE 3.2SE	この機能が導入されました。



## 機能情報の確認

ご使用のソフトウェアリリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報および警告については、使用するプラットフォームおよびソフトウェア リリースの **Bug Search Tool** およびリリース ノートを参照してください。このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このモジュールの最後にある機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator には、<http://www.cisco.com/go/cfn> からアクセスします。Cisco.com のアカウントは必要ありません。

## ポート ブロッキングに関する情報

### ポート ブロッキング

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。

## ポート ブロッキングの設定方法

### 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

#### 始める前に

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。

#### 手順

	コマンドまたはアクション	目的
ステップ 1	<b>enable</b> 例 :	特権 EXEC モードをイネーブルにします。

	コマンドまたはアクション	目的
	Device> <b>enable</b>	<ul style="list-style-type: none"> <li>パスワードを入力します（要求された場合）。</li> </ul>
ステップ 2	<b>configureterminal</b> 例： Device# <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 3	<b>interface interface-id</b> 例： Device(config)# <b>interface gigabitethernet1/0/1</b>	設定するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	<b>switchport block multicast</b> 例： Device(config-if)# <b>switchport block multicast</b>	ポートからの未知のマルチキャストの転送をブロックします。  (注) 純粋なレイヤ 2 マルチキャストトラフィックだけがブロックされます。ヘッダーに 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 5	<b>switchport block unicast</b> 例： Device(config-if)# <b>switchport block unicast</b>	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 6	<b>end</b> 例： Device(config)# <b>end</b>	特権 EXEC モードに戻ります。
ステップ 7	<b>show interfaces interface-idswitchport</b> 例： Device# <b>show interfaces gigabitethernet1/0/1 switchport</b>	入力を確認します。

	コマンドまたはアクション	目的
ステップ 8	<b>show running-config</b> 例 : Device# <b>show running-config</b>	入力を確認します。
ステップ 9	<b>copy running-config startup-config</b> 例 : Device# <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。

## ポートブロッキングの監視

表 7: ポートブロッキングの設定を表示するコマンド

コマンド	目的
<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。

## 次の作業

.

## その他の参考資料

### 関連資料

関連項目	マニュアルタイトル

## エラーメッセージデコーダ

説明	リンク
このリリースのシステムエラーメッセージを調査し解決するために、エラーメッセージデコーダツールを使用します。	<a href="https://www.cisco.com/cgi-bin/Support/Errordecoder/index.cgi">https://www.cisco.com/cgi-bin/Support/Errordecoder/index.cgi</a>

## 標準および RFC

標準/RFC	タイトル

## MIB

MB	MIB のリンク
	<p>選択したプラットフォーム、Cisco IOS リリース、およびフィチャセットに関する MIB を探してダウンロードするには、次の URL にある Cisco MIB Locator を使用します。</p> <p><a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a></p>

## シスコのテクニカル サポート

説明	リンク
<p>シスコのサポート Web サイトでは、シスコの製品やテクノロジーに関するトラブルシューティングにお役立ていただけるように、マニュアルやツールをはじめとする豊富なオンラインリソースを提供しています。</p> <p>お使いの製品のセキュリティ情報や技術情報を入手するために、Cisco Notification Service (Field Notice からアクセス)、Cisco Technical Services Newsletter、Really Simple Syndication (RSS) フィードなどの各種サービスに加入できます。</p> <p>シスコのサポート Web サイトのツールにアクセスする際は、Cisco.com のユーザ ID およびパスワードが必要です。</p>	<a href="http://www.cisco.com/support">http://www.cisco.com/support</a>

## 機能情報

リリース	機能情報
Cisco IOS XE 3.2SE	この機能が導入されました。

## ポートセキュリティの設定例

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。

```
Device(config)# interface gigabitethernet1/0/1
Device(config-if)# switchport mode access
Device(config-if)# switchport port-security
Device(config-if)# switchport port-security maximum 50
Device(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。

```
Device(config)# interface gigabitethernet1/0/2
Device(config-if)# switchport mode trunk
Device(config-if)# switchport port-security
Device(config-if)# switchport port-security mac-address 0000.0200.0004 vlan 3
```

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）。

```
Device(config)# interface tengigabitethernet1/0/1
Device(config-if)# switchport access vlan 21
Device(config-if)# switchport mode access
Device(config-if)# switchport voice vlan 22
Device(config-if)# switchport port-security
Device(config-if)# switchport port-security maximum 20
Device(config-if)# switchport port-security violation restrict
Device(config-if)# switchport port-security mac-address sticky
Device(config-if)# switchport port-security mac-address sticky 0000.0000.0002
Device(config-if)# switchport port-security mac-address 0000.0000.0003
Device(config-if)# switchport port-security mac-address sticky 0000.0000.0001 vlan voice
Device(config-if)# switchport port-security mac-address 0000.0000.0004 vlan voice
Device(config-if)# switchport port-security maximum 10 vlan access
Device(config-if)# switchport port-security maximum 10 vlan voice
```

### 関連トピック

[ポートセキュリティ \(15 ページ\)](#)

[ポートセキュリティのイネーブル化および設定 \(21 ページ\)](#)

