CHAPTER 29

ポートベースのトラフィック制御の設定

この章では、IE 3000 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手順について説明します。

（注） この章で使用してい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

ここでは、次の概要と設定情報について説明します。

ストーム制御の概要

ストーム制御は、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 ストームによって中断されるのを防ぎます。LAN ストームは、パケットが LAN でフラッディングする場合に発生するもので、過剰なトラフィックを生成し、ネットワークのパフォーマンスを低下させます。プロトコルスタック実装のエラー、ネットワーク設定の誤り、またはユーザによる DoS 攻撃（サービス拒絶攻撃）の開始がストームの原因になります。

ストーム制御（またはトラフィック抑制）は、インターフェイスからスイッチング バスに送信され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、ブロードキャストのいずれであるかを判断します。スイッチは、1 秒間隔で受信される特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測定値を比較します。

ストーム制御は、次のうちのいずれかをトラフィック アクティビティの測定方法に使用します。

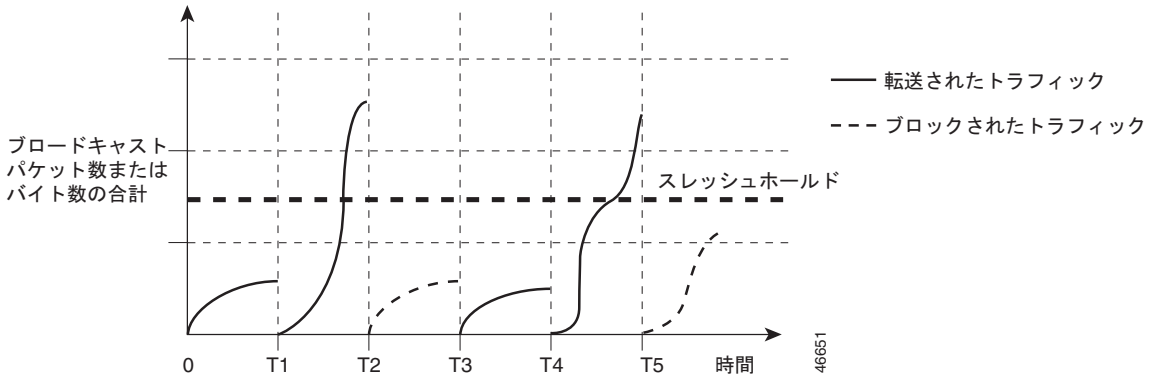
- 帯域幅（ブロードキャスト、マルチキャスト、またはユニキャスト トラフィックで利用可能なポートの全帯域幅のパーセンテージ）。
- トラフィック レート（ブロードキャスト、マルチキャスト、またはユニキャスト パケットが受信されるときの 1 秒あたりのパケット数）。
- トラフィック レート（ブロードキャスト、マルチキャスト、またはユニキャスト パケットが受信されるときの 1 秒あたりのビット数）。
- トラフィック レート（1 秒あたりのパケット数、小さいフレームの場合）。この機能は、グローバルにイネーブルになっています。小さいフレームのスレッショルドは、それぞれのインターフェイスで設定されます。

いずれの方法も、上限のスレッショ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 レートが下限のスレッショルド（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 レート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、抑制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 トラフィックのストーム制御スレッショルドに達した場合、ブリッジ プロトコル データ ユニット（BPDU）および Cisco Discovery Protocol（CDP）フレームなどのコントロール トラフィック以外のマルチキャスト トラフィックすべてがブロックされます。ただし、スイッチは、Open Shortest Path First（OSPF）および通常のマルチキャスト データ トラフィック間のように、ルーティング アップデート間を区別しないため、両方のトラフィックがブロックされます。

図 29-1 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、T1 ～ T2 間および T4 ～ T5 間の時間間隔で設定されたスレッショ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ョルドを上回ると、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 のあとの時間間隔ではブロックされています。次の時間間隔（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ョルドを上回らなければ、再度転送されます。

図 29-1　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 秒の時間間隔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くなると、より多くのパケットを通過させることができます。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。0.0 の値は、ポート上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 トラフィックをブロックします。

（注）　パケットは一定間隔で着信しないので、トラフィック アクティビティを 1 秒間隔で測定することは、トラフィック ストーム制御の動作に影響す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。

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になっています（抑制レベルは 100% です）。

ストーム制御およびスレッシュホールド レベルの設定

ポートでストーム制御を設定し、特定タイプのトラフィックで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パーセンテージ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り、実際に適用されるスレッシュホールドは、設定レベルと数 % 程度異なる場合があります。

（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。

ストーム制御およびスレッシュホールド レベルを設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id*	設定するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。

	コマンド	目的
ステップ 3	**storm-control** {**broadcast** | **multicast** | **unicast**} **level** {*level* [*level-low*] | **bps** *bps* [*bps-low*] | **pps** *pps* [*pps-low*]}	ブロードキャスト、マルチキャスト、ユニキャストのいずれかの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です。 キーワードの意味は次のとおりです。 • *level* には、ブロードキャスト、マルチキャスト、またはユニキャストの上限スレッシュホールド レベルを帯域幅のパーセンテージ（小数点以下第 2 位まで）で指定します。上限スレッシュホールドに達すると、ポートではトラフィックがブロックされます。指定できる範囲は 0.00 ～ 100.00 です。 • （任意）*level-low* には、下限スレッシュホールド レベルを帯域幅のパーセンテージ（小数点以下第 2 位まで）で指定します。この値は、上限抑制値より小さいまたは等しい必要があります。トラフィックがこのレベルより下がると、ポートでトラフィックが転送されます。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。 スレッシュホールドを最大値（100%）に設定すると、トラフィックは制限されません。スレッシュホールドを 0.0 に設定すると、ブロードキャスト、マルチキャスト、ユニキャストのすべてのトラフィックがそのポートでブロックされます。 • **bps** *bps* には、ブロードキャスト、マルチキャスト、またはユニキャスト トラフィック用に上限スレッシュホールド レベルを 1 秒あたりのビット数単位（小数点以下第 1 位まで）で指定します。上限スレッシュホールドに達すると、ポートではトラフィックがブロックされます。指定できる範囲は 0.0 ～ 10000000000.0 です。 • （任意）*bps-low* には、下限スレッシュホールド レベルを 1 秒あたりのビット数単位（小数点以下第 1 位まで）で指定します。上限スレッシュホールド レベル以下にしてください。トラフィックがこのレベルより下がると、ポートでトラフィックが転送されます。指定できる範囲は 0.0 ～ 10000000000.0 です。 • **pps** *pps* には、ブロードキャスト、マルチキャスト、またはユニキャスト トラフィック用に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単位（小数点以下第 1 位まで）で指定します。上限スレッシュホールドに達すると、ポートではトラフィックがブロックされます。指定できる範囲は 0.0 ～ 10000000000.0 です。 • （任意）*pps-low* 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単位（小数点以下第 1 位まで）で指定します。上限スレッシュホールド レベル以下にしてください。トラフィックがこのレベルより下がると、ポートでトラフィックが転送されます。指定できる範囲は **0.0 ～** 10000000000.0 です。 BPS 設定および PPS 設定には、スレッシュホールド値が大きくなる場合、k、m、g などのメトリック サフィクスを使用できます。
ステップ 4	**storm-control action** {**shutdown** | **trap**}	ストームが検出されたときのアクションを指定します。デフォルトでは、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。 • ストーム中にポートを errdisable にするには、**shutdown** キーワードを選択します。 • 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、**trap** キーワードを選択します。

	コマンド	目的
ステップ 5	**end**	特権 EXEC モードに戻ります。
ステップ 6	**show storm-control** [*interface-id*] [**broadcast** | **multicast** | **unicast**]	指定したトラフィック タイプについてインターフェイスに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 タイプを指定しない場合は、ブロードキャスト ストーム制御の設定が表示されます。
ステップ 7	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

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

```
Switch# configure terminal
Switch(config)# interface gigabitethernet1/1
Switch(config-if)# storm-control unicast level 87 65
```

次に、ポートのブロードキャスト アドレス ストーム制御を 20% のレベルでイネーブルにする例を示します。トラフィック ストーム制御インターバルで、ブロードキャスト トラフィックがポートの利用可能な全帯域幅の 20% という設定レベルを超えると、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スイッチはすべてのブロードキャスト トラフィックを廃棄します。

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

小さいフレームの着信レートの設定

着信 VLAN タグ付きパケットが 67 バイト以下のときは、*小さいフレーム*と見なされます。小さいフレームはスイッチによって転送されますが、スイッチのストーム制御カウンタは増分されません。Cisco IOS Release 12.2(44)SE 以降では、小さいフレームが指定のレート（スレッシュホールド）で着信する場合、ポートを errdisable にできます。

小さいフレームの着信機能をスイッチ上でグローバルにイネーブルにし、各インターフェイスで小さいフレームのスレッシュホールド（パケット数）を設定します。パケットが最小サイズよりも小さく、指定のレート（スレッシュホールド）で着信する場合、ポートが errdisable なので、パケットは廃棄されます。

errdisable recovery cause small-frame グローバル コンフィギュレーション コマンドを入力すると、指定の時間が経過した時点で、ポートが再びイネーブルになります（**errdisable recovery** グローバル コンフィギュレーション コマンドを使用して回復時間を指定します）。

各インターフェイスのスレッシュホールド レベルを設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**errdisable detect cause small-frame**	小さいフレームの着信レート機能をスイッチ上でイネーブルにします。
ステップ 3	**errdisable recovery interval** *interval*	（任意）指定された errdisable ステートから回復する時間を指定します。

	コマンド	目的
ステップ 4	**errdisable recovery cause small-frame**	（任意）小さいフレームの着信によりポートが errdisable になったあと、ポートが自動的に再びイネーブルになる回復時間を設定します。
ステップ 5	**interface** *interface-id*	インターフェイス コンフィギュレーション モードを開始し、設定するインターフェイスを指定します。
ステップ 6	**small violation-rate** *pps*	インターフェイスが着信パケットを廃棄するスレッシュホールドレートを設定し、ポートを errdisable にします。指定できる範囲は 1 ～ 10,000 pps（パケット / 秒）です。
ステップ 7	**end**	特権 EXEC モードに戻ります。
ステップ 8	**show interfaces** *interface-id*	設定を確認します。
ステップ 9	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

次に、小さいフレームの着信レート機能をイネーブルにする例、ポート 回復時間を設定する例、およびポートが errdisable になるスレッシュホールドを設定する例を示します。

```
Switch# configure terminal
Switch# errdisable detect cause small-frame
Switch# errdisable recovery cause small-frame
Switch(config)# interface gigabitethernet1/1
Switch(config-if)# small-frame violation rate 10000
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、あるネイバーによって生成されたトラフィックを別のネイバー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、PIM パケットなどの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 装置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、通常どおり行われます。

ここでは、次の設定情報について説明します。

- 「保護ポートのデフォルト設定」（P.29-6）
- 「保護ポートの設定時の注意事項」（P.29-7）
- 「保護ポートの設定」（P.29-7）

保護ポートのデフォルト設定

デフォルトでは、保護ポートが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（ポートチャネル 5 など）のいずれにも設定できます。特定のポート チャ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。

プライベート VLAN ポートを保護ポートとして設定しないでください。保護ポートをプライベート VLAN ポートとして設定しないでください。プライベート VLAN の独立ポートは、他の独立ポートやコミュニティ ポートにトラフィックを転送しません。プライベート VLAN の詳細については、第 19 章「プライベート VLAN の設定」を参照してください。

保護ポートの設定

ポートを保護ポートとして定義するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id*	設定するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	**switchport protected**	インターフェイスを保護ポートとして設定します。
ステップ 4	**end**	特権 EXEC モードに戻ります。
ステップ 5	**show interfaces** *interface-id* **switchport**	設定を確認します。
ステップ 6	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

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 gigabitethernet1/1
Switch(config-if)# switchport protected
Switch(config-if)# end
```

ポート ブロッキングの設定

デフォルトでは、スイッチは、宛先 MAC アドレスが不明なパケットをすべてのポートからフラッディングします。不明な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。不明な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、不明な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。

（注）　ポート ブロッキング機能はピュア 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 情報を持つマルチキャスト パケットは、ブロックされません。

ここでは、次の設定情報について説明します。

ポート ブロッキングのデフォルト設定

デフォルトでは、ポートから送信される不明な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が、これらのパケットは、すべてのポートにフラッディングされます。

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） このインターフェイスに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。特定のポート 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 グループ内の全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ユニキャスト パケットおよびレイヤ 2 マルチキャスト パケットのフラッディングをディセーブルにするには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id*	設定するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	**switchport block multicast**	ポートからの不明なマルチキャストの転送をブロックします。 **（注）** ピュア 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 情報を持つマルチキャスト パケットは、ブロックされません。
ステップ 4	**switchport block unicast**	ポートからの不明なユニキャストの転送をブロックします。
ステップ 5	**end**	特権 EXEC モードに戻ります。
ステップ 6	**show interfaces** *interface-id* **switchport**	設定を確認します。
ステップ 7	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

トラフィックがブロックされずに、ポート上で通常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レイヤ 2 マルチキャスト フラッディングをブロックする例を示します。

```
Switch# configure terminal
Switch(config)# interface gigabitethernet1/1
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 アドレスの数を 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ている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とすると、違反のフラグが立てられます。

ここでは、次の概要と設定情報について説明します。

ポート セキュリティの概要

ここでは、次の概念情報について説明します。

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と、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：ダイナミックに設定されます。これらはアドレス テーブルだけに格納され、スイッチが再起動したときに削除されます。
- スティッキ セキュア MAC アドレス：ダイナミックに学習されるか、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、スイッチが再起動するときに、インターフェイスはアドレスをダイナミックに再設定しなくてすみます。

スティッキ ラーニングをイネーブルにすると、ダイナミック MAC アドレスをスティッキ セキュア MAC アドレスに変換し、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。スティッキ ラーニングをイネーブルにするには、**switchport port-security mac-address sticky** インターフェイス コンフィギュレーション コマンドを入力します。このコマンドを入力すると、インターフェイスは、すべてのダイナミック セキュア MAC アドレス（スティッキ ラーニング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）をスティッキ セキュア MAC アドレスに変換します。すべてのスティッキ セキュア MAC アドレスが、実行コンフィギュレーションに追加されます。

スティッキ セキュア MAC アドレスは、コンフィギュレーション ファイル（スイッチ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。スティッキ セキュア MAC 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、スイッチが再起動するときに、インターフェイスはこれらのアドレスを再学習しなくてすみます。スティッキ セキュア アドレスが保存されていない場合は、アドレスは失われます。

スティッキ ラーニングをディセーブルにした場合、スティッキ セキュア MAC アドレスはダイナミック セキュア アドレスに変換され、実行コンフィギュレーションから削除されます。

スイッチに設定できるセキュア MAC アドレスの最大数は、システムで使用が許可されている MAC アドレスの最大数によって決まります。この数字はアクティブな Switch Database Management（SDM）テンプレートによって決められます。第 10 章「SDM テンプレートの設定」を参照してください。この数字は、インターフェイスで設定された他のレイヤ 2 機能やその他のセキュア MAC アドレスなど、利用可能な MAC アドレスの合計数です。

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、同じ 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 4 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 アドレス数がポートで許可されている最大制限に到達した場合、不明な送信元アドレスのパケットは廃棄されます。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か、許可す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。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 ポート上で protect 違反モードを設定することは推奨できません。protect モードでは、ポートが最大制限に達していなくても、VLAN が最大制限に達するとラーニングがディセーブルになります。

- restrict：セキュア MAC アドレス数がポートで許可されている最大制限に到達した場合、不明な送信元アドレスのパケットは廃棄されます。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か、許可す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。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ます。また、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：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、ポートの LED がオフになります。SNMP トラップが送信されます。また、Syslog メッセージがロギングされ、違反カウンタが増加します。セキュア ポートが errdisable ステートの場合は、**errdisable recovery cause** *psecure-violation* グローバル コンフィギュレーション コマンドを入力してこのステートを解除したり、**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、ポートを手動で再びイネーブルにできます（デフォルトのモードです）。
- shutdown vlan：VLAN 単位でセキュリティ違反モードを設定するときに使います。このモードでは、セキュリティ違反が起こった場合、ポート全体ではなく、VLAN が errdisable になります。

表 29-1 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アクションを示します。

表 29-1　セキュリティ違反モードのアクション

違反モード	トラフィックの転送[1]	SNMP トラップの送信	Syslog メッセージの送信	エラー メッセージの表示[2]	違反カウンタの増加	ポートのシャットダウン
protect	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
shutdown vlan	なし	あり	あり	なし	あり	なし[3]

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、スイッチはエラー メッセージを返します。
3. 違反が発生した VLAN だけをシャットダウンします。

ポート セキュリティのデフォルト設定

表 29-2 に、インターフェイス用のデフォルトのポート セキュリティ設定を示します。

表 29-2　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。
スティッキ 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。

ポート セキュリティ設定時の注意事項

ポート セキュリティを設定する場合、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 ポートをスイッチド ポート アナライザ（SPAN）の宛先ポートにすることはできません。
- セキュア ポートを Fast EtherChannel または Gigabit EtherChannel ポート グループに含めることはできません。

（注）　音声 VLAN は、アクセス ポート上だけでサポートされます。設定で許可されている場合でも、トランク ポート上ではサポートされません。

- 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 に設定する必要があります。ポートを Cisco IP Phone に接続する場合は、IP Phone に MAC アドレスが 1 つ必要です。Cisco IP Phone のアドレスは音声 VLAN 上で学習されますが、アクセス VLAN 上では学習されません。1 台の PC を Cisco IP Phone に接続する場合、MAC アドレスの追加は必要ありません。2 台以上の PC を Cisco IP Phone に接続する場合、各 PC に 1 つ、さらに Cisco IP Phone に 1 つを許可する十分なセキュア アドレスを設定する必要があります。
- ポート セキュリティが設定されているトランク ポートが、データ トラフィック用のアクセス VLAN および音声トラフィック用の音声 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無効です。

  接続先装置が同じ MAC アドレスを使用してアクセス VLAN の IP アドレスを要求し、次に、音声 VLAN の IP アドレスを要求する場合、アクセス VLAN だけに IP アドレスが割り当てられます。
- インターフェイスにセキュア アドレス最大値を入力した場合、新規の値が前回の値より大きいと、新規の値により、前回の設定値が上書きされます。新しい値が古い値より小さく、インターフェイスで設定されていたセキュア アドレス数も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 エージングはサポートしていません。

表 29-3 は、ポート セキュリティとその他のポートベース機能の互換性をまとめたものです。

表 29-3　ポート セキュリティとその他のスイッチ機能との互換性

ポートのタイプまたは機能	ポート セキュリティとの互換性
DTP[1] ポート[2]	なし
トランク ポート	あり
ダイナミック アクセス ポート[3]	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

表 29-3　ポート セキュリティとその他のスイッチ機能との互換性 （続き）

ポートのタイプまたは機能	ポート セキュリティとの互換性
音声 VLAN ポート[4]	あり
プライベート VLAN ポート	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 コマンドで設定されたポート。
3. **switchport access vlan dynamic** インターフェイス コンフィギュレーション コマンドで設定された VLAN Query Protocol（VQP）ポート。
4. ポートの最大セキュア アドレス許容数を 2 に設定し、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ことによって、インターフェイスへの入力を制限するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id*	設定するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	**switchport mode** {**access** | **trunk**}	インターフェイス スイッチポート モードを access または trunk に設定します。デフォルト モード（dynamic auto）のインターフェイスは、セキュア ポートとして設定できません。
ステップ 4	**switchport voice vlan** *vlan-id*	ポートで音声 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。
ステップ 5	**switchport port-security**	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
ステップ 6	**switchport port-security** [**maximum** *value* [**vlan** {*vlan-list* | {**access** | **voice**}}]]	（任意）インターフェイスのセキュア MAC アドレスの最大数を設定します。スイッチに設定できるセキュア MAC アドレスの最大数は、システムで使用が許可されている 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設定されます。第 10 章「スイッチ SDM テンプレートの設定」を参照してください。この数字は、インターフェイスで設定された他のレイヤ 2 機能やその他のセキュア MAC アドレスなど、利用可能な MAC アドレスの合計数です。 （任意）**vlan**：VLAN 単位の最大値を設定します。 **vlan** キーワードを入力後、次のいずれかのオプションを入力します。 • *vlan-list*：トランク ポートで、VLAN 範囲、または一連の VLAN 内の VLAN ごとに最大値を設定します。VLAN 範囲はハイフン、一連の VLAN はカンマで区切ります。VLAN を指定しない場合、VLAN ごとの最大値が使用されます。 • **access**：アクセス ポートで、VLAN をアクセス VLAN として指定します。 • **voice**：アクセス ポートで、VLAN を音声 VLAN として指定します。 **（注）** **voice** キーワードは、音声 VLAN がポートに設定されていて、そのポートがアクセス VLAN でない場合に限り、利用可能です。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。

	コマンド	目的
ステップ 7	**switchport port-security [violation** {**protect** | **restrict** | **shutdown** | **shutdown vlan**}]	（任意）違反モード、およびセキュリティ違反が検出されたときの対処方法を次のいずれかで設定します。 • **protect**：ポートのセキュア MAC アドレス数がポートで許可されている最大制限に到達した場合、不明な送信元アドレスのパケットは廃棄されます。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か、許可す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。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、ポートが最大制限に達していなくても VLAN が保護モードの最大制限に達すると、ラーニングがディセーブルになります。 • **restrict**：セキュア MAC アドレス数がポートで許可されている制限に到達した場合、不明な送信元アドレスのパケットは廃棄されます。十分な数のセキュア MAC アドレスを削除するか、許可す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。SNMP トラップが送信されます。また、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**：違反が発生し、ポートの LED がオフになると、インターフェイスが errdisable の状態になります。SNMP トラップが送信されます。また、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 vlan**：VLAN 単位でセキュリティ違反モードを設定するときに使います。このモードでは、セキュリティ違反が起こった場合、ポート全体ではなく、VLAN が errdisable になります。 （注）　セキュア ポートが errdisable ステートになっているときは、**errdisable recovery cause psecure-violatio** 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。**shutdown** および **no shutdown** インターフェイス コンフィギュレーション コマンドを入力するか、**clear errdisable interface vlan** 特権 EXEC コマンドを使用して、ポートを手動で再びイネーブルにできます。

	コマンド	目的
ステップ 8	**switchport port-security** [**mac-address** *mac-address* [**vlan** {*vlan-id* | {**access** | **voice**}}]	（任意）インターフェイスのセキュア MAC アドレスを入力します。このコマンドを使用してセキュア 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。 **（注）** このコマンドを入力したあとにスティッキ ラーニングをイネーブルにすると、ダイナミックに学習されたセキュア アドレスがスティッキ セキュア MAC アドレスに変換されて、実行コンフィギュレーションに追加されます。 （任意）**vlan**：VLAN 単位の最大値を設定します。 **vlan** キーワードを入力後、次のいずれかのオプションを入力します。 • *vlan-id*：トランク ポート上で、VLAN ID および MAC アドレスを指定します。VLAN ID を指定しないと、ネイティブ VLAN が使用されます。 • **access**：アクセス ポートで、VLAN をアクセス VLAN として指定します。 • **voice**：アクセス ポートで、VLAN を音声 VLAN として指定します。 **（注）** **voice** キーワードは、音声 VLAN がポートに設定されていて、そのポートがアクセス VLAN でない場合に限り、利用可能です。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。
ステップ 9	**switchport port-security mac-address sticky**	（任意）インターフェイスでスティッキ ラーニングをイネーブルにします。
ステップ 10	**switchport port-security mac-address sticky** [*mac-address* | **vlan** {**vlan-id** | {**access** | **voice**}}]	（任意）スティッキ セキュア MAC アドレスを入力します。必要に応じて、このコマンドを繰り返し入力します。最大数より少ないセキュア MAC アドレスを設定すると、残りの MAC アドレスはダイナミックに学習され、スティッキ セキュア MAC アドレスに変換されて、実行コンフィギュレーションに追加されます。 **（注）** このコマンドを入力する前にスティッキ ラーニング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、スティッキ セキュア MAC アドレスを入力できません。 （任意）**vlan**：VLAN 単位の最大値を設定します。 **vlan** キーワードを入力後、次のいずれかのオプションを入力します。 • *vlan-id*：トランク ポート上で、VLAN ID および MAC アドレスを指定します。VLAN ID を指定しないと、ネイティブ VLAN が使用されます。 • **access**：アクセス ポートで、VLAN をアクセス VLAN として指定します。 • **voice**：アクセス ポートで、VLAN を音声 VLAN として指定します。 **（注）** **voice** キーワードは、音声 VLAN がポートに設定されていて、そのポートがアクセス VLAN でない場合に限り、利用可能です。
ステップ 11	**end**	特権 EXEC モードに戻ります。
ステップ 12	**show port-security**	設定を確認します。
ステップ 13	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

インターフェイスをデフォルト状態の非セキュア 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。スティッキ ラーニングがイネーブルのときにこのコマンドを入力すると、スティッキ セキュア アドレスの一部は実行コンフィギュレーションのままですが、アドレス テーブルから削除されます。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状態の shutdown に戻すには、**no switchport port-security violation** {**protocol** | **restrict**} インターフェイス コンフィギュレーション コマンドを使用します。

インターフェイスでスティッキ ラーニングをディセーブルにするには、**no switchport port-security mac-address sticky** インターフェイス コンフィギュレーション コマンドを使用します。インターフェイスは、スティッキ セキュア MAC アドレスをダイナミック セキュア アドレスに変換します。ただし、スティッキ MAC アドレス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スティッキ アドレスが復元されます。

MAC アドレス テーブルからすべてのセキュア アドレスを削除するか、スイッチまたはインターフェイス上の特定タイプ（設定済み、ダイナミック、スティッキ）のすべてのセキュア アドレスを削除するには、**clear port-security** {**all** | **configured** | **dynamic** | **sticky**} 特権 EXEC コマンドを使用します。

アドレス テーブルから特定のセキュア MAC アドレスを削除するには、**no switchport port-security mac-address** *mac-address* インターフェイス コンフィギュレーション コマンドを使用します。アドレス テーブルから特定のインターフェイスのダイナミック セキュア アドレスをすべて削除するには、**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、（インターフェイスでポート セキュリティを再びイネーブルにするために）**switchport port-security** コマンドを入力します。**no switchport port-security** コマンドを入力する前に、**no switchport port-security mac-address sticky** インターフェイス コンフィギュレーション コマンドを使用して、スティッキ 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、スティッキ ラーニングはイネーブルにします。

```
Switch(config)# interface gigabitethernet1/1
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 gigabitethernet1/2
Switch(config-if)# switchport mode trunk
Switch(config-if)# switchport port-security
Switch(config-if)# switchport port-security mac-address 0000.02000.0004 vlan 3
```

次に、ポート上でスティッキ ポート セキュリティをイネーブルにして、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 アドレスの最大合計数を 20（データ VLAN に 10、音声 VLAN に 10）に設定する例を示します。

```
Switch(config)# interface FastEthernet1/1
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、ポート上のすべてのセキュア 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 ポートで装置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。セキュア アドレスのエージングはポート単位でイネーブルまたはディセーブルにできます。

ポート セキュリティ エージングを設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id*	設定するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	**switchport port-security aging** {**static** | **time** *time* | **type** {**absolute** | **inactivity**}}	セキュア ポートのスタティック エージングをイネーブルまたはディセーブルにするか、またはエージング タイムやタイプを設定します。 **（注）** スイッチは、スティッキ セキュア アドレスのポート セキュリティ エージングをサポートしていません。 このポートにスタティックに設定されたセキュア アドレスのエージングをイネーブルにする場合は、**static** を入力します。 *time* には、このポートのエージング タイムを指定します。指定できる範囲は 0 ～ 1440 分です。 **type** には、次に示すキーワードのいずれかを選択します。 • **absolute**：エージング タイプを absolute に設定します。このポートのすべてのセキュア アドレスは、指定された time（分）が経過したあとに期限切れとなり、セキュア アドレス リストから削除されます。 • **inactivity**：エージング タイプを inactivity に設定します。指定された time 期間中にセキュア送信元アドレスからのデータ トラフィックがない場合だけ、このポートのセキュア アドレスが期限切れになります。
ステップ 4	**end**	特権 EXEC モードに戻ります。

	コマンド	目的
ステップ 5	**show port-security** [**interface** *interface-id*] [**address**]	設定を確認します。
ステップ 6	**copy running-config startup-config**	(任意) 設定をコンフィギュレーション ファイルに保存します。

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 gigabitethernet1/1
Switch(config-if)# switchport port-security aging time 120
```

次に、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* 特権 EXEC コマンドを入力します。

ポート セキュリティとプライベート VLAN

管理者はポート セキュリティを使用して、ポート上で学習される MAC アドレスの数を制限したり、ポート上で学習可能な MAC アドレス を定義したりできます。

PVLAN ホストおよびプロミスキャス ポートでポート セキュリティを設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id*	設定するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	**switchport mode private-vlan** {**host** | **promiscuous**}	インターフェイスでプライベート VLAN をイネーブルにします。
ステップ 4	**switchport port-security**	インターフェイスでポート セキュリティをイネーブルにします。
ステップ 5	**end**	特権 EXEC モードに戻ります。
ステップ 6	**show port-security** [**interface** *interface-id*] [**address**]	設定を確認します。
ステップ 7	**copy running-config startup-config**	(任意) 設定をコンフィギュレーション ファイルに保存します。

```
Switch(config-if)# switchport private-vlan mapping 2061 2201-2206,3101
Switch(config-if)# switchport mode private-vlan promiscuous
Switch(config-if)# switchport port-security maximum 288
Switch(config-if)# switchport port-security
Switch(config-if)# switchport port-security violation restrict
```

（注）　ポート セキュリティとプライベート VLAN の両方が設定されているポートには、セキュア PVLAN ポートのラベル付けが可能です。セキュア アドレスがセキュア PVLAN ポートで学習されるとき、同じセキュア アドレスが、同じプライマリ VLAN に属する別のセキュア PVLAN ポートで学習されることはありません。ただし、非セキュア PVLAN ポートで学習されたアドレスは、同じプライマリ VLAN に属するセキュア PVLAN ポートでの学習が可能です。

ホスト ポートで学習されるセキュア アドレスは、関連プライマリ VLAN で自動的に複製されます。同様に、プロミスキャス ポートで学習されるセキュア アドレスは、すべての関連セカンダリ VLAN で自動的に複製されます。スタティック アドレスは、（mac-address-table static コマンドを使用して）セキュア ポートでユーザ設定できません。

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** 特権 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 storm-control** および **show port-security** 特権 EXEC コマンドを使用すると、それぞれストーム制御とポート セキュリティ設定が表示されます。

トラフィック制御情報を表示するには、表 29-4 に示す 1 つまたは複数の特権 EXEC コマンドを使用します。

表 29-4　トラフィック制御のステータスと設定の表示用コマンド

コマンド	目的
show interfaces [*interface-id*] **switchport**	すべてのスイッチング（非ルーティング）ポートまたは指定したポートについて、管理ステータスおよび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）。
show storm-control [*interface-id*] [**broadcast** | **multicast** | **unicast**]	すべてのインターフェイスまたは指定されたインターフェイスに設定されているストーム制御抑制レベルを、指定されたトラフィック タイプについて、またはブロードキャスト トラフィック（トラフィック タイプが入力されていない場合）について表示します。
show port-security [**interface** *interface-id*]	スイッチまたは指定されたインターフェイスのポート セキュリティ設定を、各インターフェイスで許可されるセキュア MAC アドレスの最大数、インターフェイスに設定されたセキュア MAC アドレスの数、発生したセキュリティ違反の数、違反モードを含めて表示します。
show port-security [**interface** *interface-id*] **address**	すべてのスイッチ インターフェイスまたは指定されたインターフェイスに設定されたすべてのセキュア MAC アドレス、および各アドレスのエージング情報を表示します。
show port-security interface *interface-id* **vlan**	指定されたインターフェイスに VLAN 単位で設定されているセキュア MAC アドレスの数を表示します。