CHAPTER 23

ポートベースのトラフィック制御の設定

この章では、Cisco ME 3400E イーサネット アクセス スイッチにポートベースのトラフィック制御機能を設定する方法について説明します。

（注） この章で使用するコマンドの構文および使用方法の詳細については、このリリースのコマンド リファレンスを参照してください。

ストーム制御の設定

ストーム制御の概要

ストーム制御は、LAN 上のトラフィックが、いずれかの物理インターフェイスのブロードキャスト、マルチキャスト、またはユニキャストのストームによって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実装内またはネットワーク設定内のエラーは、ストームの原因となる場合があります。

ストーム制御（トラフィック抑制）は、インターフェイスからスイッチング バスへ流れるパケットをモニタし、そのパケットがユニキャスト、マルチキャスト、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 秒のタイム インターバル内で受信した指定されたタイプのパケットの数をカウントして、事前定義されている抑制レベルのしきい値とその測定値を比較します。

ストーム制御では、次のうちいずれかの手法を使用してトラフィック アクティビティを測定します。

- 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トラフィックで使用できる帯域幅で、ポートで利用可能な総帯域幅に対するパーセンテージ

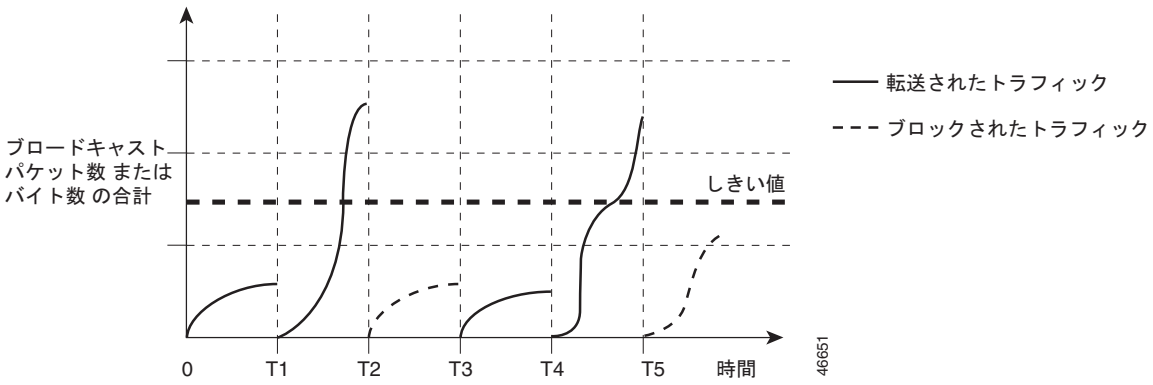
- ブロードキャスト、マルチキャスト、またはユニキャスト パケットが受信されるトラフィック レート（pps）
- ブロードキャスト、マルチキャスト、またはユニキャスト パケットが受信されるトラフィック レート（bps）

それぞれの手法では、上限しきい値に達すると、トラフィックがポートでブロックされます。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）未満に下がるまでポートはブロック状態のままとなり、下限しきい値未満に下がると、通常転送が再開されます。下限抑制レベルを指定していない場合、トラフィック レートが上限抑制レベル未満に下がるまで、スイッチではすべてのトラフィックがブロックされます。一般的には、レベルを上げると、ブロードキャスト ストームに対する保護の効果が小さくなります。

（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。

図 23-1 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 間で設定されたしきい値を上回っています。特定のトラフィックの量がしきい値を上回ると、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 トラフィックがしきい値を上回らなければ、再度転送されます。

図 23-1　　ブロードキャスト ストーム制御の例



ストーム制御の抑制レベルと 1 秒のタイム インターバルの組み合せにより、ストーム制御アルゴリズムの動作が制御されます。しきい値が高いほど、通過できるパケットが多くなります。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 1 秒のタイム インターバルを設けることによって、ストーム制御の動作に影響を与える可能性があります。

各トラフィック タイプの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）。

ストーム制御およびしきい値レベルの設定

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しきい値レベルを入力します。

（注） ME 3400E スイッチでは、ストーム制御機能が小さなフレームを適切に処理できるようにするため、スイッチのストーム制御カウンタが小さいフレームで増加するように追加の設定を行う必要はありません。

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、しきい値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、実際のしきい値は、数 % 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しきい値レベルを設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id*	設定するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	**no shutdown**	必要に応じて、ポートをイネーブルにします。デフォルトでは、User Network Interface（UNI; ユーザ ネットワーク インターフェイス）と Enhanced Network Interface（ENI; 拡張ネットワーク インターフェイス）はディセーブルに、Network Node Interface（NNI; ネットワーク ノード インターフェイス）はイネーブルに設定されています。

	コマンド	目的
ステップ 4	**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、ユニキャストのいずれかの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（小数点以下第 2 位まで）で指定します。上限しきい値に達すると、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、下限しきい値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。 しきい値を最大値（100%）に設定すると、トラフィックは制限されません。しきい値を 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、ユニキャストのいずれかのトラフィック用に上限しきい値レベルを 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。上限しきい値に達すると、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、下限しきい値レベルを 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。上限しきい値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、ユニキャストのいずれかのトラフィック用に上限しきい値レベルを 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。上限しきい値に達すると、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、下限しきい値レベルを 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。上限しきい値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、しきい値が大きくなる場合、k、m、g などのメートル法の単位を使用できます。

	コマンド	目的
ステップ 5	**storm-control action** {**shutdown** | **trap**}	ストームが検出されたときに実行する処理を指定します。デフォルトでは、トラフィックがフィルタリングされてトラップが送信されません。 • ストーム中にポートを errdisable にするには、キーワード **shutdown** を選択します。 • ストームが検出されたときに 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、キーワード **trap** を選択します。
ステップ 6	**end**	特権 EXEC モードに戻ります。
ステップ 7	**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	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

ストーム制御をディセーブルにするには、**no storm-control** {**broadcast** | **multicast** | **unicast**} **level** インターフェイス コンフィギュレーション コマンドを使用します。

以下は、上限抑制レベルを 87 %、下限抑制レベルを 65 % にして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方法の例です。

```
Switch# configure terminal
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# storm-control unicast level 87 65
```

次の例は、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方法を示します。ブロードキャスト トラフィックが、トラフィックストーム制御インターバルでポートの使用可能帯域幅全体の 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 gigabitethernet0/1
Switch(config-if)# storm-control broadcast level 20
```

保護ポートの設定

一部のアプリケーションでは、同一スイッチ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。

（注）　NNI のデフォルトは非保護ポートです。UNI および ENI はポート独立を行うため、UNI および ENI ポート上では、保護ポートを使用できません。ポート タイプの詳細については、「UNI、NNI、および ENI の各ポート タイプ」（P.10-2）を参照してください。

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のみが転送されます。保護ポート間を通過するすべてのデータ トラフィックはレイヤ 3 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

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、NNI として設定される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（仮想 LAN）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 13 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。インターフェイスは、NNI である必要があります。 **（注）**　デフォルトでは、UNI および ENI は保護ポートです。
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）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 gigabitethernet0/1
Switch(config-if)# switchport protected
Switch(config-if)# end
```

次に、保護ポートとして FastEthernet ポートを設定する例を示します。

```
Switch# configure terminal
Switch(config)# interface fastethernet 0/1
Switch(config-if)# port-type NNI
Switch(config-if)# no shutdown
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（メディア アクセス制御）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。

（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 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。

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」（P.23-7）
- 「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」（P.23-7）

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。

インターフェイスから送信されるユニキャストおよびレイヤ 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。

	コマンド	目的
ステップ 3	**no shutdown**	必要に応じて、ポートをイネーブルにします。デフォルトでは、UNI および ENI はディセーブルに、NNI はイネーブルに設定されています。
ステップ 4	**switchport block multicast**	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。 **（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 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	**switchport block unicast**	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 6	**end**	特権 EXEC モードに戻ります。
ステップ 7	**show interfaces** *interface-id* **switchport**	設定を確認します。
ステップ 8	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

トラフィックがブロックされず、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 fastethernet0/1
Switch(config-if)# no shutdown
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、次の概要および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」（P.23-9）
- 「ポート セキュリティのデフォルト設定」（P.23-10）
- 「ポート セキュリティ設定時の注意事項」（P.23-11）
- 「ポート セキュリティのイネーブル化と設定」（P.23-12）
- 「ポート セキュリティ エージングのイネーブル化と設定」（P.23-15）
- 「ポート セキュリティおよびプライベート VLAN」（P.23-17）

ポート セキュリティの概要

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を使用して手動で設定します。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 テーブルにだけ格納され、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、または手動で設定します。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、自動的には格納されません。コンフィギュレーション ファイルに固定セキュア MAC アドレスが保存されている場合は、スイッチを再起動するときに、インターフェイスはこれらのアドレスを再学習する必要がありません。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、システムで許可されている MAC アドレスの最大数によって設定されます。この数字はアクティブな SDM テンプレートによって決められます。第 7 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。

- 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。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 LED が消灯します。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できます。また、**shutdown** および **no shut down** の各インターフェイス 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。これがデフォルトのモードです。

表 23-1 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 23-1　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[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	不可	不可	不可	不可	不可	不可
restrict	不可	あり	あり	不可	あり	不可
shutdown	不可	あり	あり	不可	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 23-2 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 23-2　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 です。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 ポートは、Fast EtherChannel やギガビット EtherChannel ポート グループに属することができません。
- セキュア ポートは、プライベート VLAN ポートにできません。
- トランク ポートにポート セキュリティが設定され、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音声 VLAN に割り当てられている場合、**switchport voice** および **switchport priority extend** の各インターフェイス コンフィギュレーション コマンドは無効です。

  接続されたデバイスで同じ MAC アドレスを使用し、アクセス VLAN の IP および音声 VLAN の IP を要求した場合、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 23-3 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 23-3　ポート セキュリティとその他のスイッチ機能の互換性

ポートのタイプまたはポート上の機能	ポート セキュリティとの互換性
トランク ポート	あり
ダイナミックアクセス ポート（switchport access vlan-dynamic interface conifiguration コマンドで設定される Vlan Query Protocol [VQP]）	不可
ルーテッド ポート	不可
SPAN 送信元ポート	あり
SPAN 宛先ポート	不可
EtherChannel	不可

表 23-3　ポート セキュリティとその他のスイッチ機能の互換性 （続き）

ポートのタイプまたはポート上の機能	ポート セキュリティとの互換性
トンネリング ポート	あり
保護ポート	あり
802.1X ポート	あり
プライベート VLAN ポート	不可
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

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、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id*	設定するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	**no shutdown**	必要に応じて、ポートをイネーブルにします。デフォルトでは、UNI および ENI はディセーブルに、NNI はイネーブルに設定されています。
ステップ 4	**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 ポートとしては設定できません。
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。
ステップ 6	**switchport port-security** [**maximum** *value* [**vlan** *vlan-list* | **access**]	（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設定されます。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 7 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。 （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（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。 • **access**：アクセス ポートで、アクセス VLAN として VLAN を指定します。

	コマンド	目的
ステップ 7	**switchport port-security violation** {**protect** | **restrict** | **shutdown**}	（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。 • **protect**：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。 **（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されません。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**：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。 **（注）** セキュア ポートが errdisable ステートになった場合は、**errdisable recovery cause psecure-violation** グローバル コンフィギュレーション コマンドを使用することにより、ステートを変更できます。また、**shutdown** および **no shutdown** の各インターフェイス 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。
ステップ 8	**switchport port-security** [**mac-address** *mac-address* [**vlan** {*vlan-id* | {**access**}}]	（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。 **（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。 （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。 • **access**：アクセス ポートで、アクセス VLAN として VLAN を指定します。
ステップ 9	**switchport port-security mac-address sticky**	（任意）インターフェイスで固定学習をイネーブルにします。

	コマンド	目的
ステップ 10	**switchport port-security mac-address sticky** [*mac-address* | **vlan** {*vlan-id* | {**access**}]	（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。 **（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。 （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。 • **access**：アクセス ポートで、アクセス VLAN として VLAN を指定します。
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）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。

MAC アドレス テーブルからセキュアなアドレスをすべて削除したり、スイッチまたはインターフェイス上の特定のタイプ（設定済み、ダイナミック、または固定）のセキュア アドレスをすべて削除したりするには、**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に関するダイナミック 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、**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。

次の例では、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 に設定する方法を示します。デフォルトは違反モードで、スタティック セキュア MAC アドレスは設定されていません。また、固定学習がイネーブルに設定されています。

```
Switch(config)# interface gigabitethernet0/1
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 gigabitethernet0/2
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、ポート上で固定ポート セキュリティをイネーブルにして、データ VLAN に MAC アドレスを手動で設定し、セキュア アドレスの最大合計数を 10 に設定する例を示します。

```
Switch(config)# interface FastEthernet0/1
Switch(config-if)# no shutdown
Switch(config-if)# switchport access vlan 21
Switch(config-if)# switchport mode access
Switch(config-if)# switchport port-security
Switch(config-if)# switchport port-security maximum 10
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 maximum 10 vlan access
```

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。

	コマンド	目的
ステップ 3	**no shutdown**	必要に応じて、ポートをイネーブルにします。デフォルトでは、UNI および ENI はディセーブルに、NNI はイネーブルに設定されています。
ステップ 4	**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。 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には、**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、次のキーワードのいずれかを 1 つ選択します。 • **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。 • **inactivity**：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。
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）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 gigabitethernet0/1
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* 特権 EXEC コマンドを入力します。

ポート セキュリティおよびプライベート VLAN

ポート セキュリティでは、管理者がポートで学習された MAC アドレスの数を制限するか、またはポートで学習できる MAC アドレスを定義できます。

PVLAN ホストおよびプロミスキャス ポートにポート 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）コンフィギュレーション ファイルに設定を保存します。

```
Switch(config)# interface GigabitEthernet0/8
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は、セキュア PVLAN ポートと呼ぶ場合があります。セキュア PVLAN ポートでセキュアなアドレスが学習される場合、同じプライマリ VLAN に属しているほかのセキュア PVLAN ポートでは、同じセキュア アドレスを学習できません。ただし、アンセキュアな PVLAN ポートで学習されるアドレスは、同じプライマリ VLAN に属しているセキュア PVLAN ポートで学習できます。

ホスト ポートで学習されるセキュア アドレスは、対応付けられたプライマリ VLAN に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、対応付けられたすべてのセカンダリ VLAN に自動的に複製されます。スタティック アドレス（mac-address-table static コマンドを使用）は、セキュア ポートでは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 23-4 に示す特権 EXEC コマンドを 1 つまたは複数使用します。

表 23-4　トラフィック制御のステータスおよび設定を表示するためのコマンド

コマンド	目的
show interfaces [*interface-id*] **switchport**	すべてのスイッチング（非ルーティング）ポートまたは指定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）。
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。
show port-security [**interface** *interface-id*]	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。
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。
show port-security interface *interface-id* **vlan**	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。