CHAPTER 25

ポートベースのトラフィック制御の設定

この章では、Catalyst 3750 スイッチにポートベースのトラフィック制御機能を設定する方法について説明します。特に明記しないかぎり、*スイッチ*という用語はスタンドアロン スイッチおよびスイッチ スタックを意味します。

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

この章で説明する内容は、次のとおりです。

ストーム制御の設定

ここでは、次の概要および設定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のエラー、ネットワーク設定の誤り、DoS 攻撃をするユーザは、ストームの原因となることがあります。

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数をカウントして、事前定義されている抑制レベルのスレッシュホールドとその測定値を比較します。

ストーム制御では、トラフィック アクティビティの測定に次のいずれかの方式を使用します。

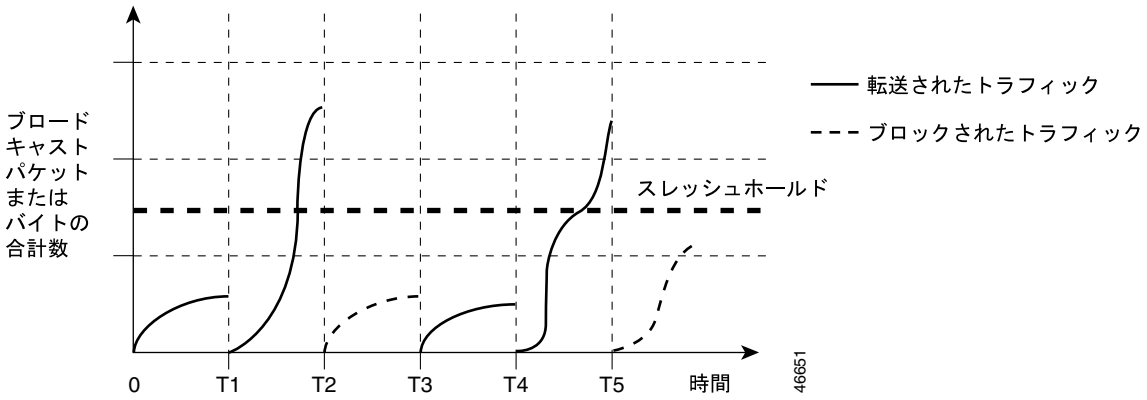
- ブロードキャスト、マルチキャスト、またはユニキャスト トラフィックで使用できるポートの使用可能な帯域幅の合計に対する割合で表される帯域幅
- ブロードキャスト、マルチキャスト、またはユニキャスト パケットを受信する際のパケット / 秒で表されるトラフィック レート（Cisco IOS Release 12.2(25)SE 以降）
- ブロードキャスト、マルチキャスト、またはユニキャスト パケットを受信する際のビット / 秒で表されるトラフィック レート（Cisco IOS Release 12.2(25)SE 以降）

上限スレッシュホールドに達すると、ポートが各方式を使用してトラフィックをブロックします。トラフィック レートが下限スレッシュホールド（指定されている場合）を下回るまでポートはブロックされたままとなり、その後、通常の転送を開始します。下限スレッシュホールド レベルが指定されていない場合、トラフィック レートが上限スレッシュホールド レベルを下回るまで、スイッチはすべてのトラフィックをブロックします。通常、レベルが上がるほどブロードキャスト ストームに対する保護効率は下がります。

（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ュホールドに達すると、Bridge Protocol Data Unit（BPDU; ブリッジ プロトコル データ ユニット）や Cisco Discovery Protocol（CDP）フレームなどの制御トラフィックを除いて、すべてのマルチキャスト トラフィックがブロックされます。ただし、スイッチでは Open Shortest Path First（OSPF）などのルーティング アップデートと、正規のマルチキャスト データ トラフィックは区別されないため、両方のトラフィック タイプがブロックされます。

図25-1のグラフは、一定時間におけるインターフェイス上のブロードキャスト トラフィック パターンを示しています。この例は、マルチキャストおよびユニキャスト トラフィックにも適用できます。この例では、転送されているブロードキャスト トラフィックが、タイム インターバル T1 ～ T2 間および T4 ～ T5 間で設定されたスレッシュホールドを上回っています。特定のトラフィックの量がスレッシュホールドを上回ると、そのタイプのすべてのトラフィックは次の一定時間にわたり、廃棄されます。したがって、ブロードキャスト トラフィックは T2 および T5 のあとのインターバルではブロックされています。次のタイム インターバル（たとえば T3）では、ブロードキャスト トラフィックがスレッシュホールドを上回らなければ、再度転送されます。

図 25-1　ブロードキャスト ストーム制御の例



ストーム制御抑制レベルと 1 秒のタイム インターバルの組み合わせにより、ストーム制御アルゴリズムの動作が制御されます。スレッシュホールドが高いほど、通過できるパケットが多くなります。スレッシュホールドの値が 100% であれば、トラフィックに対する制限はありません。値が 0.0 であれば、ポートのブロードキャスト、マルチキャスト、またはユニキャスト トラフィックがすべてブロックされます。

（注）　パケットは均一の間隔で着信するわけではないため、トラフィック アクティビティを測定する 1 秒のタイム インターバルを設けることによって、ストーム制御の動作に影響を与える可能性があります。

各トラフィック タイプのスレッシュホールドの値を設定するには、**storm-control** インターフェイス コンフィギュレーション コマンドを使用します。

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スレッシュホールド レベルの設定

ポートにストーム制御を設定して、特定のトラフィック タイプ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、実際に強制されるスレッシュホールドは、数パーセント程度、設定されたレベルと異なる場合があります。

（注） ストーム制御がサポートされるのは物理インターフェイスに限られます。EtherChannel ポート チャネル、またはポート チャネルのメンバーの物理インターフェイスでは、CLI（コマンドライン インターフェイス）でコマンドが利用できても、サポートはされません。ストーム制御が設定されている物理インターフェイスが EtherChannel に参加する場合、物理インターフェイスのストーム制御コンフィギュレーションは実行コンフィギュレーションから削除されます。

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、イネーブル EXEC モードで次の手順を実行します。

	コマンド	説明
ステップ 1	**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	説明
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、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です。 キーワードの意味は次のとおりです。 • *level* には、帯域幅割合（小数点以下 2 桁まで）で表すブロードキャスト、マルチキャスト、およびユニキャスト トラフィックの上限スレッシュホールド レベルを指定します。上限スレッシュホールドに達すると、ポートがトラフィックをブロックします。指定できる範囲は 0.00 ～ 100.00 です。 • （任意）*level-low* には、帯域幅割合（小数点以下 2 桁まで）で表す下限スレッシュホールド レベルを指定します。この値は、上限スレッシュホールド値以下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ると、ポートにより転送されます。下限スレッシュホールド レベルを設定しない場合は、上限スレッシュホールド レベルに設定されます。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%）に設定した場合、トラフィックに制限はありません。スレッシュホールドを 0.0 に設定した場合、こ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、およびユニキャスト トラフィックがブロックされます。 • **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 トラフィックの上限スレッシュホールド レベルをビット / 秒で指定します（小数点以下 1 桁まで）。上限スレッシュホールドに達すると、ポートがトラフィックをブロックします。指定できる範囲は 0.0 ～ 10000000000.0 です。 • （任意）*bps-low* には、下限スレッシュホールド レベルをビット / 秒で指定します（小数点以下 1 桁まで）。この値には、上限スレッシュホールド レベル以下の値を指定します。トラフィックがこのレベルを下回ると、ポートにより転送されます。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 トラフィックの上限スレッシュホールド レベルをパケット / 秒で指定します（小数点以下 1 桁まで）。上限スレッシュホールドに達すると、ポートがトラフィックをブロックします。指定できる範囲は 0.0 ～ 10000000000.0 です。 • （任意）*pps-low* には、下限スレッシュホールド レベルをパケット / 秒で指定します（小数点以下 1 桁まで）。この値には、上限スレッシュホールド レベル以下の値を指定します。トラフィックがこのレベルを下回ると、ポートにより転送されます。指定できる範囲は **0.0** ～ 10000000000.0 です。 BPS および PPS 設定では、数の大きなスレッシュホールドを指定する際に、k、m、および g などのメトリック サフィックスを使用できます。

	コマンド	説明
ステップ 4	**storm-control action** {**shutdown** | **trap**}	ストームが検出された場合の対処方法を指定します。デフォルトでは、トラフィックをフィルタリングして排除し、トラップを送信しません。 • **shutdown** キーワードを選択して、ストーム中のポートを errdisable にします。 • **trap**　キーワードを選択して、ストームが検出された場合に SNMP（簡易ネットワーク管理プロトコル）トラップを生成します。
ステップ 5	**end**	イネーブル 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 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。

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% の下限抑制レベルを使用してポート上でユニキャスト 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 gigabitethernet1/0/1
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 パーセントのレベルでイネーブルにする方法を示しています。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 パーセント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 gigabitethernet1/0/1
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。

保護ポートには次のような機能があります。

- 保護ポートは、他の保護ポートにいかなるトラフィック（ユニキャスト、マルチキャスト、またはブロードキャスト）も転送しません。レイヤ 2 では、保護ポート間でデータ トラフィックを転送できません。これらのパケットが CPU によって処理され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。保護ポート間を流れるすべてのトラフィックは、レイヤ 3 デバイスを経由して転送する必要があります。
- 保護ポートと非保護ポート間の転送動作は、通常どおり行われます。

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

ここでは、次の設定について説明します。

- 保護ポートのデフォルト設定（p.25-7）
- 保護ポートの設定時の注意事項（p.25-7）
- 保護ポートの設定（p.25-7）

保護ポートのデフォルト設定

デフォルトでは、保護ポートは定義されていません。

保護ポートの設定時の注意事項

保護ポートは、物理インターフェイス（ギガビット イーサネット ポート 1 など）または EtherChannel グループ（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。

保護ポートとして、プライベート VLAN を設定しないでください。プライベート VLAN として、保護ポートを設定しないでください。プライベート VLAN 隔離ポートは、トラフィックを他の隔離ポートまたはコミュニティ ポートに転送しません。プライベート VLAN の詳細については、第 16 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、イネーブル EXEC モードで次の手順を実行します。

	コマンド	説明
ステップ 1	**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**	イネーブル EXEC モードに戻ります。

	コマンド	説明
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。

次の例は、ポートを保護ポートとして設定する方法を示します。

```
Switch# configure terminal
Switch(config)# interface gigabitethernet1/0/1
Switch(config-if)# switchport protected
Switch(config-if)# end
```

ポート ブロッキングの設定

デフォルトでは、宛先 MAC（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。

ここでは、次の設定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.25-8）
- 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.25-8）

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マルチキャストおよびユニキャスト パケットのフラッディングをディセーブルにするには、イネーブル EXEC モードで次の手順を実行します。

	コマンド	説明
ステップ 1	**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	説明
ステップ 3	**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。
ステップ 4	**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 5	**end**	イネーブル 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）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、ポートでユニキャストおよびマルチキャスト 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 gigabitethernet1/0/1
Switch(config-if)# switchport block multicast
Switch(config-if)# switchport block unicast
Switch(config-if)# end
```

ポート セキュリティの設定

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

セキュア ポートとして設定されたポートのセキュア MAC アドレスが最大数に達した場合に、ポートにアクセスしようとするステーションの MAC アドレスが、識別されたどのセキュア MAC アドレスとも異なるときは、セキュリティ違反が発生します。また、あるセキュア ポートで設定または学習されたセキュア MAC アドレスを持つステーションが別のセキュア ポートにアクセスしようとすると、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、次の概要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 — 動的に設定されます。これらはアドレス テーブルにのみ格納され、スイッチが再起動するときに削除されます。
- *固定* セキュア MAC アドレス — 動的に学習されるか、または手動で設定されます。これらはアドレス テーブルに格納され、実行コンフィギュレーションに追加されます。これらのアドレスがコンフィギュレーション ファイルに保存されている場合は、スイッチを再起動するときに、インターフェイスがアドレスを動的に再設定する必要はありません。

*固定学習*をイネーブルにすると、ダイナミック MAC アドレスを固定セキュア MAC アドレスに変換し、それらを実行コンフィギュレーションに追加するように、インターフェイスを設定できます。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。固定セキュア アドレスは、保存しないと失われます。

固定学習がディセーブルの場合、固定セキュア MAC アドレスはダイナミック セキュア アドレスに変換されて、実行コンフィギュレーションから削除されます。

スイッチ スタックに設定できるセキュア MAC アドレスの最大数は、システムで許可されている MAC アドレスの最大数によって決まります。この値は、アクティブな Switch Database Management（SDM）テンプレートによって設定されます。第 8 章「SDM テンプレートの設定」を参照してください。この値は、使用可能な MAC アドレス（その他のレイヤ 2 機能やインターフェイスに設定されたその他のセキュア MAC アドレスで使用される MAC アドレスを含む）の総数です。

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、同一 VLAN（仮想 LAN）内の別のセキュア インターフェイスで認識された場合

違反発生時の対処方法に関して、次の 3 つの違反モードのいずれかにインターフェイスを設定できます。

- protect — セキュア MAC アドレスの数がポートに許容された最大限度に達した場合、十分な数のセキュア MAC アドレスを削除して最大限度以下にするか、またはアドレスの最大許容数を増やすまで、不明の送信元アドレスを持つパケットは廃棄されます。セキュリティ違反が起こっても、ユーザには通知されません。

（注） トランク ポートには protect 違反モードを設定しないでください。保護モードを使用すると、ポートが最大限度に達していない場合でも、VLAN が最大限度に達したときに、学習がディセーブルになります。

- restrict — セキュア MAC アドレスの数がポートに許容された最大限度に達した場合、十分な数のセキュア MAC アドレスを削除して最大限度以下にするか、またはアドレスの最大許容数を増やすまで、不明の送信元アドレスを持つパケットは廃棄されます。このモードでは、セキュリティ違反が起こった場合、ユーザに通知されます。SNMP トラップが送信され、Syslog メッセージが記録されて、違反カウンタが増加します。

- shutdown ― ポート セキュリティ違反が発生すると、インターフェイスは errdisable ステートになって、ただちにシャットダウンし、ポート LED が消灯します。SNMP トラップが送信され、Syslog メッセージが記録されて、違反カウンタが増加します。セキュア ポートが errdisable ステートになった場合は、**errdisable recovery cause** *psecure-violation* グローバル コンフィギュレーション コマンドを入力してこのステートを変更できます。また、**shutdown** および **no shut down** インターフェイス コンフィギュレーション コマンドを入力することにより、ポートを手動でイネーブルに戻すこともできます。デフォルトはこのモードに設定されています。

表 25-1 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 25-1　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	なし	なし	なし	なし	なし	なし
restrict	なし	あり	あり	なし	あり	なし
shutdown	なし	あり	あり	なし	あり	あり

1. 送信元アドレスが不明なパケットは、十分な数のセキュア MAC アドレスが削除されるまで、廃棄されます。
2. 手動で設定したアドレスがセキュリティ違反の原因となる場合には、スイッチによりエラー メッセージが返されます。

ポート セキュリティのデフォルト設定

表 25-2 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 25-2　ポート セキュリティのデフォルト設定

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

ポート セキュリティ設定時の注意事項

ポート セキュリティの設定時は、次の注意事項に従ってください。

- ポート セキュリティを設定できるのは、スタティック アクセス ポートまたはトランク ポートに限られます。セキュア ポートはダイナミック アクセス ポートにできません。
- セキュア ポートは、Switched Port Analyzer（SPAN; スイッチド ポート アナライザ）の宛先ポートにできません。
- セキュア ポートは、Fast EtherChannel や Gigabit EtherChannel ポート グループに属すことができません。

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

- セキュア ポートはプライベート VLAN ポートにはできません。
- インターフェイス上でポート セキュリティをイネーブルにし、さらに音声 VLAN を使用するようにも設定する場合は、ポートで許可されるセキュア アドレスの最大数を、アクセス VLAN で許可されているセキュア アドレスの最大数に 2 を加えた値に設定する必要があります。ポートが Cisco IP Phone に接続されている場合は、IP Phone に MAC アドレスが最大で 2 つ必要です。IP Phone アドレスは音声 VLAN 上で学習されますが、アクセス VLAN 上で学習される場合もあります。PC を IP Phone に接続するには、さらに MAC アドレスが必要になります。
- 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を上書きします。新しい値が古い値よりも小さく、インターフェイスに設定されたセキュア アドレス数が新しい値を超えている場合、コマンドは拒否されます。
- スイッチでは、固定セキュア MAC アドレスのポート セキュリティ エージングをサポートしません。

表 25-3 に、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について示します。

表 25-3　ポートセキュリティと他の機能との互換性

ポート 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
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
トンネル ポート	あり
保護ポート	あり
IEEE 802.1x ポート	あり
音声 VLAN ポート[4]	あり
プライベート VLAN ポート	なし
IP ソース ガード	あり
ダイナミック Address Resolution Protocol（ARP）検査	あり
Flex Link	あり

1. DTP = Dynamic Trunking Protocol
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）
4. ポートで許可されるセキュア アドレスの最大数を、アクセス VLAN で許可されているセキュア アドレスの最大数に 2 を加えた値に設定する必要があります。

ポート セキュリティのイネーブル化と設定

ポートへのアクセスが許可されたステーションの MAC アドレスを制限および識別する方法でインターフェイスへの入力を制限するには、イネーブル EXEC モードで次の手順を実行します。

	コマンド	説明
ステップ 1	**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*	音声 VLAN をポートでイネーブルにします。 *vlan-id* — 音声トラフィック用に使用する 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。
ステップ 6	**switchport port-security** [**maximum** *value* [**vlan** {*vlan-list* | {**access** | **voice**}}]]	（任意）インターフェイスについてセキュア MAC アドレスの最大数を設定します。スイッチ スタックに設定できるセキュア MAC アドレスの最大数は、システムで許可されている MAC アドレスの最大数によって決まります。この値は、アクティブな SDM テンプレートによって設定されます。第 8 章「スイッチ SDM テンプレートの設定」を参照してください。この値は、使用可能な MAC アドレス（他のレイヤ 2 機能やインターフェイスに設定された他のセキュア MAC アドレスで使用される MAC アドレスを含む）の総数です。 （任意）**vlan** — VLAN 単位の最大値を設定します。 **vlan** キーワードの入力後、次のうちいずれかのオプションを入力します。 • *vlan-list* — 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）により、VLAN 単位の最大値をトランク ポートで設定できます。指定されない VLAN については、VLAN 単位の最大値が使用されます。 • **access** — アクセス ポートにおいて、アクセス VLAN として VLAN を指定します。 • **voice** — アクセス ポートにおいて、音声 VLAN として VLAN を指定します。 **（注）** 音声 VLAN をポートで設定しており、そのポートがアクセス VLAN でない場合にのみ、**voice** キーワードを使用できます。

	コマンド	説明
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 ポートには protect モードを設定しないでください。保護モードを使用すると、ポートが最大限度に達していない場合でも、VLAN が最大限度に達したときに、学習がディセーブルになります。 • **restrict —** セキュア MAC アドレスの数がポートの許容限度に達した場合、十分な数のセキュア MAC アドレスを削除するか、またはアドレスの最大許容数を増加させるまで、不明の送信元アドレスを持つパケットは廃棄されます。SNMP トラップが送信され、Syslog メッセージが記録されて、違反カウンタが増加します。 • **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、Syslog メッセージが記録されて、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 shut down** インターフェイス コンフィギュレーション コマンドを入力することにより、手動でポートをイネーブルに戻すこともできます。

	コマンド	説明
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** キーワードの入力後、次のうち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 ポートにおいて、アクセス VLAN として VLAN を指定します。 • **voice —** アクセス ポートにおいて、音声 VLAN として VLAN を指定します。 **（注）** 音声 VLAN をポートで設定しており、そのポートがアクセス VLAN でない場合にのみ、**voice** キーワードを使用できます。
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	説明
ステップ 10	**switchport port-security mac-address sticky** [*mac-address* | **vlan** {*vlan-id* | {**access** | **voice**}}]	（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** キーワードの入力後、次のうち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 ポートにおいて、アクセス VLAN として VLAN を指定します。 • **voice —** アクセス ポートにおいて、音声 VLAN として VLAN を指定します。 **（注）** 音声 VLAN をポートで設定しており、そのポートがアクセス VLAN でない場合にのみ、**voice** キーワードを使用できます。
ステップ 11	**end**	イネーブル EXEC モードに戻ります。
ステップ 12	**show port-security**	設定を確認します。
ステップ 13	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

インターフェイスをデフォルトの非セキュア ポートに戻すには、**no switchport port-security** インターフェイス コンフィギュレーション コマンドを使用します。固定学習がイネーブルの場合にこのコマンドを入力すると、固定学習アドレスは実行コンフィギュレーション内に残りますが、アドレス テーブルからは削除されます。ここで、すべてのアドレスが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。

インターフェイス上で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**} イネーブル EXEC コマンドを使用します。

アドレス テーブルから特定のセキュア 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上のすべてのダイナミック セキュア アドレスを削除するには、**no switchport port-security** インターフェイス コンフィギュレーション コマンドのあとに、**switchport port-security** コマンドを入力して、インターフェイスのポート セキュリティをイネーブルに戻します。**no switchport port-security mac-address sticky** インターフェイス コンフィギュレーション コマンドを使用して、固定セキュア MAC アドレスをダイナミック セキュア MAC アドレスに変換してから、**no switchport port-security** コマンドを入力すると、手動で設定されたセキュア アドレスを除き、インターフェイス上のすべてのセキュア アドレスが削除されます。

no switchport port-security mac-address *mac-address* インターフェイス コンフィギュレーション コマンドを使用して、アドレス テーブルから設定済みのセキュア MAC アドレスを削除する必要があります。

次に、ポートでポート セキュリティをイネーブルにし、セキュア アドレスの最大数を 50 に設定する例を示します。違反モードはデフォルト設定、スタティック セキュア MAC アドレスは設定なし、固定学習はイネーブルにします。

```
Switch(config)# interface gigabitethernet1/0/1
Switch(config-if)# switchport mode access
Switch(config-if)# switchport port-security
Switch(config-if)# switchport port-security maximum 50
Switch(config-if)# switchport port-security mac-address sticky
```

次に、スタティック セキュア MAC アドレスをポートの VLAN 3 に設定する例を示します。

```
Switch(config)# interface gigabitethernet1/0/2
Switch(config-if)# switchport mode trunk
Switch(config-if)# switchport port-security
Switch(config-if)# switchport port-security mac-address 0000.02000.0004 vlan 3
```

次に、固定ポート セキュリティをポートでイネーブルにし、データ VLAN と音声 VLAN に MAC アドレスを手動設定し、セキュア アドレスの最大総数を 20（データ VLAN に 10、音声 VLAN に 10）に設定する例を示しています。

```
Switch(config)# interface FastEthernet1/0/1
Switch(config-if)# switchport access vlan 21
Switch(config-if)# switchport mode access
Switch(config-if)# switchport voice vlan 22
Switch(config-if)# switchport port-security
Switch(config-if)# switchport port-security maximum 20
Switch(config-if)# switchport port-security violation restrict
Switch(config-if)# switchport port-security mac-address sticky
Switch(config-if)# switchport port-security mac-address sticky 0000.0000.0002
Switch(config-if)# switchport port-security mac-address 0000.0000.0003
Switch(config-if)# switchport port-security mac-address sticky 0000.0000.0001 vlan
voice
Switch(config-if)# switchport port-security mac-address 0000.0000.0004 vlan voice
Switch(config-if)# switchport port-security maximum 10 vlan access
Switch(config-if)# switchport port-security maximum 10 vlan voice
```

ポート セキュリティ エージングのイネーブル化と設定

ポート セキュリティ エージングを使用すると、ポート上の全セキュア 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 セキュリティのエージング タイムを設定するには、イネーブル EXEC モードで次の手順を実行します。

	コマンド	説明
ステップ 1	**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 4	**end**	イネーブル EXEC モードに戻ります。
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）コンフィギュレーション ファイルに設定を保存します。

ポート上のすべてのセキュア アドレスに対してポート セキュリティ エージングをディセーブルにするには、**no switchport port-security aging time** インターフェイス コンフィギュレーション コマンドを使用します。スタティックに設定されたセキュア アドレスに対してだけエージングをディセーブルにするには、**no switchport port-security aging static** インターフェイス コンフィギュレーション コマンドを使用します。

次に、ポートのセキュア アドレスのエージング タイムを 2 時間に設定する例を示します。

```
Switch(config)# interface gigabitethernet1/0/1
Switch(config-if)# switchport port-security aging time 120
```

次に、このインターフェイスに設定されたセキュア アドレスのエージングをイネーブルにし、エージング タイプを inactivity に、エージング タイムを 2 分に設定する例を示します。

```
Switch(config-if)# switchport port-security aging time 2
Switch(config-if)# switchport port-security aging type inactivity
Switch(config-if)# switchport port-security aging static
```

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

ポート セキュリティおよびスイッチ スタック

スタックに新規に加入したスイッチは、設定済みのセキュア アドレスを取得します。他のスタック メンバーから新しいスタック メンバーに、ダイナミック セキュア アドレスがすべてダウンロードされます。

スイッチ（スタック マスターまたはスタック メンバーのいずれか）がスタックから脱退すると、残りのスタック メンバーに通知されて、そのスイッチによって設定または学習されたセキュア MAC アドレスがセキュア MAC アドレス テーブルから削除されます。スイッチ スタックの詳細については、第 5 章「スイッチ スタックの管理」を参照してください。

ポートベースのトラフィック制御設定の表示

show interfaces *interface-id* **switchport** イネーブル EXEC コマンドを使用すると、(各種の特性とともに）インターフェイスのトラフィック抑制および制御の設定が表示されます。**show storm-control** および **show port-security** イネーブル EXEC コマンドを使用すると、それぞれストーム制御とポート セキュリティ設定が表示されます。

トラフィック制御情報を表示するには、表 25-4 に示すイネーブル EXEC コマンドを 1 つまたは複数使用します。

表 25-4　トラフィック制御のステータスおよび設定表示用のコマンド

コマンド	説明
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について、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。