CHAPTER 24

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 Metro 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、ストーム制御の設定および手順について説明します。

ストーム制御の概要

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。ストームは、プロトコル スタック実装でのエラー、ネットワーク設定の誤り、および DoS 攻撃（サービス拒絶攻撃）を行うユーザにより引き起こされる可能性があります。

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法を使用します。

- ブロードキャスト、マルチキャスト、またはユニキャスト トラフィックが使用できるポートの利用可能な総帯域幅のパーセンテージとしての帯域幅
- ブロードキャスト、マルチキャスト、またはユニキャスト パケットが受信される、1 秒あたりのパケット単位のトラフィック レート（Cisco IOS Release 12.2(25)EY 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 パケットが受信される、1 秒あたりのビット単位のトラフィック レート（Cisco IOS Release 12.2(25)EY 以降）

どの方法でも、上限しきい値に達すると、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）以下になり通常の転送が再開されるまで、ポートはブロックされたままの状態になります。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。一般的に、レベルが高いほど、ブロードキャスト ストームに対する保護の効果が少なくなります。

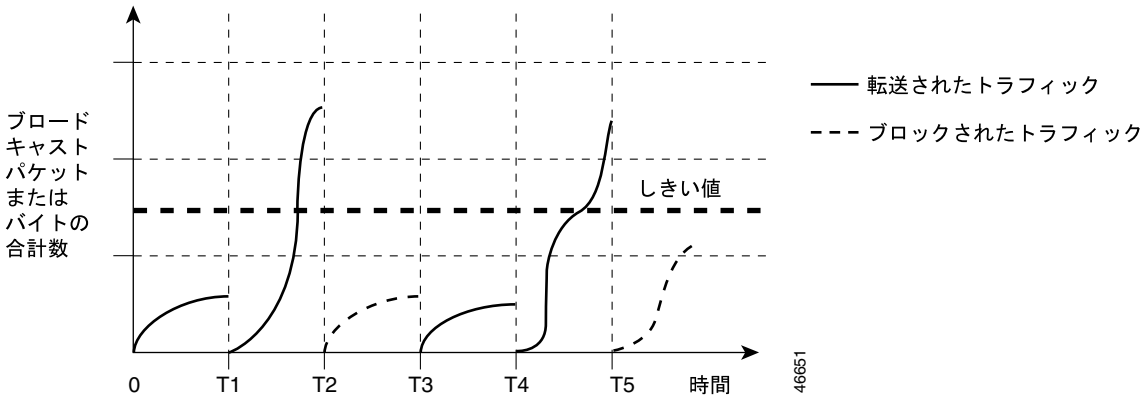
（注）　マルチキャスト トラフィックのストーム制御しきい値に達すると、Bridge Protocol Data Unit（BPDU; ブリッジ プロトコル データ ユニット）や Cisco Discovery Protocol（CDP）フレームなどの制御トラフィックを除いて、すべてのマルチキャスト トラフィックがブロックされます。ただし、スイッチでは OSPF などのルーティング アップデートと、正規のマルチキャスト データ トラフィックは区別されないため、両方のトラフィック タイプがブロックされます。

ストーム制御がイネーブルの場合、スイッチはインターフェイスからスイッチング バスへ流れるパケットをモニタし、そのパケットがユニキャスト、マルチキャスト、ブロードキャストのいずれであるかを判別します。スイッチは、受信したユニキャスト、マルチキャスト、またはブロードキャストの数を 200 ミリ秒以内のタイム インターバルでモニタし、あるタイプのトラフィックがしきい値に達すると、そのタイプのトラフィックを廃棄します。このしきい値は、ブロードキャスト（マルチキャストまたはユニキャスト）トラフィックが利用可能な総帯域幅に対する割合として指定します。

図24-1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 24-1　ブロードキャスト ストーム制御の例



ストーム制御抑制レベルと 200 ミリ秒のタイム インターバルの組み合わせにより、ストーム制御アルゴリズムの動作を制御します。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 200 ミリ秒のタイム インターバルを設けることによって、ストーム制御の動作に影響を与える可能性があります。

スイッチは、ポートのトラフィックを引き続きモニタし、利用率がしきい値のレベルを下回ると、廃棄されていたトラフィック タイプの転送を再開します。

各トラフィック タイプの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

ポート上でストーム制御を設定し、特定タイプのトラフィックに使用するしきい値の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、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。

ストーム制御の設定の際は、次の注意事項に従ってください。

- スイッチが Label Switching Router（LSR; ラベル スイッチング ルータ）として動作している場合、2 つの enhanced-services（ES）ポート間のマルチプロトコル ラベル スイッチング（MPLS）トラフィックはカウントされません。
- 階層型入力 QoS サービス ポリシーが ES ポートに付加されている場合、サービス ポリシーで指定されるアクションは、ストーム制御が有効になる前に処理されます。設定したしきい値より高いレートでスイッチがトラフィックを受信している場合でも、ストーム制御アクションが実行されないように、サービス ポリシーのアクションで、トラフィックを受信するレートが減少させられることがあります。

（注） ストーム制御は、物理インターフェイス上でサポートされます。ストーム制御は EtherChannel 上にも設定できます。ストーム制御を EtherChannel 上に設定すると、ストーム制御設定はその EtherChannel のすべての物理インターフェイスに伝播されます。

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

	コマンド	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*	インターフェイス コンフィギュレーション モードを開始し、設定する物理インターフェイスのタイプおよび番号（たとえば、**gigabitethernet1/0/1**）を入力します。
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、およびユニキャスト 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なっています。 キーワードの意味は次のとおりです。 • *level* では、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のレベルを帯域幅のパーセンテージ（小数第 2 位まで）として指定します。上限しきい値に達すると、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。 • （任意）*level-low* では、下限しきい値のレベルを帯域幅のパーセンテージ（小数第 2 位まで）として指定します。この値は、上限抑制値と等しいか、またはそれ以下で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たとき、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、上限抑制レベルと同じに設定されます。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、トラフィックの制限はなくなります。しきい値を 0.0 に設定すると、そのポートで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* では、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のレベルをビット / 秒（小数第 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。

	コマンド	説明
		• （任意）*bps-low* では、下限しきい値のレベルをビット / 秒（小数第 1 位まで）で指定します。上限しきい値のレベルと等しいかそれ以下にすることが可能です。トラフィックがこのレベルを下回ったとき、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。 • **pps** *pps* では、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のレベルをパケット / 秒（小数第 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。 • （任意）*pps-low* では、下限しきい値のレベルをパケット / 秒（小数第 1 位まで）で指定します。上限しきい値のレベルと等しいかそれ以下にすることが可能です。トラフィックがこのレベルを下回ったとき、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。 BPS および PPS 設定では、数値の大きいしきい値に対して k、m、および g などメトリックのサフィッ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に実行するアクションを指定します。デフォルトは、トラフィックをフィルタリングしてトラップを送信しないアクションです。 • ストームの際にポートをエラーディセーブルにするには、**shutdown** キーワードを選択します。 • ストームが検出されたとき 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、**trap** キーワードを選択します。
ステップ 5	**end**	特権 EXEC モードに戻ります。
ステップ 6	**show 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 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% の上限抑制レベルおよび 65% の下限抑制レベルが設定された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
```

次に、ポートで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。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内でポートに設定されたレベルである使用可能な総帯域幅の 20% を超えると、スイッチは、トラフィック ストーム制御インターバルが終わるまで、すべてのブロードキャスト トラフィックを破棄します。

```
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、保護ポート間でトラフィックを転送できません。したがって、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。

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（GigabitEthernet 1/0/1 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 ポートを保護ポートとして設定しないでください。また、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 隔離ポートは、別の隔離ポートまたはコミュニティ 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 14 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	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*	インターフェイス コンフィギュレーション モードを開始し、設定するインターフェイスのタイプおよび番号（たとえば、**gigabitethernet1/0/1**）を入力します。
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）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、インターフェイスを保護ポートとして設定する例を示します。

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

ポート ブロッキングの設定

デフォルトでは、宛先 MAC アドレスが不明のパケットは、すべてのポートからフラッディングされます。不明のユニキャストおよびマルチキャスト トラフィックが保護ポートに転送されると、セキュリティ上の問題が発生することがあります。不明のユニキャストまたはマルチキャスト トラフィックがポート間で転送されないようにするため、不明のユニキャストまたはマルチキャスト パケットが他のポートにフラッディングされないようにポート（保護ポートまたは非保護ポート）をブロックできます。

ポート ブロッキングのデフォルト設定

デフォルトでは、ポートから送信される不明のマルチキャストおよびユニキャスト トラフィックのフラッディングはブロックされません。これらのトラフィックは、すべてのポートにフラッディングされます。

インターフェイスでのフラッディング トラフィックのブロック

（注） インターフェイスとして、物理インターフェイス（GigabitEthernet 1/0/1 など）または EtherChannel グループ（port-channel 5 など）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、特権 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*	インターフェイス コンフィギュレーション モードを開始し、設定するインターフェイスのタイプおよび番号（たとえば、**gigabitethernet1/0/1**）を入力します。
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**	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）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、インターフェイス上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、ポート セキュリティの設定および手順について説明します。

ポート セキュリティの概要

ここでは、次の内容について説明します。

セキュア MAC アドレス

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 — 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、スイッチを再起動するときに、インターフェイスがアドレスをダイナミックに再設定する必要はありません。

*固定学習*をイネーブルにすると、ダイナミック MAC アドレスを固定セキュア MAC アドレスに変換し、それらを実行コンフィギュレーションに追加するように、インターフェイスを設定することができます。固定学習をイネーブルにするには、**switchport port-security mac-address sticky** インターフェイス コンフィギュレーション コマンドを入力します。このコマンドを入力すると、インターフェイスはすべてのダイナミック セキュア MAC アドレス（固定学習がイネーブルになる前にダイナミック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。

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。

- 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発生しても、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。protect モードを使用すると、ポートが最大限度に達していない場合でも、VLAN が最大限度に達すると、学習がディセーブルになります。

- restrict — セキュア MAC アドレスの数がポートに許容された最大限度に達した場合、十分な数のセキュア MAC アドレスを削除して最大限度以下にするか、またはアドレスの最大許容数を増やすまで、不明の送信元アドレスを持つパケットは廃棄されます。このモードでは、セキュリティ違反が発生した場合、ユーザに通知されます。SNMP トラップが送信され、Syslog メッセージが記録されて、違反カウンタが増加します。
- shutdown — ポート セキュリティ違反が発生すると、インターフェイスは errdisable ステートになって、ただちにシャットダウンし、ポート LED が消灯します。SNMP トラップが送信され、Syslog メッセージが記録されて、違反カウンタが増加します。セキュア ポートが errdisable ステートになった場合は、**errdisable recovery cause** *psecure-violation* グローバル コンフィギュレー

ション コマンドを入力してこのステートを変更することができます。また、**shutdown** および **no shut down** インターフェイス コンフィギュレーション コマンドを入力することにより、ポートを手動でイネーブルに戻すこともできます。デフォルトはこのモードに設定されています。

表 24-1 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 24-1　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	シャットダウン ポート
protect	なし	なし	なし	なし	なし	なし
restrict	なし	あり	あり	なし	あり	なし
shutdown	なし	あり	あり	なし	あり	あり

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

ポート セキュリティのデフォルト設定

表 24-2 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 24-2　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
各ポートのセキュア MAC アドレス最大数	1
違反モード	shutdown。セキュア MAC アドレスの最大数を超過すると、ポートはシャットダウンします。
ポート セキュリティのエージング	ディセーブル。エージング タイムは 0 です。 スタティック エージングはディセーブルです。 タイプは absolute です。

設定時の注意事項

ポート セキュリティの設定時は、次の注意事項に従ってください。

- ポート セキュリティを設定できるのは、スタティック アクセス ポート、トランク ポート、またはトンネル 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 ポートは、Switched Port Analyzer（SPAN; スイッチド ポート アナライザ）の宛先ポートにできません。
- セキュア ポートは、Fast EtherChannel や Gigabit EtherChannel ポート グループに属することはできません。
- 音声 VLAN では、スタティック セキュア MAC アドレスまたは固定セキュア MAC アドレスを設定できません。

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

- セキュア ポートはプライベート VLAN ポートにできません。
- 音声 VLAN 用にも設定されている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するときは、ポートで許可されるセキュア アドレスの最大数を 2 に設定します。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 1 つ必要です。Cisco 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 アドレスを追加する必要はありません。複数の PC を Cisco IP Phone に接続する場合は、各 PC 用に 1 つと Cisco IP Phone 用に 1 つ使用するの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。
- アクセス VLAN 上でいずれかのタイプのポート セキュリティがイネーブルの場合は、音声 VLAN 上でダイナミック ポート セキュリティが自動的にイネーブルになります。VLAN 単位でポート セキュリティを設定することはできません。
- 固定セキュア ポートとして設定されたセキュア ポートに音声 VLAN が設定されている場合、音声 VLAN のすべてのアドレスはダイナミック セキュア アドレスとして学習されます。また、ポートが属するアクセス VLAN で認識されるすべてのアドレスは、固定セキュア アドレスとして学習されます。
- インターフェイスのセキュア アドレスの最大値として入力した値が古い値よりも大きい場合は、新しい値が古い設定値よりも優先します。新しい値が古い値よりも小さく、インターフェイスに設定されたセキュア アドレス数が新しい値を超えている場合、コマンドは拒否されます。
- スイッチでは、固定セキュア MAC アドレスのポート セキュリティ エージングをサポートしません。

ポート セキュリティのイネーブル化と設定

ポートへのアクセスが許可されたステーションの MAC アドレスを制限および識別する方法でインターフェイスへの入力を制限するには、特権 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*	インターフェイス コンフィギュレーション モードを開始し、設定する物理インターフェイス（たとえば、**gigabitethernet1/0/1**）を入力します。
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 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	説明
ステップ 5	**switchport port-security maximum** *value* [**vlan** [*vlan-list*]]	（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。インターフェイスが音声 VLAN 用に設定されている場合は、最大 2 つのセキュア MAC アドレスを設定します。 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決まります。この値は、アクティブな SDM テンプレートによって決まります。第 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）トランク ポートの場合は、VLAN にセキュア MAC アドレスの最大数を設定できます。**vlan** キーワードを入力しない場合は、デフォルト値が使用されます。 • **vlan** — VLAN 単位の最大値を設定します。 • **vlan** *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）に関する VLAN 単位の最大値を設定します。指定されない VLAN については、VLAN 単位の最大値が使用されます。

	コマンド	説明
ステップ 6	**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発生しても、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。protect モードを使用すると、ポートが最大限度に達していない場合でも、VLAN が最大限度に達すると、学習がディセーブルになります。 • **restrict —** セキュア MAC アドレスの数がポート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、ステートを変更することができます。また、**shutdown** および **no shut down** インターフェイス コンフィギュレーション コマンドを入力することにより、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 7	**switchport port-security mac-address** *mac-address* [**vlan** *vlan-id*]	（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 アドレスはダイナミックに学習されます。 （任意）トランク ポートでは、VLAN ID および MAC アドレスを指定できます。VLAN ID を指定しないと、ネイティブ VLAN が使用されます。 **（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、ダイナミック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。
ステップ 8	**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 9	**switchport port-security mac-address sticky** *mac-address*	（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 アドレスはダイナミックに学習され、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。
ステップ 10	**end**	特権 EXEC モードに戻ります。
ステップ 11	**show port-security**	設定を確認します。
ステップ 12	**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の shutdown モードに戻すには、**no switchport port-security violation** {**protocol** | **restrict**} インターフェイス コンフィギュレーション コマンドを使用します。

固定学習をディセーブルにするには、**no switchport port-security mac-address sticky** インターフェイス コンフィギュレーション コマンドを実行します。インターフェイスは固定セキュア MAC アドレスをダイナミック セキュア アドレスに変換します。ただし、固定 MAC アドレスを含む設定がすでに保存されている場合は、**no switchport port-security mac-address sticky** コマンドを入力したあとに再び設定を保存する必要があります。保存しない場合スイッチを再起動すると固定アドレスが復元されます。

アドレス テーブルから特定のセキュア MAC アドレスを削除するには、**no switchport port-security mac-address** *mac-address* インターフェイス コンフィギュレーション コマンドを使用します。

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

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

次に、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、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、インターフェイスに VLAN 3 のスタティック セキュア MAC アドレスを設定する例を示します。

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

ポート セキュリティ エージングのイネーブル化と設定

ポート セキュリティ エージングを使用すると、ポート上の全セキュア アドレスにエージング タイムを設定できます。ポートごとに 2 種類のエージングがサポートされています。

- absolute — ポートのセキュア アドレスは、指定のエージング タイムの経過後に削除されます。
- 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のみです。

この機能を使用すると、既存のセキュア MAC アドレスを手動で削除しなくても、セキュア ポートでデバイスの削除や追加を実行でき、しかもポートのセキュア アドレスの数を制限することができます。また、セキュア アドレスのエージングをポート単位でイネーブルまたはディセーブルに設定することができます。

ポート セキュリティのエージング タイムを設定するには、特権 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*	ポート セキュリティ エージングをイネーブルにするポートについて、インターフェイス コンフィギュレーション モードを開始します。

	コマンド	説明
ステップ 3	**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 タイムまたは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。 このポートで、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 1 ～ 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 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**	特権 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、インターフェイス上でセキュア 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* 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

ポート セキュリティを使用すると、ポートで学習される MAC アドレス数を制限したり、ポートで学習できる MAC アドレスを定義できます。

PVLAN ホストと混合ポート上にポート 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	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 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 GigabitEthernet 1/0/8
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 ポートと呼ばれます。セキュア PVLAN ポートでセキュア アドレスが学習されると、同じプライマリ VLAN に属する他のセキュア PVLAN ポートで、同じセキュア アドレスを学習できなくなります。ただし、セキュアでない 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 ポートで学習できます。

ホスト ポートで学習されたセキュア アドレスは、関連するプライマリ VLAN に自動的に複製されます。同様に、混合ポートで学習されたセキュア アドレスは、関連する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）を、セキュア ポートでユーザが設定することはできません。

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 24-3 に示す特権 EXEC コマンドを 1 つまたは複数使用します。

表 24-3　トラフィック制御のステータスおよび設定表示用のコマンド

コマンド	説明
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。