



ポート単位のトラフィック制御の設定

この章では、Catalyst 3560 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、このリリースに対応する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 \(p.24-2\)](#)
- [保護ポートの設定 \(p.24-7\)](#)
- [ポートブロッキングの設定 \(p.24-9\)](#)
- [ポートセキュリティの設定 \(p.24-10\)](#)
- [ポート単位のトラフィック制御設定の表示 \(p.24-20\)](#)

ストーム制御の設定

ここでは、次の概念と設定情報について説明します。

- [ストーム制御の概要 \(p.24-2\)](#)
- [ストーム制御のデフォルト設定 \(p.24-3\)](#)
- [ストーム制御およびしきい値レベルの設定 \(p.24-4\)](#)

ストーム制御の概要

ストーム制御は、物理インターフェイスの 1 つで発生したブロードキャスト、マルチキャスト、またはユニキャスト ストームによって LAN 上のトラフィックが混乱することを防ぎます。LAN ストームは、LAN にパケットがフラッディングした場合に発生します。その結果、トラフィックが極端に増えてネットワーク パフォーマンスが低下します。プロトコルスタックの実装エラー、ネットワーク構成の間違い、またはユーザによって引き起こされる DoS 攻撃もストームの原因になります。

ストーム制御 (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 バスを通過するパケットをモニタし、パケットがユニキャスト、マルチキャスト、またはブロードキャストのいずれであるかを判別します。スイッチは、1 秒間に受け取った特定のタイプのパケットの数をカウントして、事前に定義された抑制レベルのしきい値とその測定結果を比較します。

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

- 帯域幅 (ブロードキャスト、マルチキャスト、またはユニキャスト トラフィックが使用できるポートの総帯域幅の割合)
- 秒単位で受信するパケット (ブロードキャスト、マルチキャスト、ユニキャスト) のトラフィック レート (Cisco IOS Release 12.2(25)SE 以降)
- 秒単位で受信するビット (ブロードキャスト、マルチキャスト、ユニキャスト) のトラフィック レート (Cisco IOS Release 12.2(25)SE 以降)

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

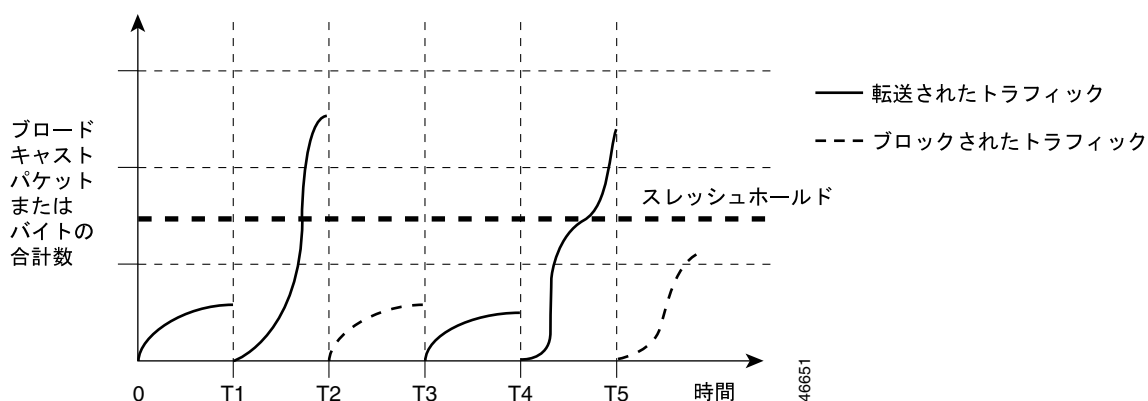


(注)

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

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当てはまります。この例では、T1 から T2、T4 から T5 のタイムインターバルで、転送するブロードキャストトラフィックが設定されたしきい値を上回っています。指定のトラフィック量がしきい値を上回ると、次のインターバルで、そのタイプのトラフィックがすべて廃棄されます。したがって、T2 と T5 のあとのインターバルの間、ブロードキャストトラフィックがブロックされます。その次のインターバル（たとえば、T3）では、しきい値を上回らないかぎり、ブロードキャストトラフィックが再び転送されます。

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 1 秒間のインターバルを組み合わせると、ストーム制御アルゴリズムの動作を制御します。しきい値が高いほど、通過するパケット数が多くなります。しきい値が 100% であれば、トラフィックに対する制限はありません。値を 0.0 にすると、そのポート上ではすべてのブロードキャスト、マルチキャスト、またはユニキャストトラフィックがブロックされます。



(注) パケットは一定の間隔で届くわけではないので、トラフィック アクティビティを測定する 1 秒間のインターバルがストーム制御の動作を左右する可能性があります。

各トラフィック タイプのしきい値を設定するには、`storm-control` インターフェイス コンフィギュレーション コマンドを使用します。

ストーム制御のデフォルト設定

デフォルトでは、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スイッチ インターフェイス上でディセーブルになります。したがって、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

ポートにストーム制御を設定し、特定のトラフィック タイプで使用するしきい値レベルを入力します。

ただし、ハードウェアの制約とともに、さまざまなサイズの packets をどのように数えるかという問題があるので、しきい値の割合はあくまでも近似値です。着信トラフィックを形成する packets のサイズによって、実際に適用されるしきい値は設定されたレベルに対して、数パーセントの差異が生じる可能性があります。



(注)

ストーム制御は、物理インターフェイス上でサポートされます。また、EtherChannel 上でもストーム制御を設定できます。ストーム制御が EtherChannel に設定されている場合、ストーム制御設定は EtherChannel 物理インターフェイスに伝播します。

ストーム制御としきい値レベルを設定するには、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	<code>configure terminal</code>	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	<code>interface interface-id</code>	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	<pre>storm-control {broadcast multicast unicast} level {level [level-low] bps bps [bps-low] pps pps [pps-low]}</pre>	<p>ブロードキャスト、マルチキャスト、またはユニキャスト ストーム制御を設定します。デフォルトでは、ストーム制御はディセーブルに設定されています。</p> <p>キーワードの意味は次のとおりです。</p> <ul style="list-style-type: none"> <i>level</i> には、ブロードキャスト、マルチキャスト、またはユニキャスト トラフィックの上限しきい値レベルを帯域幅のパーセンテージで指定します (小数点第 2 位まで)。上限しきい値に到達すると、ポートはトラフィックをブロックします。指定できる範囲は 0.00 ~ 100.00 です。 (任意) <i>level-low</i> には、下限しきい値レベルを帯域幅のパーセンテージで指定します (小数点第 2 位まで)。この値は上限抑制レベル以下の値である必要があります。トラフィックがこのレベルを下回っていれば、ポートはトラフィックを転送します。下限抑制レベルを設定していない場合、上限抑制レベルと同じ値が設定されます。指定できる範囲は 0.00 ~ 100.00 です。 しきい値に最大値 (100%) を指定した場合、トラフィックの制限はなくなります。しきい値に 0.0 を設定すると、そのポート上のすべてのブロードキャスト、マルチキャスト、またはユニキャスト トラフィックがブロックされます。 <i>bps bps</i> には、ブロードキャスト、マルチキャスト、またはユニキャスト トラフィックの上限しきい値レベルをビット / 秒で指定します (小数点第 1 位まで)。上限しきい値に到達すると、ポートはトラフィックをブロックします。指定できる範囲は 0.0 ~ 10000000000.0 です。 (任意) <i>bps-low</i> には、下限しきい値レベルをビット / 秒で指定します (小数点第 1 位まで)。この値は上限しきい値 レベル以下の値である必要があります。トラフィックがこのレベルを下回っていれば、ポートはトラフィックを転送します。指定できる範囲は 0.0 ~ 10000000000.0 です。 <i>pps pps</i> には、ブロードキャスト、マルチキャスト、またはユニキャスト トラフィックの上限しきい値レベルをパケット / 秒で指定します (小数点第 1 位まで)。上限しきい値に到達すると、ポートはトラフィックをブロックします。指定できる範囲は 0.0 ~ 10000000000.0 です。 (任意) <i>pps-low</i> には、下限しきい値レベルをパケット / 秒で指定します (小数点第 1 位まで)。この値は上限しきい値 レベル以下の値である必要があります。トラフィックがこのレベルを下回っていれば、ポートはトラフィックを転送します。指定できる範囲は 0.0 ~ 10000000000.0 です。 <p>BPS および PPS の設定には、しきい値の数値を大きく設定できるように、サフィックスに測定記号 (k、m、g など) を使用できます。</p>
ステップ 4	<pre>storm-control action {shutdown trap}</pre>	<p>ストームが検出された場合に実行するアクションを指定します。デフォルトではトラフィックにフィルタリングを実行し、トラップは送信しない設定です。</p> <ul style="list-style-type: none"> ストーム中、ポートを <code>error-disable</code> の状態にするには、<code>shutdown</code> キーワードを選択します。 ストームが検出された場合、SNMP (簡易ネットワーク管理プロトコル) トラップを生成するには、<code>trap</code> キーワードを選択します。
ステップ 5	<pre>end</pre>	<p>特権 EXEC モードに戻ります。</p>

■ ストーム制御の設定

	コマンド	目的
ステップ 6	<code>show storm-control [interface-id] [broadcast multicast unicast]</code>	指定したトラフィック タイプについて、インターフェイスで設定したストーム制御抑制レベルを確認します。トラフィック タイプを入力しなかった場合は、ブロードキャスト ストーム制御の設定が表示されます。
ステップ 7	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

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、ポート上で、上限抑制レベルを 87 %、下限抑制レベルを 65 % に設定し、ユニキャスト ストーム制御をイネーブルにする方法を示します。

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

次に、ポート上で、ブロードキャスト アドレスのストーム制御を 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にポートで使用できる総帯域幅のうち、設定された 20 パーセントのレベルを超えた場合、トラフィック ストーム制御インターバルが終わるまで、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

アプリケーションによっては、あるネイバが生成したトラフィックが別のネイバにわからないように、同一スイッチ上のポート間でレイヤ 2 トラフィックが転送されないように設定する必要があります。このような環境では、保護ポートを使用すると、スイッチ上のポート間でユニキャスト、ブロードキャスト、またはマルチキャスト トラフィックの交換が確実になくなります。

保護ポートには、次の機能があります。

- 保護ポートは、同様に保護ポートである他のポートに、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）をすべて転送するわけではありません。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。CPU で処理されてソフトウェアで転送される、Protocol Independent Multicast (PIM) パケットのような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トラフィックはすべて、レイヤ 3 デバイスを介して転送しなければなりません。
- 保護ポートと非保護ポート間の転送動作は、通常どおりに進みます。

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 \(p.24-7\)](#)
- [保護ポート設定時の注意事項 \(p.24-7\)](#)
- [保護ポートの設定 \(p.24-7\)](#)

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ません。

保護ポート設定時の注意事項

保護ポートは、物理インターフェイス（GigabitEthernet ポート 1 など）または EtherChannel グループ（port-channel 5 など）に設定できます。ポート チャンネルで保護ポートをイネーブルにした場合は、そのポート チャンネル グループ内のすべてのポートでイネーブルになります。

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 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	目的
ステップ 1	<code>configure terminal</code>	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	<code>interface interface-id</code>	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	<code>switchport protected</code>	インターフェイスを保護ポートに設定します。
ステップ 4	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 5	<code>show interfaces interface-id switchport</code>	設定を確認します。
ステップ 6	<code>copy running-config startup-config</code>	（任意）コンフィギュレーション ファイルに設定を保存します。

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
```

ポートブロッキングの設定

デフォルトでは、スイッチは未知の宛先 MAC（メディア アクセス制御）アドレスが指定されたパケットをすべてのポートからフラッディングします。未知のユニキャストおよびマルチキャストトラフィックが保護ポートに転送されると、セキュリティ上、問題になる可能性があります。未知のユニキャストおよびマルチキャストトラフィックがあるポートから別のポートに転送されないようにするために、（保護または非保護）ポートをブロックし、未知のユニキャストまたはマルチキャストパケットが他のポートにフラッディングされないようにします。

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 \(p.24-9\)](#)
- [インターフェイスでのフラッディングトラフィックのブロッキング \(p.24-9\)](#)

ポートブロッキングのデフォルト設定

デフォルトでは、ポートから未知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がブロックされず、すべてのポートにこのようなパケットが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キング



(注)

インターフェイスは物理インターフェイスまたは EtherChannel グループのいずれも可能です。ポートチャン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、ポートチャンネルグループのすべてのポートでブロックされます。

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インターフェイスで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	<code>configure terminal</code>	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	<code>interface interface-id</code>	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	<code>switchport block multicast</code>	ポートからの未知のマルチキャストの転送をブロックします。
ステップ 4	<code>switchport block unicast</code>	ポートからの未知のユニキャストの転送をブロックします。
ステップ 5	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 6	<code>show interfaces interface-id switchport</code>	設定を確認します。
ステップ 7	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

ポート上でトラフィックがブロックされずに、通常の転送が行われるデフォルトの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、ポート上の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 gigabitethernet0/1
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を許可するステーションの MAC アドレスを制限および識別して、インターフェイスへの入力を制限できます。セキュアポートにセキュア MAC アドレスを割り当てると、ポートは定義されたアドレスグループ以外の送信元アドレスを持つパケットを転送しません。セキュア MAC アドレス数を 1 つに制限し、単一のセキュア MAC アドレスを割り当てると、そのポートに接続されたワークステーションに、ポートの帯域幅全体が保証されます。

セキュアポートとしてポートを設定し、セキュア MAC アドレスが最大数に達した場合、ポートにアクセスを試みるステーションの MAC アドレスが識別されたセキュア MAC アドレスのいずれとも一致しないので、セキュリティ違反が発生します。また、あるセキュアポート上でセキュア MAC アドレスが設定または学習されているステーションが、別のセキュアポートにアクセスしようとしたときにも、違反のフラグが立てられます。

ここでは、次の概念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 \(p.24-10\)](#)
- [ポートセキュリティのデフォルト設定 \(p.24-12\)](#)
- [ポートセキュリティの設定時の注意事項 \(p.24-12\)](#)
- [ポートセキュリティのイネーブル化および設定 \(p.24-14\)](#)
- [ポートセキュリティ エージングのイネーブル化および設定 \(p.24-18\)](#)

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 \(p.24-10\)](#)
- [セキュリティ違反 \(p.24-11\)](#)

セキュア MAC アドレス

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)

最大値をインターフェイス上ですでに設定されているセキュアアドレスの数より小さい値に設定しようとすると、コマンドが拒否されます。

スイッチは、次のセキュア MAC アドレス タイプをサポートします。

- **スタティック セキュア MAC アドレス** `switchport port-security mac-address mac-address` インターフェイス コンフィギュレーション コマンドを使用して手動で設定され、アドレステーブルに保存されたのち、スイッチの実行コンフィギュレーションに追加されます。
- **ダイナミック セキュア MAC アドレス** 動的に設定されてアドレステーブルにのみ保存され、スイッチの再起動時に削除されます。
- **スティッキー セキュア MAC アドレス** 動的に学習することも、手動で設定することもできます。アドレステーブルに保存され、実行コンフィギュレーションに追加されます。このアドレスがコンフィギュレーション ファイルに保存されていると、スイッチの再起動時にインターフェイスはこれらを動的に再設定する必要がありません。

スティッキー ラーニングをイネーブルにすると、ダイナミック MAC アドレスをスティッキー セキュア MAC アドレスに変換して実行コンフィギュレーションに追加するようにインターフェイスを設定できます。スティッキー 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スティッキー ラーニングがイネーブルになる前に学習したものを含め、すべてのダイナミック セキュア MAC アドレスをスティッキー セキュア MAC アドレスに変換します。すべてのスティッキー セキュア MAC アドレスは実行コンフィギュレーションに追加されます。

スティッキー セキュア MAC アドレスは、コンフィギュレーション ファイル(スイッチが再起動されるたびに使用されるスタートアップ コンフィギュレーション)に、自動的に反映されません。スティッキー セキュア MAC アドレスをコンフィギュレーション ファイルに保存すると、スイッチの再起動時にインターフェイスはこれらを再び学習する必要がありません。スティッキー セキュア アドレスが保存されていない場合、アドレスは失われます。

スティッキー ラーニングをディセーブルにした場合、スティッキー セキュア MAC アドレスはダイナミック セキュア MAC 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)の総数です。

セキュリティ違反

次のいずれかの状況が発生すると、セキュリティ違反になります。

- 最大数のセキュア MAC アドレスがアドレス テーブルに追加されている状態で、アドレス テーブルに未登録の MAC アドレスを持つステーションがインターフェイスにアクセスしようとした場合。
- あるセキュア インターフェイスで学習または設定されたアドレスが、同一 VLAN 内の別のセキュア インターフェイスで使用された場合。

違反が発生した場合の対処に基づいて、次の 3 種類の違反モードのいずれかにインターフェイスを設定できます。

- `protect` (保護) セキュア MAC アドレスの数がポートで許可されている最大限度に達すると、最大値を下回るまで十分な数のセキュア MAC アドレスを削除するか、許可アドレス数を増やさないうえ、未知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たことは通知されません。



(注) トランク ポートに `protect` 違反モードを設定することは推奨しません。 `protect` モードの場合、ポートが最大限度に達していなくてもいずれかの VLAN が最大限度に達すると、ラーニングをディセーブルにします。

- `restrict` (制限) セキュア MAC アドレスの数がポートで許可されている最大限度に達すると、最大値を下回るまで十分な数のセキュア MAC アドレスを削除するか、許可アドレス数を増やさないうえ、未知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ことが通知されます。SNMP トラップが送信されて Syslog メッセージがログされ、違反カウンタが増加します。

■ ポートセキュリティの設定

- shutdown (シャットダウン) ポートセキュリティ違反により、インターフェイスが errdisable になり、ただちにシャットダウンされます。そのあと、ポートの LED が消灯します。SNMP トラップが送信されて Syslog メッセージがログされ、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するか、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 コマンドを入力して手動で再びイネーブルにできます。これがデフォルトのモードです。

表 24-1 に、ポートセキュリティをインターフェイスに設定した場合の違反モードおよび取られる処置について示します。

表 24-1 セキュリティ違反モードの処置

違反モード	トラフィックの転送 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. 十分な数のセキュア MAC アドレスを削除するまで未知の送信元アドレスを持つパケットが廃棄されます。
2. セキュリティ違反を引き起こすアドレスを手動で設定した場合、スイッチがエラー メッセージを返します。

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	ポート上でディセーブル
スティッキー アドレス ラーニング	ディセーブル
ポートあたりのセキュア MAC アドレスの最大数	1
違反モード	shutdown (シャットダウン)。セキュア MAC アドレスが最大数を上回ると、ポートがシャットダウンします。
ポートセキュリティ エージング	ディセーブル。エージング タイムは 0 スタティック エージングはディセーブル タイプは absolute

ポートセキュリティの設定時の注意事項

ポートセキュリティを設定するときには、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。セキュアポートをダイナミック アクセスポートにすることはできません。
- セキュアポートを Switched Port Analyzer (SPAN; スイッチドポートアナライザ) 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。



(注) 音声 VLAN はアクセスポートでのみサポートされており、設定可能であってもトランクポートではサポートされていません。

- 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 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際には、ポート上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。ポートを Cisco IP Phone に接続している場合、IP Phone には最大で 2 つの MAC アドレスが必要になります。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 つの PC を Cisco IP Phone に接続する場合、追加の MAC アドレスは不要です。複数の PC を Cisco IP Phone に接続する場合、各 PC と IP Phone に 1 つずつ使用できるように、十分な数のセキュアアドレスを設定する必要があります。
- インターフェイスの最大セキュアアドレス値を入力したときに、新しい値がそれまでの値より大きいと、それまで設定されていた値が新しい値によって上書きされます。新しい値が以前の値より小さく、インターフェイス上ですでに設定されているセキュアアドレスの数が新しい値を上回る場合は、コマンドが拒否されます。
- スイッチは、スティッキーセキュア MAC アドレスのポートセキュリティエージングをサポートしていません。

表 24-3 に、他のポートベース機能と互換性のあるポートセキュリティについてまとめます。

表 24-3 他のスイッチ機能とポートセキュリティとの互換性

ポートタイプまたはポートの機能	ポートセキュリティとの互換性
DTP 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
Switched Port Analyzer (SPAN; スイッチドポートアナライザ) 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
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; アドレス解決プロトコル) 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) ポート。



4. ポートに最大限可能なセキュアなアドレスを設定します (アクセス VLAN で可能なセキュアなアドレスの最大数に 2 を加えた数)。



ポートセキュリティのイネーブル化および設定

ポートへのアクセスを許可するステーションの MAC アドレスを制限および識別することによって、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	<code>configure terminal</code>	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	<code>interface interface-id</code>	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	<code>switchport mode {access trunk}</code>	インターフェイススイッチポートモードを <code>access</code> または <code>trunk</code> 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	<code>switchport voice vlan vlan-id</code>	ポート上で音声 VLAN をイネーブルにします。 <i>vlan-id</i> 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	<code>switchport port-security</code>	インターフェイス上でポートセキュリティをイネーブルにします。
ステップ 6	<code>switchport port-security [maximum value [vlan {vlan-list {access / voice}}]]</code>	<p>(任意) インターフェイスに対するセキュア 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「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 (その他のレイヤ 2 機能やインターフェイスに設定されたその他のセキュア MAC アドレスで使用される MAC アドレスを含む) の総数を表します。</p> <p>(任意) <code>vlan</code> VLAN 単位の最大値を設定します。</p> <p><code>vlan</code> キーワードを入力したあと、次のオプションのいずれか 1 つを入力してください。</p> <ul style="list-style-type: none"> <code>vlan-list</code> トランクポート上で、ハイフンで区切った範囲の VLAN、またはカンマで区切った一連の VLAN における、VLAN 単位の最大値を設定できます。指定されなかった VLAN には、VLAN 単位の最大値が使用されます。 <code>access</code> アクセスポート上で、アクセス VLAN として VLAN を指定します。 <code>voice</code> アクセスポート上で、音声 VLAN として VLAN を指定します。 <p> (注) <code>voice</code> キーワードは、音声 VLAN がポートに設定されていて、さらにそのポートがアクセス VLAN でない場合のみ有効です。インターフェイスに音声 VLAN が設定されている場合、セキュア MAC アドレスの最大数を 2 に設定します。</p>

コマンド	目的
ステップ 7 <code>switchport port-security violation {protect restrict shutdown}</code>	<p>(任意) 違反モード、すなわちセキュリティ違反が検出されたときの対応を、次のいずれかに設定します。</p> <ul style="list-style-type: none"> protect (保護) ポートセキュア MAC アドレスの数がポートで許可されている最大限度に達すると、最大値を下回るまで十分な数のセキュア MAC アドレスを削除するか、または許可アドレス数を増やさないかぎり、未知の送信元アドレスを持つパケットは廃棄されます。セキュリティ違反が発生したことは通知されません。 <p> (注) トランク ポートに <code>protect</code> モードを設定することは推奨しません。protect モードの場合、ポートが最大限度に達していなくてもいずれかの VLAN が最大限度に達すると、ラーニングをディセーブルにします。</p> <ul style="list-style-type: none"> restrict セキュア MAC アドレスの数がポートで許可されている最大限度に達すると、十分な数のセキュア MAC アドレスを削除するか、または許可アドレス数を増やさないかぎり、未知の送信元アドレスを持つパケットは廃棄されます。SNMP トラップが送信されて Syslog メッセージがログされ、違反カウンタが増加します。 shutdown 違反が発生すると、インターフェイスが <code>errdisable</code> になり、ポートの LED が消灯します。SNMP トラップが送信されて Syslog メッセージがログされ、違反カウンタが増加します。 <p> (注) セキュア ポートが <code>errdisable</code> ステートの場合は、<code>errdisable recovery cause psecure-violation</code> グローバル コンフィギュレーション コマンドを入力してこのステートを解除するか、<code>shutdown</code> および <code>no shutdown</code> インターフェイス コンフィギュレーション コマンドを入力して手動で再びイネーブルにできます。</p>

コマンド	目的
ステップ 8 <code>switchport port-security [mac-address mac-address [vlan {vlan-id / {access / voice}}]]</code>	<p>(任意) インターフェイスのセキュア MAC アドレスを入力します。このコマンドを使用すると、最大数のセキュア MAC アドレスを入力できます。設定したセキュア MAC アドレスが最大数より少ない場合、残りの MAC アドレスは動的に学習されます。</p> <p> (注) このコマンドの入力後にスティッキー ラーニングをイネーブルにすると、動的に学習されたセキュア アドレスがスティッキー セキュア MAC アドレスに変換されて実行コンフィギュレーションに追加されます。</p> <p>(任意) <code>vlan</code> VLAN 単位の最大値を設定します。</p> <p><code>vlan</code> キーワードを入力したあと、次のオプションのいずれか 1 つを入力してください。</p> <ul style="list-style-type: none"> • <code>vlan-id</code> トランク ポートで、VLAN ID および MAC アドレスを指定できます。VLAN ID を指定しない場合、ネイティブ VLAN が使用されます。 • <code>access</code> アクセス ポート上で、アクセス VLAN として VLAN を指定します。 • <code>voice</code> アクセス ポート上で、音声 VLAN として VLAN を指定します。 <p> (注) <code>voice</code> キーワードは、音声 VLAN がポートに設定されていて、さらにそのポートがアクセス VLAN でない場合のみ有効です。インターフェイスに音声 VLAN が設定されている場合、セキュア MAC アドレスの最大数を 2 に設定します。</p>
ステップ 9 <code>switchport port-security mac-address sticky</code>	<p>(任意) インターフェイスでスティッキー ラーニングをイネーブルにします。</p>

ステップ	コマンド	目的
ステップ 10	<pre>switchport port-security mac-address sticky [mac-address vlan {vlan-id / {access / voice}}]</pre>	<p>(任意) スティックキー セキュア MAC アドレスを入力し、必要な回数だけコマンドを繰り返します。設定したセキュア MAC アドレスの数が最大数より少ない場合、残りの MAC アドレスは動的に学習されてスティッキー セキュア MAC アドレスに変換され、実行コンフィギュレーションに追加されます。</p> <p> (注) このコマンドの入力前にスティッキー ラーニングをイネーブルにしないと、エラー メッセージが表示されてスティッキー セキュア MAC アドレスを入力できません。</p> <p>(任意) <code>vlan</code> VLAN 単位の最大値を設定します。</p> <p><code>vlan</code> キーワードを入力したあと、次のオプションのいずれか 1 つを入力してください。</p> <ul style="list-style-type: none"> <code>vlan-id</code> トランク ポートで、VLAN ID および MAC アドレスを指定できます。VLAN ID を指定しない場合、ネイティブ VLAN が使用されます。 <code>access</code> アクセス ポート上で、アクセス VLAN として VLAN を指定します。 <code>voice</code> アクセス ポート上で、音声 VLAN として VLAN を指定します。 <p> (注) <code>voice</code> キーワードは、音声 VLAN がポートに設定されていて、さらにそのポートがアクセス VLAN でない場合のみ有効です。</p>
ステップ 11	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 12	<code>show port-security</code>	設定を確認します。
ステップ 13	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

セキュア ポートではないデフォルトの状態にインターフェイスを戻す場合は、`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。スティッキー ラーニングがイネーブルの状態でのこのコマンドを入力すると、スティッキー セキュア アドレスが実行コンフィギュレーションの一部に残りますが、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場合は、`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 (shutdown モード) に戻す場合は、`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ー 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。インターフェイスがスティッキー 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、スティッキー MAC アドレスによる設定を保存した場合、`no switchport port-security mac-address sticky` コマンドの入力後に設定をもう一度保存しないと、スイッチの再起動時にスティッキー アドレスが復元されます。

MAC アドレス テーブルからスイッチまたはインターフェイス上のセキュア アドレスすべてまたは特定 (設定、ダイナミック、スティッキー) のセキュア アドレスすべてを削除するには、`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。インターフェイス上のすべてのダイナミック セキュア アドレスをアドレステーブルから削除するには、`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` コマンドを使用する前に、`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ー セキュア MAC アドレスをダイナミック セキュア MAC アドレスに変換した場合、手動で設定されたものを除き、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。

設定済みのセキュア MAC アドレスをアドレステーブルから明確に削除する場合、`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 コマンドを使用しなければなりません。

次に、ポート上でポートセキュリティをイネーブルにし、セキュアアドレスの最大数を 50 に設定する例を示します。違反モードはデフォルトです。スタティック セキュア MAC アドレスは設定せず、スティッキー ラーニングはイネーブルです。

```
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 上にスタティック セキュア MAC アドレスを設定する例を示します。

```
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、ポートのスティッキー ポートセキュリティをイネーブルにする例を示します。データ VLAN および音声 VLAN の MAC アドレスを手動で設定し、セキュアアドレスの総数を 20 に設定します (データ VLAN に 10、音声 VLAN に 10 割り当てます)。

```
Switch(config)# interface FastEthernet0/1
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および設定

ポート上のすべてのセキュアアドレスにエージング タイムを設定するには、ポートセキュリティ エージングを使用します。ポートごとに 2 つのタイプのエージングがサポートされています。

- **absolute** 指定されたエージング タイムの経過後に、ポート上のセキュアアドレスが削除されます。
- **inactivity** 指定されたエージング タイムの間、セキュアアドレスが非アクティブであった場合に限り、ポート上のセキュアアドレスが削除されます。

この機能を使用すると、既存のセキュア MAC アドレスを手動で削除しなくても、セキュアポート上のデバイスを削除および追加し、なおかつポート上のセキュア アドレス数を制限できます。セキュアアドレスのエイジングは、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	<code>configure terminal</code>	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	<code>interface interface-id</code>	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	<code>switchport port-security aging {static time time type {absolute inactivity}}</code>	<p>セキュアポートのスタティック エージングをイネーブルまたはディセーブルにします。またはエイジング タイムやタイプを設定します。</p> <p> (注) スイッチは、スティッキー セキュア アドレスのポートセキュリティ エージングをサポートしていません。</p> <p>このポートに、スタティックに設定されたセキュアアドレスのエイジングをイネーブルにする場合は、<code>static</code> を入力します。</p> <p><code>time</code> には、このポートのエイジング タイムを指定します。指定できる範囲は、0 ~ 1440 分です。</p> <p><code>type</code> には、次のキーワードのいずれか 1 つを選択します。</p> <ul style="list-style-type: none"> absolute エージング タイプを絶対エイジングとして設定します。このポートのセキュアアドレスはすべて、指定した時間(分単位)が経過すると期限切れになり、セキュアアドレス リストから削除されます。 inactivity エージング タイプを非アクティブ エージングとして設定します。指定された <code>time</code> 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に限り、このポートのセキュアアドレスが期限切れになります。
ステップ 4	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 5	<code>show port-security [interface interface-id] [address]</code>	設定を確認します。
ステップ 6	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

ポート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。静的に設定されたセキュアアドレスに対してだけエイ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、ポート上のセキュアアドレスのエイジング 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
```

■ ポート単位のトラフィック制御設定の表示

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に対して、エージングをイネーブルにし、非アクティブエージングタイプの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
```

上記のコマンドを確認するには、`show port-security interface interface-id` 特権 EXEC コマンドを使用します。

ポート単位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、(他の特性の中から) インターフェイストラフィックの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、ストーム制御およびポートセキュリティの設定が表示されます。

トラフィックの制御情報を表示するには、表 24-4 の特権 EXEC コマンドを1つまたは複数使用します。

表 24-4 トラフィック制御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
<code>show interfaces [interface-id] switchport</code>	すべてのスイッチング(非ルーティング)ポートまたは指定されたポートの管理ステータスまたは動作ステータスを、ポートブロッキングおよびポート保護の設定を含めて表示します。
<code>show storm-control [interface-id] [broadcast multicast unicast]</code>	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。
<code>show port-security [interface interface-id]</code>	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容されるセキュア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。
<code>show port-security [interface interface-id] address</code>	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。
<code>show port-security interface interface-id vlan</code>	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。