



# ポート セキュリティ

- [ポートセキュリティの概要 \(1 ページ\)](#)
- [ポートセキュリティ違反 \(2 ページ\)](#)
- [UCS 6454 でファブリック インターコネクタのポートセキュリティに関するガイドライン \(3 ページ\)](#)
- [ポートセキュリティの設定 \(3 ページ\)](#)

## ポート セキュリティの概要

ポートセキュリティ機能を使用して、このポートへのアクセスを許可されたワークステーションの MAC アドレスを制限し、明らかにすることにより、インターフェイスへの入力を制限することができます。これは、各インターフェイスの MAC アドレスの格納を学習し、制御するのに役立ちます。ハブやスイッチなどのプラグインされている CAM オーバーフロー攻撃や不正な機器から保護するために使用されます。ポートセキュリティ対応ポートはセキュアポートと呼ばれ、そのポートで許可される MAC アドレスはセキュア MAC アドレスと呼ばれます。セキュアポートにセキュア MAC アドレスを割り当てると、ポートは定義済みのアドレスのグループ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 アドレスをセキュアな MAC アドレスに割り当てると、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。

ポートに最大セキュアな MAC アドレス数を設定すると、セキュアな MAC アドレスを次のいずれかの方法でアドレス テーブルに含めることができます。

- すべてのセキュア MAC アドレスを、`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設定します。
- 接続されているデバイスの MAC アドレスで、ポートがセキュア MAC アドレスをダイナミックに設定できるようにします。
- 多数のアドレスを設定し、残りのアドレスはダイナミックに設定されるように指定します。



(注) ポートがシャットダウンされると、ダイナミックに学習されたアドレスはすべて削除されます。

- MACアドレスをステッキーに設定します。MACアドレスは動的に学習されるか、または手動で設定され、アドレステーブル内に格納され、実行コンフィギュレーションに追加されます。これらのアドレスをコンフィギュレーションファイルに保存した場合は、スイッチを再起動しても、インターフェイスはダイナミックに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を手動で設定することもできますが、推奨しません。

### MAC ラーニング

インターフェイスでポートセキュリティが有効になり、新しいMACアドレスがインターフェイスに表示された後で、新しいMACアドレスのセキュリティの検証が行われます。この検証に基づいて、MACアドレスはアドレステーブルに追加されます-通常のエン트리またはドロップエン트리としてのいずれか。

## ポートセキュリティ違反

次のいずれかの場合に、ポートセキュリティ違反が発生します。

- ポートセキュリティは、セキュアMACアドレスがセキュアポートで最大数に達した場合に、識別されたどのセキュアMACアドレスとも入力トラフィックの送信元MACアドレスが異なると、設定された違反モードを適用します。
- 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アドレスを持つトラフィックが、同一VLAN内の別のセキュアポートにアクセスしようとする時、ポートセキュリティが設定された違反モードを適用します。これは、MAC移動違反とも呼ばれる。

ポートセキュリティの3つの違反アクションがあります。これらのいずれかの違反アクションに対してポートを設定できます。

- **Shutdown**—ポートセキュリティ違反が発生すると、ポートがただちにシャットダウンします。
- **Restrict**—ポートのセキュリティ違反が発生すると、データが制限され、SecurityViolationカウンタの値が増加し、SNMPトラップが生成されます。制限アクションでは、10回の違反の後に、学習がポートで無効になります。制限は、ポートセキュリティ違反のデフォルトの動作です。
- **Protect**—ポートセキュリティ違反では、未知のMACアドレスからのデータをドロップさせます。SecurityViolationカウンタは増分されず、SNMPトラップを生成できません。

# UCS 6454 でファブリック インターコネクットのポート セキュリティに関するガイドライン

次のガイドラインは、UCS 6454 ファブリック インターコネクットのポートにポートセキュリティを設定するときに適用されます。

- ポートセキュリティは、NIV ポートでのみ設定できます。BIF ポートではサポートされません。
- VLAN ごとに 1 つの MAC アドレスのみが、NIV ポートに対してセキュリティで保護することができます。
- 仮想インターフェイスでポートセキュリティ違反の制限は、デフォルトの違反アクションです。
- 10 回の違反の後に、MAC ラーニングはセキュア ポートで無効になっています。
- セキュアな MAC アドレスは、エージアウトすることはありません。
- 設定できる最大数のセキュア MAC アドレスは次の通りです。
  - デバイス上 — ポートごとの 1 つの MAC アドレスに加えて、最大 8000 のセキュアな MAC アドレス
  - インターフェイス — インターフェイスごとの最大 1000 の MAC アドレス
  - VLAN — VLAN のポートあたり 1 つのセキュア MAC アドレスのみ

## ポート セキュリティの設定

ポートにアクセスできるステーションの MAC アドレスを制限および識別することにより、このポートを通過するトラフィックを制限するには、次の作業を行います。

### 手順

	コマンドまたはアクション	目的
ステップ 1	<code>switch(config)# interface interface_id</code>	インターフェイス設定モードを開始します。
ステップ 2	<code>switch(config-if)# switchport mode access</code>	インターフェイス モードを <code>access</code> に設定します。デフォルトモード ( <code>dynamic desirable</code> ) のインターフェイスをセキュア ポートに設定できません。

	コマンドまたはアクション	目的
ステップ 3	switch(config-if)# <b>[no] switchport port-security</b>	<p>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。</p> <p>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には、no switchport port-security インターフェイス設定コマンドを使用します。</p>
ステップ 4	switch(config-if)# <b>switchport port-security maximum value</b>	<p>インターフェイスのセキュア MAC アドレスの最大数を設定します。指定できる範囲は 1 ~ 1000 です。</p> <p>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 インターフェイス設定コマンドを使用します。</p>
ステップ 5	switch(config-if)# <b>switchport port-security violation {restrict   shutdown   protect}</b>	<p>セキュリティ違反が検出された場合に実行するアクションを設定します。次のいずれかの処理を選択できます。</p> <ul style="list-style-type: none"> <li>• <b>Shutdown</b>—ポートセキュリティ違反が発生すると、ポートがただちにシャットダウンします。</li> <li>• <b>Restrict</b>—ポートのセキュリティ違反が発生すると、データが制限され、SecurityViolation カウンタの値が増加し、SNMP トラップが生成されます。制限アクションでは、10 回の違反の後に、学習がポートで無効になります。制限は、ポートセキュリティ違反のデフォルトの動作です。</li> <li>• <b>Protect</b>—ポートセキュリティ違反では、未知の MAC アドレスからのデータをドロップさせます。SecurityViolation カウンタは増分されず、SNMP トラップを生成できません。</li> </ul> <p>違反モードをデフォルト状態 (shutdown モード) に戻すには、no switchport port-security violation {restrict  shutdown  </p>

	コマンドまたはアクション	目的
		protect} インターフェイス設定コマンドを使用します。
ステップ 6	switch(config-if)# <b>switchport port-security mac-address</b> <i>mac_address</i>	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。  アドレステーブルから特定の MAC アドレスを削除するには、no switchport port-security mac-address <i>mac_address</i> インターフェイス設定コマンドを使用します。



## 翻訳について

このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。