



## ポート セキュリティの設定

この章では、Cisco NX-OS デバイスにポート セキュリティを設定する手順について説明します。

この章は、次の項で構成されています。

- [ポート セキュリティの概要, on page 1](#)
- [ポート セキュリティの前提条件, on page 9](#)
- [ポート セキュリティのデフォルト設定, on page 9](#)
- [ポート セキュリティの注意事項と制約事項, on page 9](#)
- [vPC 上のポート セキュリティの注意事項と制約事項 \(10 ページ\)](#)
- [ポート セキュリティの設定, on page 11](#)
- [ポート セキュリティの設定の確認, on page 22](#)
- [セキュア MAC アドレスの表示, on page 23](#)
- [ポート セキュリティの設定例, on page 23](#)
- [vPC ドメインでのポート セキュリティの設定例 \(23 ページ\)](#)
- [ポート セキュリティに関する追加情報, on page 24](#)
- [VXLAN EVPN のポート セキュリティ サポート \(25 ページ\)](#)

## ポート セキュリティの概要

ポート セキュリティを使用すると、限定された MAC アドレス セットからの入力トラフィックだけを許可するようなレイヤ 2 物理インターフェイスおよびレイヤ 2 ポート チャネル インターフェイスを設定できます。この制限されたセット内の MAC アドレスは、セキュア MAC アドレスと呼ばれます。さらに、デバイスは、これらの MAC アドレスからのトラフィックでも、同じ VLAN 内の別のインターフェイスからの場合は許可しません。セキュア MAC アドレスの数は、インターフェイス単位で設定します。



### Note

特に指定がなければ、インターフェイスは物理インターフェイスとポートチャネル インターフェイスの両方を意味します。同様に、レイヤ 2 インターフェイスはレイヤ 2 物理インターフェイスとレイヤ 2 ポート チャネル インターフェイスの両方を意味します。

## セキュア MAC アドレスの学習

MAC アドレスは学習というプロセスによってセキュア アドレスになります。MAC アドレスは、1 つのインターフェイスだけでセキュア MAC アドレスになることができます。デバイスは、ポートセキュリティが有効に設定されたインターフェイスごとに、スタティックまたはダイナミック方式で、限られた数の MAC アドレスを学習できます。デバイスがセキュア MAC アドレスを格納する方法は、デバイスがセキュア MAC アドレスを学習した方法によって異なります。

### スタティック方式

スタティック学習方式では、ユーザが手動でインターフェイスの実行コンフィギュレーションにセキュア MAC アドレスを追加したり、設定から削除したりできます。実行コンフィギュレーションをスタートアップコンフィギュレーションにコピーすると、デバイスを再起動してもスタティック セキュア MAC アドレスには影響がありません。

スタティック セキュア MAC アドレスのエントリは、次のいずれかのイベントが発生するまで、インターフェイスの設定内に維持されます。

- ユーザが明示的に設定からアドレスを削除した場合。
- ユーザがそのインターフェイスをレイヤ 3 インターフェイスとして設定した場合。

スタティック方式では、ダイナミック方式のアドレス学習がイネーブルになっているかどうかに関係なく、セキュア アドレスを追加できます。

### ダイナミック方式

デフォルトでは、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すると、ダイナミック学習方式がイネーブルになります。この方式では、デバイスは、入力トラフィックがインターフェイスを通過するときに MAC アドレスをセキュア アドレスにします。アドレスがまだ保護されていず、デバイスが該当する最大値に達していない場合、デバイスはそのアドレスを保護し、トラフィックを許可します。

デバイスは、ダイナミック セキュア MAC アドレスをメモリに保存します。ダイナミック セキュア MAC アドレスのエントリは、次のいずれかのイベントが発生するまで、インターフェイスの設定内に維持されます。

- デバイスが再起動した場合
- インターフェイスが再起動した場合
- アドレスが、ユーザによって設定されたインターフェイスのエージング期限に達した場合
- ユーザがアドレスを明示的に削除した場合
- ユーザがそのインターフェイスをレイヤ 3 インターフェイスとして設定した場合

## スティッキ方式

スティッキ方式をイネーブルにすると、デバイスは、ダイナミックアドレス学習と同じ方法で MAC アドレスをセキュアアドレスにしますが、この方法で学習されたアドレスは NVRAM に保存されます。そのため、スティッキ方式で学習されたアドレスは、デバイスの再起動後も維持されます。スティッキセキュア MAC アドレスは、インターフェイスの実行コンフィギュレーション内にはありません。

ダイナミックとスティッキのアドレス学習は両方同時にイネーブルにできません。あるインターフェイスのスティッキ学習をイネーブルにした場合、デバイスはダイナミック学習を停止して、代わりにスティッキ学習を実行します。スティッキ学習をディセーブルにすると、デバイスはダイナミック学習を再開します。

スティッキセキュア MAC アドレスのエントリは、次のいずれかのイベントが発生するまで、インターフェイスの設定内に維持されます。

- ユーザがアドレスを明示的に削除した場合
- ユーザがそのインターフェイスをレイヤ 3 インターフェイスとして設定した場合

## ダイナミック アドレスのエージング

デバイスは、ダイナミック方式で学習された MAC アドレスのエージングを行い、エージングの期限に達すると、アドレスをドロップします。エージングの期限は、インターフェイスごとに設定できます。有効な範囲は 0 ～ 1440 分です。0 を設定すると、エージングはディセーブルになります。

MAC アドレスのエージングを判断するためにデバイスが使用する方法も設定できます。アドレス エージングの判断には、次に示す 2 つの方法が使用されます。

### Inactivity

適用可能なインターフェイス上のアドレスからデバイスが最後にパケットを受信して以降の経過時間。

### 絶対値 (Absolute)

デバイスがアドレスを学習して以降の経過時間。これがデフォルトのエージング方法ですが、デフォルトのエージング時間は 0 分（エージングはディセーブル）です。



#### Note

絶対エージングタイムを設定すると、送信元 MAC からのトラフィックが流れていても、MAC エージングが発生します。ただし、MAC エージングおよび再学習中に、一時的なトラフィック ドロップが発生する可能性があります。

## セキュア MAC アドレスの最大数

デフォルトでは、各インターフェイスのセキュア MAC アドレスは 1 つだけです。各インターフェイス、またはインターフェイス上の各 VLAN に許容可能な最大 MAC アドレス数を設定できます。最大数は、スタティックまたはダイナミックに学習された MAC アドレスにも適用されます。



**Tip** アドレスの最大数を 1 に設定し、接続されたデバイスの MAC アドレスを設定すると、そのデバイスにはポートの全帯域幅が保証されます。

各インターフェイスに許容されるセキュア MAC アドレスの数は、次の 3 つの制限によって決定されます。

### デバイスの最大数

デバイスが許容できるセキュア MAC アドレスの最大数は 8192 です。この値は変更できません。新しいアドレスを学習するとデバイスの最大数を超過してしまう場合、たとえインターフェイスや VLAN の最大数に達していなくても、デバイスは新しいアドレスの学習を許可しません。

### インターフェイスの最大数

ポートセキュリティで保護されるインターフェイスごとに、セキュア MAC アドレスの最大数 1025 を設定できます。デフォルトでは、インターフェイスの最大アドレス数は 1 です。インターフェイスの最大数を、デバイスの最大数より大きくすることはできません。

### VLAN の最大数

ポートセキュリティで保護される各インターフェイスについて、VLAN あたりのセキュア MAC アドレスの最大数を設定できます。VLAN の最大数は、インターフェイスに設定されている最大数より大きくできません。VLAN 最大数の設定が適しているのは、トランクポートの場合だけです。VLAN の最大数には、デフォルト値はありません。

インターフェイスあたりの、VLAN とインターフェイスの最大数は必要に応じて設定できます。ただし、新しい制限値が、適用可能なセキュアアドレス数よりも少ない場合は、まず、セキュア MAC アドレスの数を減らす必要があります。

## セキュリティ違反と処理

次の 2 つのイベントのいずれかが発生すると、ポートセキュリティ機能によってセキュリティ違反がトリガーされます。

### MAC 数違反

あるインターフェイスにセキュア MAC アドレス以外のアドレスから入力トラフィックが着信し、そのアドレスを学習するとセキュア MAC アドレスの適用可能な最大数を超過してしまう場合

あるインターフェイスに VLAN とインターフェイスの両方の最大数が設定されている場合は、どちらかの最大数を超えると、違反が発生します。たとえば、ポートセキュリティが設定されている単一のインターフェイスについて、次のように想定します。

- VLAN 1 の最大アドレス数は 5 です。
- このインターフェイスの最大アドレス数は 10 です。

デバイスは、次のいずれかが発生すると違反を検出します。

- デバイスが VLAN 1 のアドレスをすでに 5 つ学習していて、6 つめのアドレスからのインバウンドトラフィックが VLAN 1 のインターフェイスに着信した場合。
- このインターフェイス上のアドレスをすでに 10 個学習していて、11 番目のアドレスからのインバウンドトラフィックがこのインターフェイスに着信した場合。

デバイスが実行できる処理は次のとおりです。

### シャットダウン

違反をトリガーしたパケットの受信インターフェイスをシャットダウンします。このインターフェイスはエラーディセーブル状態になります。これがデフォルトの処理です。インターフェイスの再起動後も、セキュア MAC アドレスを含めて、ポートセキュリティの設定は維持されます。

シャットダウン後にデバイスが自動的にインターフェイスを再起動するように設定するには、**errdisable** グローバル コンフィギュレーション コマンドを使用します。あるいは、**shutdown** および **no shut down** のインターフェイス 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、手動でインターフェイスを再起動することもできます。

### 制限

セキュア MAC アドレス以外のアドレスからの入力トラフィックをドロップします。

デバイスはドロップされたパケット数を保持しますが、これをセキュリティ違反回数と呼びます。インターフェイスで発生するセキュリティ違反が最大数に到達するまでアドレス学習を継続します。最初のセキュリティ違反のあとに学習されたアドレスからのトラフィックはドロップされます。

### MAC 移動違反

あるインターフェイスのセキュア MAC アドレスになっているアドレスからの入力トラフィックが、そのインターフェイスと同じ VLAN 内の別のインターフェイスに着信した場合

レイヤ 2 転送モジュール (L2FM) のロギング レベルが 4 または 5 に増加した場合にのみ、MAC 移動通知が表示されます。

MAC 移動違反が発生すると、デバイスはインターフェイスのセキュリティ違反カウンタを増分し、設定された違反モードに関係なく、インターフェイスはエラーディセーブルになります。違反モードが[制限 (Restrict)]または[保護 (Protect)]に設定されている場合、違反はシステム ログに記録されます。

MAC移動違反は、設定された違反モードに関係なく、インターフェイスがエラーディセーブルになるため、**errdisable** コマンドを使用して自動 **errdisable** リカバリをイネーブルにすることを推奨します。

## ポートセキュリティとポートタイプ

ポートセキュリティを設定できるのは、レイヤ2インターフェイスだけです。各種のインターフェイスまたはポートとポートセキュリティについて次に詳しく説明します。

### アクセスポート

レイヤ2アクセスポートとして設定したインターフェイスにポートセキュリティを設定できます。アクセスポートでポートセキュリティが適用されるのは、アクセスVLANだけです。アクセスポートには、VLAN最大数を設定しても効果はありません。

### トランクポート

レイヤ2トランクポートとして設定したインターフェイスにポートセキュリティを設定できます。デバイスがVLAN最大数を適用するのは、トランクポートに関連付けられたVLANだけです。

### SPANポート

SPAN送信元ポートにはポートセキュリティを設定できますが、SPAN宛先ポートには設定できません。

### イーサネットポートチャネル

レイヤ2イーサネットポートチャネルインターフェイスのポートセキュリティはアクセスモードまたはトランクモードで設定できます。



**Note** ポートセキュリティは、Cisco Nexus 9300-FX/FX2/FX3 シリーズスイッチ上の非 vPC 展開でのみ FEX インターフェイスに対してサポートされます。Cisco NX-OS リリース 9.3(5) 以降、Cisco Nexus 9300-FX3 シリーズスイッチがサポートされます。

## ポートセキュリティとポートチャネルインターフェイス

ポートセキュリティは、レイヤ2ポートチャネルインターフェイスでサポートされます。ポートチャネルインターフェイス上で動作するポートセキュリティは、ここで説明する内容以外は、物理インターフェイスの場合と同じです。

### 一般的なガイドライン

ポートチャネルインターフェイスのポートセキュリティは、アクセスモードまたはトランクモードのいずれかで動作します。トランクモードでは、ポートセキュリティで適用されるMACアドレスの制限が、VLAN単位ですべてのメンバポートに適用されます。

ポートチャネルインターフェイスのポートセキュリティを有効にしても、ポートチャネルのロードバランシングには影響しません。

ポートセキュリティは、ポート チャンネル インターフェイスを通過するポート チャンネル制御トラフィックには適用されません。ポートセキュリティを使用すると、セキュリティ違反にならないようにして、ポート チャンネル制御パケットを通過させることができます。ポート チャンネル制御トラフィックには、次のプロトコルが含まれます。

- ポート集約プロトコル (PAgP)
- リンク集約制御プロトコル (LACP)
- Inter-Switch Link (ISL)
- IEEE 802.1Q

### セキュア メンバ ポートの設定

ポート チャンネル インターフェイスのポートセキュリティ設定は、メンバ ポートのポートセキュリティ設定には影響しません。

### メンバ ポートの追加

セキュア インターフェイスをポート チャンネル インターフェイスのメンバ ポートとして追加した場合、デバイスはメンバ ポートで学習されたダイナミック セキュア アドレスをすべて廃棄しますが、メンバ ポートのその他のポートセキュリティ設定はすべて実行コンフィギュレーションに保持します。セキュア メンバ ポートで学習されたスティック方式とスタティック方式のセキュア MAC アドレスも、NVRAM ではなく実行コンフィギュレーションに保存されます。

ポートセキュリティがメンバ ポートでは有効になっていて、ポート チャンネル インターフェイスでは有効になっていない場合、メンバ ポートをポート チャンネル インターフェイスに追加しようとするすると警告されます。セキュア メンバ ポートをセキュア ポート チャンネル インターフェイス以外のインターフェイスに強制的に追加するには、**force** キーワードを指定して **channel-group** コマンドを使用します。

ポートがポート チャンネル インターフェイスのメンバである間は、メンバ ポートのポートセキュリティを設定できません。これを行うには、まずメンバ ポートをポート チャンネル インターフェイスから削除する必要があります。

### メンバ ポートの削除

メンバ ポートをポート チャンネル インターフェイスから削除すると、メンバ ポートのポートセキュリティ設定が復元されます。ポート チャンネル インターフェイスに追加する前にそのポートで学習されたスタティック方式のセキュア MAC アドレスは、NVRAM に復元され、実行コンフィギュレーションからは削除されます。



(注) ポート チャンネル インターフェイスを削除したあとで、すべてのポートのセキュリティを必要に応じて確保するためには、すべてのメンバ ポートのポートセキュリティ設定を詳細に検査することを推奨します。

## ポート チャネル インターフェイスの削除

セキュア ポート チャネル インターフェイスを削除すると、次の処理が行われます。

- ポート チャネル インターフェイスの学習されたセキュア MAC アドレスがすべて廃棄されます。これには、ポート チャネル インターフェイスで学習されたスタティック方式のセキュア MAC アドレスが含まれます。
- 各メンバ ポートのポート セキュリティ設定が復元されます。ポート チャネル インターフェイスに追加する前にそれらのメンバポートで学習されたスタティック方式のセキュア MAC アドレスは、NVRAM に復元され、実行コンフィギュレーションからは削除されます。ポートチャネルインターフェイスへの参加前にメンバポートでポートセキュリティが有効になっていなかった場合、そのメンバポートでは、ポートチャネルインターフェイスの削除後もポートセキュリティが有効になりません。



(注) ポート チャネル インターフェイスを削除したあとで、すべてのポートのセキュリティを必要に応じて確保するためには、すべてのメンバポートのポートセキュリティ設定を詳細に検査することを推奨します。

## ポート セキュリティの無効化

いずれかのメンバポートでポートセキュリティが有効になっている場合、ポート チャネル インターフェイスのポートセキュリティを無効にできません。これを行うには、まずすべてのセキュア メンバポートをポートチャネルインターフェイスから削除します。メンバポートのポートセキュリティを無効にしたあと、必要に応じて、ポートチャネルインターフェイスに再度追加できます。

# ポートタイプの変更

レイヤ2 インターフェイスにポートセキュリティを設定し、そのインターフェイスのポートタイプを変更した場合、デバイスは次のように動作します。

## ポートからトランクポートへのアクセス

レイヤ2 インターフェイスをアクセスポートからトランクポートに変更すると、デバイスはダイナミック方式で学習されたすべてのセキュアアドレスをドロップします。デバイスは、スタティック方式で学習したアドレスをネイティブトランクVLANに移行します。

## スイッチポートからルートポート

インターフェイスをレイヤ2 インターフェイスからレイヤ3 インターフェイスに変更すると、デバイスはそのインターフェイスのポートセキュリティをディセーブルにし、そのインターフェイスのすべてのポートセキュリティ設定を廃棄します。デバイスは、学習方式に関係なく、そのインターフェイスのセキュア MAC アドレスもすべて廃棄します。



### ルートポートからスイッチポート

インターフェイスをレイヤ3インターフェイスからレイヤ2インターフェイスに変更すると、デバイス上のそのインターフェイスのポートセキュリティ設定はなくなります。

## ポートセキュリティの前提条件

ポートセキュリティの前提条件は次のとおりです。

- ポートセキュリティで保護するデバイスのポートセキュリティをグローバルにイネーブル化すること。

## ポートセキュリティのデフォルト設定

次の表に、ポートセキュリティパラメータのデフォルト設定を示します。

パラメータ	デフォルト
ポートセキュリティがグローバルにイネーブルかどうか	ディセーブル
インターフェイス単位でポートセキュリティがイネーブルかどうか	ディセーブル
MAC アドレス ラーニング方式	Dynamic
セキュア MAC アドレスのインターフェイス最大数	1
セキュリティ違反時の処理	シャットダウン

## ポートセキュリティの注意事項と制約事項

ポートセキュリティを設定する場合、次の注意事項に従ってください。

- ポートセキュリティは、スイッチドポートアナライザ（SPAN）の宛先ポートをサポートしません。
- ポートセキュリティは他の機能に依存しません。
- Cisco NX-OS リリース 10.2(1)F 以降、USB ポートの無効化は Cisco NX-OS スイッチでサポートされています。USB ポートを無効または有効にするには、**[no] port usb disable** コマンドを使用します。
- プライマリ VLAN とセカンダリ VLAN 間のアソシエーションの設定後、このアソシエーションを削除すると、プライマリ VLAN 上に作成されたすべてのスタティック MAC アドレスは、プライマリ VLAN 上に限り存続します。

**Note**

一部の状況では、エラーメッセージが表示されずに設定が受け入れられますが、コマンドには効果がありません。

プライマリ VLAN とセカンダリ VLAN 間の関連付けを設定した後、次の手順を実行します。

- セカンダリ VLAN のスタティック MAC アドレスは作成できません。
- セカンダリ VLAN を学習したダイナミック MAC アドレスは期限切れになります。

## vPC 上のポートセキュリティの注意事項と制約事項

ポートセキュリティに関する注意事項および制限事項とは別に、vPC のポートセキュリティに関する次の注意事項および制限事項を満たしていることを確認します。

- ポートセキュリティは、vPC 展開の FEX インターフェイスではサポートされません。
- vPC ドメイン内の両方の vPC ピアで、ポートセキュリティをグローバルに有効にする必要があります。
- 両方の vPC ピアの vPC インターフェイス上でポートセキュリティを有効にする必要があります。
- プライマリ vPC ピアでスタティックセキュア MAC アドレスを設定する必要があります。スタティック MAC アドレスは、セカンダリ vPC ピアと同期されます。セカンダリピアでスタティックセキュア MAC アドレスも設定できます。第二スタティック MAC アドレスはセカンダリ vPC 設定に表示されますが、有効にはなりません。
- プライマリ vPC ポートとセカンダリ vPC ポートの両方で、最大 MAC カウント値が同じであることを確認する必要があります。
- セカンダリ vPC ポートでは、スタティック MAC の制限チェックは行われません。シスコは、最大 MAC カウントで定義されているように、セカンダリ vPC ポートで同じ数のスタティック MAC を設定することを推奨します。
- 学習したすべての MAC アドレスは vPC ピア間で同期されます。
- 両方の vPC ピアは、ダイナミックまたはスタティック MAC アドレスの学習方式で設定できます。シスコは、同じ方法を使用して両方の vPC ピアを設定することを推奨します。これは、vPC ロールの変更など、特定の場合にポートのシャットダウン（errDisabled 状態）を防ぐのに役立ちます。
- ダイナミック MAC アドレスは、両方の vPC ピアでエージング期限に達した後にのみドロップされます。
- セキュア MAC アドレスの最大数は、プライマリ vPC スイッチ上で設定します。プライマリ vPC スイッチは数の検証を行い、セカンダリ スイッチで最大数設定を無視します。

- 違反時の処理は、プライマリ vPC 上で設定します。セキュリティ違反がトリガーされると、プライマリ vPC スイッチに定義されたセキュリティ処理が常に実行されます。
- 両方の vPC ピアで設定が正しいことを確認するには、**show vpc consistency-parameters id** コマンドを使用できます。
- スイッチでインサースビス ソフトウェア アップグレード (ISSU) が実行されている間、ポートセキュリティの動作はそのピア スイッチ上で停止されます。ピア スイッチはどの新しい MAC アドレスも学習せず、この動作中に発生した MAC の移動は無視されます。ISSU が完了すると、ピア スイッチに通知され、通常のポートセキュリティ機能が再開します。
- 上位バージョンへの ISSU がサポートされていますが、下位バージョンへの ISSU はサポートされていません。

## ポート セキュリティの設定

### ポートセキュリティのグローバルなイネーブル化またはディセーブル化

デバイスに対してポートセキュリティ機能のグローバルなイネーブル化またはディセーブル化が可能です。デフォルトで、ポートセキュリティはグローバルにディセーブルになっています。

ポートセキュリティをディセーブルにすると、インターフェイスのすべてのポートセキュリティ設定が無効になります。ポートセキュリティをグローバルにディセーブル化すると、すべてのポートセキュリティ設定が失われます。

#### Procedure

	Command or Action	Purpose
ステップ 1	<b>configure terminal</b>  <b>Example:</b> switch# configure terminal switch(config)#	グローバル設定モードを開始します。
ステップ 2	<b>[no] feature port-security</b>  <b>Example:</b> switch(config)# feature port-security	ポートセキュリティをグローバルにイネーブル化します。 <b>no</b> オプションを使用するとポートセキュリティはグローバルに無効化されます。
ステップ 3	(Optional) <b>show port-security</b>  <b>Example:</b> switch(config)# show port-security	ポートセキュリティのステータスを表示します。

	Command or Action	Purpose
ステップ 4	(Optional) <b>copy running-config startup-config</b>  <b>Example:</b> <pre>switch(config)# copy running-config startup-config</pre>	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

## レイヤ2インターフェイスに対するポートセキュリティのイネーブル化またはディセーブル化

レイヤ2インターフェイスに対してポートセキュリティ機能のイネーブル化またはディセーブル化が可能です。デフォルトでは、ポートセキュリティはすべてのインターフェイスでディセーブルです。

インターフェイスのポートセキュリティをディセーブルにすると、そのインターフェイスのすべてのスイッチポートのポートセキュリティ設定が失われます。

### Before you begin

ポートセキュリティがグローバルにイネーブル化されている必要があります。

レイヤ2イーサネットインターフェイスがポートチャネルインターフェイスのメンバである場合、レイヤ2イーサネットインターフェイスに対するポートセキュリティはイネーブルまたはディセーブルにできません。

セキュアレイヤ2ポートチャネルインターフェイスのメンバのいずれかのポートセキュリティがイネーブルになっている場合、先にポートチャネルインターフェイスからセキュアメンバポートをすべて削除しない限り、そのポートチャネルインターフェイスのポートセキュリティをディセーブルにできません。

### Procedure

	Command or Action	Purpose
ステップ 1	<b>configure terminal</b>  <b>Example:</b> <pre>switch# configure terminal switch(config)#</pre>	グローバル構成モードを開始します。
ステップ 2	次のいずれかのコマンドを入力します。 <ul style="list-style-type: none"> <li>• <b>interface ethernet slot/port</b></li> <li>• <b>interface port-channel channel-number</b></li> </ul> <b>Example:</b> <pre>switch(config)# interface ethernet 2/1 switch(config-if)#</pre>	ポートセキュリティを設定するイーサネットインターフェイスまたはポートチャネルインターフェイスの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。

	Command or Action	Purpose
ステップ 3	<b>switchport</b> <b>Example:</b> switch(config-if) # switchport	そのインターフェイスを、レイヤ2インターフェイスとして設定します。
ステップ 4	<b>[no] switchport port-security</b> <b>Example:</b> switch(config-if) # switchport port-security	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。 <b>no</b> オプションを使用すると、そのインターフェイスのポートセキュリティがディセーブルになります。
ステップ 5	(Optional) <b>show running-config port-security</b> <b>Example:</b> switch(config-if) # show running-config port-security	ポートセキュリティの設定を表示します。
ステップ 6	(Optional) <b>copy running-config startup-config</b> <b>Example:</b> switch(config-if) # copy running-config startup-config	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

## スティック MAC アドレス ラーニングのイネーブル化またはディセーブル化

インターフェイスのスティック MAC アドレス ラーニングをディセーブルまたはイネーブルに設定できます。スティック学習をディセーブルにすると、そのインターフェイスはダイナミック MAC アドレス ラーニング（デフォルトの学習方式）に戻ります。

デフォルトでは、スティック MAC アドレス ラーニングはディセーブルです。

### Before you begin

ポートセキュリティがグローバルにイネーブル化されている必要があります。

### Procedure

	Command or Action	Purpose
ステップ 1	<b>configure terminal</b> <b>Example:</b> switch# configure terminal switch(config) #	グローバル構成モードを開始します。

	Command or Action	Purpose
ステップ 2	次のいずれかのコマンドを入力します。  <ul style="list-style-type: none"> <li>• <b>interface ethernet slot/port</b></li> <li>• <b>interface port-channel channel-number</b></li> </ul> <b>Example:</b> switch(config)# interface ethernet 2/1 switch(config-if)#	スティック MAC アドレス ラーニングを設定するインターフェイスのインターフェイス 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	<b>switchport</b>  <b>Example:</b> switch(config-if)# switchport	そのインターフェイスを、レイヤ 2 インターフェイスとして設定します。
ステップ 4	<b>[no] switchport port-security mac-address sticky</b>  <b>Example:</b> switch(config-if)# switchport port-security mac-address sticky	そのインターフェイスのスティック MAC アドレス ラーニングをイネーブルにします。 <b>no</b> オプションを使用するとスティック MAC アドレス ラーニングが無効になります。
ステップ 5	(Optional) <b>show running-config port-security</b>  <b>Example:</b> switch(config-if)# show running-config port-security	ポート セキュリティの設定を表示します。
ステップ 6	(Optional) <b>copy running-config startup-config</b>  <b>Example:</b> switch(config-if)# copy running-config startup-config	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

## インターフェイスのスタティック セキュア MAC アドレスの追加

レイヤ 2 インターフェイスにスタティック セキュア MAC アドレスを追加できます。



**Note** MAC アドレスが任意のインターフェイスでセキュア MAC アドレスである場合、その MAC アドレスがすでにセキュア MAC アドレスとなっているインターフェイスからその MAC アドレスを削除するまで、その MAC アドレスをスタティック セキュア MAC アドレスとして別のインターフェイスに追加することはできません。

デフォルトでは、インターフェイスにスタティック セキュア MAC アドレスは設定されません。

**Before you begin**

ポートセキュリティがグローバルにイネーブル化されている必要があります。

インターフェイスのセキュア MAC アドレス最大数に達していないことを確認します。必要に応じて、セキュア MAC アドレスを削除するか、インターフェイスの最大アドレス数を変更できます。

**Procedure**

	Command or Action	Purpose
ステップ 1	<b>configure terminal</b>  <b>Example:</b> <pre>switch# configure terminal switch(config)#</pre>	グローバル構成モードを開始します。
ステップ 2	次のいずれかのコマンドを入力します。  <ul style="list-style-type: none"> <li>• <b>interface ethernet slot/port</b></li> <li>• <b>interface port-channel channel-number</b></li> </ul> <b>Example:</b> <pre>switch(config)# interface ethernet 2/1 switch(config-if)#</pre>	指定したインターフェイスのインターフェイス 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	<b>[no] switchport port-security mac-address address [vlan vlan-ID]</b>  <b>Example:</b> <pre>switch(config-if)# switchport port-security mac-address 0019.D2D0.00AE</pre>	現在のインターフェイスのポートセキュリティにスタティック MAC アドレスを設定します。そのアドレスからのトラフィックを許可する VLAN を指定する場合は、 <b>vlan</b> キーワードを使用します。
ステップ 4	(Optional) <b>show running-config port-security</b>  <b>Example:</b> <pre>switch(config-if)# show running-config port-security</pre>	ポートセキュリティの設定を表示します。
ステップ 5	(Optional) <b>copy running-config startup-config</b>  <b>Example:</b> <pre>switch(config-if)# copy running-config startup-config</pre>	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

**インターフェイスのスタティック セキュア MAC アドレスの削除**

レイヤ 2 インターフェイスのスタティック セキュア MAC アドレスを削除できます。

## Procedure

	Command or Action	Purpose
ステップ 1	<b>configure terminal</b> <b>Example:</b> <pre>switch# configure terminal switch(config)#</pre>	グローバル構成モードを開始します。
ステップ 2	次のいずれかのコマンドを入力します。 <ul style="list-style-type: none"> <li>• <b>interface ethernet slot/port</b></li> <li>• <b>interface port-channel channel-number</b></li> </ul> <b>Example:</b> <pre>switch(config)# interface ethernet 2/1 switch(config-if)#</pre>	スタティックセキュア MAC アドレスを削除するインターフェイスのインターフェイス 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	<b>no switchport port-security mac-address address</b> <b>Example:</b> <pre>switch(config-if)# no switchport port-security mac-address 0019.D2D0.00AE</pre>	現在のインターフェイスのポートセキュリティからスタティックセキュア MAC アドレスを削除します。
ステップ 4	(Optional) <b>show running-config port-security</b> <b>Example:</b> <pre>switch(config-if)# show running-config port-security</pre>	ポートセキュリティの設定を表示します。
ステップ 5	(Optional) <b>copy running-config startup-config</b> <b>Example:</b> <pre>switch(config-if)# copy running-config startup-config</pre>	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

## スティッキ セキュア MAC アドレスの削除

スティッキセキュア MAC アドレスを削除できます。この際、削除するアドレスが設定されているインターフェイスで、スティッキ方式のアドレス学習を一時的にディセーブルにする必要があります。

## 始める前に

ポートセキュリティがグローバルにイネーブル化されている必要があります。



## 手順

	コマンドまたはアクション	目的
ステップ 1	<b>configure terminal</b>  例 : <pre>switch# configure terminal switch(config)#</pre>	グローバル構成モードを開始します。
ステップ 2	次のいずれかのコマンドを入力します。  <ul style="list-style-type: none"> <li>• <b>interface ethernet slot/port</b></li> <li>• <b>interface port-channel channel-number</b></li> </ul> 例 : <pre>switch(config)# interface ethernet 2/1 switch(config-if)#</pre>	スティッキセキュア MAC アドレスを削除するインターフェイスのインターフェイス 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	<b>no switchport port-security mac-address sticky</b>  例 : <pre>switch(config-if)# no switchport port-security mac-address sticky</pre>	インターフェイスのスティッキ MAC アドレス ラーニングをディセーブルにします。これにより、インターフェイスのスティッキセキュア MAC アドレスが、ダイナミックセキュア MAC アドレスに変換されます。
ステップ 4	<b>clear port-security dynamic address address</b>  例 : <pre>switch(config-if)# clear port-security dynamic address 0019.D2D0.02GD</pre>	指定したダイナミックセキュア MAC アドレスを削除します。
ステップ 5	(任意) <b>show port-security address interface {ethernet slot/port   port-channel channel-number}</b>  例 : <pre>switch(config)# show port-security address interface ethernet 2/1</pre>	セキュア MAC アドレスを表示します。削除したアドレスは表示されません。
ステップ 6	(任意) <b>switchport port-security mac-address sticky</b>  例 : <pre>switch(config-if)# switchport port-security mac-address sticky</pre>	そのインターフェイスのスティッキ MAC アドレス ラーニングを再度イネーブルにします。

## ダイナミック セキュア MAC アドレスの削除

ダイナミックに学習されたセキュア MAC アドレスを削除できます。

### Before you begin

ポートセキュリティがグローバルにイネーブル化されている必要があります。

### Procedure

	Command or Action	Purpose
ステップ 1	<b>configure terminal</b> <b>Example:</b> <pre>switch# configure terminal switch(config)#</pre>	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	<b>clear port-security dynamic {interface ethernet slot/port   address address} [vlan vlan-ID]</b> <b>Example:</b> <pre>switch(config)# clear port-security dynamic interface ethernet 2/1</pre>	<p>ダイナミックに学習されたセキュア MAC アドレスを削除します。次の方法で指定できます。</p> <p><b>interface</b> キーワードを使用すると、指定したインターフェイスでダイナミックに学習されたアドレスがすべて削除されます。</p> <p><b>address</b> キーワードを使用すると、指定した単一のダイナミック学習アドレスが削除されます。</p> <p>特定の VLAN のアドレスを削除するようにコマンドに制限を加えるには、<b>vlan</b> キーワードを使用します。</p>
ステップ 3	(Optional) <b>show port-security address</b> <b>Example:</b> <pre>switch(config)# show port-security address</pre>	セキュア MAC アドレスを表示します。
ステップ 4	(Optional) <b>copy running-config startup-config</b> <b>Example:</b> <pre>switch(config-if)# copy running-config startup-config</pre>	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

## MAC アドレスの最大数の設定

レイヤ2インターフェイスで学習可能なMACアドレスまたはスタティックに設定可能なMACアドレスの最大数を設定できます。レイヤ2インターフェイス上のVLAN単位でもMACアドレスの最大数を設定できます。インターフェイスに設定できる最大アドレス数は1025です。システムの最大アドレス数は8192です。

デフォルトでは、各インターフェイスのセキュアMACアドレスの最大数は1です。VLANには、セキュアMACアドレス数のデフォルトの最大値はありません。



### Note

インターフェイスですでに学習されているアドレス数またはインターフェイスにスタティックに設定されたアドレス数よりも小さい数を最大数に指定すると、デバイスはこのコマンドを拒否します。ダイナミック方式で学習されたアドレスをすべて削除するには、**shutdown** および **no shutdown** のコマンドを使用して、インターフェイスを再起動します。

### Before you begin

ポートセキュリティがグローバルにイネーブル化されている必要があります。

### Procedure

	Command or Action	Purpose
ステップ1	<b>configure terminal</b>  <b>Example:</b> <pre>switch# configure terminal switch(config)#</pre>	グローバル構成モードを開始します。
ステップ2	次のいずれかのコマンドを入力します。  • <b>interface ethernet slot/port</b> • <b>interface port-channel channel-number</b>  <b>Example:</b> <pre>switch(config)# interface ethernet 2/1 switch(config-if)#</pre>	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。slot は、MACアドレスの最大数を設定するインターフェイスです。
ステップ3	<b>[no] switchport port-security maximum number [vlan vlan-ID]</b>  <b>Example:</b> <pre>switch(config-if)# switchport port-security maximum 425</pre>	現在のインターフェイスで学習可能なMACアドレスまたはスタティックに設定可能なMACアドレスの最大数を設定します。有効な number の最高値は1025です。no オプションを使用すると、MACアドレスの最大数がデフォルト値（1）にリセットされます。  最大数を適用するVLANを指定する場合は、vlan キーワードを使用します。

## ■ アドレス エージング タイプおよび時間を設定する

	Command or Action	Purpose
ステップ 4	(Optional) <b>show running-config port-security</b>  <b>Example:</b> <pre>switch(config-if)# show running-config port-security</pre>	ポート セキュリティの設定を表示します。
ステップ 5	(Optional) <b>copy running-config startup-config</b>  <b>Example:</b> <pre>switch(config-if)# copy running-config startup-config</pre>	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

## アドレス エージング タイプおよび時間を設定する

MAC アドレス エージングのタイプと期間を設定できます。デバイスは、ダイナミック方式で学習された MAC アドレスがエージング期限に到達する時期を判断するためにこれらの設定を使用します。

デフォルトのエージング タイプは絶対エージングです。

デフォルトのエージング タイムは 0 分（エージングは無効）です。

### Before you begin

ポート セキュリティがグローバルに有効にされている必要があります。

### Procedure

	Command or Action	Purpose
ステップ 1	<b>configure terminal</b>  <b>Example:</b> <pre>switch# configure terminal switch(config)#</pre>	グローバル構成モードを開始します。
ステップ 2	次のいずれかのコマンドを入力します。 <ul style="list-style-type: none"> <li><b>interface ethernet slot/port</b></li> <li><b>interface port-channel channel-number</b></li> </ul> <b>Example:</b> <pre>switch(config)# interface ethernet 2/1 switch(config-if)#</pre>	MAC エージングのタイプと期間を設定するインターフェイスのインターフェイス 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	<b>[no] switchport port-security aging type {absolute   inactivity}</b>  <b>Example:</b>	ダイナミックに学習された MAC アドレスにデバイスが適用するエージング タイプを設定します。no オプションを使

	Command or Action	Purpose
	switch(config-if)# switchport port-security aging type inactivity	用すると、エージング タイプがデフォルト値（絶対エージング）にリセットされます。
ステップ 4	<b>[no] switchport port-security aging time minutes</b>  <b>Example:</b>  switch(config-if)# switchport port-security aging time 120	ダイナミックに学習された MAC アドレスがドロップされるまでのエージング タイムを分単位で設定します。 <i>minutes</i> の最大値は 1440 です。 <b>no</b> オプションを使用すると、エージング タイムがデフォルト値である 0（エージングは無効）にリセットされます。
ステップ 5	(Optional) <b>show running-config port-security</b>  <b>Example:</b>  switch(config-if)# show running-config port-security	ポートセキュリティの設定を表示します。
ステップ 6	(Optional) <b>copy running-config startup-config</b>  <b>Example:</b>  switch(config-if)# copy running-config startup-config	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

## セキュリティ違反時の処理の設定

セキュリティ違反が発生した場合にデバイスが実行する処理を設定できます。違反時の処理は、ポートセキュリティをイネーブルにしたインターフェイスごとに設定できます。

デフォルトのセキュリティ処理では、セキュリティ違反が発生したポートがシャットダウンされます。

### Before you begin

ポートセキュリティがグローバルにイネーブル化されている必要があります。

### Procedure

	Command or Action	Purpose
ステップ 1	<b>configure terminal</b>  <b>Example:</b>  switch# configure terminal switch(config)#	グローバル構成モードを開始します。

	Command or Action	Purpose
ステップ 2	次のいずれかのコマンドを入力します。  <ul style="list-style-type: none"> <li>• <b>interface ethernet slot/port</b></li> <li>• <b>interface port-channel channel-number</b></li> </ul> <b>Example:</b> <pre>switch(config)# interface ethernet 2/1 switch(config-if)#</pre>	セキュリティ違反時の処理を設定するインターフェイスのインターフェイス 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	<b>[no] switchport port-security violation {protect   restrict   shutdown}</b>  <b>Example:</b> <pre>switch(config-if)# switchport port-security violation restrict</pre>	現在のインターフェイスのポートセキュリティにセキュリティ違反時の処理を設定します。 <b>no</b> オプションを使用すると、違反時の処理がデフォルト値（インターフェイスのシャットダウン）にリセットされます。
ステップ 4	(Optional) <b>show running-config port-security</b>  <b>Example:</b> <pre>switch(config-if)# show running-config port-security</pre>	ポートセキュリティの設定を表示します。
ステップ 5	(Optional) <b>copy running-config startup-config</b>  <b>Example:</b> <pre>switch(config-if)# copy running-config startup-config</pre>	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

## ポートセキュリティの設定の確認

ポートセキュリティの設定情報を表示するには、次のいずれかの作業を行います。

コマンド	目的
<b>show running-config port-security</b>	ポートセキュリティの設定を表示します。
<b>show port-security</b>	デバイスのポートセキュリティのステータスを表示します。
<b>show port-security interface</b>	特定のインターフェイスのポートセキュリティのステータスを表示します。
<b>show port-security address</b>	セキュア MAC アドレスを表示します。
<b>show vpc consistency-parameters vpc id</b>	両方の vPC ピアの設定を確認します。

## セキュア MAC アドレスの表示

セキュア MAC アドレスを表示するには、**show port-security address** コマンドを使用します。

## ポート セキュリティの設定例

次に示す例は、VLAN とインターフェイスのセキュア アドレス最大数が指定されているイーサネット 2/1 インターフェイスのポートセキュリティ設定です。この例のインターフェイスはトランク ポートです。違反時の処理は Restrict（制限）に設定されています。

```
feature port-security
interface Ethernet 2/1
  switchport
  switchport port-security
  switchport port-security maximum 10
  switchport port-security maximum 7 vlan 10
  switchport port-security maximum 3 vlan 20
  switchport port-security violation restrict
```

## vPC ドメインでのポート セキュリティの設定例

次に、vPC ドメインで vPC ピア上のポート セキュリティをイネーブルにして設定する例を示します。最初のスイッチがプライマリ vPC ピアであり、2 番目のスイッチがセカンダリ vPC ピアです。スイッチでポートセキュリティを設定する前に、vPC ドメインを作成し、vPC ピアリンク 隣接関係が確立されていることを確認します。

### 例：孤立ポートでのポート セキュリティの設定

```
primary_switch(config)# feature port-security
primary_switch(config-if)# int e1/1
primary_switch(config-if)# switchport port-security
primary_switch(config-if)# switchport port-security max 1025
primary_switch(config-if)# switchport port-security violation restrict
primary_switch(config-if)# switchport port-security aging time 4
primary_switch(config-if)# switchport port-security aging type absolute
primary_switch(config-if)# switchport port-security mac sticky
primary_switch(config-if)# switchport port-security mac-address 0.0.1 vlan 101
primary_switch(config-if)# switchport port-security mac-address 0.0.2 vlan 101
primary_switch(config-if)# copy running-config startup-config

secondary_switch(config)# feature port-security
secondary_switch(config)# int e3/1
secondary_switch(config-if)# switchport port-security
secondary_switch(config-if)# switchport port-security max 1025
secondary_switch(config-if)# switchport port-security violation restrict
secondary_switch(config-if)# switchport port-security aging time 4
secondary_switch(config-if)# switchport port-security aging type absolute
secondary_switch(config-if)# switchport port-security mac sticky
secondary_switch(config-if)# switchport port-security mac-address 0.0.1 vlan 101
```

## 例：vPC レッグ上のポートセキュリティの設定

```
secondary_switch(config-if)# switchport port-security mac-address 0.0.2 vlan 101
secondary_switch(config-if)# copy running-config startup-config
```

## 例：vPC レッグ上のポートセキュリティの設定

```
primary_switch(config)# feature port-security
primary_switch(config-if)# int po10
primary_switch(config-if)# switchport port-security
primary_switch(config-if)# switchport port-security max 1025
primary_switch(config-if)# switchport port-security violation restrict
primary_switch(config-if)# switchport port-security aging time 4
primary_switch(config-if)# switchport port-security aging type absolute
primary_switch(config-if)# switchport port-security mac sticky
primary_switch(config-if)# switchport port-security mac-address 0.0.1 vlan 101
primary_switch(config-if)# switchport port-security mac-address 0.0.2 vlan 101
primary_switch(config-if)# vpc 10
primary_switch(config-if)# copy running-config startup-config

secondary_switch(config)# feature port-security
secondary_switch(config)# int po10
secondary_switch(config-if)# switchport port-security
secondary_switch(config-if)# switchport port-security max 1025
secondary_switch(config-if)# switchport port-security violation restrict
secondary_switch(config-if)# switchport port-security aging time 4
secondary_switch(config-if)# switchport port-security aging type absolute
secondary_switch(config-if)# switchport port-security mac sticky
secondary_switch(config-if)# switchport port-security mac-address 0.0.1 vlan 101
secondary_switch(config-if)# switchport port-security mac-address 0.0.2 vlan 101
secondary_switch(config-if)# vpc 10
secondary_switch(config-if)# copy running-config startup-config
```

## ポートセキュリティに関する追加情報

## 関連資料

関連項目	マニュアルタイトル
レイヤ2スイッチング	『Cisco Nexus 9000 Series NX-OS Layer 2 Switching Configuration Guide』

## MIB

Cisco NX-OS はポートセキュリティに関して読み取り専用の SNMP をサポートしています。

MIB	MIB のリンク
<b>CISCO-PORT-SECURITY-MIB</b>  <b>Note</b> トラップは、セキュア MAC アドレスの違反の通知についてサポートされています。	MIB を検索およびダウンロードするには、次の URL にアクセスしてください。  <a href="https://snmp.cloudapps.cisco.com/Support/SNMP/do/BrowseMIB.do?local=en&amp;step=2">https://snmp.cloudapps.cisco.com/Support/SNMP/do/BrowseMIB.do?local=en&amp;step=2</a>



# VXLAN EVPN のポート セキュリティ サポート

このセクションでは、VXLAN EVPN のポート セキュリティ機能の構成方法について説明します。

## VXLAN EVPN のポート セキュリティ サポートに関する注意事項と制約事項

VXLAN EVPN のポートセキュリティ サポートに関する注意事項と制約事項を次に示します。

- Cisco NX-OS リリース 10.3(3)F 以降、L2 ポート セキュリティ機能は、Cisco Nexus 9300-FX/FX2/FX3/GX/GX2、9408 の VXLAN BGP EVPN（シングル VTEP）および X97160YC-EX、9700-FX/GX ライン カードを搭載した Cisco Nexus 9500 スイッチでサポートされますが、次の制限があります。
  - 単一の VTEP ソリューションのみがサポートされます。ただし、セキュア MAC モビリティは VXLAN 環境ではサポートされません。
- Cisco NX-OS リリース 10.3(3)F 以降、IPv6 アンダーレイは、Cisco Nexus 9300-FX/FX2/FX3/GX/GX2 スイッチおよび X97160YC-EX、9700-FX/GX ラインカードを搭載した Cisco Nexus 9500 スイッチにおいて、VXLAN EVPN のポート セキュリティ（単一 VTEP）でサポートされます。
- ポート セキュリティは、ファブリック ピアリングではサポートされていません。
- L2 ポート セキュリティ機能が有効になっている場合、次の動作が観察されます。
  - セキュア MAC は静的 MAC として送信され、リモート VTEP では静的 MAC として認識されます。したがって、リモート VTEP 上のセキュア MAC をダイナミック MAC として学習しようとする試みがある場合（同じ MAC を持つ悪意のあるホストが原因で）、それは阻止されます。
  - 違反した MAC に **restrict** オプションが設定されている場合、これらの違反した MAC は **static drop** セットを使用して送信されます。リモート VTEP では、MAC は静的ドロップで構成されるため、リモート VTEP からこれらのホストにトラフィックを送信しようすると、リモート VTEP 自体でドロップされます。
  - ローカルの静的 MAC とセキュア MAC の両方がスティッキー ビットを使用してファブリックにアドバタイズされるため、リモート VTEP については、リモート静的 MAC がセキュア MAC または静的 MAC のどちらの VTEP からのものであっても違いはありません。
  - ローカル スタティックがすでに存在する場合は、リモート スタティック（セキュア またはスタティック）よりも優先されます。
  - MAC に対してローカルで行われたセキュリティの決定に基づいて、ローカル VTEP からファブリックへのセキュア ポートで学習された MAC に複数の更新が存在する可

能性がありますが、MAC の最終的なセキュリティ動作はローカルおよびリモート VTEP で一貫しています。

- セキュア MAC の **inactivity** 値を指定できます。アクティビティがない場合、セキュア MAC は削除され、セキュア MAC ホストは別のポートに移動することがあります。

## VXLAN EVPN のポートセキュリティ サポートの確認

VXLAN EVPN の構成情報のポートセキュリティ サポートを表示するには、次のいずれかのコマンドを入力します。

コマンド	目的
<b>show running-config interface</b> <interface-name>	インターフェイスの実行中の構成を表示します。
<b>show port-security</b>	ポートセキュリティ 構成情報を表示します。

### show running-config interface コマンドの例

```
switch(config-if)# show run inter e1/48
!Command: show running-config interface Ethernet1/48
!Running configuration last done at: Thu Feb 16 08:39:43 2023
!Time: Fri Feb 17 06:07:33 2023

version 10.3(3) Bios:version 01.08

interface Ethernet1/48
 switchport
 switchport mode trunk
 switchport trunk allowed vlan 200
 spanning-tree port type edge trunk
 switchport port-security maximum 1025
 switchport port-security
 no shutdown

LVTEP:
-----
switch(config-if)# show mac address-table inter e1/48
Legend:
      * - primary entry, G - Gateway MAC, (R) - Routed MAC, O - Overlay MAC
      age - seconds since last seen, + - primary entry using vPC Peer-Link,
      (T) - True, (F) - False, C - ControlPlane MAC, ~ - vsan,
      (NA) - Not Applicable
      VLAN      MAC Address      Type      age      Secure NTFY Ports
-----+-----+-----+-----+-----+-----+-----
* 101          0012.0100.0001    secure    -         T        F    Eth1/48
* 101          0012.0100.0002    secure    -         T        F    Eth1/48
* 101          0012.0100.0003    secure    -         T        F    Eth1/48
* 101          0012.0100.0004    secure    -         T        F    Eth1/48
```

### show port-security コマンドの例

```
switch(config-if)# show port-security
Total Secured Mac Addresses in System (excluding one mac per port)      : 1024
Max Addresses limit in System (excluding one mac per port) : 7168
```

```

-----
Secure Port      MaxSecureAddr  CurrentAddr  SecurityViolation  Security Action
              (Count)          (Count)          (Count)
-----
Ethernet1/48      1025          1025          0                  Shutdown

```

```
switch(config-if)# show port-security address interface e1/48
```

```

-----
Secure Mac Address Table
-----
Vlan      Mac Address      Type      Remaining  Remotely  Remotely  Ports
          (Count)          (mins)    learnt    aged      out
-----
101      0012.0100.0001    DYNAMIC    0          No        No        Ethernet1/48
101      0012.0100.0002    DYNAMIC    0          No        No        Ethernet1/48
101      0012.0100.0003    DYNAMIC    0          No        No        Ethernet1/48
101      0012.0100.0004    DYNAMIC    0          No        No        Ethernet1/48

```

```
RVTEP:
```

```

-----
Standalone_VTEP_EX# show mac address-table
C 101      0012.0100.0001    static    -          F        F        nve1(20:20:20::20)
C 101      0012.0100.0002    static    -          F        F        nve1(20:20:20::20)
C 101      0012.0100.0003    static    -          F        F        nve1(20:20:20::20)
C 101      0012.0100.0004    static    -          F        F        nve1(20:20:20::20)

```



## 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。