



ポート セキュリティ

この章は、次の項で構成されています。

- [ポート セキュリティと ACI について \(1 ページ\)](#)
- [ポート セキュリティに関するガイドラインと制約事項 \(1 ページ\)](#)
- [ポート レベルでのポート セキュリティ \(2 ページ\)](#)
- [ポート セキュリティおよびラーニング動作 \(5 ページ\)](#)
- [保護モード \(6 ページ\)](#)

ポート セキュリティと ACI について

ポート セキュリティ機能は、ポートごとに取得される MAC アドレスの数を制限することによって、不明な MAC アドレスでフラッドしないように ACI ファブリックを保護します。ポート セキュリティ機能のサポートは、物理ポート、ポート チャネル、および仮想ポート チャネルで使用できます。

ポート セキュリティに関するガイドラインと制約事項

次のようなガイドラインと制約事項があります。

- ポート セキュリティは、ポートごとに使用できます。
- ポートセキュリティは、物理ポート、ポートチャネル、および仮想ポートチャネル (vPC) でサポートされています。
- スタティック MAC アドレスとダイナミック MAC アドレスがサポートされています。
- セキュアなポートからセキュアでないポートへと、セキュアでないポートからセキュアなポートへの MAC アドレスの移動がサポートされています。
- MAC アドレスの制限は、MAC アドレスにのみ適用され、MAC と IP によるアドレスには実行されません。

- ポートセキュリティは、ファブリック エクステンダ (FEX) ではサポートされていません。

ポートレベルでのポートセキュリティ

APICでは、ユーザがスイッチポートのポートセキュリティを設定できます。ポート上でMACが制限の最大設定値を超過すると、超過したMACアドレスからすべてのトラフィックが転送されます。次の属性がサポートされます。

- **ポートセキュリティのタイムアウト** : 現在サポートされているタイムアウト値は、60 ~ 3600 秒の範囲でサポートされています。
- **違反行為** : 違反行為は保護モードで使用できます。保護モードでは、MACの取得が無効になるため、MACアドレスはCAMテーブルに追加されません。Mac ラーニングが設定されているタイムアウト値の後に再度有効になります。
- **最大エンドポイント** : 現在のサポートされている最大のエンドポイント設定値は、0 ~ 12000 の範囲でサポートされています。最大エンドポイント値が0の場合、そのポートではポートセキュリティポリシーが無効になります。

APIC GUI を使用したポートセキュリティの設定

- ステップ1** メニューバーで [ファブリック アクセス ポリシー (**Fabric > Access Policies**)] をクリックし、[ナビゲーション (**Navigation**)] ペインで [ポリシー インターフェイス ポートセキュリティ (**Policies > Interface > Port Security**)] を展開します。
- ステップ2** [ポートセキュリティ] 右クリックして、[ポートセキュリティ ポリシーの作成] をクリックします。
- ステップ3** [ポートセキュリティ ポリシーの作成] ダイアログ ボックスで、次の操作を実行します。
 - a) [Name] フィールドにポリシーの名前を入力します。
 - b) [ポートセキュリティのタイムアウト] フィールドに、インターフェイスのMAC ラーニングを再度有効にする前に、タイムアウトの値を選択します。
 - c) [最大エンドポイント] フィールドに、インターフェイスで学習可能なエンドポイントの最大数の希望値を選択します。
 - d) [違反アクション] フィールドで、使用可能なオプションは [保護] です。[Submit] をクリックします。ポートセキュリティ ポリシーが作成されます。
- ステップ4** (注) リーフスイッチのインターフェイスを設定するときに、使用可能なポートセキュリティポリシーのリストからポートセキュリティ ポリシーを選択することができます。

[ナビゲーション] ペインで、[ファブリック] > [インベントリ] > [トポロジ] をクリックし、目的のリーフスイッチに移動します。インターフェイスを設定する適切なポートを選択し、ポートセキュリティポリシー ドロップダウン リストから関連付けに必要なポートセキュリティ ポリシーを選択します。

これで、ポート上のポートセキュリティの設定を完了します。

REST API を使用して、ポートセキュリティの設定

ポートセキュリティを設定します。

例：

```
<polUni>
  <infraInfra>

    <l2PortSecurityPol name="testL2PortSecurityPol" maximum="10" violation="protect" timeout="300"/>

    <infraNodeP name="test">
      <infraLeafS name="test" type="range">
        <infraNodeBlk name="test" from_"101" to_"102"/>
      </infraLeafS>
      <infraRsAccPortP tDn="uni/infra/accportprof-test"/>
    </infraNodeP>

    <infraAccPortP name="test">
      <infraHPortS name="pselc" type="range">
        <infraPortBlk name="blk"
          fromCard="1" toCard="1" fromPort="20" toPort="22">
          </infraPortBlk>
        <infraRsAccBaseGrp tDn="uni/infra/funcprof/accportgrp-testPortG" />
      </infraHPortS>
    </infraAccPortP>

    <infraFuncP>
      <infraAccPortGrp name="testPortG">
        <infraRsL2PortSecurityPol tnL2PortSecurityPolName="testL2PortSecurityPol"/>
        <infraRsAttEntP tDn="uni/infra/attentp-test" />
      </infraAccPortGrp>
    </infraFuncP>

    <infraAttEntityP name="test">
      <infraRsDomP tDn="uni/phys-mininet"/>
    </infraAttEntityP>
  </infraInfra>
</polUni>
```

CLI を使用したポートセキュリティの設定

手順

	コマンドまたはアクション	目的
ステップ 1	configure 例：	コンフィギュレーションモードに入ります。

	コマンドまたはアクション	目的
	<code>apic1# configure</code>	
ステップ 2	<code>leaf node-id</code> 例： <code>apic1(config)# leaf 101</code>	設定するリーフを指定します。
ステップ 3	<code>interface type-or-range</code> 例： <code>apic1(config-leaf)# interface eth 1/2-4</code>	設定するインターフェイスまたはインターフェイスの範囲を指定します。
ステップ 4	<code>[no] switchport port-security maximum number-of-addresses</code> 例： <code>apic1(config-leaf-if)# switchport port-security maximum 1</code>	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。範囲は 0 ~ 12000 アドレスです。デフォルトは 1 アドレスです。
ステップ 5	<code>[no] switchport port-security violation protect</code> 例： <code>apic1(config-leaf-if)# switchport port-security violation protect</code>	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。 protect アクションは、十分な数のセキュア MAC アドレスを削除して最大値を下回るまで、不明な送信元アドレスのパケットをドロップします。
ステップ 6	<code>[no] switchport port-security timeout</code> 例： <code>apic1(config-leaf-if)# switchport port-security timeout 300</code>	インターフェイスのタイムアウト値を設定します。範囲は 60 ~ 3600 です。デフォルトは 60 秒です。

例

次に、イーサネットインターフェイスでポートセキュリティを設定する方法を示します。

```
apic1# configure
apic1(config)# leaf 101
apic1(config-leaf)# interface eth 1/2
apic1(config-leaf-if)# switchport port-security maximum 10
apic1(config-leaf-if)# switchport port-security violation protect
apic1(config-leaf-if)# switchport port-security timeout 300
```

次に、ポートチャネルでポートセキュリティを設定する例を示します。

```
apic1# configure
apic1(config)# leaf 101
apic1(config-leaf)# interface port-channel po2
apic1(config-leaf-if)# switchport port-security maximum 10
apic1(config-leaf-if)# switchport port-security violation protect
apic1(config-leaf-if)# switchport port-security timeout 300
```

次に、仮想ポートチャネル（VPC）でポートセキュリティを設定する例を示します。

```
apicl# configure
apicl(config)# vpc domain explicit 1 leaf 101 102
apicl(config-vpc)# exit
apicl(config)# template port-channel po4
apicl(config-if)# exit
apicl(config)# leaf 101-102
apicl(config-leaf)# interface eth 1/11-12
apicl(config-leaf-if)# channel-group po4 vpc
apicl(config-leaf-if)# exit
apicl(config-leaf)# exit
apicl(config)# vpc context leaf 101 102
apicl(config-vpc)# interface vpc po4
apicl(config-vpc-if)# switchport port-security maximum 10
apicl(config-vpc-if)# switchport port-security violation protect
apicl(config-leaf-if)# switchport port-security timeout 300
```

ポートセキュリティおよびラーニング動作

非vPCポートまたはポートチャネルでは、新しいエンドポイントに対して学習イベントが発生し、新しい学習が許可されているか確認する検証が行われます。対応するインターフェイスに設定されていない、または無効なポートセキュリティポリシーが存在する場合、エンドポイントラーニング動作はサポートされているものから変更されません。ポリシーが有効になっており制限に到達している場合、現在のサポートされているアクションは次の通りです。

- エンドポイントを学習し、ドロップアクションのハードウェアにインストールします。
- サイレントに学習を破棄します。

制限に到達していない場合、エンドポイントが学習され、この新しいエンドポイントが発生したため制限に達しているかどうか確認する検証が行われます。制限に到達しており、学習の無効化アクションが設定されている場合、インターフェイス上のハードウェアでラーニングが無効になります（物理インターフェイスまたはポートチャネルまたはvPC）。制限に到達しており、学習の無効化アクションが設定されていない場合、エンドポイントはドロップアクションでハードウェアにインストールされます。このようなエンドポイントは、他のエンドポイントのように通常期限切れです。

初めて制限に達したとき、ポートセキュリティポリシーオブジェクトの動作状態がそれを反映して更新されます。スタティックルールは、ユーザーに警告ができるように、障害の発生と定義されます。制限に到達すると、Syslogも発生します。

vPCの場合、MAC制限に到達するとピアリーフスイッチにも通知されるため、ラーニングがピアで無効になる可能性があります。vPCピアはいつでも再起動でき、vPCレグが動作不能になるか再起動できるため、この状態はピアと調和してvPCピアはこの状態に同期されません。同期しない場合は、1個のレグでラーニングが有効になり、他のレグで無効になる状況が発生する可能性があります。

デフォルトでは、制限に到達してラーニングが無効になると、60秒のデフォルトタイムアウト値の後、自動的に再度有効になります。

保護モード

保護モードはセキュリティ違反が発生している以上に増やさないようにします。MAC の制限がポートで設定されている最大値を超えると、超過したMACアドレスからすべてのトラフィックはドロップされ、さらにラーニングが無効になります。

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。