



# ポートセキュリティの設定

---

この章では、ポートセキュリティ機能を設定する手順について説明します。



(注)

この章で使用しているコマンドの構文および使用方法の詳細については、次の URL の『*Catalyst 6500 Series Switch Cisco IOS Command Reference*』 Release 12.2SX を参照してください。

<http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/122sx/cmdref/index.htm>

---

この章で説明する内容は、次のとおりです。

- ポートセキュリティの概要 (p.48-2)
- ポートセキュリティのデフォルト設定 (p.48-4)
- ポートセキュリティに関する注意事項および制約事項 (p.48-4)
- ポートセキュリティの設定 (p.48-6)
- ポートセキュリティ設定の表示 (p.48-15)

## ポートセキュリティの概要

ここでは、ポートセキュリティについて説明します。

- [ダイナミックに学習される MAC アドレスとスタティック MAC アドレスによるポートセキュリティ \(p.48-2\)](#)
- [sticky MAC アドレスによるポートセキュリティ \(p.48-3\)](#)

## ダイナミックに学習される MAC アドレスとスタティック MAC アドレスによるポートセキュリティ

ダイナミックに学習される MAC (メディア アクセス制御) アドレス、およびスタティック MAC アドレスを使用したポートセキュリティでは、ポートへのトラフィック送信を許可する MAC アドレスを制限できるので、入力トラフィックを制限できます。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入力トラフィックを転送しません。セキュア MAC アドレスの数を 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ている装置はそのポートの全帯域を使用できません。

セキュリティ違反は、次のいずれかの状況で発生します。

- セキュア ポートでセキュア MAC アドレスの最大数に達したあと、入力トラフィックの送信元 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場合は、設定済みの違反モードが適用されます。
- 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 (仮想 LAN) 内の別のセキュア ポートにアクセスしようとする、ポートセキュリティはこの違反に対し、次のいずれかの方法で対応します。
  - Release 12.2(18)SXF5 以降のリリースでは、設定済みの違反モードが適用されます。
  - Release 12.2(18)SXF5 より前のリリースでは、シャットダウン違反モードが適用されます。



**(注)** あるセキュア ポートでセキュア MAC アドレスが設定または学習されたあと、同じ VLAN 内の別のポート上でこのセキュア MAC アドレスが検出された場合に発生する一連のイベントを、MAC の移行違反と呼びます。

違反モードの詳細情報については、「[ポートでのポートセキュリティ違反モードの設定](#)」(p.48-8)を参照してください。

ポートでセキュア MAC アドレスの最大数を設定したあと、セキュア アドレスは、次のいずれかの方法でアドレス テーブルに組み込まれます。

- 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スタティックに設定できます。
- 接続されている装置の MAC アドレスによって、ポートがセキュア MAC アドレスをダイナミックに設定するように指定できます。
- 多数のアドレスをスタティックに設定し、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できます。

ポートがリンクダウン状態になると、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。

ブートアップ、リロード、またはリンクダウン状態のあとは、ポートが入力トラフィックを受信するまで、ダイナミックに学習された MAC アドレスはアドレス テーブルに書き込まれません。

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た時点で、アドレス テーブルにはない MAC アドレスからのトラフィックをポートが受信すると、セキュリティ違反となります。

ポートには、`protect`、`restrict`、または `shutdown` のいずれかの違反モードを設定できます。「[ポートセキュリティの設定](#)」(p.48-6) を参照してください。

アドレスの最大数を 1 に設定し、接続された装置の MAC アドレスを設定すると、その装置にはポートの全帯域幅が保証されます。

## sticky MAC アドレスによるポート セキュリティ

Release 12.2(18)SXE 以降のリリースでは、sticky MAC アドレスによるポート セキュリティがサポートされます。sticky MAC アドレスを使用するポート セキュリティには、スタティック MAC アドレスによるポート セキュリティと同様の多数の利点がありますが、さらに、sticky MAC アドレスはダイナミックに学習できます。sticky MAC アドレスを使用したポート セキュリティでは、リンクダウン状態の発生中も、ダイナミックに学習された MAC アドレスを維持します。

sticky MAC アドレスによるポート セキュリティでは、`write memory` または `copy running-config startup-config` コマンドを実行すると、ダイナミックに学習された MAC アドレスは `startup-config` ファイルに保存されます。したがって、ブートアップ後または再起動後に、ポートが入力トラフィックからアドレスを学習する必要がありません。

## ポートセキュリティのデフォルト設定

表 48-1 に、インターフェイス用のデフォルトのポートセキュリティ設定を示します。

表 48-1 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	ディセーブル
セキュア MAC アドレスの最大数	1
違反モード	shutdown。セキュア MAC アドレスが最大数を超過した場合、ポートはシャットダウンし、SNMP（簡易ネットワーク管理プロトコル）トラップ通知が送信されます。

## ポートセキュリティに関する注意事項および制約事項

ポートセキュリティを設定する場合は、次の注意事項に従ってください。

- **errdisable** ステートのセキュア ポートを、デフォルトのポートセキュリティ設定によって回復するには、**errdisable recovery cause shutdown** グローバル コンフィギュレーション コマンドを入力します。または、**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 コマンドを入力して、このセキュア ポートを手動で再びイネーブルに戻すこともできます。
- ダイナミックに学習されたすべてのセキュア アドレスを消去するには、**clear port-security dynamic** グローバル コンフィギュレーション コマンドを入力します。構文の詳細については、『*Catalyst 6500 Series Switch Cisco IOS Command Reference*』 Release 12.2SX を参照してください。
- 無許可の MAC アドレスは、特定のビットセットとともに学習されます。このビットセットにより、このアドレスから送信されるトラフィック、およびこのアドレス宛てに送信されるトラフィックはいずれも廃棄されます。**show mac-address-table** コマンドを使用すると、無許可の MAC アドレスを表示できますが、ビット ステートは表示されません。(CSCeb76844)
- **sticky** MAC アドレスがダイナミックに学習されたあとに、このアドレスを保持して、ブートアップまたはリロード後にポートに設定されるようにするには、**write memory** または **copy running-config startup-config** コマンドを入力して、アドレスを **startup-config** ファイルに保存する必要があります。
- Release 12.2(18)SXE 以降のリリースでは、ポートセキュリティでは Private VLAN (PVLAN) ポートがサポートされます。
- Release 12.2(18)SXE より前のリリースでは、PVLAN ポートはポートセキュリティでサポートされません。
- Release 12.2(18)SXE 以降のリリースでは、ポートセキュリティでは非交渉トランクがサポートされます。
  - ポートセキュリティは、次のコマンドで設定したトランクのみをサポートします。
 

```
switchport
switchport trunk encapsulation
switchport mode trunk
switchport nonegotiate
```
  - セキュア アクセス ポートをトランクとして再設定すると、アクセス VLAN でダイナミックに学習された、このポートのすべての **sticky** およびスタティック セキュア アドレスが、トランクのネイティブ VLAN 上の **sticky** およびスタティック セキュア アドレスに変換されます。アクセス ポートの音声 VLAN では、すべてのセキュア アドレスが削除されます。
  - セキュア トランクをアクセス ポートとして再設定すると、ネイティブ VLAN で学習されたすべての **sticky** およびスタティック アドレスは、アクセス ポートのアクセス VLAN で学習されたアドレスに変換されます。ネイティブ VLAN 以外の VLAN で学習されたすべてのアドレスは削除されます。



(注) ポートセキュリティでは、IEEE 802.1Q トランクおよび ISL (スイッチ間リンク) トランク双方に対し、**switchport trunk native vlan** コマンドで設定した VLAN ID が使用されます。

- Release 12.2(18)SXE より前のリリースでは、トランクはポートセキュリティでサポートされません。
- Release 12.2(18)SXE 以降のリリースでは、ポートセキュリティでは IEEE 802.1Q トンネルポートがサポートされます。
- Release 12.2(18)SXE より前のリリースでは、IEEE 802.1Q トンネルポートはポートセキュリティでサポートされません。
- ポートセキュリティでは、Switched Port Analyzer (SPAN; スイッチドポートアナライザ) 宛先ポートはサポートされません。
- ポートセキュリティでは、EtherChannel のポートチャネルインターフェイスはサポートされません。
- ポートセキュリティ、および 802.1X ポートベースの認証は、同一ポート上には設定できません。
  - セキュアポートで 802.1X ポートベース認証をイネーブルにしようとする、エラーメッセージが表示され、このポートで 802.1X ポートベース認証はイネーブルになりません。
  - 802.1X ポートベース認証用に設定したポートでポートセキュリティをイネーブルにしようとする、エラーメッセージが表示され、このポートでポートセキュリティはイネーブルになりません。

## ポートセキュリティの設定

ここでは、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。

- ポートセキュリティのイネーブル化 (p.48-6)
- ポートでのポートセキュリティ違反モードの設定 (p.48-8)
- ポートセキュリティのレートリミッタの設定 (p.48-9)
- セキュア MAC アドレスの最大数をポートに設定 (p.48-10)
- sticky MAC アドレスによるポートセキュリティのポートでのイネーブル化 (p.48-11)
- スタティックセキュア MAC アドレスのポートでの設定 (p.48-12)
- ポートでのセキュア MAC アドレスのエージング設定 (p.48-13)

### ポートセキュリティのイネーブル化

ここでは、ポートセキュリティをイネーブル化する手順について説明します。

- トランクでのポートセキュリティのイネーブル化 (p.48-6)
- アクセスポートでのポートセキュリティのイネーブル化 (p.48-7)

### トランクでのポートセキュリティのイネーブル化

Release 12.2(18)SXE 以降のリリースでは、ポートセキュリティでは非交渉トランクがサポートされません。



#### 注意

セキュア アドレス数はデフォルトで 1 であり、違反に対するデフォルト アクションはポートのシャットダウンであるため、トランクでポートセキュリティをイネーブルにする前に、このポートのセキュア MAC アドレスの最大数を設定します(「[セキュア MAC アドレスの最大数をポートに設定](#)」[p.48-10] を参照)。

トランクでポートセキュリティをイネーブルにするには、次の作業を行います。

	コマンド	目的
ステップ 1	Router(config)# <b>interface</b> type <sup>1</sup> slot/port	設定する LAN ポートを選択します。
ステップ 2	Router(config-if)# <b>switchport</b>	ポートをレイヤ 2 スイッチポートとして設定します。
ステップ 3	Router(config-if)# <b>switchport trunk encapsulation</b> {isl   dot1q}	カプセル化を設定して、レイヤ 2 スイッチングポートを ISL または 802.1Q トランクとして設定します。
ステップ 4	Router(config-if)# <b>switchport mode trunk</b>	無条件にポートをトランクに設定します。
ステップ 5	Router(config-if)# <b>switchport nonegotiate</b>	DTP を使用しないようにトランクを設定します。
ステップ 6	Router(config-if)# <b>switchport port-security</b>  Router(config-if)# <b>no switchport port-security</b>	トランクでポートセキュリティをイネーブルにします。  トランクでポートセキュリティをディセーブルにします。
ステップ 7	Router(config-if)# <b>do show port-security interface</b> type <sup>1</sup> slot/port   <b>include Port Security</b>	設定を確認します。



1. type = ethernet、fastethernet、gigabitethernet、または tengigabitethernet

次の例は、ポート FastEthernet 5/36 を非交渉トランクとして設定し、ポートセキュリティをイネーブルにする方法を示します。

```
Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# interface fastethernet 5/36
Router(config-if)# switchport
Router(config-if)# switchport mode trunk
Router(config-if)# switchport nonegotiate
Router(config-if)# switchport port-security
Router(config-if)# do show port-security interface fastethernet 5/36 | include Port
Security
Port Security                : Enabled
```

## アクセスポートでのポートセキュリティのイネーブル化

アクセスポートでポートセキュリティをイネーブルにするには、次の作業を行います。

	コマンド	目的
ステップ 1	Router(config)# <b>interface</b> type <sup>1</sup> slot/port	設定する LAN ポートを選択します。  (注) Release 12.2(18)SXE 以降のリリースでは、ポートをトンネル ポートまたは PVLAN ポートとして使用できます。
ステップ 2	Router(config-if)# <b>switchport</b>	ポートをレイヤ 2 スイッチポートとして設定します。
ステップ 3	Router(config-if)# <b>switchport mode access</b>	ポートをレイヤ 2 アクセスポートとして設定します。  (注) デフォルトモード (dynamic desirable) のポートは、セキュアポートとして設定できません。
ステップ 4	Router(config-if)# <b>switchport port-security</b>  Router(config-if)# <b>no switchport port-security</b>	ポートのポートセキュリティをイネーブルにします。  ポートのポートセキュリティをディセーブルにします。
ステップ 5	Router(config-if)# <b>do show port-security interface</b> type <sup>1</sup> slot/port   <b>include Port Security</b>	設定を確認します。

1. type = ethernet、fastethernet、gigabitethernet、または tengigabitethernet

次に、ポート FastEthernet 5/12 でポートセキュリティをイネーブルにする例を示します。

```
Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# interface fastethernet 5/12
Router(config-if)# switchport
Router(config-if)# switchport mode access
Router(config-if)# switchport port-security
Router(config-if)# do show port-security interface fastethernet 5/12 | include Port
Security
Port Security                : Enabled
```

## ポートでのポートセキュリティ違反モードの設定

ポートでポートセキュリティの違反モードを設定するには、次の作業を行います。

	コマンド	目的
ステップ 1	Router(config)# <b>interface</b> type <sup>1</sup> slot/port	設定する LAN ポートを選択します。
ステップ 2	Router(config-if)# <b>switchport port-security violation</b> {protect   restrict   shutdown}  Router(config-if)# <b>no switchport port-security violation</b>	(任意) 違反モード、およびセキュリティ違反が検出されたときのアクションを設定します。 デフォルト設定 ( <b>shutdown</b> ) に戻します。
ステップ 3	Router(config-if)# <b>do show port-security interface</b> type <sup>1</sup> slot/port   <b>include violation_mode</b> <sup>2</sup>	設定を確認します。

1. type = ethernet、fastethernet、gigabitethernet、または tengigabitethernet

2. violation\_mode = protect、restrict、または shutdown

ポートセキュリティの違反モードを設定する場合は、次の点に注意してください。

- **protect** — 最大値を下回るようにセキュア MAC アドレスを削除するまで、送信元アドレスが不明なパケットを廃棄します。
- **restrict** — 最大値を下回るようにセキュア MAC アドレスを削除するまで、送信元アドレスが不明なパケットを廃棄して、セキュリティ違反カウンタを増やします。
- **shutdown** — インターフェイスをただちに errdisable ステートにし、SNMP トラップ通知を送信します。



(注)

- errdisable ステートからセキュア ポートを回復するには、**errdisable recovery cause violation\_mode** グローバル コンフィギュレーション コマンドを入力します。または、**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 コマンドを入力して、手動でセキュア ポートを再びイネーブルに戻すことができます。
- CPU 使用率の過度な上昇を防止するため、**protect** または **restrict** 違反モードを設定する場合は、パケット廃棄レート リミッタを設定してください ([「ポートセキュリティのレート リミッタの設定」 \[p.48-9\]](#) を参照)。

次の例では、ポート FastEthernet 5/12 のセキュリティ違反モードを **protect** に設定します。

```
Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# interface fastethernet 3/12
Router(config-if)# switchport port-security violation protect
Router(config-if)# do show port-security interface fastethernet 5/12 | include Protect
Violation Mode                : Protect
```

次の例では、ポート FastEthernet 5/12 のセキュリティ違反モードを **restrict** に設定します。

```
Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# interface fastethernet 3/12
Router(config-if)# switchport port-security violation restrict
Router(config-if)# do show port-security interface fastethernet 5/12 | include Restrict
Violation Mode                : Restrict
```



## ポートセキュリティのレートリミッタの設定



(注)

- PFC2 はポートセキュリティレートリミッタをサポートしていません。
- truncated スイッチングモードでは、ポートセキュリティレートリミッタはサポートされません。

ポートセキュリティはセキュアポートで受信されたすべてのトラフィックを調べ、違反を検出し、新たなセキュア MAC アドレスを認識します。shutdown 違反モードを設定した場合は、違反が検出されたあとはトラフィックはセキュアポートに入力できません。この結果、違反によって CPU に過剰な負荷がかかることはありません。

protect または restrict 違反モードを設定した場合は、違反が発生したあともポートセキュリティによるトラフィック処理は続行され、その結果 CPU の負荷が高まる可能性があります。protect または restrict 違反モードを設定した場合は、過剰な負荷から CPU を保護するため、ポートセキュリティレートリミッタを設定してください。

ポートセキュリティレートリミッタを設定するには、次の作業を行います。

	コマンド	目的
ステップ 1	Router(config)# <b>mls rate-limit layer2 port-security rate_in_pps [burst_size]</b>	ポートセキュリティレートリミッタを設定します。
	Router(config)# <b>no mls rate-limit layer2 port-security</b>	デフォルト設定に戻します。
ステップ 2	Router(config)# <b>do show mls rate-limit   include PORTSEC</b>	設定を確認します。

ポートセキュリティレートリミッタを設定する場合は、次の点に注意してください。

- *rate\_in\_pps* 値に関する注意事項：
  - 有効値の範囲は 10 ~ 1,000,000 (1000000 と入力) です。
  - デフォルト値はありません。
  - 設定値が低いほど、CPU の保護が強化されます。レートリミッタは、セキュリティ違反の発生前と発生後の両方でトラフィックに適用されます。正規のトラフィックがポートセキュリティ機能に到達できるように、適度な高さの値を設定するようにしてください。
  - 1,000 (1000 と入力) 未満の値は、十分な保護を提供できます。
- *burst\_size* 値に関する注意事項：
  - 有効値の範囲は 1 ~ 255 です。
  - デフォルト値は 10 です。
  - デフォルト値で、十分な保護を提供できます。

次に、ポートセキュリティレートリミッタを設定する例を示します。


```
Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# mls rate-limit layer2 port-security 1000
Router(config)# end
```

次に、設定を確認する例を示します。

```
Router# show mls rate-limit | include PORTSEC
LAYER_2 PORTSEC On 1000 1 Not sharing
```

## セキュア MAC アドレスの最大数をポートに設定

セキュア MAC アドレスの最大数をポートに設定するには、次の作業を行います。

	コマンド	目的
ステップ 1	Router(config)# <b>interface</b> type <sup>1</sup> slot/port	設定する LAN ポートを選択します。
ステップ 2	Router(config-if)# <b>switchport port-security maximum number_of_addresses vlan {vlan_ID   vlan_range}</b>	ポートに対し、セキュア MAC アドレスの最大数を設定します (デフォルトは 1)。
		 <b>(注)</b> VLAN ごとの設定は、トランクのみでサポートされます。
	Router(config-if)# <b>no switchport port-security maximum</b>	デフォルト設定に戻します。
ステップ 3	Router(config-if)# <b>do show port-security interface type<sup>1</sup> slot/port   include Maximum</b>	設定を確認します。

1. type = ethernet、fastethernet、gigabitethernet、または tengigabitethernet

セキュア MAC アドレスの最大数をポートに設定する場合は、次の点に注意してください。

- Release 12.2(18)SXE 以降のリリースでは、*number\_of\_addresses* の有効範囲は 1 ~ 4,097 です。
- Release 12.2(18)SXE より前のリリースでは、*number\_of\_addresses* の有効範囲は 1 ~ 1,024 です。
- Release 12.2(18)SXE 以降のリリースでは、ポートセキュリティではトランクがサポートされません。
  - トランクでは、トランクおよびトランク上のすべての VLAN に対し、セキュア MAC アドレスの最大数を設定できます。
  - セキュア MAC アドレスの最大数は、1 つの VLAN、または 特定の VLAN 範囲に対して設定できます。
  - 特定の VLAN 範囲を指定するには、一組の VLAN 番号をダッシュ (-) でつなげて指定します。
  - 複数の VLAN 番号をカンマで区切って入力することも、複数組の VLAN 番号をダッシュでつなげて入力することもできます。

次の例では、ポート FastEthernet 5/12 に対し、セキュア MAC アドレスの最大数を 64 に設定します。

```
Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# interface fastethernet 3/12
Router(config-if)# switchport port-security maximum 64
Router(config-if)# do show port-security interface fastethernet 5/12 | include Maximum
Maximum MAC Addresses      : 64
```

## sticky MAC アドレスによるポートセキュリティのポートでのイネーブル化

Release 12.2(18)SXE 以降のリリースでは、sticky MAC アドレスによるポートセキュリティがサポートされます。sticky MAC アドレスによるポートセキュリティをポートでイネーブルにするには、次の作業を行います。

	コマンド	目的
ステップ 1	Router(config)# <b>interface</b> type <sup>1</sup> slot/port	設定する LAN ポートを選択します。
ステップ 2	Router(config-if)# <b>switchport port-security mac-address sticky</b>	sticky MAC アドレスによるポートセキュリティをポートでイネーブルにします。
	Router(config-if)# <b>no switchport port-security mac-address sticky</b>	sticky MAC アドレスによるポートセキュリティをポートでディセーブルにします。

1. type = ethernet、fastethernet、gigabitethernet、または tengigabitethernet

sticky MAC アドレスによるポートセキュリティをイネーブルにする場合は、次の点に注意してください。

- **switchport port-security mac-address sticky** コマンドを入力すると、次のようになります。
  - ポートでダイナミックに学習されたすべてのセキュア MAC アドレスは、sticky セキュア MAC アドレスに変換されます。
  - スタティックなセキュア MAC アドレスは、sticky MAC アドレスに変換されません。
  - 音声 VLAN でダイナミックに学習されたセキュア MAC アドレスは、sticky MAC アドレスに変換されません。
  - ダイナミックに学習された新規のセキュア MAC アドレスは、sticky アドレスとなります。
- **no switchport port-security mac-address sticky** コマンドを入力すると、ポート上のすべての sticky セキュア MAC アドレスは、ダイナミックなセキュア MAC アドレスに変換されます。
- sticky MAC アドレスがダイナミックに学習されたあとに、このアドレスを保存して、ブートアップまたはリロード後にポートに設定されるようにするには、**write memory** または **copy running-config startup-config** コマンドを入力して、アドレスを startup-config ファイルに保存する必要があります。

次の例は、sticky MAC アドレスによるポートセキュリティをポート FastEthernet 5/12 でイネーブルにします。

```
Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# interface fastethernet 5/12
Router(config-if)# switchport port-security mac-address sticky
```

## スタティックセキュア MAC アドレスのポートでの設定

スタティックセキュア MAC アドレスをポートに設定するには、次の作業を行います。

	コマンド	目的
ステップ 1	Router(config)# <b>interface</b> type <sup>1</sup> slot/port	設定する LAN ポートを選択します。
ステップ 2	Router(config-if)# <b>switchport port-security mac-address</b> [sticky] mac_address [vlan vlan_ID]	ポートに対し、スタティック MAC アドレスをセキュアアドレスとして設定します。
	Router(config-if)# <b>no switchport port-security mac-address</b> [sticky] mac_address	ポートからスタティックセキュア MAC アドレスを消去します。
ステップ 3	Router(config-if)# <b>end</b>	コンフィギュレーションモードを終了します。
ステップ 4	Router# <b>show port-security address</b>	設定を確認します。

1. type = ethernet、fastethernet、gigabithernet、または tengigabithernet

スタティックセキュア MAC アドレスをポートに設定する場合は、次の点に注意してください。

- Release 12.2(18)SXE 以降のリリースでは、sticky MAC アドレスによるポートセキュリティをイネーブルにしている場合に、sticky セキュア MAC アドレスを設定できます（「sticky MAC アドレスによるポートセキュリティのポートでのイネーブル化」 [p.48-11] を参照）。
- **switchport port-security maximum** コマンドでポートに設定するセキュア MAC アドレスの最大数により、設定可能なセキュア MAC アドレスの数が定義されます。
- 最大数より少ないセキュア MAC アドレスを設定すると、残りの MAC アドレスはダイナミックに学習されます。
- Release 12.2(18)SXE 以降のリリースでは、トランクでポートセキュリティがサポートされません。
  - トランクでは、VLAN 内でスタティックセキュア MAC アドレスを設定できます。
  - トランクでは、スタティックセキュア MAC アドレスに対応するように VLAN を設定していない場合、このアドレスは **switchport trunk native vlan** コマンドで設定した VLAN でセキュアとなります。

次に、ポート FastEthernet 5/12 で MAC アドレス 1000.2000.3000 をセキュアアドレスとして設定し、その設定を確認する例を示します。

```
Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# interface fastethernet 5/12
Router(config-if)# switchport port-security mac-address 1000.2000.3000
Router(config-if)# end
Router# show port-security address
      Secure Mac Address Table
```

```
-----
Vlan    Mac Address      Type                Ports
----    -
1       1000.2000.3000  SecureConfigured   Fa5/12
```

## ポートでのセキュア MAC アドレスのエージング設定

**absolute** キーワードを使用してエージング タイプを設定すると、ダイナミックに学習されるすべてのセキュアアドレスは、エージング タイムを過ぎると期限切れとなります。**inactivity** キーワードを使用してエージング タイプを設定すると、エージング タイムは、ダイナミックに学習されたすべてのセキュアアドレスが期限切れとなるまでの非アクティブ期間として定義されます。



(注) スタティック セキュア MAC アドレスおよび sticky セキュア MAC アドレスは、期限切れとなりません。

ここでは、ポートでセキュア MAC アドレスのエージングを設定する方法について説明します。

- [ポートでのセキュア MAC アドレスのエージング タイプの設定 \(p.48-13\)](#)
- [ポートでのセキュア MAC アドレスのエージング タイムの設定 \(p.48-14\)](#)

## ポートでのセキュア MAC アドレスのエージング タイプの設定

PFC3 および Release 12.2(18)SXE 以降のリリースでは、セキュア MAC アドレスのエージング タイプをポートに設定できます。PFC2 では、セキュア MAC アドレスのエージング タイプは設定できません。PFC2 は、absolute エージングのみをサポートしています。

セキュア MAC アドレスのエージング タイプをポートに設定するには、次の作業を行います。

	コマンド	目的
ステップ 1	Router(config)# <b>interface</b> type <sup>1</sup> slot/port	設定する LAN ポートを選択します。
ステップ 2	Router(config-if)# <b>switchport port-security aging type {absolute   inactivity}</b>  Router(config-if)# <b>no switchport port-security aging type</b>	セキュア MAC アドレスのエージング タイプをポートに設定します (デフォルトは absolute)。  デフォルトの MAC アドレス エージング タイプに戻します。
ステップ 3	Router(config-if)# <b>do show port-security interface</b> type <sup>1</sup> slot/port   <b>include Time</b>	設定を確認します。

1. type = ethernet、fastethernet、gigabithernet、または tengigabithernet

次に、ポート FastEthernet 5/12 のエージング タイプを inactivity に設定する例を示します。

```
Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# interface fastethernet 5/12
Router(config-if)# switchport port-security aging type inactivity
Router(config-if)# do show port-security interface fastethernet 5/12 | include Type
Aging Type                : Inactivity
```

## ポートでのセキュア MAC アドレスのエージング タイムの設定

セキュア MAC アドレスのエージング タイムをポートに設定するには、次の作業を行います。

	コマンド	目的
ステップ 1	Router(config)# <b>interface</b> <i>type</i> <sup>1</sup> <i>slot/port</i>	設定する LAN ポートを選択します。
ステップ 2	Router(config-if)# <b>switchport port-security aging time</b> <i>aging_time</i>  Router(config-if)# <b>no switchport port-security aging time</b>	セキュア MAC アドレスのエージング タイムをポートに設定します。 <i>aging_time</i> の有効範囲は 1 ~ 1440 分です (デフォルトは 0)。  セキュア MAC アドレスのエージング タイムをディセーブルにします。
ステップ 3	Router(config-if)# <b>do show port-security interface</b> <i>type</i> <sup>1</sup> <i>slot/port</i>   <b>include Time</b>	設定を確認します。

1. *type* = ethernet、fastethernet、gigabitethernet、または tengigabitethernet

次の例では、ポート FastEthernet 5/1 に対し、セキュア MAC アドレスのエージング タイムを 2 時間 (120 分) に設定します。

```
Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# interface fastethernet 5/1
Router(config-if)# switchport port-security aging time 120
Router(config-if)# do show port-security interface fastethernet 5/12 | include Time
Aging Time                : 120 mins
```

## ポートセキュリティ設定の表示

ポートセキュリティ設定を表示するには、次のコマンドを入力します。

コマンド	目的
Router# <b>show port-security</b> [interface {{vlan vlan_ID}   {type <sup>1</sup> slot/port}}] [address]	スイッチまたは指定のインターフェイスに対するポートセキュリティ設定を表示します。

1. *type* = ethernet、fastethernet、gigabitethernet、または tengigabitethernet

ポートセキュリティ設定を表示する場合は、次の点に注意してください。

- ポートセキュリティでは、**vlan** キーワードはトランクのみでサポートされます。
- **address** キーワードを使用してセキュア MAC アドレスを表示すると、各アドレスのエージング情報（スイッチに対するグローバル情報、またはインターフェイスごとの情報）が表示されます。
- 次の値が表示されます。
  - 各インターフェイスで許可されるセキュア MAC アドレスの最大数
  - インターフェイスに設定されたセキュア 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

次に、インターフェイスを入力しない場合の **show port-security** コマンドの出力例を示します。

```
Router# show port-security
Secure Port      MaxSecureAddr  CurrentAddr  SecurityViolation  Security
Action
                (Count)          (Count)      (Count)
-----
Fa5/1            11              11           0                  Shutdown
Fa5/5            15              5            0                  Restrict
Fa5/11           5               4            0                  Protect
-----

Total Addresses in System: 21
Max Addresses limit in System: 128
```

次に、特定のインターフェイスに対する **show port-security** コマンドの出力例を示します。

```
Router# show port-security interface fastethernet 5/1
Port Security: Enabled
Port status: SecureUp
Violation mode: Shutdown
Maximum MAC Addresses: 11
Total MAC Addresses: 11
Configured MAC Addresses: 3
Aging time: 20 mins
Aging type: Inactivity
SecureStatic address aging: Enabled
Security Violation count: 0
```

## ■ ポートセキュリティ設定の表示

次に、**show port-security address** イネーブル EXEC コマンドの出力例を示します。

```
Router# show port-security address
      Secure Mac Address Table
-----
Vlan    Mac Address          Type                Ports    Remaining Age
        -----          -
        (mins)
-----
  1     0001.0001.0001      SecureDynamic       Fa5/1    15 (I)
  1     0001.0001.0002      SecureDynamic       Fa5/1    15 (I)
  1     0001.0001.1111      SecureConfigured    Fa5/1    16 (I)
  1     0001.0001.1112      SecureConfigured    Fa5/1    -
  1     0001.0001.1113      SecureConfigured    Fa5/1    -
  1     0005.0005.0001      SecureConfigured    Fa5/5    23
  1     0005.0005.0002      SecureConfigured    Fa5/5    23
  1     0005.0005.0003      SecureConfigured    Fa5/5    23
  1     0011.0011.0001      SecureConfigured    Fa5/11   25 (I)
  1     0011.0011.0002      SecureConfigured    Fa5/11   25 (I)
-----
Total Addresses in System: 10
Max Addresses limit in System: 128
```