CHAPTER 56

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『Cisco IOS Master Command List, Release 12.2SX』を参照してください。

http://www.cisco.com/en/US/docs/ios/mcl/122sxmcl/12_2sx_mcl_book.html

ヒント Cisco Catalyst 6500 シリーズ スイッチの詳細（設定例およびトラブルシューティング情報を含む）については、次のページに示されるドキュメントを参照してください。

http://www.cisco.com/en/US/products/hw/switches/ps708/tsd_products_support_series_home.html

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

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メディア アクセス制御（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 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す。

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 内の別のセキュア ポートにアクセスしようとすると、設定された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.56-7）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。

ポートの違反モードとして、protect、restrict、または shutdown のいずれかを設定できます。「ポート セキュリティの設定」（P.56-5）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

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。

IP Phone でのポート セキュリティ

装置が IP Phone のデータ ポートを介してスイッチに接続した場合の使用例を図 56-1 に示します。

図 56-1　IP Phone を介して接続した装置

装置はスイッチに直接接続されていないため、スイッチでは、装置の接続が切断されている場合に、ポート リンクが失われていることを物理的に検出できません。最近の Cisco IP Phone は、Cisco Discovery Protocol（CDP; シスコ検出プロトコル）でホストの存在を示す Type Length Value（TLV）を送信して、接続されている装置のポートのリンク ステートの変更をスイッチに通知します。Cisco IOS Release 12.2(33)SXI 以降のリリースでは、スイッチはホストの存在を示す TLV を認識します。IP Phone のデータ ポートでのリンク ダウンを知らせる、ホストの存在を示す TLV 通知を受け取るとすぐに、ポート セキュリティでは、スタティック MAC アドレス、sticky MAC アドレス、ダイナミックに学習された MAC アドレスがすべてアドレス テーブルから削除されます。削除されたアドレスは、ダイナミックに学習されるかまたは設定された場合に限り、再び追加されます。

ポート セキュリティのデフォルト設定

表 56-1 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 56-1　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、Simple Network Management Protocol（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。

- ポート セキュリティがデフォルト設定の場合に、errdisable ステートからすべてのセキュア ポートを回復させるには、**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。
- 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、『Cisco IOS Master Command List, 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ドロップされます。**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。
- ポート セキュリティはプライベート VLAN（PVLAN）ポートです。
- ポート セキュリティは IEEE 802.1Q トンネル ポートをサポートします。
- 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。
- Cisco IOS Release 12.2(33)SXH 以降のリリースでは、同一ポート上でポート セキュリティと 802.1X ポート ベース認証を設定できます。Cisco IOS Release 12.2(33)SXH 以前のリリースの場合は次のようになります。
  - 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と、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と、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 セキュリティは、非交渉トランクをサポートしています。
  - 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だけをサポートします。

    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 またはスタティック 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 Inter Switch Link（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。

- 隣接スイッチ間で実行されている冗長リンクがある場合は、これらのスイッチに接続されているポートでポート セキュリティをイネーブルにする際に注意が必要です。これは、ポート セキュリティ違反が原因でポート セキュリティによってポートが errdisable に設定されるためです。

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

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

ポート セキュリティは、非交渉トランクをサポートしています。

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.56-9）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)# **interface** *type*[1] *slot/port*	設定する LAN ポートを選択します。
ステップ 2	Router(config-if)# **switchport**	ポートをレイヤ 2 ポートとして設定します。
ステップ 3	Router(config-if)# **switchport trunk encapsulation** {**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)# **switchport mode trunk**	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)# **switchport nonegotiate**	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)# **switchport port-security**	トランクでポート セキュリティをイネーブルにします。
ステップ 7	Router(config-if)# **do show port-security interface** *type*[1] *slot/port* | **include Port Security**	設定を確認します。

1. *type* = **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)# **interface** *type*[1] *slot/port*	設定する LAN ポートを選択します。 **（注）** ポートはトンネル ポートまたは PVLAN ポートのいずれかが可能です。
ステップ 2	Router(config-if)# **switchport**	ポートをレイヤ 2 ポートとして設定します。
ステップ 3	Router(config-if)# **switchport mode access**	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)# **switchport port-security**	ポートのポート セキュリティをイネーブルにします。
ステップ 5	Router(config-if)# **do show port-security interface** *type*[1] *slot/port* | **include Port Security**	設定を確認します。

1. *type* = **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)# interface` *type*[1] *slot/port*	設定する LAN ポートを選択します。
ステップ 2	`Router(config-if)# switchport port-security violation {protect | restrict | shutdown}`	（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。
ステップ 3	`Router(config-if)# do show port-security interface` *type*[1] *slot/port* `| include` *violation_mode*[2]	設定を確認します。

1. *type* = **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ドロップします。
- **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ドロップして、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 ドロップ 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.56-8）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）　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がありません。

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)# mls rate-limit layer2 port-security` *rate_in_pps* [*burst_size*]	ポート セキュリティ レート リミッタを設定します。
ステップ 2	`Router(config)# do show mls rate-limit | include PORTSEC`	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)# interface` *type*[1] *slot/port*	設定する LAN ポートを選択します。
ステップ 2	`Router(config-if)# switchport port-security maximum` *number_of_addresses* `vlan` {*vlan_ID* | *vlan_range*}	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）。 （注）　VLAN ごとの設定は、トランクだけでサポートされます。
ステップ 3	`Router(config-if)# do show port-security interface` *type*[1] *slot/port* `| include Maximum`	設定を確認します。

1. *type* = **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。

- *number_of_addresses* の範囲は 1 ～ 4,097 です。
- ポート セキュリティは、トランクをサポートしています。
  - 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、複数組の 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、一組の 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

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)# interface type[1] slot/port`	設定する LAN ポートを選択します。
ステップ 2	`Router(config-if)# switchport port-security mac-address sticky`	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。

1. *type* = **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)# interface type[1] slot/port`	設定する LAN ポートを選択します。
ステップ 2	`Router(config-if)# switchport port-security mac-address [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。 **（注）** VLAN ごとの設定は、トランクだけでサポートされます。

	コマンド	目的
ステップ 3	`Router(config-if)# end`	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# show port-security address`	設定を確認します。

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

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。

- 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.56-10）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。
- ポート セキュリティがトランクでサポートされています。
  - 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.56-12）
- 「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.56-12）

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

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できます。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)# **interface** *type*[1] *slot/port*	設定する LAN ポートを選択します。
ステップ 2	Router(config-if)# **switchport port-security aging type** {**absolute** | **inactivity**}	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）。
ステップ 3	Router(config-if)# **do show port-security interface** *type*[1] *slot/port* | **include Time**	設定を確認します。

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

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)# **interface** *type*[1] *slot/port*	設定する LAN ポートを選択します。
ステップ 2	Router(config-if)# **switchport port-security aging time** *aging_time*	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。*aging_time* の有効範囲は 1 ～ 1440 分です（デフォルトは 0）。
ステップ 3	Router(config-if)# **do show port-security interface** *type*[1] *slot/port* | **include Time**	設定を確認します。

1. *type* = **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# **show port-security** [**interface** {{**vlan** *vlan_ID*} | {*type*[1] *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* = **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だけ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
```

次に、**show port-security address** 特権 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
```

ヒント　Cisco Catalyst 6500 シリーズ スイッチの詳細（設定例およびトラブルシューティング情報を含む）については、次のページに示されるドキュメントを参照してください。
http://www.cisco.com/en/US/products/hw/switches/ps708/tsd_products_support_series_home.html

ヒント