CHAPTER 26

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。Release 12.1(13)E 以降のリリースで、ポート セキュリティ機能がサポートされます。

（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、『*Cisco 7600 Series Router Cisco IOS Command Reference*』を参照してください。

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

ポート セキュリティ機能を使用すると、ポートへのアクセスが許可されたワークステーションの MAC アドレスを制限および識別することによって、インターフェイスへの入力を制限できます。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パケットを転送しません。セキュア MAC アドレスの数を 1 に制限して 1 つのセキュア MAC アドレスを割り当てると、そのポートに接続されたワークステーションは、ポートの全帯域幅が保証されます。

ポートをセキュア ポートとして設定してセキュア MAC アドレスが最大数に達した場合に、ポートにアクセスしようとするワークステーションの MAC アドレスが、識別されたセキュア MAC アドレスのいずれとも異なるときは、セキュリティ違反が発生します。また、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 アドレスを持つワークステーションが別のセキュア ポートにアクセスしようとすると、違反のフラグが立てられます。

ポート上でセキュア MAC アドレスの最大数を設定すると、セキュア アドレスが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。

- **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 コマンドを使用すると、すべてのセキュア MAC アドレスを設定できます。
- 接続されたデバイスの MAC アドレスを使用すると、ポートはダイナミックにセキュア MAC アドレスを設定できます。
- アドレスをいくつか設定して、残りのアドレスはダイナミックに設定されるようにできます。

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

セキュア MAC アドレスの最大数を設定すると、そのアドレスはアドレス テーブルに保管されます。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。

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、そのアドレス テーブルに MAC アドレスがないワークステーションが、インターフェイスにアクセスしようとした場合、セキュリティ違反が発生します。

インターフェイスを 3 つの違反モード（protect、restrict、または shutdown）のいずれかに設定できます（「ポート セキュリティの設定」[p.26-4] を参照）。

ポート セキュリティのデフォルト設定

表 26-1 に、インターフェイスに対するポート セキュリティのデフォルト設定を示します。

表 26-1　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	ポート上でディセーブル
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 アドレスの最大数を超えるとポートはシャットダウンし、SNMP 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際は、次の注意事項に従ってください。

- セキュア ポートはトランク ポートにできません。
- セキュア ポートは、Switched Port Analyzer（SPAN; スイッチド ポート アナライザ）の宛先ポートにはできません。
- セキュア ポートは、EtherChannel のポートチャネル インターフェイスに属することができません。
- セキュア ポートは 802.1x ポートにできません。セキュア ポート上で 802.1x 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、802.1x はイネーブルになりません。802.1x 対応ポートをセキュア ポートに変更しようとすると、エラー メッセージが表示され、セキュリティ設定が変更されません。

ポート セキュリティの設定

ここでは、ポート セキュリティの設定手順について説明します。

インターフェイスでのポート セキュリティの設定

ポートへのアクセスが許可されたステーションの MAC アドレスを制限および識別して、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。

	コマンド	目的
ステップ 1	`Router(config)# interface interface_id`	インターフェイス コンフィギュレーション モードを開始して、設定する物理インターフェイスを入力します（例：**gigabitethernet 3/1**）。
ステップ 2	`Router(config-if)# switchport mode access`	インターフェイス モードを access に設定します。デフォルト モード（dynamic desirable）のインターフェイスは、セキュア ポートとして設定できません。
ステップ 3	`Router(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。
ステップ 4	`Router(config-if)# switchport port-security maximum value`	（任意）インターフェイスに対してセキュア MAC アドレスの最大数を設定します。設定できる範囲は 1 ～ 128 です。デフォルトでは、128 に設定されています。
ステップ 5	`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検出時の対処方法を設定します。
ステップ 6	`Router(config-if)# switchport port-security mac-address mac_address`	（任意）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してセキュア MAC アドレスの最大数を入力できます。最大値より少ない数のセキュア 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。
ステップ 7	`Router(config-if)# end`	特権 EXEC モードに戻ります。
ステップ 8	`Router# show port-security interface interface_id` `Router# show port-security address`	設定を確認します。

ポート セキュリティを設定する場合は、ポート セキュリティ違反モードに関する次の構文情報に注意してください。

- **ptotect —** セキュア MAC アドレスが削除されて最大数を下回る数になるまで、送信元アドレスが不明なパケットをドロップします。
- **restrict —** セキュア MAC アドレスが削除されて最大数を下回る数になるまで、送信元アドレスが不明なパケットをドロップし、Security Violation カウンタを増加させます。
- **shutdown —** インターフェイスはただちに errdisable ステートとなり、SNMP トラップ通知が送信されます。

（注） ポート セキュリティがイネーブルになっており、あるセキュア インターフェイスで学習または設定されたアドレスが、同一 VLAN 内の別のセキュア インターフェイスで受信された場合、このインターフェイスはただちに errdisable ステートとなります。

セキュア ポートを errdisable ステートから回復するには、**errdisable recovery cause** *psecure_violation* グローバル コンフィギュレーション コマンドを使用します。または、**shutdown** および **no shutdown** 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、手動でポートを再びイネーブルに戻すこともできます。

インターフェイスをデフォルト状態（非セキュア ポート）に戻すには、**no switchport port-security** インターフェイス コンフィギュレーション コマンドを使用します。

インターフェイスをデフォルトのセキュア MAC アドレス数に戻すには、**no switchport port-security maximum** *value* コマンドを使用します。

アドレス テーブルから MAC アドレスを削除するには、**no switchport port-security mac-address** *mac_address* コマンドを使用します。

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** {**protocol** | **restrict**} コマンドを使用します。

次に、ポート FastEthernet 12 でポート セキュリティをイネーブルにし、セキュア アドレスの最大数を 5 に設定する例を示します。違反モードはデフォルト設定で、セキュア MAC アドレスは設定されていません。

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# interface fastethernet 3/12
Router(config-if)# switchport mode access
Router(config-if)# switchport port-security
Router(config-if)# switchport port-security maximum 5
Router(config-if)# end
Router# show port-security interface fastethernet 3/12
Security Enabled:Yes, Port Status:SecureUp
Violation Mode:Shutdown
Max. Addrs:5, Current Addrs:0, Configure Addrs:0
```

次に、ポート FastEthernet 12 でセキュア MAC アドレスを設定し、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 mode access
Router(config-if)# switchport port-security
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 セキュリティ エージングの設定

ポート セキュリティ エージングを使用すると、ポート上のすべてのセキュア アドレスにエージング タイムを設定できます。

この機能を使用すると、既存のセキュア MAC アドレスを手動で削除しなくてもセキュア ポート上の PC を削除および追加でき、しかもポートのセキュア アドレスの数を制限することができます。

ポート セキュリティ エージングを設定する手順は、次のとおりです。

	コマンド	目的
ステップ 1	`Router(config)# interface interface_id`	ポート セキュリティ エージングをイネーブルにするポートで、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 2	`Router(config-if)# switchport port-security aging time aging_time`	このセキュア ポートに対して、エージング タイムを設定します。 *time* には、このポートのエージング タイムを指定します。セキュア アドレスはすべて、指定した時間（分単位）が経過すると期限切れになり、セキュア アドレス リストから削除されます。
	`Router(config-if)# no switchport port-security aging time`	エージングをディセーブルにします。
ステップ 3	`Router(config-if)# end`	特権 EXEC モードに戻ります。
ステップ 4	`Router# show port security [interface interface_id] [address]`	設定を確認します。

ポート セキュリティ エージングを設定する際、次の点に注意してください。

- すべてのリリースで、**no** キーワードを使用してエージングをディセーブルにすることができます。
- Release 12.1(19)E 以降のリリースでは、エージング タイムは 1 ～ 1440 分の範囲で設定できます。
- Release 12.1(19)E より前のリリースでは、エージング タイムは 0 ～ 1440 分の範囲で設定できます。0 を入力すると、エージングがディセーブルになります。

次に、インターフェイス FastEthernet 5/1 でセキュア アドレスのエージング タイムを 2 時間に設定する例を示します。

```
Router(config)# interface fastethernet 5/1
Router(config-if)# switchport port-security aging time 120
```

次に、エージング タイムを 2 分に設定する例を示します。

```
Router(config-if)# switchport port-security aging time 2
```

すでに設定したコマンドを確認するには、**show port-security interface** *interface_id* 特権 EXEC コマンドを入力します。

ポート セキュリティ設定の表示

show interfaces *interface_id* **switchport** 特権 EXEC コマンドを使用すると、インターフェイスのトラフィック抑制および制御の設定が表示されます。**show interfaces counters** 特権 EXEC コマンドを使用すると、廃棄されたパケット数が表示されます。**show storm control** および **show port-security** 特権 EXEC コマンドを使用すると、これらの機能が表示されます。

トラフィック制御情報を表示するには、次に示す 1 つまたは複数のコマンドを入力します。

コマンド	目的
Router# **show port-security** [**interface** *interface_id*]	インターフェイスごとのセキュア MAC アドレスの最大許容数、インターフェイスのセキュア MAC アドレス数、発生したセキュリティ違反数、違反モードなど、スイッチまたは指定したインターフェイスのポートのセキュリティ設定を表示します。
Router# **show port-security** [**interface** *interface_id*] **address**	スイッチのすべてのインターフェイスまたは指定したインターフェイスに設定されたすべてのセキュア MAC アドレスと、各アドレスのエージング情報を表示します。

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、指定された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** 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
```