CHAPTER 35

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

この章の構成は次のとおりです。

- ポート セキュリティの概要（p.35-2）
- デフォルトのポート セキュリティ設定（p.35-3）
- 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.35-3）
- ポート セキュリティの設定（p.35-4）
- ポート セキュリティ設定の表示（p.35-7）

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して、ポートへのアクセスを許可されているワークステーションの MAC（メディア アクセス制御）アドレスを制限し、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することができます。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のグループ外に送信元アドレスがあるパケットを転送しません。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ワークステーションはそのポートの全帯域の使用を保証されます。

ポートがセキュア ポートとして設定され、セキュア MAC アドレスが最大数に達した場合、ポートへのアクセスを試みるワークステーションの MAC アドレスが指定されたセキュア MAC アドレスのいずれとも異なると、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 ポートにアクセスを試みると、違反のフラグが立てられます。

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設定できます。
- 接続されている装置の MAC アドレスで、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することができます。
- アドレス数をいくつか設定し、残りのアドレスがダイナミックに設定されるようにすることができます。

（注）　ポートがシャットダウンすると、ダイナミックに学習され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 テーブルに保存されます。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。

セキュア MAC アドレスの最大数がアドレス 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を試みる場合、セキュリティ違反が発生します。

protect、restrict、または shutdown の違反モードのいずれかにインターフェイスを設定できます（「ポート セキュリティの設定」[p.35-4] を参照）。

デフォルトのポート セキュリティ設定

表 35-1 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 35-1　デフォルトのポート セキュリティ設定

機能	デフォルトの設定
ポート セキュリティ	ポートで、ディセーブルに設定されています。
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際は、次の注意事項に従ってください。

- セキュア ポートは PVLAN（プライベート VLAN）に置くことはできません。
- セキュア ポートはトランク ポートにはなれません。
- 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）用の宛先ポートにはなれません。
- セキュア ポートは、EtherChannel ポート チャネル インターフェイスに属することはできません。
- 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しても、エラー メッセージが表示され、セキュリティ設定は変更されません。

ポート セキュリティの設定

ここでは、ポート セキュリティを設定する手順について説明します。

- インターフェイス上でのポート セキュリティの設定（p.35-4）
- ポート セキュリティ エージングの設定（p.35-5）

インターフェイス上でのポート 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手順は、次のとおりです。

	コマンド	説明
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、設定する物理インターフェイス、たとえば、**gigabitethernet 3/1** を入力します。
ステップ 2	`Router(config-if)# switchport mode access`	インターフェイス モードをアクセスとして設定します。デフォルト モード（dynamic desirable）のインターフェイスはセキュア ポートとしては設定できません。
ステップ 3	`Router(config-if)# switchport port-security`	インターフェイス上のポート 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最大数のセキュア MAC アドレスを設定します。指定できる範囲は 1 ～ 128 です。デフォルトは 128 です。
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が検出されたときの対応方法を設定します。
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。最大数より少ない 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`	イネーブル 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`	入力を確認します。

ポート セキュリティを設定する場合、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。

- **protect** — 十分な数のセキュア MAC アドレスを削除して MAC アドレス数が最大値を下回るまで、送信元アドレスが不明なパケットを廃棄します。
- **restrict** — 十分な数のセキュア MAC アドレスを削除して MAC アドレス数が最大値を下回るまで、送信元アドレスが不明なパケットを廃棄し、SecurityViolation カウンタを増分させます。
- **shutdown** — インターフェイスをただちに errordisable ステートにして、SNMP トラップ通知を送信します。

（注）　ポート セキュリティがイネーブルのときに、セキュア インターフェイス上で学習または設定されたアドレスが、同じ VLAN（仮想 LAN）内の別のセキュア インターフェイス上で検出された場合、ポート セキュリティはそのインターフェイスをただちに errdisable ステートにします。

errdisable ステートからセキュア ポートを回復するには、**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。

インターフェイスを、デフォルト（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の状態（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 3/12 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。違反モードがデフォルト設定で、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 5/12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 エージングを使用して、ポート上の全セキュア アドレスのエージング タイムを設定できます。

この機能を使用すると、ポート上のセキュア アドレスの数を制限しながら、一方で既存のセキュア 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 を削除したり追加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	説明
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に対して、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`	セキュア ポートにエージング 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。エージング タイムの有効な範囲は 1 ～ 1440 分です。指定した時間（分）が経過した直後に、すべてのセキュア アドレスが期限切れになり、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`	イネーブル EXEC モードに戻ります。
ステップ 4	`Router# show port security [interface interface_id] [address]`	入力を確認します。

次に、インターフェイス FastEthernet 5/1 のセキュア 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
```

show port-security interface *interface_id* イネーブル EXEC コマンドを入力して、前に設定したコマンドを確認することができます。

ポート セキュリティ設定の表示

show interfaces *interface_id* **switchport** イネーブル EXEC コマンドを使用すると、インターフェイストラフィックの抑制と制御の設定が表示されます。**show interfaces counters** イネーブル 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** イネーブル 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	説明
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、ルータ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**	ルータのすべてのポートまたは指定したポート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表示します。

```
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** 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
```