



## ネットワーク セキュリティの設定

---

この章では、Cisco 7600 シリーズ ルータ固有のネットワーク セキュリティ機能について説明します。これは、次のマニュアルに記載されているネットワーク セキュリティに関する情報および手順を補足するためのものです。

- 次の URL の『*Cisco IOS Security Configuration Guide*』 Release 12.2  
[http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fsecur\\_c/index.htm](http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fsecur_c/index.htm)
- 次の URL の『*Cisco IOS Security Command Reference*』 Release 12.2  
[http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fsecur\\_r/index.htm](http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fsecur_r/index.htm)

この章の構成は次のとおりです。

- MAC アドレスベースのトラフィック ブロッキングの設定 (p.27-2)
- TCP インターセプトの設定 (p.27-2)
- ユニキャスト RPF チェックの設定 (p.27-3)

## MAC アドレスベースのトラフィック ブロッキングの設定

特定の VLAN（仮想 LAN）内の MAC（メディア アクセス制御）アドレスを経由するすべてのトラフィックをブロックするには、次の作業を行います。

コマンド	説明
Router(config)# <b>mac-address-table static mac_address vlan vlan_ID drop</b>	特定の VLAN で設定されている MAC アドレスを経由するすべてのトラフィックをブロックします。
Router(config)# <b>no mac-address-table static mac_address vlan vlan_ID</b>	MAC アドレスベースのブロッキングを消去します。

次に、VLAN 12 内で MAC アドレス 0050.3e8d.6400 を経由するすべてのトラフィックをブロックする例を示します。

```
Router# configure terminal
Router(config)# mac-address-table static 0050.3e8d.6400 vlan 12 drop
```

## TCP インターセプトの設定

TCP インターセプト フローはハードウェアで処理されます。

設定手順については、下記の URL にある『Cisco IOS Security Configuration Guide』 Release 12.2 の「Traffic Filtering and Firewalls」、「Configuring TCP Intercept (Preventing Denial-of-Service Attacks)」を参照してください。

[http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fsecur\\_c/fracfwl/scfdenl.htm](http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fsecur_c/fracfwl/scfdenl.htm)

## ユニキャスト RPF チェックの設定

ここでは、Cisco IOS ユニキャスト Reverse Path Forwarding (RPF) チェック (ユニキャスト RPF チェック) について説明します。

- [PFC3 ユニキャスト RPF チェックのサポートの概要 \(p.27-3\)](#)
- [ユニキャスト RPF チェックの設定 \(p.27-4\)](#)

### PFC3 ユニキャスト RPF チェックのサポートの概要

ユニキャスト RPF チェック機能概要の詳細については、次の URL にある『Cisco IOS Security Configuration Guide』Release 12.2 の「Other Security Features」、「Configuring Unicast Reverse Path Forwarding」を参照してください。

[http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fsecur\\_c/fothersf/scfrpf.htm](http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fsecur_c/fothersf/scfrpf.htm)

Policy Feature Card3 (PFC3; ポリシー フィーチャ カード 3) は、複数のインターフェイスからのトラフィックの RPF チェックをハードウェアでサポートします。

strict 方式ユニキャスト RPF チェックの場合、PFC3 はルーティング テーブルのプレフィクスすべてに対し 2 つの平行パスと、4 つのユーザ設定変更可能な RPF インターフェイス グループ (インターフェイス グループごとに 4 つのインターフェイスを収容可能) のいずれかを通じて到達したプレフィクスに対し最大 4 つの平行パスをサポートします。

loose 方式ユニキャスト RPF チェック (別名 exist-only 方式) の場合、PFC3 は最大 8 つのリバースパス インターフェイスをサポートします (Cisco IOS ソフトウェアはルーティング テーブルでは 8 つのリバースパスに制限されます)。

Cisco IOS でユニキャスト RPF チェックを実行する方式は、次の 4 つです。

- strict ユニキャスト RPF チェック
- allow-default を使用した strict ユニキャスト RPF チェック
- loose ユニキャスト RPF チェック
- allow-default を使用した loose ユニキャスト RPF チェック

ユニキャスト RPF チェックをインターフェイス単位で設定できますが、ユニキャスト RPF チェックがイネーブルであるインターフェイスすべてに対して PFC3 がサポートするのは、ユニキャスト RPF 方式のみです。現在設定されている方式とは異なるユニキャスト RPF 方式を使用するようにインターフェイスを設定する場合、ユニキャスト RPF チェックがイネーブルになっているシステムのインターフェイスすべてが、新しい方式を使用します。

### PFC2 ユニキャスト RPF チェックのサポートの概要

PFC2 は、1 つのリターンパスを持つパケットをハードウェアで処理することによってユニキャスト RPF をサポートしています。Multilayer Switch Feature Card 2 (MSFC2; マルチレイヤ スイッチ フィーチャ カード 2) は、複数のリターンパスを持つトラフィックをソフトウェアで処理します (負荷分散など)。

PFC2 の場合、Access Control List (ACL; アクセス制御リスト) を使用してフィルタ処理するようにユニキャスト RPF を設定する場合、PFC2 はトラフィックが ACL と一致するかどうかを判断します。PFC2 は、RPF ACL に拒否されたトラフィックを MSFC2 へ送信してユニキャスト RPF チェックを受けます。

## ユニキャスト RPF チェックに関する注意事項および制約事項

- ユニキャスト RPF チェックを設定し、Access Control List (ACL; アクセス制御リスト) でフィルタをかける場合、PFC はトラフィックが ACL と一致するかどうかを判断します。PFC は RPF ACL に拒否されたトラフィックを Multilayer Switch Feature Card (MSFC; マルチレイヤ スイッチ フィーチャ カード) へ送信し、MSFC がユニキャスト RPF チェックを行います。PFC2 または PFC3A の場合、ACL で許可されたパケットは、ユニキャスト RPF チェックを受けずにハードウェアで転送されます。PFC3BXL を使用する場合、ACL で許可されたパケットは MSFC3 上で RPF チェックされます。
- 通常、DoS 攻撃のパケットは拒否 Access Control Entry (ACE; アクセス制御エントリ) と一致し、ユニキャスト RPF チェックを受けるため MSFC に送信されます。そのため、送信されたパケットで MSFC は過負荷状態になる可能性があります。
- PFC は、ユニキャスト RPF チェックの ACL とは一致しなくても、入力セキュリティ ACL と一致するトラフィックをハードウェアでサポートします。
- PFC では、Policy-Based Routing (PBR; ポリシーベース ルーティング) トラフィックのユニキャスト RPF チェックをハードウェアでサポートしません (CSCea53554)。

## ユニキャスト RPF チェックの設定

ここでは、ユニキャスト RPF チェックの設定手順について説明します。

- [ユニキャスト RPF チェック モードの設定 \(p.27-4\)](#)
- [PFC3 での複数パスのユニキャスト RPF チェック モードの設定 \(p.27-6\)](#)
- [self-ping のイネーブル化 \(p.27-7\)](#)

## ユニキャスト RPF チェック モードの設定


ユニキャスト RPF には、次に示す 2 つのチェック モードがあります。

- strict チェック モード — 送信元 IP アドレスが Forwarding Information Base (FIB; 転送情報ベース) テーブルにあること、および入力ポートから到達可能な範囲内にあることを確認します。
- exist-only チェック モード — 送信元 IP アドレスが FIB テーブルにあるかどうかだけを確認します。



(注) ユニキャスト RPF チェック用に設定されたすべてのポートには、その時点で設定されているモードが自動的に適用されます。

ユニキャスト RPF チェック モードを設定するには、次の作業を行います。

	コマンド	説明
ステップ 1	Router(config)# <b>interface</b> {{vlan vlan_ID}   {type <sup>1</sup> slot/port}   {port-channel number}}	設定するインターフェイスを選択します。   (注) ユニキャスト RPF チェックは次の宛先にパケットを転送する前に、入力ポートに基づいて、最適なリターンパスを確認します。
ステップ 2	Router(config-if)# <b>ip verify unicast source reachable-via</b> {rx   any} [allow-default] [list] Router(config-if)# <b>no ip verify unicast</b>	ユニキャスト RPF チェック モードを設定します。  デフォルトのユニキャスト RPF チェック モードに戻します。

	コマンド	説明
ステップ 3	Router(config-if)# <b>exit</b>	インターフェイス 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 mls cef ip rpf</b>	設定を確認します。

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

ユニキャスト RPF チェック モードを設定する際、次の構文情報に注意してください。

- strict チェック モードをイネーブルにするには、**rx** キーワードを使用します。
- exist-only チェック モードをイネーブルにするには、**any** キーワードを使用します。
- RPF の確認にデフォルト ルートを使用できるようにするには、**allow-default** キーワードを使用します。
- アクセス リストを識別するには、*list* オプションを使用します。
  - アクセス リストによってネットワークへのアクセスが拒否された場合は、スプーフィングされたパケットがポートで廃棄されます。
  - アクセス リストによってネットワークへのアクセスが許可された場合は、スプーフィングされたパケットが宛先アドレスに転送されます。転送されたパケットは、インターフェイスの統計情報にカウントされます。
  - アクセス リストにログアクションが含まれている場合、スプーフィングされたパケットに関する情報がログ サーバに送信されます。



(注) **ip verify unicast source reachable-via** コマンドを入力すると、ユニキャスト RPF チェック モードがルータのすべてのポートで変更されます。

次に、ポート GigabitEthernet 4/1 でユニキャスト RPF の exist-only チェック モードをイネーブルにする例を示します。

```
Router(config)# interface gigabitethernet 4/1
Router(config-if)# ip verify unicast source reachable-via any
Router(config-if)# end
Router#
```

次に、ポート GigabitEthernet 4/2 でユニキャスト RPF の strict チェック モードをイネーブルにする例を示します。

```
Router(config)# interface gigabitethernet 4/2
Router(config-if)# ip verify unicast source reachable-via rx
Router(config-if)# end
Router#
```

次に、設定を確認する例を示します。

```
Router# show running-config interface gigabitethernet 4/2
Building configuration...
Current configuration : 114 bytes
!
interface GigabitEthernet4/2
ip address 42.0.0.1 255.0.0.0
ip verify unicast reverse-path
no cdp enable
end
Router# show running-config interface gigabitethernet 4/1
Building configuration...
Current configuration : 114 bytes
!
interface GigabitEthernet4/1
ip address 41.0.0.1 255.0.0.0
→ ip verify unicast reverse-path (RPF mode on g4/1 also changed to strict-check RPF
mode)
no cdp enable
end
Router#
```

### PFC3 での複数パスのユニキャスト RPF チェック モードの設定

PFC3 で複数パスのユニキャスト RPF チェック モードを設定するには、次の作業を行います。

	コマンド	説明
ステップ 1	Router(config)# <b>mls ip cef rpf mpath {punt   pass   interface-group}</b>  Router(config)# <b>no mls ip cef rpf mpath {punt   interface-group}</b>	PFC3 で複数のパス RPF チェック モードを設定します。  デフォルト値に戻します ( <b>mls ip cef rpf mpath punt</b> )。
ステップ 2	Router(config)# <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 3	Router# <b>show mls cef ip rpf</b>	設定を確認します。

複数のパス RPF チェックを設定する場合、次の構文情報に注意してください。

- **punt** (デフォルト) — プレフィクスごとに最大 2 つのインターフェイスに対して、PFC3 はユニキャスト RPF チェックをハードウェアで実行します。追加のインターフェイスに着信するパケットは MSFC3 にリダイレクト (パント) されて、ソフトウェアでユニキャスト RPF チェックが実行されます。
- **pass** — パスが 1 つまたは 2 つのプレフィクスの場合、PFC3 はユニキャスト RPF チェックをハードウェアで実行します。ユニキャスト RPF チェックは、3 つ以上のリバースパス インターフェイスのある **multipath** プレフィクスから着信するパケットに対し、ディセーブルです (このパケットは常にユニキャスト RPF チェックに合格します)。
- **interface-group** — パスが 1 つまたは 2 つのプレフィクスの場合、PFC3 はユニキャスト RPF チェックをハードウェアで実行します。PFC3 はプレフィクス単位で最大 4 つの追加インターフェイスに対し、ユーザ設定変更可能なマルチパス ユーザ RPF チェック インターフェイスグループを介して、ユニキャスト RPF チェックを実行します。ユニキャスト RPF チェックは、3 つ以上のリバースパス インターフェイスのある他の **multipath** プレフィクスから着信するパケットに対し、ディセーブルです (このパケットは常にユニキャスト RPF チェックが行われず)。

次に、複数パスの RPF チェックを設定する例を示します。

```
Router(config)# mls ip cef rpf mpath punt
```

## PFC3 での複数パスのインターフェイス グループの設定

複数パスのユニキャスト RPF インターフェイス グループを PFC3 に設定するには、次の作業を行います。

	コマンド	説明
ステップ 1	<code>Router(config)# mls ip cef rpf interface-group [0   1   2   3] interface1 [interface2 [interface3 [interface4]]]</code>	複数パスの RPF インターフェイス グループを PFC3 に設定します。
ステップ 2	<code>Router(config)# mls ip cef rpf interface-group group_number</code>	インターフェイス グループを削除します。
ステップ 3	<code>Router(config)# end</code>	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	<code>Router# show mls cef ip rpf</code>	設定を確認します。

次に、インターフェイス グループ 2 を設定する例を示します。

```
Router(config)# mls ip cef rpf interface-group 2 fastethernet 3/3 fastethernet 3/4
fastethernet 3/5 fastethernet 3/6
```

## self-ping のイネーブル化

ユニキャスト RPF チェックがイネーブルの場合、ルータはデフォルトで self-ping を実行できません。

self-ping をイネーブルにするには、次の作業を行います。

	コマンド	説明
ステップ 1	<code>Router(config)# interface {{vlan vlan_ID}   {type<sup>1</sup> slot/port}   {port-channel number}}</code>	設定するインターフェイスを選択します。
ステップ 2	<code>Router(config-if)# ip verify unicast source reachable-via any allow-self-ping</code>  <code>Router(config-if)# no ip verify unicast source reachable-via any allow-self-ping</code>	self-ping またはセカンダリ アドレスへの ping を実行できるように、ルータをイネーブルにします。 self-ping をディセーブルにします。
ステップ 3	<code>Router(config-if)# exit</code>	インターフェイス コンフィギュレーション モードを終了します。

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

次に、self-ping をイネーブルにする例を示します。

```
Router(config)# interface gigabithernet 4/1
Router(config-if)# ip verify unicast source reachable-via any allow-self-ping
Router(config-if)# end
```

