CHAPTER 23

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 セキュリティ情報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の補足になります。

- 次の URL の『*Cisco IOS Security Configuration Guide*』Release 12.1
  http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121cgcr/secur_c/index.htm
- 次の URL の『*Cisco IOS Security Command Reference*』Release 12.1
  http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121cgcr/secur_r/index.htm

この章で説明する内容は、次のとおりです。

（注） Release 12.1(11b)E 以降のリリースを使用する場合、コンフィギュレーション モードで EXEC モードレベルのコマンドを入力するには、EXEC モードレベルのコマンドの前に **do** キーワードを入力します。

ACL 設定時の注意事項

Access Control List（ACL; アクセス コントロール リスト）の設定に関する注意事項は、次のとおりです。

- 各タイプの ACL（IP、IPX、および MAC）は、対応するトラフィック タイプだけをフィルタリングします。MAC ACL が IP または IPX トラフィックと一致することはありません。
- パケットがアクセス グループによって拒否された場合、デフォルトでは、MSFC は Internet Control Message Protocol（ICMP; インターネット制御メッセージ プロトコル）到達不能メッセージを送信します。

  ip unreachables コマンドがイネーブル（デフォルト）の場合、Supervisor Engine 2 は拒否されたパケットの大部分をハードウェアでドロップし、一部のパケット（最大で 1 秒当たり 10 パケット）のみを MSFC2 に送信して、そこでドロップします。これにより、ICMP 到達不能メッセージが生成されます。

  ip unreachables コマンドがイネーブルの場合、Supervisor Engine 1 は拒否されたパケットをすべて MSFC に送信して、そこでドロップします。これにより、ICMP 到達不能メッセージが生成されます。Supervisor Engine 1 を使用する場合、アクセス リストによって拒否されたパケットをハードウェアでドロップするには、**no ip unreachables** 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 ICMP 到達不能メッセージをディセーブルにする必要があります。

  拒否されたパケットをドロップし、ICMP 到達不能メッセージを生成することによって MSFC CPU にかかる負荷を軽減するには、次の作業を行います。

  - Supervisor Engine 1 の場合、**no ip unreachables** インターフェイス コンフィギュレーション コマンドを入力します。
  - Supervisor Engine 2 の場合、**no ip unreachables** および **no ip redirects** インターフェイス コンフィギュレーション コマンドを入力します（CSCdr33918）。
- パケットが VACL によって拒否された場合、ICMP 到達不能メッセージは送信されません。

ハードウェアおよびソフトウェア ACL のサポート

ACL は、Policy Feature Card（PFC; ポリシー フィーチャ カード、または PFC2）、Distributed Forwarding Card（DFC）のハードウェア、または Multilayer Switch Feature Card（MSFC; マルチレイヤ スイッチ フィーチャ カード、または MSFC2）のソフトウェアのいずれかで処理できます。次に、ソフトウェアおよびハードウェアによる ACL の取り扱いについて説明します。

- 標準 ACL および拡張 ACL（入力および出力）の [deny] ステートメントに一致する ACL フローは、[ip unreachables] がディセーブルに設定されている場合、ハードウェアによってドロップされます。
- 標準 ACL および拡張 ACL（入力および出力）の [permit] ステートメントに一致する ACL フローは、ハードウェアで処理されます。
- VACL フローはハードウェアで処理されます。VACL で指定されたフィールドがハードウェア処理でサポートされていない場合、このフィールドは無視されるか（ACL の **log** キーワードなど）、またはコンフィギュレーション全体が拒否されます（サポート対象外の IPX ACL パラメータを含む VACL など）。
- VACL ロギングはソフトウェアで処理されます。
- ダイナミック ACL フローはハードウェアで処理されます。ただし、アイドル タイムアウトはソフトウェアで処理されます。
- 特定のポートの ACL アクセス違反に関する IP アカウンティングは、そのポートで拒否された全パケットを MSFC に転送してソフトウェアで処理させることによってサポートされます。この動作は他のフローには影響しません。
- 名前ベースの拡張 MAC アドレス ACL は、ハードウェアでサポートされています。
- 次の ACL タイプは、ソフトウェアによって処理されます。
  - 標準 XNS アクセス リスト
  - 拡張 XNS アクセス リスト
  - DECnet アクセス リスト
  - Internetwork Packet Exchange（IPX）アクセス リスト
  - 拡張 MAC アドレス アクセス リスト
  - プロトコル タイプコード アクセス リスト

（注） ヘッダー長が 5 未満の IP パケットは、アクセス コントロールが行われません。

- ロギングを必要とするフローは、ソフトウェアによって処理されます。この動作は、ロギングを必要としないフローのハードウェア上での処理には影響しません。
- ソフトウェアで処理されるフローの転送レートは、ハードウェアで処理されるフローに比べると、大幅に小さくなります。
- **show ip access-list** コマンドの入力の際に表示されるマッチ カウントには、ハードウェアで処理されたパケットは含まれません。

ACL におけるレイヤ 4 演算子の使用上の注意事項および制約事項

ここでは、レイヤ 4 ポート演算を含む ACL を設定する場合の注意事項および制約事項について説明します。

レイヤ 4 演算の使用

次のタイプの演算子を指定できます。

- gt（geater than：より大きい）
- lt（less than：より小さい）
- neq（not equal：等しくない）
- eq（equal：等しい）
- range（inclusive range：包含範囲）

1 つの ACL に指定する演算は、*9* つまでにしてください。この数を超えると、新しい演算によって影響される ACE が、複数の ACE に分割されることがあります。

レイヤ 4 演算を使用する際は、次の 2 つの注意事項に従ってください。

- レイヤ 4 演算は、演算子またはオペランドが異なっていると、違う演算であるとみなされます。たとえば、次の ACL には 3 つの異なるレイヤ 4 演算が定義されています（[gt 10] と [gt 11] は 2 つの異なるレイヤ 4 演算とみなされます）。

```
... gt 10 permit
... lt 9 deny
... gt 11 deny
```

（注）　[eq] 演算子の使用に制限はありません。[eq] 演算子は Logical Operation Unit（LOU; 論理演算ユニット）またはレイヤ 4 演算ビットを使用しないためです。LOU については、「LOU の使用」（p.23-4）を参照してください。

- レイヤ 4 演算は、同じ演算子 / オペランドの組み合わせでも、送信元ポートに適用するか宛先ポートに適用するかによって異なる演算とみなされます。たとえば次の ACL では、1 つの ACE には送信元ポート、もう 1 つの ACE には宛先ポートが指定されているので、2 つの異なるレイヤ 4 演算が定義されていることになります。

```
... Src gt 10 ...
... Dst gt 10
```

LOU の使用

LOU は、演算子 / オペランドの組み合わせを保存するレジスタです。ACL はすべて、LOU を使用します。最大 32 の LOU があります。各 LOU には、2 つの異なる演算子 / オペランドの組み合わせを保存できますが、range 演算子だけは例外です。レイヤ 4 演算は、次のように LOU を使用します。

- gt は、1/2 LOU を使用します。
- lt は、1/2 LOU を使用します。
- neq は、1/2 LOU を使用します。
- range は、1 LOU を使用します。
- eq は、LOU を使用しません。

たとえば、次の ACL では、1 つの LOU に 2 つの異なる演算子 / オペランドの組み合わせが保存されます。

```
... Src gt 10 ...
... Dst gt 10
```

以下は、より詳細な例です。

```
ACL1
... (dst port) gt 10 permit
... (dst port) lt 9 deny
... (dst port) gt 11 deny
... (dst port) neq 6 permit
... (src port) neq 6 deny
... (dst port) gt 10 deny

ACL2
... (dst port) gt 20 deny
... (src port) lt 9 deny
... (src port) range 11 13 deny
... (dst port) neq 6 permit
```

レイヤ 4 演算数と LOU 数は、次のとおりです。

- ACL1 のレイヤ 4 演算：5
- ACL2 のレイヤ 4 演算：4
- LOU：4

LOU は、次のように使用されています。

- LOU 1 に、[gt 10] および [lt 9] が保存されます。
- LOU 2 に、[gt 11] および [neq 6] が保存されます。
- LOU 3 に、[gt 20] が保存されます（半分は空き）。
- LOU 4 に、[range 11 13] が保存されます（range は 1 LOU を使用）。

Cisco IOS のファイアウォール フィーチャ セットの設定

（注）　Release 12.1(11b)E 以降のリリースに、ファイアウォール フィーチャ セット イメージが含まれます。

ここでは、Cisco 7600 シリーズ ルータに Cisco IOS のファイアウォール フィーチャ セットを設定する手順について説明します。

Cisco IOS ファイアウォール フィーチャ セットのサポートの概要

ファイアウォール フィーチャ セット イメージは、次の Cisco IOS ファイアウォール機能をサポートしています。

- Context-Based Access Control（CBAC; コンテキスト ベース アクセス コントロール）
- Port-to-Application Mapping（PAM; ポートツーアプリケーション マッピング）
- 認証プロキシ

ファイアウォール フィーチャ セット イメージ名は、次のとおりです。

- c6sup22-jo3sv-mz
- c6sup22-po3sv-mz
- c6sup12-jo3sv-mz
- c6sup12-po3sv-mz

Cisco IOS ファイアウォール機能の詳細については、オンラインの『*Cisco IOS Security Configuration Guide*』Release 12.1 の「Traffic Filtering and Firewalls」を参照してください。

- 次の URL の「Cisco IOS Firewall Overview」
  http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121cgcr/secur_c/scprt3/scdfirwl.htm
- 次の URL の「Configuring Context-Based Access Control」
  http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121cgcr/secur_c/scprt3/scdcbac.htm
- 次の URL の「Configuring Authentication Proxy」
  http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121cgcr/secur_c/scprt3/scdauthp.htm
- 次の URL の『Cisco IOS Security Command Reference』
  http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121cgcr/secur_r/index.htm

Cisco IOS ファイアウォール イメージを使用するかどうかに関係なく、次のフィーチャ セットがサポートされます。

- 標準アクセス リストおよびスタティック拡張アクセス リスト
- Lock-and-Key（ダイナミック アクセス リスト）
- IP セッション フィルタリング（リフレクシブ アクセス リスト）
- TCP 代行受信
- セキュリティ サーバ サポート
- Network Address Translation（NAT; ネットワーク アドレス変換）
- 近接ルータ認証

- イベント ロギング
- ユーザ認証および許可

（注）　Cisco 7600 シリーズ ルータは、Intrusion Detection System Module（IDSM）（WS-X6381-IDS）をサポートしています。Cisco 7600 シリーズ ルータは、**ip audit** コマンドを使用して設定する Cisco IOS ファイアウォール IDS 機能はサポートしていません。

ファイアウォール設定時の注意事項および制約事項

Cisco IOS ファイアウォール機能を設定する際、次に示す注意事項および制約事項に注意してください。

制約事項

- 他のプラットフォームで、特定のポートに関して **ip inspect** コマンドを入力すると、検査されたトラフィックがネットワーク デバイスを通過できるように、他のポートの ACL が CBAC によって変更されます。他のポート経由のトラフィックを拒否する ACL で、トラフィックの通過を許可するには、Cisco 7600 シリーズ ルータ上で、**mls ip inspect** コマンドを入力する必要があります。「Cisco 7600 シリーズ ルータ 上での CBAC の設定」（p.23-8）を参照してください。
- Supervisor Engine 2 および PFC2 では、リフレクシブ ACL および CBAC のフロー マスクの要件が異なっています。Supervisor Engine 2 および PFC2 を搭載したスイッチ上で CBAC を設定すると、リフレクシブ ACL は MSFC2 のソフトウェアで処理されます。
- CBAC は VACL と互換性がありません。CBAC および VACL はスイッチ上に設定できますが、同じサブネット（VLAN）内または同じインターフェイス上には設定できません。

（注）　IDSM は、VACL を使用してトラフィックを選択します。CBAC が設定されているサブネット内で IDSM を使用するには、**mls ip ids** *acl_name* インターフェイス コマンドを入力します。*acl_name* は、IDSM のトラフィックを選択する場合に設定します。

注意事項

- Microsoft NetMeeting（2.0 以降）のトラフィックを検査するには、**h323** および **tcp** の両方の検査をオンにします。
- Web トラフィックを検査するには、**tcp** 検査をオンにします。パフォーマンスの低下を回避するには、Java をブロックするために **http** 検査をオンにしないでください。
- CBAC は、レイヤ 3 インターフェイスとして設定された物理ポート、および VLAN インターフェイスに設定できます。
- QoS および CBAC は相互に作用したり、干渉したりしません。

Cisco 7600 シリーズ ルータ 上での CBAC の設定

Cisco 7600 シリーズ ルータに、CBAC の追加設定を行う必要があります。Cisco 7600 シリーズ ルータ以外のネットワーク デバイス上でポートがトラフィックを拒否するように **ip inspect** コマンドで設定されている場合は、CBAC はトラフィックをポート経由で双方向に送信できるようにします。これと同じ状況は、トラフィックが通過する必要がある他のポートにも当てはまります（次の例を参照）。

```
Router(config)# ip inspect name permit_ftp ftp
Router(config)# interface vlan 100
Router(config-if)# ip inspect permit_ftp in
Router(config-if)# ip access-group deny_ftp_a in
Router(config-if)# ip access-group deny_ftp_b out
Router(config-if)# exit
Router(config)# interface vlan 200
Router(config-if)# ip access-group deny_ftp_c in
Router(config-if)# ip access-group deny_ftp_d out
Router(config-if)# exit
Router(config)# interface vlan 300
Router(config-if)# ip access-group deny_ftp_e in
Router(config-if)# ip access-group deny_ftp_f out
Router(config-if)# end
```

FTP セッションを VLAN 100 で開始し、VLAN 200 で終了しなければならない場合、CBAC を使用すると、ACL の deny_ftp_a、deny_ftp_b、deny_ftp_c、および deny_ftp_d によって FTP トラフィックが許可されます。別の FTP セッションを VLAN 100 で開始し、VLAN 300 で終了しなければならない場合は、ACL の deny_ftp_a、deny_ftp_b、deny_ftp_e、および deny_ftp_f によって FTP トラフィックが許可されます。

Cisco 7600 シリーズ ルータのポートがトラフィックを拒否するように設定されている場合、CBAC を使用すると、**ip inspect** コマンドで設定されたポートを経由してのみトラフィックを双方向に送信できます。他のポートは、**mls ip inspect** コマンドを使用して設定する必要があります。

FTP セッションを VLAN 100 で開始し、VLAN 200 で終了しなければならない場合、Cisco 7600 シリーズ ルータ上の CBAC によって、FTP トラフィックは ACL の deny_ftp_a および deny_ftp_b だけを通過することが許可されます。ACL deny_ftp_c および deny_ftp_d をトラフィックが通過できるようにするには、次の例のように、**mls ip inspect deny_ftp_c** および **mls ip inspect deny_ftp_d** コマンドを入力する必要があります。

```
Router(config)# mls ip inspect deny_ftp_c
Router(config)# mls ip inspect deny_ftp_d
```

この設定例では、VLAN 300 で FTP トラフィックを終了するには、**mls ip inspect deny_ftp_e** および **mls ip inspect deny_ftp_f** コマンドを入力する必要があります。設定を確認するには、**show fm insp** [**detail**] コマンドを入力します。

show fm insp [**detail**] コマンドを実行すると、ACL のリスト、CBAC が設定されているポート、およびステータス（**ACTIVE** または **INACTIVE**）が表示されます（次の例を参照）。

```
Router# show fm insp
         interface:Vlan305(in) status :ACTIVE
         acl name:deny
           interfaces:
              Vlan305(out):status ACTIVE
```

VLAN 305 では、着信方向の検査がアクティブで、ACL は設定されていません。VLAN 305 では、ACL **deny** が発信方向に適用されていて、検査がアクティブです。

すべてのフロー情報を表示するには、**detail** キーワードを使用します。

CBAC を設定する前に VACL がポートに設定されている場合は、表示されるステータスは INACTIVE です。それ以外の場合のステータスは ACTIVE です。PFC リソースがなくなっている場合にこのコマンドを実行すると、[BRIDGE] と表示され、そのあとに、処理のために MSFC2 に送信されている NetFlow 要求のうち、失敗した現在アクティブな NetFlow 要求の数が表示されます。

MAC アドレスベースのトラフィック ブロッキングの設定

12.1(13)E 以降のリリースで、特定の VLAN 上の MAC アドレスを経由するトラフィックをすべてブロックするには、次の作業を行います。

コマンド	目的
`Router(config)# mac-address-table static` *mac_address* `vlan` *vlan_ID* `drop`	指定された VLAN 内の設定された 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)# no mac-address-table static` *mac_address* `vlan` *vlan_ID*	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 内の 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
```

VLAN ACL の設定

（注）　Releases 12.1(11b)E 以降のリリースで VACL がサポートされます。

ここでは VACL について説明します。

VACL

ここでは VACL について説明します。

VACL の概要

VACL は、VLAN 内でブリッジングされるパケット、VLAN または（Release 12.1(13)E 以降の場合）VACL キャプチャ用の WAN インターフェイス内外にルーティングされるすべてのパケットについて、アクセスを制御できます。ルータ インターフェイスでのみ設定され、ルーテッド パケットにのみ適用される通常の Cisco IOS 標準 ACL または拡張 ACL と異なり、VACL はすべてのパケットに適用され、どの VLAN または WAN インターフェイスにも適用できます。VACL はハードウェアで処理されます。VACL は Cisco IOS ACL を使用します。VACL は、ハードウェアでサポートされない Cisco IOS ACL フィールドについてはすべて無視します。

VACL は、IP、IPX、および MAC レイヤ トラフィックに対して設定できます。WAN インターフェイスに適用される VACL は、VACL キャプチャ用の IP トラフィックだけをサポートします。

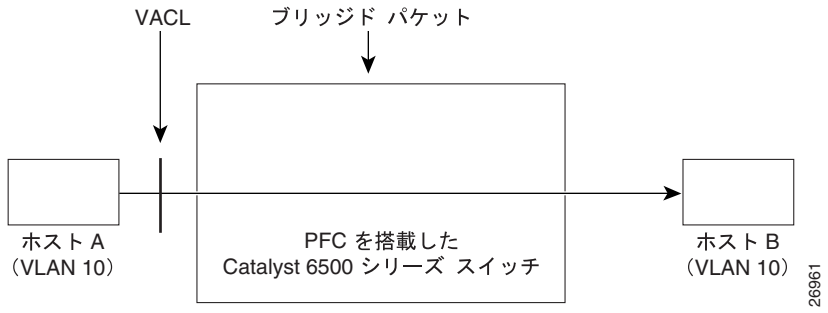
VACL を設定して VLAN に適用すると、VLAN に着信するすべてのパケットが、この VACL と照合されます。VACL を VLAN に適用し、ACL を VLAN 内のルーテッド インターフェイスに適用すると、VLAN に着信するパケットは最初に VACL と照合されます。そこで許可されると、次に入力 ACL と照合され、それからルーテッド インターフェイスで処理されます。別の VLAN にルーティングされるパケットは、最初に、ルーテッド インターフェイスに適用される出力 ACL と照合されます。そこで許可されると、宛先 VLAN 用に設定された VACL が適用されます。VACL が特定のパケット タイプ用に設定されていて、VACL と該当タイプのパケットとが一致しない場合、デフォルト動作では、パケットが拒否されます。

（注）
- VACL および CBAC は、同じインターフェイス上には設定できません。
- VACL と同じインターフェイスに設定されている場合、TCP 代行受信およびリフレクシブ ACL は、VACL よりも優先されます。
- IGMP パケットは VACL と照合されません。

ブリッジド パケット

図 23-1 に、ブリッジド パケットに適用される VACL を示します。

図 23-1　ブリッジド パケットへの VACL の適用

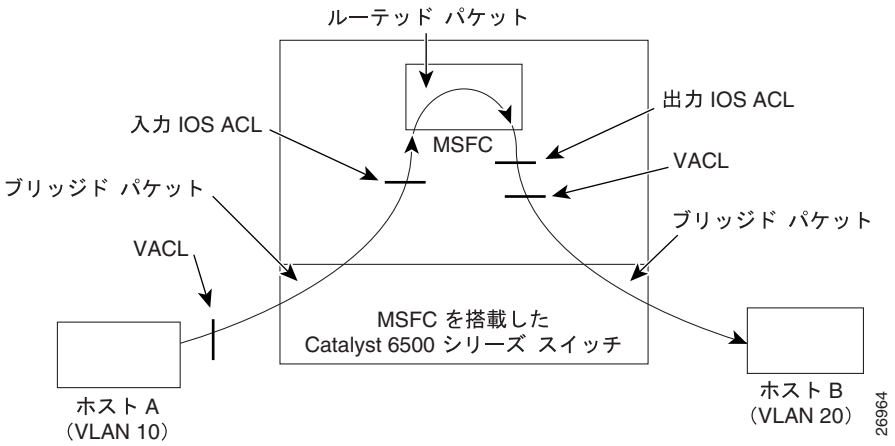


ルーテッド パケット

図 23-2 に、ルーテッド パケットおよびレイヤ 3 スイッチド パケットに ACL を適用する方法を示します。ルーテッド パケットおよびレイヤ 3 スイッチド パケットに対して、ACL は次の順番で適用されます。

1. 入力 VLAN 用 VACL
2. 入力 Cisco IOS ACL
3. 出力 Cisco IOS ACL
4. 出力 VLAN 用 VACL

図 23-2　ルーテッド パケットへの VACL の適用

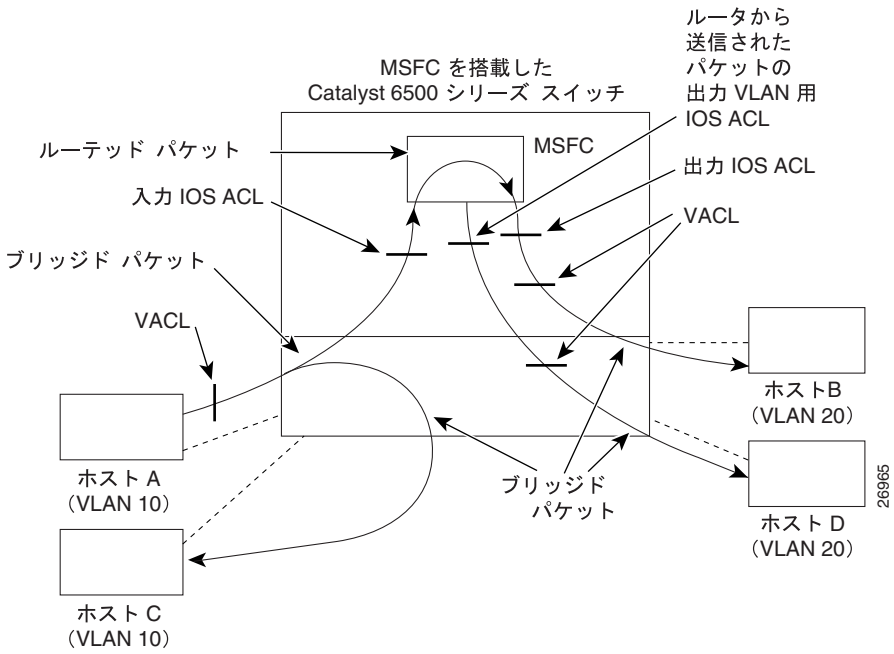


マルチキャスト パケット

図 23-3 に、マルチキャスト拡張が必要なパケットに ACL を適用する方法を示します。マルチキャスト拡張が必要なパケットに対して、ACL は次の順番で適用されます。

1. マルチキャスト拡張が必要なパケット
   a. 入力 VLAN 用 VACL
   b. 入力 Cisco IOS ACL
2. マルチキャスト拡張後のパケット
   a. 出力 Cisco IOS ACL
   b. 出力 VLAN 用 VACL（PFC2 によるサポート対象外）
3. ルータから送信されるパケット — 出力 VLAN 用 VACL

図 23-3　マルチキャスト パケットへの VACL の適用



VACL の設定

ここでは VACL の設定について説明します。

VACL の設定の概要

VACL は標準および拡張 Cisco IOS IP および IPX ACL、および MAC レイヤの名前付き ACL（「MAC レイヤ名前付きアクセス リストの設定（任意）」（p.32-40）を参照）、さらに VLAN アクセス マップを使用します。

VLAN アクセス マップは、VLAN または（Release 12.1(13)E 以降の場合）VACL キャプチャ用の WAN インターフェイスに対して適用できます。WAN インターフェイスに適用する VACL は、VACL キャプチャ用の標準および拡張 Cisco IOS IP ACL だけをサポートします。

各 VLAN アクセス マップは、1 つまたは複数のマップ シーケンスで構成できます。各シーケンスには match コマンドと action コマンドが含まれます。match コマンドはトラフィック フィルタリング用の IP、IPX、または MAC ACL を指定します。action コマンドは一致した場合に実行するアクションを指定します。フローが許可 ACL エントリと一致した場合、関連づけられたアクションが実行され、それ以降の残りのシーケンスに対してフローはチェックされません。フローが拒否 ACL エントリと一致した場合、同じシーケンス内の次の ACL、または次のシーケンスに対してフローがチェックされます。フローがどの ACL エントリとも一致せず、1 つまたは複数の ACL がそのパケット タイプ用に設定されている場合、パケットは拒否されます。

ブリッジド トラフィックおよびルーテッド トラフィックの両方にアクセス コントロールを使用するには、VACL を単独で使用するか、または VACL と ACL を組み合わせて使用します。入力と出力の両方のルーテッド トラフィックに対してアクセス コントロールを使用するには、VLAN インターフェイス上で ACL を定義します。ブリッジド トラフィックに対してアクセス コントロールを使用するには、VACL を定義します。

VACL と共に ACL を使用する場合は、次の点に注意してください。

- 発信 ACL にログオンする必要があるパケットは、VACL で拒否された場合、ログオンしません。
- VACL は NAT 変換前のパケットに適用されます。アクセス コントロールの対象でない変換フローは、VACL コンフィギュレーションにより、変換後にアクセス コントロールの対象となる場合があります。

VACL 内の action コマンドは、forward（転送）、drop（ドロップ）、capture（キャプチャ）、または redirect（リダイレクト）です。トラフィックのロギングもできます。WAN インターフェイスに適用された VACL は、リダイレクトまたはログ アクションをサポートしません。

（注）　VACL のマップの最後には、暗黙的な拒否エントリがあります。パケットがどの ACL エントリとも一致せず、そのパケット タイプ用に設定されている ACL が最低でも 1 つある場合、パケットは拒否されます。

（注）　空または未定義の ACL が VACL 内で指定されている場合、すべてのパケットはこの ACL に一致し、関連づけられたアクションが実行されます。

VLAN アクセス マップの定義

VLAN アクセス マップを定義するには、次の作業を行います。

コマンド	目的
`Router(config)# vlan access-map map_name [0-65535]`	VLAN アクセス マップを定義します。任意で、VLAN アクセス マップのシーケンス番号を指定できます。
`Router(config)# no vlan access-map map_name 0-65535`	VLAN アクセス マップからマップ シーケンスを削除します。
`Router(config)# no vlan access-map map_name`	VLAN アクセス マップを削除します。

VLAN アクセス マップを定義する際、構文について次の点に注意してください。

- エントリを追加または変更する場合は、マップのシーケンス番号を指定します。
- マップのシーケンス番号を指定しない場合、番号が自動的に割り当てられます。
- 各マップ シーケンスには、match コマンドおよび action コマンドをそれぞれ 1 つのみ指定できます。
- マップ シーケンスを削除する場合は、シーケンス番号を指定して **no** キーワードを使用します。
- マップを削除する場合は、シーケンス番号を指定しないで、**no** キーワードを使用します。

「VLAN アクセス マップの設定および確認の例」（p.23-17）を参照してください。

VLAN アクセス マップ シーケンスでの match コマンドの設定

VLAN アクセス マップ シーケンスに match コマンドを設定するには、次の作業を行います。

コマンド	目的
`Router(config-access-map)# match {ip address {1-199 | 1300-2699 | acl_name} | ipx address {800-999 | acl_name}| mac address acl_name}`	VLAN アクセス マップ シーケンスに match コマンドを設定します。
`Router(config-access-map)# no match {ip address {1-199 | 1300-2699 | acl_name} | ipx address {800-999 | acl_name}| mac address acl_name}`	VLAN アクセス マップから match コマンドを削除します。

VLAN アクセス マップ シーケンスに match コマンドを設定する際、構文について次の点に注意してください。

- 1 つまたは複数の ACL を選択できます。
- WAN インターフェイスに適用する VACL は、標準および拡張 Cisco IOS IP ACL だけをサポートします。
- match コマンドを削除したり、match コマンド内の特定の ACL を削除する場合は、**no** キーワードを使用します。
- 名前付き MAC レイヤ ACL については、「MAC レイヤ名前付きアクセス リストの設定（任意）」（p.32-40）を参照してください。
- Cisco IOS ACL については、次の URL で、『*Cisco IOS Security Configuration Guide*』Release 12.1 の「Traffic Filtering and Firewalls」、「Access Control Lists:Overview and Guidelines」を参照してください。

  http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121cgcr/secur_c/scprt3/index.htm

「VLAN アクセス マップの設定および確認の例」（p.23-17）を参照してください。

VLAN アクセス マップ シーケンスでの action コマンドの設定

VLAN アクセス マップ シーケンスに action コマンドを設定するには、次の作業を行います。

コマンド	目的
`Router(config-access-map)# action {drop [log]} | {forward [capture]} | {redirect {{ethernet | fastethernet | gigabitethernet | tengigabitethernet} slot/port} | {port-channel channel_id}}`	VLAN アクセス マップ シーケンスに action コマンドを設定します。
`Router(config-access-map)# no action {drop [log]} | {forward [capture]} | {redirect {{ethernet | fastethernet | gigabitethernet | tengigabitethernet} slot/port} | {port-channel channel_id}}`	VLAN アクセス マップ シーケンスから action コマンドを削除します。

VLAN アクセス マップ シーケンスに action コマンドを設定する際、構文について次の点に注意してください。

- パケットに対する drop（ドロップ）、forward（転送）、forward capture（転送キャプチャ）、または redirect（リダイレクト）のアクションが設定できます。
- WAN インターフェイスに適用された VACL は、forward capture アクションだけをサポートします。WAN インターフェイスに適用された VACL は、drop、forward、または redirect の各アクションをサポートしません。
- 転送されたパケットも、設定済み Cisco IOS セキュリティ ACL の対象になります。
- **capture** アクションは、転送されたパケットのキャプチャ ビットを設定し、キャプチャ機能がイネーブルに設定されているポートがそのパケットを受信できるようにします。転送されたパケットだけが、キャプチャ可能です。**capture** アクションの詳細については、「キャプチャ ポートの設定」（p.23-17）を参照してください。
- **log** アクションは、Supervisor Engine 2 上でのみサポートされます。
- WAN インターフェイスに適用された VACL は、**log** アクションをサポートしません。
- **log** アクションが指定されている場合、ドロップされたパケットがソフトウェアで記録されます。記録できるのは、ドロップされた IP パケットだけです。
- **redirect** アクションを指定すると、物理インターフェイスまたは EtherChannel のいずれかのインターフェイスを 5 つまで指定できます。EtherChannel メンバーまたは VLAN インターフェイスにパケットをリダイレクトするように指定することはできません。
- Supervisor Engine 2 を搭載したシステムでは、VACL アクセス マップが設定されている VLAN 上に、リダイレクト インターフェイスが存在する必要があります。Supervisor Engine 1 を搭載したシステムでは、リダイレクトされるパケットの送信元 VLAN 上に、リダイレクト インターフェイスが存在する必要があります。
- action コマンド、または指定したリダイレクト インターフェイスを削除する場合は、**no** キーワードを使用します。

「VLAN アクセス マップの設定および確認の例」（p.23-17）を参照してください。

VLAN アクセス マップの適用

VLAN アクセス マップを適用するには、次の作業を行います。

コマンド	目的
`Router(config)# vlan filter map_name {vlan-list vlan_list | interface type[1] number[2] } CP_CmdPlain`	指定された VLAN または WAN インターフェイスに VLAN アクセス マップを適用します。
`Router(config)# no vlan filter map_name [vlan-list vlan_list | interface type[1] number[2]]`	指定された VLAN または WAN インターフェイスから VLAN アクセス マップを削除します。

1. *type* = **pos**、**atm**、または **serial**
2. number = *slot*/*port* または *slot*/*port_adapter*/*port*、サブインターフェイスまたはチャネル グループ記述子が指定可能

VLAN アクセス マップを適用する際、構文について次の点に注意してください。

- VLAN アクセス マップは、1 つまたは複数の VLAN または WAN インターフェイスに適用できます。
- *vlan_list* パラメータには、単一の VLAN ID、カンマで区切った VLAN ID リスト、または VLAN ID 範囲（*vlan_ID–vlan_ID*）を指定できます。
- VACL が適用されている WAN インターフェイスを削除すると、インターフェイス上の VACL 設定も削除されます。
- 各 VLAN または WAN インターフェイスに適用できる VLAN アクセス マップは 1 つだけです。
- VACL がアクティブになるのは、レイヤ 3 VLAN インターフェイスが設定されている VLAN に適用された場合だけです。レイヤ 3 VLAN インターフェイスを備えていない VLAN に適用された VACL は、非アクティブです。Release 12.1(13)E 以降のリリースでは、レイヤ 3 VLAN インターフェイスを備えていない VLAN に VLAN アクセス マップを適用すると、VLAN アクセス マップをサポートするために、管理上ダウンのレイヤ 3 VLAN インターフェイスが作成されます。レイヤ 3 VLAN インターフェイスを作成できなかった場合、VACL はアクティブになりません。
- セカンダリ プライベート VLAN に VACL を適用することはできません。プライマリ プライベート VLAN に適用された VACL が、セカンダリ プライベート VLAN にも適用されます。
- VLAN または WAN インターフェイスから VLAN アクセス マップを消去する場合は、**no** キーワードを使用します。

「VLAN アクセス マップの設定および確認の例」（p.23-17）を参照してください。

VLAN アクセス マップの設定の確認

VLAN アクセス マップの設定を確認するには、次の作業を行います。

コマンド	目的
`Router# show vlan access-map [map_name]`	VLAN アクセス マップの内容を表示して、VLAN アクセス マップの設定を確認します。
`Router# show vlan filter [access-map map_name | vlan vlan_id | interface type[1] number[2] ]`	VACL と VLAN 間のマッピングを表示して、VLAN アクセス マップの設定を確認します。

1. *type* = **pos**、**atm**、または **serial**
2. number = *slot*/*port* または *slot*/*port_adapter*/*port*、サブインターフェイスまたはチャネル グループ記述子が指定可能

VLAN アクセス マップの設定および確認の例

net_10 および **any_host** という名前付き IP ACL が、次のように定義されていると想定します。

```
Router# show ip access-lists net_10
Extended IP access list net_10
    permit ip 10.0.0.0 0.255.255.255 any

Router# show ip access-lists any_host
Standard IP access list any_host
    permit any
```

次に、VLAN アクセス マップを定義して、転送された IP パケットに適用する例を示します。この例では、net_10 に一致する IP トラフィックは転送され、それ以外のすべての IP パケットはデフォルトの drop アクションによってドロップされます。このマップは VLAN 12 ～ 16 に適用されます。

```
Router(config)# vlan access-map thor 10
Router(config-access-map)# match ip address net_10
Router(config-access-map)# action forward
Router(config-access-map)# exit
Router(config)# vlan filter thor vlan-list 12-16
```

次に、VLAN アクセス マップを定義および適用して、IP パケットをドロップおよび記録する例を示します。この例では、net_10 に一致する IP トラフィックはドロップおよびロギングされ、それ以外のすべての IP パケットは転送されます。

```
Router(config)# vlan access-map ganymede 10
Router(config-access-map)# match ip address net_10
Router(config-access-map)# action drop log
Router(config-access-map)# exit
Router(config)# vlan access-map ganymede 20
Router(config-access-map)# match ip address any_host
Router(config-access-map)# action forward
Router(config-access-map)# exit
Router(config)# vlan filter ganymede vlan-list 7-9
```

次に、VLAN アクセス マップを定義および適用して、IP パケットを転送およびキャプチャする例を示します。この例では、net_10 に一致する IP トラフィックは転送およびキャプチャされ、それ以外のすべての IP パケットはドロップされます。

```
Router(config)# vlan access-map mordred 10
Router(config-access-map)# match ip address net_10
Router(config-access-map)# action forward capture
Router(config-access-map)# exit
Router(config)# vlan filter mordred vlan-list 2, 4-6
```

キャプチャ ポートの設定

VACL でフィルタリングされたトラフィックをキャプチャするように設定されたポートを、キャプチャ ポートといいます。

（注） キャプチャされたトラフィックに IEEE 802.1Q または ISL タグを適用するには、無条件にトランキングするようにキャプチャ ポートを設定します（「ISL または 802.1Q トランクとしてのレイヤ 2 スイッチング ポートの設定」[p.7-9] および「DTP を使用しないようにするためのレイヤ 2 トランクの設定」[p.7-10] を参照）。

キャプチャ ポートを設定するには、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}`	設定するインターフェイスを指定します。
ステップ 2	`Router(config-if)# switchport capture allowed vlan {add | all | except | remove} vlan_list`	（任意）Release 12.1(13)E 以降のリリースを使用する場合、キャプチャするトラフィックを宛先 VLAN 単位でフィルタリングします。デフォルトは **all** です。
	`Router(config-if)# no switchport capture allowed vlan`	設定された宛先 VLAN リストを消去し、デフォルト値（**all**）に戻します。
ステップ 3	`Router(config-if)# switchport capture`	VACL でフィルタリングされたトラフィックをキャプチャするようにポートを設定します。
	`Router(config-if)# no switchport capture`	インターフェイス上でキャプチャ機能をディセーブルにします。

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

キャプチャ ポートを設定する際、構文について次の点に注意してください。

- Release 12.1(13)E 以降のリリースでは、任意のポートをキャプチャ ポートとして設定できます。それより前のリリースでは、キャプチャ ポートとして設定できるのは、IDS モジュール上のギガビット イーサネット モニタ ポートだけです。
- Release 12.1(13)E 以降のリリースを使用する場合、キャプチャ ポートを設定する際、構文について次の点に注意してください。
  - *vlan_list* パラメータには、単一の VLAN ID、カンマで区切った VLAN ID リスト、または VLAN ID 範囲（*vlan_ID–vlan_ID*）を指定できます。
  - キャプチャされたトラフィックをカプセル化するには、キャプチャ　ポートに **switchport trunk encapsulation** コマンド（「トランクとしてのレイヤ 2 スイッチング ポートの設定」[p.7-9] を参照）を設定してから、**switchport capture** コマンドを入力します。
  - キャプチャされたトラフィックをカプセル化しないようにするには、キャプチャ ポートに **switchport mode access** コマンド(「レイヤ 2 アクセス ポートとしての LAN インターフェイスの設定」[p.7-15] を参照）を設定してから、**switchport capture** コマンドを入力します。
  - キャプチャ ポートがサポートするのは、出トラフィックだけです。キャプチャ ポート経由でトラフィックがルータに入ることはできません。

次に、インターフェイス Fast Ethernet 5/1 をキャプチャ ポートとして設定する例を示します。

```
Router(config)# interface gigabitEthernet 5/1
Router(config-if)# switchport capture
Router(config-if)# end
```

次に、VLAN アクセス マップ情報を表示する例を示します。

```
Router# show vlan access-map mordred
Vlan access-map "mordred"  10
        match: ip address net_10
        action: forward capture
Router#
```

次に、VACL と VLAN のマッピングを表示する例を示します。VACL マップごとに、マップが設定されている VLAN、およびマップがアクティブになっている VLAN に関する情報が表示されます。VLAN にインターフェイスがない場合、VACL はアクティブではありません。

```
Router# show vlan filter
VLAN Map mordred:
        Configured on VLANs:  2,4-6
            Active on VLANs:  2,4-6
Router#
```

VACL ロギングの設定

VACL ロギングが設定されているときに、次の状況で IP パケットが拒否されると、ログ メッセージが生成されます。

- 一致する最初のパケットが受信された場合
- 直前の 5 分間に一致するパケットが受信された場合
- 5 分経過する前にしきい値に達している場合

ログ メッセージはフロー単位で生成されます。フローは、同じ IP アドレスおよびレイヤ 4（UDP または TCP）ポート番号を持つパケットとして定義されます。ログ メッセージが生成されると、タイマーおよびパケット カウンタがリセットされます。

VACL ロギングには次の制約事項が適用されます。

- Supervisor Engine 2 でのみサポートされます。
- リダイレクトされたパケットのレート制限機能により、VACL ログ カウンタが不正確になることがあります。
- 拒否された IP パケットのみが記録されます。

VACL ロギングを設定するには、VLAN アクセス マップ サブモードの **action drop log** コマンド アクションを使用します（設定手順については、「VACL の設定」[p.23-12] を参照）。この作業をグローバル コンフィギュレーション モード内で実行して、グローバル VACL ログ パラメータを指定します。

	コマンド	目的
ステップ 1	`Router(config)# vlan access-log maxflow max_number`	ログ テーブルのサイズを設定します。ログ テーブルの内容を削除するには、maxflow の番号を 0 に設定します。デフォルトは 500 で、有効範囲は 0 ～ 2048 です。ログ テーブルが満杯になると、新しいフローから記録されたパケットがソフトウェアによってドロップされます。
ステップ 2	`Router(config)# vlan access-log ratelimit pps`	VACL ロギング パケットの最大リダイレクト速度を設定します。デフォルトのパケット転送速度は 2000 パケット / 秒で、有効範囲は 0 ～ 5000 パケット / 秒です。限度を超えたパケットは、ハードウェアによってドロップされます。
ステップ 3	`Router(config)# vlan access-log threshold pkt_count`	ロギングしきい値を設定します。5 分経過する前にフローのしきい値に達すると、ロギング メッセージが生成されます。デフォルトでは、しきい値は設定されません。
ステップ 4	`Router(config)# exit`	VLAN アクセス マップ コンフィギュレーション モードを終了します。
ステップ 5	`Router# show vlan access-log config`	（任意）設定された VACL ロギング プロパティを表示します。
ステップ 6	`Router# show vlan access-log flow protocol {{src_addr src_mask} | any | {host {hostname | host_ip}}} {{dst_addr dst_mask} | any | {host {hostname | host_ip}}} [vlan vlan_id]`	（任意）VACL ログ テーブルの内容を表示します。
ステップ 7	`Router# show vlan access-log statistics`	（任意）パケット数、メッセージ数などの統計情報を表示します。

次に、グローバル VACL ロギングをハードウェア内で設定する例を示します。

```
Router(config)# vlan access-log maxflow 800
Router(config)# vlan access-log ratelimit 2200
Router(config)# vlan access-log threshold 4000
```

TCP 代行受信の設定

Supervisor Engine 2 および PFC2 を使用する場合、TCP 代行受信フローはハードウェアで処理されます。

Supervisor Engine 1 および PFC を使用する場合、TCP 代行受信フローはソフトウェアで処理されます。

設定手順については、次の URL で『*Cisco IOS Security Configuration Guide*』Release 12.1 の「Traffic Filtering and Firewalls」の「Configuring TCP Intercept」を参照してください。

http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121cgcr/secur_c/scprt3/scddenl.htm

ユニキャスト RPF の設定

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

ユニキャスト RPF サポートの概要

PFC2 は、単一のリターン パスを持つパケットに関して、ユニキャスト RPF をハードウェア処理でサポートしています。MSFC2 は、複数のリターン パスを持つトラフィック（ロードシェアリングなど）をソフトウェアで処理します。

ACL でフィルタリングするようにユニキャスト RPF を設定すると、PFC2 はトラフィックが ACL と一致するかどうかを判別します。PFC2 はユニキャスト RPF チェックを行うために、RPF の ACL で拒否されたトラフィックを MSFC2 に送信します。

（注）

- DoS 攻撃（サービス拒絶攻撃）のパケットはたいてい拒否 ACE と一致し、ユニキャスト RPF チェックのために MSFC2 に送信されるので、MSFC2 が過負荷になることがあります。
- PFC2 は、ユニキャスト RPF の ACL と一致しなくても、入力されたセキュリティ ACL と一致するトラフィックに対して、ハードウェア サポートを提供します。

Supervisor Engine 1 および PFC を使用する場合、MSFC または MSFC 2 はユニキャスト RPF をソフトウェアでサポートします。

ユニキャスト RPF の設定

設定手順については、次の URL で『*Cisco IOS Security Configuration Guide*』Release 12.1 の「Other Security Features」の「Configuring Unicast Reverse Path Forwarding」を参照してください。

http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121cgcr/secur_c/scprt5/scdrpf.htm

self-ping のイネーブル化

ユニキャスト RPF がイネーブルに設定してある場合、ルータは自分自身に 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	目的
ステップ 1	`Router(config)# interface {{vlan vlan_ID} | {type[1] slot/port} | {port-channel number}}`	設定するインターフェイスを選択します。
ステップ 2	`Router(config-if)# ip verify unicast source reachable-via any allow-self-ping`	self-ping やセカンダリ 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。
	`Router(config-if)# no ip verify unicast source reachable-via any allow-self-ping`	self-ping をディセーブルにします。

	コマンド	目的
ステップ 3	`Router(config-if)# exit`	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**、**gigabitethernet**、または **tengigabitethernet**

次に、self-ping 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 allow-self-ping
Router(config-if)# end
```

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 FIB 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 テーブルにあることのみを確認します。

（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	目的
ステップ 1	`Router(config)# interface {{vlan vlan_ID} | {type[1] 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 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)# ip verify unicast source reachable-via {rx | any} [allow-default] [list]`	ユニキャスト RPF チェック モードを設定します。
	`Router(config-if)# no ip verify unicast`	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。
ステップ 3	`Router(config-if)# exit`	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**、**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、構文について次の点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ドロップされます。

- 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#
```

ユニキャスト フラッディング保護の設定

ユニキャスト フラッディング保護機能は、システムがユニキャスト フラッディングによって中断されないように保護します。Cisco 7600 シリーズ ルータは転送テーブルを使用し、フレームの VLAN 番号および宛先 MAC アドレスに基づいて、特定のポートにトラフィックを転送します。着信 VLAN 上にフレームの宛先 MAC アドレスに対応するエントリがない場合、そのフレームは該当する VLAN 上のすべての転送ポートに送信され、フラッディングが起こります。限られたフラッディングであれば通常のスイッチング プロセスの範囲内ですが、フラッディングが続くと、ネットワークのパフォーマンスに悪影響が及ぶことがあります。

ユニキャスト フラッディング保護機能をイネーブルにすると、システムは不明なユニキャスト フラッディングがしきい値を超過した場合に、レート制限を超過した時点でアラートを送信するか、トラフィックをフィルタするか、またはフラッディングを発生させているポートをシャットダウンします。

ユニキャスト フラッディング保護を設定するには、次の作業を行います。

	コマンド	目的
ステップ 1	`Router(config)# [no] mac-address-table unicast-flood {limit kfps} {vlan vlan} {filter timeout | alert | shutdown}`	ユニキャスト フラッディング保護をグローバルにイネーブルにします。
ステップ 2	`Router# show mac-address-table unicast-flood`	ユニキャスト フラッディング保護に関する情報を表示します。

ユニキャスト フラッディング保護を設定する際、構文について次の点に注意してください。

- 送信元 MAC アドレスおよび VLAN 単位でユニキャスト フラッディングを指定するには、**limit** キーワードを使用します。1 ～ 4000 フラッド / 秒（fps）の範囲で指定できます。
- ユニキャスト フラッディング トラフィックをフィルタリングする時間を指定するには、**filter** キーワードを使用します。1 ～ 34560 分の範囲で指定できます。
- ユニキャスト フラッディングのフレームがフラッディングのレート制限を超過した場合に、システムがアラート メッセージを送信するように設定するには、**alert** キーワードを使用します。
- ユニキャスト フラッディングのフレームがフラッディングのレート制限を超過した場合に、システムがフラッディングを発生させている入力ポートをシャットダウンするように設定するには、**shutdown** キーワードを使用します。

次に、ユニキャスト フラッディング トラフィックを 5 分間にわたってフィルタリングし、フラッディングのレート制限を 3000 fps に設定する例を示します。

```
Router(config)# mac-address-table unicast-flood limit 3 vlan 100 filter 5
Router # show mac-address-table unicast-flood
Unicast Flood Protection status: enabled

Configuration:
 vlan      Kfps         action       timeout
------+----------+-----------------+----------
  100          3             filter         5

Mac filters:
 No.   vlan   souce mac addr.           installed on           time left (mm:ss)
-----+------+----------------+------------------------------+------------------

Router(config)#
```

MAC 移動通知の設定

MAC 移動通知を設定すると、MAC アドレスが 1 つのポートから別のポートへ移動した場合にメッセージが生成されます。

（注）　MAC アドレス移動通知機能では、新しい MAC アドレスが CAM に追加された場合、または MAC アドレスが CAM から削除された場合には通知を生成しません。

MAC 移動通知を設定するには、次の作業を行います。

	コマンド	目的
ステップ 1	`Router(config)# [no] mac-address-table notification mac-move`	MAC 移動通知をグローバルにイネーブルにします。
ステップ 2	`Router# show mac-address-table notification mac-move`	MAC 移動通知に関する情報を表示します。

次に、MAC 移動通知機能をイネーブルにする例を示します。

```
Router(config)# mac-address-table notification mac-move
Router# show mac-address-table notification mac-move
MAC Move Notification: enabled
Router#
```