CHAPTER 73

ポート ACL（PACL）

（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、次の資料を参照してください。

  http://www.cisco.com/en/US/products/ps11846/prod_command_reference_list.html
- Cisco IOS Release 15.1SY は、イーサネット インターフェイスだけをサポートしています。Cisco IOS Release 15.1SY は、WAN 機能またはコマンドをサポートしていません。
- ポート ACL は access-list キーワードである **log** または **reflexive** をサポートしません。アクセス リスト内のこれらのキーワードは無視されます。OAL は PACL をサポートしません。
- PACL はプライベート VLAN 上ではサポートされません。

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

技術マニュアルのアイデア フォーラムに参加する

PACL の前提条件

なし。

PACL の制約事項

- 同じレイヤ 2 インターフェイスに方向別に適用できるのは、多くても IP アクセス リストを 1 つと MAC アクセス リストを 1 つです。
- PACL は MPLS、または ARP メッセージに適用されません。

- IP アクセス リストは、IPv4 および IPv6 パケットだけをフィルタリングします。IP アクセス リストでは、標準アクセスリスト、拡張アクセスリスト、または名前付きアクセスリストを定義できます。
- MAC アクセス リストは、イーサネット データグラムのフィールドに基づいて、サポートされないタイプの入力パケット（IP、ARP、MPLS 以外のパケット）をフィルタリングします。MAC アクセス リストは、IP、MPLS、または ARP メッセージには適用されません。定義できるのは名前付き MAC アクセス リストだけです。
- PACL の一部として設定できる ACL と ACE の数は、スイッチのハードウェア リソースにより制限されます。これらのハードウェア リソースは、システムに設定されているさまざまな ACL 機能（VACL など）により共有されます。PACL をハードウェアにプログラミングするのに十分なハードウェア リソースがない場合は、PACL が適用されません。
- PACL は access-list **log** および **reflect/evaluate** キーワードをサポートしません。これらのキーワードを PACL のアクセス リストに追加しても、無視されます。
- OAL は PACL をサポートしません。
- アクセス グループ モードを使用して、その他の ACL との PACL の対話形式を変更できます。シスコ プラットフォーム全体の動作を一貫させるには、デフォルトのアクセス グループ モード（マージ モード）を使用します。
- PACL は、CDP、VTP、DTP、PAgP、UDLD、および STP などの物理リンク プロトコルおよび論理リンク プロトコルをフィルタリングできません。これらのプロトコルは ACL が有効になる前に RP にリダイレクトされるためです。物理リンク プロトコルおよび論理リンク プロトコル トラフィックに CoPP または QoS を適用できます。

PACL について

PACL の概要

PACL は、レイヤ 3 情報、レイヤ 4 ヘッダー情報、または非 IP レイヤ 2 情報を使用して、レイヤ 2 インターフェイスに着信するトラフィックをフィルタリングします。

PACL 機能は、ポートに適用する標準 IP ACL または拡張 IP ACL、または名前付き MAC 拡張 ACL を使用します。

ポート ACL によるアクセス コントロールは、指定されたレイヤ 2 ポートに着信するすべてのトラフィックに対して行われます。

PACL および VACL は、レイヤ 3 アドレス（IP プロトコル向け）またはレイヤ 2 MAC アドレス（IP 以外のプロトコル向け）に基づいてアクセス コントロールを行います。

ポート ACL 機能により、特定のレイヤ 2 ポートに対してアクセス コントロールを行うことができます。レイヤ 2 ポートは、VLAN に属する物理的な LAN ポートまたはトランク ポートです。ポート ACL は、入力トラフィックだけに適用されます。ポート ACL 機能は、ハードウェアだけでサポートされます（ポート ACL は、ソフトウェアでルーティングされたパケットには適用されません）。

ポート ACL を作成すると、ACL TCAM にエントリが作成されます。利用可能な TCAM スペースを確認するには、**show tcam counts** コマンドを使用します。

PACL 機能は、ポートで受信するレイヤ 2 制御パケットには影響を与えません。

PACL とその他の ACL との相互作用の方法を変更するには、**access-group mode** コマンドを使用します。

PACL は次のモードを使用します。

- 優先ポート モード : PACL がレイヤ 2 インターフェイスで設定されている場合は、PACL が有効になり、その他の ACL（Cisco IOS ACL および VACL）を無効になります。PACL 機能がレイヤ 2 インターフェイスで設定されていない場合は、そのインターフェイスに適用可能なその他の機能が結合されて適用されます。
- マージ モード : このモードでは、図 73-2 に示す論理シリアル モデルに従って、PACL、VACL、および Cisco IOS ACL が入力方向に結合されます。これがデフォルトのアクセス グループ モードです。

各インターフェイスで **access-group mode** コマンドを設定します。デフォルトはマージ モードです。

（注） PACL は、優先ポート モードが選択された場合だけ、トランク ポート上で設定できます。トランク ポートはマージ モードをサポートしません。

アクセス グループ モードについて説明するために、VLAN100 に属する物理ポートに次の ACL が設定されているとします。

- Cisco IOS ACL R1 がルーテッド インターフェイス VLAN100 に適用されます。
- VACL（VLAN フィルタ）V1 が VLAN100 に適用されます。
- PACL P1 が物理ポートに適用されます。

この状況では、次のような ACL の相互作用が行われます。

- 優先ポート モードでは、Cisco IOS ACL R1 および VACL V1 は無視されます。
- マージ モードでは、Cisco IOS ACL R1、VACL V1、および PACL P1 は結合され、ポートに適用されます。

（注） PACL を作成するための CLI 構文は、Cisco IOS ACL を作成する構文と同じです。レイヤ 2 ポートにマッピングされている ACL のインスタンスが PACL です。レイヤ 3 インターフェイスにマッピングされている ACL のインスタンスは Cisco IOA ACL です。同じ ACL をレイヤ 2 ポートとレイヤ 3 インターフェイスの両方にマッピングできます。

PACL 機能は MAC ACL、IPv4 および IPv6 ACL をサポートします。PACL 機能は ARP、またはマルチプロトコル ラベル スイッチング（MPLS）トラフィック用の ACL をサポートしません。

EtherChannel と PACL の相互作用

ここでは、EtherChannel と PACL の相互作用における注意事項について説明します。

- PACL はメイン レイヤ 2 チャネル インターフェイス上でサポートされますが、ポート メンバ上ではサポートされません。PACL が設定されているポートは、EtherChannel メンバ ポートとして設定されていない場合があります。EtherChannel コンフィギュレーション コマンドは、PACL が設定されたポートでは使用できません。

- 論理ポートの設定変更は、チャネル内のすべてのポートに影響します。チャネルに属する論理ポートに ACL をマッピングすると、そのチャネル内のすべてのポートにもマッピングされます。

ダイナミック ACL（マージ モードだけに適用）

ダイナミック ACL は VLAN ベースで、CBAC および GWIP の 2 つの機能によって使用されます。マージ モードは、ダイナミック ACL と PACL の結合をサポート*しません*。マージ モードでは、次のような設定はできません。

- 対応する VLAN にダイナミック ACL がマッピングされているポートに PACL を設定しようとすること。この場合、PACL はポート上のトラフィックに適用されません。
- 構成ポートの 1 つに PACL がインストールされている VLAN にダイナミック ACL を適用しようとすること。この場合、動的 ACL は適用されません。

トランク ポート

トランク ポートで PACL を設定するには、ポート優先モードを先に設定する必要があります。**access-group mode prefer port** インターフェイス コマンドを入力してポート優先モードを設定するまで、トランク ポートまたはダイナミック ポートに PACL を適用するコンフィギュレーション コマンドは使用できません。トランク ポートはマージ モードをサポートしません。

レイヤ 2 ポートからレイヤ 3 ポートへの変換

ポートをレイヤ 2 からレイヤ 3 に再設定する場合、ポート上に設定されているすべての PACL は非アクティブになりますが、設定からは削除されません。その後ポートをレイヤ 2 として設定すると、ポート上に設定されているすべての PACL は再度アクティブになります。

ポート/VLAN アソシエーション変更

ポート/VLAN アソシエーションを変更するポート コンフィギュレーション コマンドを入力すると、ACL 再結合を開始できます。

PACL、VACL、または Cisco IOS ACL をマッピング解除したあとに再度マッピングすると、再結合が自動的に開始されます。

マージ モードでは、モジュール上のポートに PACL が設定されている場合は、スイッチング モジュールの活性挿抜によっても再結合が開始されます。

PACL と VACL の相互作用

- 「PACL の VACL および Cisco IOS ACL との相互作用」（P.73-5）
- 「ブリッジド パケット」（P.73-5）
- 「ルーティング対象パケット」（P.73-5）
- 「マルチキャスト パケット」（P.73-6）

PACL の VACL および Cisco IOS ACL との相互作用

ここでは、PACL の VACL および Cisco IOS ACL との相互作用における注意事項について説明します。

PACL はまず、物理ポートの着信パケットに適用されます。パケットが PACL により許可されると、次に入力 VLAN の VACL が適用されます。パケットがレイヤ 3 で転送され、VACL により許可される場合は、同じ VLAN 上の Cisco IOS ACL によりフィルタリングされます。出力方向では同じプロセスが逆に発生します。ただし、出力 PACL はハードウェアで現在サポートされていません。

ポートが優先ポート モードに設定されている場合、PACL により VACL と Cisco IOS ACL の両方が無効になります。このルールの 1 つの例外は、パケットがルート プロセッサ（RP）によってソフトウェアで転送される場合です。RP は PACL モードに関係なく入力 Cisco IOS ACL を適用します。パケットがソフトウェアで転送される 2 つの例は、次のとおりです。

- 出力ブリッジド パケット（ロギングや NAT などの機能のため）
- IP オプションが指定されたパケット

ブリッジド パケット

図 73-1 に、ブリッジド パケットに適用される PACL および VACL を示します。マージ モードでは、ACL は次の順序で適用されます。

1. 入力ポートの PACL
2. 入力 VLAN の VACL
3. 出力 VLAN の VACL

図 73-1　　ブリッジド パケットへの ACL の適用

優先ポート モードでは、入力パケットに適用されるのは PACL だけです（入力 VACL は適用されません）。

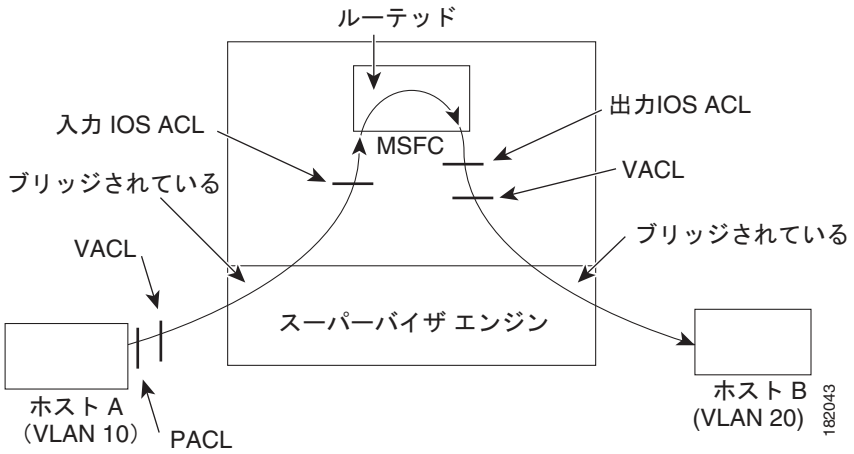
ルーティング対象パケット

図 73-2 に、ルーティング対象パケットおよびレイヤ 3 スイッチング対象パケットに ACL を適用する方法を示します。マージ モードでは、ACL は次の順序で適用されます。

1. 入力ポートの PACL
2. 入力 VLAN の VACL
3. 入力 Cisco IOS ACL
4. 出力 Cisco IOS ACL
5. 出力 VLAN の VACL

優先ポート モードでは、入力パケットに適用されるのは PACL だけです（入力 VACL および Cisco IOS ACL は適用されません）。

図 73-2　ルーテッド パケットへの ACL の適用



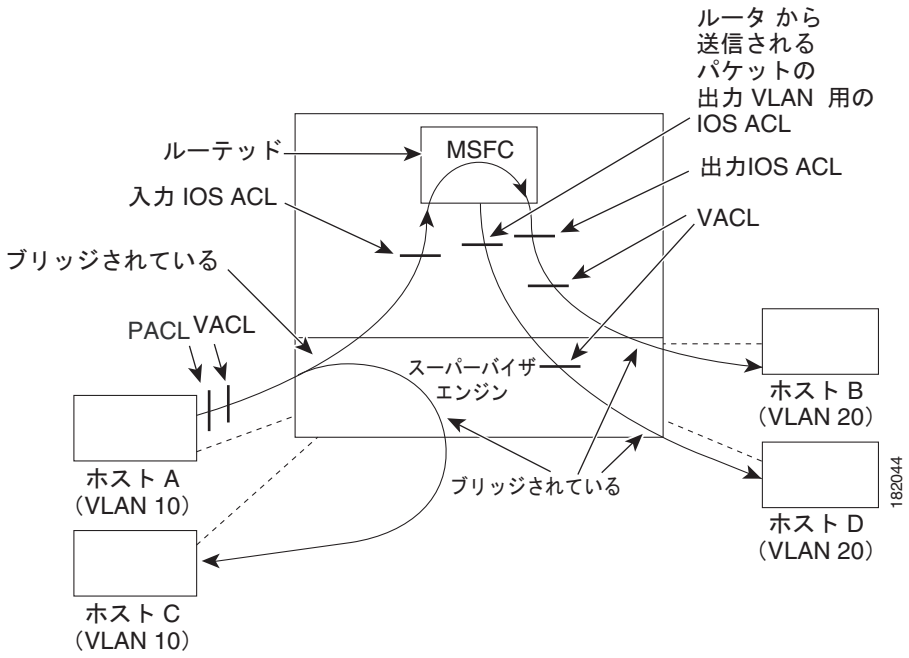
マルチキャスト パケット

図 73-3 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. 入力ポートの PACL
   b. 入力 VLAN の VACL
   c. 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 の VACL
3. ルータから送られるパケット
   a. 出力 Cisco IOS ACL
   b. 出力 VLAN の VACL

優先ポート モードでは、入力パケットに適用されるのは PACL だけです（入力 VACL および Cisco IOS ACL は適用されません）。

図 73-3　マルチキャスト パケットへの ACL の適用



PACL の設定方法

レイヤ 2 インターフェイスの IP ACL および MAC ACL の設定

IP ACL および MAC ACL はレイヤ 2 物理インターフェイスに適用できます。（番号付き、名前付き）標準 IP ACL、（番号付き、名前付き）拡張 IP ACL、および名前付き拡張 MAC ACL がサポートされています。

レイヤ 2 インターフェイス上に IP ACL または MAC ACL を適用するには、次の作業を行います。

	コマンド	目的
ステップ 1	`Switch# configure terminal`	グローバル 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	`Switch(config)# interface interface`	レイヤ 2 ポートのインターフェイス コンフィギュレーション モードを開始します。

	コマンド	目的
ステップ 3	`Switch(config-if)# {ip | mac} access-group {name | number | in | out}`	番号付き ACL または名前付き ACL をレイヤ 2 インターフェイスに適用します。
ステップ 4	`Switch(config)# show running-config`	アクセス リストの設定を表示します。

次に、すべての TCP トラフィックを許可し、他のすべての IP トラフィックを暗黙的に拒否する名前付き拡張 IP ACL simple-ip-acl を設定する例を示します。

```
Switch(config)# ip access-list extended simple-ip-acl
Switch(config-ext-nacl)# permit tcp any any
Switch(config-ext-nacl)# end
```

次に、送信元ホスト 000.000.011 を任意の宛先ホストで許可する、名前付き拡張 MAC ACL simple-mac-acl を設定する例を示します。

```
Switch(config)# mac access-list extended simple-mac-acl
Switch(config-ext-macl)# permit host 000.000.011 any
Switch(config-ext-macl)# end
```

レイヤ 2 インターフェイス上でのアクセス グループ モードの設定

アクセス モードをレイヤ 2 インターフェイス上で設定するには、次の作業を行います。

	コマンド	目的
ステップ 1	`Switch# configure terminal`	グローバル 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	`Switch(config)# interface` *interface*	レイヤ 2 ポートのインターフェイス コンフィギュレーション モードを開始します。
ステップ 3	`Switch(config-if)# [no] access-group mode {prefer port | merge}`	このレイヤ 2 インターフェイスのモードを設定します。**no** プレフィックスは、モードをデフォルト（マージ）に設定します。
ステップ 4	`Switch(config)# show running-config`	アクセス リストの設定を表示します。

次の例では、優先ポート モードを使用するようインターフェイスを設定します。

```
Switch# configure terminal
Switch(config)# interface gigabitEthernet 6/1
Switch(config-if)# access-group mode prefer port
```

次の例では、マージ モードを使用するようインターフェイスを設定します。

```
Switch# configure terminal
Switch(config)# interface gigabitEthernet 6/1
Switch(config-if)# access-group mode merge
```

レイヤ 2 インターフェイスへの ACL の適用

レイヤ 2 インターフェイスに IP ACL および MAC ACL を適用するには、次のいずれかの作業を行います。

コマンド	目的
Switch(config-if)# **ip access-group** *ip-acl* **in**	IP ACL をレイヤ 2 インターフェイスに適用します。
Switch(config-if)# **mac access-group** *mac-acl* **in**	レイヤ 2 インターフェイスに MAC ACL を適用します。

次に、名前付き拡張 IP ACL simple-ip-acl をインターフェイス GigabitEthernet 6/1 入力トラフィックに適用する例を示します。

```
Switch# configure t
Switch(config)# interface gigabitEthernet 6/1
Switch(config-if)# ip access-group simple-ip-acl in
```

次に、名前付き拡張 MAC ACL simple-mac-acl をインターフェイス GigabitEthernet 6/1 入力トラフィックに適用する例を示します。

```
Switch# configure t
Switch(config)# interface gigabitEthernet 6/1
Switch(config-if)# mac access-group simple-mac-acl in
```

ポート チャネルへの ACL の適用

ポート チャネルの論理インターフェイスに IP ACL および MAC ACL を適用にするには、次の作業を行います。

コマンド	目的
Switch(config-if)# **interface port-channel** *number*	ポート チャネルのコンフィギュレーション モードを開始します。
Switch(config-if)# **ip access-group** *ip-acl* {**in** | **out**}	IP ACL をポート チャネル インターフェイスに適用します。
Switch(config-if)# **mac access-group** *mac-acl* {**in** | **out**}	MAC ACL をポート チャネル インターフェイスに適用します。

次に、名前付き拡張 IP ACL simple-ip-acl をポート チャネル 3 入力トラフィックに適用する例を示します。

```
Switch# configure t
Switch(config)# interface port-channel 3
Switch(config-if)# ip access-group simple-ip-acl in
```

レイヤ 2 インターフェイス上の ACL 設定の表示

レイヤ 2 インターフェイス上の ACL 設定に関する情報を表示するには、次のいずれかの作業を行います。

コマンド	目的
Switch# **show ip access-lists** [**interface** *interface-name*]	インターフェイス上の IP アクセス グループ設定を表示します。

コマンド	目的
Switch# **show mac access-group** [**interface** *interface-name*]	インターフェイス上の MAC アクセス グループ設定を表示します。
Switch# **show access-group mode** [**interface** *interface-name*]	インターフェイス上のアクセス グループ モード設定を表示します。

次に、IP アクセス グループ simple-ip-acl がインターフェイス fa6/1 の着信方向に設定されている例を示します。

```
Switch# show ip interface gigabitethernet 6/1
GigabitEthernet6/1 is up, line protocol is up
  Inbound  access list is simple-ip-acl
  Outgoing access list is not set
```

次に、MAC アクセス グループ simple-mac-acl がインターフェイス Gigabit Ethernet 6/1 の着信方向に設定されている例を示します。

```
Switch# show mac access-group interface gigabitethernet 6/1
Interface GigabitEthernet6/1:
   Inbound access-list is simple-mac-acl
   Outbound access-list is not set
```

次に、アクセス グループ統合がインターフェイス Gigabit Ethernet 6/1 に設定されている例を示します。

```
Switch# show access-group mode interface gigabitethernet 6/1
Interface GigabitEthernet6/1:
   Access group mode is: merge
```

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

技術マニュアルのアイデア フォーラムに参加する