CHAPTER 5

# IPv4 および IPv6 のアクセス制御リストの設定

Cisco MDS 9000 ファミリ スイッチ製品は、イーサネットとファイバ チャネル インターフェイスの間で Internet Protocol（IP）バージョン 4（IPv4）トラフィックをルーティングできます。IP スタティック ルーティング機能が Virtual Storage Area Network（VSAN; 仮想ストレージ エリア ネットワーク）間のトラフィックをルーティングします。これを行うためには、各 VSAN が 異なる IPv4 サブネットワークに属していなければなりません。各 Cisco MDS 9000 ファミリ スイッチは Network Management System（NMS; ネットワーク管理システム）に対して次のサービスを提供します。

- スーパーバイザ モジュールの前面パネルに設けられたアウトオブバンド イーサネット インターフェイス（mgmt0）での IP 転送。
- IP over Fibre Channel（IPFC）機能を使用したインバンド ファイバ チャネル インターフェイス上の IP 転送：IPFC は、カプセル化手法を利用して IP フレームをファイバ チャネル上で転送するための方法を定義しています。IP フレームはファイバ チャネル フレームにカプセル化されるため、オーバーレイ イーサネット ネットワークを使用しなくても、ファイバ チャネル ネットワーク上で NMS 情報を伝達できます。
- IP ルーティング（デフォルト ルーティングおよびスタティック ルーティング）：外部ルータを必要としない設定の場合は、スタティック ルーティングを使用してデフォルト ルートを設定できます。

スイッチの Virtual Router Redundancy Protocol（VRRP; 仮想ルータ冗長プロトコル）機能は RFC 2338 標準規格に準拠しています。VRRP は、冗長な代替パスをゲートウェイ スイッチに提供する、再起動可能なアプリケーションです。

IPv4 アクセス コントロール リスト（IPv4-ACL および IPv6-ACL）は、すべての Cisco MDS 9000 ファミリ スイッチに基本的なネットワーク セキュリティを提供します。IPv4-ACL および IPv6-ACL は、設定された IP フィルタに基づいて IP 関連トラフィックを規制します。フィルタには IP パケットと一致させる規則が含まれています。パケットが一致すると、規則に基づいてパケットの許可または拒否が判別されます。

Cisco MDS 9000 ファミリの各スイッチには合計最大 128 の IPv4-ACL または 128 の IPv6-ACL を設定でき、各 IPv4-ACL または IPv6-ACL に最大 256 のフィルタを設定できます。

この章の内容は、次のとおりです。

# IPv4-ACL および IPv6-ACL の設定時の注意事項

Cisco MDS 9000 ファミリのスイッチまたはディレクタに IPv4-ACL または IPv6-ACL を設定する場合には、次の注意事項に従ってください。

- IPv4-ACL または IPv6-ACL は、VSAN インターフェイス、管理用インターフェイス、Intrusion Prevention System（IPS; 侵入防御システム）モジュールおよび 14/2 Multiprotocol Services（MPS-14/2; 14/2 マルチプロトコル サービス）モジュール上のギガビット イーサネット、およびイーサネット ポートチャネル インターフェイスに適用できます。

**ヒント**　ギガビット イーサネット インターフェイスに IPv4-ACL または IPv6-ACL がすでに設定されている場合は、このインターフェイスをイーサネット ポートチャネル グループに追加することができません。IPv4-ACL の設定に関する注意事項については、『Cisco Fabric Manager IP Services Configuration Guide』を参照してください。

**注意**　IPv4-ACL または IPv6-ACL の適用は、ポートチャネル グループ内の 1 つのメンバーだけに限定しないでください。IPv4-ACL または IPv6-ACL はチャネル グループ全体に適用します。

- 条件の順序は正確に設定します。IPv4-ACL または IPv6-ACL フィルタは IP フローに順番に適用されるので、最初の一致によって動作が決定されます。以降の一致は考慮されません。最も重要な条件を最初に設定してください。どの条件とも一致しなかった場合、パケットは廃棄されます。
- IP ストレージ ギガビット イーサネット ポートには暗黙の拒否は影響しないので、IP ACL を適用するにはこれらのポートに明示的な拒否を設定します。

# フィルタの内容について

IP フィルタにはプロトコル、アドレス、ポート、Internet Control Message Protocol（ICMP）タイプ、および Type of Service（ToS; サービス タイプ）に基づく IP パケットの一致規則が含まれます。

ここで説明する内容は、次のとおりです。



## プロトコル情報

各フィルタには、プロトコル情報が必要です。この情報により、IP プロトコルの名前または番号を識別します。IP プロトコルは、次のいずれかの方法で指定できます。

- 0 ～ 255 の範囲の整数を指定します。この数字は、IP プロトコルを示します。
- プロトコルの名前を指定します。指定できるプロトコルには、Internet Protorol（IP）、Transmission Control Protocol（TCP）、User Datagram Protocol（UDP）、Internet Control Message Protocol（ICMP）などがあります。

（注）　ただし、ギガビット イーサネット インターフェイスに IPv4-ACL または IPv6-ACL を設定する場合は、TCP または ICMP オプションだけを使用します。

# アドレス情報

各フィルタには、アドレス情報が必要です。アドレス情報により、次の詳細を識別します。

- 送信元：パケット送信元のネットワークまたはホストのアドレス
- 送信元ワイルドカード：送信元に適用されるワイルドカード ビット
- 宛先：パケットの送信先となるネットワークまたはホストの番号
- 宛先ワイルドカード：宛先に適用されるワイルドカード ビット

送信元/送信元ワイルドカードおよび宛先/宛先ワイルドカードは、次のいずれかの方法で指定します。

- 4 つに区切られたドット付き 10 進表記の 32 ビット数を使用します（10.1.1.2/0.0.0.0 はホスト 10.1.1.2 と同じ）。
  - 各ワイルドカード ビットをゼロに設定する場合には、パケットの IPv4 アドレス内の対応するビット位置と送信元の対応するビット位置で、ビット値が正確に一致している必要があります。
  - 各ワイルドカード ビットを 1 に設定する場合は、パケットの IPv4 または IPv6 アドレス内の対応する位置のビット値が 0 および 1 のいずれであっても、現在のアクセス リスト エントリと一致すると見なされます。無視するビット位置に 1 を入れます。たとえば、0.0.255.255 の場合、送信元の最初の 16 ビットだけが完全に一致する必要があります。複数のワイルドカード ビットを 1 に設定する場合、これらのビットが送信元ワイルドカード内で連続している必要はありません。たとえば、送信元ワイルドカード 0.255.0.64 は有効です。
- 送信元/送信元ワイルドカードまたは宛先/宛先ワイルドカード（0.0.0.0/255.255.255.255）の短縮形として、**any** オプションを使用します。

# ポート情報

ポート情報はオプションです。送信元ポートと宛先ポートを比較するためには、**eq**（等号）オプション、**gt**（より大きい）オプション、**lt**（より小さい）オプション、または **range**（ポート範囲）オプションを使用します。ポート情報は次のいずれかの方法で指定できます。

- ポート番号を指定します。ポート番号の有効範囲は 0 ～ 65535 です。表 5-1 に、関連 TCP ポートおよび UDP ポートについて、Cisco NX-OS ソフトウェアが認識するポート番号を示します。
- TCP または UDP ポートの名前を次のように指定します。
  - TCP ポート名は、TCP をフィルタリングする場合に限って使用できます。
  - UDP ポート名は、UDP をフィルタリングする場合に限って使用できます。

表 5-1　TCP および UDP のポート番号

| プロトコル | ポート | 番号 |
|---|---|---|
| UDP | dns | 53 |
| | tftp | 69 |
| | ntp | 123 |
| | radius accounting | 1646 または 1813 |
| | radius authentication | 1645 または 1812 |
| | snmp | 161 |
| | snmp-trap | 162 |
| | Syslog | 514 |
| TCP[1] | ftp | 20 |
| | ftp-data | 21 |
| | ssh | 22 |
| | telnet | 23 |
| | smtp | 25 |
| | tasacs-ds | 65 |
| | www | 80 |
| | sftp | 115 |
| | http | 143 |
| | wbem-http | 5988 |
| | wbem-https | 5989 |

1. TCP 接続が確立済みの場合は、**established** オプションを使用して適合するものを探してください。TCP データグラムが ACK、FIN、PSH、RST または URG のコントロール ビット セットを持つ場合は、適合と見なされます。

# ICMP 情報

オプションとして IP パケットは次の ICMP 条件に基づいて選別できます。

- icmp-type：ICMP メッセージ タイプは 0 ～ 255 の番号から 1 つ選びます。
- icmp-code：ICMP メッセージ コードは 0 ～ 255 の番号から 1 つ選びます。

表 5-2 に各 ICMP タイプの値を示します。

表 5-2　ICMP タイプの値

| ICMP タイプ[1] | コード番号 |
|---|---|
| エコー | 8 |
| エコー応答 | 0 |
| 宛先不達 | 3 |
| traceroute | 30 |
| 時間超過 | 11 |

1. ICMP リダイレクト パケットは必ず拒否されます。

## ToS 情報

オプションとして IP パケットは次の ToS 条件に基づいてフィルタにより選別できます。

- ToS レベル：レベルは 0 ～ 15 の番号で指定します。
- ToS 名：名前は max-reliability、max-throughput、min-delay、min-monetary-cost、および normal から選択できます。

# IP-ACL ウィザードを使用した IPv4-ACL または IPv6-ACL の作成

スイッチに入ったトラフィックは、スイッチ内でフィルタが現れる順番に従って IPv4-ACL または IPv6-ACL のフィルタと比較されます。新しいフィルタは IPv4-ACL または IPv6-ACL の末尾に追加されます。スイッチは合致するまで照合を続けます。フィルタの最後に達して合致するものがなかった場合は、そのトラフィックは拒否されます。そのため、フィルタの最上部にはヒットする確立の高いフィルタを置きます。許可されないトラフィックに対しては *implied deny* が用意されています。1 つの拒否エントリしか持たないシングルエントリの IPv4-ACL または IPv6-ACL には、すべてのトラフィックを拒否する効果があります。

IPv4-ACL または IPv6-ACL を設定する手順は、次のとおりです。

**ステップ 1**　IPv4-ACL または IPv6-ACL の作成にはフィルタ名と 1 つ以上のアクセス条件を指定します。フィルタには条件に合致する発信元と宛先のアドレスが必要です。適切な粒度を設定するためにオプションのキーワードを使用できます。

**（注）**　フィルタのエントリは順番に実行されます。エントリはリストの最後にだけ追加できます。正しい順番でエントリを追加するように注意してください。

**ステップ 2**　指定したインターフェイスにアクセス フィルタを適用します。

IPv4-ACL または IPv6-ACL の名前付きプロファイルの中に順番に並べた IP フィルタのリストを、Fabric Manager の IPv4-ACL ウィザードを使用して作成する手順は、次のとおりです。

**ステップ 1**　Fabric Manager ツールバーで [IP ACL Wizard] アイコンをクリックします（図 5-1 を参照）。

**図 5-1　[IP ACL Wizard]**


IP ACL ウィザードが表示されます。

**ステップ 2**　IP-ACL プロファイルの名前を入力します。

（注）　IPv6-ACL を作成する場合は、IPv6 チェックボックスをオンにします。

**ステップ 3**　[Add] ボタンをクリックし、この IP-ACL に新しいルールを追加します。テーブルに新しい規則とデフォルト値が表示されます。

**ステップ 4**　必要に応じて、フィルタの送信元 IP および送信元マスクを修正します。

（注）　IP-ACL ウィザードで作成できるのは、着信 IP フィルタだけです。

**ステップ 5**　[Application] ドロップダウン リストで、適切なフィルタ タイプを選択します。

**ステップ 6**　[Action] ドロップダウン リストで [permit] または [deny] を選択します。

**ステップ 7**　追加する IP フィルタに対して、ステップ 3 ～ステップ 6 を繰り返します。

**ステップ 8**　[Up] ボタンまたは [Down] ボタンをクリックして、IP-ACL フィルタの順序を決定します。

**ヒント**　IP フィルタの順序は慎重に決定してください。トラフィックは、指定された順序で IP フィルタと比較されます。最初の一致が適用され、以降のフィルタは無視されます。

**ステップ 9**　[Next] ボタンをクリックします。

この IP-ACL を適用できるスイッチのリストが表示されます。

**ステップ 10**　この IP-ACL を適用したくないスイッチは、選択を取り消します。

**ステップ 11**　この IP-ACL を適用する**インターフェイス**を選択します。

**ステップ 12**　[Finish] ボタンをクリックして、この IP-ACL を作成し、選択したスイッチに適用します。

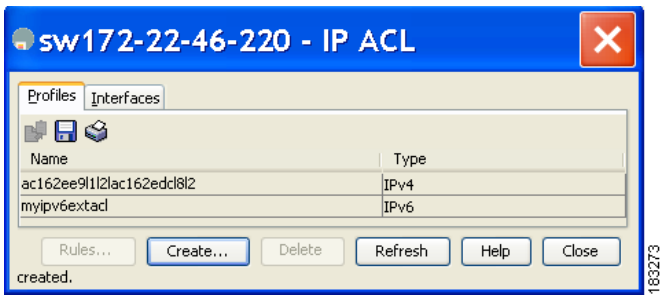
# Device Manager での IPv4-ACL または IPv6-ACL の作成

Device Manager を使用して既存の IPv4-ACL または IPv6-ACL にエントリを追加する手順は、次のとおりです。

**ステップ 1**　[Security] > [IP ACL] を選択します。

[IP ACL] ダイアログボックスが表示されます（図 5-2 を参照）。

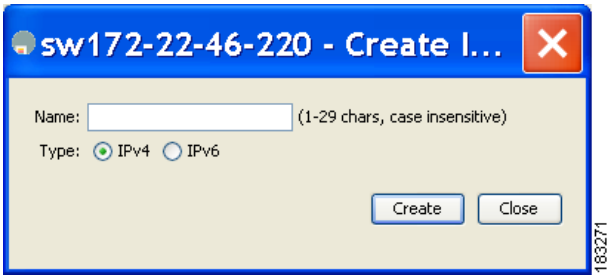
**図 5-2　[IP ACL] ダイアログボックス**



**ステップ 2**　[Create] ボタンをクリックして、IP-ACL プロファイルを作成します。

[Create IP ACL Profiles] ダイアログボックスが表示されます（図 5-3 を参照）。

**図 5-3　[Create IP ACL Profiles] ダイアログボックス**




**ステップ 3**　IP-ACL プロファイルの名前を入力します。

**ステップ 4**　[Create] ボタンをクリックしてから [Close] ボタンをクリックします。

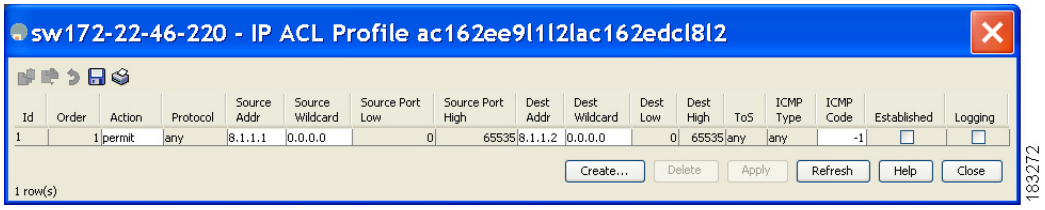
新しい IP-ACL プロファイルを作成します。

**ステップ 5**　作成した IP-ACL をクリックし、[Rules] ボタンをクリックします。

Device Manager を使用している場合は、IPv4-ACL または IPv6-ACL の作成後に、続く IP フィルタを IPv4-ACL または IPv6-ACL の最後に追加できます。Fabric Manager を利用すると、1 つのプロファイルに対する既存のルールを並び替えることができます。IPv4-ACL または IPv6-ACL の中間にはフィルタを挿入できません。設定された各エントリは、自動的に IPv4-ACL または IPv6-ACL の最後に追加されます。

[IP ACL] ダイアログボックスが表示されます（図 5-4 を参照）。

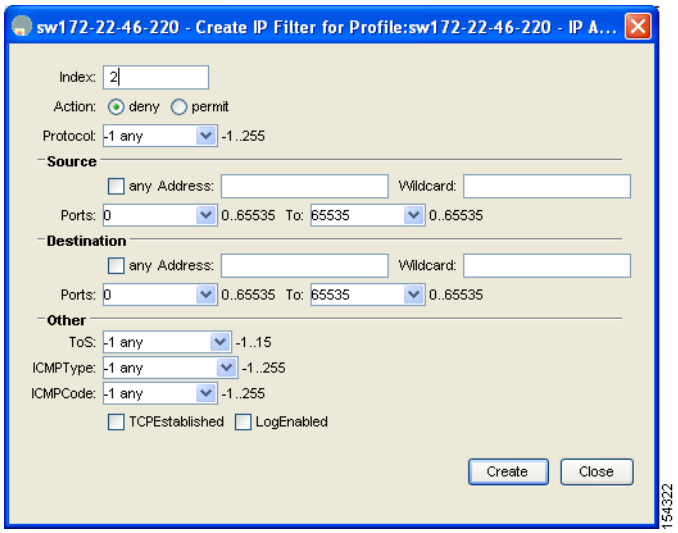
**図 5-4　[IP ACL Profile] ダイアログボックス**




**ステップ 6**　[Create] ボタンをクリックして、IP フィルタを作成します。

[Create IP Filter] ダイアログボックスが表示されます（図 5-5 を参照）。

図 5-5　[Create IP Filter] ダイアログボックス




**ステップ 7**　[Action] から [permit] または [deny] のいずれかのオプション ボタンを選択し、[Protocol] フィールドに IP 番号を設定します。ドロップダウン メニューには、一般的なフィルタリングされたプロトコルが提供されています。

**ステップ 8**　フィルタを適用する送信元 IP アドレスおよびワイルドカード マスクを設定します。すべての IP アドレスに対して適用する場合には、[any] チェックボックスをオンにします。

これにより、フレームの送信元 IP アドレスをチェックする IP フィルタが作成されます。

**（注）**　ワイルドカード マスクには、一致させる IP アドレスのサブネットを指定します。フィルタは、指定したアドレス範囲に対して適用されます。

**ステップ 9**　TCP または UDP のプロトコルを選択した場合には、トランスポート レイヤの送信元ポート範囲を設定します。

**ステップ 10**　宛先 IP アドレスおよびポート範囲について、ステップ 8 とステップ 9 を繰り返します。

これにより、フレームの宛先 IP アドレスをチェックする IP フィルタが作成されます。

**ステップ 11**　必要に応じて、[ToS]、[ICMPType]、および [ICMPCode] フィールドを設定します。

**ステップ 12**　ACK、FIN、PSH、RST、SYN、または URG 制御ビット セットを含む TCP 接続を一致させたい場合には、[TCPEstablished] チェックボックスをオンにします。

**ステップ 13**　この IP フィルタと一致する全フレームのログを作成する場合には、[LogEnabled] チェックボックスをオンにします。

**ステップ 14**　[Create] ボタンをクリックして、この IP フィルタを作成し、IP-ACL に追加します。

# 既存の IPv4-ACL または IPv6-ACL からの IP フィルタの削除

Device Manager を使用して既存の IPv4-ACL または IPv6-ACL から、設定したエントリを削除する手順は、次のとおりです。

**ステップ 1**　[Security] > [IP ACLs] を選択します。

[IP ACL] ダイアログボックスが表示されます（図 5-2 を参照）。

**ステップ 2**　修正する IP-ACL をクリックしてから [Rules] ボタンをクリックします。

このプロファイルに関連する IP フィルタのリストが表示されます（図 5-4 を参照）。

**ステップ 3**　削除するフィルタを選択してから [Delete] ボタンをクリックし、その IP フィルタを削除します。

## IP-ACL の削除

IP-ACL を削除する前に、IP-ACL とインターフェイスの関連付けを削除する必要があります。

Fabric Manager で IP-ACL を削除する手順は、次のとおりです。

**ステップ 1**　[Physical Attributes] ペインで [Switches] > [Security] を展開し、[IP ACL] を選択します。

[Information] ペインに、IP-ACL の設定が表示されます。

**ステップ 2**　[Profiles] タブをクリックします。

スイッチ、ACL、およびプロファイル名のリストが表示されます。

**ステップ 3**　削除する行を選択します。複数の行を削除する場合は、Shift キーを押しながら行を選択します。

**ステップ 4**　[Delete Row] をクリックします。IP-ACL が削除されます。

# IP-ACL ログ ダンプの読み取り

このフィルタに合致するパケットに関する情報をログに記録するには、IP フィルタ作成の際に [LogEnabled] チェックボックスを使用します。ログ出力には ACL の番号、許可または拒否のステータス、およびポート情報が表示されます。

入力 ACL に対しては、ログは無加工の Media Access Control（MAC; メディア アクセス制御）情報を表示します。キーワード「MAC=」は、MAC アドレス情報を持つイーサネットの MAC フレームの表示ではなく、ログにダンプされるレイヤ 2 の MAC レイヤ情報を指しています。出力 ACL に対しては、無加工のレイヤ 2 情報はログに記録されません。

入力 ACL ログ ダンプの例を次に示します。

```
Jul 17 20:38:44 excal-2
%KERN-7-SYSTEM_MSG:
%IPACL-7-DENY:IN=vsan1 OUT=
MAC=10:00:00:05:30:00:47:df:10:00:00:05:30:00:8a:1f:aa:aa:03:00:00:00:08:00:45:00:00:54:00
:00:40:00:40:01:0e:86:0b:0b:0b:0c:0b:0b:0b:02:08:00:ff:9c:01:15:05:00:6f:09:17:3f:80:02:01
:00:08:09:0a:0b:0c:0d:0e:0f:10:11:12:13:14:15:16:17:18:19:1a:1b:1c:1d:1e:1f:20:21:22:23:24
:25:26:27:28:29:2a:2b SRC=11.11.11.12 DST=11.11.11.2 LEN=84 TOS=0x00 PREC=0x00 TTL=64 ID=0
DF PROTO=ICMP TYPE=8 CODE=0 ID=277 SEQ=1280
```

出力 ACL ログ ダンプの例を次に示します。

```
Jul 17 20:38:44 excal-2
%KERN-7-SYSTEM_MSG:
%IPACL-7-DENY:IN= OUT=vsan1 SRC=11.11.11.2 DST=11.11.11.12 LEN=84 TOS=0x00 PREC=0x00
TTL=255 ID=38095 PROTO=ICMP TYPE=0 CODE=0 ID=277 SEQ=1280
```

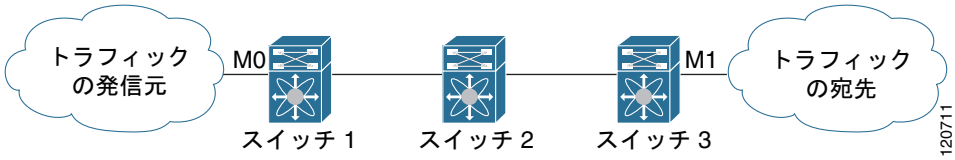
# インターフェイスへの IP-ACL の適用

IP-ACL は適用しなくても定義できます。しかし、IP-ACL はスイッチのインターフェイスに適用されるまで効果は出ません。IP-ACL は、VSAN インターフェイス、管理用インターフェイス、IPS モジュールおよび MPS-14/2 モジュール上のギガビット イーサネット、およびイーサネット ポートチャネル インターフェイスに適用できます。

**ヒント**　トラフィックフの送信元に一番近いインターフェイスに IP-ACL を適用してください。

送信元から宛先へ流れるトラフィックをブロックする場合は、スイッチ 3 の M1 に対するアウトバンドフィルタのかわりに、スイッチ 1 の M0 にインバウンド IPv4-ACL を適用できます（図 5-6 を参照）。

**図 5-6　インバウンド インターフェイス上のトラフィックの拒否**




**access-group** オプションによりインターフェイスへのアクセスを規制できます。各インターフェイスは、1 つの方向につき 1 つの IP-ACL にしか関連付けできません。入力方向には、出力方向とは異なる IP-ACL を持たせることができます。IP-ACL はインターフェイスに適用されたときにアクティブになります。

**ヒント**　IP-ACL の中の条件は、インターフェイスに適用する前にすべて作成しておいてください。

**注意**　IP-ACL を作成前にインターフェイスに適用すると、IP-ACL が空白であるため、そのインターフェイスのすべてのパケットが排除されます。

スイッチにおいては、用語の*イン*、*アウト*、*送信元*、*宛先*は次の意味になります。

- イン：インターフェイスに到達してスイッチ内を通過するトラフィック。送信元はそのトラフィックが発信された場所で、宛先は送信される先（ルータの反対側で）を意味します。

**ヒント**　入力トラフィック用インターフェイスに適用された IP-ACL はローカルおよびリモート両方のトラフィックに作用します。

- アウト：スイッチを通過済みで、インターフェイスから離れたトラフィック。送信元はこれが送信された場所であり、宛先は送信先を意味します。

**ヒント**　出力トラフィック用インターフェイスに適用された IP-ACL はローカル トラフィックだけに作用します。

# mgmt0 への IP-ACL の適用

mgmt0 と呼ばれるシステムのデフォルト ACL は、mgmt0 インターフェイスに存在します。mgmt0 は予約済みの ACL 名であり、使用することができないので、ユーザには表示されません。mgmt0 ACL はほとんどのポートをブロックし、許可されたセキュリティ ポリシーに準拠した必須のポートへのアクセスだけを可能にします。

Fabric Manager を使用してインターフェイスに IP-ACL を適用する手順は、次のとおりです。

**ステップ 1**　[Physical Attributes] ペインで [Switches] > [Security] を展開し、[IP ACL] を選択します。

[Information] ペインに、IP-ACL の設定が表示されます。

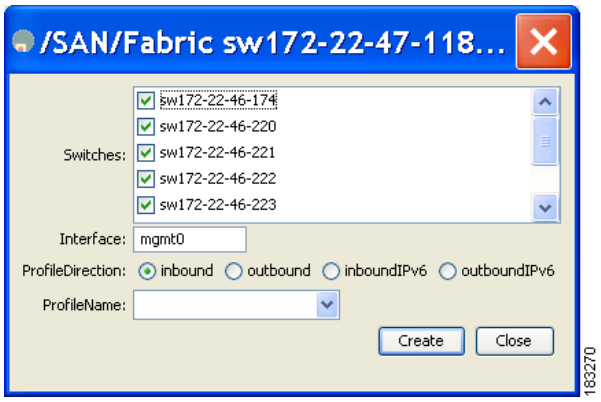
**ステップ 2**　[Interfaces] タブをクリックします。

インターフェイスおよび関連 IP-ACL のリストが表示されます。

**ステップ 3**　[Create Row] アイコンをクリックします。

[Create Interfaces] ダイアログボックスが表示されます（図 5-7 を参照）。

**図 5-7　[Create Interfaces] ダイアログボックス**




**ステップ 4**　（任意）IP-ACL に含めないスイッチを削除する場合は、スイッチ アドレス横のチェックボックスをオフにします。

IPv4-ACL または IPv6-ACL に関連付けるインターフェイスを [Interface] フィールドで設定します。

**ステップ 5**　[ProfileDirection]（[inbound] または [outbound] のいずれか）を選択します。

**ステップ 6**　[Profile Name] フィールドに IP-ACL の名前を入力します。

**（注）**　この IP-ACL 名は、すでに [Create Profiles] ダイアログボックスを使用して作成済みでなければなりません。作成されていない場合、[Create Profiles] ダイアログボックスを開いてプロファイルを作成するまで、どのフィルタもイネーブルになりません。

**ステップ 7**　[Creat] ボタンをクリックして IP-ACL に関連付けます。

新しく関連づけたアクセス リストが IP-ACL のリストの中に表示されます。

# IP-ACL 設定の例

管理アクセスを規制する IP-ACL を、Device Manager を使用して定義する手順は、次のとおりです。

**ステップ 1**　[Security] > [IP ACL] を選択します。

[IP-ACL] ダイアログボックスが表示されます（図 5-2 を参照）。

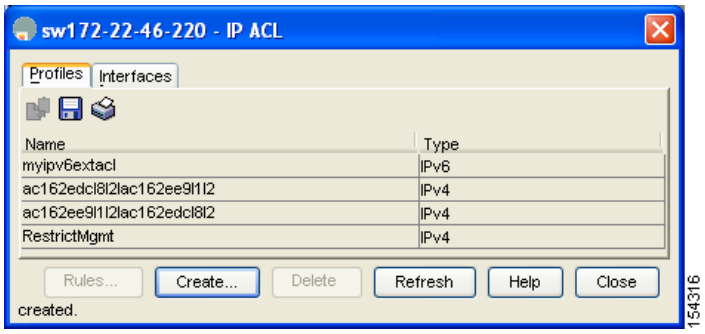
**ステップ 2**　[Create] ボタンをクリックして IP-ACL を作成します。

[Create IP ACL Profiles] ダイアログボックスが表示されます（図 5-3 を参照）。

**ステップ 3**　プロファイル名として **RestrictMgmt** を入力してから [Create] ボタンをクリックします。

RestrictMgmt という名前の空の IP-ACL が作成されます（図 5-8 を参照）。

**図 5-8　リストに追加された RestrictMgmt プロファイル**




**ステップ 4**　[RestrictMgmt] を選択してから [Rules] ボタンをクリックします。

このプロファイルに関連する IP フィルタの空のリストが表示されます。

**ステップ 5**　[Create] ボタンをクリックして最初の IP フィルタを作成します。

[Create IP Filter] ダイアログボックスが表示されます（図 5-5 を参照）。

**ステップ 6**　信頼できるサブネットからの管理コミュニケーションを許可するための IP フィルタを作成します。

**a.**　[Action] から [permit] オプション ボタンを選択し、[Protocol] ドロップダウン メニューで [0 IP] を選択します。

**b.**　送信元 IP アドレスを 10.67.16.0 に、ワイルドカード マスクを 0.0.0.255 に設定します。

**（注）**　ワイルドカード マスクには、一致させる IP アドレスのサブネットを指定します。フィルタは、指定したアドレス範囲に対して適用されます。

**c.**　宛先アドレスとして [any] チェックボックスをオンにします。

**d.**　[Create] ボタンをクリックしてこの IP フィルタを作成し、RestrictMgmt IP-ACL に追加します。

ステップ a ～ステップ d を繰り返して、10.67.16.0/24 サブネットのすべてのアドレスに通信を許可する IP フィルタを作成します。

**ステップ 7**　ICMP ping コマンドを許可するフィルタを次の手順で作成します。

**a.**　[Action] から [permit] オプション ボタンを選択し、[Protocol] ドロップダウン メニューで [1-ICMP] を選択します。

**b.** 送信元アドレスとして [any] チェックボックスをオンにします。

**c.** 宛先アドレスとして [any] チェックボックスをオンにします。

**d.** [ICMPType] ドロップダウン メニューで [8 echo] を選択します。

**e.** [Create] ボタンをクリックしてこの IP フィルタを作成し、RestrictMgmt IP-ACL に追加します。

ステップ a ～ステップ e を繰り返して、ICMP ping を許可する IP フィルタを作成します。

**ステップ 8**　他のすべてのトラフィックをブロックする最後の IP フィルタを次の手順で作成します。

**a.** [Action] から [deny] オプション ボタンを選択し、[Protocol] ドロップダウン メニューで [0 IP] を選択します。

**b.** 送信元アドレスとして [any] チェックボックスをオンにします。

**c.** 宛先アドレスとして [any] チェックボックスをオンにします。

**d.** [Create] ボタンをクリックしてこの IP フィルタを作成し、RestrictMgmt IP-ACL に追加します。

**e.** [Close] ボタンをクリックして、[Create IP Filter] ダイアログボックスを閉じます。

ステップ a ～ステップ d を繰り返して、他のすべてのトラフィックをブロックする IP フィルタを作成します。

**ステップ 9**　次の手順で mgmt0 インターフェイスに RestrictMgmt IP ACL を適用します。

**a.** [Security] をクリックし、[IP ACL] を選択してから [IP ACL] ダイアログボックスで [Interfaces] タブをクリックします。

**b.** [Create] ボタンをクリックします。

[Create IP-ACL Interfaces] ダイアログボックスが表示されます。

**c.** [Interfaces] ドロップダウン メニューで [mgmt0] を選択します。

**d.** [Profile Director] の [inbound] オプション ボタンを選択します。

**e.** [ProfileName] ドロップダウン メニューで [RestrictMgmt] を選択します。

**f.** [Create] ボタンをクリックして RestrictMgmt IP-ACL を mgmt0 インターフェイスに適用します。

ステップ a ～ステップ f を繰り返して、IP-ACL を mgmt0 インターフェイスに適用します。