ACL の設定

この章では、ML シリーズ カードに組み込まれている Access Control List（ACL; アクセス制御リスト）について説明します。

この章の内容は次のとおりです。

ACL の概要

ACL は、ネットワークの制御とセキュリティを実現する機能で、ML シリーズのインターフェイスに出入りするパケットのフローをフィルタリングできます。フィルタとも呼ばれる ACL により、特定のユーザや装置によるネットワークの使用を制限できます。ACL はプロトコルごとに作成し、着信トラフィックまたは発信トラフィックのどちらか一方のインターフェイスに適用します。ACL はコントロール プレーンの発信トラフィックには適用されません。1 つの方向、1 つのサブインターフェイスごとに適用できる ACL フィルタは 1 つだけです。

ACL を作成する場合は、ML シリーズ カードが処理する各パケットに適用する基準を定義します。これによって ML シリーズ カードでは、パケットがリストの基準に一致するかどうかに基づいて、パケットを転送するか、ブロックするかを決定します。リストのどの基準にも一致しないパケットは、各 ACL の末尾にある暗黙的な [deny all traffic] 基準ステートメントによって、自動的にブロックされます。

ML シリーズにおける ACL サポート

制御プレーン ACL とデータ プレーン ACL は、どちらも ML シリーズ カードでサポートされます。

- 制御プレーン ACL：ML シリーズ カードの CPU によって処理される制御データをフィルタするための ACL（たとえば、ルーティング情報、Internet Group Membership Protocol [IGMP] 加入の配布など）。
- データ プレーン ACL：ML シリーズのハードウェアを使用してルーティングまたはブリッジされているユーザ データをフィルタするための ACL（たとえば、ホストへのアクセスの拒否など）。データ プレーン ACL は、**ip access-group** コマンドを使用して入力方向または出力方向のインターフェイスに適用されます。

データ プレーン ACL を ML シリーズ カード上で使用する際には、次の制限があります。

- ACL は、ブリッジド インターフェイスを含む、あらゆる種類のインターフェイスでサポートされます。
- 再帰的 ACL とダイナミック ACL は、ML シリーズ カードではサポートされません。
- アクセス違反のアカウンティングは、ML シリーズ カードではサポートされません。
- ACL のロギングは、交換されたパケットではなく、CPU に送信するパケットに対してのみサポートされます。
- 出力ブリッジド インターフェイスに適用された IP 標準 ACL は、データ プレーンではサポートされません。ブリッジングの場合は、ACL は入力側でのみサポートされます。

IP ACL

IP に対しては、次のような ACL 形式がサポートされています。

- 標準 IP ACL：送信元アドレスを使用してマッチングを行います。
- 拡張 IP ACL（制御プレーン専用）：送信元アドレスおよび宛先アドレスを使用してマッチングを行います。さらに細かく制御するためには、任意でプロトコル タイプとポート番号を使用します。
- 名前付き ACL：送信元アドレスを使用してマッチングを行います。

（注）　デフォルトでは、ACL の末尾には、末尾に到達する前に一致するステートメントが見つからなかった場合のための暗黙的な拒否ステートメントがあります。標準 ACL では、関連付けられた IP ホスト アドレスの ACL 指定からマスクを省略すると、マスクが 0.0.0.0 であるとみなされます。

ACL を作成したら、その ACL をインターフェイスに適用する必要があります。「インターフェイスへの ACL の適用」（p.16-5）を参照してください。

名前付き IP ACL

IP ACL は名前で特定できます。ただし、名前は英数字の文字列である必要があります。名前付き IP ACL を使用すると、番号付き ACL の場合よりも多くの IP ACL を 1 つのルータに設定できます。数値の文字列ではなく英字の文字列で ACL を特定する場合は、モードとコマンドの構文が多少異なります。

次の事項を検討してから名前付き ACL を設定してください。

- 標準 ACL と拡張 ACL に同じ名前を付けることはできません。
- 番号付き ACL も利用できます。「番号付き標準および拡張 IP ACL の作成」（p.16-3）を参照してください。

ユーザの注意事項

IP ネットワークのアクセス制御を設定するときは、次のことに留意してください。

- Ternary CAM（TCAM）内に ACL エントリをプログラムできます。
- ACL の末尾には、すべてを拒否するステートメントが暗黙的に指定されているため、入力する必要がありません。
- ACL エントリはどのような順序で入力しても、パフォーマンスに影響しません。
- 8 個の TCAM エントリごとに、ML シリーズ カードは TCAM の管理用のエントリを 1 個使用します。
- パケット損失を引き起こす条件を設定しないでください。パケット損失は、特定のサービスのパケットを拒否する ACL が設定されたネットワークで、そのサービスをアドバタイズするように装置またはインターフェイスが設定されている場合に発生します。
- IP ACL は、ダブルタグ（QinQ）パケットに対してサポートされていません。ただし、IP ACL は QinQ アクセス ポートに着信する IP パケットに対して適用されます。

IP ACL の作成

ここでは、番号付き標準 IP ACL、拡張 IP ACL、および名前付き標準 IP ACL の作成方法について説明します。

- 番号付き標準および拡張 IP ACL の作成（p.16-3）
- 名前付き標準 IP ACL の作成（p.16-4）
- 名前付き拡張 IP ACL の作成（制御プレーン専用）（p.16-4）
- インターフェイスへの ACL の適用（p.16-5）

番号付き標準および拡張 IP ACL の作成

表 16-1 に、番号付き標準 IP ACL と拡張 IP ACL の作成に使用するグローバル コンフィギュレーション コマンドを示します。

表 16-1　番号付き標準および拡張 IP ACL のコマンド

コマンドの説明	目的
Router(config)# **access-list** *access-list-number* {**deny** | **permit**} *source* [*source-wildcard*]	送信元アドレスとワイルドカードを使用して標準 IP ACL を定義します。
Router(config)# **access-list** *access-list-number* {**deny** | **permit**} **any**	0.0.0.0 255.255.255.255 という送信元と送信元マスクの省略形を使用して標準 IP ACL を定義します。
Router(config)# **access-list** *extended-access-list-number* {**deny** | **permit**} *protocol source source-wildcard destination destination-wildcard* [**precedence** *precedence*] [**tos** *tos*]	拡張 IP ACL 番号とアクセス条件を定義します。
Router(config)# **access-list** *extended-access-list-number* {**deny** | **permit**} *protocol* **any any**	0.0.0.0 255.255.255.255 という送信元と送信元ワイルドカードの省略形と、0.0.0.0 255.255.255.255 という宛先と宛先ワイルドカードの省略形を使用して、拡張 IP ACL を定義します。
Router(config)# **access-list** *extended-access-list-number* {**deny** | **permit**} *protocol* **host** *source* **host** *destination*	source 0.0.0.0 という送信元と送信元ワイルドカードの省略形と、destination 0.0.0.0 という宛先と宛先ワイルドカードの省略形を使用して、拡張 IP ACL を定義します。

名前付き標準 IP ACL の作成

名前付き標準 IP ACL を作成するには、グローバル コンフィギュレーション モードで次の手順を実行します。

	コマンドの説明	目的
ステップ 1	`Router(config)# ip access-list standard name`	英字の名前を使用して標準 IP ACL を定義します。

ステップ 2	`Router(config-std-nac1)# deny {source [source-wildcard] | any}`
	
	または
	
	`permit {source [source-wildcard] | any}`
		アクセス リスト設定モードで、許可または拒否する条件を 1 つ以上指定します。これによって、パケットを通過させるか、廃棄するかが決定します。

ステップ 3	`Router(config)# exit`	アクセス リスト コンフィギュレーション モードを終了します。

名前付き拡張 IP ACL の作成（制御プレーン専用）

名前付き拡張 IP ACL を作成するには、グローバル コンフィギュレーション モードで次の手順を実行します。

	コマンドの説明	目的
ステップ 1	`Router(config)# ip access-list extended name`	英字の名前を使用して拡張 IP ACL を定義します。
ステップ 2	`Router(config-ext-nacl)# {deny | permit} protocol source source-wildcard destination destination-wildcard [precedence precedence] [tos tos]`	アクセス リスト コンフィギュレーション モードで、許可または拒否する条件を指定します。
	または `{deny | permit} protocol any any`	または 0.0.0.0 255.255.255.255 という送信元と送信元ワイルドカードの省略形と、0.0.0.0 255.255.255.255 という宛先と宛先ワイルドカードの省略形を使用して、拡張 IP ACL を定義します。
	または `{deny | permit} protocol host source host destination`	または *source* 0.0.0.0 という送信元と送信元ワイルドカードの省略形と、*destination* 0.0.0.0 という宛先と宛先ワイルドカードの省略形を使用して、拡張 IP ACL を定義します。

インターフェイスへの ACL の適用

ACL を作成したら、その ACL を 1 つ以上のインターフェイスに適用できます。ACL を適用できるのは、インターフェイスの着信方向または発信方向のどちらか一方です。インターフェイスへのアクセスを制御するには、名前または番号を使用します。標準 ACL を適用した場合、ML シリーズカードは送信元 IP アドレスを ACL と比較します。ACL を 1 つ以上のインターフェイスに適用するには、表 16-2 に示すコマンドを使用します。

（注）　Bridge Group Virtual Interface（BVI; ブリッジ グループ仮想インターフェイス）の入力側に適用された IP 標準 ACL は、BVI 入力トラフィックだけでなく、関連付けられたブリッジ グループ内のブリッジされたすべての IP トラフィックに適用されます。

表 16-2　インターフェイスへの ACL の適用

コマンドの説明	目的
ip access-group {*access-list-number* | *name*} {**in** | **out**}	インターフェイスへのアクセスを制御します。

ACL TCAM サイズの変更

TCAM サイズを変更するには、**sdm access-list** コマンドを入力します。ACL TCAM サイズの詳細については、「TCAM の ACL のサイズ設定」（p.15-4）を参照してください。例 16-1 には、ACL の変更と確認の例を示します。

（注） ACL TCAM サイズを増やすには、IP、IP マルチキャスト、L2 スイッチングなどの別の領域の TCAM サイズを縮小する必要があります。

注意 次のエラー メッセージが表示された場合は、TCAM サイズを増やす必要があります。

```
Warning:Programming TCAM entries failed
Please remove last ACL command to re-activate ACL operation.
!<ACL number or name> <IP or IPX> <INPUT_ACL or OUTPUT_ACL> from TCAM group for
!<interface>
Please see the documentation to see if TCAM space can be
increased on this platform to alleviate the problem.
```

例 16-1　ACL のモニタリングと確認

```
Router# show ip access-lists 1
Standard IP access list 1
    permit 192.168.1.1
    permit 192.168.1.2
```