CHAPTER 21

# アクセス コントロール リスト（ACL）の設定

この章では、Access Control List（ACL; アクセス コントロール リスト）の設定方法について説明します。

この章で説明する内容は、次のとおりです。



## ACL について

ACL とは、トラフィックのフィルタリングに使用する順序付きのルール セットのことです。各ルールには、パケットがルールに一致するために満たさなければならない条件のセットが規定されています。スイッチは、あるパケットに対してある ACL を適用するかどうかを判断するとき、そのパケットを ACL 内のすべてのルールの条件に対してテストします。一致する条件が最初に見つかった時点で、パケットを許可するか拒否するかが決まります。一致する条件が見つからないと、スイッチは適用可能なデフォルトのルールを適用します。許可されたパケットについては処理が続行され、拒否されたパケットはドロップされます。詳細については、「暗黙のルール」（P.21-3）を参照してください。

ACL を使用すると、ネットワークおよび特定のホストを、不要なトラフィックや望ましくないトラフィックから保護できます。たとえば、ACL を使用して、厳重にセキュリティ保護されたネットワークからインターネットに HyperText Transfer Protocol（HTTP; ハイパー テキスト トランスファ プロトコル）トラフィックが流入するのを禁止できます。また、特定のサイトへの HTTP トラフィックだけを許可することもできます。その場合は、サイトの IP アドレスが、IP ACL に指定されているかどうかによって判定します。

ここでは、次の内容について説明します。

# IP ACL のタイプと適用

Cisco Nexus 4001I/4005I Switch Module for IBM BladeCenterは、セキュリティ トラフィック フィルタリング用に、IPv4 および MAC の各 ACL をサポートしています。また、IP ACL を、ポート ACL および Virtual Local Area Network（VLAN; 仮想ローカル エリア ネットワーク）ACL として使用することもできます（表 21-1 を参照）。

**表 21-1　セキュリティ ACL の適用**

| 適用例 | サポートするインターフェイス | サポートする ACL のタイプ |
|---|---|---|
| ポート ACL（PACL） | ACL は、次のいずれかに適用した場合、ポート ACL と見なされます。<br>• イーサネット インターフェイス<br>• イーサネット ポート チャネル インターフェイス<br>ポート ACL をトランク ポートに適用すると、その ACL は、当該トランク ポート上のすべての VLAN 上のトラフィックをフィルタリングします。 | IPv4 ACL<br>MAC ACL |
| VLAN ACL（VACL） | アクセス マップを使用して ACL をアクションにアソシエートし、そのアクセス マップを VLAN に適用する場合、その ACL は VACL と見なされます。 | IPv4 ACL<br>MAC ACL |

## 適用順序

スイッチは、パケットを処理するとき、そのパケットの転送パスを決定します。このパスによって、スイッチがトラフィックに適用する ACL が決まります。スイッチは、まず、ポート ACL を適用します。

# ルール

アクセス リスト コンフィギュレーション モードでルールを作成するには、**permit** または **deny** コマンドを使用します。スイッチは、許可ルールに指定された基準に一致するトラフィックを許可し、拒否ルールに指定された基準に一致するトラフィックをブロックします。ルールに一致するためにトラフィックが満たさなければならない基準を設定するためのオプションが多数用意されています。

ここでは、次の内容について説明します。



## 送信元と宛先

各ルールには、ルールに一致するトラフィックの送信元と宛先を指定します。指定する送信元および宛先には、特定のホスト、ホストのネットワークまたはグループ、あるいは任意のホストを使用できます。

## プロトコル

ACL では、プロトコルによってトラフィックを識別できます。指定の際の手間を省くために、一部のプロトコルは名前で指定できます。たとえば、IPv4 ACL では、ICMP を名前で指定できます。

プロトコルはすべて番号で指定できます。IPv4 ACL では、インターネット プロトコル番号を表す整数でプロトコルを指定できます。たとえば、Layer 2 Tunneling Protocol（L2TP; レイヤ 2 トンネリング プロトコル）を指定するには、115 を使用します。

## 暗黙のルール

IP ACL および MAC ACL には暗黙のルールがあります。暗黙のルールとは、実行コンフィギュレーションには（明示的には）指定されていないが、ACL の他のルールが一致しないとき、トラフィックに適用されるルールのことです。

すべての IPv4 ACL には、次の暗黙のルールがあります。

```
deny ip any any
```

この暗黙のルールによって、どの条件にも一致しない IP トラフィックは拒否されます。

すべての MAC ACL には、次の暗黙のルールがあります。

```
deny mac any any
```

この暗黙のルールによって、どの条件にも一致しない MAC トラフィックは拒否されます。

## その他のフィルタリング オプション

追加のオプションを使用してトラフィックを識別できます。

IPv4 ACL には、次の追加フィルタリング オプションが用意されています。

- レイヤ 4 プロトコル
- TCP/UDP ポート
- ICMP タイプおよびコード
- IGMP タイプ
- 優先レベル
- Differentiated Services Code Point（DSCP; DiffServ コード ポイント）値
- ACK、FIN、PSH、RST、SYN、または URG ビットがセットされた TCP パケット
- 確立済み TCP 接続

MAC ACL は L3 プロトコルをサポートします。

## シーケンス番号

本スイッチでは、ルールにシーケンス番号を付けることができます。入力されたすべてのルールには、ユーザによって、またはスイッチによって自動的に、シーケンス番号が付けられます。シーケンス番号によって、次の ACL 設定作業が容易になります。

- 既存のルールの間に新規のルールを追加する：シーケンス番号を指定することによって、ACL 内での新規ルールの挿入場所を指定します。たとえば、ルール番号 100 と 110 の間に新しいルールを挿入する必要がある場合は、シーケンス番号 105 を新しいルールに割り当てます。

- ルールを削除する：シーケンス番号を使用しない場合は、ルールを削除するのに、次のようにルール全体を入力する必要があります。

  ```
  switch(config-acl)# no permit tcp 10.0.0.0/8 any
  ```

  このルールに 101 番のシーケンス番号が付いていれば、次コマンドだけでルールを削除できます。

  ```
  switch(config-acl)# no 101
  ```

- ルールを移動する：シーケンス番号を使用すれば、同じ ACL 内の異なる場所にルールを移動する必要がある場合に、そのルールのコピーをシーケンス番号で正しい位置に挿入してから、元のルールを削除できます。この方法により、トラフィックを中断せずにルールを移動できます。

シーケンス番号なしでルールを入力すると、そのルールは ACL の末尾に追加され、直前のルールのシーケンス番号に 10 を足した番号が付けられます。たとえば、ACL の最後のルールのシーケンス番号が 225 の場合にシーケンス番号なしでルールを追加すると、新しいルールにシーケンス番号 235 が付けられます。

また、スイッチでは、ACL 内ルールのシーケンス番号を再割り当てできます。シーケンス番号の再割り当ては、ACL 内に、100、101 のように連続するシーケンス番号のルールがある場合、それらのルールの間に 1 つ以上のルールを挿入する必要があるときに便利です。

### 論理演算子と論理演算ユニット

TCP および UDP トラフィックの IP ACL ルールでは、論理演算子を使用して、ポート番号に基づきトラフィックをフィルタリングできます。

スイッチは、演算子とオペランドの組み合わせを、Logical Operator Unit（LOU; 論理演算ユニット）と呼ばれるレジスタ内に格納します。

eq 演算子で LOU を使用しても、LOU への格納は行われません。range 演算子は境界値も含みます。

演算子とオペランドの組み合わせが LOU に格納されるかどうかの判断基準を次に示します。

- 演算子またはオペランドが、他のルールで使用されている演算子とオペランドの組み合わせと異なる場合、この組み合わせは LOU に格納されます。

  たとえば、演算子とオペランドの組み合わせ gt 10 と gt 11 は、それぞれ LOU の半分を使用して別々に格納されます。gt 10 と lt 10 も別々に格納されます。

- 演算子とオペランドの組み合わせがルール内の送信元ポートと宛先ポートのうちどちらに適用されるかは、LOU の使用方法に影響を与えます。同じ組み合わせの一方が送信元ポートに、他方が宛先ポートに別々に適用される場合は、2 つの同じ組み合わせが別々に格納されます。

  たとえば、あるルールによって、演算子とオペランドの組み合わせ gt 10 が送信元ポートに、別のルールによって同じ組み合わせ gt 10 が宛先ポートに適用される場合、両方の組み合わせが LOU の半分に格納され、結果として 1 つの LOU 全体が使用されることになります。このため、gt 10 を使用するルールが追加されても、それ以上 LOU は使用されません。

# IPv4 ACL の設定

ここでは、次の内容について説明します。

# IPv4 ACL の作成

スイッチに IPv4 ACL を作成し、その ACL にルールを追加できます。IP ACL を作成する手順は、次のとおりです。

| | コマンド | 目的 |
|---|---|---|
| ステップ 1 | `switch# configure terminal` | 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)# ip access-list` *name* | IP ACL を作成して、IP ACL コンフィギュレーション モードを開始します。*name* 引数は 64 文字以内で指定します。 |
| ステップ 3 | `switch(config-acl)# [`*sequence-number*`] {permit\|deny}` *protocol source destination* | IP ACL 内にルールを作成します。多数のルールを作成できます。*sequence-number* 引数には、1 ～ 4294967295 の整数を指定します。<br>**permit** コマンドと **deny** コマンドには、トラフィックを識別するための多くの方法が用意されています。詳細は、『*Cisco Nexus 4000I and 4005I Switch Module for IBM BladeCenter NX-OS Command Reference*』を参照してください。 |
| ステップ 4 | `switch(config-acl)# statistics per-entry` | （任意）ACL に規定されたルールに一致するパケットのグローバルな統計情報をスイッチ内に保持するように指定します。 |
| ステップ 5 | `switch(config-acl)# show ip access-lists` *name* | （任意）IP ACL の設定を表示します。 |
| ステップ 6 | `switch(config-acl)# copy running-config startup-config` | （任意）実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーします。 |

次に、IPv4 ACL を作成する例を示します。

```
switch# configure terminal
switch(config)# ip access-list acl-01
switch(config-acl)# permit ip 192.0.2.0/24 any
switch(config-acl)# statistics per-entry
switch(config-acl)# show ip access-lists acl-01
switch(config-acl)# copy running-config startup-config
```

# IP ACL の変更

既存の IPv4 ACL に対してルールの追加または削除を行うことができます。既存のルールは変更できません。ルールを変更するには、そのルールを削除してから、変更を加えたルールを再作成します。

既存のルールの間に新しいルールを挿入する必要がある場合で、現在のシーケンス番号の空き状況ではすべてを挿入できないときは、**resequence** コマンドを使用してシーケンス番号を再割り当てします。詳細については、「IP ACL 内のシーケンス番号の変更」（P.21-7）を参照してください。

IP ACL を変更する手順は、次のとおりです。

| | コマンド | 目的 |
|---|---|---|
| ステップ 1 | `switch# configure terminal` | 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)# ip access-list` *name* | 名前で指定した ACL の IP ACL 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-acl)# [`*sequence-number*`] {permit\|deny}` *protocol source destination* | （任意）IP ACL 内にルールを作成します。シーケンス番号を指定すると、ACL 内のルール挿入位置を指定できます。シーケンス番号を指定しないと、ルールは ACL の末尾に追加されます。*sequence-number* 引数には、1 ～ 4294967295 の整数を指定します。<br>**permit** コマンドと **deny** コマンドには、トラフィックを識別するための多くの方法が用意されています。詳細は、『*Cisco Nexus 4000I and 4005I Switch Module for IBM BladeCenter NX-OS Command Reference*』を参照してください。 |
| ステップ 4 | `switch(config-acl)# no {`*sequence-number* `\| {permit\|deny}` *protocol source destination*`}` | （任意）指定したルールを IP ACL から削除します。<br>**permit** コマンドと **deny** コマンドには、トラフィックを識別するための多くの方法が用意されています。詳細は、『*Cisco Nexus 4000I and 4005I Switch Module for IBM BladeCenter NX-OS Command Reference*』を参照してください。 |
| ステップ 5 | `switch(config-acl)# [no] statistics` | （任意）ACL に規定されたルールに一致するパケットのグローバルな統計情報をスイッチ内に保持するように指定します。<br>**no** オプションを指定すると、ACL のグローバルな統計情報がスイッチ内に保持されなくなります。 |
| ステップ 6 | `switch(config-acl)# show ip access-lists` *name* | （任意）IP ACL の設定を表示します。 |
| ステップ 7 | `switch(config-acl)# copy running-config startup-config` | （任意）実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーします。 |

# IP ACL の削除

スイッチから IP ACL を削除できます。

スイッチから IP ACL を削除する前に、ACL がインターフェイスに適用されているかどうかを確認してください。削除できるのは、現在適用されている ACL だけです。ACL を削除しても、その ACL が適用されていたインターフェイスの設定は影響を受けません。スイッチは、削除対象の ACL が空であると見なします。

スイッチから IP ACL を削除する手順は、次のとおりです。

| | コマンド | 目的 |
|---|---|---|
| ステップ 1 | `switch# configure terminal` | 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)# no ip access-list name` | 名前で指定した IP ACL を実行コンフィギュレーションから削除します。 |
| ステップ 3 | `switch(config)# show running-config` | （任意）ACL の設定を表示します。削除された IP ACL は表示されないはずです。 |
| ステップ 4 | `switch(config)# copy running-config startup-config` | （任意）実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーします。 |

# IP ACL 内のシーケンス番号の変更

IP ACL 内のルールに付けられたすべてのシーケンス番号を変更できます。シーケンス番号を変更する手順は、次のとおりです。

| | コマンド | 目的 |
|---|---|---|
| ステップ 1 | `switch# configure terminal` | 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)# resequence ip access-list name starting-sequence-number increment` | ACL 内に記述されているルールにシーケンス番号を付けます。指定した開始シーケンス番号が最初のルールに付けられます。後続の各ルールには、直前のルールよりも大きい番号が付けられます。番号の間隔は、指定した増分によって決まります。*starting-sequence-number* 引数と *increment* 引数は、1 ～ 4294967295 の整数で指定します。 |
| ステップ 3 | `switch(config)# show ip access-lists name` | （任意）IP ACL の設定を表示します。 |
| ステップ 4 | `switch(config)# copy running-config startup-config` | （任意）実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーします。 |

# IP ACL のポート ACL としての適用

IPv4 ACL は、物理イーサネット インターフェイスまたはポート チャネルに適用できます。これらのインターフェイス タイプに適用された ACL は、ポート ACL と見なされます。IP ACL を適用する手順は、次のとおりです。

| | コマンド | 目的 |
|---|---|---|
| ステップ 1 | `switch# configure terminal` | 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 ethernet` *slot/port* | 指定したインターフェイス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。 |
| | `switch(config)# interface port-channel` *channel-number* | ポート チャネル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)# [ip \| mac] port access-group access-list in` | IPv4 ACL を、インターフェイスまたはポート チャネルに適用します。ポート ACL では、インバウンド フィルタリングだけがサポートされています。1 つのインターフェイスに 1 つのポート ACL を適用できます。 |
| ステップ 4 | `switch(config-if)# show running-config` | （任意）ACL の設定を表示します。 |
| ステップ 5 | `switch(config-if)# copy running-config startup-config` | （任意）実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーします。 |

次に、IPv4 ACL をポート チャネルに適用する例を示します。

```
switch# configure terminal
switch(config)# interface port-channel 5
switch(config-if)# ip port access-group acl-l2-marketing-group in
switch(config-if)# show running-config
switch(config-if)# copy running-config startup-config
```

次に、acl-01 という名前の IPv4 ACL を作成して、イーサネット インターフェイス 1/1（レイヤ 2 インターフェイス）に適用する例を示します。

```
ip access-list acl-01
  permit ip 192.168.2.0/24 any
interface ethernet 1/1
  ip access-group acl-01 in
```

# IP ACL の VACL としての適用

VACL の設定については、「VACL の設定」（P.21-15）を参照してください。

## IP ACL の設定の確認

IP ACL の設定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 running-config` | ACL の設定（IP ACL の設定と IP ACL が適用されるインターフェイス）を表示します。 |
| `switch# show ip access-lists` | IP ACL の設定を表示します。 |
| `switch# show running-config interface` | ACL が適用されたインターフェイスの設定を表示します。 |

これらのコマンドの出力に表示される各フィールドの詳細については、『*Cisco Nexus 4000I and 4005I Switch Module for IBM BladeCenter NX-OS Command Reference*』を参照してください。

## IP ACL 統計情報の表示と消去

IP ACL に関する統計情報（各ルールに一致したパケットの数など）を表示するには、**show ip access-lists** コマンドを使用します。このコマンドの出力に表示される各フィールドの詳細については、『*Cisco Nexus 4000I and 4005I Switch Module for IBM BladeCenter NX-OS Command Reference*』を参照してください。

（注）　MAC アクセス リストは、非 IPv4 トラフィックだけに適用可能です。

VACL 統計情報を表示または消去するには、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` | IP ACL の設定を表示します。IP ACL に **statistics** コマンドが指定されている場合は、**show ip access-lists** コマンドの出力に、各ルールに一致したパケットの数が表示されます。 |
| `switch# clear ip access-list counters` | すべての IP ACL、または特定の IP ACL の統計情報を消去します。 |

これらのコマンドの詳細については、『*Cisco Nexus 4000I and 4005I Switch Module for IBM BladeCenter NX-OS Command Reference*』を参照してください。

# MAC ACL の設定

ここでは、次の内容について説明します。

# MAC ACL の作成

MAC ACL を作成し、その MAC ACL にルールを追加する手順は、次のとおりです。

| | コマンド | 目的 |
|---|---|---|
| ステップ 1 | `switch# configure terminal` | 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# mac access-list name` | MAC ACL を作成して、ACL 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-mac-acl)# [sequence number] {permit \| deny} source destination protocol` | MAC ACL 内にルールを作成します。<br>**permit** オプションと **deny** オプションには、トラフィックを識別するための多くの方法が用意されています。詳細は、『*Cisco Nexus 4000I and 4005I Switch Module for IBM BladeCenter NX-OS Command Reference*』を参照してください。 |
| ステップ 4 | `switch(config-mac-acl)# statistics per-entry` | （任意）ACL に規定されたルールに一致するパケットのグローバルな統計情報をスイッチ内に保持するように指定します。 |
| ステップ 5 | `switch(config-mac-acl)# show mac access-lists name` | （任意）MAC ACL の設定を表示します。 |
| ステップ 6 | `switch(config-mac-acl)# copy running-config startup-config` | （任意）実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーします。 |

次に、MAC ACL を作成して、ルールを追加する例を示します。

```
switch# configure terminal
switch(config)# mac access-list acl-mac-01
switch(config-mac-acl)# permit 00c0.4f00.0000 0000.00ff.ffff any
switch(config-mac-acl)# statistics per-entry
switch(config-mac-acl)# show mac access-lists acl-mac-01
switch(config-mac-acl)# copy running-config startup-config
```

# MAC ACL の変更

既存の MAC ACL 内で、ルールの追加または削除を実行できます。既存のルールは変更できません。ルールを変更するには、そのルールを削除してから、変更を加えたルールを再作成します。

既存のルールの間に新しいルールを挿入する必要がある場合で、現在のシーケンス番号の空き状況ではすべてを挿入できないときは、**resequence** コマンドを使用してシーケンス番号を再割り当てします。詳細については、「IP ACL 内のシーケンス番号の変更」（P.21-7）を参照してください。

MAC ACL を変更する手順は、次のとおりです。

| | コマンド | 目的 |
|---|---|---|
| ステップ 1 | `switch# configure terminal` | 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)# mac access-list` *name* | 名前で指定した ACL の ACL 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-mac-acl)# [`*sequence-number*`] {permit\|deny}` *source destination protocol* | （任意）MAC ACL 内にルールを作成します。シーケンス番号を指定すると、ACL 内のルール挿入位置を指定できます。シーケンス番号を指定しないと、ルールは ACL の末尾に追加されます。<br>**permit** コマンドと **deny** コマンドには、トラフィックを識別するための多くの方法が用意されています。 |
| ステップ 4 | `switch(config-mac-acl)# no {`*sequence-number* `\| {permit\|deny}` *protocol source destination*`}` | （任意）MAC ACL から指定したルールを削除します。<br>**permit** コマンドと **deny** コマンドには、トラフィックを識別するための多くの方法が用意されています。 |
| ステップ 5 | `switch(config-mac-acl)# [no] statistics per-entry` | （任意）ACL に規定されたルールに一致するパケットのグローバルな統計情報をスイッチ内に保持するように指定します。<br>**no** オプションを指定すると、ACL のグローバルな統計情報がスイッチ内に保持されなくなります。 |
| ステップ 6 | `switch(config-mac-acl)# show mac access-lists` *name* | （任意）MAC ACL の設定を表示します。 |
| ステップ 7 | `switch(config-mac-acl)# copy running-config startup-config` | （任意）実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーします。 |

次に、MAC ACL を変更する例を示します。

```
switch# configure terminal
switch(config)# mac access-list acl-mac-01
switch(config-mac-acl)# 100 permit mac 00c0.4f00.00 0000.00ff.ffff any
switch(config-mac-acl)# statistics per-entry
switch(config-mac-acl)# show mac access-lists acl-mac-01
switch(config-mac-acl)# copy running-config startup-config
```

# MAC ACL の削除

スイッチから MAC ACL を削除できます。

ACL がインターフェイスに適用されているかどうかを確認してください。削除できるのは、現在適用されている ACL だけです。ACL を削除しても、その ACL が適用されていたインターフェイスの設定は影響を受けません。スイッチは、削除対象の ACL が空であると見なします。

MAC ACL を削除する手順は、次のとおりです。

| | コマンド | 目的 |
|---|---|---|
| ステップ 1 | `switch# configure terminal` | 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)# no mac access-list` *name* | 名前で指定した MAC ACL を実行コンフィギュレーションから削除します。 |
| ステップ 3 | `switch(config)# show mac access-lists` | （任意）MAC ACL の設定を表示します。 |
| ステップ 4 | `switch(config)# copy running-config startup-config` | （任意）実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーします。 |

# MAC ACL 内のシーケンス番号の変更

MAC ACL 内のルールに付けられたすべてのシーケンス番号を変更できます。ACL にルールを挿入する必要がある場合で、シーケンス番号が不足しているときは、再割り当てすると便利です。詳細については、「ルール」（P.21-2）を参照してください。

MAC ACL 内のルールに付けられたすべてのシーケンス番号を変更する手順は、次のとおりです。

| | コマンド | 目的 |
|---|---|---|
| ステップ 1 | `switch# configure terminal` | 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)# resequence mac access-list` *name starting-sequence-number increment* | ACL 内に記述されているルールにシーケンス番号を付けます。starting-sequence number に指定したシーケンス番号が最初のルールに付けられます。後続の各ルールには、直前のルールよりも大きい番号が付けられます。番号の間隔は、指定した増分によって決まります。 |
| ステップ 3 | `switch(config)# show mac access-lists` *name* | （任意）MAC ACL の設定を表示します。 |
| ステップ 4 | `switch(config)# copy running-config startup-config` | （任意）実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーします。 |

# MAC ACL のポート ACL としての適用

MAC ACL をポート ACL として、次のいずれかのインターフェイス タイプに適用できます。

- レイヤ 2 インターフェイス
- ポート チャネル インターフェイス

適用する ACL が存在しており、この適用で要求されているとおりにトラフィックをフィルタリングするように設定されていることを確認してください。MAC ACL の設定の詳細については、「IPv4 ACL の設定」（P.21-4）を参照してください。

MAC ACL をポート ACL として適用する手順は、次のとおりです。

| | コマンド | 目的 |
|---|---|---|
| ステップ 1 | `switch# configure terminal` | 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 ethernet`*slot/port* | 指定したインターフェイス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。 |
| | `switch(config)# interface port-channel`*channel-number*} | ポート チャネル インターフェイス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)# [ip \| mac] port access-group` *access-list* | MAC ACL をインターフェイスに適用します。 |
| ステップ 4 | `switch(config-if)# show running-config` | （任意）ACL の設定を表示します。 |
| ステップ 5 | `switch(config-if)# copy running-config startup-config` | （任意）実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーします。 |

# MAC ACL の VACL としての適用

MAC ACL を VACL として適用できます。MAC ACL を使用して VACL を作成する方法の詳細については、「VACL の作成または変更」（P.21-15）を参照してください。

# MAC ACL の設定の確認

MAC ACL の設定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 |
|---|---|
| **show mac access-lists** | MAC ACL の設定を表示します。 |
| **show running-config** | ACL の設定（MAC ACL と MAC ACL が適用されるインターフェイス）を表示します。 |
| **show running-config interface** | ACL を適用したインターフェイスの設定を表示します。 |

# MAC ACL 統計情報の表示と消去

MAC ACL に関する統計情報（各ルールに一致したパケットの数など）を表示するには、**show mac access-lists** コマンドを使用します。

MAC ACL 統計情報を表示または消去するには、次のいずれかの作業を行います。

| コマンド | 目的 |
|---|---|
| **show mac access-lists** | MAC ACL の設定を表示します。MAC ACL に **statistics** コマンドが指定されている場合は、**show mac access-lists** コマンドの出力に、各ルールに一致したパケットの数が表示されます。 |
| **clear mac access-list counters** | すべての MAC ACL、または特定の MAC ACL の統計情報を消去します。 |

次に、acl-mac-01 という名前の MAC ACL を作成して、イーサネット インターフェイス 2/1（レイヤ 2 インターフェイス）に適用する例を示します。

```
mac access-list acl-mac-01
  permit 00c0.4f00.0000 0000.00ff.ffff any
interface ethernet 2/1
  mac access-group acl-mac-01
```

# VLAN ACL について

VLAN ACL（VACL）は、MAC ACL または IP ACL の適用例の 1 つです。VACL を設定して、VLAN 内でブリッジされているすべてのパケットに適用できます。VACL は、セキュリティ パケットのフィルタリングだけに使用します。VACL は方向（入力または出力）で定義されることはありません。

ACL の種類と適用例の詳細については、「ACL について」（P.21-1）を参照してください。

ここでは、次の内容について説明します。

- 「VACL とアクセス マップ」（P.21-14）
- 「VACL とアクション」（P.21-14）
- 「統計情報」（P.21-15）

## VACL とアクセス マップ

VACL では、アクセス マップを使用して、IP ACL または MAC ACL をアクションとリンクさせます。スイッチは、VACL によって許可されたパケットに設定されているアクションを実行します。

## VACL とアクション

アクセス マップ コンフィギュレーション モードでは、**action** コマンドを使用して、次のいずれかのアクションを指定します。

- フォワード：スイッチの通常の動作によって決定された宛先にトラフィックを送信します。
- ドロップ：トラフィックをドロップします。

## 統計情報

スイッチは、VACL 内の各ルールについて、グローバルな統計情報を保持できます。VACL を複数の VLAN に適用した場合、保持されるルール統計情報は、その VACL が適用されている各インターフェイス上で一致（ヒット）したパケットの総数になります。

（注）　スイッチは、インターフェイス単位の VACL 統計情報はサポートしていません。

設定する各 VLAN アクセス マップごとに、VACL の統計情報をスイッチ内に保持するかどうかを指定できます。これにより、VACL によってフィルタリングされたトラフィックをモニタリングするため、あるいは VLAN アクセス マップの設定のトラブルシューティングを行うために、VACL 統計情報の収集のオン/オフを必要に応じて切り替えることができます。

VACL 統計情報の表示の詳細については、「IP ACL 統計情報の表示と消去」（P.21-9）を参照してください。

# VACL の設定

ここでは、次の内容について説明します。



## VACL の作成または変更

VACL を作成または変更できます。VACL の作成には、IP ACL または MAC ACL を、一致したトラフィックに適用するアクションとアソシエートさせるアクセス マップの作成が含まれます。

VACL を作成または変更する手順は、次のとおりです。

| | コマンド | 目的 |
|---|---|---|
| ステップ 1 | `switch# configure terminal` | 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)# vlan access-map map-name [sequence number]` | 指定したアクセス マップのアクセス マップ 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-access-map)# match ip address ip-access-list` | マップの IPv4 ACL を指定します。 |
| | `switch(config-access-map)# match mac address mac-access-list` | マップの MAC ACL を指定します。 |

| | コマンド | 目的 |
|---|---|---|
| ステップ 4 | `switch(config-access-map)# action {drop\|forward\|redirect}` | スイッチが、ACL に一致したトラフィックに適用するアクションを指定します。 |
| ステップ 5 | `switch(config-access-map)# [no] statistics` | （任意）VACL に規定されたルールに一致するパケットのグローバルな統計情報をスイッチ内に保持するように指定します。<br>**no** オプションを指定すると、VACL のグローバルな統計情報がスイッチ内に保持されなくなります。 |
| ステップ 6 | `switch(config-access-map)# show running-config` | （任意）ACL の設定を表示します。 |
| ステップ 7 | `switch(config-access-map)# copy running-config startup-config` | （任意）実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーします。 |

# VACL の削除

VACL を削除できます。これにより、VLAN アクセス マップも削除されます。

VACL が VLAN に適用されているかどうかを確認してください。削除できるのは、現在適用されている VACL だけです。VACL を削除しても、その VACL が適用されていた VLAN の設定は影響を受けません。スイッチは、削除対象の VACL が空であると見なします。

VACL を削除する手順は、次のとおりです。

| | コマンド | 目的 |
|---|---|---|
| ステップ 1 | `switch# configure terminal` | 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)# no vlan access-map` *map-name* | 指定したアクセス マップの VLAN アクセス マップの設定を削除します。 |
| ステップ 3 | `switch(config)# show running-config` | （任意）ACL の設定を表示します。 |
| ステップ 4 | `switch(config)# copy running-config startup-config` | （任意）実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーします。 |

# VACL の VLAN への適用

VACL を VLAN に適用できます。VACL ドロップダウン リストが [Advanced Settings] 領域に表示されます。

VACL を VLAN に適用する手順は、次のとおりです。

| | コマンド | 目的 |
|---|---|---|
| ステップ 1 | `switch# configure terminal` | 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)# [no] vlan filter` *map-name* `vlan-list` *list* | 指定したリストによって、VACL を VLAN に適用します。**no** を使用すると、VACL の適用が解除されます。<br>**vlan-list** コマンドで指定できる VLAN は最大 32 個ですが、複数の **vlan-list** コマンドを設定すれば 32 個を超える VLAN を指定できます。 |
| ステップ 3 | `switch(config)# show running-config` | （任意）ACL の設定を表示します。 |
| ステップ 4 | `switch(config)# copy running-config startup-config` | （任意）実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーします。 |

# VACL の設定の確認

VACL の設定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 running-config aclmgr` | VACL 関連の設定を含む、ACL の設定を表示します。 |
| `switch# show vlan filter` | VLAN に適用されている VACL の情報を表示します。 |
| `switch# show vlan access-map` | VLAN アクセス マップに関する情報を表示します。 |

# VACL 統計情報の表示と消去

VACL 統計情報を表示または消去するには、次のいずれかの作業を行います。

| コマンド | 目的 |
|---|---|
| `switch# show vlan access-list` | VACL の設定を表示します。VLAN アクセス マップに **statistics** コマンドが指定されている場合は、**show vlan access-list** コマンドの出力に、各ルールに一致したパケットの数が表示されます。 |
| `switch# clear vlan access-list counters` | すべての VACL、または特定の VACL の統計情報を消去します。 |

次に、acl-01 という名前の IP ACL によって許可されたトラフィックを転送するように VACL を設定し、その VACL を VLAN 50 ～ 82 に適用する例を示します。

```
switch(config)# ip access-list acl-01
switch(config-acl)# permit ip 192.168.0.0/16 any
switch(config-acl)# statistics per-entry
switch(config-acl)# show ip access-lists acl-01
IP access list acl-01
        statistics per-entry
```

```
        10 permit ip 192.168.0.0/16 any
switch(config-acl)# copy running-config startup-config
[########################################] 100%
switch(config-acl)# exit
switch(config)# vlan access-map acl-ip-map 40
switch(config-access-map)# match ip address acl-01
switch(config-access-map)# action forward
switch(config-access-map)# vlan filter acl-ip-map vlan-list 50-82
```

# デフォルト設定

表 21-2 に、IP ACL パラメータのデフォルト設定を示します。

**表 21-2　IP ACL のデフォルト パラメータ**

| パラメータ | デフォルト |
|---|---|
| IP ACL | デフォルトの IP ACL は存在しません。 |
| ACL ルール | すべての ACL に暗黙のルールが適用されます。<br>「暗黙のルール」（P.21-3）を参照してください。 |

表 21-3 に、MAC ACL パラメータのデフォルト設定値を示します。

**表 21-3　MAC ACL のデフォルト パラメータ**

| パラメータ | デフォルト |
|---|---|
| MAC ACL | デフォルトの MAC ACL は存在しません。 |
| ACL ルール | すべての ACL に暗黙のルールが適用されます。<br>「暗黙のルール」（P.21-3）を参照してください。 |

表 21-4 に、VACL パラメータのデフォルト設定値を示します。

**表 21-4　デフォルトの VACL パラメータ**

| パラメータ | デフォルト |
|---|---|
| VACL | デフォルトの IP ACL は存在しません。 |
| ACL ルール | すべての ACL に暗黙のルールが適用されます。<br>「暗黙のルール」（P.21-3）を参照してください。 |