

# ハードウェアパケットフィルター

概要・基本設定 . . . . .	2
基本動作 . . . . .	2
フィルターの構成 . . . . .	2
フィルター処理の流れ . . . . .	3
設定手順 . . . . .	3
コマンド例 . . . . .	4
注意事項 . . . . .	4
本体宛てのパケット . . . . .	5
IGMP Snooping 機能との併用 . . . . .	5
コマンドリファレンス編 . . . . .	6
機能別コマンド索引 . . . . .	6
CREATE ACL . . . . .	7
DESTROY ACL . . . . .	8
PURGE ACL . . . . .	9
SET ACL . . . . .	10
SHOW ACL . . . . .	11

## 概要・基本設定

ハードウェアパケットフィルターは、ハードウェア（ASIC）レベルで入力パケットをフィルタリング（許可・拒否）する機能です。

ハードウェアパケットフィルターには以下の特長があります。

- ハードウェアで処理するため高速
- 入力ポート単位でフィルタリングが可能

パケットのフィルタリング条件には、以下の各項目を使用できます。フィルタリング条件は、汎用のパケットフィルターであるクラシファイアによって定義します。クラシファイアの詳細については「クラシファイア」の章をご覧ください。

- Ethernet の送信元・宛先 MAC アドレス、フレームフォーマットとプロトコルタイプ（タグ付き、タグなし）
- 入力 VLAN
- 802.1p プライオリティ値
- IP ヘッダーの TOS 優先度（precedence）または DSCP（DiffServ Code Point）、プロトコル、始点・終点 IP アドレス
- TCP ヘッダーの始点・終点ポート、制御フラグのフィールド値
- UDP ヘッダーの始点・終点ポート

条件に一致したパケットに対しては、以下の処理（アクション）が可能です。

- 許可（permit）
- 破棄（deny）

## 基本動作

ハードウェアパケットフィルターの基本動作について説明します。

### フィルターの構成

ハードウェアパケットフィルターは、複数のエントリーをリストとして保持する「アクセスコントロールリスト（ACL）」から構成されます。エントリーは、クラシファイア（汎用パケットフィルター）とアクション、および適用対象のスイッチポート（入力ポート）で構成されます。

エントリーの構成は、次のとおりです。

ACL	エントリーの ID
DESCRIPTION	エントリーの説明
ACTION	マッチした場合のアクション
CLASSIFIERLIST	エントリーに割り当てるクラシファイアの ID
PORTLIST	エントリーに割り当てるポート

表 1:

ACL の仕様は、次のとおりです。

- 最大エントリー数は 64 個
- 同一ポートに複数のエントリーを割り当てることができる（ただし、同じクラシファイアを含むエントリーを、同一ポートに割り当ててはできない）
- 同一エントリーを複数ポートに割り当てることができる
- 1 ポートに割り当てられるクラシファイアの数、128 個まで（ポリシーベース QoS とハードウェアパケットフィルター機能合わせて）

## フィルター処理の流れ

ハードウェアパケットフィルターでは、パケット受信時に次の処理が行われます。

- 以下の説明は、設定上の便宜を最優先して書いたものであり、実際の内部動作を正確に記述したものではありません。
1. 受信したパケットがエントリーにマッチするかどうか調べます。
  2. 許可するエントリーにマッチした場合、そのパケットを出力します。
  3. 許可するエントリーにマッチせず、破棄するエントリーにマッチした場合、そのパケットを破棄します。
  4. エントリーにマッチしないパケットを出力します。

## 設定手順

ハードウェアパケットフィルターの設定は、次の流れで行います。

1. クラシファイアの作成（CREATE CLASSIFIER コマンド（「クラシファイア」の 6 ページ））
2. ACL のエントリーの作成（CREATE ACL コマンド（7 ページ））

以下、各手順について詳しく解説します。

ここでは例として、ポート 8 に接続されているクライアントから、サーバー 192.168.10.5 宛てのパケットを遮断するよう設定します。

1. クラシファイアを作成します。詳細は「クラシファイア」の章をご覧ください。

```
CREATE CLASSIFIER=1 IPDADDR=192.168.10.5 ↓
```

2. ACL にエントリーを追加します。エントリーを追加するには、クラシファイア、マッチ時のアクション（許可か破棄）エントリーを適用する入力ポートの指定が必要です。

```
CREATE ACL=1 ACTION=DENY CLASSIFIERLIST=1 PORTLIST=8 ↓
```

基本設定は以上です。

## コマンド例

送信元 MAC アドレスが、00-00-f4-33-22-11 のパケットを破棄

```
CREATE CLASSIFIER=1 MACSADDR=00-00-f4-33-22-11 ↓
CREATE ACL=1 ACTION=DENY CLASSIFIERLIST=1 PORTLIST=6 ↓
```

192.168.10.100 から 192.168.20.0/24 への IP パケットを破棄

```
CREATE CLASSIFIER=1 IPSADDR=192.168.10.100/32 IPDADDR=192.168.20.0/24 ↓
CREATE ACL=1 ACTION=DENY CLASSIFIERLIST=1 PORTLIST=5 ↓
```

192.168.30.100 への telnet パケットを破棄。

```
CREATE CLASSIFIER=1 IPDADDR=192.168.30.100/32 TCPDPORT=23 ↓
CREATE ACL=1 ACTION=DENY CLASSIFIERLIST=1 PORTLIST=4 ↓
```

ACL の一覧を表示するには、SHOW ACL コマンド (11 ページ) を使います。

```
SHOW ACL ↓
```

クラシファイアの一覧を表示するには、SHOW CLASSIFIER コマンド (「クラシファイア」の 13 ページ) を実行します。CLASSIFIER パラメーターに番号を指定すれば、該当するクラシファイアのみが表示されます。

```
SHOW CLASSIFIER ↓
SHOW CLASSIFIER=1-3 ↓
```

ACL からエントリーを削除するには、DESTROY ACL コマンド (8 ページ) を使います。

```
DESTROY ACL=1 ↓
```

- ACL からエントリーを削除しても、クラシファイアは削除されません。ACL とクラシファイアの関連付けが削除されるだけです。クラシファイアを削除するには、DESTROY CLASSIFIER コマンド (「クラシファイア」の 9 ページ) を使います。

## 注意事項

ここでは、設定時に注意が必要なハードウェアパケットフィルターの仕様について解説します。

### 本体宛てのパケット

スイッチ本体（CPU）宛てのパケットに対し、ハードウェアパケットフィルター機能は動作します。

### IGMP Snooping 機能との併用

ハードウェアパケットフィルターで、IPPROTOCOL に IGMP を指定したクラシファイアを使用した場合は、IGMP Snooping 機能は有効にできません。

## コマンドリファレンス編

### 機能別コマンド索引

#### 一般コマンド

CREATE ACL . . . . .	7
DESTROY ACL . . . . .	8
PURGE ACL . . . . .	9
SET ACL . . . . .	10
SHOW ACL . . . . .	11

## CREATE ACL

カテゴリー：ハードウェアパケットフィルター / 一般コマンド

```
CREATE ACL=0..255 [DESCRIPTION=string] [ACTION={DENY | PERMIT}]
[CLASSIFIERLIST={rule-list|NONE}] [PORTLIST={port-list|ALL|NONE}]
```

**string**: 文字列（1～15 文字。空白を含む場合はダブルクォートで囲む）

**rule-list**: クラシファイア番号（1～9999。ハイフン、カンマを使った複数指定も可能）

**port-list**: スイッチポート番号（1～。ハイフン、カンマを使った複数指定も可能）

### 解説

ACL にエントリーを追加する。

パケットをフィルタリングするためのパラメーター（MAC アドレス、IP アドレスなど）は、汎用のパケットフィルターであるクラシファイア（CREATE CLASSIFIER コマンドで作成）で定義する。本コマンドでは、クラシファイア番号とマッチ時のアクションを一組のエントリーとして ACL に追加する。

### パラメーター

**ACL** 作成するエントリーの ID。

**DESCRIPTION** 作成するエントリーの説明。

**ACTION** パケットがクラシファイアに一致したときのアクション。PERMIT（許可）、DENY（破棄）から選択する。デフォルトは DENY。

**CLASSIFIERLIST** ACL に対応づけるクラシファイアの ID を指定する。デフォルトは NONE。

**PORTLIST** ACL を割り当てるポートを指定する。デフォルトは NONE。

### 例

ACL にエントリーを追加する。

```
CREATE ACL=1 ACTION=DENY CLASSIFIERLIST=1 PORTLIST=8
```

### 関連コマンド

DESTROY ACL（8 ページ）

SHOW ACL（11 ページ）

## DESTROY ACL

カテゴリー：ハードウェアパケットフィルター / 一般コマンド

**DESTROY ACL=0..255**

### 解説

ACL のエントリーを削除する。

### パラメーター

**ACL** 削除するエントリーの ID。

### 例

ACL のエントリーを削除する。

DESTROY ACL=1

### 関連コマンド

CREATE ACL ( 7 ページ )

SHOW ACL ( 11 ページ )



## PURGE ACL

カテゴリー：ハードウェアパケットフィルター / 一般コマンド

**PURGE ACL**

### 解説

ACL の設定を工場出荷時の状態に戻す。

### 例

ACL の設定を工場出荷時の状態に戻す。

PURGE ACL

### 関連コマンド

SHOW ACL ( 11 ページ )

## SET ACL

カテゴリー：ハードウェアパケットフィルター / 一般コマンド

```
SET ACL=0..255 [DESCRIPTION=string] [ACTION={DENY |PERMIT}]
               [CLASSIFIERLIST={rule-list|NONE}] [PORTLIST={port-list|ALL|NONE}]
```

**string**: 文字列（1～15 文字。空白を含む場合はダブルクォートで囲む）

**rule-list**: クラシファイア番号（1～9999。ハイフン、カンマを使った複数指定も可能）

**port-list**: スイッチポート番号（1～。ハイフン、カンマを使った複数指定も可能）

### 解説

ACL エントリーの設定を変更する。

### パラメーター

**ACL** 変更するエントリーの ID。

**DESCRIPTION** 作成するエントリーの説明。

**ACTION** パケットがクラシファイアに一致したときのアクション。PERMIT（許可）、DENY（破棄）から選択する。デフォルトは DENY。

**CLASSIFIERLIST** ACL に対応づけるクラシファイアの ID を指定する。デフォルトは NONE。

**PORTLIST** ACL を割り当てるポートを指定する。デフォルトは NONE。

### 例

ACL エントリーの設定を変更する。

```
SET ACL=1 CLASSIFIERLIST=2-5
```

### 関連コマンド

SHOW ACL（11 ページ）

## SHOW ACL

カテゴリー：ハードウェアパケットフィルター / 一般コマンド

**SHOW ACL** [= {*id-list* | All}]

**id-list**: ACL の ID (0 ~ 255)。ハイフン、カンマを使った複数指定も可能)

### 解説

ACL のエントリーを表示する。

### パラメーター

**ACL** 表示するエントリーの ID。省略時および ALL を指定した場合は、すべてのフローグループ情報が表示される。

### 入力・出力・画面例

```
# show acl

-----
ACL ID ..... 1
Description .....
Action ..... Deny
Classifier List ..... 1
Port List ..... 8
Is Active ..... Yes
```

ACL ID	エントリーの ID
Description	エントリーの説明
Action	パケットがクラシファイアに一致したときのアクション。Permit または Deny
Classifier List	クラシファイアの ID
Port List	エントリーを割り当てるポート
Is Active	エントリーがポートに割り当てられている (Yes) またはいない (No)

表 2:

### 関連コマンド

CREATE ACL (7 ページ)

DESTROY ACL (8 ページ)