

# 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	3
設定例	5
特定スイッチポートからのみ UDP 通信を許可	5
TCP 片方向通信	6
注意事項	7
本体宛てのパケット	7
DHCP Snooping 機能との併用	7
コマンドリファレンス編	8
機能別コマンド索引	8
CREATE ACL	9
DESTROY ACL	11
PURGE ACL	12
RESET ACL COUNTER	13
SET ACL	14
SHOW ACL	15
SHOW ACL COUNTER	17

## 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 プライオリティー値
- 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

### 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。

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、ACL のエントリー ID の番号順に調べます。
2. 条件にマッチした場合は、残りの条件は調べずに、その条件のアクションをします。
3. エントリーにマッチしないパケットを出力します。

✎ 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。

### 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（9 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 TCPPDPORT=23 ↓
CREATE ACL=1 ACTION=DENY CLASSIFIERLIST=1 PORTLIST=4 ↓
```

192.168.20.100 のみ双方向の通信が可能。

```
CREATE CLASSIFIER=1 IPDADDR=192.168.20.100/32 ↓
CREATE CLASSIFIER=2 IPSADDR=192.168.20.100/32 ↓
CREATE CLASSIFIER=3 PROTOCOL=ARP ↓
CREATE CLASSIFIER=4 ↓
CREATE ACL=1 ACTION=PERMIT CLASSIFIERLIST=1 PORTLIST=ALL ↓
CREATE ACL=2 ACTION=PERMIT CLASSIFIERLIST=2 PORTLIST=ALL ↓
CREATE ACL=3 ACTION=PERMIT CLASSIFIERLIST=3 PORTLIST=ALL ↓
CREATE ACL=4 ACTION=DENY CLASSIFIERLIST=4 PORTLIST=ALL ↓
```

ARP のみ双方向の通信が可能。

```
CREATE CLASSIFIER=1 PROTOCOL=ARP ↓
CREATE CLASSIFIER=2 PROTOCOL=ANY ↓
CREATE ACL=1 ACTION=PERMIT CLASSIFIERLIST=1 PORTLIST=ALL ↓
CREATE ACL=2 ACTION=DENY CLASSIFIERLIST=2 PORTLIST=ALL ↓
```

ACL の一覧を表示するには、SHOW ACL コマンド (15 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 14 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 からエントリを削除するには、DESTROY ACL コマンド（11 ページ）を使います。

```
DESTROY ACL=1 ↓
```

- ※ ACL からエントリを削除しても、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。

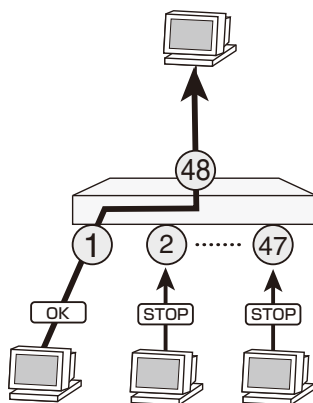
## 設定例

### 特定スイッチポートからのみ UDP 通信を許可

ハードウェアパケットフィルターを利用して、特定ポートからのみ UDP 通信を許可する設定例を示します。ここでは、次のようなネットワーク構成を例に説明します。

VLAN 名 (VID)	untagged ポート	tagged ポート
default(1)	1 ~ 48	なし

表 2:



ここでは、次のようなフィルタリング条件を考えます。

- UDP トラフィックは原則として拒否する。
- ただし、ポート 1、48 の UDP 通信を許可する。

ポート単位でのフィルタリングには、DHCP クライアントの IP アドレスが変更された場合でも対応できるメリットがあります。

ハードウェアパケットフィルターの設定を行います。

- 1. クラシファイアを作成します。ここではUDP トラフィックだけを対象とするため、IP プロトコル フィールド (IPPROTOCOL) に UDP を指定します。

```
CREATE CLASSIFIER=1 IPPROTO=UDP ↵
```

- 2. ポートとアクションを指定し、ACL にエントリーを追加します。ここでは受信ポートが 2～47 のト ラフィックを破棄するよう指定します。

```
CREATE ACL=1 ACTION=DENY CLASSIFIERLIST=1 PORTLIST=2-47 ↵
```

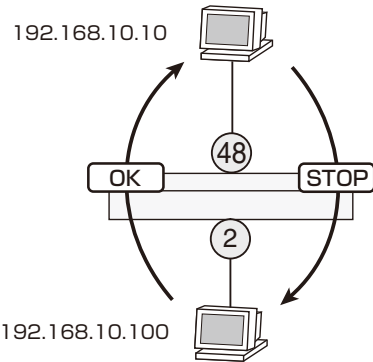
設定は以上です。

TCP 片方向通信

マッチ条件として TCP の制御フラグ Syn を使用し、192.168.10.100 からのみ TCP の通信を開始できるよ うに設定します。

VLAN 名 ( VID )	untagged ポート	tagged ポート	IP アドレス
default(1)	1 ~ 48	なし	192.168.10.1

表 3:



ここでは、次のようなフィルタリング条件を考えます。

- TCP は 192.168.10.100 から 192.168.10.10 への通信 (セッション開始) のみを許可。192.168.10.10 から 192.168.10.100 への通信は拒否する。
- その他のプロトコルはすべて許可する。

- 1. クラシファイアの設定を行います。  
ここでは始点 IP アドレスに 192.168.10.10、終点 IP アドレスに 192.168.10.100、TCP ヘッダー制御 フラグ (TCPFLAGS) に SYN を指定します。

```
CREATE CLASSIFIER=1 IPSADDR=192.168.10.10 IPDADDR=192.168.10.100  
TCPFLAGS=SYN ↓
```

2. アクションを指定し、ACL にエントリーを追加します。

```
CREATE ACL=1 ACTION=DENY CLASSIFIERLIST=1 PORTLIST=48 ↓
```

設定は以上です。

## 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。

### DHCP Snooping 機能との併用

ハードウェアパケットフィルターと DHCP Snooping を併用した場合、ハードウェアパケットフィルターのフィルタリングが優先され、通信が許可および破棄されます。

ただし、DHCP パケットに関してのみ、ハードウェアパケットフィルターのフィルタリングは優先されず、DHCP Snooping による DHCP パケットの通信が許可されます。

# コマンドリファレンス編

## 機能別コマンド索引

### 概要・基本設定

CREATE ACL . . . . .	9
DESTROY ACL . . . . .	11
PURGE ACL . . . . .	12
RESET ACL COUNTER . . . . .	13
SET ACL . . . . .	14
SHOW ACL . . . . .	15
SHOW ACL COUNTER . . . . .	17

## CREATE ACL

カテゴリー：ハードウェアパケットフィルター

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

*string*: 文字列（1～31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。連番でなくてもかまわない。

**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

### 入力・出力・画面例

```
Manager > create acl=1 action=deny classifierlist=1 portlist=8

Operation successful.
```

### 例

ACL にエントリーを追加する

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

### 備考・注意事項

作成したエントリーの順番を変えるときは、エントリーを削除し、作成し直す必要がある。

### 関連コマンド

DESTROY ACL ( 11 ページ )

PURGE ACL ( 12 ページ )

RESET ACL COUNTER ( 13 ページ )

SET ACL ( 14 ページ )

SHOW ACL ( 15 ページ )

SHOW ACL COUNTER ( 17 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

**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。

### 入力・出力・画面例

```
Manager > destroy acl=1  
  
Operation successful.
```

### 例

ACL のエントリーを削除する

DESTROY ACL=1

### 関連コマンド

CREATE ACL ( 9 ページ )

SET ACL ( 14 ページ )

SHOW ACL ( 15 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

### PURGE ACL

#### 解説

ACL の設定を工場出荷時の状態に戻す。

#### 入力・出力・画面例

```
Manager > purge acl  
  
Operation successful.
```

#### 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

CREATE ACL ( 9 ページ )

DESTROY ACL ( 11 ページ )

SET ACL ( 14 ページ )

SHOW ACL ( 15 ページ )

## RESET ACL COUNTER

カテゴリー：ハードウェアパケットフィルター

**RESET ACL** [= {*id-list* | ALL}] **COUNTER**

*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

指定された ACL に割り当てられているクラシファイアのカウンターをリセットする。

### パラメーター

**ACL** カウンターをリセットするエントリーの ID。省略時および ALL を指定した場合は、すべての ACL に割り当てられているクラシファイアのカウンターをリセットする

### 入力・出力・画面例

```
Manager > reset acl=1 counter  
  
Operation successful.
```

### 関連コマンド

SHOW ACL COUNTER (17 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

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

*string*: 文字列 (1~31 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。

**CLASSIFIERLIST** ACL に対応づけるクラシファイアの ID を指定する。

**PORTLIST** ACL を割り当てるポートを指定する。

### 入力・出力・画面例

```
Manager > set acl=1 classifierlist=2-5

Operation successful.
```

### 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

CREATE ACL (9 ページ)

DESTROY ACL (11 ページ)

SHOW ACL (15 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

**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、すべてのエントリー情報が表示される。

### 入力・出力・画面例

```
Manager > 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、割り当てられていない (No)

表 4:

### 例

ACL のエントリーを表示する

SHOW ACL

### 関連コマンド

CREATE ACL ( 9 ページ )

DESTROY ACL ( 11 ページ )

SET ACL ( 14 ページ )

## SHOW ACL COUNTER

カテゴリー：ハードウェアパケットフィルター

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

*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 に割り当てられているクラシファイアごとのカウンターを表示する。

### 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、すべてのエントリー情報が表示される。

### 入力・出力・画面例

Manager > show acl counter				
ACL		Classifier		Hit Counter
1	ACL 1	1	Classifier 1	334412
2	ACL 2	2	Classifier 2	1349
3	ACL 3	3	Classifier 3	1394055485
4	ACL 4	4	Classifier 4	4348500

ACL	ACL ID と CREATE ACL コマンドで設定したエントリーの説明を表示。設定されていない場合、“ACL id” フォーマットで表記
Classifier	クラシファイア ID と CREATE CLASSIFIER コマンドで設定したクラシファイアの説明を表示。設定されていない場合、“Classifier id” フォーマットで表記
Hit Counter	フィルターにマッチした数を表示

表 5:

### 例

ACL に割り当てられているクラシファイアごとのカウンターを表示する

SHOW ACL COUNTER

## 関連コマンド

RESET ACL COUNTER ( 13 ページ )