

# 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外部への UDP 通信を許可	5
TCP 片方向通信	6
「マルチプル VLAN」的構成例	8
特定ホスト通信許可の構成例	9
注意事項	10
本体宛てのパケット	10
IGMP Snooping 機能との併用	10
コマンドリファレンス編	12
機能別コマンド索引	12
CREATE ACL	13
DESTROY ACL	15
PURGE ACL	16
RESET ACL COUNTER	17
SET ACL	18
SHOW ACL	19
SHOW ACL COUNTER	21

## 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
- ACL を介してポートに割り当てられるクラシファイアの数、システム全体で 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（13 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 (19 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 (15 ページ) を使います。

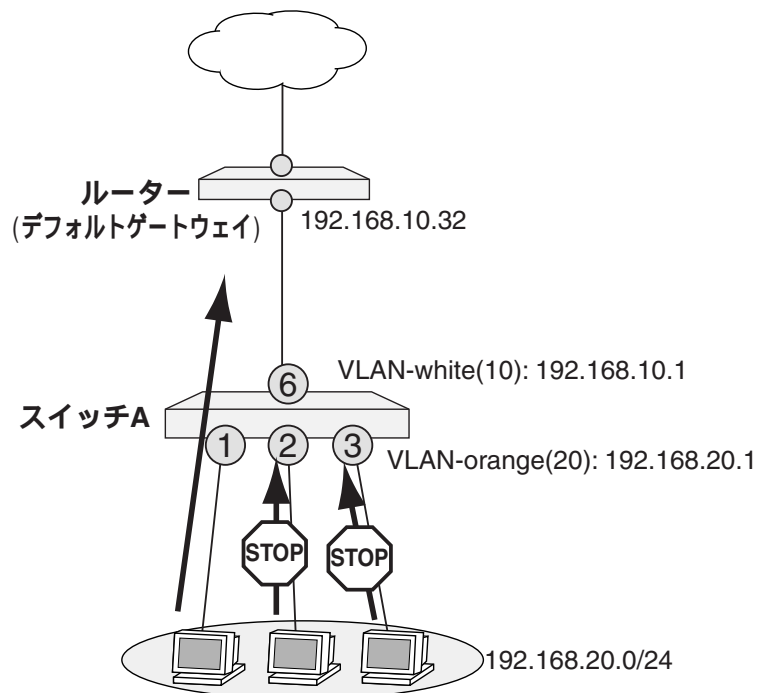
DESTROY ACL=1 ↓

- ✎ 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。

## 設定例

### 特定スイッチポートからのみ外部への 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、VLAN 内の特定ポートからのみ外部への 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。



ここでは、次のようなフィルタリング条件を考えます。

- VLAN orange から外部への UDP トラフィックは原則として拒否する。

- ただし、ポート 1 から外部へは 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。

#### スイッチ A の設定

1. VLAN の設定を行います。

```
CREATE VLAN=white VID=10 ↵
CREATE VLAN=orange VID=20 ↵
ADD VLAN=white PORT=6 ↵
ADD VLAN=orange PORT=1-3 ↵
```

2. VLAN インターフェースに IP アドレスを設定します。

```
ADD IP INT=vlan-white IP=192.168.10.1 MASK=255.255.255.0 ↵
ADD IP INT=vlan-orange IP=192.168.20.1 MASK=255.255.255.0 ↵
```

3. デフォルトルートを設定します。

```
ADD IP ROUTE=0.0.0.0 MASK=0.0.0.0 INT=vlan-white
NEXTTHOP=192.168.10.32 ↵
```

4. ハードウェアパケットフィルタの設定を行います。

- 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 ↵
```

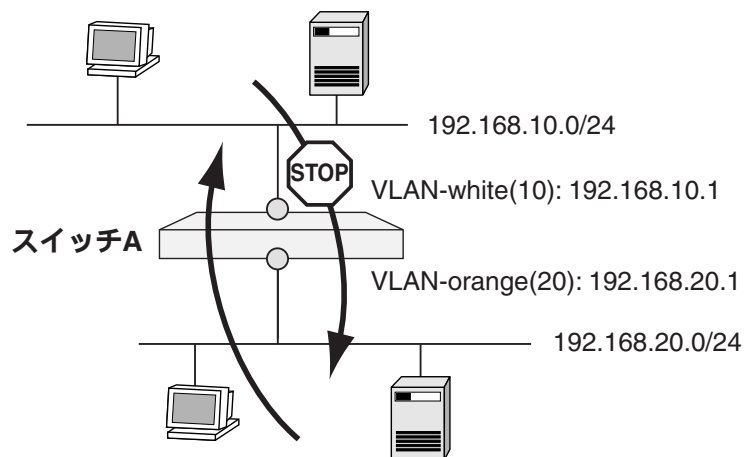
- ポートとアクションを指定し、ACL にエントリーを追加します。ここでは受信ポートが 2 か 3 のトラフィックを破棄するよう指定します。

```
CREATE ACL=1 ACTION=DENY CLASSIFIERLIST=1 PORTLIST=2,3 ↵
```

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 と Ack を使用し、片方の VLAN からのみ TCP の通信を開始でき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。



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 VLAN orange から white への通信（セッション開始）のみを許可。white から orange 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。

#### スイッチ A の設定

1. VLAN の設定を行います。

```
CREATE VLAN=white VID=10 ↓
CREATE VLAN=orange VID=20 ↓
ADD VLAN=white PORT=1-12 ↓
ADD VLAN=orange PORT=13-24 ↓
```

2. VLAN インターフェースに IP アドレスを設定します。

```
ADD IP INT=vlan-white IP=192.168.10.1 MASK=255.255.255.0 ↓
ADD IP INT=vlan-orange IP=192.168.20.1 MASK=255.255.255.0 ↓
```

3. ハードウェアパケットフィルタの設定を行います。

- クラシファイアを作成します。ここでは始点 IP アドレスに 192.168.10.0/24、終点 IP アドレスに 192.168.20.0/24、TCP ヘッダー制御フラグ (TCPFLAGS) に SYN を指定します。

```
CREATE CLASSIFIER=1 IPSADDR=192.168.10.0/24
IPDADDR=192.168.20.0/24 TCPFLAGS=SYN ↓
```

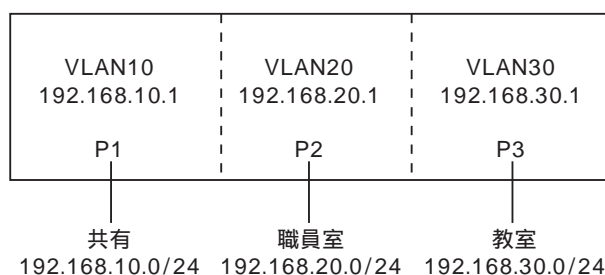
- ポートとアクションを指定し、ACL にエントリーを追加します。ここでは受信ポートが 1 から 12 のトラフィックを破棄するよう指定します。

```
CREATE ACL=1 ACTION=DENY CLASSIFIERLIST=1 PORTLIST=1-12 ↓
```

設定は以上です。

### 「マルチプル VLAN」的構成例

ポート 1 を VLAN10(共有)、ポート 2 を VLAN20(職員室)、ポート 3 を VLAN30(教室) とし、VLAN10 からは VLAN20 と VLAN30 両方に通信できるが、VLAN20 と VLAN30 間の通信は禁止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。



### スイッチ A の設定

1. VLAN の設定を行います。

```
CREATE VLAN=p1 VID=10 ↓
CREATE VLAN=p2 VID=20 ↓
CREATE VLAN=p3 VID=30 ↓
ADD VLAN=p1 PORT=1 ↓
ADD VLAN=p2 PORT=2 ↓
ADD VLAN=p3 PORT=3 ↓
```

2. VLAN インターフェースに IP アドレスを設定します。

```
ADD IP INT=vlan-p1 IP=192.168.10.1 MASK=255.255.255.0 ↓
ADD IP INT=vlan-p2 IP=192.168.20.1 MASK=255.255.255.0 ↓
ADD IP INT=vlan-p3 IP=192.168.30.1 MASK=255.255.255.0 ↓
```

3. ハードウェアパケットフィルターの設定を行います。

- 以下の 2 個のクラシファイアを作成します。

始点 IP アドレス 192.168.20.0/24 から 終点 IP アドレス 192.168.30.0/24。

始点 IP アドレス 192.168.30.0/24 から 終点 IP アドレス 192.168.20.0/24。



```
CREATE CLASSIFIER=1 IPSADDR=192.168.20.0/24
  IPDADDR=192.168.30.0/24 ↵
CREATE CLASSIFIER=2 IPSADDR=192.168.30.0/24
  IPDADDR=192.168.20.0/24 ↵
```

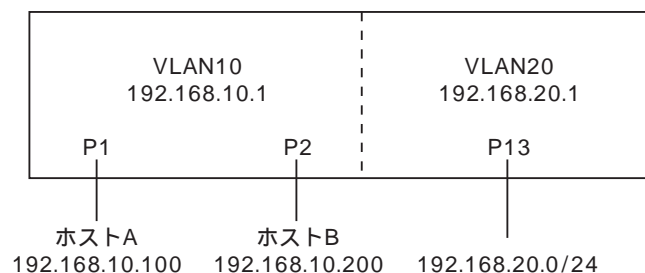
- ポートとアクションを指定し、ACL にエントリーを追加します。ここでは受信ポート 2 にクラシファイア 1 を、受信ポート 3 にクラシファイア 2 を割り当て、トラフィックを破棄するよう指定します。

```
CREATE ACL=1 ACTION=DENY CLASSIFIERLIST=1 PORTLIST=2 ↵
CREATE ACL=2 ACTION=DENY CLASSIFIERLIST=2 PORTLIST=3 ↵
```

設定は以上です。

#### 特定ホスト通信許可の構成例

VLAN10 と VLAN20 間の通信は破棄するが、ホスト A(192.168.10.100) の通信は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。



#### スイッチ A の設定

1. VLAN の設定を行います。

```
CREATE VLAN=v10 VID=10 ↵
CREATE VLAN=v20 VID=20 ↵
ADD VLAN=v10 PORT=1-12 ↵
ADD VLAN=v20 PORT=13-24 ↵
```

2. VLAN インターフェースに IP アドレスを設定します。

```
ADD IP INT=vlan-v10 IP=192.168.10.1 MASK=255.255.255.0 ↵
ADD IP INT=vlan-v20 IP=192.168.20.1 MASK=255.255.255.0 ↵
```

### 3. ハードウェアパケットフィルターの設定を行います。

- ホスト A の通信を許可する 2 個のクラシファイアを作成します。

始点 IP アドレス 192.168.10.100/32 から 終点 IP アドレス 192.168.20.0/24。

始点 IP アドレス 192.168.20.0/24 から 終点 IP アドレス 192.168.10.100/32。

```
CREATE CLASSIFIER=1 IPSADDR=192.168.10.100/32
    IPDADDR=192.168.20.0/24 ↵
CREATE CLASSIFIER=2 IPSADDR=192.168.20.0/24
    IPDADDR=192.168.10.100/32 ↵
```

- VLAN 間の通信を破棄する 2 個のクラシファイアを作成します。

始点 IP アドレス 192.168.10.0/24 から 終点 IP アドレス 192.168.20.0/24。

始点 IP アドレス 192.168.20.0/24 から 終点 IP アドレス 192.168.10.0/24。

```
CREATE CLASSIFIER=3 IPSADDR=192.168.10.0/24
    IPDADDR=192.168.20.0/24 ↵
CREATE CLASSIFIER=4 IPSADDR=192.168.20.0/24
    IPDADDR=192.168.10.0/24 ↵
```

- 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。ここではクラシファイア 1、2 のトラフィックを許可するように、クラシファイア 3、4 のトラフィックを破棄するように指定します。

```
CREATE ACL=1 ACTION=PERMIT CLASSIFIERLIST=1 PORTLIST=1-12 ↵
CREATE ACL=2 ACTION=PERMIT CLASSIFIERLIST=2 PORTLIST=13-24 ↵
CREATE ACL=3 ACTION=DENY CLASSIFIERLIST=3 PORTLIST=1-12 ↵
CREATE ACL=4 ACTION=DENY CLASSIFIERLIST=4 PORTLIST=13-24 ↵
```

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。

### IGMP Snooping 機能との併用

ハードウェアパケットフィルタで、IPPROTOCOL に IGMP を指定したクラシファイアを使用した場合、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 . . . . .	13
DESTROY ACL . . . . .	15
PURGE ACL . . . . .	16
RESET ACL COUNTER . . . . .	17
SET ACL . . . . .	18
SHOW ACL . . . . .	19
SHOW ACL COUNTER . . . . .	21

## 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 (1~31 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。

### 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 (15 ページ)

PURGE ACL (16 ページ)

RESET ACL COUNTER (17 ページ)

SET ACL ( 18 ページ )

SHOW ACL ( 19 ページ )

SHOW ACL COUNTER ( 21 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**={*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 ( 13 ページ )

PURGE ACL ( 16 ページ )

RESET ACL COUNTER ( 17 ページ )

SET ACL ( 18 ページ )

SHOW ACL ( 19 ページ )

SHOW ACL COUNTER ( 21 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

CREATE ACL ( 13 ページ )

DESTROY ACL ( 15 ページ )

RESET ACL COUNTER ( 17 ページ )

SET ACL ( 18 ページ )

SHOW ACL ( 19 ページ )

SHOW ACL COUNTER ( 21 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 / 一般コマンド

**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すべての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。

### 関連コマンド

CREATE ACL (13 ページ)

DESTROY ACL (15 ページ)

PURGE ACL (16 ページ)

SET ACL (18 ページ)

SHOW ACL (19 ページ)

SHOW ACL COUNTER (21 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 (1~31 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** 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。

### 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 (13 ページ)

DESTROY ACL (15 ページ)

PURGE ACL (16 ページ)

RESET ACL COUNTER (17 ページ)

SHOW ACL (19 ページ)

SHOW ACL COUNTER (21 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、すべてのエントリー情報が表示される。

### 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 (13 ページ)

DESTROY ACL (15 ページ)

PURGE ACL (16 ページ)

RESET ACL COUNTER ( 17 ページ )

SET ACL ( 18 ページ )

SHOW ACL COUNTER ( 21 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 / 一般コマンド

**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（条件にマッチしたパケット数）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

# show acl counter				
ACL		Classifier		Hit Counter
-----				
1	ACL 1	1	Classifier 1	334412
		2	Classifier 2	730934
2	ACL 2	3	Classifier 3	1349
3	ACL 3	4	Classifier 4	1394055485
4	ACL 4	5	Classifier 5	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 3:

### 関連コマンド

CREATE ACL ( 13 ページ )

DESTROY ACL ( 15 ページ )

PURGE ACL ( 16 ページ )

RESET ACL COUNTER ( 17 ページ )

