

## 第 12 章

# フィルタ

SEIL が IPv4/IPv6 ルータとして動作するとき、及び、SEIL が end-to-end で IPv4/IPv6 通信を行なうとき、セキュリティ向上のために適用可能なパケットフィルタリング機能を提供しています。

### 12.1 SEIL のフィルタ機能の概要

SEIL は設定されたフィルタルールに従い、SEIL が中継しようとするパケットや SEIL が送受信しようとするパケットを、通過 (PASS) させる、または拒否 (BLOCK) することができます。

フィルタルールは、パケットが持つアドレスやプロトコル等の情報を条件として複数設定でき、パケットが通過しようとするインターフェイスごとに優先度の高い順に評価されます。また、どのフィルタルールにもマッチしなかったパケットは通過します。

TCP/UDP のパケットに対しては、フィルタルールの適用により動的に生成・消滅する通過ルールを生成することも可能です。(動的フィルタ)

なお、工場出荷状態ではフィルタルールは設定されていませんので、SEIL を導入するネットワークのセキュリティポリシーにあわせて適切なフィルタ設定を行うことをお勧めします。

フィルタ設定範囲

T1	128	2FE	ATM	IPv4(filter),IPv6(filter6) 各 64 個
Plus				IPv4(filter),IPv6(filter6) 各 512 個
Turbo				IPv4(filter),IPv6(filter6) 各 1024 個

## 12.2 フィルタ設定コマンド

フィルタルールを設定するコマンドについて、次の入力例を元に各キーワードについて説明します。

```
1| # filter add HTTP interface pppoe0 direction in action pass protocol tcp dst 192.168.0.8/32
   dstport 80
2| # filter add Default interface pppoe0 direction in action block logging off
```

- 1| pppoe0 インターフェイスへの入力パケットが、ホスト 192.168.0.8 の TCP 80 番ポートへのアクセスであれば通過させます。
- 2| pppoe0 インターフェイスへの入力パケットはすべて拒否します。  
1 行目にマッチしなかったパケットが評価対象です。

### 12.2.1 フィルタルールの管理コマンド

```
1| # filter add HTTP interface pppoe0 direction in action pass protocol tcp dst 192.168.0.8/32
   dstport 80
2| # filter add Default interface pppoe0 direction in action block logging off
```

- 1| filter [add | delete | modify] <filter name> IPv4 用
- 2| filter6 [add | delete | modify] <filter name> IPv6 用

フィルタルールを追加 (add)、削除 (delete)、変更 (modify) するコマンドです。

filter(filter6) コマンドに続いてフィルタリング条件や処理方法を指定し、フィルタルールを設定します。<filter name> は、識別子として、削除や変更時のキーワードとなります。

フィルタルールを追加するときに順位の指定が無い場合は最下行に追加されますが、追加位置 (評価順位) を指定して追加することもできます。

"filter delete <filter name>" もしくは "filter delete all" で、指定した <filter name> もしくはすべてのフィルタルールを削除できます。

また、既存のルールは "filter modify <filter name>" に続き、変更したいパラメータを入力することで対象範囲や処理方法を変更することができます。

**filter [enable / disable] <filter name>**

**filter6 [enable / disable] <filter name>**

フィルタルールの有効/無効を指定します。"disable" は、"delete" と異なり設定を削除することなくルールを無効にします。

"filter disable <filter name>" や、"filter enable all" (all はすべてのルールに適用) といった入力で状態を変更することができます。

"filter add <filter name> disable" として無効な状態で追加することも可能です。入力例の様に add 時に指定が無い場合は enable となります。

## 12.2.2 フィルタ条件

```
# filter add HTTP interface pppoe0 direction in action pass protocol tcp dst 192.168.0.8/32
dstport 80
# filter add Default interface pppoe0 direction in action block logging off
```

通過を許可/拒否したいパケットを特定する条件を、キーワードとパラメータの対で指定します。1行のフィルタルール中の条件にすべてマッチするパケットについて、許可/拒否の処理を行います。フィルタルールには以下の条件を指定することができます。

**interface** [**lanX** | **wanX** | **pppoeX** | **pvcX** | **lisX** | **tunnelX** | **vlanX** | **ipsecX**]

lan0 や pppoe0 といった、SEIL 各機種が搭載している物理/論理インターフェイスを指定し、指定したインターフェイスを通過しようとするパケットを評価対象とします。

※ interface の指定を省略することはできません。

**direction** [**in** | **out** | **in/out**]

インターフェイスに対する、指定した入出力方向のパケットを評価対象とします。"in/out" を指定した場合は、入力・出力どちらも評価対象とします。

※ direction の指定を省略することはできません。

**protocol** [**any** | **icmp** | **igmp** | **tcp** | **tcp-established** | **tcp-synonly** | **tcpudp** | **udp** <protocol number>]

パケットのプロトコル (プロトコル番号) が指定と一致するか評価します。

TCP については、接続要求パケット (tcp-synonly) やセッション確立済みパケット (tcp-established) であるかの評価が可能です。指定を省略した場合"protocol any"の扱いになり、すべての IP パケットがマッチします。

**src** / **dst** [<IP address/prefixlen>]

パケットの Source アドレス、Destination アドレスが指定と一致するか評価します。

NAT/NAPT が適用される通信をフィルタする場合は、NAT/NAPT 変換後のアドレスを指定します。指定を省略した場合は、アドレスを条件にしません。

**srcport** / **dstport** [<port (0-65535), or port range (e.g. 137-139)>]

パケットのプロトコルが TCP/UDP の場合に、Source ポート番号、Destination ポート番号が指定と一致するか評価します。ポート番号は "-" を使用して範囲指定が可能です。

指定を省略した場合は、ポート番号を条件にしません。