

# アクセスフィルター

|                                      |    |
|--------------------------------------|----|
| 概要・基本設定 . . . . .                    | 2  |
| アクセスフィルターの基本設定 . . . . .             | 2  |
| コマンド例 . . . . .                      | 3  |
| デフォルトアクションの設定例 . . . . .             | 3  |
| エントリーの作成例 . . . . .                  | 3  |
| 設定内容の確認 . . . . .                    | 4  |
| マッチ判定 . . . . .                      | 4  |
| フィルター適用のまとめ . . . . .                | 5  |
| コマンドリファレンス編 . . . . .                | 7  |
| 機能別コマンド索引 . . . . .                  | 7  |
| ADD ACCESS FILTER . . . . .          | 8  |
| DELETE ACCESS FILTER ENTRY . . . . . | 10 |
| DISABLE ACCESS FILTER . . . . .      | 11 |
| ENABLE ACCESS FILTER . . . . .       | 12 |
| SET ACCESS FILTER . . . . .          | 13 |
| SET ACCESS FILTER ENTRY . . . . .    | 15 |
| SHOW ACCESS FILTER . . . . .         | 17 |

## 概要・基本設定

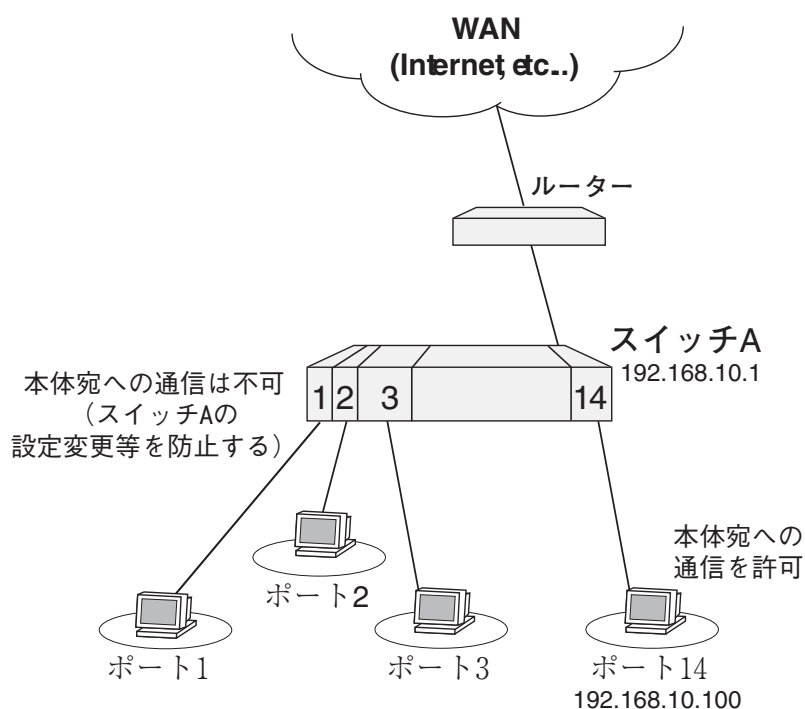
アクセスフィルターとは本製品宛への通信に適用するセキュリティー機能です。本製品宛のパケットを受信すると、受信パケットに関連付けられたフィルターを参照し、受信を許可するか、拒否するかを決定を行います。

本製品では、各種サービス（IP、TELNET、FTP、TFTP、SNMP）に IP アドレスおよび受信ポートを組み合わせて関連付けたフィルタリングに対応しています。各組み合わせパターンをエントリーと呼び、システム全体で 512 件まで登録できます。

## アクセスフィルターの基本設定

アクセスフィルターのコマンド例をいくつか示します。本製品への IP アドレスの付与については、「IP」をご覧ください。

■ 管理用端末（192.168.10.100）からのアクセスを除き、本製品（192.168.10.1）宛へのすべてのアクセスを拒否するよう設定します。



1. ENABLE ACCESS FILTER コマンド（12 ページ）でアクセスフィルター機能を有効にします。ここでは、あらゆるプロトコル・サービスを含むグローバルフィルターを設定します。

```
Manager > ENABLE ACCESS FILTER=GLOBAL ↵
```

2. 次に、SET ACCESS FILTER コマンド（13 ページ）で、デフォルトのアクション（処理）ではパケットを破棄するよう設定します。

```
Manager > SET ACCESS FILTER=GLOBAL DEFAULT=DISCARD ↵
```

3. エントリーを作成します。ADD ACCESS FILTER コマンド (8 ページ) で、管理用端末 (ポート : 14、IP アドレス : 192.168.10.100) からのすべてのパケットを許可するエントリーを作成します。ここで、MASK に指定するのはこの IP アドレスのサブネットマスクではなく、この IP アドレスのどこまでをマスクするか指定するものです。

```
Manager > ADD ACCESS FILTER=GLOBAL IPADDRESS=192.168.10.100
MASK=255.255.255.255 ACTION=PASS PORT=14 ↵
```

4. 設定内容をファイルに保存し、起動スクリプトに指定します。

```
Manager > CREATE CONFIG=basic.cfg ↵
```


```
Manager > SET CONFIG=basic.cfg ↵
```

5. アクセスフィルター関連コマンドは、再起動後に反映されるため、RESTART REBOOT コマンド (「システム」の 14 ページ) で再起動します。

```
Manager > RESTART REBOOT ↵
```

Do restart system now ? (Y/N):Y

以上で設定は終わりです。

 アクセスフィルター機能はデフォルトで無効になっています。


## コマンド例

上記基本設定の手順 2 と 3 にあたるコマンドについて、いくつか例を示します。

### デフォルトアクションの設定例

■ デフォルトのアクションでは、すべてのサービス (SNMP、FTP、TELNET、TFTP、ICMP、GLOBAL のすべて) のパケットを破棄します。

```
SET ACCESS FILTER=ALL DEFAULT=DISCARD ↵
```

 FILTER オプションの GLOBAL はすべてのサービスを意味します。ALL を指定した場合、SNMP、FTP、TELNET、TFTP、ICMP、GLOBAL を指定したことになります。

■ デフォルトのアクションでは、ICMP (PING など) のみ許可します。

```
SET ACCESS FILTER=ICMP DEFAULT=PASS ↵
```

### エントリーの作成例

- 管理用端末（ポート：1、IP アドレス：192.168.10.100）からの ICMP（PING パケットなど）を許可します。

```
ADD ACCESS FILTER=ICMP IPADDRESS=192.168.10.100 MASK=255.255.255.255
ACTION=PASS PORT=1 ↵
```

- ポート 5 配下の、IP アドレス：192.168.30.n からの ICMP（PING パケットなど）を拒否します。

```
ADD ACCESS FILTER=ICMP IPADDRESS=192.168.30.0 MASK=255.255.255.0
ACTION=DISCARD PORT=5 ↵
```

- ポート 7 配下の、IP アドレス：192.168.50.n からのすべてのパケットを許可します。

```
ADD ACCESS FILTER=GLOBAL IPADDRESS=192.168.50.0 MASK=255.255.255.0
ACTION=PASS PORT=7 ↵
```

- ポート 9 配下の、IP アドレス：192.168.70.n からの FTP と Telnet のパケットを許可します。

```
ADD ACCESS FILTER=FTP IPADDRESS=192.168.70.0 MASK=255.255.255.0
ACTION=PASS PORT=9 ↵
```

```
ADD ACCESS FILTER=TELNET IPADDRESS=192.168.70.0 MASK=255.255.255.0
ACTION=PASS PORT=9 ↵
```

- 🔗 エントリーとして設定するサービスは、ENABLE ACCESS FILTER コマンド（12 ページ）で有効にする必要があります。デフォルトでは無効になっています。

## 設定内容の確認

- 各サービスの有効/無効を確認します。

```
SHOW ACCESS FILTER ↵
```

- Telnet サービスのエントリー内容を確認します。

```
SHOW ACCESS FILTER=TELNET ↵
```

- 🔗 アクセスフィルターコマンドを有効にするには、RESTART REBOOT コマンド（「システム」の 14 ページ）で再起動が必要です。

## マッチ判定

受信パケットが複数のエントリーに一致した場合は、より限定された条件のエントリーの処理が適用されま

す（最長マッチ）。

■ Telnet サービスに対し、次のコマンドを実行したとします。

```
ENABLE ACCESS FILTER=TELNET ↓
```

```
SET ACCESS FILTER=TELNET DEFAULT=DISCARD ↓
```

```
ADD ACCESS FILTER=TELNET IPADDRESS=192.168.0.0 MASK=255.255.0.0  
ACTION=PASS PORT=1 ↓
```

```
ADD ACCESS FILTER=TELNET IPADDRESS=192.168.1.0 MASK=255.255.255.0  
ACTION=DISCARD PORT=1 ↓
```

| エントリー番号                   | ポート | マスク           | IP アドレス     | 処理      |
|---------------------------|-----|---------------|-------------|---------|
| (なし。Telnet サービスに対するデフォルト) | なし  | 0.0.0.0       | 0.0.0.0     | DISCARD |
| 1                         | 1   | 255.255.0.0   | 192.168.0.0 | PASS    |
| 2                         | 1   | 255.255.255.0 | 192.168.1.0 | DISCARD |

表 1:

受信パケットの送信元 IP アドレスが 192.168.1.1 であるとします。

このとき

<エントリー 1> 192.168.1.1 AND 255.255.0.0 -> 192.168.0.0 (一致)

<エントリー 2> 192.168.1.1 AND 255.255.255.0 -> 192.168.1.0 (一致)

となり、エントリー 1 とエントリー 2 の 2 つが一致します。

各エントリーのマスク長（マスクビット数）はエントリー 2（24 ビット） > エントリー 1（16 ビット）ですので、エントリー 2 の処理が適用されます。

したがって上記の Telnet フィルターグループは

「192.168.x.x は（192.168.1.x を除いて）許可」

「その他はすべて破棄」

という動作になります。

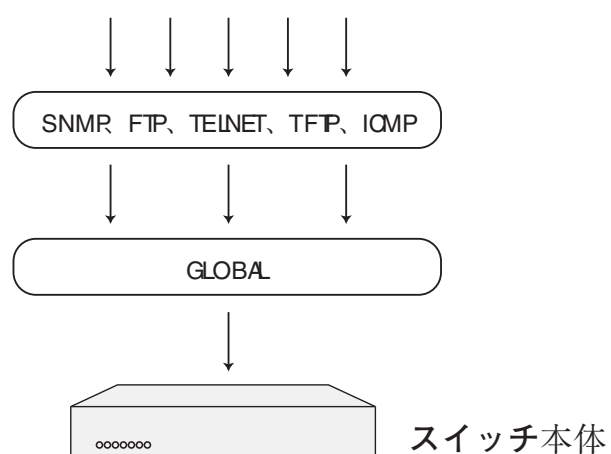
※マスク長：32 - 値が 1 である最下位ビット番号

## フィルター適用のまとめ

フィルタリング対象パケットは

1. 各サービス（Telnet、SNMP など）に関連付けられたフィルター
2. グローバルフィルター

の順でフィルタリングされます。



上記で一致した場合、さらなるマッチ判定は

1. 各ポートによるフィルター
2. PORT=ALL のフィルター
3. フィルターグループのデフォルト

の順で判定されます。

## 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

|                                      |    |
|--------------------------------------|----|
| ADD ACCESS FILTER . . . . .          | 8  |
| DELETE ACCESS FILTER ENTRY . . . . . | 10 |
| DISABLE ACCESS FILTER . . . . .      | 11 |
| ENABLE ACCESS FILTER . . . . .       | 12 |
| SET ACCESS FILTER . . . . .          | 13 |
| SET ACCESS FILTER ENTRY . . . . .    | 15 |
| SHOW ACCESS FILTER . . . . .         | 17 |

## ADD ACCESS FILTER

カテゴリー：アクセスフィルター

**ADD ACCESS FILTER**=**{SNMP|FTP|TELNET|TFTP|ICMP|GLOBAL}** **IPADDRESS**=*ipadd*  
**MASK**=*mask* **ACTION**=**{PASS|DISCARD}** **PORT**=**{*port-list*|ALL}**

*ipadd*: IP アドレス。xxx.xxx.xxx.xxx の形式

*mask*: マスクパターン。xxx.xxx.xxx.xxx の形式

*port-list*: スイッチポート番号 (FS808M: 1~8、FS816M: 1~16。ハイフン [-]、カンマ [,] を使った複数指定も可能)

### 解説

アクセスフィルターグループへエントリを追加する。システム全体で 512 個まで追加可能

### パラメーター

**FILTER** サービスに対応するグループ名。GLOBAL はここにリストされていないサービスを含む全サービス。

**IPADDRESS** フィルタリング対象の IP アドレス

**MASK** マスクパターン

**ACTION** パケットがフィルターの条件に一致したときのアクション。PASS は許可、DISCARD は破棄

**PORT** 対象となるスイッチポート番号または ALL。ALL を指定した場合はすべてのスイッチポートが対象となる

### 入力・出力・画面例

```
Manager > add access filter=telnet ipaddress=192.168.1.2 mask=255.255.255.0 action=discard port=all

Operation successful.
```

### 例

■Telnet グループに、IP アドレス (192.168.1.2) からのアクセスを拒否するエントリを追加する (全ポート対象)

```
ADD ACCESS FILTER=TELNET IPADDRESS=192.168.1.2 MASK=255.255.255.255
ACTION=DISCARD PORT=ALL
```

### 備考・注意事項



アクセスフィルター関連コマンドは、再起動後に設定内容が反映される

### 関連コマンド

DELETE ACCESS FILTER ENTRY (10 ページ)

ENABLE ACCESS FILTER (12 ページ)

SET ACCESS FILTER (13 ページ)

SET ACCESS FILTER ENTRY (15 ページ)

SHOW ACCESS FILTER (17 ページ)

## DELETE ACCESS FILTER ENTRY

カテゴリー：アクセスフィルター

**DELETE ACCESS FILTER**={SNMP|FTP|TELNET|TFTP|ICMP|GLOBAL} **ENTRY**=*num*

*num*: エントリー番号

### 解説

アクセスフィルターグループからエントリーを削除する

### パラメーター

**FILTER** 各サービスに対応するグループ名

**ENTRY** 対象となるアクセスフィルターのエントリー番号

### 入力・出力・画面例

```
Manager > delete access filter=telnet entry=1

Operation successful.
```

### 例

■Telnet グループのエントリー 1 を削除する

DELETE ACCESS FILTER=TELNET ENTRY=1

### 備考・注意事項

アクセスフィルター関連コマンドは、再起動後に設定内容が反映される

### 関連コマンド

ADD ACCESS FILTER (8 ページ)

ENABLE ACCESS FILTER (12 ページ)

SET ACCESS FILTER (13 ページ)

SET ACCESS FILTER ENTRY (15 ページ)

SHOW ACCESS FILTER (17 ページ)

## DISABLE ACCESS FILTER

カテゴリー：アクセスフィルター

**DISABLE ACCESS FILTER**=**{SNMP|FTP|TELNET|TFTP|ICMP|GLOBAL|ALL}**

### 解説

本システムへのアクセスフィルター機能を無効にする。デフォルトは無効。有効/無効の変更は（CREATE CONFIG コマンドで設定ファイルに保存し）、再起動したあと適用される

### パラメーター

**FILTER** 各サービスに対応するグループ名

### 入力・出力・画面例

```
Manager > disable access filter

Operation successful.
```

### 例

■TFTP サービスのアクセスフィルターを無効にする

DISABLE ACCESS FILTER=TFTP

### 備考・注意事項

アクセスフィルター関連コマンドは、再起動後に設定内容が反映される

### 関連コマンド

ADD ACCESS FILTER (8 ページ)

DELETE ACCESS FILTER ENTRY (10 ページ)

ENABLE ACCESS FILTER (12 ページ)

SET ACCESS FILTER (13 ページ)

SET ACCESS FILTER ENTRY (15 ページ)

SHOW ACCESS FILTER (17 ページ)

## ENABLE ACCESS FILTER

カテゴリー：アクセスフィルター

**ENABLE ACCESS FILTER**=**{SNMP|FTP|TELNET|TFTP|ICMP|GLOBAL|ALL}**

### 解説

本システムへのアクセスフィルター機能を有効にする。デフォルトは無効。有効/無効の変更は（CREATE CONFIG コマンドで設定ファイルに保存し）、再起動したあと適用される

### パラメーター

**FILTER** 各サービスに対応するグループ名

### 入力・出力・画面例

```
Manager > enable access filter

Operation successful.
```

### 例

■SNMP サービスのアクセスフィルターを有効にする

ENABLE ACCESS FILTER=SNMP

### 備考・注意事項

アクセスフィルター関連コマンドは、再起動後に設定内容が反映される

### 関連コマンド

ADD ACCESS FILTER (8 ページ)

DELETE ACCESS FILTER ENTRY (10 ページ)

DISABLE ACCESS FILTER (11 ページ)

SET ACCESS FILTER (13 ページ)

SET ACCESS FILTER ENTRY (15 ページ)

SHOW ACCESS FILTER (17 ページ)

## SET ACCESS FILTER

カテゴリー：アクセスフィルター

**SET ACCESS FILTER**=**{SNMP|FTP|TELNET|TFTP|ICMP|GLOBAL|ALL}** **DEFAULT**=**{PASS|DISCARD}**

### 解説

アクセスフィルターグループの設定を変更する

### パラメーター

**FILTER** 各サービスに対応するグループ名。GLOBAL はここにリストされていないサービスを含む全サービス。ALL を指定すると、SNMP、FTP、TELNET、TFTP、ICMP、GLOBAL すべてを指定することになる

**DEFAULT** 対応するフィルターグループのデフォルト処理。PASS は許可、DISCARD は破棄

### 入力・出力・画面例

```
Manager > set access filter=snmp default=discard

Operation successful.
```

### 例

■SNMP グループの IP アドレスを、デフォルトですべて破棄する設定に変更する

SET ACCESS FILTER=SNMP DEFAULT=DISCARD

### 備考・注意事項

アクセスフィルター関連コマンドは、再起動後に設定内容が反映される

### 関連コマンド

ADD ACCESS FILTER (8 ページ)

DELETE ACCESS FILTER ENTRY (10 ページ)

DISABLE ACCESS FILTER (11 ページ)

ENABLE ACCESS FILTER (12 ページ)

SET ACCESS FILTER ENTRY (15 ページ)

SHOW ACCESS FILTER (17 ページ)

## SET ACCESS FILTER ENTRY

カテゴリー：アクセスフィルター

```
SET ACCESS FILTER={SNMP|FTP|TELNET|TFTP|ICMP|GLOBAL} ENTRY=num
    [IPADDRESS=ipadd] [MASK=mask] [ACTION={PASS|DISCARD}] [PORT={port-list|
    ALL}]
```

**num**: エントリー番号

**ipadd**: IP アドレス。xxx.xxx.xxx.xxx の形式

**mask**: マスクパターン。xxx.xxx.xxx.xxx の形式

**port-list**: スイッチポート番号 (FS808M: 1~8、FS816M: 1~16。ハイフン [-]、カンマ [,] を使った複数指定も可能)

### 解説

アクセスフィルターグループのエントリーを変更する

### パラメーター

**FILTER** 各サービスに対応するグループ名

**ENTRY** 対象となるアクセスフィルターのエントリー番号

**IPADDRESS** フィルタリング対象の IP アドレス

**MASK** マスクパターン

**ACTION** パケットがフィルターの条件に一致したときのアクション

**PORT** 対象となるスイッチポート番号または ALL。ALL を指定した場合はすべてのスイッチポートが対象となる

### 入力・出力・画面例

```
Manager > set access filter=telnet entry=1 ipaddress=192.168.1.2 mask=255.255.255.255 ac-
tion=pass port=1-7

Operation successful.
```

### 例

■Telnet グループのエントリー 1 を変更する

```
SET ACCESS FILTER=TELNET ENTRY=1 IPADDRESS=192.168.1.2
    MASK=255.255.255.255 ACTION=PASS PORT=1-7
```

### 備考・注意事項

アクセスフィルター関連コマンドは、再起動後に設定内容が反映される

### 関連コマンド

ADD ACCESS FILTER (8 ページ)

DELETE ACCESS FILTER ENTRY (10 ページ)

DISABLE ACCESS FILTER (11 ページ)

ENABLE ACCESS FILTER (12 ページ)

SET ACCESS FILTER (13 ページ)

SHOW ACCESS FILTER (17 ページ)



## SHOW ACCESS FILTER

カテゴリー：アクセスフィルター

**SHOW ACCESS FILTER** [= {SNMP|FTP|TELNET|TFTP|ICMP|GLOBAL|ALL}]

### 解説

アクセスフィルターグループの設定内容を表示する

### パラメーター

**FILTER** 各サービスに対応するグループ名。GLOBAL はここにリストされていないサービスを含む全サービス。ALL を指定すると、SNMP、FTP、TELNET、TFTP、ICMP、GLOBAL すべてを指定することになる。省略すると簡易一覧表示となる

### 入力・出力・画面例

```
Manager > show access filter
```

| Filter | Default | Status   |
|--------|---------|----------|
| SNMP   | Pass    | Enabled  |
| FTP    | Discard | Enabled  |
| TELNET | Pass    | Disabled |
| TFTP   | Pass    | Enabled  |
| ICMP   | Discard | Enabled  |
| GLOBAL | Pass    | Enabled  |

```
Manager > show access filter=telnet
```

TELNET:

Access Filtering ..... Enabled

Port ..... 23

Default..... Discard

| Entry | IP           | MASK          | ACTION | PORT |
|-------|--------------|---------------|--------|------|
| 1     | 192.168.1.2  | 255.255.255.0 | Pass   | ALL  |
| 2     | 192.168.8.5  | 255.255.255.0 | Pass   | 1-7  |
| 3     | 192.168.40.5 | 255.255.0.0   | Pass   | 2    |

|         |   |
|---------|---|
| Filter  | フィルターグループ名                                      |
| Default | 対応するフィルターグループのデフォルト処理。許可 (Pass) または破棄 (Discard) |
| Status  | 有効 (Enabled) または無効 (Disabled)                   |

表 2:

|                  |  |
|------------------|--|
| Access Filtering | アクセスフィルタ機能の有効 (Enabled) または無効 (Disabled)             |
| Port             | 対象となる接続ポート番号   |
| Default          | 対応するフィルターグループのデフォルト処理。許可 (Pass) または破棄 (Discard)      |
| Entry            | エントリー番号  |
| IP               | フィルタリング対象の IP アドレス                                   |
| MASK             | マスクパターン  |
| ACTION           | パケットがフィルターの条件に一致したときのアクション。許可 (Pass) または破棄 (Discard) |
| PORT             | 対象となるポート番号 (数字) またはすべてのスイッチポート (ALL)                 |

表 3: FILTER オプション指定時

## 例

■フィルターグループ情報を一覧表示する

```
SHOW ACCESS FILTER
```

■Telnet グループの設定内容を表示する

```
SHOW ACCESS FILTER=TELNET
```

## 備考・注意事項

アクセスフィルター関連コマンドは、再起動後に設定内容が反映される

## 関連コマンド

ADD ACCESS FILTER (8 ページ)

DELETE ACCESS FILTER ENTRY (10 ページ)

DISABLE ACCESS FILTER (11 ページ)

ENABLE ACCESS FILTER (12 ページ)

SET ACCESS FILTER (13 ページ)

SET ACCESS FILTER ENTRY (15 ページ)