

# 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 . . . . .	12
ENABLE ACCESS FILTER . . . . .	14
SET ACCESS FILTER . . . . .	16
SET ACCESS FILTER ENTRY . . . . .	18
SHOW ACCESS FILTER . . . . .	20

## 概要・基本設定

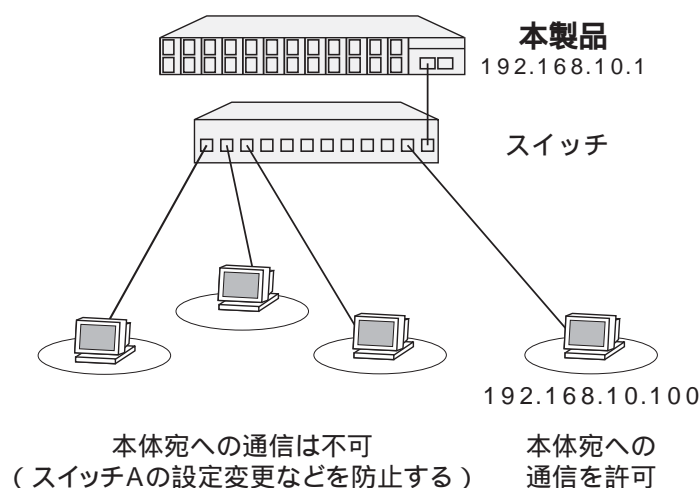
アクセスフィルタとは本製品宛への通信に適用するセキュリティ機能です。本製品宛のパケットを受信すると、受信パケットに関連付けられたフィルタを参照し、受信を許可するか、拒否するか決定を行います。

本製品では、各種サービス（IP、TELNET、FTP、SNMP）に IP アドレスおよび受信ポートを組み合わせ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。

## アクセスフィルタの基本設定

アクセスフィルタ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（14 ページ）でアクセスフィルタ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を設定します。

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

2. 次に、SET ACCESS FILTER コマンド（16 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（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 ↵
```

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 コマンド（「システム」の 13 ページ）で再起動します。システム全体を再起動する場合は、RESTART コマンド（「システム」の 13 ページ）に REBOOT オプションを指定します。

```
Manager > RESTART REBOOT

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

マネージメントモジュールのみを再起動する場合は、RESTART コマンド（「システム」の 13 ページ）に MGMT オプションを指定します。

```
Manager > RESTART MGMT ↵
```

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、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、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 (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 ↵
```

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 ↵
```

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 ↵
```

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 ↵
```

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

- ㄨ エントリーとして設定するサービスは、ENABLE ACCESS FILTER コマンド (14 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 ↵
```

- ㄨ アクセスフィルターコマンドを有効にするには、RESTART コマンド (「システム」の 13 ページ) を実行して、システムを再起動する必要があります。

## 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 ↵
```

```
ADD ACCESS FILTER=TELNET IPADDRESS=192.168.1.0 MASK=255.255.255.0  
ACTION=DISCARD ↵
```

エントリー番号	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)	0.0.0.0	0.0.0.0	DISCARD
1	255.255.0.0	192.168.0.0	PASS
2	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 であるとしてします。

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。

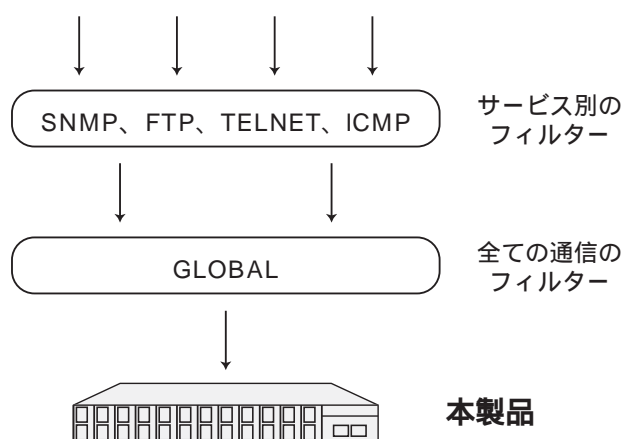
マスク長: 32 - 値が 1 である最下位ビット番号

### 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。



## 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

ADD ACCESS FILTER . . . . .	8
DELETE ACCESS FILTER ENTRY . . . . .	10
DISABLE ACCESS FILTER . . . . .	12
ENABLE ACCESS FILTER . . . . .	14
SET ACCESS FILTER . . . . .	16
SET ACCESS FILTER ENTRY . . . . .	18
SHOW ACCESS FILTER . . . . .	20

## ADD ACCESS FILTER

カテゴリー：アクセスフィルター / 一般コマンド

対象機種：MC2600、MC2700

```
ADD ACCESS FILTER={SNMP|FTP|TELNET|ICMP|GLOBAL} IPADDRESS=ipadd
      MASK=mask ACTION={PASS|DISCARD}
```

***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

### 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** 各サービスに対応するグループ名。GLOBAL は SNMP、FTP、TELNET、ICMP 以外を含む全サービス

**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

### 入力・出力・画面例

```
Manager > add access filter=telnet ipaddress=192.168.1.2 mask=255.255.255.255 ac-
tion= discard

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

```
ADD ACCESS FILTER=TELNET IPADDRESS=192.168.1.2 MASK=255.255.255.255
      ACTION=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

DELETE ACCESS FILTER ENTRY ( 10 ページ )

ENABLE ACCESS FILTER ( 14 ページ )

SET ACCESS FILTER ( 16 ページ )

SET ACCESS FILTER ENTRY ( 18 ページ )

SHOW ACCESS FILTER ( 20 ページ )

## DELETE ACCESS FILTER ENTRY

カテゴリー：アクセスフィルター / 一般コマンド

対象機種：MC2600、MC2700

**DELETE ACCESS FILTER**=**{SNMP|FTP|TELNET|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。GLOBAL は SNMP、FTP、TELNET、ICMP 以外を含む全サービス

**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 ( 14 ページ )

SET ACCESS FILTER ( 16 ページ )

SET ACCESS FILTER ENTRY ( 18 ページ )

SHOW ACCESS FILTER ( 20 ページ )

## DISABLE ACCESS FILTER

カテゴリー：アクセスフィルター / 一般コマンド

対象機種：MC2600、MC2700

**DISABLE ACCESS FILTER**={SNMP|FTP|TELNET|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、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。GLOBAL は SNMP、FTP、TELNET、ICMP 以外を含む全サービス。ALL を指定すると、SNMP、FTP、TELNET、ICMP、GLOBAL のすべてのグループを指定することになる

### 入力・出力・画面例

```
Manager > disable access filter

Operation successful.
```

### 例

FTP サービスのアクセスフィルターを無効にする

DISABLE ACCESS FILTER=FTP

### 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 ( 14 ページ )

SET ACCESS FILTER ( 16 ページ )

SET ACCESS FILTER ENTRY ( 18 ページ )

SHOW ACCESS FILTER ( 20 ページ )

## ENABLE ACCESS FILTER

カテゴリー：アクセスフィルター / 一般コマンド

対象機種：MC2600、MC2700

**ENABLE ACCESS FILTER**={SNMP|FTP|TELNET|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、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。GLOBAL は SNMP、FTP、TELNET、ICMP 以外を含む全サービス。ALL を指定すると、SNMP、FTP、TELNET、ICMP、GLOBAL のすべてのグループを指定することになる

### 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 ( 12 ページ )

SET ACCESS FILTER ( 16 ページ )

SET ACCESS FILTER ENTRY ( 18 ページ )

SHOW ACCESS FILTER ( 20 ページ )

## SET ACCESS FILTER

カテゴリー：アクセスフィルター / 一般コマンド

対象機種：MC2600、MC2700

```
SET ACCESS FILTER={SNMP|FTP|TELNET|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 SNMP、FTP、TELNET、ICMP 以外を含む全サービス。ALL を指定すると、SNMP、FTP、TELNET、ICMP、GLOBAL のすべてのグループ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 ( 12 ページ )

ENABLE ACCESS FILTER ( 14 ページ )



SET ACCESS FILTER ENTRY ( 18 ページ )

SHOW ACCESS FILTER ( 20 ページ )

## SET ACCESS FILTER ENTRY

カテゴリー：アクセスフィルター / 一般コマンド

対象機種：MC2600、MC2700

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

**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

### 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。GLOBAL は SNMP、FTP、TELNET、ICMP 以外を含む全サービス

**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

### 入力・出力・画面例

```
Manager > set access filter=telnet entry=1 ipaddress=192.168.1.2 mask=255.255.255.255 action=pass
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
```

### 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 ( 12 ページ )

ENABLE ACCESS FILTER ( 14 ページ )

SET ACCESS FILTER ( 16 ページ )

SHOW ACCESS FILTER ( 20 ページ )

## SHOW ACCESS FILTER

カテゴリー：アクセスフィルター / 一般コマンド

対象機種：MC2600、MC2700

**SHOW ACCESS FILTER** [= {SNMP|FTP|TELNET|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 SNMP、FTP、TELNET、ICMP 以外を含む全サービス。ALL を指定すると、SNMP、FTP、TELNET、ICMP、GLOBAL のすべてのグループ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
ICMP    Discard   Enabled
GLOBAL  Pass      Enabled
-----

Manager > show access filter=telnet

TELNET:
Access Filtering..... Enabled
Port ..... 23
Default..... Discard

Entry    IP             MASK             ACTION
-----
1        192.168.1.2    255.255.255.255 Pass
2        192.168.8.5    255.255.255.255 Pass
3        192.168.40.5   255.255.255.255 Pass
-----

Manager >
```

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 ( 12 ページ )

ENABLE ACCESS FILTER ( 14 ページ )

SET ACCESS FILTER ( 16 ページ )

SET ACCESS FILTER ENTRY ( 18 ページ )