



管理 ACL コマンド

この章は、次の項で構成されています。

- [deny \(管理\) \(2 ページ\)](#)
- [permit \(管理\) \(4 ページ\)](#)
- [management access-list \(6 ページ\)](#)
- [management access-class \(8 ページ\)](#)
- [show management access-list \(9 ページ\)](#)
- [show management access-class \(10 ページ\)](#)

deny (管理)

管理アクセスリスト (ACL) の **permit** ルール (ACE) を設定するには、**deny** 管理アクセスリスト コンフィギュレーション モード コマンドを使用します。

構文

```
deny [interface-id] [service service]
```

```
deny ip-source {ipv4-address | ipv6-address/ipv6-prefix-length} [mask {mask | prefix-length}]  
[interface-id] [service service]
```

パラメータ

- **interface-id** : (オプション) インターフェイス ID を指定します。インターフェイス ID には次のタイプのいずれかを指定できます: イーサネット ポート、ポート チャネルまたは VLAN
- **service service** : (オプション) サービス タイプを指定します。使用可能な値は、Telnet、SSH、HTTP、HTTPS、および SNMP です。
- **ipv4-address** : 送信元 IPv4 アドレスを指定します。
- **ipv6-address/ipv6-prefix-length** : 送信元 IPv6 アドレスと送信元 IPv6 アドレスのプレフィックス長を指定します。プレフィックス長は、スラッシュ (/) で開始する必要があります。パラメータは、省略可能です。
- **mask mask** : 送信元 IPv4 アドレス ネットワーク マスクを指定します。パラメータは、IPv4 アドレスにのみ関連します。
- **mask prefix-length** : 送信元 IPv4 アドレス プレフィックスを構成するビット数を指定します。プレフィックス長は、スラッシュ (/) で開始する必要があります。パラメータは、IPv4 アドレスにのみ関連します。(範囲: 0 ~ 32)

デフォルト設定

ルールは設定されていません。

コマンドモード

管理アクセスリスト コンフィギュレーション モード

使用上のガイドライン

IP アドレスが適切なインターフェイスで定義されている場合は、イーサネット、VLAN、ポート チャネル パラメータのルールが有効です。

例

次の例では、**mlist** と呼ばれる ACL のすべてのポートを拒否します。

```
switchxxxxxx(config)# management access-list mlist  
switchxxxxxx(config-macl)# deny
```

permit (管理)

管理アクセスリスト (ACL) の **permit** ルール (ACE) を設定するには、**permit** 管理アクセスリスト コンフィギュレーション モード コマンドを使用します。

構文

```
permit [interface-id] [service service]
```

```
permit ip-source {ipv4-address | ipv6-address/ipv6-prefix-length} [mask {mask | prefix-length}]  
[interface-id] [service service]
```

パラメータ

- **interface-id** : (オプション) インターフェイス ID を指定します。インターフェイス ID には次のタイプのいずれかを指定できます: イーサネットポート、ポートチャネルまたは VLAN
- **service service** : (オプション) サービスタイプを指定します。使用可能な値は、Telnet、SSH、HTTP、HTTPS、および SNMP です。
- **ipv4-address** : 送信元 IPv4 アドレスを指定します。
- **ipv6-address/ipv6-prefix-length** : 送信元 IPv6 アドレスおよび送信元 IPv6 アドレスのプレフィックス長を指定します。プレフィックス長は、スラッシュ (/) で開始する必要があります。パラメータは、省略可能です。
- **mask mask** : 送信元 IPv4 アドレス ネットワーク マスクを指定します。このパラメータは、IPv4 アドレスにのみ関連します。
- **mask prefix-length** : 送信元 IPv4 アドレス プレフィックスを構成するビット数を指定します。プレフィックス長は、スラッシュ (/) で開始する必要があります。このパラメータは、IPv4 アドレスにのみ関連します。(範囲: 0 ~ 32)

デフォルト設定

ルールは設定されていません。

コマンドモード

管理アクセスリスト コンフィギュレーション モード

使用上のガイドライン

IP アドレスが適切なインターフェイスで定義されている場合は、イーサネット、VLAN、ポートチャネルパラメータのルールが有効です。

例

次の例では、**mlist** と呼ばれる ACL のすべてのポートを許可します

```
switchxxxxxx(config)# management access-list mlist  
switchxxxxxx(config-macl)# permit
```

management access-list

管理アクセスリスト (ACL) を設定して、管理アクセスリスト コンフィギュレーション モードを開始するには、**management access-list** グローバル コンフィギュレーション モード コマンドを使用します。ACL を削除するには、このコマンドの **no** 形式を使用します。

構文

management access-list *name*

no management access-list *name*

パラメータ

name : ACL 名を指定します。(長さ : 1 ~ 32 文字)

コマンドモード

グローバル コンフィギュレーション モード

使用上のガイドライン

このコマンドを使用すると、管理アクセスリストを設定できます。このコマンドは、管理アクセスリスト コンフィギュレーション モードを開始します。ここでは、拒否アクセス条件または許可アクセス条件が **deny** と **permit** コマンドを使用して定義されています。

一致条件が定義されていない場合、デフォルト値は **deny** です。

アクセス リスト コンテキストを再入力すると、新しいルールがアクセス リストの最後に入力されます。

[management access-class \(8 ページ\)](#) コマンドを使用すると、アクティブなアクセス リストを選択できます。

アクティブな管理リストは更新または削除することはできません。

IPv4 パケットでトンネル化されている IPv6 管理トラフィックの場合、管理 ACL が外部 IPv4 ヘッダーに最初に適用され (サービス フィールドのルールは無視され)、次に内部 IPv6 ヘッダーに適用されます。

例 1 : 次に、**mlist** という管理アクセスリストを作成し、管理 **gi1/0/1** と **gi1/0/9** を設定し、新しいアクセスリストをアクティブリストにする例を示します。

```
switchxxxxxx(config)# management access-list mlist
switchxxxxxx(config-macl)# permit gi1/0/1
switchxxxxxx(config-macl)# permit gi1/0/9
switchxxxxxx(config-macl)# exit
switchxxxxxx(config)#
```

例 2 : 次に、「mlist」という管理アクセスリストを作成し、**gi1/0/1** と **gi1/0/9** を除くすべてのインターフェイスを管理インターフェイスに設定し、新しいアクセスリストをアクティブリストにする例を示します。

```
switchxxxxxx(config)# management access-list mlist  
switchxxxxxx(config-macl)# deny gil/0/1  
switchxxxxxx(config-macl)# deny gil/0/9  
switchxxxxxx(config-macl)# permit  
switchxxxxxx(config-macl)# exit  
switchxxxxxx(config)#
```

management access-class

アクティブな管理アクセス リスト (ACL) を定義して管理接続を制限するには、**management access-class** グローバル コンフィギュレーション モード コマンドを使用します。管理接続制限を無効にするには、このコマンドの **no** 形式を使用します。

構文

```
management access-class {console-only | name}
```

```
no management access-class
```

パラメータ

- **console-only** : デバイスをコンソールのみから管理できるように指定します。
- **name** : 使用する ACL 名を指定します。(長さ: 1 ~ 32 文字)

デフォルト設定

デフォルト設定では、管理接続が制限されていません。

コマンドモード

グローバル コンフィギュレーション モード

例

次の例では、**m1ist** と呼ばれるアクセス リストをアクティブな管理アクセス リストとして定義します。

```
switchxxxxxxx(config)# management access-class m1ist
```

show management access-list

管理アクセスリスト (ACL) を表示するには、**show management access-list** 特権 EXEC モード コマンドを使用します。

構文

```
show management access-list [name]
```

パラメータ

name : (オプション) 表示する管理アクセスリストの名前を指定します。(長さ : 1 ~ 32 文字)

デフォルト設定

すべての管理 ACL が表示されます。

コマンドモード

特権 EXEC モード

例

次の例では、**m1** 管理 ACL を表示します。

```
switchxxxxx# show management access-list m1
m1
--
deny service telnet
permit gil/0/1 service telnet
! (Note: all other access implicitly denied)
console(config-macl)#
```

show management access-class

アクティブな管理アクセスリスト (ACL) の情報を表示するには、**show management access-class** 特権 EXEC モード コマンドを使用します。

構文

show management access-class

パラメータ

このコマンドには引数またはキーワードはありません。

コマンドモード

特権 EXEC モード

例

次の例では、アクティブな管理 ACL 情報を表示します。

```
switchxxxxxx# show management access-class  
Management access-class is enabled, using access list mlist
```

翻訳について

このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。