



M コマンド

この章では、M で始まる Cisco NX-OS セキュリティ コマンドについて説明します。

mac access-list

Media Access Control (MAC; メディア アクセス コントロール) アクセス コントロール リスト (ACL) を作成するか、または特定の ACL の MAC 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、**mac access-list** コマンドを使用します。MAC ACL を削除するには、このコマンドの **no** 形式を使用します。

mac access-list *access-list-name*

no mac access-list *access-list-name*

構文の説明

<i>access-list-name</i>	MAC ACL の名前。最大 64 文字で、大文字と小文字を区別した英数字で指定します。
-------------------------	--

コマンド デフォルト

デフォルトでは、MAC ACL は定義されません。

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

コマンド履歴

リリース	変更内容
4.0(0)N1(1a)	このコマンドが追加されました。

使用上のガイドライン

非 IP トラフィックをフィルタリングするには、MAC ACL を使用します。

mac access-list コマンドを使用すると、スイッチで MAC アクセス リスト コンフィギュレーション モードが開始されます。このモードで、**MAC deny** コマンドおよび **permit** コマンドを使用し、ACL のルールを設定します。指定した ACL が存在しない場合は、このコマンドの入力時にスイッチで新しい ACL が作成されます。

ACL をインターフェイスに適用するには、**mac access-group** コマンドを使用します。

すべての MAC ACL は、最終ルールとして、次の暗黙ルールが設定されます。

```
deny any any protocol
```

この暗黙のルールにより、トラフィックのレイヤ 2 ヘッダーに指定されたプロトコルに関係なく、一致しないトラフィックがスイッチによって確実に拒否されます。

例

次に、**mac-acl-01** という MAC ACL の MAC アクセス リスト コンフィギュレーション モードを開始する例を示します。

```
switch(config)# mac access-list mac-acl-01
switch(config-acl)#
```

関連コマンド

コマンド	説明
deny (MAC)	MAC ACL に拒否 (deny) ルールを設定します。
mac access-group	MAC ACL をインターフェイスに適用します。
permit (MAC)	MAC ACL に許可 (permit) ルールを設定します。
show mac access-lists	すべての MAC ACL または特定の MAC ACL を表示します。

mac port access-group

MAC アクセス コントロール リスト (ACL) をインターフェイスに適用するには、**mac port access-group** コマンドを使用します。インターフェイスから MAC ACL を削除するには、このコマンドの **no** 形式を使用します。

mac port access-group *access-list-name*

no mac port access-group *access-list-name*

構文の説明

<i>access-list-name</i>	MAC ACL の名前。最大 64 文字で、大文字と小文字を区別した英数字で指定します。
-------------------------	--

コマンド デフォルト

なし

コマンド モード

インターフェイス コンフィギュレーション モード
仮想イーサネット インターフェイス コンフィギュレーション モード

コマンド履歴

リリース	変更内容
4.0(0)N1(1a)	このコマンドが追加されました。
5.1(3)N1(1)	このコマンドのサポートが、仮想イーサネット インターフェイスに追加されました。

使用上のガイドライン

デフォルトでは、インターフェイスに MAC ACL は適用されません。

MAC ACL を非 IP トラフィックに適用します。

mac port access-group コマンドを使用することにより、次のインターフェイス タイプに対して、MAC ACL をポート ACL として適用できます。

- レイヤ 2 インターフェイス
- レイヤ 2 EtherChannel インターフェイス
- 仮想イーサネット インターフェイス

MAC ACL を VLAN ACL として適用することもできます。詳細については、**match** コマンドを参照してください。

スイッチで MAC ACL が適用されるのは、着信トラフィックだけです。スイッチは、MAC ACL を適用すると、パケットを ACL のルールに対してチェックします。最初の一致ルールによってパケットが許可されると、そのパケットはスイッチで引き続き処理されます。最初の一致ルールによってパケットが拒否されると、そのパケットはスイッチで廃棄され、ICMP ホスト到達不能メッセージが戻されません。

スイッチから特定の ACL を削除した場合、インターフェイスからその ACL を削除しなくても、削除した ACL はインターフェイス上のトラフィックには影響しません。

例

次に、イーサネット インターフェイス 1/2 に対して、mac-acl-01 という MAC ACL を適用する例を示します。

```
switch(config)# interface ethernet 1/2
switch(config-if)# mac port access-group mac-acl-01
switch(config-if)#
```

次に、イーサネット インターフェイス 1/2 から、mac-acl-01 という MAC ACL を削除する例を示します。

```
switch(config)# interface ethernet 1/2
switch(config-if)# no mac port access-group mac-acl-01
switch(config-if)#
```

次に、特定の仮想イーサネット インターフェイスに対して、mac-acl-03 という名前の MAC ACL を適用する例を示します。

```
switch# configure terminal
switch(config)# interface vethernet 1
switch(config-if)# mac port access-group mac-acl-03
switch(config-if)#
```

関連コマンド

コマンド	説明
interface vethernet	仮想イーサネット インターフェイスを設定します。
mac access-list	MAC ACL を設定します。
show access-lists	すべての ACL を表示します。
show mac access-lists	特定の MAC ACL またはすべての MAC ACL を表示します。
show running-config interface	すべてのインターフェイスまたは特定のインターフェイスの実行コンフィギュレーションを表示します。

match

VLAN アクセス マップ内のトラフィック フィルタリング用としてアクセス コントロール リスト (ACL) を指定するには、**match** コマンドを使用します。VLAN アクセス マップから **match** コマンドを削除するには、このコマンドの **no** 形式を使用します。

```
match {ip | ipv6 | mac} address access-list-name
```

```
no match {ip | ipv6 | mac} address access-list-name
```

構文の説明

ip	IPv4 ACL を指定します。
ipv6	IPv6 ACL を指定します。
mac	MAC ACL を指定します。
address <i>access-list-name</i>	IPv4 アドレス、IPv6 アドレス、または MAC アドレス、およびアクセス リスト名を指定します。名前では最大 64 文字までの英数字を使用でき、大文字と小文字が区別されます。

コマンド デフォルト

デフォルトでは、スイッチによりトラフィックが分類され、IPv4 トラフィックには IPv4 ACL が、その他のすべてのトラフィックには MAC ACL が適用されます。

コマンド モード

VLAN アクセスマップ コンフィギュレーション モード

コマンド履歴

リリース	変更内容
4.0(0)N1(1a)	このコマンドが追加されました。

使用上のガイドライン

指定できる **match** コマンドは、アクセス マップごとに 1 つだけです。

例

次に、**vlan-map-01** という名前で VLAN アクセス マップを作成して、そのマップに **ip-acl-01** という名前の IPv4 ACL を割り当て、スイッチが ACL に一致するパケットを転送するよう指定し、マップに一致するトラフィックの統計情報をイネーブルにする例を示します。

```
switch(config)# vlan access-map vlan-map-01
switch(config-access-map)# match ip address ip-acl-01
switch(config-access-map)# action forward
switch(config-access-map)# statistics
```

関連コマンド

コマンド	説明
action	VLAN アクセス マップにトラフィック フィルタリングのアクションを指定します。
show vlan access-map	すべての VLAN アクセス マップまたは 1 つの VLAN アクセス マップを表示します。

コマンド	説明
show vlan filter	VLAN アクセス マップが適用されている方法に関する情報を表示します。
vlan access-map	VLAN アクセス マップを設定します。
vlan filter	1 つ以上の VLAN に VLAN アクセス マップを適用します。

