



## 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

Mac Access Control List (ACL; アクセス コントロール リスト) 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。スペースまたは引用符は使用できません。				
デフォルト	なし				
コマンド モード	グローバル コンフィギュレーション				
サポートされるユーザロール	network-admin vdc-admin				
コマンド履歴	<table><thead><tr><th>リリース</th><th>変更内容</th></tr></thead><tbody><tr><td>4.0(1)</td><td>このコマンドが追加されました。</td></tr></tbody></table>	リリース	変更内容	4.0(1)	このコマンドが追加されました。
リリース	変更内容				
4.0(1)	このコマンドが追加されました。				
使用上のガイドライン	デフォルトでは、MAC ACL は定義されません。 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。パケットの分類をディセーブルにした場合は、MAC ACL を使用して、すべてのトラフィックをフィルタリングできます。				

**mac access-list** コマンドを使用すると、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 port 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確実に拒否されます。

MAC ACL の各ルールの統計情報を記録するには、**statistics per-entry** コマンドを使用します。デバイスは、暗黙ルールの統計情報を記録しません。暗黙ルールに一致したパケットの統計情報を記録するには、パケットの **deny** (拒否) ルールを明示的に設定する必要があります。

このコマンドには、ライセンスは不要です。

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

## 関連コマンド

コマンド	説明
<b>deny (MAC)</b>	MAC ACL に拒否 (deny) ルールを設定します。
<b>mac port access-group</b>	MAC ACL をインターフェイスに適用します。
<b>permit (MAC)</b>	MAC ACL に permit (許可) ルールを設定します。
<b>show mac access-lists</b>	すべての MAC ACL または特定の MAC ACL を表示します。
<b>statistics per-entry</b>	ACL の各エントリの統計情報の収集をイネーブルにします。

# mac packet-classify

レイヤ 2 インターフェイスの MAC パケット分類をイネーブルにするには、**mac packet-classify** コマンドを使用します。MAC パケット分類をディセーブルにするには、このコマンドの **no** 形式を使用します。

**mac packet-classify**

**no mac packet-classify**

## 構文の説明

このコマンドには、引数またはキーワードはありません。

## 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

## サポートされるユーザロール

network-admin  
vdc-admin

## コマンド履歴

リリース	変更内容
4.2(1)	このコマンドが追加されました。

## 使用上のガイドライン

このコマンドには、ライセンスは不要です。

MAC パケット分類を使用すると、レイヤ 2 インターフェイス上の MAC ACL が、IP トラフィックを含む、インターフェイスに入るすべてのトラフィックに適用されるか、または非 IP トラフィックだけに適用されるかを、コントロールできます。

レイヤ 2 インターフェイス上で MAC パケット分類がイネーブルにされているとき、インターフェイス上の MAC ACL は、IP トラフィックを含む、インターフェイスに入るすべてのトラフィックに適用されます。また、インターフェイス上の IP ポート ACL は適用できません。

レイヤ 2 インターフェイス上で MAC パケット分類がディセーブルにされているとき、インターフェイス上の MAC ACL は、インターフェイスに入る非 IP トラフィックだけに適用されます。また、インターフェイス上の IP ポート ACL を適用できます。

レイヤ 2 インターフェイスとしてインターフェイスを設定するには、**switchport** コマンドを使用します。

## 例

次の例では、イーサネット インターフェイスがレイヤ 2 インターフェイスとして動作するよう設定し、MAC パケット分類をイネーブルにする方法を示します。

```
switch# conf t
switch(config)# interface ethernet 2/3
switch(config-if)# switchport
switch(config-if)# mac packet-classify
switch(config-if)#
```

次に、MAC パケット分類がイネーブルのときに、インターフェイスに IP ポート ACL の適用を試行する場合に、表示されるイーサネット インターフェイスとエラー メッセージの設定を参照する方法を示します。

```
switch(config)# show running-config interface ethernet 2/3

!Command: show running-config interface Ethernet2/3
!Time: Wed Jun 24 13:06:49 2009

version 4.2(1)

interface Ethernet2/3
 ip access-group ipacl in
 mac port access-group macacl
 switchport
 mac packet-classify

switch(config)# interface ethernet 2/3
switch(config-if)# ip port access-group ipacl in
ERROR: The given policy cannot be applied as mac packet classification is enable
d on this port
switch(config-if)#
```

## 関連コマンド

コマンド	説明
<b>ip port access-group</b>	IPV4 ACL をポート ACL としてインターフェイスに適用します。
<b>ipv6 port traffic-filter</b>	IPV6 ACL をポート ACL としてインターフェイスに適用します。
<b>switchport</b>	インターフェイスが、レイヤ 2 インターフェイスとして動作するよう設定します。

# mac port access-group

MAC Access Control List (ACL; アクセス コントロール リスト) 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

*access-list-name* 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。

## 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

## サポートされるユーザロール

network-admin  
vdc-admin

## コマンド履歴

リリース	変更内容
4.0(1)	このコマンドが追加されました。

## 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。

デバイス上にレイヤ 3 ヘッダーに基づくトラフィック分類が設定されていない場合を除き、MAC ACL は非 IP トラフィックに適用されます。パケット分類がディセーブルの場合は、MAC ACL がすべてのトラフィックに適用されます。

**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 イーサネット ポートチャネル 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、[P.339](#)の [match \(VLAN アクセス マップ\)](#) コマンドを参照してください。

MAC ACL が適用されるのは、インバウンドトラフィックだけです。MAC ACL が適用されると、パケットが ACL のルールに対してチェックされます。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、そのパケットはドロップされ、ICMP ホスト到達不能メッセージが戻されます。

デバイスから特定の 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。

このコマンドには、ライセンスは不要です。

## 例

次に、イーサネット インターフェイス 2/1 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 t
switch(config)# interface ethernet 2/1
switch(config-if)# mac port access-group mac-acl-01
```

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

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

## 関連コマンド

コマンド	説明
<b>mac access-list</b>	MAC ACL を設定します。
<b>show access-lists</b>	すべての ACL を表示します。
<b>show mac access-lists</b>	特定の MAC ACL またはすべての MAC ACL を表示します。
<b>show running-config interface</b>	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 (クラス マップ)

コントロールプレーン クラス マップの一致基準を設定するには、**match** コマンドを使用します。コントロールプレーン ポリシー マップの一致基準を削除するには、このコマンドの **no** 形式を使用します。

**match access-group name** *access-list*

**match exception** {[ip | ipv6] {icmp {redirect | unreachable} | option}}

**match protocol arp**

**match redirect** {arp-inspect | dhcp-snoop}

**no match access-group name** *access-list*

**no match exception** {[ip | ipv6] {icmp {redirect | unreachable} | option}}

**no match protocol arp**

**no match redirect** {arp-inspect | dhcp-snoop}

## 構文の説明

<b>access-group name</b> <i>access-list</i>	IP ACL または MAC ACL と一致させます。
<b>exception</b>	例外パケットを一致させます。
<b>ip</b>	IPv4 例外パケットを一致させます。
<b>ipv6</b>	IPv6 例外パケットを一致させます。
<b>icmp</b>	IPv4 または IPv6 の ICMP パケットを一致させます。
<b>redirect</b>	IPv4 または IPv6 の ICMP リダイレクトパケットを一致させます。
<b>unreachable</b>	IPv4 または IPv6 の ICMP 到達不能パケットを一致させます。
<b>option</b>	IPv4 または IPv6 の ICMP オプションパケットを一致させます。
<b>protocol arp</b>	Address Resolution Protocol (ARP; アドレス解決プロトコル) パケットを一致させます。
<b>redirect {arp-inspect   dhcp-snoop}</b>	ダイナミック ARP インスペクションまたは DHCP スヌーピング リダイレクトパケットを一致させます。

## デフォルト

なし

## コマンド モード

クラス マップ コンフィギュレーション

## サポートされるユーザロール

network-admin  
vdc-admin

## コマンド履歴

リリース	変更内容
4.0(3)	ポリシング IPv6 パケットのサポートが追加されました。
4.0(1)	このコマンドが追加されました。

## 使用上のガイドライン

このコマンドで ACL を指定するには、事前に IP ACL または MAC ACL を作成しておく必要があります。

このコマンドを使用できるのは、デフォルトの VDC だけです。

このコマンドには、ライセンスは不要です。

## 例

次に、コントロールプレーン クラス マップの一致基準を指定する例を示します。

```
switch# config t
switch(config)# class-map type control-plane ClassMapA
switch(config-pmap)# match exception ip icmp redirect
switch(config-pmap)# match redirect arp-inspect
```

次に、コントロールプレーン クラス マップの一致基準を削除する例を示します。

```
switch# config t
switch(config)# class-map type control-plane ClassMapA
switch(config-pmap)# no match exception ip icmp redirect
```

## 関連コマンド

コマンド	説明
<b>class-map type control-plane</b>	コントロールプレーン クラス マップを作成または指定して、クラス マップ コンフィギュレーション モードを開始します。
<b>show class-map type control-plane</b>	コントロールプレーン ポリシー マップの設定情報を表示します。



## match (VLAN アクセス マップ)

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 Access Control List (ACL; アクセス コントロール リスト) 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

<b>address</b>	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。 <i>access-list-name</i>
<b>ip</b>	ACL が IPv4 ACL になるように指定します。
<b>ipv6</b>	ACL が IPv6 ACL になるように指定します。
<b>mac</b>	ACL が MAC ACL になるように指定します。

### デフォルト

なし

### 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

### サポートされるユーザ ロール

network-admin  
vdc-admin

### コマンド履歴

リリース	変更内容
4.1(2)	<b>ipv6</b> キーワードが追加されました。
4.0(1)	このコマンドが追加されました。

### 使用上のガイドライン

VLAN アクセス マップでは、1 つのエントリについて 1 つまたは複数の **match** コマンドを指定できます。

デフォルトでは、デバイス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、IPv6 トラフィックには IPv6 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。

このコマンドには、ライセンスは不要です。

## ■ match (VLAN アクセス マップ)

## 例

次の例では、vlan-map-01 という名前の VLAN アクセス マップを作成し、それぞれに 2 つの **match** コマンドと 1 つの **action** コマンドがある 2 つのエントリを追加する方法を示します。

```
switch(config-access-map) # 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) # match mac address mac-acl-00f
switch(config-access-map) # vlan access-map vlan-map-01
switch(config-access-map) # match ip address ip-acl-320
switch(config-access-map) # match mac address mac-acl-00e
switch(config-access-map) # action drop
switch(config-access-map) # show vlan access-map

Vlan access-map vlan-map-01 10
    match ip: ip-acl-01
    match mac: mac-acl-00f
    action: forward
Vlan access-map vlan-map-01 20
    match ip: ip-acl-320
    match mac: mac-acl-00e
    action: drop
```

## 関連コマンド

コマンド	説明
<b>action</b>	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。
<b>show vlan access-map</b>	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。
<b>show vlan filter</b>	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。
<b>vlan access-map</b>	VLAN アクセス マップを設定します。
<b>vlan filter</b>	1 つまたは複数の VLAN に VLAN アクセス マップを適用します。