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*

シンタックスの説明

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。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

リリース	変更内容
4.0(1)	このコマンドが導入されました。

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** 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。暗黙ルールの統計情報は記録されません。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
deny（MAC）	MAC ACL に deny（拒否）ルールを設定します。
mac port access-group	MAC ACL をインターフェイスに適用します。
permit（MAC）	MAC ACL に permit（許可）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。
statistics per-entry	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 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*

シンタックスの説明

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)	このコマンドが導入されました。

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、「match（VLAN アクセス マップ）」（p.191）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
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）

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** | **mac**} **address** *access-list-name*

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

シンタックスの説明

address *access-list-name*	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。
ip	ACL が IPv4 ACL であることを指定します。
mac	ACL が MAC ACL であることを指定します。

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
4.0(1)	このコマンドが導入されました。

使用上のガイドライン

1 つのアクセス マップについて、1 つの **match** コマンドだけを指定できます。

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、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。

例

次に、vlan-map-01 という VLAN アクセス マップを作成し、このマップに ip-acl-01 という IPv4 ACL を割り当て、ACL と一致するパケットを転送し、マップと一致したトラフィックの統計情報を記録する例を示します。

```
switch# config t
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 per-entry
```

関連コマンド

コマンド	説明
action	VLAN アクセス マップ内のトラフィック フィルタリング用の処理を指定します。
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。
show vlan filter	VLAN アクセス マップの適用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。

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 クラス 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**}

シンタックスの説明

access-group name *access-list*	IP ACL または MAC ACL と一致させます。
exception	例外パケットを一致させます。
ip	IPv4 例外パケットを一致させます。
ipv6	IPv6 例外パケットを一致させます。
icmp	IPv4 または IPv6 ICMP パケットを一致させます。
redirect	IPv4 または IPv6 ICMP リダイレクト パケットを一致させます。
unreachable	IPv4 または IPv6 ICMP 到達不能パケットを一致させます。
option	IPv4 または IPv6 ICMP オプション パケットを一致させます。
protocol arp	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。
redirect {**arp-inspect** | **dhcp-snoop**}	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(1)	このコマンドが導入されました。
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。

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
class-map type control-plane	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。
show class-map type control-plane	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。