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

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	変更箇所
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
```

この暗黙ルールによって、デバイスは、トラフィックのレイヤ 2 ヘッダーに指定されているプロトコルに関係なく、不一致トラフィックを確実に拒否します。

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、ライセンスは必要ありません。

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 に拒否（deny）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。
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 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	変更箇所
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、ライセンスは必要ありません。

MAC パケット分類により、レイヤ 2 インターフェイス上の MAC ACL を、IP トラフィックなどインターフェイスに入るすべてのトラフィックに適用するか、非 IP トラフィックだけに適用するかを制御できます。

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にするには、**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
ip port access-group	IPV4 ACL をポート ACL としてインターフェイスに適用します。
ipv6 port traffic-filter	IPV6 ACL をポート ACL としてインターフェイスに適用します。
switchport	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 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

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	変更箇所
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.394 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、ライセンスは必要ありません。

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（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

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	（任意）IPv4 例外パケットを一致させます。
ipv6	（任意）IPv6 例外パケットを一致させます。
icmp	IPv4 または IPv6 の ICMP パケットを一致させます。
redirect	IPv4 または IPv6 の ICMP リダイレクト パケットを一致させます。
unreachable	IPv4 または IPv6 の ICMP 到達不能パケットを一致させます。
option	IPv4 または IPv6 の ICMP オプション パケットを一致させます。
protocol arp	アドレス解決プロトコル（ARP）パケットを一致させます。
redirect	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。
arp-inspect	ダイナミック ARP インスペクションを一致させます。
dhcp-snoop	ダイナミック DHCP スヌーピングを一致させます。

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	変更箇所
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。

このコマンドは、デフォルトの VDC に限り使用できます。

このコマンドには、ライセンスは必要ありません。

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。

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	ACL が IPv4 ACL になるように指定します。
ipv6	ACL が IPv6 ACL になるように指定します。
mac	ACL が MAC ACL になるように指定します。
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。

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	変更箇所
4.1(2)	**ipv6** 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、ライセンスは必要ありません。

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
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。
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。

monitor session

インターフェイスまたは VLAN 上のトラフィックを選択的にモニタするため、アクセス コントロール リスト（ACL）キャプチャ セッションを設定するには、**monitor session** コマンドを使用します。

monitor session *session* **type acl-capture**

構文の説明

session	セッション ID。指定できる範囲は 0 ～ 48 です。
type	セッションのタイプを指定します。
acl-capture	ACL キャプチャ セッションを作成します。

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	変更箇所
5.2(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、ライセンスは必要ありません。

例

次に、ACL キャプチャ セッションを設定する例を示します。

```
switch# configure terminal
switch(config)# monitor session 5 type acl-capture
switch(config-acl-capture)#
```

コマンド	説明
hardware access-list capture	すべての仮想デバイス コンテキスト（VDC）上でアクセス コントロール リスト（ACL）のキャプチャをイネーブルにします。
destination interface	ACL キャプチャ パケットの宛先を設定します。
show ip-access capture session	ACL のキャプチャ セッションの設定を表示します。