



O コマンド

この章では、O 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。

object-group (アイデンティティ ポリシー)

アイデンティティ ポリシー用の MAC Access Control List (ACL; アクセス コントロール リスト) を指定するには、**object-group** コマンドを使用します。アイデンティティ ポリシーから ACL を削除するには、このコマンドの **no** 形式を使用します。

object-group *acl-name*

no object-group *acl-name*

構文の説明	<i>acl-name</i>	MAC ACL の名前。名前では、大文字と小文字が区別されます。
デフォルト		なし
コマンド モード		アイデンティティ ポリシー 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 VDC user	
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	mac access-list コマンドでは、アイデンティティ ポリシーに割り当てる MAC ACL を作成します。このコマンドには、ライセンスは不要です。	

■ object-group (アイデンティティ ポリシー)

例

次に、アイデンティティ ポリシー用の ACL を設定する例を示します。

```
switch# config t
switch(config)# identity policy AdminPolicy
switch(config-id-policy)# object-group
```

次に、アイデンティティ ポリシーから ACL を削除する例を示します。

```
switch# config t
switch(config)# identity policy AdminPolicy
switch(config-id-policy)# no object-group
```

関連コマンド

コマンド	説明
identity policy	アイデンティティ ポリシーを作成または指定して、アイデンティティ ポリシー コンフィギュレーション モードを開始します。
mac access-list	MAC ACL を作成して、MAC ACL コンフィギュレーション モードを開始します。
show identity policy	アイデンティティ ポリシーの情報を表示します。

object-group ip address

IPv4 アドレス オブジェクト グループを定義する、または特定の IPv4 アドレス オブジェクト グループでオブジェクト グループ コンフィギュレーション モードを開始するには、**object-group ip address** コマンドを使用します。IPv4 アドレス オブジェクト グループを削除するには、このコマンドの **no** 形式を使用します。

object-group ip address name

no object-group ip address name

構文の説明

<i>name</i>	IPv4 アドレス オブジェクト グループの名前。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

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)	このコマンドが追加されました。

使用上のガイドライン

IPv4 オブジェクト グループは、Ipv4 Access Control List (ACL; アクセス コントロール リスト) の **permit** コマンドおよび **deny** コマンドで使用できます。

IPv4 アドレス オブジェクト グループには、方向は設定されません。グループ メンバーを送信元または宛先のどちらのアドレスと一致させるか、またはオブジェクト グループをインバウンドまたはアウトバウンドのどちらのトラフィックに適用するかは、IPv4 ACL でのオブジェクト グループの使用方法によって異なります。

このコマンドには、ライセンスは不要です。

例

次に、`ipv4-addr-group-13` という IPv4 アドレス オブジェクト グループを作成し、グループ メンバーとして 2 つの特定の IPv4 アドレスと、1 つのサブネット `10.23.176.0` を設定する例を示します。

```
switch# config t
switch(config)# object-group ip address ipv4-addr-group-13
switch(config-ipaddr-ogroup)# host 10.121.57.102
switch(config-ipaddr-ogroup)# 10.121.57.234/32
```

```
switch(config-ipaddr-ogroup)# 10.23.176.0 0.0.0.255
switch(config-ipaddr-ogroup)# show object-group ipv4-addr-group-13
    10 host 10.121.57.102
    20 host 10.121.57.234
    30 10.23.176.0/24
switch(config-ipaddr-ogroup)#
```

関連コマンド

コマンド	説明
host (IPv4)	IPv4 アドレス オブジェクト グループのグループ メンバーを設定します。
show object-group	オブジェクト グループを表示します。

object-group ip port

IP ポート オブジェクト グループを定義する、または特定の IP ポート オブジェクト グループでオブジェクト グループ コンフィギュレーション モードを開始するには、**object-group ip port** コマンドを使用します。IP ポート オブジェクト グループを削除するには、このコマンドの **no** 形式を使用します。

object-group ip port name

no object-group ip port name

構文の説明

<i>name</i>	IP ポート オブジェクト グループの名前。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

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)	このコマンドが追加されました。

使用上のガイドライン

IP ポート オブジェクト グループは、IPv4 および IPv6 の Access Control List (ACL; アクセス コントロール リスト) の **permit** コマンドおよび **deny** コマンドで使用できます。

IP ポート オブジェクト グループには方向性がありません。グループ メンバーを送信元または宛先のどちらのポートと一致させるか、またはオブジェクト グループをインバウンドまたはアウトバウンドのどちらのトラフィックに適用するかは、ACL でのオブジェクト グループの使用方法によって異なります。

このコマンドには、ライセンスは不要です。

例

次に、**port-group-05** という名前の IP ポート オブジェクト グループを作成し、ポート 443 で送受信されたトラフィックと一致させるグループ メンバーを設定する例を示します。

```
switch# config t
switch(config)# object-group ip port port-group-05
switch(config-port-ogroup)# eq 443
switch(config-port-ogroup)# show object-group port-group-05
10 eq 443
switch(config-port-ogroup)#
```

関連コマンド

コマンド	説明
eq	IP ポート オブジェクト グループに equal-to (等しい) グループ メンバーを指定します。
gt	IP ポート オブジェクト グループに greater-than (より大きい) グループ メンバーを指定します。
lt	IP ポート オブジェクト グループに less-than (より小さい) グループ メンバーを指定します。
neq	IP ポート オブジェクト グループに not-equal-to (等しくない) グループ メンバーを指定します。
range	IP ポート オブジェクト グループに port-range グループ メンバーを指定します。
show object-group	オブジェクト グループを表示します。

object-group ipv6 address

IPv6 アドレス オブジェクト グループを定義する、または特定の IPv6 アドレス オブジェクト グループで IPv6 オブジェクト グループ コンフィギュレーション モードを開始するには、**object-group ipv6 address** コマンドを使用します。IPv6 アドレス オブジェクト グループを削除するには、このコマンドの **no** 形式を使用します。

object-group ipv6 address name

no object-group ipv6 address name

構文の説明

<i>name</i>	IPv6 アドレス グループ オブジェクトの名前。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

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)	このコマンドが追加されました。

使用上のガイドライン

IPv6 オブジェクト グループは、IPv6 ACL の **permit** コマンドおよび **deny** コマンドで使用できます。IPv6 アドレス オブジェクト グループには、方向は設定されません。グループ メンバーを送信元または宛先のどちらのアドレスと一致させるか、またはオブジェクト グループをインバウンドまたはアウトバウンドのどちらのトラフィックに適用するかは、IPv6 ACL でのオブジェクト グループの使用方法によって異なります。

このコマンドには、ライセンスは不要です。

例

次に、**ipv6-addr-group-A7** という IPv6 アドレス オブジェクト グループを作成し、グループ メンバーとして 2 つの特定の IPv6 アドレスと、1 つのサブネット **2001:db8:0:3ab7::** を設定する例を示します。

```
switch# config t
switch(config)# object-group ipv6 address ipv6-addr-group-A7
switch(config-ipv6addr-ogroup)# host 2001:db8:0:3ab0::1
switch(config-ipv6addr-ogroup)# 2001:db8:0:3ab0::2/128
```

■ object-group ipv6 address

```
switch(config-ipv6addr-ogroup)# 2001:db8:0:3ab7::/96
switch(config-ipv6addr-ogroup)# show object-group ipv6-addr-group-A7
    10 host 2001:db8:0:3ab0::1
    20 host 2001:db8:0:3ab0::2
    30 2001:db8:0:3ab7::/96
switch(config-ipv6addr-ogroup)#
```

関連コマンド

コマンド	説明
host (IPv6)	IPv6 アドレス オブジェクト グループのグループ メンバーを設定します。
show object-group	オブジェクト グループを表示します。