I コマンド

この章では、I 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。

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 モードを開始するには、**identity policy** コマンドを使用します。アイデンティティ ポリシーを削除するには、このコマンドの **no** 形式を使用します。

identity policy *policy-name*

no identity policy *policy-name*

シンタックスの説明

policy-name	アイデンティティ ポリシーの名前。名前は、最大 100 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
VDC user

コマンド履歴

リリース	変更内容
4.0(1)	このコマンドが導入されました。

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。

例

次に、アイデンティティ ポリシーを作成して、アイデンティティ ポリシー コンフィギュレーション モードを開始する例を示します。

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

次に、アイデンティティ ポリシーを削除する例を示します。

```
switch# config t
switch(config)# no identity policy AdminPolicy
```

関連コマンド

コマンド	説明
show identity policy	アイデンティティ ポリシーの情報を表示します。

identity profile eapoudp

Extensible Authentication Protocol over User Datagram Protocol（EAPoUDP）アイデンティティ プロファイルを作成して、アイデンティティ プロファイル コンフィギュレーション モードを開始するには、**identity profile eapoudp** コマンドを使用します。EAPoUDP アイデンティティ プロファイル設定を削除するには、このコマンドの **no** 形式を使用します。

identity profile eapoudp

no identity profile eapoudp

シンタックスの説明 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 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
VDC user

コマンド履歴

リリース	変更内容
4.0(1)	このコマンドが導入されました。

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。

例 次に、EAPoUDP アイデンティティ プロファイルを作成して、アイデンティティ プロファイル 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 t
switch(config)# identity profile eapoudp
switch(config-id-policy)#
```

次に、EAPoUDP アイデンティティ プロファイル設定を削除する例を示します。

```
switch# config t
switch(config)# no identity profile eapoudp
```

関連コマンド

コマンド	説明
show identity profile	アイデンティティ プロファイルの情報を表示します。

interface policy deny

ユーザ ロールに対してインターフェイス ポリシー コンフィギュレーション モードを開始するには、**interface policy deny** コマンドを使用します。ユーザ ロールのインターフェイス ポリシーをデフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

interface policy deny

no interface policy deny

シンタックスの説明 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 すべてのインターフェイス

コマンド モード ユーザ ロール 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 このコマンドを使用すると、ユーザ ロール インターフェイス ポリシー コンフィギュレーション モードで **permit interface** コマンドを使用して許可したインターフェイスを除き、ユーザ ロールへのすべてのインターフェイスが拒否されます。

このコマンドには、ライセンスは不要です。

例 次に、ユーザ ロールに対して、ユーザ ロール インターフェイス ポリシー 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 t
switch(config)# role name MyRole
switch(config-role)# interface policy deny
switch(config-role-interface)#
```

次に、ユーザ ロールのインターフェイス ポリシーをデフォルト設定に戻す例を示します。

```
switch# config t
switch(config)# role name MyRole
switch(config-role)# no interface policy deny
```

関連コマンド

コマンド	説明
permit interface	ロール インターフェイス ポリシーでインターフェイスを許可します。
role name	ユーザ ロールを作成または指定して、ユーザ ロール コンフィギュレーション モードを開始します。
show role	ユーザ ロールの情報を表示します。

ip access-group

IPv4 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のルータ ACL として適用するには、**ip access-group** コマンドを使用します。インターフェイスから IPv4 ACL を削除するには、このコマンドの **no** 形式を使用します。

ip access-group *access-list-name* {**in** | **out**}

no ip access-group *access-list-name* {**in** | **out**}

シンタックスの説明

access-list-name	IPv4 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。
in	（任意）ACL をインバウンド トラフィックに適用します。
out	（任意）ACL をアウトバウンド トラフィックに適用します。

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 IPv4 ACL は適用されません。

ip 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、IPv4 ACL をルータ ACL として適用できます。

- VLAN インターフェイス

（注） VLAN インターフェイスを設定する前に、VLAN インターフェイスをグローバルでイネーブルにする必要があります。詳細については、『*Cisco NX-OS Interfaces Command Reference*』の **feature interface-vlan** コマンドを参照してください。

- レイヤ 3 イーサネット インターフェイス
- レイヤ 3 イーサネット サブインターフェイス
- レイヤ 3 イーサネット ポートチャネル インターフェイスおよびサブインターフェイス
- トンネル
- ループバック インターフェイス
- 管理インターフェイス

また、**ip access-group** コマンドを使用して、次のインターフェイス タイプに対しても、IPv4 ACL をルータ ACL として適用できます。

- レイヤ 2 イーサネット 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

ただし、**ip access-group** コマンドを使用してレイヤ 2 に適用した ACL は、ポート モードをルーテッド（レイヤ 3）モードに変更しない限り、アクティブになりません。IPv4 ACL をポート ACL として適用するには、**ip port access-group** コマンドを使用します。

IPv4 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。

ルータ ACL は、アウトバウンドまたはインバウンドのどちらかのトラフィックに適用されます。ACL がインバウンド トラフィックに適用されると、インバウンド 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。

アウトバウンド アクセス リストの場合は、受信したパケットはインターフェイスにルーティングされたあとで、ACL 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、そのパケットは指定された宛先に送信されます。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、ip-acl-01 という IPv4 ACL を適用する例を示します。

```
switch# config t
switch(config)# interface ethernet 2/1
switch(config-if)# ip access-group ip-acl-01 in
```

次に、イーサネット インターフェイス 2/1 から、ip-acl-01 という IPv4 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 ip access-group ip-acl-01 in
```

関連コマンド

コマンド	説明
ip access-list	IPv4 ACL を設定します。
ip port access-group	IPv4 ACL をポート ACL として適用します。
show access-lists	すべての ACL を表示します。
show ip access-lists	特定の IPv4 ACL またはすべての IPv4 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。

ip access-list

IPv4 Access Control List（ACL; アクセス コントロール リスト）を作成して、特定の ACL の IP 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、**ip access-list** コマンドを使用します。IPv4 ACL を削除するには、このコマンドの **no** 形式を使用します。

ip access-list *access-list-name*

no ip access-list *access-list-name*

シンタックスの説明

access-list-name	IPv4 ACL の名前。名前は最大 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、IPv4 ACL は定義されません。

IPv4 トラフィックをフィルタリングするには、IPv4 ACL を使用します。

ip access-list コマンドを使用すると、IP 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、IPv4 **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 をルータ ACL としてインターフェイスに適用するには、**ip access-group** コマンドを使用します。ACL をポート ACL としてインターフェイスに適用するには、**ip port access-group** コマンドを使用します。

すべての IPv4 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 ip any any
```

この暗黙ルールにより、一致しなかった IP トラフィックはすべて拒否されます。

IPv4 ACL には、近隣探索プロセスをイネーブルにする暗黙ルールは追加されません。Address Resolution Protocol（ARP; アドレス解決プロトコル）は、別のデータ リンク レイヤ プロトコルを使用します。デフォルトでは、IPv4 ACL は、インターフェイス上での ARP パケットの送受信を暗黙で許可します。

IPv4 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。暗黙の **deny ip any any** ルールに一致したパケットの統計情報を記録するには、まったく同じ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、ip-acl-01 という IPv4 ACL の IP 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)# ip access-list ip-acl-01
switch(config-acl)#
```

関連コマンド

コマンド	説明
access-class	IPv4 ACL を VTY 回線に適用します。
deny（IPv4）	IPv4 ACL に拒否（deny）ルールを設定します。
ip access-group	IPV4 ACL をルータ ACL としてインターフェイスに適用します。
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。
permit（IPv4）	IPv4 ACL に許可（permit）ルールを設定します。
show ip access-lists	すべての IPv4 ACL または特定の IPv4 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。

ip arp inspection filter

ARP Access Control List（ACL; アクセス コントロール リスト）を VLAN リストに適用するには、**ip arp inspection filter** コマンドを使用します。VLAN リストから ARP ACL を削除するには、このコマンドの **no** 形式を使用します。

ip arp inspection filter *acl-name* **vlan** *vlan-list*

no ip arp inspection filter *acl-name* **vlan** *vlan-list*

シンタックスの説明

acl-name	ARP 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。
vlan *vlan-list*	ARP ACL でフィルタリングする VLAN を指定します。*vlan-list* 引数には、単一 VLAN ID、VLAN ID 範囲、またはカンマで区切った ID と範囲を指定できます（例のセクションを参照）。有効な VLAN ID は、1 ～ 4096 です。

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)	このコマンドが導入されました。

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。

例

次に、VLAN 15 および 37 ～ 48 に対して、arp-acl-01 という ARP ACL を適用する例を示します。

```
switch# configure terminal
switch(config)# ip arp inspection filter arp-acl-01 vlan 15,37-48
switch(config)#
```

関連コマンド

コマンド	説明
arp access-list	ARP ACL を設定します。
ip arp inspection vlan	指定した VLAN リストの Dynamic ARP Inspection（DAI）をイネーブルにします。
show ip arp inspection	DAI 設定ステータスを表示します。
show running-config dhcp	DAI 設定を含む、DHCP スヌーピング設定を表示します。

ip arp inspection log-buffer

Dynamic ARP Inspection（DAI）ロギング バッファのサイズを設定するには、**ip arp inspection log-buffer** コマンドを使用します。DAI ロギング バッファをデフォルトのサイズに戻すには、このコマンドの **no** 形式を使用します。

ip arp inspection log-buffer entries *number*

no ip arp inspection log-buffer entries *number*

シンタックスの説明

entries *number*	0 ～ 1024 メッセージの範囲で、バッファ サイズを指定します。

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)	このコマンドが導入されました。

使用上のガイドライン

DAI ロギング バッファのデフォルトのサイズは、32 メッセージです。

このコマンドには、ライセンスは不要です。

例

次に、DAI ロギング バッファのサイズを設定する例を示します。

```
switch# configure terminal
switch(config)# ip arp inspection log-buffer entries 64
switch(config)#
```

関連コマンド

コマンド	説明
clear ip arp inspection log	DAI ロギング バッファをクリアします。
show ip arp inspection	DAI の設定ステータスを表示します。
show running-config dhcp	DAI 設定を含む、DHCP スヌーピング設定を表示します。

ip arp inspection trust

レイヤ 2 インターフェイスを信頼できる ARP インターフェイスとして設定するには、**ip arp inspection trust** コマンドを使用します。レイヤ 2 インターフェイスを信頼できない ARP インターフェイスとして設定するには、このコマンドの **no** 形式を使用します。

ip arp inspection trust

no ip arp inspection trust

シンタックスの説明

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

デフォルトでは、すべてのインターフェイスが信頼できない ARP インターフェイスです。

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

信頼できる ARP インターフェイスとして設定できるのは、レイヤ 2 イーサネット インターフェイスだけです。

このコマンドには、ライセンスは不要です。

例

次に、レイヤ 2 インターフェイスを信頼できる ARP インターフェイスとして設定する例を示します。

```
switch# configure terminal
switch(config)# interface ethernet 2/1
switch(config-if)# ip arp inspection trust
switch(config-if)#
```

関連コマンド

コマンド	説明
show ip arp inspection	Dynamic ARP Inspection（DAI）の設定ステータスを表示します。
show ip arp inspection interface	特定のインターフェイスの信頼状態および ARP パケット レートを表示します。
show running-config dhcp	DAI 設定を含む、DHCP スヌーピング設定を表示します。

ip arp inspection validate

追加の Dynamic ARP Inspection（DAI）検証をイネーブルにするには、**ip arp inspection validate** コマンドを使用します。追加の DAI 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。

ip arp inspection validate {**dst-mac** [**ip**] [**src-mac**]}

ip arp inspection validate {[**dst-mac**] **ip** [**src-mac**]}

ip arp inspection validate {[**dst-mac**] [**ip**] **src-mac**}

no ip arp inspection validate {**dst-mac** [**ip**] [**src-mac**]}

no ip arp inspection validate {[**dst-mac**] **ip** [**src-mac**]}

no ip arp inspection validate {[**dst-mac**] [**ip**] **src-mac**}

シンタックスの説明

dst-mac	（任意）イーサネット ヘッダーの宛先 MAC アドレスを、ARP 応答の ARP 本文にあるターゲット MAC アドレスと照合します。MAC アドレスが一致していないパケットは無効として分類され、ドロップされます。
ip	（任意）ARP 本文が有効で、予期された IP アドレスかどうかを検証します。アドレスには、0.0.0.0、255.255.255.255、およびすべての IP マルチキャスト アドレスが含まれます。送信側 IP アドレスは、すべての ARP 要求および ARP 応答でチェックされます。ターゲット IP アドレスは ARP 応答でのみチェックされます。
src-mac	（任意）イーサネット ヘッダーの送信元 MAC アドレスを、ARP 要求および応答の ARP 本文にある送信側 MAC アドレスと照合します。MAC アドレスが一致していないパケットは無効として分類され、ドロップされます。

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)	このコマンドが導入されました。

使用上のガイドライン

最小限、1 つのキーワードを指定する必要があります。複数のキーワードを指定する場合、順序は影響しません。

このコマンドには、ライセンスは不要です。

例

次に、追加の DAI 検証をイネーブルにする例を示します。

```
switch# configure terminal
switch(config)# ip arp inspection validate src-mac dst-mac ip
switch(config)#
```

関連コマンド

コマンド	説明
show ip arp inspection	DAI の設定ステータスを表示します。
show running-config dhcp	DAI 設定を含む、DHCP スヌーピング設定を表示します。

ip arp inspection vlan

VLAN リストに対して Dynamic ARP Inspection（DAI）をイネーブルにするには、**ip arp inspection vlan** コマンドを使用します。VLAN リストの DAI 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。

ip arp inspection vlan *vlan-list* [**logging dhcp-bindings** {**permit | all | none**}]

no ip arp inspection vlan *vlan-list* [**logging dhcp-bindings** {**permit | all | none**}]

シンタックスの説明

vlan-list	DAI をアクティブにする VLAN。*vlan-list* 引数には、単一 VLAN ID、VLAN ID 範囲、またはカンマで区切った ID と範囲を指定できます（例のセクションを参照）。有効な VLAN ID は、1 ～ 4096 です。
logging	（任意）指定した VLAN の DAI ロギングをイネーブルにします。 − **all —** DHCP バインディングと一致するすべてのパケットをロギングします。 − **none —** DHCP バインディング パケットをロギングしません（このオプションは、ロギングをディセーブルにする場合に使用します）。 − **permit —** DHCP バインディングで許可されたパケットをロギングします。
dhcp-bindings	DHCP バインディングの一致に基づくロギングをイネーブルにします。
permit	DHCP バインディング一致による許可パケットのロギングをイネーブルにします。
all	すべてのパケットのロギングをイネーブルにします。
none	ロギングをディセーブルにします。

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)	このコマンドが導入されました。

使用上のガイドライン

デフォルトでは、DAI によって検査されたパケットはロギングされません。

このコマンドには、ライセンスは不要です。

例

次に、VLAN 13、15、および 17 ～ 23 で DAI をイネーブルにする例を示します。

```
switch# configure terminal
switch(config)# ip arp inspection vlan 13,15,17-23
switch(config)#
```

関連コマンド

コマンド	説明
ip arp inspection validate	追加の DAI 検証をイネーブルにします。
show ip arp inspection	DAI の設定ステータスを表示します。
show ip arp inspection vlan	特定の VLAN リストの DAI ステータスを表示します。
show running-config dhcp	DAI 設定を含む、DHCP スヌーピング設定を表示します。

ip dhcp relay address

インターフェイス上に DHCP サーバの IP アドレスを設定するには、**ip dhcp relay address** コマンドを使用します。DHCP サーバの IP アドレスを削除するには、このコマンドの **no** 形式を使用します。

ip dhcp relay address *IP-address*

no ip dhcp relay address *IP-address*

シンタックスの説明

IP-address	DHCP サーバの IPv4 アドレス

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。
4.0(3)	レイヤ 3 イーサネット インターフェイスまたはサブインターフェイスの設定に、最大 4 つの **ip dhcp relay address** コマンドを追加できるようになりました。

使用上のガイドライン

このコマンドを使用するには、DHCP スヌーピング機能をイネーブルにする必要があります（**feature dhcp** コマンドを参照）。

レイヤ 3 イーサネット インターフェイスおよびサブインターフェイス、VLAN インターフェイス、およびレイヤ 3 ポート チャネルに、それぞれ最大 4 つの DHCP サーバ IP アドレスを設定できます。Cisco NX-OS Release 4.0.2 以前のリリースでは、1 つのインターフェイスに設定できる DHCP サーバ IP アドレスは 1 つだけです。

インターフェイス上にインバウンド DHCP BOOTREQUEST パケットが到達すると、リレー エージェントによって、そのインターフェイスに設定されているすべての DHCP サーバ IP アドレスに、パケットが転送されます。また、リレー エージェントにより、すべての DHCP サーバからの応答が、要求を送信したホストに戻されます。

このコマンドには、ライセンスは不要です。

例

次に、特定のレイヤ 3 イーサネット インターフェイス上で受信した BOOTREQUEST がリレー エージェントによって転送されるように、インターフェイスに 2 つの DHCP サーバ IP アドレスを設定する例を示します。

```
switch# configure terminal
switch(config)# interface ethernet 2/1
switch(config-if)# ip dhcp relay address 10.132.7.120
switch(config-if)# ip dhcp relay address 10.132.7.175
switch(config-if)#
```

次に、VLAN インターフェイス上に DHCP サーバの IP アドレスを設定する例を示します。

```
switch# configure terminal
switch(config)# interface vlan 13
switch(config-if)# ip dhcp relay address 10.132.7.120
switch(config-if)#
```

次に、レイヤ 3 ポートチャネル インターフェイス上に DHCP サーバの IP アドレスを設定する例を示します。

```
switch# configure terminal
switch(config)# interface port-channel 7
switch(config-if)# ip dhcp relay address 10.132.7.120
switch(config-if)#
```

関連コマンド

コマンド	説明
ip dhcp relay information option	DHCP パケットの option-82 情報の挿入および削除をイネーブルにします。
ip dhcp snooping	デバイス上で DHCP スヌーピングをグローバルにイネーブルにします。
service dhcp	DHCP リレー エージェントをイネーブルまたはディセーブルにします。
show ip dhcp snooping	DHCP スヌーピングの全般情報を表示します。
show running-config dhcp	IP ソース ガード設定を含む、DHCP スヌーピング設定を表示します。

ip dhcp relay information option

リレー エージェントによって転送された DHCP パケットでの option-82 情報の挿入および削除をイネーブルにするには、**ip dhcp relay information option** コマンドを使用します。option-82 情報の挿入および削除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。

ip dhcp relay information option

no ip dhcp relay information option

シンタックスの説明

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

デフォルトでは、リレー エージェントによって転送された DHCP パケットでの option-82 情報の挿入および削除は実行されません。

コマンド モード

グローバル コンフィギュレーション

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

このコマンドを使用するには、DHCP スヌーピング機能をイネーブルにする必要があります（**feature dhcp** コマンドを参照）。

このコマンドには、ライセンスは不要です。

例

次に、DHCP リレー エージェントによって転送されるパケットでの option-82 情報の挿入および削除をイネーブルにする例を示します。

```
switch# configure terminal
switch(config)# ip dhcp relay information option
switch(config)#
```

関連コマンド

コマンド	説明
ip dhcp relay address	インターフェイス上に DHCP サーバの IP アドレスを設定します。
ip dhcp snooping	デバイス上で DHCP スヌーピングをグローバルにイネーブルにします。
ip dhcp snooping information option	DHCP リレー エージェントを使用しないで転送された DHCP パケットでの option-82 情報の挿入および削除をイネーブルにします。
service dhcp	DHCP リレー エージェントをイネーブルまたはディセーブルにします。
show running-config dhcp	IP ソース ガード設定を含む、DHCP スヌーピング設定を表示します。

ip dhcp snooping

デバイス上で DHCP スヌーピングをグローバルでイネーブルにするには、**ip dhcp snooping** コマンドを使用します。DHCP スヌーピングをグローバルで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。

ip dhcp snooping

no ip dhcp snooping

シンタックスの説明

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

デフォルトでは、DHCP スヌーピングはグローバルでディセーブルです。

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

このコマンドを使用するには、DHCP スヌーピング機能をイネーブルにする必要があります（**feature dhcp** コマンドを参照）。

no ip dhcp snooping コマンドを使用して DHCP スヌーピングをディセーブルにすると、デバイスの DHCP スヌーピング設定が保持されます。

このコマンドには、ライセンスは不要です。

例

次に、DHCP スヌーピングをグローバルでイネーブルにする例を示します。

```
switch# configure terminal
switch(config)# ip dhcp snooping
switch(config)#
```

関連コマンド

コマンド	説明
feature dhcp	デバイス上で DHCP スヌーピング機能をイネーブルにします。
ip dhcp snooping information option	DHCP リレー エージェントを使用しないで転送された DHCP パケットでの option-82 情報の挿入および削除をイネーブルにします。
ip dhcp snooping trust	インターフェイスを、DHCP メッセージの信頼できる送信元として設定します。
ip dhcp snooping vlan	特定の VLAN 上で DHCP スヌーピングをイネーブルにします。
service dhcp	DHCP リレー エージェントをイネーブルまたはディセーブルにします。
show ip dhcp snooping	DHCP スヌーピングの全般情報を表示します。
show running-config dhcp	IP ソース ガード設定を含む、DHCP スヌーピング設定を表示します。

ip dhcp snooping information option

DHCP パケットの option-82 情報の挿入および削除をイネーブルにするには、**ip dhcp snooping information option** コマンドを使用します。option-82 情報の挿入および削除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。

ip dhcp snooping information option

no ip dhcp snooping information option

シンタックスの説明 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 デフォルトでは、option-82 情報の挿入および削除は実行されません。

コマンド モード グローバル コンフィギュレーション

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 このコマンドを使用するには、DHCP スヌーピング機能をイネーブルにする必要があります（**feature dhcp** コマンドを参照）。

このコマンドには、ライセンスは不要です。

例 次に、DHCP パケットの opiton-82 情報の挿入および削除をイネーブルにする例を示します。

```
switch# configure terminal
switch(config)# ip dhcp snooping information option
switch(config)#
```

関連コマンド

コマンド	説明
ip dhcp relay information option	DHCP パケットの option-82 情報の挿入および削除をイネーブルにします。
ip dhcp snooping	デバイス上で DHCP スヌーピングをグローバルにイネーブルにします。
ip dhcp snooping trust	インターフェイスを、DHCP メッセージの信頼できる送信元として設定します。
ip dhcp snooping vlan	特定の VLAN 上で DHCP スヌーピングをイネーブルにします。
show ip dhcp snooping	DHCP スヌーピングの全般情報を表示します。
show running-config dhcp	IP ソース ガード設定を含む、DHCP スヌーピング設定を表示します。

ip dhcp snooping trust

インターフェイスを DHCP メッセージの信頼できる送信元として設定するには、**ip dhcp snooping trust** コマンドを使用します。インターフェイスを DHCP メッセージの信頼できない送信元として設定するには、このコマンドの **no** 形式を使用します。

ip dhcp snooping trust

no ip dhcp snooping trust

シンタックスの説明

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

デフォルトでは、DHCP メッセージの信頼できる送信元として設定されるインターフェイスはありません。

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

このコマンドを使用するには、DHCP スヌーピング機能をイネーブルにする必要があります（**feature dhcp** コマンドを参照）。

DHCP メッセージの信頼できる送信元として設定できるのは、次のタイプのインターフェイスです。

- レイヤ 3 イーサネット インターフェイスおよびサブインターフェイス
- レイヤ 2 イーサネット インターフェイス
- プライベート VLAN インターフェイス

このコマンドには、ライセンスは不要です。

例

次に、インターフェイスを DHCP メッセージの信頼できる送信元として設定する例を示します。

```
switch# configure terminal
switch(config)# interface ethernet 2/1
switch(config-if)# ip dhcp snooping trust
switch(config-if)#
```

関連コマンド

コマンド	説明
ip dhcp snooping	デバイス上で DHCP スヌーピングをグローバルにイネーブルにします。
ip dhcp snooping information option	DHCP リレー エージェントを使用しないで転送された DHCP パケットでの option-82 情報の挿入および削除をイネーブルにします。
ip dhcp snooping verify mac-address	MAC アドレス検証を、DHCP スヌーピングの一部としてイネーブルにします。
ip dhcp snooping vlan	特定の VLAN 上で DHCP スヌーピングをイネーブルにします。
show ip dhcp snooping	DHCP スヌーピングの全般情報を表示します。
show running-config dhcp	IP ソース ガード設定を含む、DHCP スヌーピング設定を表示します。

ip dhcp snooping verify mac-address

DHCP スヌーピングの MAC アドレス検証をイネーブルにするには、**ip dhcp snooping verify mac-address** コマンドを使用します。DHCP スヌーピングの MAC アドレス検証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。

ip dhcp snooping verify mac-address

no ip dhcp snooping verify mac-address

シンタックスの説明

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

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、DHCP スヌーピングでの MAC アドレス検証はディセーブルです。

このコマンドを使用するには、DHCP スヌーピング機能をイネーブルにする必要があります（**feature dhcp** コマンドを参照）。

信頼できないインターフェイス上でパケットを受信し、パケットの送信元 MAC アドレスと DHCP クライアント ハードウェア アドレスが一致しない場合、そのパケットはアドレス検証によってドロップされます。

このコマンドには、ライセンスは不要です。

例

次に、DHCP スヌーピングの MAC アドレス検証をイネーブルにする例を示します。

```
switch# configure terminal
switch(config)# ip dhcp snooping verify mac-address
switch(config)#
```

関連コマンド

コマンド	説明
ip dhcp snooping	デバイス上で DHCP スヌーピングをグローバルにイネーブルにします。
ip dhcp snooping information option	DHCP リレー エージェントを使用しないで転送された DHCP パケットでの option-82 情報の挿入および削除をイネーブルにします。
ip dhcp snooping trust	インターフェイスを、DHCP メッセージの信頼できる送信元として設定します。
ip dhcp snooping vlan	特定の VLAN 上で DHCP スヌーピングをイネーブルにします。
service dhcp	DHCP リレー エージェントをイネーブルまたはディセーブルにします。
show ip dhcp snooping	DHCP スヌーピングの全般情報を表示します。
show running-config dhcp	IP ソース ガード設定を含む、DHCP スヌーピング設定を表示します。

ip dhcp snooping vlan

1 つまたは複数の VLAN 上で DHCP スヌーピングをイネーブルにするには、**ip dhcp snooping vlan** コマンドを使用します。1 つまたは複数の VLAN 上で DHCP スヌーピング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。

ip dhcp snooping vlan *vlan-list*

no ip dhcp snooping vlan *vlan-list*

シンタックスの説明

vlan-list	DHCP スヌーピングをイネーブルにする VLAN 範囲。*vlan-list* 引数には、単一 VLAN ID、VLAN ID 範囲、またはカンマで区切った ID と範囲を指定できます（例のセクションを参照）。有効な VLAN ID は、1 ～ 4096 です。

デフォルト

デフォルトでは、すべての VLAN 上で DHCP スヌーピングはディセーブルです。

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

このコマンドを使用するには、DHCP スヌーピング機能をイネーブルにする必要があります（**feature dhcp** コマンドを参照）。

このコマンドには、ライセンスは不要です。

例

次に、VLAN 100、200、および 250 ～ 252 で DHCP スヌーピングをイネーブルにする例を示します。

```
switch# configure terminal
switch(config)# ip dhcp snooping vlan 100,200,250-252
switch(config)#
```

関連コマンド

コマンド	説明
ip dhcp snooping	デバイス上で DHCP スヌーピングをグローバルにイネーブルにします。
ip dhcp snooping information option	DHCP リレー エージェントを使用しないで転送された DHCP パケットでの option-82 情報の挿入および削除をイネーブルにします。
ip dhcp snooping trust	インターフェイスを、DHCP メッセージの信頼できる送信元として設定します。
ip dhcp snooping verify mac-address	MAC アドレス検証を、DHCP スヌーピングの一部としてイネーブルにします。
show ip dhcp snooping	DHCP スヌーピングの全般情報を表示します。
show running-config dhcp	IP ソース ガード設定を含む、DHCP スヌーピング設定を表示します。

ip port access-group

IPv4 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のポート ACL として適用するには、**ip port access-group** コマンドを使用します。インターフェイスから IPv4 ACL を削除するには、このコマンドの **no** 形式を使用します。

ip port access-group *access-list-name* **in**

no ip port access-group *access-list-name* **in**

シンタックスの説明

access-list-name	IPv4 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。
in	ACL をインバウンド トラフィックに適用します。

デフォルト

in

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 IPv4 ACL は適用されません。

ip 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、IPv4 ACL をポート ACL として適用できます。

- レイヤ 2 イーサネット 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

また、**ip port access-group** コマンドを使用して、次のインターフェイス タイプにも、IPv4 ACL をポート ACL として適用できます。

- VLAN インターフェイス

（注） VLAN インターフェイスを設定する前に、VLAN インターフェイスをグローバルでイネーブルにする必要があります。詳細については、『*Cisco NX-OS Interfaces Command Reference*』の **feature interface-vlan** コマンドを参照してください。

- レイヤ 3 イーサネット インターフェイス
- レイヤ 3 イーサネット サブインターフェイス
- レイヤ 3 イーサネット ポートチャネル インターフェイスおよびサブインターフェイス
- トンネル
- ループバック インターフェイス
- 管理インターフェイス

ただし、**ip port access-group** コマンドを使用してレイヤ 3 インターフェイスに適用した ACL は、ポート モードをアクセスまたはトランク（レイヤ 2）モードに変更しない限り、アクティブになりません。IPv4 ACL をルータ ACL として適用するには、**ip access-group** コマンドを使用します。

IPv4 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。

ポート 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。インバウンド パケットは、デバイス上で 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、ip-acl-01 という IPv4 ACL をポート ACL として適用する例を示します。

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

次に、イーサネット インターフェイス 2/1 から、ip-acl-01 という IPv4 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 ip port access-group ip-acl-01 in
```

関連コマンド

コマンド	説明
ip access-group	IPV4 ACL をルータ ACL としてインターフェイスに適用します。
ip access-list	IPv4 ACL を設定します。
show access-lists	すべての ACL を表示します。
show ip access-lists	特定の IPv4 ACL またはすべての IPv4 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。
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。

ip source binding

レイヤ 2 イーサネット インターフェイス用の固定 IP ソース エントリを作成するには、**ip source binding** コマンドを使用します。固定 IP ソース エントリ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。

ip source binding *IP-address MAC-address* **vlan** *vlan-id* **interface ethernet** *slot*/*port*

no ip source binding *IP-address MAC-address* **vlan** *vlan-id* **interface ethernet** *slot*/*port*

シンタックスの説明

IP-address	特定のインターフェイス上で使用する IPv4 アドレス。有効なエントリは、ドット付き 10 進表記です。
MAC-address	特定のインターフェイス上で使用する MAC アドレス。有効なエントリは、ドット付き 16 進表記です。
vlan *vlan-id*	IP ソース エントリに関連付ける VLAN を指定します。
interface ethernet *slot*/*port*	固定 IP エントリに関連付けるレイヤ 2 イーサネット インターフェイスを指定します。

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)	このコマンドが導入されました。

使用上のガイドライン

デフォルトでは、固定 IP ソース エントリは作成されません。

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 2/3 上に、VLAN 100 に関連付ける固定 IP ソース エントリを作成する例を示します。

```
switch# configure terminal
switch(config)# ip source binding 10.5.22.7 001f.28bd.0013 vlan 100 interface ethernet
2/3
switch(config)#
```

関連コマンド

コマンド	説明
ip verify source dhcp-snooping-vlan	インターフェイス上で IP ソース ガードをイネーブルにします。
show ip verify source	IP と MAC アドレスのバインディングを表示します。
show running-config dhcp	IP ソース ガード設定を含む、DHCP スヌーピング設定を表示します。

ip verify source dhcp-snooping-vlan

レイヤ 2 イーサネット インターフェイス上で IP ソース ガードをイネーブルにするには、**ip verify source dhcp-snooping-vlan** コマンドを使用します。インターフェイス上で IP ソース ガード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。

ip verify source dhcp-snooping-vlan

no ip verify source dhcp-snooping-vlan

シンタックスの説明 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
4.0(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、すべてのインターフェイス上で IP ソース ガードはディセーブルです。

このコマンドには、ライセンスは不要です。

例 次に、インターフェイス上で IP ソース ガードをイネーブルにする例を示します。

```
switch# configure terminal
switch(config)# interface ethernet 2/1
switch(config-if)# ip verify source dhcp-snooping-vlan
switch(config-if)#
```

関連コマンド

コマンド	説明
ip source binding	特定のイーサネット インターフェイス用の固定 IP ソース エントリを作成します。
show ip verify source	IP と MAC アドレスのバインディングを表示します。

ip verify unicast source reachable-via

インターフェイス上で Unicast Reverse Path Forwarding（ユニキャスト RPF）を設定するには、**ip verify unicast source reachable-via** コマンドを使用します。インターフェイスからユニキャスト RPF を削除するには、このコマンドの **no** 形式を使用します。

ip verify unicast source reachable-via {**any** [**allow-default**] | **rx**}

no ip verify unicast source reachable-via {**any** [**allow-default**] | **rx**}

シンタックスの説明

any	ルーズ チェックを指定します。
allow-default	（任意）特定のインターフェイス上で使用する MAC アドレスを指定します。
rx	ストリクト チェックを指定します。

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

入力側インターフェイスで、次のユニキャスト RPF モードの 1 つを設定できます。

ストリクト ユニキャスト RPF モード **—** ストリクト モード チェックは、次の一致が検出された場合に成功します。

- ユニキャスト RPF が、Forwarding Information Base（FIB; 転送情報ベース）でパケット送信元アドレスの一致を検出。
- パケットを受信した入力側インターフェイスが、FIB 一致のユニキャスト PRF インターフェイスの 1 つと一致。

これらのチェックに失敗すると、パケットは廃棄されます。このタイプのユニキャスト RPF チェックは、パケット フローが対称であると想定される場所で使用できます。

ルーズ ユニキャスト RPF モード **—** ルーズ モード チェックは、FIB でのパケット送信元アドレスの検索が一致し、最低 1 つの実インターフェイスを経由して送信元に到達可能であるという FIB 結果が示された場合に成功します。パケットを受信した入力側インターフェイスが、FIB 結果のいずれかのインターフェイスと一致する必要はありません。

このコマンドには、ライセンスは不要です。

例

次に、インターフェイス上にルーズ ユニキャスト RPF チェックを設定する例を示します。

```
switch# configure terminal
switch(config)# interface ethernet 2/3
switch(config-if)# ip verify unicast source reachable-via any
```

次に、インターフェイス上にストリクト ユニキャスト RPF チェックを設定する例を示します。

```
switch# configure terminal
switch(config)# interface ethernet 2/3
switch(config-if)# ip verify unicast source reachable-via rx
```

関連コマンド

コマンド	説明
show ip interface ethernet	インターフェイスの IP 関連情報を表示します。
show running-config interface ethernet	実行コンフィギュレーションのインターフェイス設定を表示します。
show running-config ip	実行コンフィギュレーションの IP 設定を表示します。
show startup-config interface ethernet	スタートアップ コンフィギュレーションのインターフェイス設定を表示します。
show startup-config ip	スタートアップ コンフィギュレーションの IP 設定を表示します。