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。

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

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。

コマンド 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 モード

コマンド履歴

リリース	変更内容
4.0(0)N1(1a)	このコマンドが追加されました。

例

次に、ユーザ ロールのインターフェイス 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)# 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)# role name MyRole
switch(config-role)# no interface policy deny
```

関連コマンド

コマンド	説明
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-class

仮想端末回線（VTY）の着信または発信トラフィックを制限するために IPv4 アクセス クラスを作成または設定するには、**ip access-class** コマンドを使用します。アクセス クラスを削除するには、このコマンドの **no** 形式を使用します。

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

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

構文の説明

access-list-name	IPv4 ACL クラスの名前。名前は、最大 64 文字まで指定できます。名前には、文字、数字、ハイフン、および下線を使用できます。名前にはスペースまたは引用符を含めることはできません。
in	着信接続が特定の Cisco Nexus 5000 シリーズ スイッチとアクセス リストのアドレス間で制限されていることを指定します。
out	発信接続が特定の Cisco Nexus 5000 シリーズ スイッチとアクセス リストのアドレス間で制限されていることを指定します。

コマンド デフォルト

なし

コマンド モード

ライン コンフィギュレーション モード

コマンド履歴

リリース	変更内容
5.0(2)N1(1)	このコマンドが追加されました。

例

次の例では、着信パケットを制限するために VTY 回線の IP アクセス クラスを設定する例を示します。

```
switch# configure terminal
switch(config)# line vty
switch(config-line)# ip access-class VTY_ACCESS in
switch(config-line)#
```

次の例では、着信パケットを制限する IP アクセス クラスを削除する例を示します。

```
switch(config)# line vty
switch(config-line)# no ip access-class VTY_ACCESS in
switch(config-line)#
```

関連コマンド

コマンド	説明
access-class	VTY のアクセス クラスを設定します。
copy running-config startup-config	実行コンフィギュレーションをスタートアップ コンフィギュレーション ファイルにコピーします。
show line	特定の端末ラインのアクセス リストを表示します。

コマンド	説明
show running-config aclmgr	ACL の実行コンフィギュレーションを表示します。
show startup-config aclmgr	ACL のスタートアップ コンフィギュレーションを表示します。
ssh	IPv4 を使用して SSH セッションを開始します。
telnet	IPv4 を使用して Telnet セッションを開始します。

ip access-group

ルータの ACL としてレイヤ 3 インターフェイスに IPv4 アクセス コントロール リスト（ACL）を適用するには、**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**}

構文の説明

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 を着信トラフィックに適用するように指定します。
out	ACL を発信トラフィックに適用するように指定します。

コマンド 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 モード
サブインターフェイス コンフィギュレーション モード

コマンド履歴

リリース	変更内容
5.0(3)N1(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、IPv4 ACL はレイヤ 3 ルーテッド インターフェイスには適用されません。

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
- 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
- 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。

- 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。

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、レイヤ 3 イーサネット インターフェイス 1/2 に対して、ip-acl-01 という IPv4 ACL を適用する例を示します。

```
switch# configure terminal
switch(config)# interface ethernet 2/1
switch(config-if)# no switchport
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# configure terminal
switch(config)# interface ethernet 2/1
switch(config-if)# no switchport
switch(config-if)# ip access-group ip-acl-01 in
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。
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。

ipv6 access-class

仮想端末回線（VTY）の着信または発信トラフィックを制限するために IPv6 アクセス クラスを作成または設定するには、**ipv6 access-class** コマンドを使用します。アクセス クラスを削除するには、このコマンドの **no** 形式を使用します。

ipv6 access-class *access-list-name* {**in** | **out**}

no ipv6 access-class *access-list-name* {**in** | **out**}

構文の説明

access-list-name	IPv6 ACL クラスの名前。名前は、最大 64 文字まで指定できます。名前には、文字、数字、ハイフン、および下線を使用できます。名前にはスペースまたは引用符を含めることはできません。
in	着信接続が特定の Cisco Nexus 5000 シリーズ スイッチとアクセス リストのアドレス間で制限されていることを指定します。
out	発信接続が特定の Cisco Nexus 5000 シリーズ スイッチとアクセス リストのアドレス間で制限されていることを指定します。

コマンド デフォルト

なし

コマンド モード

ライン コンフィギュレーション モード

コマンド履歴

リリース	変更内容
5.0(2)N1(1)	このコマンドが追加されました。

例

次に、着信パケットを制限するために VTY 回線の IPv6 アクセス クラスを設定する例を示します。

```
switch# configure terminal
switch(config)# line vty
switch(config-line)# ipv6 access-class VTY_I6ACCESS in
switch(config-line)#
```

次に、着信パケットの数を制限する IPv6 アクセス クラスを削除する例を示します。

```
switch(config)# line vty
switch(config-line)# no ipv6 access-class VTY_I6ACCESS in
switch(config-line)#
```

関連コマンド

コマンド	説明
access-class	VTY のアクセス クラスを設定します。
copy running-config startup-config	実行コンフィギュレーションをスタートアップ コンフィギュレーション ファイルにコピーします。
show ipv6 access-class	IPv6 アクセス クラスを表示します。

コマンド	説明
show line	特定の端末ラインのアクセス リストを表示します。
show running-config aclmgr	ACL の実行コンフィギュレーションを表示します。
show startup-config aclmgr	ACL のスタートアップ コンフィギュレーションを表示します。
ssh6	IPv6 を使用して SSH セッションを開始します。
telnet6	IPv6 を使用して Telnet セッションを開始します。

ip access-list

IPv4 アクセス コントロール リスト（ACL）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*

構文の説明

access-list-name	IPv4 ACL の名前で、最大 64 の英数字です。名前にはスペースまたは引用符を含めることはできません。

コマンド デフォルト

デフォルトでは、IPv4 ACL は定義されません。

コマンド モード

グローバル コンフィギュレーション モード

コマンド履歴

リリース	変更内容
4.0(0)N1(1a)	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 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、スイッチで 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** 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、このコマンドの入力時にスイッチで新しい 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、**ip 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
```

この暗黙のルールによって、どの条件にも一致しない IP トラフィックは拒否されます。

IPv4 ACL には、ネイバー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。IPv4 では、IPv6 ネイバー探索プロセスと同等の Address Resolution Protocol（ARP; アドレス解決プロトコル）は、別のデータリンク層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。

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(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。

ip arp event-history errors

イベント履歴バッファにアドレス解決プロトコル（ARP）のデバッグ イベントをログに記録するには、**ip arp event-history errors** コマンドを使用します。

ip arp event-history errors size {**disabled** | **large** | **medium** | **small**}

no ip arp event-history errors size {**disabled** | **large** | **medium** | **small**}

構文の説明

size	イベント履歴バッファ サイズを設定するように指定します。
disabled	イベント履歴バッファ サイズをディセーブルに指定します。
large	イベント履歴バッファ サイズが大であることを指定します。
medium	イベント履歴バッファ サイズが中であることを指定します。
small	イベント履歴バッファ サイズが小であることを指定します。これがデフォルトのバッファ サイズです。

コマンド デフォルト

デフォルトでは、イベント履歴バッファは小になります。

コマンド モード

グローバル コンフィギュレーション モード

コマンド履歴

リリース	変更内容
5.0(2)N1(1)	このコマンドが追加されました。

例

次に、サイズが「中」の ARP イベント履歴バッファを設定する例を示します。

```
switch(config)# ip arp event-history errors size medium
switch(config)#
```

次に、ARP イベント履歴バッファをデフォルトに設定する例を示します。

```
switch(config)# no ip arp event-history errors size medium
switch(config)#
```

関連コマンド

コマンド	説明
show running-config arp all	デフォルト設定を含む ARP 設定を表示します。

ip arp inspection log-buffer

ダイナミック ARP インスペクション（DAI）ロギング バッファ 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*

構文の説明

entries *number*	1 ～ 1024 メッセージの範囲で、バッファ サイズを指定します。

コマンド 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 モード

コマンド履歴

リリース	変更内容
5.0(3)N1(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

このコマンドを使用する前に、**feature dhcp** コマンドを使用して、ダイナミック ホスト コンフィギュレーション プロトコル（DHCP）スヌーピングをイネーブルにしてください。

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。

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。
feature dhcp	DHCP スヌーピングをイネーブルにします。
show ip arp inspection log	DAI のログ設定を表示します。
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 {**ip** [**dst-mac**] [**src-mac**]}

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

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

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

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

構文の説明

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。すべての ARP 要求と ARP 応答で送信者 IP アドレスを検査し、ARP 応答でターゲット IP アドレスのみを検査します。
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。

コマンド 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 モード

コマンド履歴

リリース	変更内容
5.0(3)N1(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

このコマンドを使用する前に、**feature dhcp** コマンドを使用して、ダイナミック ホスト コンフィギュレーション プロトコル（DHCP）スヌーピングをイネーブルにしてください。

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。

送信元 MAC 検証をイネーブルにすると、ARP パケットはパケット本体の送信側イーサネット アドレスが ARP フレーム ヘッダーの送信側イーサネット アドレスと同じである場合にだけ有効と見なされます。宛先 MAC 検証をイネーブルにすると、ARP 要求フレームはターゲット イーサネット アドレスが ARP フレーム ヘッダーの宛先イーサネット アドレスと同じである場合にだけ有効と見なされます。

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)#
```

次に、追加の DAI 検証をディセーブルにする例を示します。

```
switch(config)# no ip arp inspection validate src-mac dst-mac ip
switch(config)#
```

関連コマンド

コマンド	説明
feature dhcp	DHCP スヌーピング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 設定を含めて、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**}]

構文の説明

vlan-list	DAI をアクティブにする VLAN。vlan-list 引数は 1 つの VLAN ID、VLAN ID の範囲、カンマ区切りの ID と範囲を指定できます（「例」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**：ダイナミック ホスト コンフィギュレーション プロトコル（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。

コマンド デフォルト

ドロップされたパケットのロギング

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
5.0(3)N1(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、デバイスは DAI によって検査され、ドロップされたパケットをロギングします。

このコマンドには、ライセンスは必要ありません。

例

次に、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 設定ステータスを表示します。
show ip arp inspection vlan	VLAN の指定されたリストの DAI ステータスを表示します。
show running-config dhcp	DAI 設定を含めて、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

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。

コマンド 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 モード

コマンド履歴

リリース	変更内容
5.0(3)N1(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

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、ライセンスは必要ありません。

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	指定された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 設定を含めて、DHCP スヌーピング設定を表示します。

ip dhcp packet strict-validation

DHCP スヌーピング機能によるダイナミック ホスト コンフィギュレーション プロトコル（DHCP）パケットの厳密な検証をイネーブルにするには、**ip dhcp packet strict-validation** コマンドを使用します。DHCP パケットの厳密な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 packet strict-validation

no ip dhcp packet strict-validation

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。

コマンド 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 モード

コマンド履歴

リリース	変更内容
5.0(2)N2(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 dhcp packet strict-validation コマンドを使用する前に、DHCP スヌーピングをイネーブルにする必要があります。

DHCP パケットの厳密な検証では、DHCP パケットの DHCP オプション フィールドの先頭 4 バイトの「magic cookie」値を含め、このオプション フィールドが有効であるかをチェックします。DHCP パケットの厳密な検証がイネーブルにされている場合、デバイスは検証に失敗した DHCP パケットをドロップします。

例

次に、DHCP パケットの厳密な検証をイネーブルにする例を示します。

```
switch# configure terminal
switch(config)# ip dhcp packet strict-validation
switch(config)#
```

関連コマンド

コマンド	説明
feature dhcp	スイッチをスヌーピングする DHCP をイネーブルにします。
show ip dhcp snooping	DHCP スヌーピングに関する一般的な情報を表示します。
show running-config dhcp	現在の DHCP 設定を表示します。

ip dhcp snooping

デバイスでダイナミック ホスト コンフィギュレーション プロトコル（DHCP）スヌーピングをグローバルに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

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。

コマンド 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にディセーブルです。

コマンド モード

グローバル コンフィギュレーション モード

コマンド履歴

リリース	変更内容
5.0(2)N2(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

このコマンドを使用するには、**feature dhcp** コマンドを使用して 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。

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。

例

次に、DHCP スヌーピングをグローバルに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	デバイスの 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。
show ip dhcp snooping	DHCP スヌーピングに関する一般的な情報を表示します。
show running-config dhcp	IP ソース ガード設定を含めて、DHCP スヌーピング設定を表示します。

ip dhcp snooping information option

ダイナミック ホスト コンフィギュレーション プロトコル（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

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。

コマンド 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 モード

コマンド履歴

リリース	変更内容
5.0(2)N2(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

このコマンドを使用するには、**feature dhcp** コマンドを使用して 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。

例

次に、DHCP スヌーピングをグローバルに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
feature dhcp	デバイスの DHCP スヌーピング機能をイネーブルにします。
ip dhcp snooping	デバイスの 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 スヌーピングに関する一般的な情報を表示します。
show running-config dhcp	IP ソース ガード設定を含めて、DHCP スヌーピング設定を表示します。

ip dhcp snooping trust

ダイナミック ホスト コンフィギュレーション プロトコル（DHCP）メッセージの信頼できる送信元としてインターフェイスを設定するには、**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

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。

コマンド 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 モード

コマンド履歴

リリース	変更内容
5.0(2)N2(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 の信頼状態は、次のタイプのインターフェイスに設定できます。

- 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

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	デバイスの 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 vlan	特定の VLAN 上で DHCP スヌーピングをイネーブルにします。

コマンド	説明
show ip dhcp snooping	DHCP スヌーピングに関する一般的な情報を表示します。
show running-config dhcp	IP ソース ガード設定を含めて、DHCP スヌーピング設定を表示します。

ip dhcp snooping verify mac-address

MAC アドレス検証のダイナミック ホスト コンフィギュレーション プロトコル（DHCP）スヌーピング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

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。

コマンド 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 モード

コマンド履歴

リリース	変更内容
5.0(2)N2(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、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、**feature dhcp** コマンドを使用して 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。

信頼できないインターフェイスからパケットを受信し、この送信元 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、アドレス検証によってデバイスはパケットをドロップします。

例

次の例では、DHCP スヌーピングを MAC アドレス検証でイネーブルにする方法を示します。

```
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
feature dhcp	スイッチをスヌーピングする DHCP をイネーブルにします。
show running-config dhcp	DHCP スヌーピングの設定を表示します。

ip dhcp snooping vlan

1 つ以上の VLAN でダイナミック ホスト コンフィギュレーション プロトコル（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*

構文の説明

vlan-list	DHCP スヌーピングをイネーブルにする VLAN 範囲。*vlan-list* 引数は 1 つの VLAN ID、VLAN ID の範囲、カンマ区切りの ID と範囲を指定できます。有効な VLAN ID は 1 ～ 4094 です。内部用に予約されている VLAN は除きます。 ハイフン（-）を使用して、VLAN ID の範囲の開始 ID と終了 ID を区別します（たとえば、70-100）。 カンマ（,）を使用して、各 VLAN ID および VLAN ID の範囲を区別します（たとえば、20,70-100,142）。

コマンド 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 モード

コマンド履歴

リリース	変更内容
5.0(2)N2(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

このコマンドを使用するには、**feature dhcp** コマンドを使用して 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。

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
feature dhcp	スイッチをスヌーピングする DHCP をイネーブルにします。
show ip dhcp snooping	DHCP スヌーピングに関する一般的な情報を表示します。
show running-config dhcp	IP ソース ガード設定を含めて、DHCP スヌーピング設定を表示します。

ip port access-group

IPv4 アクセス コントロール リスト（ACL）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**

構文の説明

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 を着信トラフィックに適用するように指定します。

コマンド 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 モード
仮想イーサネット インターフェイス コンフィギュレーション モード

コマンド履歴

リリース	変更内容
4.0(0)N1(1a)	このコマンドが追加されました。
5.1(3)N1(1)	このコマンドのサポートが、仮想イーサネット インターフェイスに導入されました。

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 EtherChannel インターフェイス
- 仮想イーサネット インターフェイス

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** コマンドを参照してください。

スイッチでポート ACL が適用されるのは、着信トラフィックだけです。着信パケットは、スイッチ上で 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、そのパケットはスイッチで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、そのパケットはスイッチで廃棄され、ICMP ホスト到達不能メッセージが戻されます。

スイッチから特定の 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。

例

次に、イーサネット インターフェイス 1/2 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)# interface ethernet 1/2
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 1/2 から、ip-acl-01 という IPv4 ACL を削除する例を示します。

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

次に、仮想イーサネット インターフェイス 1 に対して、ip-acl-03 という IPv4 ACL をポート ACL として適用する例を示します。

```
switch# configure terminal
switch(config)# interface vethernet 1
switch(config-if)# ip port access-group ip-acl-03 in
switch(config-if)#
```

関連コマンド

コマンド	説明
interface vethernet	仮想イーサネット インターフェイスを設定します。
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。

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* | **port-channel** *channel-no*}

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

構文の説明

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。スロット番号には 1 ～ 255、ポート番号には 1 ～ 128 を指定できます。
port-channel *channel-no*	EtherChannel インターフェイスを指定します。番号は、1 ～ 4096 です。

コマンド 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 モード

コマンド履歴

リリース	変更内容
5.0(2)N2(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、固定 IP ソース エントリは作成されません。

このコマンドを使用するには、**feature dhcp** コマンドを使用してダイナミック ホスト コンフィギュレーション プロトコル（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。

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
feature dhcp	スイッチをスヌーピングする DHCP 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 interface	インターフェイス コンフィギュレーションを表示します。
show running-config dhcp	DHCP スヌーピング設定情報を表示します。

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。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

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。

コマンド デフォルト

ディセーブル

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 モード

コマンド履歴

リリース	変更内容
5.0(3)N1(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

このコマンドを使用する前に、**feature dhcp** コマンドを使用して、ダイナミック ホスト コンフィギュレーション プロトコル（DHCP）スヌーピングをイネーブルにしてください。

IP ソース ガードは、インターフェイス上の IP トラフィックを、IP-MAC アドレス バインディング テーブル エントリまたはスタティック IP ソース エントリに送信元が含まれているトラフィックだけに制限します。

IP ソース ガードの機能は、DHCP スヌーピング（IP-MAC アドレス バインディング テーブルの構築および維持に関して）、またはスタティック IP ソース エントリの手動での維持に依存しています。

このコマンドには、ライセンスは必要ありません。

例

次に、レイヤ 2 インターフェイスの 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 1/5
switch(config-if)# ip verify source dhcp-snooping-vlan
switch(config-if)#
```

次に、レイヤ 2 インターフェイスの IP ソース ガードをディセーブルにする例を示します。

```
switch# configure terminal
switch(config)# interface ethernet 1/5
switch(config-if)# no ip verify source dhcp-snooping-vlan
switch(config-if)#
```

関連コマンド

コマンド	説明
feature dhcp	スイッチをスヌーピングする DHCP をイネーブルにします。
ip source binding	レイヤ 2 イーサネット インターフェイスのスタティック IP ソース エントリを作成します。
show ip verify source	インターフェイスの 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	実行コンフィギュレーションの IP 設定を表示します。
show running-config interface ethernet	実行コンフィギュレーション内のインターフェイスの設定を表示します。

ip verify unicast source reachable-via

インターフェイス上でユニキャスト リバース パス転送（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**}

構文の説明

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。

コマンド 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 モード

コマンド履歴

リリース	変更内容
5.0(3)N1(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

入力インターフェイスに次のいずれかのユニキャスト RPF モードを設定できます。

- 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予想される場合に使用できます。
- 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インターフェイスが FIB 内のインターフェイスのいずれかと一致する必要はありません。

このコマンドには、ライセンスは必要ありません。

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内のインターフェイスの設定を表示します。
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。

ipv6 access-list

IPv6 アクセス コントロール リスト（ACL）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、**ipv6 access-list** コマンドを使用します。IPv6 ACL を削除するには、このコマンドの **no** 形式を使用します。

ipv6 access-list *access-list-name*

no ipv6 access-list *access-list-name*

構文の説明

access-list-name	IPv6 ACL の名前で、最大 64 の英数字です。名前にはスペースまたは引用符を含めることはできません。

コマンド デフォルト

デフォルトでは、IPv6 ACL は定義されません。

コマンド モード

グローバル コンフィギュレーション モード

コマンド履歴

リリース	変更内容
4.0(1a)N1(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 トラフィックをフィルタリングするには、IPv6 ACL を使用します。

ipv6 access-list コマンドを使用すると、スイッチで 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、IPv6 の **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、このコマンドの入力時にスイッチで新しい ACL が作成されます。

すべての IPv6 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 ipv6 any any
```

この暗黙のルールによって、どの条件にも一致しない IP トラフィックは拒否されます。

例

次に、ipv6-acl-01 という名前の IPv6 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(config)# ipv6 access-list ipv6-acl-01
switch(config-ipv6-acl)#
```

関連コマンド

コマンド	説明
deny（IPv6）	IPv6 ACL に拒否（deny）ルールを設定します。
permit（IPv6）	IPv6 ACL に許可（permit）ルールを設定します。

ipv6 port traffic-filter

IPv6 アクセス コントロール リスト（ACL）をインターフェイスのポート ACL として適用するには、**ipv6 port traffic-filter** コマンドを使用します。インターフェイスから IPv6 ACL を削除するには、このコマンドの **no** 形式を使用します。

ipv6 port traffic-filter *access-list-name* **in**

no ipv6 port traffic-filter *access-list-name* **in**

構文の説明

access-list-name	IPv6 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	デバイスが ACL を着信トラフィックに適用するように指定します。

コマンド 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 モード
仮想イーサネット インターフェイス コンフィギュレーション モード

コマンド履歴

リリース	変更内容
4.0(1a)N1(1)	このコマンドが追加されました。
5.1(3)N1(1)	このコマンドのサポートが、仮想イーサネット インターフェイスに導入されました。

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 IPv6 ACL は適用されません。

ipv6 port traffic-filter 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、IPv6 ACL をポート ACL として適用できます。

- イーサネット インターフェイス
- EtherChannel インターフェイス
- 仮想イーサネット インターフェイス

ipv6 port traffic-filter 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、IPv6 ACL をポート ACL として適用もできます。

- 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、**feature interface-vlan** コマンドを参照してください。

スイッチでポート ACL が適用されるのは、着信トラフィックだけです。着信パケットは、スイッチ上で 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、そのパケットはスイッチで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、そのパケットはスイッチで廃棄され、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。

例

次に、イーサネット インターフェイス 1/3 に対して、ipv6-acl という IPv6 ACL を適用する例を示します。

```
switch# configure terminal
switch(config)# interface ethernet 1/3
switch(config-if)# ipv6 port traffic-filter ipv6-acl in
switch(config-if)#
```

次に、イーサネット インターフェイス 1/3 から、ipv6-acl という IPv6 ACL を削除する例を示します。

```
switch# configure terminal
switch(config)# interface ethernet 1/3
switch(config-if)# no ipv6 port traffic-filter ipv6-acl in
switch(config-if)#
```

次に、特定の仮想イーサネット インターフェイスに対して、ipv6-acl-03 という名前の IPv6 ACL を適用する例を示します。

```
switch# configure terminal
switch(config)# interface vethernet 1
switch(config-if)# ipv6 port traffic-filter ipv6-acl-03 in
switch(config-if)#
```

関連コマンド

コマンド	説明
interface vethernet	仮想イーサネット インターフェイスを設定します。
ipv6 access-list	IPv6 ACL を設定します。
show access-lists	すべての ACL を表示します。
show ipv6 access-lists	特定の IPv6 ACL またはすべての IPv6 ACL を表示します。