



IP ソース ガードの設定

この章では、Cisco NX-OS デバイスで IP ソース ガードを設定する手順について説明します。

この章は、次の項で構成されています。

- [IP ソース ガードについて, 1 ページ](#)
- [IP ソース ガードのライセンス要件, 2 ページ](#)
- [IP ソース ガードの前提条件, 2 ページ](#)
- [IP ソース ガードの注意事項と制約事項, 3 ページ](#)
- [IP ソース ガードのデフォルト設定, 3 ページ](#)
- [IP ソース ガードの設定, 4 ページ](#)
- [IP ソース ガード バインディングの表示, 7 ページ](#)
- [IP ソース ガードの統計情報のクリア, 7 ページ](#)
- [IP ソース ガードの設定例, 8 ページ](#)
- [その他の参考資料, 8 ページ](#)

IP ソース ガードについて

IP ソース ガードは、インターフェイス単位のトラフィック フィルタです。各パケットの IP アドレスと MAC アドレスが、IP と MAC のアドレス バインディングのうち、次に示す2つの送信元のどちらかと一致する場合だけ、IP トラフィックを許可します。

- Dynamic Host Configuration Protocol (DHCP) スヌーピング バインディング テーブル内のエントリ
- 設定したスタティック IP ソース エントリ

信頼できる IP および MAC のアドレス バインディングのフィルタリングは、スプーフィング攻撃（有効なホストの IP アドレスを使用して不正なネットワーク アクセス権を取得する攻撃）の防止

に役立ちます。IP ソース ガードを妨ぐためには、攻撃者は有効なホストの IP アドレスと MAC アドレスを両方スプーフィングする必要があります。

DHCP スヌーピングで信頼状態になっていないレイヤ 2 インターフェイスの IP ソース ガードをイネーブルにできます。IP ソース ガードは、アクセス モードとトランク モードで動作するように設定されているインターフェイスをサポートしています。IP ソース ガードを最初にイネーブルにすると、次のトラフィックを除いて、そのインターフェイス上のインバウンド IP トラフィックがすべてブロックされます。

- DHCP パケット。DHCP パケットは、DHCP スヌーピングによって検査が実行され、その結果に応じて転送またはドロップされます。
- Cisco NX-OS デバイスに設定したスタティック IP ソース エントリからの IP トラフィック。

デバイスが IP トラフィックを許可するのは、DHCP スヌーピングによって IP パケットの IP アドレスと MAC アドレスのバインディング テーブル エントリが追加された場合、またはユーザがスタティック IP ソース エントリを設定した場合です。

パケットの IP アドレスと MAC アドレスがバインディング テーブル エントリにも、スタティック IP ソース エントリにもない場合、その IP パケットはドロップされます。たとえば、**show ip dhcp snooping binding** コマンドによって表示されたバインディング テーブル エントリが次のとおりであるとします。

MacAddress	IpAddress	LeaseSec	Type	VLAN	Interface
00:02:B3:3F:3B:99	10.5.5.2	6943	dhcp-snooping	10	Ethernet2/3

IP アドレスが 10.5.5.2 の IP パケットをデバイスが受信した場合、IP ソース ガードによってこのパケットが転送されるのは、このパケットの MAC アドレスが 00:02:B3:3F:3B:99 のときだけです。

IP ソース ガードのライセンス要件

次の表に、IP ソース ガードのライセンス要件を示します。

製品	ライセンス要件
Cisco NX-OS	IP ソース ガードにはライセンスは必要ありません。ライセンスパッケージに含まれていない機能は nx-os イメージにバンドルされており、無料で提供されます。Cisco NX-OS ライセンス方式の詳細については、『 <i>Cisco NX-OS Licensing Guide</i> 』を参照してください。

IP ソース ガードの前提条件

IP ソース ガードの前提条件は次のとおりです。

- IP ソース ガードを設定するには、その前に DHCP 機能および DHCP スヌーピングをイネーブルにする必要があります。 [DHCP の設定](#) を参照してください。
- **hardware access-list tcam region ipsg** コマンドを使用して、IP ソース ガード用の ACL TCAM のリージョン サイズを設定する必要があります。 [ACL TCAM リージョン サイズの設定](#) を参照してください。



(注) デフォルトでは、ipsg のリージョン サイズはゼロです。SMAC-IP バインディングの保存と適用をするには、このリージョンに十分なエントリを割り当てる必要があります。

IP ソース ガイドの注意事項と制約事項

IP ソース ガードに関する注意事項と制約事項は次のとおりです。

- 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。インターフェイス上の IP ソース ガードを初めてイネーブルにする際には、そのインターフェイス上のホストが DHCP サーバから新しい IP アドレスを受信するまで、IP トラフィックが中断されることがあります。
- 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。
- IP ソース ガードは、Fabric Extender (FEX) および汎用拡張モジュール (GEM) ポートではサポートされていません。
- 次の注意事項と制約事項は、Cisco Nexus 9200 シリーズ スイッチに適用されます。
 - 着信インターフェイスで IPSG がイネーブルであると IPv6 の隣接関係は形成されません。
 - IPSG は HSRP スタンバイで ARP パケットを廃棄します。
 - DHCP スヌーピングおよび IPSG がイネーブルにされている場合、ホストのバインディング エントリが存在すると、ARP がなくてもトラフィックはホストに転送されます。

IP ソース ガードのデフォルト設定

次の表に、IP ソース ガードのパラメータのデフォルト設定を示します。

表 1: IP ソース ガードのパラメータのデフォルト値

パラメータ	デフォルト
IP ソース ガード	各インターフェイスでディセーブル
IP ソース エントリ	なし。デフォルトではスタティック IP ソース エントリはありません。デフォルトの IP ソース エントリもありません。

IP ソース ガードの設定

レイヤ2インターフェイスに対する IP ソース ガードのイネーブル化またはディセーブル化

レイヤ2インターフェイスに対して IP ソース ガードをイネーブルまたはディセーブルに設定できます。デフォルトでは、すべてのインターフェイスに対して IP ソース ガードはディセーブル。

はじめる前に

DHCP 機能および DHCP スヌーピングがイネーブルにされていることを確認します。

IPSG (ipsg) の ACL TCAM リージョン サイズが設定されていることを確認します。

手順の概要

1. **configure terminal**
2. **interface ethernet slot/port**
3. **[no] ip verify source dhcp-snooping-vlan**
4. (任意) **show running-config dhcp**
5. (任意) **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例 : <pre>switch# configure terminal switch(config)#</pre>	グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 2	interface ethernet slot/port 例： switch(config)# interface ethernet 2/3 switch(config-if)#	指定したインターフェイスに対してインターフェイス コンフィギュレーション モードを開始します。
ステップ 3	[no] ip verify source dhcp-snooping-vlan 例： switch(config-if)# ip verify source dhcp-snooping vlan	インターフェイスの IP ソース ガードをイネーブルにします。このコマンドの no 形式を使用すると、そのインターフェイスの IP ソース ガードがディセーブルになります。
ステップ 4	show running-config dhcp 例： switch(config-if)# show running-config dhcp	(任意) IP ソース ガードの設定も含めて、DHCP スヌーピングの実行コンフィギュレーションを表示します。
ステップ 5	copy running-config startup-config 例： switch(config-if)# copy running-config startup-config	(任意) 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にコピーします。

スタティック IP ソース エントリの追加または削除

デバイス上のスタティック IP ソース エントリの追加または削除を実行できます。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。

手順の概要

1. **configure terminal**
2. **[no] ip source binding ip-address mac-address vlan-id interface interface-type slot/port**
3. (任意) **show ip dhcp snooping binding [interface interface-type slot/port]**
4. (任意) **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例： switch# configure terminal switch(config)#	グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 2	[no] ip source binding ip-address mac-address vlan vlan-id [interface interface-type slot/port] 例： <pre>switch(config)# ip source binding 10.5.22.17 001f.28bd.0013 vlan 100 interface ethernet 2/3</pre>	現在の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。このコマンドの no 形式を使用すると、スタティック IP ソース エントリが削除されます。
ステップ 3	show ip dhcp snooping binding [interface interface-type slot/port] 例： <pre>switch(config)# show ip dhcp snooping binding interface ethernet 2/3</pre>	(任意) スタティック IP ソース エントリを含めて、指定したインターフェイスの IP-MAC アドレス バインディングを表示します。スタティック エントリは、Type カラムの表示で示されます。
ステップ 4	copy running-config startup-config 例： <pre>switch(config)# copy running-config startup-config</pre>	(任意) 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にコピーします。

トランク ポート用 IP ソース ガードの設定

あるポートに IP ソース ガードが設定されている場合、それを TCAM 内で許可する DHCP スヌーピング エントリがない限り、そのポートに着信するトラフィックはドロップされます。ただし、IP ソース ガードがトランク ポートに設定されていて特定の VLAN で着信するトラフィックではこのチェックを行いたくない場合（それらで DHCP スヌーピングがイネーブルにされていない場合であっても）、除外したい VLAN のリストを指定できます。

はじめる前に

DHCP 機能および DHCP スヌーピングがイネーブルにされていることを確認します。

手順の概要

1. **configure terminal**
2. **[no] ip dhcp snooping ipsg-excluded vlan vlan-list**
3. (任意) **show ip ver source [ethernet slot/port | port-channel channel-number]**
4. (任意) **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例： switch# configure terminal switch(config)#	グローバル コンフィギュレーション モードを開始します。
ステップ 2	[no] ip dhcp snooping ipsg-excluded vlanvlan-list 例： switch(config)# ip dhcp snooping ipsg-excluded vlan 1001-1256,3097	トランク ポートの IP ソース ガードで DHCP スヌーピングのチェックから除外したい VLAN のリストを指定します。
ステップ 3	show ip ver source [ethernetslot/port port-channelchannel-number] 例： switch(config)# show ip ver source	(任意) どの VLAN が除外されるかを表示します。
ステップ 4	copy running-config startup-config 例： switch(config)# copy running-config startup-config	(任意) 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にコピーします。

IP ソース ガード バインディングの表示

IP-MAC アドレス バインディングを表示させるには、**show ip ver source[ethernetslot/port | port-channelchannel-number]** コマンドを使用します。

IP ソース ガードの統計情報のクリア

IP ソース ガードの統計情報のクリアを行うには、次の表に示すコマンドを使用します。

コマンド	目的
clear access-list ipsg stats [instancenumber modulenummer]	IP ソース ガードの統計情報をクリアします。

IP ソース ガードの設定例

スタティック IP ソース エントリを作成し、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。

```
ip source binding 10.5.22.17 001f.28bd.0013 vlan 100 interface ethernet 2/3
interface ethernet 2/3
no shutdown
ip verify source dhcp-snooping-vlan
show ip ver source
```

```
IP source guard excluded vlans:
```

```
-----
None
```

```
-----
IP source guard is enabled on the following interfaces:
```

```
-----
ethernet2/3
```

その他の参考資料

関連資料

関連項目	マニュアルタイトル
ACL TCAM リージョン	IP ACL の設定
『DHCP and DHCP snooping』	DHCP の設定