CHAPTER 16

IP ソース ガードの設定

この章では、IP ソースガードを設定する手順について説明します。

この章の内容は次のとおりです。

IP ソース ガードの概要

IP ソース ガードは、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にのみ IP トラフィックを許可するインターフェイス単位のトラフィック フィルタです。

- 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に依存した攻撃（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 ガードを妨げるためには、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。
- 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、次のようなバインディング テーブル エントリが表示されるとします。:

```
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。

バーチャライゼーション サポート

Virtual Device Context（VDC; バーチャル デバイス コンテキスト）で使用される IP ソース ガードには、次の事項が適用されます。

- IP-MAC アドレス バインディングは各 VDC に固有です。ある VDC 内のバインディングが他の VDC の IP ソース ガードに影響を及ぼすことはありません。
- NX-OS は、バインディング データベースのサイズを VDC 単位では制限しません。

IP ソース ガードのライセンス要件

この機能のライセンス要件は次の表のとおりです。

製品	ライセンス要件
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、Cisco NX-OS システム イメージにバンドルされており、追加料金なしで利用できます。NX-OS のライセンス スキームに関する詳細は、『*Cisco NX-OS Licensing Guide*』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 ガードを設定するためには、DHCP スヌーピングについての知識が必要です。
- DHCP スヌーピングがイネーブルになっている必要があります（「DHCP スヌーピングの設定」[p.14-7] を参照）。

注意事項および制約事項

IP ソース ガードの設定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 ガードの設定

ここでは、次の作業について説明します。

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。

作業を開始する前に

デフォルトでは、IP ソース ガードはすべてのインターフェイスでディセーブルです。

DHCP スヌーピングがイネーブルになっていることを確認します。詳細については、「DHCP スヌーピング機能のイネーブル化またはディセーブル化」（p.14-8）を参照してください。

手順の概要

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

詳細な手順

	コマンド	目的

ステップ 1	**config t**
	
	例：
	`switch# config t`
	`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	**interface ethernet** *slot/port*
	
	例：
	`switch(config)# interface ethernet 2/3`
	`switch(config-if)#`
		特定のインターフェイスのインターフェイス 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。**no** オプションを使用すると、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。

	コマンド	目的
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。

作業を開始する前に

デフォルトでは、デバイスにはスタティック IP ソース エントリは設定されていません。

手順の概要

1. **config t**
2. [**no**] **ip source binding** *IP-address MAC-address* **vlan** *vlan-ID* **interface ethernet** *slot*/*port*
3. **show ip dhcp snooping binding [interface ethernet** *slot*/*port*]
4. **copy running-config startup-config**

詳細な手順

	コマンド	目的

ステップ 1	**config t**
	
	例：
	`switch# config t`
	`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 source binding** *IP-address MAC-address* **vlan** *vlan-ID* **interface ethernet** *slot*/*port* **例：** `switch(config)# ip source binding 10.5.22.17 001f.28bd.0013 vlan 100 interface ethernet 2/3`	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。スタティック IP ソース エントリを削除する場合は、**no** オプションを使用します。
ステップ 3	**show ip dhcp snooping binding** [**interface ethernet** *slot*/*port*] **例：** `switch(config)# show ip dhcp snooping binding interface ethernet 2/3`	（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 カラムに「static」と表示されています。
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 ガードの設定の確認

IP ソース ガードの設定情報を表示するには、次のいずれかの作業を行います。

コマンド	目的
show running-config dhcp	IP ソース ガードの設定を含めて、DHCP スヌーピングの設定を表示します。
show ip dhcp snooping binding	スタティック IP ソース エントリを含めて、IP-MAC アドレス バインディングを表示します。

これらのコマンドの出力フィールドに関する詳細は、『*Cisco NX-OS Security Command Reference*』を参照してください。

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するには、**show ip verify source** コマンドを使用します。

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
```

デフォルト設定

表 16-1 に IP ソース ガードのパラメータのデフォルト設定値を示します。

表 16-1　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。

その他の参考資料

IP ソース ガードの実装に関する詳細情報については、次を参照してください。

- 関連資料（p.16-7）
- 規格（p.16-7）

関連資料

関連事項	タイトル
DHCP スヌーピングの概要（p.14-2）	『*Cisco NX-OS Security Configuration Guide*』
IP ソース ガードのコマンド：完全なコマンド構文、コマンド モード、コマンド履歴、デフォルト値、使用上の注意、例	『*Cisco NX-OS Security Command Reference*』
DHCP スヌーピングのコマンド：完全なコマンド構文、コマンド モード、コマンド履歴、デフォルト値、使用上の注意、例	『*Cisco NX-OS Security Command Reference*』

規格

規格	タイトル
この機能のサポート対象の規格には、新規規格も変更された規格もありません。また、この機能は既存の規格に対するサポートに影響を及ぼしません。	—