IP ソース ガードの設定

この章では、Cisco Nexus 5000 シリーズ スイッチ上で IP ソース ガードを設定する方法について説明します。

この章は、次の内容で構成されています。

IP ソース ガードの概要

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、次のバインディング 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。

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すべて Cisco NX-OS システム イメージにバンドルされており、追加費用は一切発生しません。 Cisco NX-OS ライセンス方式に関する詳細は、『*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。

- DHCP 機能をイネーブルにする必要があります。

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
IPSG	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 機能がイネーブルであることを確認します。

手順

	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	**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。
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。

関連トピック

スタティック IP ソース エントリの追加または削除, （4 ページ）

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、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

	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 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 カラムの表示で示されます。
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。

関連トピック

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, （3 ページ）
IP ソース ガード バインディングの表示, （5 ページ）

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
```

IP ソース ガードに関する追加情報

関連資料

関連項目	参照先
IP ソース ガード 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 Nexus 7000 Series 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 Nexus 7000 Series NX-OS Security Command Reference*』

標準

標準	タイトル
この機能でサポートされる新規または改訂された標準規格はありません。また、この機能による既存の標準規格サポートの変更はありません。	—