CHAPTER 49

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。IP ソース ガードは Cisco IOS Release 12.2(33)SXH 以降のリリースでサポートされます。

（注） この章で使用しているコマンドの構文および使用方法の詳細については、次の URL の『Cisco IOS Master Command List, Release 12.2SX』を参照してください。

http://www.cisco.com/en/US/docs/ios/mcl/122sxmcl/12_2sx_mcl_book.html

ヒント Cisco Catalyst 6500 シリーズ スイッチの詳細（設定例およびトラブルシューティング情報を含む）については、次のページに示されるドキュメントを参照してください。

http://www.cisco.com/en/US/products/hw/switches/ps708/tsd_products_support_series_home.html

この章で説明する内容は、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、レイヤ 2 ポートでソース IP アドレス フィルタリングを提供して、悪意のあるホストが正規のホストの IP アドレスを装うことで正規のホストを偽装することを防ぎます。この機能では、ダイナミックな Dynamic Host Configuration Protocol（DHCP）スヌーピングおよびスタティックな IP ソース バインディングを使用して、IP アドレスと信頼できないレイヤ 2 アクセス ポート上のホストを照合します。

まず、DHCP パケットを除く、保護済みポート上の全 IP トラフィックがブロックされます。クライアントが DHCP サーバから IP アドレスを受信したあと、またスタティック IP ソース バインディングが管理者によって設定されたあと、その IP 送信元アドレスのある全トラフィックがそのクライアントから許可されます。他のホストからのトラフィックは拒否されます。このフィルタリングは、ネイバー ホストの IP アドレスを要求することで、ネットワークを攻撃するホストの能力を制限します。IP ソース ガードは、暗黙的な Port Access Control List（PACL; ポート アクセス 制御リスト）を自動的に作成するポートベースの機能です。

IP ソース ガードと VLAN ベース機能との相互作用

access-group mode コマンドを使用して、IP ソース ガードと Virtual LAN（VLAN; 仮想 LAN）ベース機能（VACL、Cisco IOS ACL、RACL 等）との相互作用方法を指定します。

優先ポート モードでは、IP ソース ガードがインターフェイスに設定されている場合、IP ソース ガードが他の VLAN ベース機能を無効にします。IP ソース ガードがインターフェイスに設定されていない場合、他の VLAN ベース機能が入力方向に結合されてインターフェイスに適用されます。

結合モードでは、IP ソース ガードと VLAN ベース機能が入力方向に結合されて、インターフェイスに適用されます。これがデフォルトのアクセスグループ モードです。

チャネル ポート

IP ソース ガードは、メインのレイヤ 2 チャネル インターフェイスでサポートされていますが、ポート メンバーではサポートされていません。IP ソース ガードがメインのレイヤ 2 チャネル インターフェイスで適用されている場合、チャネル内のすべてのメンバー ポートに適用されます。

トランク ポート

IP ソース ガードはトランク ポートでサポートされていません。

レイヤ 2 および レイヤ 3 ポート変換

IP ソース ガード ポリシーがレイヤ 2 ポートに適用されて、その後そのポートをレイヤ 3 ポートに変更した場合、IP ソース ガード ポリシーは機能しなくなりますが、設定内には残ります。ポートをレイヤ 2 ポートに変更し戻すと、IP ソース ガード ポリシーが再び有効になります。

IP ソース ガードと音声 VLAN

IP ソース ガードは、音声 VLAN に属するレイヤ 2 ポートをサポートしています。レイヤ 2 ポートに音声 VLAN を設定するには、**switchport voice vlan** コマンドを使用します。音声 VLAN でアクティブになっている IP ソース ガードの場合、DHCP スヌーピングが音声 VLAN でイネーブルになっている必要があります。結合モードで、IP ソース ガード機能はアクセス VLAN 上に設定されている VLAN ACL（VACL）と Cisco IOS ACL に結合されます。

IP ソース ガードと Web ベース認証

Cisco IOS Release 12.2(33)SXI2 よりも前のリリースでは、同じインターフェイスでの IP ソース ガードと Web ベース認証の設定がサポートされていません。

Cisco IOS Release 12.2(33)SXI2 以降のリリースでは、同じインターフェイスで IP ソース ガードと Web ベース認証を設定できます。DHCP スヌーピングもアクセス VLAN でイネーブルにする場合は、グローバル コンフィギュレーション モードで **mls acl tcam override dynamic dhcp-snooping** コマンドを入力して、2 つの機能の矛盾を回避する必要があります。IP ソース ガードと Web ベース認証が組み合わされているときは、その他の VLAN ベース機能はサポートされません。

IP ソース ガードの制約事項

IP ソース ガード機能はハードウェアでだけサポートされているため、十分なハードウェア リソースが利用できない場合 IP ソース ガードは適用されません。これらのハードウェア リソースはシステムに設定されている他のさまざまな ACL 機能と共有されています。次の制約事項が IP ソース ガードに適用されます。

- 入力レイヤ 2 ポートでだけサポートされています。
- ハードウェアでだけサポートされています。
- ソフトウェアで処理されるトラフィックには適用されません。
- Media Access Control（MAC; メディア アクセス制御）アドレスに基づくトラフィックのフィルタリングはサポートしていません。
- プライベート VLAN ではサポートされません。

スイッチ上での IP ソース ガードの設定

IP ソース ガードをイネーブルにするには、次の作業を行います。

	コマンド	目的
ステップ 1	`Router(config)# ip dhcp snooping`	DHCP スヌーピングをグローバルにイネーブル化します。 **no** キーワードを使用して DHCP スヌーピングをディセーブルにできます。
ステップ 2	`Router(config)# ip dhcp snooping vlan` *number* [*number*]	VLAN 上で DHCP スヌーピングをイネーブルにします。
ステップ 3	`Router(config)# interface` *interface-name*	設定するインターフェイスを選択します。
ステップ 4	`Router(config-if)# no ip dhcp snooping trust`	インターフェイスを信頼できないと設定する場合は、**no** キーワードを使用します。
ステップ 5	`Router(config-if)# ip verify source vlan dhcp-snooping` [**port-security**]	IP ソース ガード、送信元 IP アドレス フィルタリングをポートでイネーブルにします。コマンド パラメータは次のとおりです。 • **vlan** の場合、インターフェイス上の特定の VLAN にだけ機能が適用されます。**dhcp-snooping** オプションの場合、DHCP スヌーピングがイネーブルであるインターフェイス上にあるすべての VLAN に機能が適用されます。 • **port-security** により MAC アドレス フィルタリングがイネーブルになります。この機能は現在サポートされていません。
ステップ 6	`Router(config-if)# exit`	グローバル コンフィギュレーション モードに戻ります。
ステップ 7	`Router(config)# ip source binding` *mac-address* **vlan** *vlan-id ip-address* **interface** *interface-name*	（任意）スタティック IP バインディングをポートに設定します。

	コマンド	目的
ステップ 8	`Router(config)# end`	コンフィギュレーション モードを終了します。
ステップ 9	`Router# show ip verify source [interface interface-name]`	設定を確認します。

（注）　スタティック IP ソース バインディングは、レイヤ 2 ポートにだけ設定可能です。**ip source binding vlan interface** コマンドをレイヤ 3 ポートに設定した場合、次のようなエラー メッセージを受信します。

```
Static IP source binding can only be configured on switch port.
```

no キーワードは、対応する IP ソース バインディング エントリを削除します。削除が正常に実行されるために、このコマンドではすべての必須パラメータが正確に一致しなければなりません。

次に、VLAN 10 ～ 20 上においてレイヤ 2 単位で IP ソース ガードをイネーブルにする例を示します。

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# ip dhcp snooping
Router(config)# ip dhcp snooping vlan 10 20
Router(config)# interface fa6/1
Router(config-if)# switchport mode access
Router(config-if)# switchport access vlan 10
Router(config-if)# no ip dhcp snooping trust
Router(config-if)# ip verify source vlan dhcp-snooping
Router(config-if)# end
Router# show ip verify source interface f6/1
Interface  Filter-type  Filter-mode  IP-address       Mac-address        Vlan
---------  -----------  -----------  ---------------  -----------------  ----------
Fa6/1      ip           active       10.0.0.1                            10
Fa6/1      ip           active       deny-all                            11-20
Router#
```

出力は、VLAN 10 に対して有効な DHCP バインディングが 1 つあることを示しています。

次の例では、優先ポート モードを使用するようインターフェイスを設定します。

```
Router# configure terminal
Router(config)# interface gigabitEthernet 6/1
Router(config-if)# access-group mode prefer port
```

次の例では、マージ モードを使用するようインターフェイスを設定します。

```
Router# configure terminal
Router(config)# interface gigabitEthernet 6/1
Router(config-if)# access-group mode merge
```

IP ソース ガード情報の表示

スイッチ上にあるすべてのインターフェイスの IP ソース ガード PACL 情報を表示するには、次の作業を行います。

コマンド	目的
Router# **show ip verify source** [**interface** *interface-name*]	スイッチ上にあるすべてのインターフェイスまたは指定のインターフェイス上にある IP ソース ガード PACL 情報を表示します。

次に、DHCP スヌーピングが VLAN 10 ～ 20 でイネーブルであり、インターフェイス fa6/1 が IP フィルタリング用に設定されていて、既存の IP アドレス バインディング 10.0.01 が VLAN 10 上にある例を示します。

```
Router# show ip verify source interface fa6/1
Interface  Filter-type  Filter-mode  IP-address       Mac-address     Vlan
---------  -----------  -----------  ---------------  --------------  ---------
fa6/1      ip           active       10.0.0.1                         10
fa6/1      ip           active       deny-all                         11-20
```

（注） 2 番めのエントリは、デフォルト PACL（全 IP トラフィックを拒否）が有効な IP ソース バインディングのないスヌーピング対応 VLAN のポートにインストールされていることを示しています。

次に、信頼できるポートの PACL 情報が表示されている例を示します。

```
Interface  Filter-type  Filter-mode  IP-address       Mac-address     Vlan
---------  -----------  -----------  ---------------  --------------  ---------
fa6/2      ip           inactive-trust-port
```

次に、DHCP スヌーピングが設定されていない VLAN 内にあるポートの PACL 情報が表示されている例を示します。

```
Interface  Filter-type  Filter-mode  IP-address       Mac-address     Vlan
---------  -----------  -----------  ---------------  --------------  ---------
fa6/3      ip           inactive-no-snooping-vlan
```

次に、IP/MAC フィルタリング用に設定された複数のバインディングのあるポートの PACL 情報が表示されている例を示します。

```
Interface  Filter-type  Filter-mode  IP-address       Mac-address     Vlan
---------  -----------  -----------  ---------------  --------------  ---------
fa6/4      ip           active       10.0.0.2         aaaa.bbbb.cccc  10
fa6/4      ip           active       11.0.0.1         aaaa.bbbb.cccd  11
fa6/4      ip           active       deny-all         deny-all        12-20
```

次に、IP/MAC フィルタリングが設定されているもののポート セキュリティが設定されていないポートの PACL 情報が表示されている例を示します。

```
Interface  Filter-type  Filter-mode  IP-address       Mac-address     Vlan
---------  -----------  -----------  ---------------  --------------  ---------
fa6/5      ip           active       10.0.0.3         permit-all      10
fa6/5      ip           active       deny-all         permit-all      11-20
```

（注） ポート セキュリティがイネーブルでないため MAC アドレス フィルタは全許可を示しているので、MAC フィルタはポート/VLAN に適用されておらず、事実上ディセーブルです。常にポート セキュリティを最初にイネーブルにしてください。

次に、IP 送信元フィルタ モードが設定されていないポートで **show ip verify source** コマンドを入力したときのエラー メッセージの例を示します。

```
Router# show ip verify source interface fa6/6
IP Source Guard is not configured on the interface fa6/6.
```

次に、IP ソース ガードがイネーブルであるスイッチの全インターフェイスを表示する例を示します。

```
Router# show ip verify source
Interface  Filter-type  Filter-mode  IP-address       Mac-address     Vlan
---------  -----------  -----------  ---------------  --------------  ---------
fa6/1      ip           active       10.0.0.1                         10
fa6/1      ip           active       deny-all                         11-20
fa6/2      ip           inactive-trust-port
fa6/3      ip           inactive-no-snooping-vlan
fa6/4      ip           active       10.0.0.2         aaaa.bbbb.cccc  10
fa6/4      ip           active       11.0.0.1         aaaa.bbbb.cccd  11
fa6/4      ip           active       deny-all         deny-all        12-20
fa6/5      ip           active       10.0.0.3         permit-all      10
fa6/5      ip           active       deny-all         permit-all      11-20
```

IP ソース バインディング情報の表示

スイッチ上にあるすべてのインターフェイスに設定されたすべての IP ソース バインディングを表示するには、次の作業を行います。

コマンド	目的
Router# **show ip source binding** [*ip-address*] [*mac-address*] [**dhcp-snooping** | **static**] [**vlan** *vlan-id*] [**interface** *interface-name*]	オプションの指定表示フィルタを使用した IP ソース バインディングを表示します。 **dhcp-snooping** フィルタは、DHCP スヌーピングがイネーブルであるインターフェイス上にあるすべての VLAN を表示します。

次に、スイッチ上にあるすべてのインターフェイスに設定されたすべての IP ソース バインディングを表示する例を示します。

```
Router# show ip source binding
MacAddress          IpAddress        Lease(sec)  Type           VLAN  Interface
------------------  ---------------  ----------  -------------  ----  --------------------
00:02:B3:3F:3B:99   55.5.5.2         6522        dhcp-snooping  10    FastEthernet6/10
00:00:00:0A:00:0B   11.0.0.1         infinite    static         10    FastEthernet6/10
Router#
```

表 49-1 では、**show ip source binding** コマンドの出力結果における各フィールドについて説明します。

表 49-1　show ip source binding コマンドの出力結果

フィールド	説明
MAC Address	クライアント ハードウェアの MAC アドレス
IP Address	DHCP サーバから割り当てられたクライアント IP アドレス
Lease (seconds)	IP アドレスのリース期間
Type	バインディング タイプ。Command Line Interface（CLI; コマンドライン インターフェイス）から DHCP スヌーピングで学習されたダイナミック バインディングに設定されたスタティック バインディング
VLAN	クライアント インターフェイスの VLAN 番号
Interface	DHCP クライアント ホストに接続されるインターフェイス

ヒント　Cisco Catalyst 6500 シリーズ スイッチの詳細（設定例およびトラブルシューティング情報を含む）については、次のページに示されるドキュメントを参照してください。
http://www.cisco.com/en/US/products/hw/switches/ps708/tsd_products_support_series_home.html

ヒント