CHAPTER 39

DAI の設定

この章では、Catalyst 6500 シリーズ スイッチに Dynamic Address Resolution Protocol（ARP; アドレス解決プロトコル）Inspection（DAI; ダイナミック ARP 検査）を設定する方法について説明します。Release 12.2(18)SXE 以降のリリースでは、PFC3 は DAI をサポートします。PFC2 は、DAI をサポートしません。

（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 で『*Catalyst 6500 Series Switch Cisco IOS Command Reference*』Release 12.2SX を参照してください。

http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/122sx/cmdref/index.htm

この章で説明する内容は、次のとおりです。

DAI の概要

ここでは、DAI によって ARP スプーフィング攻撃を防止する方法について説明します。

ARP の概要

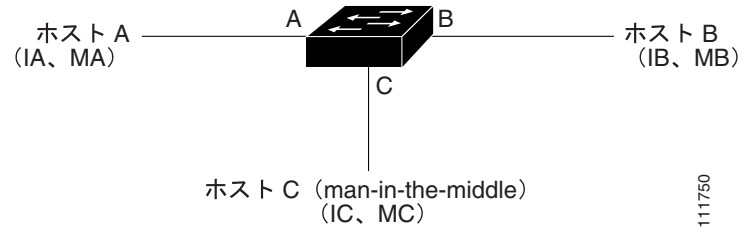
ARP では、IP アドレスを MAC（メディア アクセス制御）アドレスにマッピングすることで、レイヤ 2 ブロードキャスト ドメイン内の IP 通信を実現します。たとえば、ホスト B がホスト A に情報を送信しようとする場合、ホスト B の ARP キャッシュにホスト A の MAC アドレスが存在しないとします。ホスト B はホスト A の IP アドレスに関連付けられた MAC アドレスを取得するため、このブロードキャスト ドメイン内の全ホストに対してブロードキャスト メッセージを送信します。ブロードキャスト ドメイン内の全ホストはこの ARP 要求を受信し、これに対してホスト A は自身の MAC アドレスを返します。

ARP スプーフィング攻撃の概要

ARP スプーフィング攻撃と ARP キャッシュ ポイズニングは、ARP 要求を受信していない場合でも ARP によってホストが無償応答できるため発生する可能性があります。攻撃が開始されると、攻撃を受けた機器からのすべてのトラフィックは、攻撃者のコンピュータを経由してルータ、スイッチ、またはホストに送信されるようになります。

ARP スプーフィング攻撃では、サブネットに接続されたシステムの ARP キャッシュをポイズニング（汚染）し、このサブネット上の他のホスト宛てのトラフィックを代行受信することで、レイヤ 2 ネットワークに接続されたホスト、スイッチ、およびルータを攻撃します。図 39-1 は、ARP キャッシュ ポイズニングの例を示します。

図 39-1　ARP キャッシュ ポイズニング



ホスト A、B、C は、それぞれインターフェイス A、B、C を介してスイッチに接続されています。すべてのホストは同一サブネットに属します。カッコ内は、各ホストの IP および MAC アドレスを示します。たとえば、ホスト A は IP アドレス [IA]、および MAC アドレス [MA] を使用します。ホスト A が IP レイヤ上でホスト B と通信する場合は、ホスト A は IP アドレス IB に関連付けられた MAC アドレスを尋ねる ARP 要求をブロードキャストします。スイッチとホスト B はこの ARP 要求を受信すると、IP アドレス IA および MAC アドレス MA を持つホストの ARP バインディングを、それぞれの ARP キャッシュ内に書き込みます。たとえば、IP アドレス IA は MAC アドレス MA にバインドされます。ホスト B が応答すると、スイッチとホスト A は、IP アドレス IB および MAC アドレス MB を持つホストのバインディングを、それぞれの ARP キャッシュ内に書き込みます。

ホスト C は、IP アドレス IA（または IB）および MAC アドレス MC を持つホストのバインディングによって偽装した ARP 応答をブロードキャストすることで、スイッチ、ホスト A、およびホスト B の ARP キャッシュをポイズニングできます。ARP キャッシュがポイズニングされたホストは、IA または IB 宛てのトラフィックに、宛先 MAC アドレスとして MAC アドレス MC を使用します。つまり、ホスト C がこのトラフィックを代行受信することになります。ホスト C は IA および IB に関連付けられた本物の MAC アドレスを知っているため、正しい MAC アドレスを宛先として使用することで、代行受信したトラフィックをこれらのホストに転送できます。ホスト C は、ホスト A からホスト　B　へのトラフィック　ストリーム内に自身を割り込ませています。これは、*man-in-the-middle* 攻撃の典型的なトポロジーです。

DAI および ARP スプーフィング攻撃の概要

DAI は、ネットワーク内の ARP パケットを検証するセキュリティ機能です。DAI は、IP アドレスと MAC アドレスとの無効なバインディングを持つ ARP パケットを代行受信、ログ記録、および廃棄します。この機能により、一部の man-in-the-middle 攻撃からネットワークを保護できます。

DAI を使用することで、有効な ARP 要求および応答だけが中継されることを保証できます。スイッチの動作は次のとおりです。

- 信頼できないポートを経由したすべての ARP 要求および ARP 応答を代行受信します。
- 代行受信した各パケットが、IP アドレスと MAC アドレスの有効なバインディングを持つことを確認してから、ローカル ARP キャッシュを更新するか、または適切な宛先にパケットを転送します。
- 無効な ARP パケットは廃棄します。

DAI は信頼できるデータベースに保存された有効な IP アドレスおよび MAC アドレス バインディングに基づき、ARP パケットの有効性を判断します。このデータベースを、DHCP スヌーピング バインディング データベースと呼びます。このデータベースは、VLAN およびスイッチ上で Dynamic Host Configuration Protocol（DHCP）スヌーピングがイネーブルにされている場合に、DHCP スヌーピングによって構築されます。信頼できるインターフェイス上で ARP パケットを受信した場合は、スイッチはこのパケットを検査せずに転送します。信頼できないインターフェイスでは、スイッチは有効性を確認できたパケットのみを転送します。

DAI では、スタティックに設定した IP アドレスを持つホストに対し、ユーザ定義の Access Control List（ACL; アクセス制御リスト）に照合することで ARP パケットを検証できます（「DAI フィルタリングのための ARP ACL の適用」[p.39-10] を参照）。スイッチは、廃棄されたパケットを記録します（「廃棄パケットのロギング」[p.39-5] を参照）。

DAI では、パケット内の IP アドレスが無効な場合に ARP パケットを廃棄するのか、または ARP パケット本体の MAC アドレスがイーサネット ヘッダーに指定されたアドレスと一致しない場合に ARP パケットを廃棄するのかを設定できます（「その他の検証のイネーブル化」[p.39-12] を参照）。

インターフェイスの信頼状態とネットワーク セキュリティ

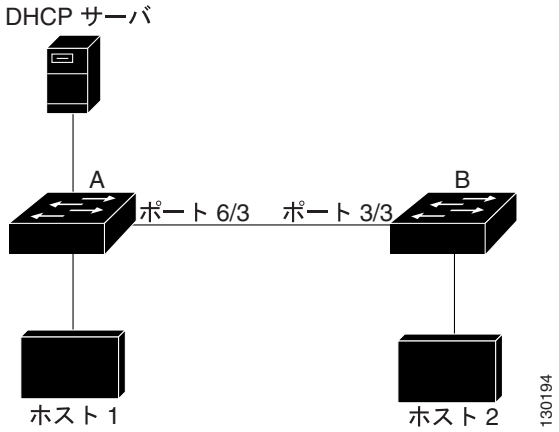
DAI は、スイッチの各インターフェイスに信頼状態を関連付けます。信頼できるインターフェイス上で受信されたパケットは、DAI のすべての有効性検査をバイパスしますが、信頼できないインターフェイス上で受信されたパケットには、DAI の有効性検査が行われます。

一般的なネットワーク設定では、ホスト ポートに接続されているすべてのスイッチ ポートを信頼できないポートとして、スイッチに接続されているすべてのスイッチ ポートは信頼できるポートとして設定します。この設定では、特定スイッチからネットワークに送信されるすべての ARP パケットは、セキュリティ検査をバイパスします。VLAN 内、またはネットワーク内のその他の場所では、他の検査を実行する必要はありません。信頼状態を設定するには、**ip arp inspection trust** インターフェイス コンフィギュレーション コマンドを使用します。

注意　信頼状態の設定は、慎重に行ってください。信頼すべきインターフェイスを信頼できないインターフェイスとして設定すると、接続が失われる場合があります。

図 39-2 では、スイッチ A とスイッチ B の両方が、ホスト 1 およびホスト 2 を収容する VLAN 上で DAI を実行していると仮定します。ホスト 1 とホスト 2 がスイッチ A に接続されている DHCP サーバから IP アドレスを取得すると、スイッチ A だけがホスト 1 の IP/MAC アドレスをバインドします。したがって、スイッチ A とスイッチ B 間のインターフェイスが信頼できない場合は、ホスト 1 からの ARP パケットはスイッチ B では廃棄されます。こうして、ホスト 1 とホスト 2 の間の接続が失われます。

図 39-2　DAI をイネーブルにした VLAN での ARP パケット検証



実際には信頼できないインターフェイスを信頼できるインターフェイスとして設定すると、ネットワーク内にセキュリティ ホールが生じます。スイッチ A が DAI を実行していなければ、ホスト 1 はスイッチ B（スイッチ間のリンクが信頼可能として設定されている場合はホスト 2 も同様）の ARP キャッシュを簡単にポイズニングできます。この状況は、スイッチ B が DAI を実行している場合でも起こりえます。

DAI は、DAI を実行するスイッチに接続された、信頼できないインターフェイス上のホストが、ネットワーク内の他のホストの ARP キャッシュをポイズニングしないように保証します。しかし、ネットワークのその他の場所にあるホストが、DAI を実行するスイッチに接続されたホストのキャッシュをポイズニングする可能性は防止できません。

VLAN 内の一部のスイッチが DAI を実行し、他のスイッチは DAI を実行していない状況では、これらのスイッチに接続されたインターフェイスを信頼できないインターフェイスとして設定します。ただし、DAI が設定されていないスイッチからのパケットのバインディングを検証するには、DAI を実行するスイッチ上で ARP ACL を設定します。こうしたバインディングを判断できない場合は、レイヤ 3 において、DAI を実行するスイッチを DAI を実行しないスイッチから切り離します。設定の詳細については、「例 2：1 つのスイッチが DAI をサポートする場合」（p.39-23）を参照してください。

（注）　DHCP サーバとネットワークのセットアップ方法によっては、VLAN 内のすべてのスイッチで、特定の ARP パケットを検証できない場合もあります。

ARP パケットのレート制限

スイッチは、DAI 有効性検査を実行することで着信 ARP パケットをレート制限して、DoS 攻撃を防止します。デフォルトでは、信頼できないインターフェイスのレートは 15 pps（パケット / 秒）です。信頼できるインターフェイスは、レート制限されません。この設定を変更するには、**ip arp inspection limit** インターフェイス コンフィギュレーション コマンドを使用します。

着信 ARP パケットのレートが、設定したレート制限を超えると、スイッチはこのポートを errdisable ステートに設定します。ユーザが介入するまで、ポートはこの状態を維持します。**errdisable recovery** グローバル コンフィギュレーション コマンドを使用すると、errdisable ステートの回復をイネーブルにできます。これによって、ポートは指定のタイムアウト期間が経過すると、この状態から自動的に回復するようになります。

設定の詳細については、「ARP パケットのレート制限の設定」（p.39-11）を参照してください。

ARP ACL および DHCP スヌーピング エントリの相対的なプライオリティ

DAI では DHCP スヌーピング バインディング データベースを使用して、有効な IP アドレスおよび MAC アドレスのバインディング一覧を維持します。

DHCP スヌーピング バインディング データベース内のエントリより、ARP ACL のほうが優先されます。ACL は、**ip arp inspection filter** グローバル コンフィギュレーション コマンドを使用してスイッチを設定している場合に限り、スイッチに適用されます。スイッチはまず、ARP パケットを、ユーザが設定した ARP ACL と照合します。ARP パケットが ARP ACL によって拒否される場合は、DHCP スヌーピングによって書き込まれた有効なバインディングがデータベース内に存在する場合であっても、スイッチはこのパケットを拒否します。

廃棄パケットのロギング

スイッチはパケットを廃棄すると、ログ バッファ内にエントリを作成して、レート制限に基づくシステム メッセージを生成します。メッセージが生成されたあとは、スイッチはこのエントリをログ バッファから消去します。各ログ エントリには、受信側の VLAN、ポート番号、送信元および宛先 IP アドレス、送信元および宛先 MAC アドレスといったフロー情報が記録されます。

ip arp inspection log-buffer グローバル コンフィギュレーション コマンドを使用すると、バッファ内のエントリ数や、システム メッセージ生成までの指定のインターバルに必要とされるエントリ数を設定できます。ログ記録されるパケットの種類を指定するには、**ip arp inspection vlan logging** グローバル コンフィギュレーション コマンドを使用します。設定の詳細については、「DAI ログ機能の設定」（p.39-14）を参照してください。

DAI のデフォルト設定

表 39-1 に、DAI のデフォルト設定を示します。

表 39-1　DAI のデフォルト設定

機能	デフォルト設定
DAI	すべての VLAN でディセーブル。
インターフェイスの信頼状態	すべてのインターフェイスは untrusted。
着信 ARP パケットのレート制限	信頼できないインターフェイスでは、レートを 15 pps に制限。ネットワークがレイヤ 2 スイッチド ネットワークであり、ホストが 1 秒間に 15 の新規ホストに接続することが前提です。 信頼できるすべてのインターフェイスでは、レート制限は行われません。 バースト インターバルは 1 秒です。
非 DHCP 環境に対する ARP ACL	ARP ACL は定義されません。
有効性検査	検査は実行されません。
ログ バッファ	DAI をイネーブルにした場合は、拒否または廃棄されたすべての ARP パケットがログ記録されます。 ログ内のエントリ数は 32 です。 システム メッセージ数は、毎秒 5 つに制限されます。 ロギング レート インターバルは 1 秒です。
VLAN 単位のロギング	拒否または廃棄されたすべての ARP パケットが記録されます。

DAI 設定時の注意事項および制約事項

DAI を設定する場合は、次の注意事項および制約事項に従ってください。

- DAI は入力セキュリティ機能であり、出力検査は行いません。
- DAI は、DAI をサポートしないスイッチ、またはこの機能がイネーブルにされていないスイッチに接続されたホストに対しては、効果がありません。man-in-the-middle 攻撃は 1 つのレイヤ 2 ブロードキャスト ドメインに限定されるため、DAI 検査が有効なドメインを、DAI 検査の行われないドメインから切り離します。これにより、DAI をイネーブルにしたドメイン内のホストの ARP キャッシュをセキュリティ保護できます。
- DAI では、受信する ARP 要求および ARP 応答内の IP および MAC アドレス バインディングを、DHCP スヌーピング バインディング データベース内のエントリに基づいて検証します。IP アドレスをダイナミックに割り当てられた ARP パケットを許可するには、DHCP スヌーピングをイネーブルにする必要があります。詳細については、第 38 章「DHCP スヌーピングの設定」を参照してください。
- DHCP スヌーピングをディセーブルにしている場合、または DHCP 以外の環境では、ARP ACL を使用してパケットの許可および拒否を行います。
- DAI は、アクセス ポート、トランク ポート、EtherChannel ポート、およびプライベート VLAN ポートでサポートされます。
- 物理ポートを EtherChannel ポート チャネルに結合するには、この物理ポートとチャネル ポートの信頼状態が一致する必要があります。そうでない物理ポートは、ポート チャネル内で中断状態のままとなります。ポート チャネルは、チャネルと結合された最初の物理ポートの信頼状態を継承します。したがって、最初の物理ポートの信頼状態は、チャネルの信頼状態と一致する必要はありません。

  逆に、ポート チャネルの信頼状態を変更すると、スイッチはチャネルを構成するすべての物理ポートに対し、新たにこの信頼状態を設定します。
- ポート チャネルの動作レートは、チャネル内のすべての物理ポートによる累積値です。たとえば、ポート チャネルの ARP レート制限を 400 pps に設定すると、このチャネルに結合されたすべてのインターフェイスは、合計で 400 pps を受信します。EtherChannel ポートで受信される ARP パケットのレートは、すべてのチャネル メンバーからの受信パケット レートの合計となります。EtherChannel ポートのレート制限は、各チャネル ポート メンバーが受信する ARP パケットのレートを確認してから設定してください。

  物理ポートで受信されるパケットのレートは、物理ポートの設定ではなく、ポート チャネルの設定に照合して検査されます。ポート チャネルのレート制限設定は、物理ポートの設定には依存しません。

  EtherChannel が、設定したレートより多くの ARP パケットを受信すると、このチャネル（すべての物理ポートを含む）は errdisable ステートとなります。
- 受信トランク ポートでは、ARP パケットを必ずレート制限してください。トランク ポートは、各ポートの集約値を考慮し、DAI をイネーブルにした複数の VLAN でパケットを処理できるように、高い値に設定します。また、**ip arp inspection limit none** インターフェイス コンフィギュレーション コマンドを使用すると、レートを無制限として設定できます。1 つの VLAN に高いレート制限値を設定すると、ソフトウェアによってこのポートが errdisable ステートにされた場合に、他の VLAN への DoS 攻撃を招く可能性があります。

DAI の設定

ここでは、DAI の設定手順について説明します。

VLAN での DAI のイネーブル化

VLAN で DAI 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# configure terminal`	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	`Router(config)# ip arp inspection vlan {vlan_ID | vlan_range}`	VLAN で DAI をイネーブルにします（デフォルトではディセーブル）。
	`Router(config)# no ip arp inspection vlan {vlan_ID | vlan_range}`	VLAN で DAI をディセーブルにします。
ステップ 3	`Router(config-if)# do show ip arp inspection vlan {vlan_ID | vlan_range} | begin Vlan`	設定を確認します。

DAI は 1 つの VLAN、または特定の VLAN 範囲でイネーブルにできます。

- 1 つの VLAN でイネーブルにするには、1 つの VLAN 番号を入力します。
- 特定の VLAN 範囲でイネーブルにするには、一組の VLAN 番号をダッシュ（-）でつなげて指定します。
- 複数の VLAN 番号をカンマで区切って入力することも、一組の VLAN 番号をダッシュでつなげて入力することもできます。

次に、VLAN 10 ～ 12 で DAI をイネーブルにする例を示します。

```
Router# configure terminal
Router(config)# ip arp inspection vlan 10-12
```

次に、VLAN 10 ～ 12 で DAI をイネーブルにするもう 1 つの方法を示します。

```
Router# configure terminal
Router(config)# ip arp inspection vlan 10,11,12
```

次に、VLAN 10 ～ 12、および VLAN 15 で DAI をイネーブルにする例を示します。

```
Router# configure terminal
Router(config)# ip arp inspection vlan 10-12,15
```

次に、設定を確認する例を示します。

```
Router(config)# do show ip arp inspection vlan 10-12,15 | begin Vlan
Vlan     Configuration    Operation   ACL Match          Static ACL
 ----     -------------    ---------   ---------          ----------
   10     Enabled          Inactive
   11     Enabled          Inactive
   12     Enabled          Inactive
   15     Enabled          Inactive

 Vlan     ACL Logging      DHCP Logging
 ----     -----------      ------------
   10     Deny             Deny
   11     Deny             Deny
   12     Deny             Deny
   15     Deny             Deny
```

DAI インターフェイスの信頼状態の設定

スイッチは、信頼できるインターフェイス上の他のスイッチから受信した ARP パケットは検査しません。この場合、パケットはそのまま転送されます。

信頼できないインターフェイスでは、スイッチはすべての ARP 要求および ARP 応答を代行受信します。スイッチは、代行受信した各パケットが、IP アドレスと MAC アドレスとの有効なバインディングを持つことを確認してから、ローカル キャッシュを更新するか、または適切な宛先にパケットを転送します。スイッチは無効なパケットを廃棄し、**ip arp inspection vlan logging** グローバル コンフィギュレーション コマンドで指定されたログ設定に基づき、ログ バッファに廃棄パケットを記録します。詳細については、「DAI ログ機能の設定」（p.39-14）を参照してください。

DAI インターフェイスの信頼状態を設定するには、次の作業を行います。

	コマンド	目的
ステップ 1	`Router# configure terminal`	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	`Router(config)# interface {`*type*[1] *slot/port* | **port-channel** *number*`}`	別のスイッチに接続されているインターフェイスを指定して、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	`Router(config-if)# ip arp inspection trust`	スイッチ間の接続を、trusted として設定します（デフォルトでは untrusted）。
	`Router(config)# no ip arp inspection trust`	スイッチ間の接続を、untrusted として設定します。
ステップ 4	`Router(config-if)# do show ip arp inspection interfaces`	DAI の設定を確認します。

1. *type* = **ethernet**、**fastethernet**、**gigabitethernet**、または **tengigabitethernet**

次に、ポート FastEthernet 5/12 を信頼できるポートとして設定する例を示します。

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# interface fastethernet 5/12
Router(config-if)# ip arp inspection trust
Router(config-if)# do show ip arp inspection interfaces | include Int|--|5/12
Interface        Trust State     Rate (pps)    Burst Interval
 ---------------  -----------     ----------    --------------
 Fa5/12           Trusted              None              N/A
```

DAI フィルタリングのための ARP ACL の適用

（注）　**arp access-list** コマンドの詳細については、『*Catalyst 6500 Series Switch Cisco IOS Command Reference*』Release 12.2SX を参照してください。

ARP ACL を適用するには、次の作業を行います。

	コマンド	目的
ステップ 1	`Router# configure terminal`	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	`Router# ip arp inspection filter arp_acl_name vlan {vlan_ID | vlan_range} [static]`	ARP ACL を VLAN に適用します。
ステップ 3	`Router(config)# do show ip arp inspection vlan {vlan_ID | vlan_range}`	設定を確認します。

ARP ACL を適用する場合は、次の点に注意してください。

- *vlan_range* には、1 つの VLAN、または特定の VLAN 範囲を指定できます。
  - 1 つの VLAN を指定するには、1 つの VLAN 番号を入力します。
  - 特定の VLAN 範囲を指定するには、一組の VLAN 番号をダッシュ（-）でつなげて指定します。
  - 複数の VLAN 番号をカンマで区切って入力することも、一組の VLAN 番号をダッシュでつなげて入力することもできます。
- （任意）**static** を指定すると、ARP ACL 内の暗黙的な拒否が明示的な拒否とみなされ、それ以前に指定された ACL 内のすべてのコマンドに一致しないパケットは廃棄されます。DHCP バインディングは使用されません。

  このキーワードを指定しない場合は、ACL 内にはパケットを拒否する明示的な拒否が存在しないことになります。この場合は、ACL 内のどのコマンドとも一致しないパケットを許可するか拒否するかは、DHCP バインディングによって決定されます。
- IP アドレスおよび MAC アドレスのバインディングしか持たない ARP パケットは、ACL に照合されます。パケットは、アクセス リストで許可された場合のみに許可されます。

次に、example_arp_acl という名前の ARP ACL を、VLAN 10 ～ 12、および VLAN 15 に適用する例を示します。

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# ip arp inspection filter example_arp_acl vlan 10-12,15
Router(config)# do show ip arp inspection vlan 10-12,15 | begin Vlan
 Vlan     Configuration    Operation   ACL Match          Static ACL
 ----     -------------    ---------   ---------          ----------
   10     Enabled          Inactive    example_arp_acl   No
   11     Enabled          Inactive    example_arp_acl   No
   12     Enabled          Inactive    example_arp_acl   No
   15     Enabled          Inactive    example_arp_acl   No

 Vlan     ACL Logging      DHCP Logging
 ----     -----------      ------------
   10     Deny             Deny
   11     Deny             Deny
   12     Deny             Deny
   15     Deny             Deny
```

ARP パケットのレート制限の設定

DAI をイネーブルにすると、スイッチは ARP パケットの有効性検査を実行します。これにより、スイッチは ARP パケットの DoS 攻撃を受けやすくなります。ARP パケットをレート制限することで、ARP パケットの DoS 攻撃を防止できます。

ARP パケットのレート制限をポートに設定するには、次の作業を行います。

	コマンド	目的
ステップ 1	`Router# configure terminal`	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	`Router(config)# interface {`*type*[1] *slot/port* `| port-channel` *number*`}`	設定するインターフェイスを選択します。
ステップ 3	`Router(config-if)# ip arp inspection limit {rate` *pps* `[burst interval` *seconds*`] | none}` `Router(config-if)# no ip arp inspection limit`	（任意）ARP パケットのレート制限を設定します。 ARP パケットのレート制限設定を解除します。
ステップ 4	`Router(config-if)# do show ip arp inspection interfaces`	設定を確認します。

1. *type* = **ethernet**、**fastethernet**、**gigabitethernet**、または **tengigabitethernet**

ARP パケットのレート制限を設定する場合は、次の点に注意してください。

- デフォルト レートは、信頼できないインターフェイスでは 15 pps、信頼できるインターフェイスでは無制限です。
- **rate** *pps* には、1 秒あたりに処理される着信パケット数の上限を指定します。有効な範囲は 0 ～ 2048 pps です。
- **rate none** キーワードは、処理できる着信 ARP パケットのレートに上限がないことを指定します。
- （任意）**burst interval** *seconds*（デフォルトは 1）には、インターフェイスをモニタして高レートの ARP パケットの有無を確認するための、連続するインターバルを秒単位で指定します。有効な範囲は 1 ～ 15 です。
- 着信　ARP　パケットのレートが、設定したレート制限を超えると、スイッチはこのポートを errdisable ステートに設定します。ポートは、errdisable ステートの回復がイネーブルにされるまで、errdisable ステートを維持します。errdisable ステートの回復をイネーブルにすると、指定のタイムアウト時間が経過した時点で、ポートは errdisable ステートから回復します。
- インターフェイスのレート制限値を設定しないかぎり、インターフェイスの信頼状態を変更すると、このレート制限値も、設定した信頼状態に対応するデフォルト値に変更されます。レート制限値を設定すると、信頼状態を変更した場合でも、インターフェイスはこのレート制限値を維持します。**no ip arp inspection limit** インターフェイス コンフィギュレーション コマンドを入力すると、インターフェイスはデフォルトのレート制限値に戻ります。
- トランク ポートおよび EtherChannel ポートで受信される ARP パケットのレート制限を設定する上での注意事項については、「DAI 設定時の注意事項および制約事項」（p.39-7）を参照してください。

次に、ポート FastEthernet 5/14 に ARP パケットのレート制限を設定する例を示します。

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# interface fastethernet 5/14
Router(config-if)# ip arp inspection limit rate 20 burst interval 2
Router(config-if)# do show ip arp inspection interfaces | include Int|--|5/14
 Interface        Trust State     Rate (pps)     Burst Interval
 ---------------  -----------     ----------     --------------
 Fa5/14           Untrusted               20                  2
```

DAI errdisable ステート回復のイネーブル化

DAI の errdisable ステート回復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# configure terminal`	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	`Router(config)# errdisable recovery cause arp-inspection`	（任意）DAI の errdisable ステート回復をイネーブルにします（デフォルトはディセーブル）。
	`Router(config-if)# no errdisable recovery cause arp-inspection`	DAI の errdisable ステート回復をディセーブルにします。
ステップ 3	`Router(config)# do show errdisable recovery | include Reason|---|arp-`	設定を確認します。

次の例は、DAI の errdisable ステート回復をイネーブルにします。

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# errdisable recovery cause arp-inspection
Router(config)# do show errdisable recovery | include Reason|---|arp-
ErrDisable Reason    Timer Status
-----------------    --------------
arp-inspection       Enabled
```

その他の検証のイネーブル化

DAI は、IP アドレスと MAC アドレスとの無効なバインディングを持つ ARP パケットを代行受信、ログ記録、および廃棄します。宛先 MAC アドレス、送信元および宛先 IP アドレス、送信元 MAC アドレスに対し、追加検証をイネーブルにすることができます。

追加検証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# configure terminal`	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	`Router(config)# ip arp inspection validate {[dst-mac] [ip] [src-mac]}`	（任意）追加検証をイネーブルにします（デフォルトはなし）。
	`Router(config)# no ip arp inspection validate {[dst-mac] [ip] [src-mac]}`	追加検証をディセーブルにします。
ステップ 3	`Router(config)# do show ip arp inspection | include abled$`	設定を確認します。

追加検証をイネーブルにする場合は、次の点に注意してください。

- 少なくとも 1 つのキーワードを指定する必要があります。
- 各 **ip arp inspection validate** コマンドは、それまでに指定したコマンドの設定を上書きします。**ip arp inspection validate** コマンドによって **src** および **dst mac** 検証をイネーブルにし、2 つめの **ip arp inspection validate** コマンドで IP 検証のみをイネーブルにした場合は、2 つめのコマンドの結果によって **src** および **dst mac** 検証がディセーブルになります。

- 次の追加検証を実行できます。
  - **dst-mac —** イーサネット ヘッダー内の宛先 MAC アドレスを、ARP 本体のターゲット MAC アドレスと比較して検査します。この検査は、ARP 応答に対して実行されます。イネーブルにすると、異なる MAC アドレスを持つパケットは無効パケットとして分類され、廃棄されます。
  - **ip —** ARP 本体を検査し、無効かつ予期されない IP アドレスの有無を確認します。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。送信元 IP アドレスはすべての ARP 要求および ARP 応答内で検査され、宛先 IP アドレスは ARP 応答内のみで検査されます。
  - **src-mac —** イーサネット ヘッダー内の送信元 MAC アドレスを、ARP 本体の送信元 MAC アドレスと比較して検査します。この検査は、ARP 要求および ARP 応答の両方に対して実行されます。イネーブルにすると、異なる MAC アドレスを持つパケットは無効パケットとして分類され、廃棄されます。

次に、src-mac 追加検証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 arp inspection validate src-mac
Router(config)# do show ip arp inspection | include abled$
Source Mac Validation      : Enabled
Destination Mac Validation : Disabled
IP Address Validation      : Disabled
```

次に、dst-mac 追加検証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 arp inspection validate dst-mac
Router(config)# do show ip arp inspection | include abled$
Source Mac Validation      : Disabled
Destination Mac Validation : Enabled
IP Address Validation      : Disabled
```

次に、ip 追加検証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 arp inspection validate ip
Router(config)# do show ip arp inspection | include abled$
Source Mac Validation      : Disabled
Destination Mac Validation : Disabled
IP Address Validation      : Enabled
```

次に、src-mac および dst-mac 追加検証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 arp inspection validate src-mac dst-mac
Router(config)# do show ip arp inspection | include abled$
Source Mac Validation      : Enabled
Destination Mac Validation : Enabled
IP Address Validation      : Disabled
```

次に、src-mac、dst-mac、および ip 追加検証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 arp inspection validate src-mac dst-mac ip
Router(config)# do show ip arp inspection | include abled$
Source Mac Validation      : Enabled
Destination Mac Validation : Enabled
IP Address Validation      : Enabled
```

DAI ログ機能の設定

ここでは DAI ログ機能について説明します。

DAI ログ機能の概要

DAI はパケットを廃棄すると、ログ バッファ内にエントリを作成して、レート制限に基づくシステム メッセージを生成します。メッセージが生成されたあとは、DAI はこのエントリをログ バッファから消去します。各ログ エントリには、受信側の VLAN、ポート番号、送信元および宛先 IP アドレス、送信元および宛先 MAC アドレスといったフロー情報が記録されます。

1 つのログ バッファ エントリによって、複数のパケットを表現できます。たとえば、同じ ARP パラメータを持つ同一 VLAN 上で、1 つのインターフェイスが多数のパケットを受信した場合は、DAI のログ バッファではこれらのパケットが 1 つのエントリとして結合され、このエントリに対して 1 つのシステム メッセージが生成されます。

ログ バッファでオーバーフローが生じた場合は、1 つのログ イベントがログ バッファ内に収まらなかったことを意味し、**show ip arp inspection log** イネーブル EXEC コマンドによる出力が影響を受けます。この場合は、パケット数と時間のみが表示され、あとはデータの代わりに 2 つのダッシュ（--）が表示されます。このエントリに対しては、その他の統計情報は表示されません。このようなエントリが表示された場合は、ログ バッファ内のエントリ数を増やすか、またはログ レートを高くしてください。

DAI のログ バッファ サイズの設定

DAI のログ バッファ サイズを設定するには、次の作業を行います。

	コマンド	目的
ステップ 1	`Router# configure terminal`	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	`Router(config)# ip arp inspection log-buffer entries` *number* `Router(config)# no ip arp inspection log-buffer entries`	DAI のログ バッファ サイズを設定します（有効範囲は 0 ～ 1024）。 デフォルトのバッファ サイズ（32）に戻します。
ステップ 3	`Router(config)# do show ip arp inspection log | include Size`	設定を確認します。

次に、DAI ログ バッファを 64 メッセージに設定する例を示します。

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# ip arp inspection log-buffer entries 64
Router(config)# do show ip arp inspection log | include Size
Total Log Buffer Size : 64
```

DAI のログ システム メッセージの設定

DAI のログ システム メッセージを設定するには、次の作業を行います。

	コマンド	目的
ステップ 1	`Router# configure terminal`	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	`Router(config)# ip arp inspection log-buffer logs` *number_of_messages* `interval` *length_in_seconds*	DAI のログ バッファ サイズを設定します。
	`Router(config)# no ip arp inspection log-buffer logs`	デフォルトのシステム メッセージ設定に戻します。
ステップ 3	`Router(config)# do show ip arp inspection log`	設定を確認します。

DAI のログ システム メッセージを設定する場合は、次の点に注意してください。

- **logs** *number_of_messages* の有効範囲は 0 ～ 1024 です（デフォルトは 5）。0 は、エントリはログ バッファ内に入力されますが、システム メッセージが生成されないことを意味します。
- **interval** *length_in_seconds* の有効範囲は 0 秒 ～ 86400 秒（1 日）です（デフォルトは 1）。0 は、システム メッセージがただちに生成されることを意味します。この場合、ログ バッファは常に空となります。インターバル値を 0 に設定すると、ログ値 0 は上書きされます。
- システム メッセージは、*length_in_seconds* 秒あたり *number_of_messages* 個の割合で送信されます。

次に、2 秒あたり 12 個のメッセージが送信されるように DAI のログ レートを設定する例を示します。

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# ip arp inspection log-buffer logs 12 interval 2
Router(config)# do show ip arp inspection log | include Syslog
Syslog rate : 12 entries per 2 seconds.
```

次に、60 秒あたり 20 個のメッセージが送信されるように DAI のログ レートを設定する例を示します。

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# ip arp inspection log-buffer logs 20 interval 60
Router(config)# do show ip arp inspection log | include Syslog
Syslog rate : 20 entries per 60 seconds.
```

DAI のログ フィルタリングの設定

DAI のログ フィルタリングを設定するには、次の作業を行います。

	コマンド	目的
ステップ 1	`Router# configure terminal`	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	`Router(config)# ip arp inspection vlan` *vlan_range* `logging {acl-match {matchlog | none} | dhcp-bindings {all | none | permit}}`	各 VLAN に対するログ フィルタリングを設定します。
ステップ 3	`Router(config)# do show running-config | include ip arp inspection vlan` *vlan_range*	設定を確認します。

DAI のログ フィルタリングを設定する場合は、次の点に注意してください。

- デフォルトでは、拒否されたすべてのパケットがログ記録されます。
- *vlan_range* には、1 つの VLAN、または特定の VLAN 範囲を指定できます。
  - 1 つの VLAN を指定するには、1 つの VLAN 番号を入力します。
  - 特定の VLAN 範囲を指定するには、一組の VLAN 番号をダッシュ（-）でつなげて指定します。
  - 複数の VLAN 番号をカンマで区切って入力することも、複数組の VLAN 番号をダッシュでつなげて入力することもできます。
- **acl-match matchlog —** DAI ACL の設定に基づきパケットをログ記録します。このコマンドに **matchlog** キーワードを指定して、さらに **permit** または **deny** ARP アクセス リスト設定コマンドに **log** キーワードを指定すると、ACL によって許可または拒否された ARP パケットがログ記録されます。
- **acl-match none —** ACL と一致したパケットをログ記録しません。
- **dhcp-bindings all —** DHCP バインディングと一致したすべてのパケットがログ記録されます。
- **dhcp-bindings none —** DHCP バインディングと一致したパケットはログ記録されません。
- **dhcp-bindings permit —** DHCP バインディングによって許可されたパケットがログ記録されます。

次の例は、VLAN 100 の DAI ログ フィルタリングを、ACL と一致したパケットをログ記録しないように設定する方法を示します。

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# ip arp inspection vlan 100 logging acl-match none
Router(config)# do show running-config | include ip arp inspection vlan 100
ip arp inspection vlan 100 logging acl-match none
```

DAI 情報の表示

DAI 情報を表示するには、表 39-2 に示す各イネーブル EXEC コマンドを使用します。

表 39-2　DAI 情報を表示するためのコマンド

コマンド	目的
show arp access-list [*acl_name*]	ARP ACL についての詳細情報を表示します。
show ip arp inspection interfaces [*interface_id*]	指定のインターフェイス、またはすべてのインターフェイスに対して、ARP パケットの信頼状態およびレート制限を表示します。
show ip arp inspection vlan *vlan_range*	指定の VLAN に対し、DAI の設定内容および動作状態を表示します。VLAN を指定しない場合、または VLAN を範囲で指定した場合は、DAI がイネーブル（アクティブ）にされている VLAN のみの情報が表示されます。

DAI 統計情報を消去または表示するには、表 39-3 に示す各イネーブル EXEC コマンドを使用します。

表 39-3　DAI 統計情報を消去または表示するためのコマンド

コマンド	目的
clear ip arp inspection statistics	DAI 統計情報を消去します。
show ip arp inspection statistics [**vlan** *vlan_range*]	指定の VLAN において、転送されたパケット、廃棄されたパケット、MAC 検証に失敗したパケット、IP 検証に失敗したパケット、ACL によって許可または拒否されたパケット、DHCP によって許可または拒否されたパケットの統計情報を表示します。VLAN を指定しない場合、または VLAN を範囲で指定した場合は、DAI がイネーブル（アクティブ）にされている VLAN のみの情報が表示されます。

show ip arp inspection statistics コマンドでは、スイッチは信頼できる DAI ポートにおいて、個々の ARP 要求および応答パケットに対して転送されたパケット数を増分します。スイッチは送信元 MAC、宛先 MAC、または IP 検証の結果拒否された各パケットに対し、ACL によって許可されたパケット、または DHCP によって許可されたパケットの数を増分します。また、該当する失敗回数の値も増分します。スイッチ

DAI ログ情報を消去または表示するには、表 39-4 に示す各イネーブル EXEC コマンドを使用します。

表 39-4　DAI ログ情報を消去または表示するためのコマンド

コマンド	目的
clear ip arp inspection log	DAI のログ バッファを消去します。
show ip arp inspection log	DAI ログ バッファの設定および内容を表示します。

DAI の設定例

ここでは、次の例について説明します。

例 1：2 つのスイッチが DAI をサポートする場合

この手順は、2 つのスイッチが DAI 機能をサポートする場合の DAI の設定方法を示します。図 39-2 に示すように、ホスト 1 はスイッチ A に、ホスト 2 はスイッチ B にそれぞれ接続されています。両方のスイッチは、各ホストが属する VLAN 1 上で DAI を実行しています。DHCP サーバはスイッチ A に接続されています。両方のホストは、同一の DHCP サーバから IP アドレスを取得します。スイッチ A はホスト 1 およびホスト 2 のバインディングを持ち、スイッチ B はホスト 2 のバインディングを持ちます。スイッチ A のポート Fast Ethernet 6/3 は、スイッチ B のポート Fast Ethernet 3/3 に接続されています。

（注）

- DAI では、受信する ARP 要求および ARP 応答内の IP および MAC アドレス バインディングを、DHCP スヌーピング バインディング データベース内のエントリに基づいて検証します。IP アドレスをダイナミックに割り当てられた ARP パケットを許可するには、DHCP スヌーピングをイネーブルにする必要があります。詳細については、第 38 章「DHCP スヌーピングの設定」を参照してください。
- この構成は、DHCP サーバがスイッチ A から別の場所に移動されてしまうと機能しません。
- この構成によってセキュリティが損なわれないようにするには、スイッチ A のポート Fast Ethernet 6/3、およびスイッチ B のポート Fast Ethernet 3/3 を、信頼できるポートとして設定します。

スイッチ A の設定

スイッチ A において DAI をイネーブルにし、ポート Fast Ethernet 6/3 を信頼できるポートとして設定するには、次の作業を行います。

ステップ 1　スイッチ A およびスイッチ B 間の接続を確認します。

```
SwitchA# show cdp neighbors
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater, P - Phone

Device ID        Local Intrfce     Holdtme    Capability  Platform  Port ID
SwitchB          Fas 6/3            177         R S I     WS-C6506  Fas 3/3
SwitchA#
```

ステップ 2　VLAN 1 で DAI をイネーブルにし、設定を確認します。

```
SwitchA# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
SwitchA(config)# ip arp inspection vlan 1
SwitchA(config)# end
SwitchA# show ip arp inspection vlan 1

Source Mac Validation      : Disabled
Destination Mac Validation : Disabled
IP Address Validation      : Disabled

 Vlan     Configuration    Operation   ACL Match          Static ACL
 ----     -------------    ---------   ---------          ----------
    1     Enabled          Active

 Vlan     ACL Logging      DHCP Logging
 ----     -----------      ------------
    1     Deny             Deny
SwitchA#
```

ステップ 3　ポート Fast Ethernet 6/3 を、信頼できるポートとして設定します。

```
SwitchA# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
SwitchA(config)# interface fastethernet 6/3
SwitchA(config-if)# ip arp inspection trust
SwitchA(config-if)# end
SwitchA# show ip arp inspection interfaces fastethernet 6/3

Interface        Trust State     Rate (pps)
 ---------------  -----------     ----------
 Fa6/3            Trusted              None
SwitchA#
```

ステップ 4　バインディングを確認します。

```
SwitchA# show ip dhcp snooping binding
MacAddress          IpAddress        Lease(sec)  Type           VLAN  Interface
------------------  ---------------  ----------  -------------  ----
--------------------
00:02:00:02:00:02   1.1.1.2          4993        dhcp-snooping  1     FastEthernet6/4
SwitchA#
```

ステップ 5　DAI がパケットを処理する前、およびあとの統計情報を調べます。

```
SwitchA# show ip arp inspection statistics vlan 1

Vlan      Forwarded        Dropped     DHCP Drops     ACL Drops
 ----      ---------        -------     ----------     ----------
    1              0              0              0              0

 Vlan   DHCP Permits    ACL Permits   Source MAC Failures
 ----   ------------    -----------   -------------------
    1              0              0                     0

 Vlan   Dest MAC Failures   IP Validation Failures
 ----   -----------------   ----------------------
    1                  0                       0
SwitchA#
```

このあと、ホスト 1 が IP アドレス 1.1.1.2 および MAC アドレス 0002.0002.0002 を持つ 2 つの ARP 要求を送信すると、両方の要求が許可されます。これは、次の統計情報で確認できます。

```
SwitchA# show ip arp inspection statistics vlan 1

 Vlan      Forwarded        Dropped     DHCP Drops     ACL Drops
 ----      ---------        -------     ----------     ----------
    1              2              0              0              0

 Vlan   DHCP Permits    ACL Permits   Source MAC Failures
 ----   ------------    -----------   -------------------
    1              2              0                     0

 Vlan   Dest MAC Failures   IP Validation Failures
 ----   -----------------   ----------------------
    1                  0                        0
SwitchA#
```

ホスト 1 がこのあと、IP アドレス 1.1.1.3 を持つ ARP 要求を送信しようとすると、このパケットは廃棄され、エラー メッセージがログ記録されます。

```
00:12:08: %SW_DAI-4-DHCP_SNOOPING_DENY: 2 Invalid ARPs (Req) on Fa6/4, vlan
1.([0002.0002.0002/1.1.1.3/0000.0000.0000/0.0.0.0/02:42:35 UTC Tue Jul 10 2001])
SwitchA# show ip arp inspection statistics vlan 1
SwitchA#
```

この場合に表示される統計情報は次のようになります。

```
Vlan      Forwarded        Dropped     DHCP Drops     ACL Drops
 ----      ---------        -------     ----------     ----------
    1              2              2              2              0

 Vlan   DHCP Permits    ACL Permits   Source MAC Failures
 ----   ------------    -----------   -------------------
    1              2              0                     0

 Vlan   Dest MAC Failures   IP Validation Failures
 ----   -----------------   ----------------------
    1                  0                        0
SwitchA#
```

スイッチ B の設定

スイッチ B において DAI をイネーブルにし、ポート Fast Ethernet 3/3 を信頼できるポートとして設定するには、次の作業を行います。

ステップ 1　接続を確認します。

```
SwitchA# show cdp neighbors
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater, P - Phone

Device ID        Local Intrfce     Holdtme    Capability  Platform  Port ID
SwitchB          Fas 3/3            120         R S I     WS-C6506  Fas 6/3
SwitchB#
```

ステップ 2　VLAN 1 で DAI をイネーブルにし、設定を確認します。

```
SwitchB# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
SwitchB(config)# ip arp inspection vlan 1
SwitchB(config)# end
SwitchB# show ip arp inspection vlan 1

Source Mac Validation      : Disabled
Destination Mac Validation : Disabled
IP Address Validation      : Disabled

 Vlan     Configuration    Operation   ACL Match          Static ACL
 ----     -------------    ---------   ---------          ----------
    1     Enabled          Active

 Vlan     ACL Logging      DHCP Logging
 ----     -----------      ------------
    1     Deny             Deny
SwitchB#
```

ステップ 3　ポート Fast Ethernet 3/3 を、信頼できるポートとして設定します。

```
SwitchB# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
SwitchB(config)# interface fastethernet 3/3
SwitchB(config-if)# ip arp inspection trust
SwitchB(config-if)# end
SwitchB# show ip arp inspection interfaces

Interface        Trust State     Rate (pps)
 ---------------  -----------     ----------
 Gi1/1            Untrusted              15
 Gi1/2            Untrusted              15
 Gi3/1            Untrusted              15
 Gi3/2            Untrusted              15
 Fa3/3            Trusted               None
 Fa3/4            Untrusted              15
 Fa3/5            Untrusted              15
 Fa3/6            Untrusted              15
 Fa3/7            Untrusted              15

(テキスト出力は省略)
SwitchB#
```

ステップ 4　DHCP スヌーピング バインディングのリストを確認します。

```
SwitchB# show ip dhcp snooping binding
MacAddress          IpAddress        Lease(sec)  Type           VLAN  Interface
------------------  ---------------  ----------  -------------  ----
--------------------
00:01:00:01:00:01   1.1.1.1          4995        dhcp-snooping  1     FastEthernet3/4
SwitchB#
```

ステップ 5　DAI がパケットを処理する前、および後の統計情報を調べます。

```
SwitchB# show ip arp inspection statistics vlan 1

Vlan      Forwarded        Dropped     DHCP Drops     ACL Drops
 ----      ---------        -------     ----------     ----------
    1              0              0              0              0

 Vlan   DHCP Permits    ACL Permits   Source MAC Failures
 ----   ------------    -----------   -------------------
    1              0              0                    0

 Vlan   Dest MAC Failures   IP Validation Failures
 ----   -----------------   ----------------------
    1                  0                        0
SwitchB#
```

ホスト 2 がこのあと、IP アドレス 1.1.1.1 および MAC アドレス 0001.0001.0001 を持つ ARP 要求を送信すると、このパケットは転送され、統計情報も適切に更新されます。

```
SwitchB# show ip arp inspection statistics vlan 1

Vlan      Forwarded        Dropped     DHCP Drops     ACL Drops
 ----      ---------        -------     ----------     ----------
    1              1              0              0              0

 Vlan   DHCP Permits    ACL Permits   Source MAC Failures
 ----   ------------    -----------   -------------------
    1              1              0                    0

 Vlan   Dest MAC Failures   IP Validation Failures
 ----   -----------------   ----------------------
    1                  0                        0
SwitchB#
```

ホスト 2 が IP アドレス 1.1.1.2 を持つ ARP 要求を送信しようとすると、この要求は廃棄され、システム メッセージがログ記録されます。

```
00:18:08: %SW_DAI-4-DHCP_SNOOPING_DENY: 1 Invalid ARPs (Req) on Fa3/4, vlan
1.([0001.0001.0001/1.1.1.2/0000.0000.0000/0.0.0.0/01:53:21 UTC Fri May 23 2003])
SwitchB#
```

この場合に表示される統計情報は次のようになります。

```
SwitchB# show ip arp inspection statistics vlan 1

Vlan      Forwarded        Dropped     DHCP Drops     ACL Drops
 ----      ---------        -------     ----------     ----------
    1              1              1              1              0

 Vlan   DHCP Permits    ACL Permits   Source MAC Failures
 ----   ------------    -----------   -------------------
    1              1              0                    0

 Vlan   Dest MAC Failures   IP Validation Failures
 ----   -----------------   ----------------------
    1                  0                        0
SwitchB#
```

例 2：1 つのスイッチが DAI をサポートする場合

この手順では、図 39-2 に示すスイッチ B が、DAI および DHCP スヌーピングをサポートしていない場合に DAI を設定する方法を示します。

スイッチ B が DAI および DHCP スヌーピングをサポートしていない場合は、スイッチ A のポート Fast Ethernet 6/3 を信頼できるポートとして設定すると、セキュリティ ホールが生じます。これは、スイッチ A およびホスト 1 が、スイッチ B またはホスト 2 によって攻撃される可能性があるためです。

この可能性を排除するには、スイッチ A のポート Fast Ethernet 6/3 を信頼できないポートとして設定する必要があります。ホスト 2 からの ARP パケットを許可するには、ARP ACL をセットアップして、これを VLAN 1 に適用する必要があります。ホスト 2 の IP アドレスがスタティックではない場合は、スイッチ A に ACL 設定を適用できなくなるため、レイヤ 3 でスイッチ B からスイッチ A を切り離す必要があります。これらのスイッチ間では、ルータを使用してパケットをルーティングします。

スイッチ A に対して ARP ACL をセットアップするには、次の作業を行います。

ステップ 1　IP アドレス 1.1.1.1 および MAC アドレス 0001.0001.0001 を許可するアクセス リストを設定して、設定内容を確認します。

```
SwitchA# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
SwitchA(config)# arp access-list H2
SwitchA(config-arp-nacl)# permit ip host 1.1.1.1 mac host 1.1.1
SwitchA(config-arp-nacl)# end
SwitchA# show arp access-list
ARP access list H2
    permit ip host 1.1.1.1 mac host 0001.0001.0001
```

ステップ 2　VLAN 1 に ACL を適用して、設定を確認します。

```
SwitchA# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
SwitchA(config)# ip arp inspection filter H2 vlan 1
SwitchA(config)# end
SwitchA#

SwitchA# show ip arp inspection vlan 1

Source Mac Validation      : Disabled
Destination Mac Validation : Disabled
IP Address Validation      : Disabled

 Vlan     Configuration    Operation   ACL Match          Static ACL
 ----     -------------    ---------   ---------          ----------
    1     Enabled          Active      H2                 No

 Vlan     ACL Logging      DHCP Logging
 ----     -----------      ------------
    1     Deny             Deny
SwitchA#
```

ステップ 3　ポート Fast Ethernet 6/3 を信頼できないポートとして設定し、設定内容を確認します。

```
SwitchA# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
SwitchA(config)# interface fastethernet 6/3
SwitchA(config-if)# no ip arp inspection trust
SwitchA(config-if)# end
Switch# show ip arp inspection interfaces fastethernet 6/3

 Interface        Trust State     Rate (pps)
 ---------------  -----------     ----------
 Fa6/3            Untrusted               15

Switch#
```

ホスト 2 がスイッチ A のポート Fast Ethernet 6/3 から 5 つの ARP 要求を送信し、1 つの get 要求がスイッチ A によって許可された場合は、統計情報は次のように適切に更新されます。

```
Switch# show ip arp inspection statistics vlan 1
Vlan      Forwarded        Dropped     DHCP Drops     ACL Drops
 ----      ---------        -------     ----------     ----------
    1              5              0              0              0
Vlan   DHCP Permits    ACL Permits   Source MAC Failures
 ----   ------------    -----------   -------------------
    1              0              5                    0
Vlan   Dest MAC Failures   IP Validation Failures
 ----   -----------------   ----------------------
    1                  0                       0
Switch#
```