CHAPTER 27

ダイナミック ARP 検査の設定

この章では、IE 3000 スイッチに Dynamic Address Resolution Protocol（ARP; アドレス解決プロトコル）Inspection（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。この機能は、スイッチに対する悪意ある攻撃を防ぐため、無効な ARP 要求および ARP 応答が、同じ VLAN 内の他のポートにリレーされないようにします。

（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、このリリースのコマンド リファレンスを参照してください。

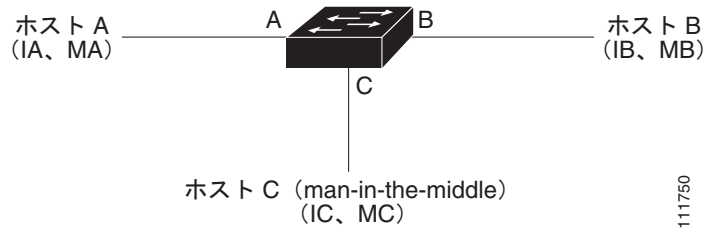
この章で説明する内容は、次のとおりです。

ダイナミック ARP 検査の概要

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 ドメイン内のすべての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 ドメイン内のすべてのホストがこの 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。ただし、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、ARP スプーフィング攻撃や ARP キャッシュのポイズニングが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。

悪意あるユーザは、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できます。図 27-1 に、ARP キャッシュ ポイズニングの例を示します。

図 27-1　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 で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 の IP アドレスは IA、MAC アドレスは MA です。ホスト A が IP レイヤ上でホスト B と通信する必要がある場合、ホスト A は、IP アドレス IB に関連付けられた MAC アドレスに対する 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 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 が 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、典型的な *man-in-the-middle* 攻撃です。

ダイナミック ARP 検査は、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。この機能は、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。

ダイナミック ARP 検査を使用することで、有効な ARP 要求および ARP 応答だけがリレーされるようにできます。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 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。

ダイナミック ARP 検査は、信頼できるデータベースに保存された IP アドレスと MAC アドレスとの有効な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 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、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だけを転送します。

ダイナミック ARP 検査を VLAN 単位でイネーブルにするには、**ip arp inspection vlan** *vlan-range* 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、「DHCP 環境におけるダイナミック ARP 検査の設定」（P.27-7）を参照してください。

非 DHCP 環境におけるダイナミック ARP 検査では、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 ARP 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。ARP ACL を定義するには、**arp access-list** *acl-name* 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、「非 DHCP 環境に対する ARP ACL の設定」（P.27-9）を参照してください。スイッチは、廃棄されたパケットをログ記録します。ログ バッファの詳細については、「廃棄パケットのロギング」（P.27-5）を参照してください。

ダイナミック ARP 検査では、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。**ip arp inspection validate** {[**src-mac**] [**dst-mac**] [**ip**]} 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ください。詳細については、「有効性検査の実行」（P.27-12）を参照してください。

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

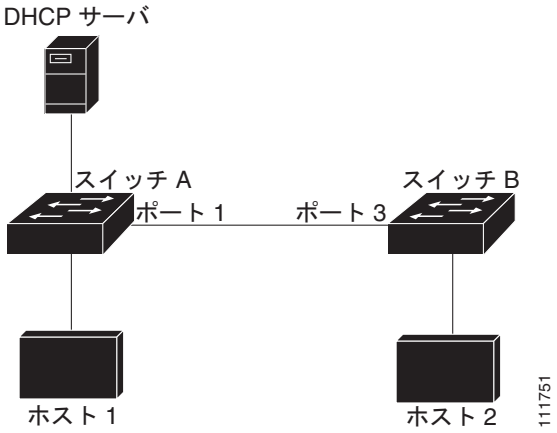
ダイナミック ARP 検査は、スイッチの各インターフェイスに信頼状態を関連付けます。信頼できるインターフェイス上で受信されたパケットは、ダイナミック ARP 検査のすべての有効性検査をバイパスしますが、信頼できないインターフェイス上で受信されたパケットには、ダイナミック ARP 検査の有効性検査が行われます。

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 ポートを信頼できるポートとして設定します。この設定では、指定の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 27-2 では、スイッチ A とスイッチ B の両方が、ホスト 1 とホスト 2 が属する VLAN 上でダイナミック ARP 検査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 アドレスと 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 の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 27-2　ダイナミック ARP 検査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 がダイナミック ARP 検査を実行していなければ、ホスト 1 は（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）、スイッチ B 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 がダイナミック ARP 検査を実行している場合でも起こりえます。

ダイナミック ARP 検査は、ダイナミック ARP 検査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、ダイナミック ARP 検査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。

ダイナミック ARP 検査を実行するスイッチと実行しないスイッチが VLAN 内にある場合は、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、ダイナミック ARP 検査を実行し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、ダイナミック ARP 検査を実行するスイッチに 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、ダイナミック ARP 検査を実行するスイッチ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、「非 DHCP 環境に対する ARP ACL の設定」（P.27-9）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、指定の 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

スイッチの CPU は、ダイナミック ARP 検査の有効性を確認することによって、着信 ARP パケット数をレート制限し、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 ステート回復をイネーブルにするには、**errdisable recovery** グローバル コンフィギュレーション コマンドを使用します。これによって、ポートは指定のタイムアウト時間が経過すると、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、「着信 ARP パケットのレート制限」（P.27-11）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

ダイナミック ARP 検査では、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、IP アドレスと MAC アドレスとの有効なバインディングのリストを維持します。

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 vlan** 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。メッセージの生成後、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。

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するには、**ip arp inspection log-buffer** グローバル コンフィギュレーション コマンドを使用します。ログ記録されるパケットのタイプを指定するには、**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、「ログ バッファの設定」（P.27-13）を参照してください。

ダイナミック ARP 検査の設定

ここでは、次の設定情報について説明します。

ダイナミック ARP 検査のデフォルト設定

表 27-1 に、ダイナミック ARP 検査のデフォルト設定を示します。

表 27-1　ダイナミック ARP 検査のデフォルト設定

機能	デフォルト設定
ダイナミック ARP インスペクション	すべての VLAN でディセーブルです。
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信頼できない状態です。

表 27-1　ダイナミック ARP 検査のデフォルト設定 （続き）

機能	デフォルト設定
着信 ARP パケットのレート制限	このレートは、信頼できないインターフェイス上で 15 pps に設定されています。ただし、1 台のホストが 1 秒間に 15 台の新規ホストに接続できるスイッチド ネットワークであると仮定しています。 信頼できるすべてのインターフェイスでは、レートは無制限です。 バースト インターバルは 1 秒に設定されています。
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	どの検証も実行されません。
ログ バッファ	ダイナミック ARP 検査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 メッセージの数は 1 秒あたり 5 つに制限されています。 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 パケットがログ記録されます。

ダイナミック ARP 検査設定時の注意事項

ダイナミック ARP 検査設定時の注意事項を次に示します。

- ダイナミック ARP 検査は入力セキュリティ機能であり、出力検査は行いません。
- ダイナミック ARP 検査は、ダイナミック ARP 検査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、ダイナミック ARP 検査が有効なドメインを、ダイナミック ARP 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、ダイナミック ARP 検査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。
- ダイナミック ARP 検査では、受信する ARP 要求および ARP 応答内の IP と MAC アドレス とのバインディングを、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 アドレスが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。設定の詳細については、第 26 章「DHCP 機能と IP ソース ガード機能の設定」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。
- ダイナミック ARP 検査は、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 ポート上でサポートされています。

（注）　RSPAN VLAN 上では、ダイナミック ARP 検査をイネーブルにしないでください。RSPAN VLAN 上でダイナミック ARP 検査をイネーブルにすると、ダイナミック ARP 検査パケットが RSPAN 宛先ポートに到達しないことがあります。

- 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、ダイナミック ARP 検査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。

- スイッチ上でダイナミック ARP 検査をイネーブルにすると、ARP トラフィックに対して設定されていたポリサーは効力を失います。その結果、すべての ARP トラフィックが CPU に送信されるようになります。

DHCP 環境におけるダイナミック ARP 検査の設定

この手順は、2 つのスイッチがダイナミック ARP 検査機能をサポートする場合の設定方法を示します。図 27-2（P.27-4）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 上でダイナミック ARP 検査を実行しています。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、同じ DHCP サーバから IP アドレスを取得します。したがって、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。

（注） ダイナミック ARP 検査では、受信する ARP 要求および ARP 応答内の IP と MAC アドレス とのバインディングを、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 アドレスが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。設定の詳細については、第 26 章「DHCP 機能と IP ソース ガード機能の設定」を参照してください。

1 台のスイッチだけがダイナミック ARP 検査機能をサポートしている場合の設定方法については、「非 DHCP 環境に対する ARP ACL の設定」（P.27-9）を参照してください。

ダイナミック ARP 検査を設定するには、特権 EXEC モードで次の手順を実行します。両方のスイッチでこの手順を実行する必要があります。この手順は必須です。

	コマンド	目的
ステップ 1	**show cdp neighbors**	スイッチ間の接続を確認します。
ステップ 2	**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 3	**ip arp inspection *vlan*** *vlan-range*	VLAN 単位でダイナミック ARP 検査をイネーブルにします。デフォルトでは、すべての VLAN 上でダイナミック ARP 検査がディセーブルになっています。 *vlan-range* には、VLAN ID 番号で識別された単一の VLAN、ハイフンで区切られた VLAN 範囲、またはカンマで区切られた一連の VLAN を指定できます。指定できる範囲は 1 ～ 4094 です。 両方のスイッチに対して同じ VLAN ID を指定します。
ステップ 4	**interface** *interface-id*	別のスイッチに接続されたインターフェイスを指定し、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 5	**ip arp inspection trust**	スイッチ間の接続を、信頼できる接続として設定します。 デフォルトでは、すべてのインターフェイスは信頼できない状態です。 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の場合、スイッチはすべての ARP 要求と ARP 応答を代行受信します。ローカル キャッシュを更新し、該当する宛先にパケットを転送する前に、代行受信したパケットが有効な IP/MAC アドレス バインディングを持つかどうかを検証します。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ギング設定に従ってログ バッファに記録します。詳細については、「ログ バッファの設定」（P.27-13）を参照してください。
ステップ 6	**end**	特権 EXEC モードに戻ります。
ステップ 7	**show ip arp inspection interfaces** **show ip arp inspection vlan** *vlan-range*	ダイナミック ARP 検査の設定を確認します。
ステップ 8	**show ip dhcp snooping binding**	DHCP バインディングを確認します。
ステップ 9	**show ip arp inspection statistics vlan** *vlan-range*	ダイナミック ARP 検査の統計情報を確認します。
ステップ 10	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

ダイナミック ARP 検査をディセーブルにするには、**no ip arp inspection vlan** *vlan-range* 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。インターフェイスを信頼できない状態に戻すには、**no 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。

次に、VLAN 1 内のスイッチ A にダイナミック ARP 検査を設定する例を示します。スイッチ B にも同様の手順を実行します。

```
Switch(config)# ip arp inspection vlan 1
Switch(config)# interface gigabitethernet1/1
Switch(config-if)# ip arp inspection trust
```

非 DHCP 環境に対する ARP ACL の設定

この手順では、図 27-2（P.27-4）に示すスイッチ B がダイナミック ARP 検査および DHCP スヌーピングをサポートしていない場合の、ダイナミック ARP 検査の設定方法を示します。

スイッチ A のポート 1 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 1 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 を設定して 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 ARP ACL を設定するには、特権 EXEC モードで次の手順を実行します。この手順は、非 DHCP 環境では必須です。

	コマンド	目的
ステップ 1	**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	**arp access-list** *acl-name*	ARP ACL を定義し、ARP アクセスリスト コンフィギュレーション モードを開始します。デフォルトでは、ARP アクセスリストは定義されていません。 **（注）** ARP アクセス リストの末尾には、暗黙的な **deny ip any mac any** コマンドが指定されています。
ステップ 3	**permit ip host** *sender-ip* **mac host** *sender-mac* [**log**]	指定したホスト（ホスト 2）からの ARP パケットを許可します。 • *sender-ip* には、ホスト 2 の IP アドレスを入力します。 • *sender-mac* には、ホスト 2 の MAC アドレスを入力します。 • （任意）Access Control Entry（ACE; アクセス制御エントリ）と一致したパケットをログ バッファに記録するには、**log** を指定します。**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 **matchlog** キーワードを設定している場合も、一致したパケットがログ記録されます。詳細については、「ログ バッファの設定」（P.27-13）を参照してください。
ステップ 4	**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。

	コマンド	目的
ステップ 5	**ip arp inspection filter** *arp-acl-name* **vlan** *vlan-range* [**static**]	ARP ACL を VLAN に適用します。デフォルトでは、VLAN に適用される ARP ACL は定義されていません。 • *arp-acl-name* には、ステップ 2 で作成した ACL の名前を指定します。 • *vlan-range* には、スイッチとホストが属する VLAN を指定します。VLAN ID 番号で識別された 1 つの VLAN、それぞれをハイフンで区切った VLAN 範囲、またはカンマで区切った一連の VLAN を指定できます。指定できる範囲は 1 ～ 4094 です。 • （任意）ARP ACL 内の暗黙の拒否を明示的な拒否として取り扱い、ACL 内の前の句に一致しないパケットを廃棄するために、**static** を指定します。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、パケットを拒否する明示的な拒否が ACL 内にないことを意味し、パケットが ACL 内の句に一致しないと DHCP バインディングがパケットの許可または拒否を決定します。 IP アドレスと MAC アドレスと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にだけ許可されます。
ステップ 6	**interface** *interface-id*	スイッチ B に接続されているスイッチ A のインターフェイスを指定し、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 7	**no ip arp inspection trust**	スイッチ B に接続されているスイッチ A の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。 デフォルトでは、すべてのインターフェイスは信頼できない状態です。 信頼できないインターフェイスの場合、スイッチはすべての ARP 要求と ARP 応答を代行受信します。ローカル キャッシュを更新し、該当する宛先にパケットを転送する前に、代行受信したパケットが有効な IP/MAC アドレス バインディングを持つかどうかを検証します。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ギング設定に従ってログ バッファに記録します。詳細については、「ログ バッファの設定」（P.27-13）を参照してください。
ステップ 8	**end**	特権 EXEC モードに戻ります。
ステップ 9	**show arp access-list** [*acl-name*] **show ip arp inspection vlan** *vlan-range* **show ip arp inspection interfaces**	設定を確認します。
ステップ 10	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

ARP ACL を削除するには、**no arp access-list** 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。VLAN に関連付けられた ARP ACL を削除するには、**no ip arp inspection filter** *arp-acl-name* **vlan** *vlan-range* 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。

次に、スイッチ A に *host2* という ARP ACL を設定し、ホスト 2（IP アドレス 1.1.1.1、MAC アドレス 0001.0001.0001）からの ARP パケットを許可し、ACL を VLAN 1 に適用し、スイッチ A のポート 1 を信頼できないポートとして設定する例を示します。

```
Switch(config)# arp access-list host2
Switch(config-arp-acl)# permit ip host 1.1.1.1 mac host 1.1.1
Switch(config-arp-acl)# exit
Switch(config)# ip arp inspection filter host2 vlan 1
Switch(config)# interface gigabitethernet1/1
Switch(config-if)# no ip arp inspection trust
```

着信 ARP パケットのレート制限

スイッチの CPU は、ダイナミック ARP 検査の有効性を確認することによって、着信 ARP パケット数をレート制限し、DoS 攻撃を防止します。

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。ポートは、errdisable ステート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、ポートは自動的にこのステートから回復します。

（注）　インターフェイス上のレート制限を設定しない限り、インターフェイスの信頼状態を変更すると、レート制限も信頼状態のデフォルト値に変更されます。レート制限を設定すると、インターフェイスはその信頼状態が変更された場合でも設定されたレート制限を維持します。**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に戻ります。

トランク ポートおよび EtherChannel ポートのレート制限設定時の注意事項については、「ダイナミック ARP 検査設定時の注意事項」（P.27-6）を参照してください。

着信 ARP パケットのレートを制限するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	**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	**interface** *interface-id*	レート制限するインターフェイスを指定し、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。

	コマンド	目的
ステップ 3	**ip arp inspection limit** {**rate** *pps* [**burst interval** *seconds*] | **none**}	インターフェイスに着信する ARP 要求および ARP 応答のレートを制限します。 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。バースト インターバルは 1 秒に設定されています。 キーワードの意味は次のとおりです。 • **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。指定できる範囲は 0 ～ 2048 pps です。 • （任意）**burst interval** *seconds* には、レートの高い ARP パケットの有無についてインターフェイスをモニタする間隔（秒）を指定します。指定できる範囲は 1 ～ 15 です。 • **rate none** の場合は、処理できる着信 ARP パケットのレートの上限を指定しません。
ステップ 4	**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 5	**errdisable recovery cause arp-inspection interval** *interval*	（任意）ダイナミック ARP 検査の errdisable ステートからの回復をイネーブルにします。 デフォルトでは、回復はディセーブルに、回復間隔は 300 秒に設定されています。 **interval** *interval* には、errdisable ステートから回復する時間を秒単位で指定します。指定できる範囲は 30 ～ 86400 です。
ステップ 6	**exit**	特権 EXEC モードに戻ります。
ステップ 7	**show ip arp inspection interfaces** **show errdisable recovery**	設定を確認します。
ステップ 8	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

デフォルトのレート制限設定に戻すには、**no ip arp inspection limit** インターフェイス コンフィギュレーション コマンドを使用します。ダイナミック ARP 検査のエラー回復をディセーブルにするには、**no errdisable recovery cause arp-inspection** 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。

有効性検査の実行

ダイナミック ARP 検査は、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、送信元と宛先の IP アドレス、および送信元 MAC アドレスに対する追加の検査を実行するように、スイッチを設定できます。

着信 ARP パケットに特定の検査を実行するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	**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	**ip arp inspection validate** {[**src-mac**] [**dst-mac**] [**ip**]}	着信 ARP パケットに特定の検査を実行します。デフォルトでは、どの検査も実行されません。 キーワードの意味は次のとおりです。 • **src-mac** の場合は、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 アドレスと比較します。この検証は、ARP 要求と ARP 応答に両方に対して実行されます。このチェックがイネーブルの場合、異なる MAC アドレスを持つパケットは無効として分類され、廃棄されます。 • **dst-mac** の場合は、イーサネット ヘッダー内の宛先 MAC アドレスを、ARP 本体の宛先 MAC アドレスと比較します。この検証は、ARP 応答に対して実行されます。このチェックがイネーブルの場合、異なる MAC アドレスを持つパケットは無効として分類され、廃棄されます。 • **ip** の場合は、無効な IP アドレスや予期しない IP アドレスが ARP 本体にないかどうかを確認します。0.0.0.0、255.255.255.255、およびすべての IP マルチキャスト アドレスがこれに該当します。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 応答内だけで検査されます。 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。コマンドを実行するたびに、その前のコマンドの設定は上書きされます。つまり、あるコマンドで **src mac** および **dst mac** の検証をイネーブルにし、2 番めのコマンドで IP 検証だけをイネーブルにした場合は、2 番めのコマンドによって **src mac** および **dst mac** の検証がディセーブルになります。
ステップ 3	**exit**	特権 EXEC モードに戻ります。
ステップ 4	**show ip arp inspection vlan** *vlan-range*	設定を確認します。
ステップ 5	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

検査をディセーブルにするには、**no ip arp inspection validate** [**src-mac**] [**dst-mac**] [**ip**] 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。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、および IP 検証に失敗したパケットの統計情報を表示するには、**show ip arp inspection statistics** 特権 EXEC コマンドを使用します。

ログ バッファの設定

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。メッセージの生成後、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。

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、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 バッファがオーバーフローする場合は、ログ イベントがログ バッファに収まらないことを意味しており、**show ip arp inspection log** 特権 EXEC コマンドの出力が影響を受けます。パケット数および時間以外のすべてのデータの代わりに [--] が表示されます。このエントリに関してそれ以外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。

ログ バッファを設定するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	**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	**ip arp inspection log-buffer** {**entries** *number* | **logs** *number* **interval** *seconds*}	ダイナミック ARP 検査のログ バッファを設定します。 デフォルトでは、ダイナミック ARP 検査をイネーブルにした場合は、拒否または廃棄された ARP パケットがログ記録されます。ログ エントリ数は、32 です。システム メッセージの数は 1 秒あたり 5 つに制限されています。ロギングレート インターバルは、1 秒です。 キーワードの意味は次のとおりです。 • **entries** *number* には、バッファにログ記録するエントリの数を指定します。指定できる範囲は 0 ～ 1024 です。 • **logs** *number* **interval** *seconds* には、指定のインターバルでシステム メッセージを生成するエントリの数を指定します。 **logs** *number* に指定できる範囲は 0 ～ 1024 です。値を 0 に設定すると、エントリはログ バッファに配置されますが、システム メッセージが生成されません。 指定できる **interval** *seconds* の範囲は 0 ～ 86400 秒（1 日）です。値を 0 に設定すると、システム メッセージがただちに生成されます（ログ バッファは常に空になります）。 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。 **logs** および **interval** の設定は、相互に作用します。**logs** *number* X が **interval** *seconds* Y より大きい場合は、X を Y で割って（X/Y）求められたシステム メッセージ数が 1 秒間に送信されます。それ以外の場合は、Y を X で割って（Y/X）求められた間隔（秒）で 1 つのシステム メッセージが送信されます。

	コマンド	目的
ステップ 3	**ip arp inspection vlan** *vlan-range* **logging** {**acl-match** {**matchlog** | **none**} | **dhcp-bindings** {**all** | **none** | **permit**}}	VLAN 単位でログ記録するパケットのタイプを制御します。デフォルトでは、拒否または廃棄されたすべてのパケットがログ記録されます。*ログ記録される*という表現は、エントリがログ バッファに格納されることと、システム メッセージが生成されることを意味しています。 キーワードの意味は次のとおりです。 • *vlan-range* には、VLAN ID 番号で識別された単一の VLAN、ハイフンで区切られた VLAN 範囲、またはカンマで区切られた一連の VLAN を指定できます。指定できる範囲は 1 ～ 4094 です。 • **acl-match matchlog** の場合は、ACE ロギング設定に基づいて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 コンフィギュレーション 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** の場合は、ACL と一致したパケットをログ記録しません。 • **dhcp-bindings all** の場合は、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** の場合は、DHCP バインディングと一致したパケットをログ記録しません。 • **dhcp-bindings permit** の場合は、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。
ステップ 4	**exit**	特権 EXEC モードに戻ります。
ステップ 5	**show ip arp inspection log**	設定を確認します。
ステップ 6	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

デフォルトのログ バッファ設定に戻すには、**no ip arp inspection log-buffer** {**entries** | **logs**} 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。デフォルトの VLAN ログ設定に戻すには、**no ip arp inspection vlan** *vlan-range* **logging** {**acl-match** | **dhcp-bindings**} 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。ログ バッファを消去するには、**clear ip arp inspection log** 特権 EXEC コマンドを使用します。

ダイナミック ARP 検査情報の表示

ダイナミック ARP 検査情報を表示するには、表 27-2 に示す各特権 EXEC コマンドを使用します。

表 27-2　ダイナミック ARP 検査情報を表示するためのコマンド

コマンド	説明
show arp access-list [*acl-name*]	ARP ACL に関する詳細情報を表示します。
show ip arp inspection interfaces [*interface-id*]	指定されたインターフェイスまたはすべてのインターフェイスに関して、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*	指定された VLAN のダイナミック ARP インスペクションの設定および動作ステートを表示します。VLAN を指定しない場合、または VLAN を範囲で指定した場合は、ダイナミック ARP 検査がイネーブル（アクティブ）にされている VLAN の情報だけが表示されます。

ダイナミック ARP 検査の統計情報を消去または表示するには、表 27-3 に示す各特権 EXEC コマンドを使用します。

表 27-3　ダイナミック ARP 検査の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	説明
clear ip arp inspection statistics	ダイナミック ARP 検査の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、ダイナミック ARP 検査がイネーブル（アクティブ）にされている VLAN の情報だけが表示されます。

show ip arp inspection statistics コマンドでは、スイッチは信頼されたダイナミック ARP インスペクション ポート上の各 ARP 要求および応答パケットの転送済みパケット数を増加させます。スイッチは、送信元 MAC、宛先 MAC、または IP 検証チェックによって拒否された各パケットの ACL または DHCP 許可済みパケット数を増加させ、適切な失敗数を増加させます。

ダイナミック ARP 検査のログ情報を消去または表示するには、表 27-4 に示す各特権 EXEC コマンドを使用します。

表 27-4　ダイナミック ARP 検査の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	説明
clear ip arp inspection log	ダイナミック ARP インスペクション ログ バッファを消去します。
show ip arp inspection log	ダイナミック ARP インスペクション ログ バッファの設定と内容を表示します。

これらのコマンドの詳細については、このリリースのコマンド リファレンスを参照してください。