CHAPTER 12

DHCP スヌーピングの設定

この章では、Cisco Nexus 1000V での Dynamic Host Configuration Protocol（DHCP）スヌーピングの設定手順を説明します。

ここでは、次の内容について説明します。

DHCP スヌーピングの概要

DHCP スヌーピングは、信頼できないホストと信頼できる DHCP サーバとの間でファイアウォールのような役割を果たします。具体的には、次の処理を実行します。

- 信頼できない発信元からの DHCP メッセージを検証するとともに、DHCP サーバからの無効な応答メッセージを除外します。
- DHCP スヌーピング バインディング データベースを構築し維持します。このデータベースには、リースされた IP アドレスを持つ信頼できないホストに関する情報が含まれます。
- 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、信頼できないホストからの以降の要求を検証します。

DAI（ダイナミック ARP インスペクション）および IP ソース ガードも、DHCP スヌーピング バインディング データベースに格納された情報を使用します。この 3 つの機能の詳細については、第 13 章「DAI の設定」と第 14 章「IP ソース ガードの設定」を参照してください。

DHCP スヌーピングは VLAN 単位でイネーブルにします。デフォルトでは、この機能はすべての VLAN で非アクティブです。この機能は 1 つの VLAN、または特定の VLAN 範囲でイネーブルにできます。

ここでは、次の内容について説明します。

信頼できる送信元と信頼できない送信元

DHCP スヌーピングの根底にあるのは、ポートが信頼できるものかどうかを明確にするという概念です。この機能がイネーブルのときに、デフォルトでは、vEthernet ポートはすべて「信頼できない」となり、イーサネット ポート（アップリンク）、ポート チャネル、特殊な vEthernet ポート（VSD などの機能の動作に使用される）はすべて「信頼できる」となります。トラフィックの送信元を DHCP の処理において信頼できるものと見なすかどうかを、管理者が設定できます。

企業ネットワークでは、信頼できる送信元はその企業の管理制御下にあるデバイスです。ファイアウォールの外にあるデバイスやネットワーク外のデバイスは、信頼できない送信元です。一般的に、ホスト ポートは信頼できない送信元として扱われます。

サービス プロバイダー環境では、サービス プロバイダー ネットワーク内にないデバイスは信頼できない送信元です（カスタマーのスイッチなど）。ホスト ポートは信頼できない送信元です。

Cisco Nexus 1000V では、特定の発信元が信頼できることを管理者が指定できます。指定するには、その発信元が接続しているインターフェイスの信頼状態を設定します。アップリンク ポート（アップリンク機能を持つことがポート プロファイルで定義されている）は、信頼できるポートです。したがって、信頼できないポートであると設定することはできません。このような制約があるので、レート制限への非適合や DHCP 応答が理由でアップリンクがシャットダウンされることはなくなります。

管理者は、他のインターフェイスも「信頼できる」と設定することができますが、それには、そのインターフェイスがネットワーク内部のデバイス（スイッチやルータなど）に接続されているか、管理者が DHCP サーバを VM 内で実行していることが条件となります。通常は、管理者がホスト ポート インターフェイスを「信頼できる」と設定することはありません。

（注）　DHCP スヌーピングを適切に機能させるためには、すべての DHCP サーバが信頼できるインターフェイスを介してデバイスと接続される必要があります。

DHCP スヌーピング バインディング データベース

DHCP スヌーピングが代行受信した DHCP メッセージから抽出された情報を使用して、各 VEM 上のデータベースが動的に構築され、維持されます。このデータベースには、リースされた IP アドレスを持つ信頼できないホスト 1 つにつき 1 つのエントリが格納されます。このデータベースに登録されるのは、そのホストが関連付けられている VLAN で DHCP スヌーピングがイネーブルになっている場合です。このデータベースには、信頼できるインターフェイスを通じて接続されたホストのエントリは含まれていません。

（注）　DHCP スヌーピング バインディング データベースは、「DHCP スヌーピング バインディング テーブル」と呼ばれることもあります。

デバイスが特定の DHCP メッセージを受信すると、DHCP スヌーピングはデータベースをアップデートします。たとえば、デバイスが DHCPACK メッセージをサーバから受信すると、この機能によってデータベースにエントリが追加されます。このデータベースからエントリが削除されるのは、IP アドレスのリース期限が過ぎたとき、またはデバイスが DHCP クライアントから DHCPRELEASE または DHCP DECLINE を受信したとき、またはデバイスが DHCP サーバから DHCPNACK を受信したときです。

DHCP スヌーピング バインディング データベースの各エントリの内容は、ホストの MAC アドレス、リースされた IP アドレス、リース期間、バインディングの種類、およびホストに関連付けられた VLAN（仮想 LAN）の番号とインターフェイス情報です。

動的に追加されたエントリをバインディング データベースから削除するには、**clear ip dhcp snooping binding** コマンドを使用します。詳細については、「DHCP スヌーピング バインディング データベースのクリア」（P.12-13）を参照してください。

ハイ アベイラビリティ

VEM 上に作成された DHCP スヌーピング バインディング テーブルとすべてのデータベース エントリは、VSM にエクスポートされ、VSM のリブート後も維持されます。

DHCP スヌーピングの前提条件

DHCP スヌーピングの前提条件は次のとおりです。

- DHCP スヌーピングを設定するには、DHCP に関する知識が必要です。

注意事項および制約事項

DHCP スヌーピングに関する注意事項と制約事項は次のとおりです。

- DHCP スヌーピング データベースは各 VEM 上に作成され、1 つのデータベースに最大 1024 個のバインディングを格納できます。
- DHCP スヌーピングをシームレスにするために、仮想サービス ドメイン（VSD）サービス VM ポートは、デフォルトで信頼できるポートとなっています。管理者がそのポートを「信頼できない」と設定しても、この設定は無視されます。
- VSM の接続に VEM が使用される場合、つまり VSM の VSM AIPC、管理、およびインバンドのポートが特定の VEM 上にある場合は、これらの仮想イーサネット インターフェイスが信頼できるインターフェイスとして設定されている必要があります。

デフォルト設定

表 12-1 に、DHCP スヌーピングのデフォルトを示します。

表 12-1　DHCP スヌーピングのパラメータのデフォルト値

パラメータ	デフォルト
DHCP スヌーピングのグローバルなイネーブル化	不可
DHCP スヌーピング VLAN	ディセーブル

表 12-1　DHCP スヌーピングのパラメータのデフォルト値（続き）

パラメータ	デフォルト
DHCP スヌーピングの MAC アドレス検証	イネーブル
DHCP スヌーピング信頼状態	信頼できる：イーサネット インターフェイス、vEthernet インターフェイス、およびポート チャネル（VSD 機能に参加しているもの）信頼できない：VSD 機能に参加していない vEthernet インターフェイス

DHCP スヌーピングの設定

ここでは、次の内容について説明します。

DHCP スヌーピングの最小設定

DHCP スヌーピングの最小設定は次のとおりです。

ステップ 1　DHCP スヌーピングをグローバルにイネーブル化します。詳細については、「DHCP スヌーピングのグローバルなイネーブル化またはディセーブル化」（P.12-5）を参照してください。

ステップ 2　少なくとも 1 つの VLAN で DHCP スヌーピングをイネーブルにします。詳細については、「VLAN に対する DHCP スヌーピングのイネーブル化またはディセーブル化」（P.12-6）を参照してください。

デフォルトでは、DHCP スヌーピングはすべての VLAN でディセーブルになります。

ステップ 3　DHCP サーバとデバイスが、信頼できるインターフェイスを使用して接続されていることを確認します。詳細については、「インターフェイスの信頼状態の設定」（P.12-8）を参照してください。

DHCP スヌーピングのグローバルなイネーブル化またはディセーブル化

ここでは、DHCP スヌーピングをグローバルにイネーブルまたはディセーブルにする手順を説明します。

始める前に

この手順を開始する前に、次のことを確認または実行する必要があります。

- DHCP スヌーピングをサポートするソフトウェア リリース（リリース 4.0(4)SV1(2) 以降）が VSM およびすべての VEM で実行されていることと、VEM 機能レベルが更新されていることを確認します（『*Cisco Nexus 1000V Software Upgrade Guide, Release 4.0(4)SV1(3)*』を参照）。
- デフォルトでは、DHCP スヌーピングはグローバルにディセーブルです。
- DHCP スヌーピングがグローバルにディセーブルになると、DHCP スヌーピングはすべて停止し、DHCP メッセージは中継されなくなります。
- DHCP スヌーピングを設定した後でグローバルにディセーブルにした場合も、残りの設定は維持されます。

手順の概要

1. **config t**
2. **[no] ip dhcp snooping**
3. **show running-config dhcp**
4. **copy running-config startup-config**

手順の詳細

	コマンド	目的

ステップ 1	**config t**
	
	例：
	`n1000v# config t`
	`n1000v(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 dhcp snooping** **例：** `n1000v(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** オプションを使用すると、DHCP スヌーピングがディセーブルになりますが、既存の DHCP スヌーピング設定は維持されます。
ステップ 3	**show running-config dhcp** **例：** `n1000v(config)# show running-config dhcp`	DHCP スヌーピングの設定を表示します。
ステップ 4	**copy running-config startup-config** **例：** `n1000v(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、リブートと再起動を行って、永久的に保存します。

VLAN に対する DHCP スヌーピングのイネーブル化またはディセーブル化

ここでは、1 つまたは複数の VLAN に対して DHCP スヌーピングをイネーブルまたはディセーブルにする手順を説明します。

始める前に

この手順を開始する前に、次のことを確認または実行する必要があります。

- この機能をサポートするソフトウェア リリース（リリース 4.0(4)SV1(2) 以降）が VSM およびすべての VEM で実行されていることと、VEM 機能レベルが更新されていることを確認します（『*Cisco Nexus 1000V Software Upgrade Guide, Release 4.0(4)SV1(3)*』を参照）。
- デフォルトでは、DHCP スヌーピングはすべての VLAN でディセーブルになります。

手順の概要

1. **config t**
2. [**no**] **ip dhcp snooping vlan** *vlan-list*
3. **show running-config dhcp**
4. **copy running-config startup-config**

手順の詳細

	コマンド	目的

ステップ 1	**config t**
	
	例：
	`n1000v# config t`
	`n1000v(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 dhcp snooping vlan** *vlan-list* 例： `n1000v(config)# ip dhcp snooping vlan 100,200,250-252`	*vlan-list* で指定する VLAN の DHCP スヌーピングをイネーブルにします。**no** オプションを使用すると、指定した VLAN の DHCP スヌーピングがディセーブルになります。
ステップ 3	**show running-config dhcp** 例： `n1000v(config)# show running-config dhcp`	DHCP スヌーピングの設定を表示します。
ステップ 4	**copy running-config startup-config** 例： `n1000v(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、リブートと再起動を行って、永久的に保存します。

DHCP スヌーピングの MAC アドレス検証のイネーブル化またはディセーブル化

ここでは、DHCP スヌーピングの MAC アドレス検証をイネーブルまたはディセーブルにする手順を説明します。信頼できないインターフェイスからパケットを受信し、この送信元 MAC アドレスと DHCP クライアント ハードウェア アドレスが一致しない場合、アドレス検証によってデバイスはパケットをドロップします。

始める前に

この手順を開始する前に、次のことを確認または実行する必要があります。

- この機能をサポートするソフトウェア リリース（リリース 4.0(4)SV1(2) 以降）が VSM およびすべての VEM で実行されていることと、VEM 機能レベルが更新されていることを確認します（『*Cisco Nexus 1000V Software Upgrade Guide, Release 4.0(4)SV1(3)*』を参照）。
- MAC アドレス検証はデフォルトでイネーブルになります。

手順の概要

1. **config t**
2. **[no] ip dhcp snooping verify mac-address**
3. **show running-config dhcp**
4. **copy running-config startup-config**

手順の詳細

	コマンド	目的

ステップ 1	**config t**
	
	例：
	`n1000v# config t`
	`n1000v(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 dhcp snooping verify mac-address** **例：** `n1000v(config)# ip dhcp snooping verify mac-address`	DHCP スヌーピングの MAC アドレス検証をイネーブルにします。**no** オプションを使用すると MAC アドレス検証がディセーブルになります。
ステップ 3	**show running-config dhcp** **例：** `n1000v(config)# show running-config dhcp`	DHCP スヌーピングの設定を表示します。
ステップ 4	**copy running-config startup-config** **例：** `n1000v(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、リブートと再起動を行って、永久的に保存します。

インターフェイスの信頼状態の設定

ここでは、特定の仮想インターフェイスが DHCP メッセージの送信元として信頼できるものかどうかを設定する手順を説明します。次のものの DHCP 信頼状態を設定できます。

- レイヤ 2 vEthernet インターフェイス
- レイヤ 2 vEthernet インターフェイスのポート プロファイル

始める前に

この手順を開始する前に、次のことを確認または実行する必要があります。

- この機能をサポートするソフトウェア リリース（リリース 4.0(4)SV1(2) 以降）が VSM およびすべての VEM で実行されていることと、VEM 機能レベルが更新されていることを確認します（『*Cisco Nexus 1000V Software Upgrade Guide, Release 4.0(4)SV1(3)*』を参照）。
- デフォルトでは、vEthernet インターフェイスは「信頼できない」となっています。ただし、信頼できる他の機能（VSD など）によって使用される特殊な vEthernet ポートは例外です。
- vEthernet インターフェイスがレイヤ 2 インターフェイスとして設定されていることを確認します。
- DHCP スヌーピング、DAI、および IP ソース ガードをシームレスにするために、仮想サービス ドメイン（VSD）サービス VM ポートはデフォルトで信頼できるポートとなっています。管理者がそのポートを「信頼できない」と設定しても、この設定は無視されます。

手順の概要

1. **config t**
2. **interface vethernet** *interface-number*

   port-profile *profilename*
3. [**no**] **ip dhcp snooping trust**
4. **show running-config dhcp**
5. **copy running-config startup-config**

手順の詳細

	コマンド	目的
ステップ 1	**config t** 例： n1000v# config t n1000v(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 vethernet** *interface-number* 例： n1000v(config)# interface vethernet 3 n1000v(config-if)#	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。*interface-number* は、DHCP スヌーピングにおいて信頼できるものとして扱うかどうかを設定する vEthernet インターフェイスです。
	port-profile *profilename* 例： n1000v(config)# port-profile vm-data n1000v(config-port-prof)#	指定したポート プロファイルのポート プロファイル コンフィギュレーション モードを開始します。*profilename* は最大 80 文字の一意の名前です。
ステップ 3	[**no**] **ip dhcp snooping trust** 例： n1000v(config-if)# ip dhcp snooping trust	DHCP スヌーピングに関して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します。**no** オプションを使用すると、ポートは信頼できないインターフェイスとして設定されます。
ステップ 4	**show running-config dhcp** 例： n1000v(config-if)# show running-config dhcp	DHCP スヌーピングの設定を表示します。
ステップ 5	**copy running-config startup-config** 例： n1000v(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、リブートと再起動を行って、永久的に保存します。

DHCP パケットのレート制限の設定

ここでは、各ポートで受信される DHCP パケットのレート制限を設定する手順を説明します。

始める前に

この手順を開始する前に、次のことを確認または実行する必要があります。

- この機能をサポートするソフトウェア リリース（リリース 4.0(4)SV1(2) 以降）が VSM およびすべての VEM で実行されていることと、VEM 機能レベルが更新されていることを確認します（『*Cisco Nexus 1000V Software Upgrade Guide, Release 4.0(4)SV1(3)*』を参照）。
- 設定されたレートに違反すると、ポートは自動的に errdisable 状態になります。

手順の概要

1. **config t**
2. **interface vethernet** *interface-number*

   port-profile *profilename*
3. **[no] ip dhcp snooping limit rate** *rate*

4. **show running-config dhcp**
5. **copy running-config startup-config**

手順の詳細

	コマンド	目的
ステップ 1	**config t** 例： n1000v# config t n1000v(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 vethernet** *interface-number* 例： n1000v(config)# interface vethernet 3 n1000v(config-if)#	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。*interface-number* は、DHCP スヌーピングにおいて信頼できるものとして扱うかどうかを設定する vEthernet インターフェイスです。
	port-profile *profilename* 例： n1000v(config)# port-profile vm-data n1000v(config-port-prof)#	指定したポート プロファイルのポート プロファイル コンフィギュレーション モードを開始します。*profilename* は最大 80 文字の一意の名前です。
ステップ 3	[**no**] **ip dhcp snooping limit rate** *rate* 例： n1000v(config-if)# ip dhcp snooping limit rate 30	DHCP 制限レートを設定します。**no** オプションを指定すると、この設定が削除されます。
ステップ 4	**show running-config dhcp** 例： n1000v(config-if)# show running-config dhcp	DHCP スヌーピングの設定を表示します。
ステップ 5	**copy running-config startup-config** 例： n1000v(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、リブートと再起動を行って、永久的に保存します。

DHCP Error-Disabled 検出のイネーブル化またはディセーブル化

ここでは、DHCP レート制限を超過したポートに対する error-disabled 検出をイネーブルまたはディセーブルにする手順を説明します。

始める前に

この手順を開始する前に、次のことを確認または実行する必要があります。

- この機能をサポートするソフトウェア リリース（リリース 4.0(4)SV1(2) 以降）が VSM およびすべての VEM で実行されていることと、VEM 機能レベルが更新されていることを確認します（『*Cisco Nexus 1000V Software Upgrade Guide, Release 4.0(4)SV1(3)*』を参照）。
- 設定されたレートに違反すると、ポートは自動的に errdisable 状態になります。
- error-disabled 状態のインターフェイスを手動で回復するには、**shutdown** コマンドを入力してから **no shutdown** コマンドを入力する必要があります。

手順の概要

1. **config t**
2. **[no] errdisable detect cause dhcp-rate-limit**
3. **show running-config dhcp**
4. **copy running-config startup-config**

手順の詳細

	コマンド	目的

ステップ 1	**config t**
	
	例：
	`n1000v# config t`
	`n1000v(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] errdisable detect cause dhcp-rate-limit** **例：** `n1000v(config)# errdisable detect cause dhcp-rate-limit`	DHCP error-disabled 検出をイネーブルにします。**no** オプションを使用すると、DHCP error-disabled 検出がディセーブルになります。
ステップ 3	**show running-config dhcp** **例：** `n1000v(config)# show running-config dhcp`	DHCP スヌーピングの設定を表示します。
ステップ 4	**copy running-config startup-config** **例：** `n1000v(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、リブートと再起動を行って、永久的に保存します。

DHCP Error-Disabled 回復のイネーブル化またはディセーブル化

ここでは、DHCP レート制限を超過したポートに対する error-disabled 回復をイネーブルまたはディセーブルにする手順を説明します。

始める前に

この手順を開始する前に、次のことを確認または実行する必要があります。

- この機能をサポートするソフトウェア リリース（リリース 4.0(4)SV1(2) 以降）が VSM およびすべての VEM で実行されていることと、VEM 機能レベルが更新されていることを確認します（『*Cisco Nexus 1000V Software Upgrade Guide, Release 4.0(4)SV1(3)*』を参照）。
- 設定されたレートに違反すると、ポートは自動的に errdisable 状態になります。
- error-disabled 状態のインターフェイスを手動で回復するには、**shutdown** コマンドを入力してから **no shutdown** コマンドを入力する必要があります。

手順の概要

1. **config t**
2. **[no] errdisable recovery cause dhcp-rate-limit**

3. **errdisable recovery interval** *timer-interval*
4. **show running-config dhcp**
5. **copy running-config startup-config**

手順の詳細

	コマンド	目的

ステップ 1	**config t**
	
	例：
	`n1000v# config t`
	`n1000v(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] errdisable recovery cause dhcp-rate-limit** **例：** `n1000v(config)# errdisable detect cause dhcp-rate-limit`	DHCP error-disabled 回復をイネーブルにします。**no** オプションを使用すると、DHCP error-disabled 回復がディセーブルになります。
ステップ 3	**errdisable recovery interval** *timer-interval* **例：** `n1000v(config)# errdisable recovery interval 30`	DHCP error-disabled 回復間隔を設定します。*timer-interval* は秒数（30 ～ 65535）です。
ステップ 4	**show running-config dhcp** **例：** `n1000v(config)# show running-config dhcp`	DHCP スヌーピングの設定を表示します。
ステップ 5	**copy running-config startup-config** **例：** `n1000v(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、リブートと再起動を行って、永久的に保存します。

DHCP スヌーピングの設定の確認

DHCP スヌーピングの設定情報を表示するには、次のコマンドを使用します。

コマンド	目的
show running-config dhcp	DHCP スヌーピングの設定を表示します。
show ip dhcp snooping	DHCP スヌーピングに関する一般的な情報を表示します。

これらのコマンドの出力フィールドの詳細については、『*Cisco Nexus 1000V Command Reference, Release 4.0(4)SV1(3)*』を参照してください。

DHCP バインディングの表示

DHCP バインディング テーブルを表示するには、**show ip dhcp snooping binding** コマンドを使用します。このコマンドの出力フィールドの詳細については、『*Cisco Nexus 1000V Command Reference, Release 4.0(4)SV1(3)*』を参照してください。

DHCP スヌーピング バインディング データベースのクリア

ここでは、DHCP スヌーピング バインディング データベースからすべてのエントリを削除する手順を説明します。

始める前に

この手順を開始する前に、次のことを確認または実行する必要があります。

- この機能をサポートするソフトウェア リリース（リリース 4.0(4)SV1(2) 以降）が VSM およびすべての VEM で実行されていることと、VEM 機能レベルが更新されていることを確認します（『*Cisco Nexus 1000V Software Upgrade Guide, Release 4.0(4)SV1(3)*』を参照）。

手順の概要

1. **clear ip dhcp snooping binding**
2. **show ip dhcp snooping binding**

手順の詳細

	コマンド	目的
ステップ 1	**clear ip dhcp snooping binding** **例：** `n1000v# clear ip dhcp snooping binding`	DHCP スヌーピング バインディング データベースに動的に追加されたエントリを消去します。
ステップ 2	**show ip dhcp snooping binding** **例：** `n1000v# show ip dhcp snooping binding`	DHCP スヌーピング バインディング データベースを表示します。

DHCP スヌーピングの統計情報の表示

DHCP スヌーピングの統計情報を表示するには、**show ip dhcp snooping statistics** コマンドを使用します。このコマンドの出力フィールドの詳細については、『*Cisco Nexus 1000V Command Reference, Release 4.0(4)SV1(3)*』を参照してください。

DHCP スヌーピングの設定例

次に、2 つの VLAN 上で DHCP スヌーピングをイネーブルにする例を示します。vEthernet インターフェイス 5 が「信頼できる（trusted）」となっているのは、DHCP サーバがこのインターフェイスに接続されているからです。

```
ip dhcp snooping

interface vethernet 5
  ip dhcp snooping trust
ip dhcp snooping vlan 1
ip dhcp snooping vlan 50
```

その他の関連資料

DHCP スヌーピングの実装に関する詳細情報については、次の項を参照してください。

- 「関連資料」（P.12-14）
- 「標準規格」（P.12-14）

関連資料

関連項目	マニュアル タイトル
IP ソース ガード	『*Cisco Nexus 1000V セキュリティ コンフィギュレーション ガイド リリース 4.0(4)SV1(3)*』の第 14 章「IP ソース ガードの設定」
DAI	『*Cisco Nexus 1000V セキュリティ コンフィギュレーション ガイド リリース 4.0(4)SV1(3)*』の第 13 章「DAI の設定」
DHCP スヌーピング コマンド：すべてのコマンド構文、コマンド モード、コマンド履歴、デフォルト値、使用上の注意事項、例	『*Cisco Nexus 1000V Command Reference, Release 4.0(4)SV1(3)*』

標準規格

標準規格	タイトル
RFC-2131	『*Dynamic Host Configuration Protocol*』（http://tools.ietf.org/html/rfc2131）

DHCP スヌーピング機能の履歴

表 12-2 に、この機能のリリース履歴を示します。

表 12-2　DHCP スヌーピング機能の履歴

機能名	リリース	機能情報
DHCP スヌーピング	4.0(4)SV1(2)	この機能が追加されました。