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 4.2(1) SV1(4b)

2012 年 3 月 29 日

Text Part Number: OL-26704-01-J

【注意】シスコ製品をご使用になる前に、安全上の注意（www.cisco.com/jp/go/safety_warning/）をご確認ください。

本書は、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動 / 変更されている場合がありますことをご了承ください。
あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。

また、契約等の記述については、弊社販売パートナー、または、弊社担当者にご確認ください。

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 4.2(1) SV1(4b)

CONTENTS

新機能および変更された機能に関する情報

この章では、このマニュアルの各リリースで追加または変更された情報と、その情報が記載されている場所を示します。

機能	説明	対象リリース	参照先
UUFB	スイッチの転送パスがフラッディングしないように不明なユニキャスト パケットをブロックできます。	4.2(1)SV1(4a)	第 16 章「不明なユニキャスト フラッディングのブロック」
DHCP スヌーピング リレー エージェント（オプション 82）	DHCP パケットの VSM MAC およびポート情報をリレーするように DHCP を設定できます。	4.2(1)SV1(4)	第 12 章「DHCP スヌーピングの設定」
DHCP スヌーピング バインディング テーブル	インターフェイスの DHCP スヌーピング バインディング テーブル エントリを消去できます。	4.2(1)SV1(4)	第 12 章「DHCP スヌーピングの設定」
DHCP のイネーブル化	**feature DHCP** コマンドを使用して DHCP をグローバルにイネーブルまたはディセーブルにできます。	4.2(1)SV1(4)	第 12 章「DHCP スヌーピングの設定」
SSH サーバのイネーブル化	**feature DHCP** コマンドを使用して SSH サーバをイネーブルまたはディセーブルにできます。	4.2(1)SV1(4)	第 7 章「SSH の設定」
Telnet サーバをイネーブルにする	**feature DHCP** コマンドを使用して Telnet サーバをイネーブルまたはディセーブルにできます。	4.2(1)SV1(4)	第 8 章「Telnet の設定」
HTTP サーバのディセーブル化	HTTP サーバをセキュリティ目的でディセーブルにします。	4.2(1)SV1(4)	第 15 章「HTTP サーバのディセーブル化」
VSD	Virtual Service Domain（VSD; 仮想サービス ドメイン）を利用すると、ネットワーク サービスのためのトラフィックの分類と分離が可能になります。	4.0(4)SV1(2)	第 3 章「VSD の設定」
DHCP スヌーピング	DHCP（Dynamic Host Configuration Protocol）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。	4.0(4)SV1(2)	第 12 章「DHCP スヌーピングの設定」

機能	説明	対象リリース	参照先
Dynamic ARP Inspection（DAI; ダイナミック ARP インスペクション）	DAI（Dynamic ARP Inspection）とは、レイヤ 2 ブロードキャスト ドメイン内の IP 通信を実現するために、IP アドレスを MAC（メディア アクセス コントロール）アドレスにマッピングする機能です。	4.0(4)SV1(2)	第 13 章「Dynamic ARP Inspection の設定」
IPSG	IP ソース ガードは、IP アドレスと MAC を調べてトラフィックを許可する、インターフェイス単位のフィルタです。	4.0(4)SV1(2)	第 14 章「IP ソース ガードの設定」

はじめに

セキュリティ設定に関するこのマニュアルでは、AAA、VSD、SSH などのセキュリティ機能を設定する手順を示します。

この「はじめに」では、このマニュアルの次の点について説明します。

対象読者

このマニュアルは、ネットワーク システムの上級ユーザを対象としています。

マニュアルの構成

このマニュアルは、次の章で構成されています。

章とタイトル	説明
第 1 章「セキュリティの概要」	セキュリティ機能について説明します。
第 2 章「ユーザ アカウントの管理」	ユーザ アカウントを設定する手順について説明します。
第 3 章「VSD の設定」	VSD を設定する手順について説明します。
第 4 章「AAA の設定」	AAA を設定する手順について説明します。
第 5 章「RADIUS の設定」	RADIUS を設定する手順について説明します。
第 6 章「TACACS+ の設定」	TACACS+ を設定する手順について説明します。
第 7 章「SSH の設定」	SSH を設定する手順について説明します。
第 8 章「Telnet の設定」	Telnet を設定する手順について説明します。
第 9 章「IP ACL の設定」	トラフィックをフィルタリングするための IP Access Control List（ACL; アクセス コントロール リスト）を設定する手順について説明します。

章とタイトル	説明
第 10 章「MAC ACL の設定」	トラフィックをフィルタリングするための MAC アクセス コントロール リスト（ACL）を設定する手順について説明します。
第 11 章「ポート セキュリティの設定」	ポート セキュリティを設定する手順について説明します。
第 12 章「DHCP スヌーピングの設定」	DHCP スヌーピングの設定方法について説明します。
第 13 章「Dynamic ARP Inspection の設定」	Dynamic ARP Inspection（DAI; ダイナミック ARP インスペクション）を設定する方法について説明します。
第 14 章「IP ソース ガードの設定」	IP ソース ガードを設定する手順について説明します。
第 15 章「HTTP サーバのディセーブル化」	HTTP サーバをディセーブルにする方法について説明します。
第 16 章「不明なユニキャスト フラッディングのブロック」	転送パスの不明なユニキャスト パケットのフラッディング（UUFB）をブロックする方法について説明します。
第 17 章「セキュリティ設定の制限値」	セキュリティ機能の設定制限値について説明します。

表記法

コマンドの説明では、次の表記法を使用しています。

太字	コマンドおよびキーワードは太字で示しています。
イタリック体	ユーザが値を指定する引数は、イタリック体で示しています。
{ }	波カッコの中の要素は、必須の選択要素です。
[ ]	角カッコの中の要素は、省略可能です。
x | y | z	いずれか 1 つを選択する要素は、縦線で区切って示されます。
string	引用符を付けない一組の文字。string の前後には引用符を使用しません。引用符を使用すると、その引用符も含めて string とみなされます。

出力例では、次の表記法を使用しています。

`screen フォント`	デバイスが表示するターミナル セッションおよび情報は、screen フォントで示しています。
太字の screen フォント	ユーザが入力しなければならない情報は、太字の screen フォントで示しています。
イタリック体の screen フォント	ユーザが値を指定する引数は、イタリック体の screen フォントで示しています。
< >	パスワードのように出力されない文字は、山カッコ（< >）で囲んで示しています。
[ ]	システム プロンプトに対するデフォルトの応答は、角カッコで囲んで示しています。
!、#	コードの先頭に感嘆符（!）またはポンド記号（#）がある場合には、コメント行であることを示します。

このマニュアルでは、注釈および注意に次の表記法を使用しています。

（注） 「*注釈*」です。役立つ情報や、このマニュアル以外の参照資料などを紹介しています。

注意 「*要注意*」の意味です。機器の損傷またはデータ損失を予防するための注意事項が記述されています。

関連資料

この項では、Cisco Nexus 1000 とともに使用されるマニュアルの一覧を示します。これらのマニュアルは、Cisco.com の次に示す URL で入手できます。

http://www.cisco.com/en/US/products/ps9902/tsd_products_support_series_home.html

一般情報

『Cisco Nexus 1000V Documentation Roadmap, Release 4.2(1)SV1(4a)』

『Cisco Nexus 1000V Release Notes, Release 4.2(1)SV1(4b)』

『Cisco Nexus 1000V Compatibility Information, Release 4.2(1)SV1(4b)』

『Cisco Nexus 1010 Management Software Release Notes, Release 4.2(1)SP1(4)』

インストール & アップグレード

『Cisco Nexus 1000V Software Installation Guide, Release 4.2(1)SV1(4b)』

『Cisco Nexus 1000V Software Upgrade Guide, Release 4.2(1)SV1(4b)』

『Cisco Nexus 1000V VEM Software Installation and Upgrade Guide, Release 4.2(1)SV1(4b)』

『Cisco Nexus 1010 Virtual Services Appliance Hardware Installation Guide』

『Cisco Nexus 1010 Software Installation and Upgrade Guide, Release 4.2(1)SP1(4)』

コンフィギュレーション ガイド

『Cisco Nexus 1000V License Configuration Guide, Release 4.2(1)SV1(4a)』

『Cisco Nexus 1000V Getting Started Guide, Release 4.2(1)SV1(4b)』

『Cisco Nexus 1000V High Availability and Redundancy Configuration Guide, Release 4.2(1)SV1(4b)』

『Cisco Nexus 1000V Interface Configuration Guide, Release 4.2(1)SV1(4a)』

『Cisco Nexus 1000V Layer 2 Switching Configuration Guide, Release 4.2(1)SV1(4)』

『Cisco Nexus 1000V Port Profile Configuration Guide, Release 4.2(1)SV1(4a)』

『Cisco Nexus 1000V Quality of Service Configuration Guide, Release 4.2(1)SV1(4)』

『Cisco Nexus 1000V Security Configuration Guide, Release 4.2(1)SV1(4b)』

『Cisco Nexus 1000V System Management Configuration Guide, Release 4.2(1)SV1(4b)』

『Cisco Nexus 1010 ソフトウェア コンフィギュレーション ガイド リリース Release 4.2(1)SP1(4)』

プログラミング ガイド

『Cisco Nexus 1000V XML API User Guide, Release 4.2(1)SV1(4)』

リファレンス

『Cisco Nexus 1000V Command Reference, Release 4.2(1)SV1(4)』

『Cisco Nexus 1000V MIB Quick Reference』

『Cisco Nexus 1010 Command Reference, Release 4.2(1)SP1(4)』

トラブルシューティング & アラート

『Cisco Nexus 1000V Troubleshooting Guide, Release 4.2(1)SV1(4a)』

『Cisco Nexus 1000V Password Recovery Guide』

『Cisco NX-OS System Messages Reference』

Virtual Security Gateway マニュアル

『Cisco Virtual Security Gateway for Nexus 1000V Series Switch』

Virtual Network Management Center

「Cisco Virtual Network Management Center」

ネットワーク解析モジュール マニュアル

『Cisco Prime Network Analysis Module Software Documentation Guide, 5.1』

『Cisco Prime Network Analysis Module (NAM) for Nexus 1010 Installation and Configuration Guide, 5.1』

『Cisco Prime Network Analysis Module Command Reference Guide 5.1』

『Cisco Prime Network Analysis Module Software 5.1 Release Notes』

『Cisco Prime Network Analysis Module Software 5.1 User Guide』

マニュアルの入手方法およびテクニカル サポート

マニュアルの入手方法、テクニカル サポート、その他の有用な情報について、次の URL で、毎月更新される『*What's New in Cisco Product Documentation*』を参照してください。シスコの新規および改訂版の技術マニュアルの一覧も示されています。

http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html

『*What's New in Cisco Product Documentation*』は RSS フィードとして購読できます。また、リーダー アプリケーションを使用してコンテンツがデスクトップに直接配信されるように設定することもできます。RSS フィードは無料のサービスです。シスコは現在、RSS バージョン 2.0 をサポートしています。

CHAPTER 1

セキュリティの概要

この章では、Cisco Nexus 1000V で使用される次のセキュリティ機能の概要について説明します。

ユーザ アカウント

Cisco Nexus 1000V にアクセスするには、ユーザ アカウントをセットアップする必要があります。このユーザ アカウントによって、各ユーザに許可される具体的なアクションが定義されます。ユーザ アカウントは最大 256 個作成できます。管理者は、各ユーザ アカウントに対して、ロール、ユーザ名、パスワード、および有効期限を定義します。ユーザ カウントの設定および管理の方法については、第 2 章「ユーザ アカウントの管理」を参照してください。

仮想サービス ドメイン

仮想サービス ドメイン（VSD）を使用すると、ネットワーク サービスのためのトラフィックの分類と分離が可能になります。このネットワーク サービスの例としては、ファイアウォールやトラフィック監視があり、その他にコンプライアンス目標（たとえば Sarbanes Oxley）の達成支援のためのサービスなどがあります。VSD の設定および管理の方法については、第 3 章「VSD の設定」を参照してください。

認証、許可、アカウンティング（AAA）

AAA（トリプル A と呼ばれます）は、3 つの独立した、一貫性のあるモジュラ型のセキュリティ機能を設定するためのアーキテクチャ フレームワークです。

- 認証：ログイン/パスワード ダイアログ、チャレンジ/レスポンス、メッセージング サポート、および暗号化（選択したセキュリティ プロトコルに基づく）などによるユーザの識別方法を提供します。認証は、ユーザに対してネットワークとネットワーク サービスへのアクセスを許可する前に、ユーザの識別を行う方法です。AAA 認証を設定するには、まず認証方式の名前付きリストを定義し、そのリストを各種インターフェイスに適用します。
- 認可：ワンタイム許可またはサービスごとの許可、ユーザ単位のアカウント リストとプロファイル、ユーザ グループ サポート、および IP、IPX、ARA、Telnet のサポートなど、リモート アクセスの制御方法を提供します。

  RADIUS や TACACS+ などのリモート セキュリティ サーバは、適切なユーザで該当する権利を定義した属性値（AV）のペアをアソシエートすることによって、ユーザに特定の権限を付与します。AAA 認可は、ユーザが認可された操作を示す一連の属性を組み合わせて実行します。これらの属性とデータベースに格納されている指定されたユーザの情報とが比較され、その結果が AAA に返されてユーザの実際の権限と制限事項が決定されます。
- アカウンティング：ユーザ ID、開始時刻と終了時刻、実行コマンド（PPP など）、パケット数、バイト数といった、課金、監査、およびレポートに使用するセキュリティ サーバ情報の収集と送信を行う手段を提供します。アカウンティングを使用することで、ユーザがアクセスしているサービスや、ユーザが消費しているネットワーク リソース量を追跡できます。

（注）　認証は AAA と別個に設定することができます。ただし RADIUS または TACACS+ を使用する場合や、バックアップの認証方式を設定する場合は、AAA を設定する必要があります。

AAA の設定手順については、第 4 章「AAA の設定」を参照してください。

RADIUS セキュリティ プロトコル

AAA は、ネットワーク アクセス サーバと RADIUS セキュリティ サーバ間の通信を確立します。

RADIUS は、不正アクセスからネットワークを保護する分散型クライアント/サーバ システムで、AAA を使用して実装されます。シスコの実装では RADIUS クライアントは Cisco ルータ上で稼動します。認証要求は、すべてのユーザ認証情報とネットワーク サービス アクセス情報が格納されている中央の RADIUS サーバに送信されます。

RADIUS の設定手順については、第 5 章「RADIUS の設定」を参照してください。

TACACS+ セキュリティ プロトコル

AAA は、ネットワーク アクセス サーバと TACACS+ セキュリティ サーバ間の通信を確立します。

TACACS+ は、ルータまたはネットワーク アクセス サーバにアクセスしようとするユーザの検証を集中的に行うセキュリティ アプリケーションで、AAA を使用して実装されます。TACACS+ サービスは、通常 UNIX または Windows NT ワークステーション上で稼動する TACACS+ デーモンのデータベースで管理されます。TACACS+ は独立したモジュラ型の認証、許可、およびアカウンティング機能を提供します。

TACACS+ の設定手順については、第 6 章「TACACS+ の設定」を参照してください。

SSH

Secure Shell（SSH; セキュア シェル）サーバを使用すると、SSH クライアントはデバイスとの間でセキュアな暗号化された接続を確立できます。SSH は強化暗号化を使用して認証を行います。SSH サーバは、市販の一般的な SSH クライアントとの相互運用が可能です。

SSH クライアントは、市販の一般的な SSH サーバと連動します。

詳細については、第 7 章「SSH の設定」を参照してください。

Telnet

Telnet プロトコルは、ホストとの TCP/IP 接続を確立するのに使用できます。Telnet を使用すると、あるサイトのユーザが別のサイトのログイン サーバと TCP 接続を確立し、デバイス間でキーストロークをやり取りできます。Telnet は、リモート デバイス アドレスとして IP アドレスまたはドメイン名のいずれかを受け入れます。詳細については、第 8 章「Telnet の設定」を参照してください。

アクセス コントロール リスト（ACL）

ACL は、トラフィックをフィルタリングするための順番に並べられた一連のルールです。デバイスは、パケットを適用する ACL を決定する際に、パケットをルールに対してテストしていきます。最初に一致したルールで、そのパケットが許可されるか拒否されるかが決定されます。一致するルールがない場合は、そのデバイスでのデフォルト ルールが適用されます。デバイスは、許可されたパケットは処理し、拒否されたパケットは廃棄します。

ACL は、ネットワークおよび特定のホストを不必要なトラフィックや望ましくないトラフィックから保護します。たとえば、高セキュリティ ネットワークからインターネットへの HTTP トラフィックを禁止することができます。ACL では、サイトの IP アドレスを使用して IP ACL 内でサイトを識別することにより、特定のサイトへの HTTP トラフィックだけを許可するといったこともできます。

詳細については、次の説明を参照してください。

- 第 9 章「IP ACL の設定」
- 第 10 章「MAC ACL の設定」

ポート セキュリティ

ポート セキュリティを使用すると、限定的なセキュア MAC アドレスからのインバウンド トラフィックを許可するようにレイヤ 2 インターフェイスを設定することができます。セキュアな MAC アドレスからのトラフィックは、同じ VLAN 内の別のインターフェイス上では許可されません。「セキュア」にできる MAC アドレスの数は、インターフェイス単位で設定します。

詳細については、第 11 章「ポート セキュリティの設定」を参照してください。

DHCP スヌーピング

DHCP スヌーピングとは、DHCP サーバになりすました悪意あるホストによって IP アドレス（および関連する設定）が DHCP クライアントに割り当てられるのを防ぐためのメカニズムです。さらに、DHCP スヌーピングには、DHCP サーバに対するある種の DoS 攻撃を防止する働きもあります。

DHCP スヌーピングを使用するには、ポートの信頼状態を設定する必要があります。この設定を使用して、信頼できる DHCP サーバと信頼できない DHCP サーバが区別されます。

さらに、DHCP スヌーピングは、DHCP サーバによって割り当てられた IP アドレスを学習するようになっているので、インターフェイスへの IP アドレスの割り当てに DHCP が使用されるときに、他のセキュリティ機能（たとえば、ダイナミック ARP インスペクションや IP ソース ガード）を機能させることができます。

詳細については、第 12 章「DHCP スヌーピングの設定」を参照してください。

ダイナミック ARP インスペクション（DAI）

ダイナミック ARP インスペクション（DAI）とは、有効な ARP 要求と応答だけが中継されるようにするための機能です。信頼できないポート上でのすべての ARP 要求と応答は、この機能によって代行受信されます。代行受信されたパケットが有効な IP-to-MAC アドレス バインディングを持つことが検証されると、ローカル ARP キャッシュが更新されるか、適切な宛先にパケットが転送されます。この機能がイネーブルのときは、無効な ARP パケットはドロップされます。

詳細については、第 13 章「Dynamic ARP Inspection の設定」を参照してください。

IPSG

IP ソース ガードとは、インターフェイス単位のトラフィック フィルタです。パケットの IP アドレスと MAC アドレスが、次に示す 2 つの送信元のいずれかに一致する場合にのみ IP トラフィックを許可します。

- DHCP スヌーピング バインディング内の IP アドレスと MAC アドレス
- 管理者が設定したスタティック IP ソース エントリ

詳細については、第 14 章「IP ソース ガードの設定」を参照してください。

CHAPTER 2

ユーザ アカウントの管理

この章では、ユーザ アカウントを設定する方法を説明します。内容は次のとおりです。

ユーザ アカウントについて

Cisco Nexus 1000V にアクセスするには、ユーザ アカウントをセットアップする必要があります。このユーザ アカウントによって、各ユーザに許可される具体的なアクションが定義されます。ユーザ アカウントは最大 256 個作成できます。各ユーザ アカウントには、次の情報が含まれています。

ロール

ロールとは、同じグループのユーザによって共有可能なアクションを具体的に定義する規則の集合です。たとえば、次のような幅広い権限を持つロールをユーザ アカウントに割り当てることができます。これらのロールは Cisco Nexus 1000V 内であらかじめ定義されたものであり、変更はできません。

```
role: network-admin
  description: Predefined network admin role has access to all commands
  on the switch
  ------------------------------------------------------------------
  Rule    Perm    Type        Scope               Entity
  ------------------------------------------------------------------
  1       permit  read-write

role: network-operator
```

```
  description: Predefined network operator role has access to all read
  commands on the switch
  ------------------------------------------------------------------
  Rule    Perm    Type        Scope               Entity
  ------------------------------------------------------------------
  1       permit  read
```

管理者は、ユーザのアクセス権を定義するロールをこの他に 64 個作成できます。

各ユーザ アカウントには少なくとも 1 つのロールを割り当てる必要があり、最大 64 個を割り当てることができます。

管理者が作成できるロールでは、アクセスを許可できるコマンドがデフォルトでは次のものに限られています。機能の設定をユーザに許可するには、規則を追加する必要があります。

- **show**
- **exit**
- **end**
- **configure terminal**

表 2-1 に、ロールを構成するコンポーネントの説明を示します。

表 2-1　ロールのコンポーネント

コンポーネント	説明

ルール	定義済みロール基準の 1 つ（たとえば、許可または拒否するコマンド）。各ロールには最大 256 個の規則を追加できます。
	事前定義されているロールの規則は次のとおりです。
	• **role: network-admin**
	`Rule Perm Type Scope Entity`
	`1 permit read-write`
	• **role: network-operator**
	`Rule Perm Type Scope Entity`
	`1 permit read-only`

機能	個々の機能（syslog や TACACS+ など）。この機能に対するアクセス権を規則の中で定義することができます。使用可能な機能の一覧を表示するには、**show role feature** コマンドを使用します。
機能グループ	機能をグループ化したもの。このグループに対するアクセス権を規則の中で定義することができます。このグループは、最大 64 個作成できます。使用可能な機能グループの一覧を表示するには、**show role feature-group** コマンドを使用します。
コマンド	単一のコマンド、または 1 つの正規表現で表現されるコマンドの集合。このコマンドに対するアクセス権を規則の中で定義することができます。 コマンドへのアクセスを許可するロールは、そのコマンドへのアクセスを拒否するロールよりも優先されます。たとえば、あるユーザに割り当てられているロールの 1 つではコンフィギュレーション コマンドへのアクセスが拒否されているけれども、このユーザに割り当てられた別のロールでそのコマンドへのアクセスが許可されている場合は、アクセスは許可されます。

ユーザ名

ユーザ名とは、個々のユーザを特定するための一意の文字列です（たとえば「daveGreen」）。ユーザ名は、最大 28 文字で、英数字を使用でき、大文字と小文字が区別されます。数字だけで構成されたユーザ名は許可されません。AAA サーバに数字だけのユーザ名が存在する場合、ログイン時に入力しても、そのユーザはログインできません。

パスワード

パスワードは、大文字と小文字が区別される文字列です。パスワードによって特定のユーザによるアクセスが可能になり、不正なアクセスの防止に役立ちます。パスワードを指定せずにユーザを追加することもできますが、そのユーザはデバイスにアクセスできなくなる可能性があります。パスワードは、強力なものでなければなりません。容易に推測できるパスワードは、不正アクセスの原因となります。

次の文字は、クリア テキスト パスワードには使用できません。

- ドル記号（$）
- スペース

次の特殊文字は、パスワードの先頭には使用できません。

- 引用符（" および '）
- 縦線（|）
- 右山カッコ（>）

表 2-2 に、強力なパスワードの特性を示します。

表 2-2　強力なパスワードの特性

強力なパスワードに含まれるもの	強力なパスワードに含まれないもの
• 最低 8 文字 • 大文字の英字 • 小文字の英字 • 数字 • 特殊文字	• 連続する文字（例：abcd） • 文字の繰り返し（例：aaabbb） • 辞書に載っている単語 • 固有名詞

強固なパスワードの例を次に示します。

- If2CoM18
- 2004AsdfLkj30
- Cb1955S21

パスワード強度のチェック

デバイスによるパスワード強度のチェックは、デフォルトでは自動的に行われます。管理者がユーザ名とパスワードを追加するときに、パスワードの強度が評価されます。パスワードの強度が低い場合は、次に示すエラー メッセージが表示されます。

```
n1000v# config t
n1000v(config)# username daveGreen password davey
password is weak
```

```
Password should contain characters from at least three of the classes:
 lower case letters,upper case letters, digits, and special characters
```

パスワード強度チェックはディセーブルにすることができます。

有効期限

デフォルトでは、ユーザ アカウントは無期限に有効です。ただし、管理者はアカウントがディセーブルになる有効期限を明示的に設定することができます。

注意事項および制約事項

ユーザ アクセスに関する注意事項と制約事項は次のとおりです。

- あらかじめ定義された 2 つのユーザ ロールに加えて、最大 64 個のロールを作成できます。
- 1 つのユーザ ロールに最大 256 個の規則を作成できます。
- 最大 64 個の機能グループを作成できます。
- 最大 256 人のユーザを追加できます。
- 1 つのユーザ アカウントに最大 64 個のユーザ ロールを割り当てられます。
- ローカル ユーザ アカウントと同じ名前のリモート ユーザ アカウントが AAA サーバ上に存在する場合は、そのリモート ユーザには AAA サーバ上で設定されているユーザ ロールでなく、ローカル ユーザ アカウントのユーザ ロールが適用されます。

デフォルト設定

表 2-3 に、ユーザ アクセスのデフォルト設定を示します。

表 2-3　ユーザ アクセスのデフォルト

パラメータ	デフォルト
ユーザ アカウント パスワード	未定義
ユーザ アカウントの有効期限	なし
ユーザ アカウント ロール	network-operator
インターフェイス ポリシー	すべてのインターフェイスがアクセス可能
VLAN ポリシー	すべての VLAN がアクセス可能

ユーザ アクセスの設定

ここでは、次の内容について説明します。

- 「機能グループの作成」（P.2-11）
- 「インターフェイス アクセスの設定」（P.2-12）
- 「VLAN アクセスの設定」（P.2-14）

パスワード強度チェックのイネーブル化

ここでは、強度の低いパスワードの作成を防ぐための Cisco Nexus 1000V によるパスワード強度チェックをイネーブルにする手順を説明します。

はじめる前に

この手順を開始する前に、次のことを確認または実行しておく必要があります。

- EXEC モードで CLI にログインしていること。
- パスワード強度のチェックは、デフォルトではイネーブルになっています。ディセーブルにされていても、ここで説明する手順を実行すれば再度イネーブルにすることができます。

手順の概要

1. **config t**
2. **password strength-check**
3. **show password strength-check**
4. **copy running-config startup-config**

手順の詳細

	コマンド	目的

ステップ 1	**config t**
	
	Example:
	`n1000v# config t`
	`n1000v(config)#`
		CLI 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	**password strength-check** **Example:** `n1000v(config)# password strength-check`	パスワードの強度確認をイネーブルにします。デフォルトはイネーブルです。 パスワード強度のチェックをディセーブルにするには、このコマンドの **no** 形式を使用します。

ステップ 3	**show password strength-check**
	
	Example:
	`n1000v# show password strength-check`
	`Password strength check enabled`
	`n1000v(config)#`
		（任意）パスワード強度チェックの設定を表示します。

ステップ 4	**copy running-config startup-config** **Example:** `n1000v# copy running-config startup-config`	（任意）リブート後に永続的な実行コンフィギュレーションを保存し、スタートアップ コンフィギュレーションにコピーして再起動します。

パスワード強度チェックのディセーブル化

ここでは、パスワード強度のチェックをディセーブルにする手順を説明します。

はじめる前に

この手順を開始する前に、次のことを確認または実行しておく必要があります。

- EXEC モードで CLI にログインしていること。
- パスワード強度のチェックは、デフォルトではイネーブルになっています。この手順を使用すると、ディセーブルにすることができます。

手順の概要

1. **config t**
2. **no password strength-check**
3. **show password strength-check**
4. **copy running-config startup-config**

手順の詳細

	コマンド	目的

ステップ 1	**config t**
	
	Example:
	`n1000v# config t`
	`n1000v(config)#`
		CLI 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 password strength-check**
	
	Example:
	`n1000v(config)# no password strength-check`
	`n1000v(config)#`
		パスワード強度のチェックをディセーブルにします。
		デフォルトはイネーブルです。

ステップ 3	**show password strength-check**
	
	Example:
	`n1000v# show password strength-check`
	`Password strength check not enabled`
	`n1000v(config)#`
		（任意）パスワード強度チェックの設定を表示します。

ステップ 4	**copy running-config startup-config** **Example:** `n1000v# copy running-config startup-config`	（任意）リブート後に永続的な実行コンフィギュレーションを保存し、スタートアップ コンフィギュレーションにコピーして再起動します。

ユーザ アカウントの作成

ここでは、ユーザ アカウントを作成して設定する手順を説明します。このアカウントによって、Cisco Nexus 1000V に対するアクセス権が定義されます。

はじめる前に

この手順を開始する前に、次のことを確認または実行しておく必要があります。

- EXEC モードで CLI にログインしていること。
- ユーザ アカウントは最大 256 個追加できます。
- ユーザ アカウントに対する変更が有効になるのは、そのユーザがログインして新しいセッションを作成したときです。
- 次に示す語をユーザ アカウントで使用しないでください。これらは、他の目的のために予約されています。

adm	gdm	mtsuser	rpcuser
bin	gopher	news	shutdown
daemon	haltlp	nobody	sync
ftp	mail	nscd	sys
ftpuser	mailnull	operator	uucp
games	man	rpc	xfs

- 追加するユーザ パスワードは、クリア テキストと暗号化テキストのどちらでも指定できます。
  - クリア テキストのパスワードは、実行コンフィギュレーションに保存される前に暗号化されます。
  - 暗号化されたパスワードは、それ以上の暗号化を行わずに実行コンフィギュレーションに保存されます。
- 1 つのユーザ アカウントが最大 64 個のロールを持つことができますが、少なくとも 1 つのロールを持つ必要があります。ロールの詳細については、「ロール」（P.2-1）を参照してください。
- 管理者がパスワードを指定しない場合は、そのユーザがログインできなくなる可能性があります。
- パスワードでなく SSH 公開キーを使用する手順については、「公開キーを持つユーザ アカウントの設定」（P.7-5）を参照してください。

手順の概要

1. **config t**
2. **show role**
3. **username** *user-name* **[password [0 | 5]***password***] [expire** *date***] [role** *role-name***]**
4. **show user-account** *user-name*
5. **copy running-config startup-config**

手順の詳細

	コマンド	目的
ステップ 1	**config t** **Example:** n1000v# config t n1000v(config)#	CLI 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	**show role** **Example:** n1000v(config)# show role	（任意）ユーザに割り当てることのできるロールを表示します。 新しいユーザ ロールを作成する場合は、「ロールの作成」（P.2-9）の手順を使用してください。
ステップ 3	**username** *name* [**password** [**0** | **5**] *password*] [expire date] [role *role-name*] **Example:** n1000v(config)# username NewUser password 4Ty18Rnt	ユーザ アカウントを作成します。 • **name**：最大 28 文字の英数字ストリングです。大文字と小文字が区別されます。 • **password**：デフォルト パスワードは未定義です。 – **0** =（デフォルト）入力するパスワードがクリア テキストであることを指定します。Cisco Nexus 1000V は、クリア テキストのパスワードを実行コンフィギュレーションに保存する前に暗号化します。 例では、実行コンフィギュレーションのパスワード **4Ty18Rnt** は password 5 形式で暗号化されています。 – **5** = 入力するパスワードがすでに暗号化形式であることを指定します。Cisco Nexus 1000V は、パスワードを実行コンフィギュレーションに保存する前に暗号化しません。 ユーザのパスワードは、設定ファイルでは表示されません。 • **expire date**：YYYY-MM-DD。デフォルトは無期限です。 • **role**：少なくとも 1 つのロールを割り当てる必要があります。最大 64 個のロールを割り当てることができます。デフォルトのロールは、**network-operator** です。

	コマンド	目的

ステップ 4	**show user-account** *username*
	
	Example:
	`n1000v(config)# show user-account NewUser`
	`user:NewUser`
	`  this user account has no expiry date`
	`  roles:network-operator network-admin`
	`n1000v(config)#`
		新しいユーザ アカウントの設定を表示します。

ステップ 5	**copy running-config startup-config** **Example:** `n1000v# copy running-config startup-config`	（任意）リブート後に永続的な実行コンフィギュレーションを保存し、スタートアップ コンフィギュレーションにコピーして再起動します。

ロールの作成

ここでは、許可または拒否する具体的なアクションのセットを定義するロールを作成します。このロールは、定義されているアクションに一致するアクセス権を必要とするユーザに割り当てます。

はじめる前に

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。

- EXEC モードで CLI にログインしていること。
- 最大 64 個のユーザ ロールを設定できます。
- 1 つのロールに最大 256 個の規則を設定できます。
- 1 つのロールを複数のユーザに割り当てることができます。
- 規則番号は、その規則が適用される順序を表します。規則は番号の降順で適用されます。たとえば、あるロールに 3 つの規則がある場合は、最初に規則 3 が適用され、次に規則 2、最後に規則 1 が適用されます。
- デフォルトでは、管理者が作成するユーザ ロールでアクセスを許可できるコマンドは、**show**、**exit**、**end**、および **configure terminal** コマンドだけです。機能の設定をユーザに許可するには、規則を追加する必要があります。

手順の概要

1. **config t**
2. **role name** *role-name*
3. （任意）**description** *string*
4. **rule** *number* {**deny** | **permit**} **command** *command-string*

   rule *number* {**deny** | **permit**} {**read** | **read-write**}

   rule *number* {**deny** | **permit**} {**read** | **read-write**} **feature** *feature-name*

   rule *number* {**deny** | **permit**} {**read** | **read-write**} **feature-group** *group-name*
5. 手順 4. を繰り返して、このロールに必要なルールをすべて作成します。
6. **show role**
7. **copy running-config startup-config**

手順の詳細

	コマンド	目的
ステップ 1	**config t** **Example:** n1000v# config t n1000v(config)#	CLI 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	**role name** *role-name* **Example:** n1000v(config)# role name UserA n1000v(config-role)#	ユーザ ロールの名前を指定して、そのロールのロール コンフィギュレーション モードを開始します。 名前は最大 16 文字の英数字ストリングです。大文字と小文字が区別されます。
ステップ 3	**description** *description-string* **Example:** n1000v(config-role)# description Prohibits use of clear commands	（任意）ロールの説明を設定します。説明にはスペースを含めることができます。
ステップ 4	**rule** *number* {**deny** | **permit**} **command** *command-string* **Example:** n1000v(config-role)# rule 1 deny command clear users	特定のコマンドを許可または拒否する規則を作成します。 指定するコマンドには、スペースや正規表現を含めることができます。たとえば、「interface ethernet *」と指定すると、すべてのイーサネット インターフェイスへのアクセスが許可または拒否されます。 この例の規則では、**clear users** コマンドへのアクセスが拒否されます。
	rule *number* {**deny** | **permit**} {**read** | **read-write**} **Example:** n1000v(config-role)# rule 2 deny read-write	あらゆる操作を許可または拒否するための包括的規則を作成します。 この例の規則では、どの操作に対しても読み取りアクセスだけが許可されます。
	rule *number* {**deny** | **permit**} {**read** | **read-write**} **feature** *feature-name* **Example:** n1000v(config-role)# rule 3 permit read feature eth-port-sec	機能アクセスの規則を作成します。 **show role feature** コマンドを実行すると、使用可能な機能の一覧が表示されます。 この例の規則では、イーサネット ポート セキュリティ機能に対する読み取り専用アクセスがユーザに許可されます。
	rule *number* {**deny** | **permit**} {**read** | **read-write**} **feature-group** *group-name* **Example:** n1000v(config-role)# rule 4 deny read-write feature-group eth-port-sec	機能グループ アクセスの規則を作成します。 **show role feature-group** コマンドを使用すれば、機能グループのリストが表示されます。 この例の規則では、特定の機能グループへのアクセスが拒否されます。
ステップ 5	ステップ 4 を繰り返して、指定したロールに必要な規則をすべて作成します。	

	コマンド	目的
ステップ 6	**show role** **Example:** `n1000v(config)# show role`	（任意）ユーザ ロールの設定を表示します。
ステップ 7	**copy running-config startup-config** **Example:** `n1000v(config)# copy running-config startup-config`	（任意）リブート後に永続的な実行コンフィギュレーションを保存し、スタートアップ コンフィギュレーションにコピーして再起動します。

機能グループの作成

ここでは、機能グループを作成して設定する手順を説明します。

はじめる前に

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。

- EXEC モードで CLI にログインしていること。
- 最大 64 個のカスタム機能グループを作成できます。

手順の概要

1. **config t**
2. **role feature-group name** *group-name*
3. show role feature
4. **feature** *feature-name*
5. 機能グループに追加するすべての機能について、4. を繰り返します。
6. **show role feature-group**
7. **copy running-config startup-config**

手順の詳細

	コマンド	目的

ステップ 1	**config t**
	
	Example:
	`n1000v# config t`
	`n1000v(config)#`
		CLI 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	**role feature-group name** *group-name*
	
	Example:
	`n1000v(config)# role feature-group name GroupA`
	`n1000v(config-role-featuregrp)#`
		グループ名を指定して、そのグループのロール機能グループ コンフィギュレーション モードを開始します。
		• **group-name**：最大 32 文字の英数字ストリングです。大文字と小文字が区別されます。

	コマンド	目的
ステップ 3	**show role feature** **Example:** n1000v(config-role-featuregrp)# **show role feature** feature: aaa feature: access-list feature: cdp feature: install . . . n1000v(config-role-featuregrp)#	機能グループを定義するときに使用できる機能の一覧を表示します。
ステップ 4	**feature** *feature-name* **Example:** n1000v(config-role-featuregrp)# feature syslog n1000v(config-role-featuregrp)#	機能を機能グループに追加します。
ステップ 5	機能グループに追加するすべての機能について、ステップ 6 を繰り返します。	
ステップ 6	**show role feature-group** **Example:** n1000v(config-role-featuregrp)# show role feature-group feature group: GroupA feature: syslog feature: snmp feature: ping n1000v(config-role-featuregrp)#	（任意）機能グループの設定を表示します。
ステップ 7	**copy running-config startup-config** **Example:** n1000v(config-role-featuregrp)# copy running-config startup-config	（任意）リブート後に永続的な実行コンフィギュレーションを保存し、スタートアップ コンフィギュレーションにコピーして再起動します。

インターフェイス アクセスの設定

ここでは、特定のロールのインターフェイス アクセスを設定する手順を説明します。

はじめる前に

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。

- EXEC モードで CLI にログインしていること。
- 「ロールの作成」（P.2-9）の手順 を使用してユーザ ロールが 1 つ以上作成済みであるものとします。この手順では、作成済みのロールに変更を加えます。
- デフォルトでは、ロールによってすべてのインターフェイスへのアクセスが許可されます。この手順では、すべてのインターフェイスへのアクセスを拒否してから、特定のインターフェイスへのアクセスを許可します。

手順の概要

1. **config t**
2. **role name** *role-name*

3. **interface policy deny**
4. **permit interface** *interface-list*
5. **show role**
6. **copy running-config startup-config**

手順の詳細

	コマンド	目的
ステップ 1	**config t** **Example:** n1000v# config t n1000v(config)#	CLI 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	**role name** *role-name* **Example:** n1000v(config)# role name network-observer n1000v(config-role)#	ユーザ ロールを指定して、そのロールのロール 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	**interface policy deny** **Example:** n1000v(config-role)# interface policy deny n1000v(config-role-interface)#	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、このロールによるすべてのインターフェイス アクセスを拒否します。 これで、**permit interface** コマンドを使用して明示的に定義しない限り、このロールはインターフェイスに一切アクセスできなくなりました。
ステップ 4	**permit interface** *interface-list* **Example:** n1000v(config-role-interface)# permit interface ethernet 2/1-4	このロールに割り当てられたユーザにアクセスを許可するインターフェイスを指定します。 このロールに割り当てられたユーザにアクセスを許可するインターフェイスがすべて指定されるまで、このコマンドを繰り返します。

ステップ 5	**show role** *role-name*
	
	Example:
	n1000v(config-role-interface)# show role name network-observer
	
	role: network-observer
	  description: temp
	  Vlan policy: permit (default)
	  Interface policy: deny
	  Permitted interfaces: Ethernet2/1-4
		（任意）ロールの設定を表示します。

ステップ 6	**copy running-config startup-config** **Example:** n1000v(config-role-featuregrp)# copy running-config startup-config	（任意）リブート後に永続的な実行コンフィギュレーションを保存し、スタートアップ コンフィギュレーションにコピーして再起動します。

VLAN アクセスの設定

ここでは、特定のロールの VLAN アクセスを定義する手順を説明します。

はじめる前に

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。

- EXEC モードで CLI にログインしていること。
- 「ロールの作成」（P.2-9）の手順 を使用してユーザ ロールが 1 つ以上作成済みであるものとします。この手順では、作成済みのロールに変更を加えます。
- デフォルトでは、すべての VLAN へのアクセスが許可されます。この手順では、すべての VLAN へのアクセスを拒否してから、特定の VLAN へのアクセスを許可します。

手順の概要

1. **config t**
2. **role name** *role-name*
3. **vlan policy deny**
4. **permit vlan** *vlan-range*
5. **exit**
6. **show role**
7. **copy running-config startup-config**

手順の詳細

	コマンド	目的

ステップ 1	**config t**
	
	Example:
	`n1000v# config t`
	`n1000v(config)#`
		CLI 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	**role name** *role-name*
	
	Example:
	`n1000v(config)# role name network-observer`
	`n1000v(config-role)#`
		ユーザ ロールを指定し、ロール 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	**vlan policy deny**
	
	Example:
	`n1000v(config-role)# vlan policy deny`
	`n1000v(config-role-vlan)#`
		VLAN コンフィギュレーション モードを開始し、このロールによるすべての VLAN アクセスを拒否します。
		これで、**permit vlan** コマンドを使用して明示的に定義しない限り、このロールは VLAN に一切アクセスできなくなりました。

ステップ 4	**permit vlan** *vlan-list* **Example:** `n1000v(config-role-vlan)# permit vlan 1-4`	このロールに割り当てられたユーザにアクセスを許可する VLAN を指定します。 このロールに割り当てられたユーザにアクセスを許可する VLAN がすべて指定されるまで、このコマンドを繰り返します。

	コマンド	目的

ステップ 5	**show role** *role-name*
	
	Example:
	n1000v(config-role)# show role network-observer
	
	role: network-observer
	  description: temp
	  Vlan policy: deny
	  Permitted vlans: vlan 1-4
	  Interface policy: deny
	  Permitted interfaces: Ethernet2/1-4
		（任意）ロールの設定を表示します。

ステップ 6	**copy running-config startup-config** **Example:** n1000v(config-role)# copy running-config startup-config	（任意）リブート後に永続的な実行コンフィギュレーションを保存し、スタートアップ コンフィギュレーションにコピーして再起動します。

ユーザ アクセス設定の確認

ユーザ アカウントおよび RBAC 設定情報を表示するには、次のいずれかの作業を行います。

コマンド	目的
show role	使用可能なユーザ ロールとその規則を表示します。
show role feature	使用可能な機能のリストを表示します。
show role feature-group	使用可能な機能グループのリストを表示します。
show startup-config security	スタートアップ コンフィギュレーションのユーザ アカウント設定を表示します。
show running-config security [**all**]	実行コンフィギュレーションのユーザ アカウント設定を表示します。**all** キーワードを指定すると、ユーザ アカウントのデフォルト値が表示されます。
show user-account	ユーザ アカウント情報を表示します。

構成例

次に、ロールを設定する例を示します。

```
role name UserA
  rule 3 permit read feature snmp
  rule 2 permit read feature dot1x
  rule 1 deny command clear *
```

次に、機能グループを設定する例を示します。

```
role feature-group name Security-features
  feature radius
  feature tacacs
  feature dot1x
  feature aaa
  feature snmp
  feature acl
  feature access-list
```

その他の関連資料

RBAC の実装に関連する詳細情報については、次を参照してください。

- 「関連資料」（P.2-16）
- 「標準」（P.2-16）
- 「管理情報ベース（MIB）」（P.2-16）

関連資料

関連項目	参照先
ユーザ アクセスのコマンド	『*Cisco Nexus 1000V Command Reference, Release 4.2(1)SV1(4a)*』
スイッチ上のユーザの管理	『*Cisco Nexus 1000V Getting Started Guide, Release 4.2(1)SV1(4a)*』

標準

標準	タイトル
この機能でサポートされる新規の標準または変更された標準はありません。また、既存の標準のサポートは変更されていません。	—

管理情報ベース（MIB）

MIB	MIB のリンク
• CISCO-COMMON-MGMT-MIB	MIB を検索およびダウンロードするには、次の URL にアクセスしてください。 http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml

ユーザ アカウント機能の履歴

ここでは、ユーザ アカウントのリリース履歴を示します。

機能名	リリース	機能情報
ユーザ アカウント	4.0(4)SV1(1)	この機能が導入されました。

CHAPTER 3

VSD の設定

この章では、VSD を設定する方法を説明します。内容は次のとおりです。

仮想サービス ドメインについて

仮想サービス ドメイン（VSD）を使用すると、ネットワーク サービスのためのトラフィックの分類と分離が可能になります。このネットワーク サービスの例としては、ファイアウォールやトラフィック監視があり、その他にコンプライアンス目標（たとえば Sarbanes Oxley）の達成支援のためのサービスなどがあります。

サービス仮想マシン

Service VM（SVM; サービス仮想マシン）は、専門サービス、たとえばファイアウォール、ディープ パケット インスペクション（アプリケーション認識型ネットワーキング）、監視などを実行します。各 SVM には、次の 3 つの仮想インターフェイスがあります。

インターフェイス	説明
管理	SVM を管理する標準のインターフェイス 用途に応じて、レイヤ 2 またはレイヤ 3 接続を必要とします。

インターフェイス	説明
着信	VSD に着信するトラフィックを保護します。 VSD に着信するパケットはすべて、このインターフェイスを通過する必要があります。
発信	VSD から外部に発信されるトラフィックを保護します。 VSD から外部に発信されるパケットはすべて、SVM を通過する必要があり、発信インターフェイスから送出されます。

これらのインターフェイスでの送信元 MAC 学習は行われません。SVM はそれぞれ、セキュアな VSD を作成します。VSD 内のインターフェイスは、SVM によって防御されます。

ポート プロファイル

VSD は、セキュリティ サービスを実行する SVM によって保護されるインターフェイスの集合です。VSD に着信するトラフィックや VSD から発信されるトラフィックはすべて、SVM を通過する必要があります。

トラフィックの発信元と宛先の両方が同じ VSD の中にある場合は、そのトラフィックは安全と見なされるので、SVM を経由する必要はありません。

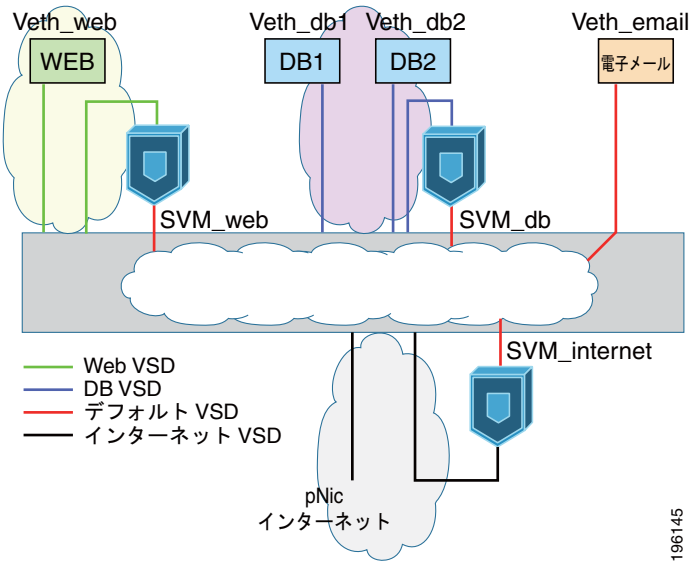
VSD を形成するには、次のポート プロファイルを作成します。

ポート プロファイル	説明
内側	VSD メンバーが発信元であるトラフィックは、内側ポートを通って SVM に入り、外側ポートから出て宛先へ転送されます。
外側	宛先が VSD メンバーであるトラフィックは、外側ポートを通って SVM に入り、内側ポートから出て宛先へ転送されます。
メンバ	個々の内側 VM が存在する場所。

図 3-1 では、ただ 1 つの VEM がいくつもの vswitch の役割を果たしています。SVM によって次の VSD が定義されます。

VSD	SVM（保護）	内側ポート プロファイル	外側ポート プロファイル	メンバー ポート プロファイル
DB VSD	SVM_db	SVM_db_inside	SVM_db_outside	vEth_db1 vEth_db2
Web VSD	SVM_web	SVM_web_inside	SVM_web_outside	vEth_web
インターネット VSD	SVM_Internet	SVM_internet_inside	SVM_internet_outside	
デフォルト		SVM VSD		vEth Email

図 3-1　仮想サービス ドメイン（VSD）の例



注意事項および制約事項

仮想サービス ドメイン（VSD）に関する注意事項と制約事項は次のとおりです。

- トラフィックの遅延を防ぐために、トラフィックのセキュリティ維持の手段は VSD だけを使用してください。
- ホストあたり最大 6 個の VSD を設定できます。VSM 上には最大 64 個を設定できます。
- VSD あたり最大 214 個のインターフェイスが 1 つのホスト上でサポートされ、VSM 上では 2048 個のインターフェイスがサポートされます。
- Vmotion は、SVM に対してはサポートされないので、ディセーブルにしてください。
- VSM リロードやネットワーク中断の後にネットワーク ループが発生するのを防ぐには、SVM のすべてのポート プロファイルにおいて制御 VLAN とパケット VLAN をディセーブルにする必要があります。
- SVM に対して設定されたポート プロファイルにサービス ポートが指定されていない場合は、ネットワーク上でパケット フラッディングが発生します。
- SVM に対してポート プロファイルを設定するときは、初めにその SVM を停止させてください。このようにすれば、ポート プロファイルがサービス ポートを持たないように誤って設定されても、ネットワーク上でパケット フラッディングが発生することはありません。設定と確認が完了したら、SVM を再び稼動させます。
- VShield 4.1 は VSD をサポートしません。VSD 機能は、VShield 4.1 とともに使用する場合は予想どおりに機能しません。

デフォルト設定

次の表に、Telnet のデフォルトを示します。

パラメータ	デフォルト
service-port default-action	forward
switchport trunk allowed vlan	all

VSD の設定

ここでは、次の手順について説明します。

- 「内側または外側 VSD ポート プロファイルの設定」（P.3-4）
- 「メンバー VSD ポート プロファイルの設定」（P.3-7）

内側または外側 VSD ポート プロファイルの設定

ここでは、SVM に入る接続および SVM から出る接続を定義するポート プロファイルを設定する手順を説明します。

はじめる前に

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。

- EXEC モードで CLI にログインしていること。
- 設定エラーによるネットワークのフラッディングを防ぐために、SVM を停止させてください。設定と確認が完了したら、SVM を再び稼動させます。
- サービス ポートが設定されていない場合は、SVM は通常の VM として起動するので、ネットワーク上でパケット フラッディングが発生します。
- 選択 VLAN フィルタリングは、このコンフィギュレーションではサポートされません。代わりに、デフォルトを使用してください。デフォルトでは、すべての VLAN がポート上で許可されます。

手順の概要

1. **config t**
2. **port-profile** *name*
3. **switchport mode trunk**
4. **switchport trunk allowed vlan** *vlanID*
5. **virtual-service-domain** *name*
6. **no shut**
7. **vmware port-group** *pg-name*
8. **service-port** {**inside** | **outside**} [**default-action** {**drop** | **forward**}]
9. **state enabled**
10. **show virtual-service-domain** *name*

11. **copy running-config startup-config**

手順の詳細

	コマンド	目的

ステップ 1	**config t**
	
	Example:
	`n1000v# config t`
	`n1000v(config)#`
		CLI 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	**port-profile** *name*
	
	Example:
	`n1000v(config)# port-profile webserver-inside`
	`n1000v(config-port-profile)#`
		ポート プロファイルを作成し、このポート 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。
		ポート プロファイルには最大 80 文字の名前を設定できます。ポート プロファイル名は、Cisco Nexus 1000V 上の各ポート プロファイルに対して一意である必要があります。

ステップ 3	**switchport mode trunk**
	Example:
	`n1000v(config-port-profile)# switchport mode trunk`
	`n1000v(config-port-profile)#`
		インターフェイスがスイッチ トランク ポートであることを指定します。

ステップ 4	**switchport trunk allowed vlan** *vlanID*
	Example:
	`n1000v(config-port-profile)# switchport trunk allowed vlan all`
	`n1000v(config-port-profile)#`
		すべての VLAN をポート上で許可します。

ステップ 5	**virtual-service-domain** *name*
	Example:
	`n1000v(config-port-profile)# virtual-service-domain vsd1-webserver`
	`n1000v(config-port-profile)#`
		このポート プロファイルに VSD 名を追加します。

ステップ 6	**no shutdown**
	Example:
	`n1000v(config-port-prof)# no shutdown`
	`n1000v(config-port-prof)#`
		管理上の目的でプロファイル内のすべてのポートをイネーブルにします。

ステップ 7	**vmware port-group** *pg-name*
	Example:
	`n1000v(config-port-prof)# vmware port-group webservers-inside-protected`
	`n1000v(config-port-prof)#`
		VMware ポート グループとしてポート プロファイルを指定します。
		ポート プロファイルは、同じ名前の VMware ポート グループにマッピングされます。vCenter Server 接続が確立すると、Cisco Nexus 1000V で作成されたポート グループは、vCenter Server の仮想スイッチに配信されます。
		name：ポート グループ名。pg-name を指定しない場合、ポート グループ名は、ポート プロファイル名と同じになります。ポート プロファイルを異なるポート グループ名にマッピングする場合は、pg-name オプションのあとに別の名前を続けます。

	コマンド	目的
ステップ 8	**service-port** {**inside** | **outside**} [**default-action** {**drop** | **forward**}]	インターフェイスを内側（inside）または外側（outside）として設定するとともに、サービス ポートがダウンした場合にパケットを転送するかドロップするかを指定します（default-action）。 default-action を省略すると、デフォルトでは **forward** 設定が使用されます。 **注意**　サービス ポートが設定されていない場合は、SVM は通常の VM として起動するので、ネットワーク上でパケット フラッディングが発生します。

	Example:
	`n1000v(config-port-prof)# service-port inside default-action forward`
	`n1000v(config-port-prof)#`
		この例では、内側 VSD を設定します。この VSD では、サービス ポートがダウンした場合にパケットは転送されます。

	Example:
	`n1000v(config-port-prof)# service-port outside default-action forward`
	`n1000v(config-port-prof)#`
		この例では、外側 VSD を設定します。この VSD では、サービス ポートがダウンした場合にパケットは転送されます。

ステップ 9	**state enabled**
	Example:
	`n1000v(config-port-prof)# state enabled`
	`n1000v(config-port-prof)#`
		VSD ポート プロファイルをイネーブルにします。
		このポート プロファイルの設定が、割り当てられたポートに適用されます。また、vCenter Server 上の VMware vSwitch 内にポート グループが作成されます。

ステップ 10	**show virtual-service-domain** *name*
	Example:
	`n1000v(config-port-prof)# show virtual-service-domain vsd1-webserver`
	`Default Action: forward`
	`_____________________________`
	`Interface  Type`
	`_____________________________`
	`Vethernet1  Member`
	`Vethernet2  Member`
	`Vethernet3  Member`
	`Vethernet7  Inside`
	`Vethernet8  Outside`
	`n1000v(config-port-prof)#`
		（任意）この VSD ポート プロファイルの設定を表示します。この表示を使用して、ポート プロファイルが正しく設定されていること確認します。

ステップ 11	**copy running-config startup-config**
	Example:
	`n1000v(config-port-prof)# copy running-config startup-config`
	`[########################################] 100%`
	`n1000v(config-port-prof)#`
		（任意）リブート後に永続的な実行コンフィギュレーションを保存し、スタートアップ コンフィギュレーションにコピーして再起動します。

メンバー VSD ポート プロファイルの設定

ここでは、個々のメンバーが存在する場所である VSD ポート プロファイルを設定する手順を説明します。

はじめる前に

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。

- EXEC モードで CLI にログインしていること。
- メンバー VSD ポート プロファイルを SVM に対して設定しないでください。

  メンバー VSD ポート プロファイルはサービス ポートを持たないので、SVM に対して設定されると、ネットワーク上でパケット フラッディングが発生します。

手順の概要

1. **config t**
2. **port-profile** *name*
3. **switchport access vlan** *vlanID*
4. **switchport trunk allowed vlan** *vlanID*
5. **virtual-service-domain** *name*
6. **no shut**
7. **state enabled**
8. **show virtual-service-domain** *name*
9. **copy running-config startup-config**

手順の詳細

	コマンド	目的

ステップ 1	**config t**
	
	Example:
	`n1000v# config t`
	`n1000v(config)#`
		CLI 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 1	**port-profile** *name*
	
	Example:
	`n1000v(config)# port-profile vsd1-member`
	`n1000v(config-port-profile)#`
		ポート プロファイルを作成し、このポート 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。
		ポート プロファイルには最大 80 文字の名前を設定できます。ポート プロファイル名は、Cisco Nexus 1000V 上の各ポート プロファイルに対して一意である必要があります。

ステップ 2	**switchport access vlan** *vlanID*
	
	Example:
	`n1000v(config-port-profile)# switchport access vlan 315`
	`n1000v(config-port-profile)#`
		このポート プロファイルのアクセス ポートに VLAN ID を割り当てます。

	コマンド	目的

ステップ 3	**virtual-service-domain** *name*
	
	Example:
	`n1000v(config-port-profile)# virtual-service-domain vsd1-webserver`
	`n1000v(config-port-profile)#`
		VSD 名をこのポート プロファイルに割り当てます。

ステップ 4	**no shutdown**
	
	Example:
	`n1000v(config-port-prof)# no shutdown`
	`n1000v(config-port-prof)#`
		管理上の目的でプロファイル内のすべてのポートをイネーブルにします。

ステップ 5	**state enabled**
	
	Example:
	`n1000v(config-port-prof)# state enabled`
	`n1000v(config-port-prof)#`
		VSD ポート プロファイルをイネーブルにします。
		
		このポート プロファイルの設定が、割り当てられたポートに適用されます。また、vCenter Server 上の VMware vSwitch 内にポート グループが作成されます。

ステップ 6	**show virtual-service-domain** *name*
	
	Example:
	`n1000v(config-port-prof)# show virtual-service-domain vsd1-webserver`
	`Default Action: forward`
	
	`_____________________________`
	`Interface Type`
	
	`_____________________________`
	`Vethernet1 Member`
	`Vethernet2 Member`
	`Vethernet3 Member`
	`Vethernet6 Member`
	`Vethernet7 Inside`
	`Vethernet8 Outside`
	`n1000v(config-port-prof)#`
		（任意）この VSD ポート プロファイルの設定を表示します。この表示を使用して、ポート プロファイルが正しく設定されていること確認します。

ステップ 7	**copy running-config startup-config**
	
	Example:
	`n1000v(config-port-prof)# copy running-config startup-config`
	`[########################################] 100%`
	`n1000v(config-port-prof)#`
		（任意）リブート後に永続的な実行コンフィギュレーションを保存し、スタートアップ コンフィギュレーションにコピーして再起動します。

設定の確認

VSD 設定を表示するには、次のコマンドを使用します。

コマンド	目的
show virtual-service-domain name *vsd-name*	特定の VSD の設定を表示します。 例 3-1（P.3-9）を参照してください。
show virtual-service-domain brief	すべての VSD 設定の要約を表示します。 例 3-2（P.3-9）を参照してください。

コマンド	目的
show virtual-service-domain interface	すべての VSD のインターフェイス設定を表示します。 例 3-3（P.3-9）を参照してください。
module vem *module_number* **execute vemcmd show vsd**	VEM の VSD 設定を表示するために、リモートの Cisco Nexus 1000V から VEM にコマンドを送信します。 例 3-4（P.3-10）を参照してください。
module vem *module_number* **execute vemcmd show vsd ports**	VEM の VSD ポート設定を表示するために、リモートの Cisco Nexus 1000V から VEM にコマンドを送信します。 例 3-5（P.3-10）を参照してください。

これらのコマンドの出力の詳しい説明については、『*Cisco Nexus 1000V Command Reference, Release 4.2(1)SV1(4a)*』を参照してください。

例 3-1　show virtual-service-domain name *vsd_name*

```
n1000v## show virtual-service-domain name vsd1
Default Action: drop

_____________________________
Interface        Type
_____________________________
Vethernet1       Member
Vethernet2       Member
Vethernet3       Member
Vethernet6       Member
Vethernet7       Inside
Vethernet8       Outside

n1000v#
```

例 3-2　show virtual-service-domain brief

```
n1000v# show virtual-service-domain brief
Name   vsd-id    default action    in-ports   out-ports   mem-ports    Modules with
                                                                      VSD Enabled
zone    1         forward           1          1           2            4
n1000v#
```

例 3-3　show virtual-service-domain interface

```
n1000v# sho virtual-service-domain interface
_ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _
Name             Interface             Type      Status
_ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _
vsd1             Vethernet1            Member    Active
vsd1             Vethernet2            Member    Active
vsd1             Vethernet3            Member    Active
vsd1             Vethernet6            Member    Active
vsd1             Vethernet7            Inside    Active
vsd1             Vethernet8            Outside   Active
vsd2             Vethernet9            Inside    Active
vsd2             Vethernet10           Outside   Active
```

例 3-4　module *module_number* execute vemcmd show vsd

```
n1000v# module vem 4 execute vemcmd show vsd
ID Def_Act ILTL OLTL NMLTL State Member LTLs
1 FRWD 51 50 1 ENA 49
n1000v#
```

例 3-5　module *module_number* execute vemcmd show vsd ports

```
n1000v# module vem 4 execute vemcmd show vsd ports
LTL IfIndex VSD_ID VSD_PORT_TYPE
49 1c000010 1 REGULAR
50 1c000040 1 OUTSIDE
51 1c000030 1 INSIDE
n1000v#
```

設定例

次に、VSD を設定する例を示します。

```
port-profile vsd1_member
  vmware port-group
  switchport access vlan 315
  virtual-service-domain vsd1
  no shutdown
  state enabled
port-profile svm_vsd1_in
  vmware port-group
  switchport mode trunk
  switchport trunk allowed vlan 310-319
  virtual-service-domain vsd1
  service-port inside default-action drop
  no shutdown
  state enabled
port-profile svm_vsd1_out
  vmware port-group
  switchport mode trunk
  switchport trunk allowed vlan 310-319
  virtual-service-domain vsd1
  service-port outside default-action drop
  no shutdown
```

その他の関連資料

VSD の設定に関連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.3-11）
- 「標準」（P.3-11）

関連資料

関連項目	参照先
ポート プロファイル	『*Cisco Nexus 1000V Port Profile Configuration Guide, Release 4.2(1)SV1(4a)*』
CLI	『*Cisco Nexus 1000V Getting Started Guide, Release 4.2(1)SV1(4a)*』 『*Cisco Nexus 1000V Command Reference, Release 4.2(1)SV1(4a)*』

標準

標準	タイトル
この機能でサポートされる新規の標準または変更された標準はありません。また、既存の標準のサポートは変更されていません。	—

機能の履歴

ここでは、VSD のリリース履歴を示します。

機能名	リリース	機能情報
VSD	4.0(4)SV1(2)	この機能が導入されました。

CHAPTER 4

AAA の設定

この章では、Authentication, Authorization, and Accounting（AAA; 認証、認可、アカウンティング）を設定する手順について次の内容で説明します。

AAA について

ここでは、次の内容について説明します。

AAA セキュリティ サービス

AAA は、ユーザ ID とパスワードの組み合わせに基づいて、ユーザを認証および許可するために使用されます。キーは、AAA サーバとの通信を保護します。

多くの場合、AAA は RADIUS または TACACS+ などのプロトコルを使用してセキュリティ機能を管理します。ルータまたはアクセス サーバがネットワーク アクセス サーバとして動作している場合は、ネットワーク アクセス サーバと RADIUS または TACACS+ セキュリティ サーバとの間の通信を確立する手段に、AAA が使用されます。

AAA は主要な（推奨される）アクセス コントロール方式ですが、さらに、ローカル ユーザ名認証、回線パスワード認証、イネーブル パスワード認証など、AAA の範囲外で簡単なアクセス コントロールを行う機能も用意されています。ただし、これらの機能では、AAA を使用した場合と同レベルのアクセス コントロールは実現できません。

次のサービスごとに別個の AAA 設定が作成されます。

- User Telnet または Secure Shell（SSH）ログイン認証
- コンソール ログイン認証
- ユーザ管理セッション アカウンティング

表 4-1 に、AAA サービスを設定するための CLI の関連コマンドを示します。

表 4-1　AAA サービス コンフィギュレーション コマンド

AAA サービス コンフィギュレーション オプション	関連コマンド
Telnet または SSH ログイン	**aaa authentication login default**
コンソール ログイン	**aaa authentication login console**

AAA では次の保護を行います。

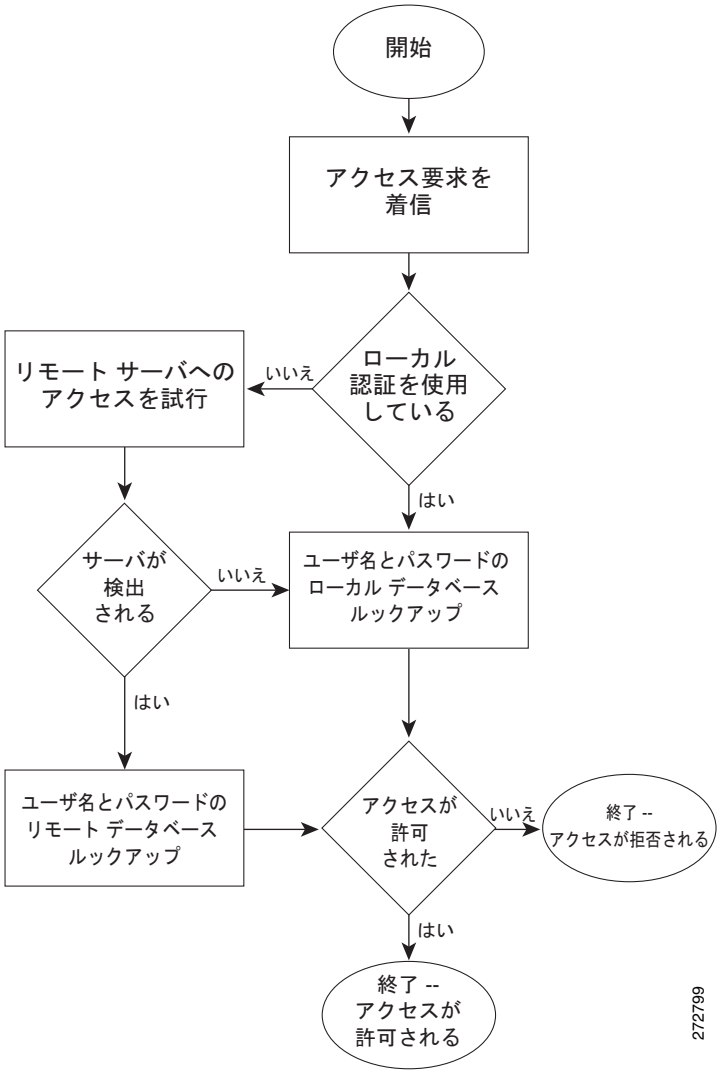
- 「認証」（P.4-2）
- 「許可」（P.4-3）
- 「アカウンティング」（P.4-3）

認証

認証では、ログインとパスワード、メッセージング、および暗号化によってユーザを識別します。認証は次のように実行されます。

認証方法	説明
ローカル データベース	ユーザ名またはパスワードのローカル ルックアップ データベースによって次の認証を行います。 • コンソール ログイン認証 • ユーザ ログイン認証 • ユーザ管理セッション アカウンティング
リモート RADIUS または TACACS+ サーバ	ユーザ名およびパスワードのリモート サーバ ルックアップ データベースを使用して次の認証を行います。 • コンソール ログイン認証 • ユーザ ログイン認証 • ユーザ管理セッション アカウンティング
なし	ユーザ名だけで次の認証を行います。 • コンソール ログイン認証 • ユーザ ログイン認証 • ユーザ管理セッション アカウンティング

図 4-1　ユーザ ログインの認証



許可

許可では、ユーザが実行を許可される操作を制限します。

アカウンティング

アカウンティングでは、すべての SVS 管理セッションを追跡し、ログに記録して管理します。この情報を使用して、トラブルシューティングや監査のためのレポートを生成できます。アカウンティング ログは、ローカルに保存することもできれば、リモート AAA サーバに送信することもできます。

AAA サーバ グループ

リモート AAA サーバ グループは、1 つのリモート AAA サーバが応答できない場合に備えて、フェールオーバーを提供することができます。グループ内の最初のサーバが応答しない場合は、同じグループ内の次のサーバが試行され、サーバが応答するまでこの処理が行われます。これと同じように、複数のサーバ グループが相互にフェールオーバーを提供できます。

すべてのリモート サーバ グループが応答しない場合は、ローカル データベースが認証に使用されます。

AAA の前提条件

リモート AAA サーバを使用する認証では、次の準備が整っている必要があります。

- 少なくとも 1 台の TACACS+ サーバまたは RADIUS サーバが IP で到達可能になっていること。
- VSM が AAA サーバのクライアントとして設定されていること。
- 共有秘密キーが VSM およびリモート AAA サーバに設定されていること。

  「共有キーの設定」（P.6-9）の手順を参照してください。

AAA のガイドラインと制限事項

Cisco Nexus 1000V は、すべて数字で構成されたユーザ名をサポートしていません。そのため、すべて数字で構成されたローカル ユーザ名は作成しません。すべて数字で構成されたユーザ名が AAA サーバ上に存在していて、ログイン時に入力された場合には、そのユーザは Cisco Nexus 1000V で認証されます。

デフォルト設定

次の表に、AAA のデフォルトを示します。

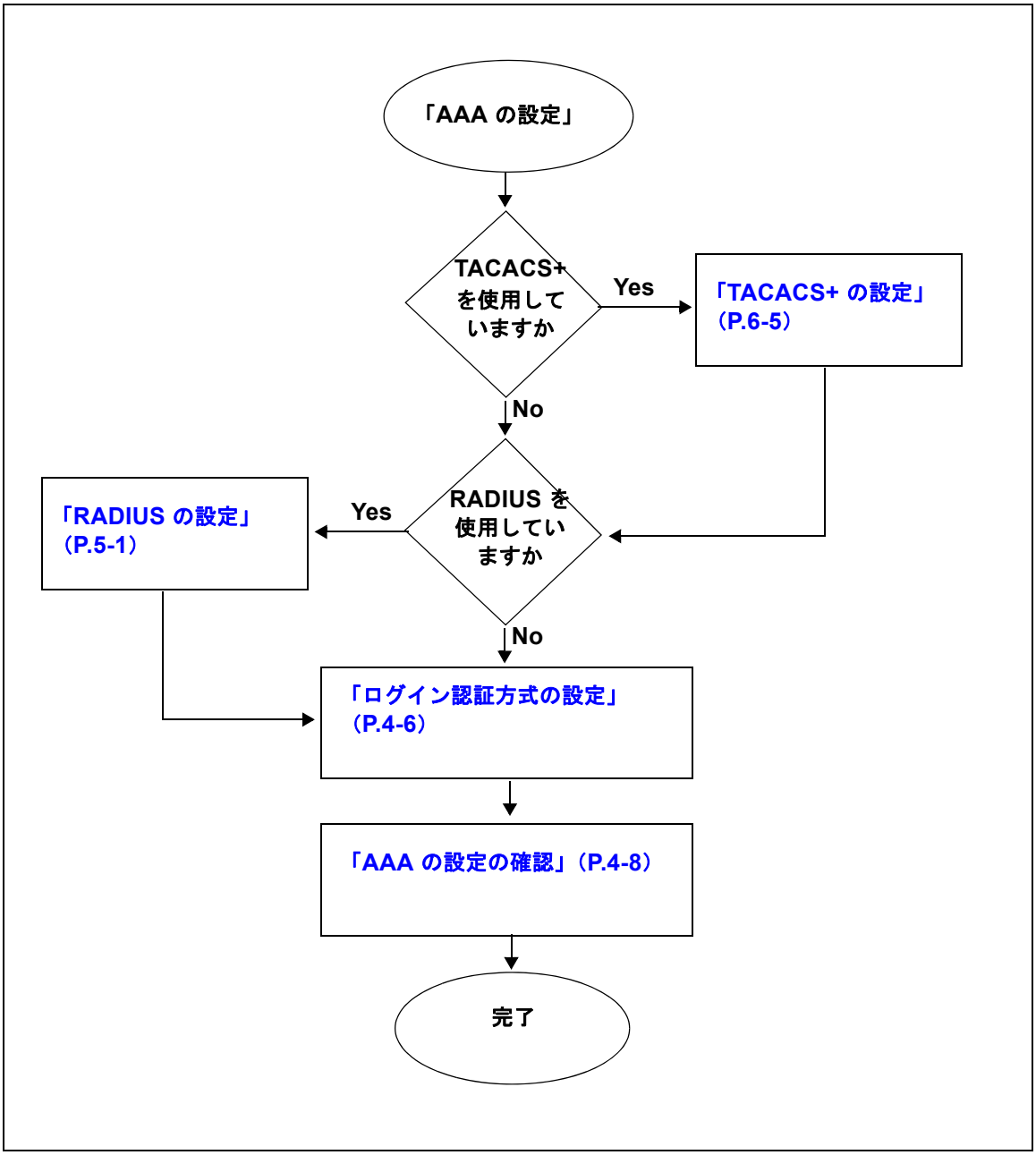
パラメータ	デフォルト
コンソール認証方式	ローカル
デフォルト認証方式	ローカル
ログイン認証失敗メッセージ	ディセーブル

AAA の設定

ここでは、次の内容について説明します。

AAA を設定するには、次のフロー チャートを使用します。

フロー チャート：「AAA の設定」



ログイン認証方式の設定

ログイン認証方式を設定するには、次の手順を実行します。

はじめる前に

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。

- EXEC モードで CLI にログインしていること。
- TACACS+ サーバ グループを使用して認証が行われる場合は、グループが追加済みです。詳細については、「TACACS+ サーバ グループの設定」（P.6-12）を参照してください。

手順の概要

1. **config t**
2. **aaa authentication login {console | default}** {**group** *group-list* [**none**] | **local** | **none**}
3. **exit**
4. **show aaa authentication**
5. **copy running-config start-config**

手順の詳細

	コマンド	目的
ステップ 1	**config t** **Example:** n1000v# config t n1000v(config)#	CLI 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	**aaa authentication login {console | default}** {**group** *group-list* [**none**]| **local** | **none**} **Example:** n1000v(config)# aaa authentication login console group tacgroup	コンソールまたはデフォルト ログイン認証方式を設定します。 • **group**：サーバ グループによって認証が行われます。 – **group-list**：スペースで区切ったサーバ グループ名のリストです。認証なしの場合は none です。 • **local**：ローカル データベースが認証に使用されます。 （注）　デフォルトは local で、方式が設定されていない場合、または設定されたすべての認証方式で応答が得られなかった場合に使用されます。 • **none**：ユーザ名によって認証が行われます。
ステップ 3	**exit** **Example:** n1000v(config)# exit n1000v#	CLI グローバル コンフィギュレーション モードを終了し、EXEC モードに戻ります。

	コマンド	目的
ステップ 4	**show aaa authentication** **Example:** n1000v# show aaa authentication default: group tacgroup console: group tacgroup n1000v#	（任意）設定されたログイン認証方式を表示します。
ステップ 5	**copy running-config startup-config** **Example:** n1000v# 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。

ログイン認証失敗メッセージのイネーブル化

リモート AAA サーバが応答しない場合のログイン認証エラー メッセージの表示をイネーブルにするには、次の手順を実行します。

はじめる前に

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。

- EXEC モードで CLI にログインしていること。
- 次に、ログイン認証エラー メッセージを示します。

```
Remote AAA servers unreachable; local authentication done.
Remote AAA servers unreachable; local authentication failed.
```

手順の概要

1. **config t**
2. **aaa authentication login error-enable**
3. **exit**
4. **show aaa authentication login error-enable**
5. **copy running-config start-config**

手順の詳細

	コマンド	目的
ステップ 1	**config t** **Example:** n1000v# config t n1000v(config)#	CLI 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	**aaa authentication login error-enable** **Example:** n1000v(config)# aaa authentication login error-enable n1000v(config)#	ログイン認証失敗メッセージをイネーブルにします。デフォルトはディセーブルです。

	コマンド	目的
ステップ 3	**exit** **Example:** n1000v(config)# exit n1000v#	CLI グローバル コンフィギュレーション モードを終了し、EXEC モードに戻ります。
ステップ 4	**show aaa authentication login error-enable** **Example:** n1000v# show aaa authentication login error-enable enabled n1000v#	（任意）ログイン失敗メッセージの設定を表示します。
ステップ 5	**copy running-config startup-config** **Example:** n1000v# 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。

AAA の設定の確認

AAA の設定情報を表示するには、次のいずれかの作業を行います。

コマンド	目的
show aaa authentication [**login** {**error-enable** | **mschap**}]	AAA 認証情報を表示します。 例 4-1（P.4-8）を参照してください。
show aaa groups	AAA サーバ グループの設定を表示します。
show running-config aaa [**all**]	実行コンフィギュレーションの AAA 設定を表示します。 例 4-2（P.4-8）を参照してください。
show startup-config aaa	スタートアップ コンフィギュレーションの AAA 設定を表示します。 例 4-3（P.4-9）を参照してください。

例 4-1　show aaa authentication

```
n1000v# show aaa authentication login error-enable
disabled
```

例 4-2　show running config aaa

```
n1000v# show running-config aaa all
version 4.0(1)
aaa authentication login default local
aaa accounting default local
no aaa authentication login error-enable
no aaa authentication login mschap enable
no radius-server directed-request
no snmp-server enable traps aaa server-state-change
```

```
no tacacs-server directed-request
n1000v#
```

例 4-3　show startup-config aaa

```
n1000v# show startup-config aaa
version 4.0(1)svs#
```

AAA の設定例

次に、AAA の設定例を示します。

```
aaa authentication login default group tacacs
aaa authentication login console group tacacs
```

その他の関連資料

AAA の実装に関する詳細情報については、次を参照してください。

- 「関連資料」（P.4-9）
- 「標準」（P.4-9）

関連資料

関連項目	参照先
システム管理	*『Cisco Nexus 1000V System Management Configuration Guide, Release 4.2(1)SV1(4a)』*
CLI	*『Cisco Nexus 1000V Getting Started Guide, Release 4.2(1)SV1(4a)』*
TACACS+ セキュリティ プロトコル	第 6 章「TACACS+ の設定」

標準

標準	タイトル
この機能でサポートされる新規の標準または変更された標準はありません。また、既存の標準のサポートは変更されていません。	—

AAA 機能の履歴

ここでは、AAA のリリース履歴について説明します。

機能名	リリース	機能情報
AAA	4.0(4)SV1(1)	この機能が導入されました。

CHAPTER 5

RADIUS の設定

この章では、Cisco NX-OS デバイスで RADIUS プロトコルを設定する手順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。

RADIUS の概要

RADIUS 分散クライアント / サーバ システムを使用すると、不正アクセスからネットワークを保護できます。シスコの実装では、RADIUS クライアントは Cisco NX-OS デバイス上で稼動します。認証要求とアカウンティング要求は、すべてのユーザ認証情報とネットワーク サービス アクセス情報が格納されている中央の RADIUS サーバに送信されます。

ここでは、次の内容について説明します。

RADIUS のネットワーク環境

RADIUS は、高度なセキュリティを必要とし、同時にリモート ユーザのネットワーク アクセスを維持する必要があるさまざまなネットワーク環境に実装できます。

RADIUS は、アクセス セキュリティを必要とする次のネットワーク環境で使用します。

- RADIUS をサポートしている複数ベンダーのネットワーク デバイスを使用したネットワーク たとえば、複数ベンダーのネットワーク デバイスで、単一の RADIUS サーバ ベースのセキュリティ データベースを使用できます。
- すでに RADIUS を使用中のネットワーク。RADIUS 機能を持つ Cisco NX-OS デバイスをネットワークに追加できます。この作業は、AAA サーバに移行するときの最初の手順になります。
- リソース アカウンティングが必要なネットワーク。RADIUS アカウンティングは、RADIUS 認証または RADIUS 許可とは個別に使用できます。RADIUS アカウンティング機能を使用すると、サービスの開始および終了時に、セッション中に使用したリソース（時間、パケット、バイトなど）の量を示すデータを送信できます。インターネット サービス プロバイダー（ISP）は、RADIUS アクセス コントロールおよびアカウンティング用ソフトウェアのフリーウェア版を使用して、特殊なセキュリティおよび課金ニーズに対応しています。
- 認証プロファイルをサポートするネットワーク ネットワークで RADIUS サーバを使用すると、AAA 認証を設定し、ユーザごとのプロファイルをセットアップできます。ユーザ単位のプロファイルにより、既存の RADIUS ソリューションを使用するポートの管理性が向上し、共有リソースを効率的に管理して、各種のサービスレベル契約を提供できるようになります。

RADIUS の動作

RADIUS を使用する NX-OS デバイスにユーザがログインおよび認証を試みると、次の処理が行われます。

1. ユーザが、ユーザ名とパスワードの入力を求められ、入力します。
2. ユーザ名および暗号化されたパスワードが、ネットワーク経由で RADIUS サーバに送信されます。
3. ユーザは、RADIUS サーバから次のいずれかの応答を受信します。
   - ACCEPT：ユーザが認証されたことを表します。
   - REJECT：ユーザは認証されず、ユーザ名とパスワードの再入力を求められるか、アクセスを拒否されます。
   - CHALLENGE：RADIUS サーバによってチャレンジが発行されます。チャレンジは、ユーザから追加データを収集します。
   - CHANGE PASSWORD：RADIUS サーバからユーザに対して新しいパスワードの選択を求める要求が発行されます。

ACCEPT または REJECT 応答には、EXEC またはネットワーク認可に使用される追加データが含まれています。RADIUS 許可を使用するには、まず RADIUS 認証を完了する必要があります。ACCEPT または REJECT パケットに含まれる追加データの内容は次のとおりです。

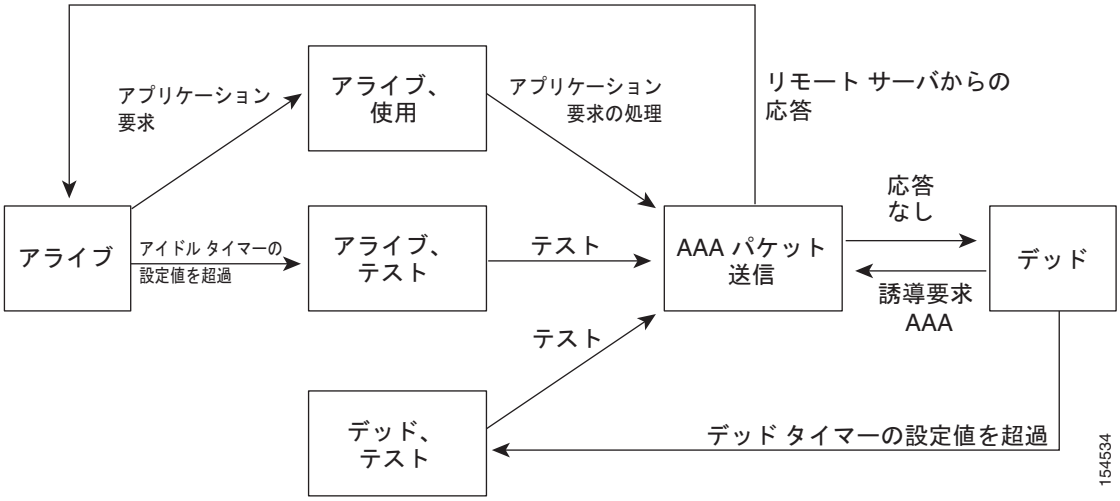
- ユーザがアクセス可能なサービス（Telnet、rlogin、または local-area transport（LAT; ローカルエリア トランスポート）接続、PPP（ポイントツーポイント プロトコル）、Serial Line Internet Protocol（SLIP; シリアル ライン インターネット プロトコル）、EXEC サービスなど）
- ホストまたはクライアントの IPv4 アドレス、アクセス リスト、ユーザ タイムアウトなどの接続パラメータ

RADIUS サーバ モニタリング

応答しない RADIUS サーバがあると、AAA 要求の処理が遅れることがあります。AAA 要求の処理時間を短縮するために、RADIUS サーバを定期的にモニタして RADIUS サーバが応答している（アライブ）かどうかを調べることができます。応答しない RADIUS サーバはデッド（dead）としてマークさ

れ、AAA 要求は送信されません。デッド RADIUS サーバは定期的にモニタされ、応答があればアライブ状態に戻されます。このモニタリング プロセスにより、RADIUS サーバが稼動状態であることを確認してから、実際の AAA 要求が送信されます。RADIUS サーバがデッドまたはアライブの状態に変わると Simple Network Management Protocol（SNMP; 簡易ネットワーク管理プロトコル）トラップが生成され、障害が発生していることを示すエラー メッセージが表示されます。図 5-1 を参照してください。

図 5-1　RADIUS サーバの状態



（注）　アライブ サーバとデッド サーバのモニタリング間隔は異なります。これらはユーザが設定できます。RADIUS サーバ モニタリングを実行するには、テスト認証要求を RADIUS サーバに送信します。

ベンダー固有属性（VSA）

Internet Engineering Task Force（IETF; インターネット技術特別調査委員会）が、ネットワーク アクセス サーバと RADIUS サーバの間での VSA の通信のための方式を規定する標準を作成しています。IETF は、属性 26 を使用します。VSA を使用するとベンダーは、一般的な用途には適合しない独自の拡張属性をサポートできます。シスコの RADIUS 実装は、この仕様で推奨される形式を使用して、1 つのベンダー固有オプションをサポートしています。シスコのベンダー ID は 9 で、サポートするオプションはベンダー タイプ 1、名前は cisco-av-pair です。値は、次の形式のストリングです。

```
protocol : attribute separator value *
```

protocol は、特定の許可タイプを表すシスコの属性です。separator は、必須属性の場合は =（等号）、任意の属性の場合は *（アスタリスク）です。

認証に RADIUS サーバを使用した場合、RADIUS プロトコルでは RADIUS サーバに対して、認証結果とともに権限付与情報などのユーザ属性を返すように指示します。この許可情報は、VSA で指定されます。

次に、サポートされる VSA プロトコル オプションを示します。

- shell：ユーザ プロファイル情報を提供する access-accept パケットで使用されるプロトコル。
- Accounting：accounting-request パケットで使用されるプロトコル。値にスペースが含まれている場合は、二重引用符で囲む必要があります。

次に、サポートされる属性を示します。

- roles：ユーザが属するすべてのロールの一覧です。値フィールドは、スペースで区切られたロール名を一覧表示したストリングです。たとえば、ユーザが属しているロールが network-operator と vdc-admin ならば、値フィールドは「network-operator vdc-admin」となります。この属性は、RADIUS サーバから送信される Access-Accept フレームの VSA 部分に格納されます。この属性はシェル プロトコル値とだけ併用できます。次に、Cisco ACS でサポートされるロール属性の例を示します。

  ```
  shell:roles="network-operator vdc-admin"

  shell:roles*"network-operator vdc-admin"
  ```

  次に、FreeRADIUS でサポートされるロール属性の例を示します。

  ```
  Cisco-AVPair = "shell:roles=\"network-operator vdc-admin\""

  Cisco-AVPair = "shell:roles*\"network-operator vdc-admin\""
  ```

  Cisco ACS を使用していて、Cisco Nexus 1000V と Cisco UCS 認証の両方に同じ ACS グループを使用する場合は、次のロール属性を使用します。

  ```
  cisco-av-pair*shell:roles="network-admin admin"
  ```

（注）　VSA を shell:roles*"network-operator vdc-admin" または "shell:roles*\"network-operator vdc-admin\"" として指定した場合、この VSA はオプション属性としてフラグ設定され、他のシスコ デバイスはこの属性を無視します。

- accountinginfo：標準の RADIUS アカウンティング プロトコルで処理される属性に加えて、アカウンティング情報が格納されます。この属性は、スイッチ上の RADIUS クライアントからの Account-Request フレームの VSA 部分だけに送信されます。この属性と共に使用できるのは、アカウンティングの Protocol Data Unit（PDU; プロトコル データ ユニット）だけです。

RADIUS の前提条件

RADIUS には、次の前提条件があります。

- RADIUS サーバの IP アドレスまたはホスト名がわかっていること。
- ネットワーク内での RADIUS 通信を保護するために使用されるキーがわかっていること。
- デバイスが AAA サーバの RADIUS クライアントとして設定されていること。

注意事項および制約事項

RADIUS に関する注意事項と制約事項は次のとおりです。

- 最大 64 の RADIUS サーバを設定できます。

デフォルト設定

表 5-1 に、RADIUS のデフォルト設定を示します。

表 5-1　デフォルトの RADIUS パラメータ

パラメータ	デフォルト
サーバの役割	認証とアカウンティング
デッド タイマー間隔	0 分
再送信回数	1
再送信タイマー間隔	5 秒
アイドル タイマー間隔	0 分
サーバの定期的モニタリングのユーザ名	test
サーバの定期的モニタリングのパスワード	test

RADIUS サーバの設定

ここでは、次の内容について説明します。

（注）　この機能に対応する Cisco NX-OS コマンドは、Cisco IOS で使用されているコマンドと異なる場合があるので注意してください。

RADIUS サーバ ホストの設定

認証に使用される各 RADIUS サーバの IP アドレスまたはホスト名を設定するには、次の手順を実行します。

はじめる前に

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。

- EXEC モードで CLI にログインしていること。
- 最大 64 の RADIUS サーバを設定できます。
- すべての RADIUS サーバ ホストは自動的にデフォルトの RADIUS サーバ グループに追加されます。

手順の概要

1. **config t**
2. **radius-server host** {*ipv4-address* | *host-name*}
3. **exit**
4. **show radius-server**
5. **copy running-config startup-config**

手順の詳細

	コマンド	目的

ステップ 1	**config t**
	
	Example:
	`n1000v# config t`
	`n1000v(config)#`
		CLI 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	**radius-server host** {*ipv4-address* | *host-name*} **Example:** `n1000v(config)# radius-server host 10.10.1.1`	RADIUS サーバの IP アドレスまたはホスト名を定義します。

ステップ 3	**exit**
	
	Example:
	`n1000v(config)# exit`
	`n1000v#`
		CLI EXEC モードに戻ります。

ステップ 4	**show radius-server** **Example:** `n1000v# show radius-server`	（任意）RADIUS サーバの設定を表示します。
ステップ 5	**copy running-config startup-config** **Example:** `n1000v# copy running-config startup-config`	（任意）この実行コンフィギュレーションの変更内容を、スタートアップ コンフィギュレーションに保存します。

RADIUS グローバル キーの設定

すべての RADIUS サーバが Cisco Nexus 1000V での認証に使用するキーを設定するには、次の手順を実行します。

はじめる前に

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。

- EXEC モードで CLI にログインしていること。
- RADIUS サーバ認証に使用されるグローバル キーがわかっています。

手順の概要

1. **config t**
2. **radius-server key** [**0** | **7**] *key-value*
3. **exit**
4. **show radius-server**
5. **copy running-config startup-config**

手順の詳細

グローバル事前共有キーを設定するには、次の手順を実行します。

	コマンド	目的

ステップ 1	**config t**
	
	Example:
	`n1000v# config t`
	`n1000v(config)#`
		CLI 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	**radius-server key** [**0** | **7**] *key-value* **Example:** `n1000v(config)# radius-server key 0 QsEfThUkO`	すべての RADIUS サーバで使用する事前共有キーを指定します。クリア テキスト形式（**0**）または暗号化形式（**7**）の事前共有キーを指定できます。デフォルトの形式はクリア テキストです。最大で 63 文字の長さまで指定可能です。 デフォルトでは、事前共有キーは設定されません。

ステップ 3	**exit**
	
	Example:
	`n1000v(config)# exit`
	`n1000v#`
		CLI EXEC モードに戻ります。

	コマンド	目的
ステップ 4	**show radius-server** **Example:** n1000v# show radius-server	（任意）RADIUS サーバの設定を表示します。 **（注）** 事前共有キーは、実行コンフィギュレーション内に暗号化形式で保存されます。暗号化された事前共有キーを表示するには、**show running-config** コマンドを使用します。
ステップ 5	**copy running-config startup-config** **Example:** n1000v# copy running-config startup-config	（任意）この実行コンフィギュレーションの変更内容を、スタートアップ コンフィギュレーションに保存します。

RADIUS サーバ キーの設定

単一の RADIUS サーバ ホストのキーを設定するには、次の手順を実行します。

はじめる前に

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。

- EXEC モードで CLI にログインしていること。
- リモート RADIUS ホストに使用されるキーを取得しています。

手順の概要

1. **config t**
2. **radius-server host** {*ipv4-address* | *host-name*} **key** *key-value*
3. **exit**
4. **show radius-server**
5. **copy running-config startup-config**

手順の詳細

	コマンド	目的
ステップ 1	**config t** **Example:** n1000v# config t n1000v(config)#	CLI 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	**radius-server host** {*ipv4-address* | *host-name*} **key** [**0** | **7**] *key-value* **Example:** n1000v(config)# radius-server host 10.10.1.1 key 0 PlIjUhYg	特定の RADIUS サーバの事前共有キーを指定します。クリア テキスト形式（**0**）または暗号化形式（**7**）の事前共有キーを指定できます。デフォルトの形式はクリア テキストです。最大で 63 文字の長さまで指定可能です。 この事前共有キーがグローバル事前共有キーの代わりに使用されます。

	コマンド	目的
ステップ 3	**exit** **Example:** n1000v(config)# exit n1000v#	CLI EXEC モードに戻ります。
ステップ 4	**show radius-server** **Example:** n1000v# show radius-server	（任意）RADIUS サーバの設定を表示します。 **（注）** 事前共有キーは、実行コンフィギュレーション内に暗号化形式で保存されます。暗号化された事前共有キーを表示するには、**show running-config** コマンドを使用します。
ステップ 5	**copy running-config startup-config** **Example:** n1000v# copy running-config startup-config	（任意）この実行コンフィギュレーションの変更内容を、スタートアップ コンフィギュレーションに保存します。

RADIUS サーバ グループの設定

メンバー サーバが認証機能を共有する RADIUS サーバ グループを設定するには、次の手順を実行します。

はじめる前に

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。

- EXEC モードで CLI にログインしていること。
- RADIUS サーバ グループ内のすべてのサーバが、同じ RADIUS プロトコルに属しています。
- グループ内のサーバへのアクセスは、サーバを設定した順番で行われます。

手順の概要

1. **config t**
2. **aaa group server radius** *group-name*
3. **server** {*ipv4-address* | *server-name*}
4. **deadtime** *minutes*
5. **use-vrf** *vrf-name*
6. （任意）**source-interface** {*interface-type*} {*interface-number*}
7. （任意）show radius-server groups [*group-name*]
8. （任意）**copy running-config startup-config**

手順の詳細

	コマンド	目的

ステップ 1	**config t**
	
	Example:
	`n1000v# config t`
	`n1000v(config)#`
		CLI 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	**aaa group server radius** *group-name*
	
	Example:
	`n1000v(config)# aaa group server radius RadServer`
	`n1000v(config-radius)#`
		RADIUS サーバ グループを作成し、そのグループの RADIUS サーバ グループ コンフィギュレーション モードを開始します。*group-name* 引数は、最大 127 文字の長さの英数字のストリングで、大文字小文字が区別されます。

ステップ 3	**server** {*ipv4-address* | *server-name*} **Example:** `n1000v(config-radius)# server 10.10.1.1`	RADIUS サーバを、RADIUS サーバ グループのメンバーとして設定します。 **ヒント** 指定した RADIUS サーバが見つからない場合は、**radius-server host** コマンドを使用してサーバを設定し、このコマンドをもう一度実行します。
ステップ 4	**deadtime** *minutes* **Example:** `n1000v(config-radius)# deadtime 30`	（任意）モニタリング デッド タイムを設定します。デフォルト値は 0 分です。指定できる範囲は 1 ～ 1440 です。 **（注）** デッド タイム間隔がゼロ（0）より大きい RADIUS サーバ グループの場合は、その値がグローバル デット タイム値に優先します（「グローバル デッド タイム間隔の設定」（P.5-20）を参照）。
ステップ 5	**use-vrf** *vrf-name* **Example:** `n1000v(config-radius)# use-vrf vrf1`	（任意）サーバ グループ内のサーバとの接続に使用する VRF を指定します。

ステップ 6	**source-interface** {*interface-type*} {*interface-number*}
	
	Example:
	`n1000v(config-radius)# source-interface mgmt0`
	`n1000v(config-radius)#`
		（任意）RADIUS サーバに到達するために使用される送信元インターフェイスを指定します。
		• loopback = 0 ～ 1023 の仮想インターフェイス番号
		• mgmt = 管理インターフェイス 0
		• null = ヌル インターフェイス 0
		• port-channel = 1 ～ 4096 のポート チャネル番号

	コマンド	目的
ステップ 7	**show radius-server groups** [*group-name*]	（任意）RADIUS サーバ グループの設定を表示します。

Example:
```
n1000v(config-radius)# show radius-server group
total number of groups:2

following RADIUS server groups are configured:
        group Radserver:
                server: 10.10.1.1
                deadtime is 30
        group test:
                deadtime is 30
```

ステップ 8	**copy running-config startup-config** **Example:** `n1000v(config-radius)# copy running-config startup-config`	（任意）この実行コンフィギュレーションの変更内容を、スタートアップ コンフィギュレーションに保存します。

RADIUS サーバの誘導要求のイネーブル化

認証要求の送信先の RADIUS サーバをユーザが指定できるようにするには、次の手順を実行します。これは directed-request（誘導要求）と呼ばれます。

このオプションをイネーブルにした場合、ユーザは *username@vrfname*:*hostname* としてログインできます。ここで、*vrfname* は使用する VRF、*hostname* は設定された RADIUS サーバの名前です。

（注）　ユーザ指定のログインは Telnet セッションに限りサポートされます。

はじめる前に

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。

- EXEC モードで CLI にログインしていること。
- デフォルトでは、誘導要求はディセーブルです。

手順の概要

1. **config t**
2. **radius-server directed-request**
3. **exit**
4. **show radius-server directed-request**
5. **copy running-config startup-config**

手順の詳細

	コマンド	目的
ステップ 1	**config t** **Example:** n1000v# config t n1000v(config)#	CLI 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	n1000v(config)# radius-server directed-request **Example:** n1000v(config)# radius-server directed-request	誘導要求をイネーブルにします。デフォルトはディセーブルです。
ステップ 3	**exit** **Example:** n1000v(config)# exit n1000v#	CLI EXEC モードに戻ります。
ステップ 4	**show radius-server directed-request** **Example:** n1000v# show radius-server directed-request	（任意）指定要求設定を表示します。
ステップ 5	**copy running-config startup-config** **Example:** n1000v# 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。

すべての RADIUS サーバのグローバル タイムアウトの設定

ここでは、RADIUS サーバからの応答を待つ時間を指定するグローバル タイムアウト間隔の設定手順を説明します。この時間が経過すると、タイムアウト障害となります。

はじめる前に

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。

- EXEC モードで CLI にログインしていること。
- 「単一 RADIUS サーバのタイムアウト間隔の設定」（P.5-14）の手順で指定したタイムアウトは、RADIUS のグローバル タイムアウトに優先します。

手順の概要

1. **config t**
2. **radius-server timeout** *seconds*
3. **exit**
4. **show radius-server**
5. **copy running-config startup-config**

手順の詳細

	コマンド	目的
ステップ 1	**config t** **Example:** n1000v# config t n1000v(config)#	CLI 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	**radius-server timeout** *seconds* **Example:** n1000v(config)# radius-server timeout 10	RADIUS サーバの送信タイムアウト間隔を指定します。デフォルトのタイムアウト間隔は 5 秒です。有効な範囲は 1 ～ 60 秒です。
ステップ 3	**exit** **Example:** n1000v(config)# exit n1000v#	CLI EXEC モードに戻ります。
ステップ 4	**show radius-server** **Example:** n1000v# show radius-server	（任意）RADIUS サーバの設定を表示します。
ステップ 5	**copy running-config startup-config** **Example:** n1000v# copy running-config startup-config	（任意）この実行コンフィギュレーションの変更内容を、スタートアップ コンフィギュレーションに保存します。

すべての RADIUS サーバのグローバル リトライ回数の設定

ローカル認証に切り換える前に RADIUS サーバへの送信を再試行する最大回数を設定するには、次の手順を実行します。この設定はすべての RADIUS サーバに適用されます。

はじめる前に

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。

- EXEC モードで CLI にログインしていること。
- デフォルトでは、ローカル認証に切り換える前に、RADIUS サーバへの再送信を 1 回だけ試行します。
- リトライ回数は最大 5 回まで増やすことができます。
- 「単一 RADIUS サーバのリトライ回数の設定」（P.5-15）の手順で単一の RADIUS サーバに指定したリトライ回数は、このグローバル設定に優先します。

手順の概要

1. **config t**
2. **radius-server retransmission** *count*
3. **radius-server timeout** *seconds*
4. **exit**
5. **show radius-server**
6. **copy running-config startup-config**

手順の詳細

	コマンド	目的
ステップ 1	**config t** **Example:** n1000v# config t n1000v(config)#	CLI 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	**radius-server retransmit** *count* **Example:** n1000v(config)# radius-server retransmit 3	ローカル認証に切り換える前に許可する再送信回数を定義します。これはすべての RADIUS サーバに適用されるグローバル設定です。デフォルトの再送信回数は 1 です。有効な範囲は 0 ～ 5 です。
ステップ 3	**exit** **Example:** n1000v(config)# exit n1000v#	CLI EXEC モードに戻ります。
ステップ 4	**show radius-server** **Example:** n1000v# show radius-server	（任意）RADIUS サーバの設定を表示します。
ステップ 5	**copy running-config startup-config** **Example:** n1000v# copy running-config startup-config	（任意）この実行コンフィギュレーションの変更内容を、スタートアップ コンフィギュレーションに保存します。

単一 RADIUS サーバのタイムアウト間隔の設定

ここでは、RADIUS サーバからの応答を待つ時間を設定する手順を説明します。この時間が経過すると、タイムアウト障害となります。

はじめる前に

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。

- EXEC モードで CLI にログインしていること。
- 単一の RADIUS サーバに指定したタイムアウトは、「すべての RADIUS サーバのグローバル タイムアウトの設定」（P.5-12）の手順で定義したタイムアウトに優先します。

手順の概要

1. **config t**
2. **radius-server host** {*ipv4-address* | *host-name*} **timeout** *seconds*
3. **exit**
4. **show radius-server**
5. **copy running-config startup-config**

手順の詳細

	コマンド	目的

ステップ 1	**config t**
	
	Example:
	`n1000v# config t`
	`n1000v(config)#`
		CLI 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	**radius-server host** {*ipv4-address* | *host-name*} **timeout** *seconds* **Example:** `n1000v(config)# radius-server host server1 timeout 10`	特定のサーバのタイムアウト間隔を指定します。デフォルトのタイムアウト間隔は 5 秒です。有効な範囲は 1 ～ 60 秒です。 **（注）** 単一の RADIUS サーバに指定したタイムアウトは、RADIUS のグローバル タイムアウトに優先します。

ステップ 3	**exit**
	
	Example:
	`n1000v(config)# exit`
	`n1000v#`
		CLI EXEC モードに戻ります。

ステップ 4	**show radius-server** **Example:** `n1000v# show radius-server`	（任意）RADIUS サーバの設定を表示します。
ステップ 5	**copy running-config startup-config** **Example:** `n1000v# copy running-config startup-config`	（任意）この実行コンフィギュレーションの変更内容を、スタートアップ コンフィギュレーションに保存します。

単一 RADIUS サーバのリトライ回数の設定

ローカル認証に切り換える前に RADIUS サーバへの送信を再試行する最大回数を設定するには、次の手順を実行します。この設定は単一の RADIUS サーバに適用され、グローバル リトライ回数に優先します。

はじめる前に

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。

- EXEC モードで CLI にログインしていること。
- デフォルトでは、ローカル認証に切り換える前に、RADIUS サーバへの再送信を 1 回だけ試行します。
- リトライ回数は最大 5 回まで増やすことができます。
- 単一の RADIUS サーバに指定したリトライ回数は、すべての RADIUS サーバ用に作成されるグローバル設定に優先します。

手順の概要

1. **config t**
2. **radius-server host** {*ipv4-address* | *host-name*} **retransmit** *count*
3. **exit**

4. **show radius-server**
5. **copy running-config startup-config**

手順の詳細

	コマンド	目的

ステップ 1	**config t**
	
	Example:
	`n1000v# config t`
	`n1000v(config)#`
		CLI 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	**radius-server host** {*ipv4-address* | *host-name*} **retransmit** *count* **Example:** `n1000v(config)# radius-server host server1 retransmit 3`	特定のサーバに対する再送信回数を指定します。デフォルトはグローバル値です。 **（注）** この単一 RADIUS サーバの再送信回数は、すべての RADIUS サーバ用のグローバル設定に優先します。

ステップ 3	**exit**
	
	Example:
	`n1000v(config)# exit`
	`n1000v#`
		CLI EXEC モードに戻ります。

ステップ 4	**show radius-server** **Example:** `n1000v# show radius-server`	（任意）RADIUS サーバの設定を表示します。
ステップ 5	**copy running-config startup-config** **Example:** `n1000v# copy running-config startup-config`	（任意）この実行コンフィギュレーションの変更内容を、スタートアップ コンフィギュレーションに保存します。

RADIUS アカウンティング サーバの設定

アカウンティング機能を実行するサーバを設定するには、次の手順を実行します。

はじめる前に

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。

- EXEC モードで CLI にログインしていること。
- デフォルトでは、RADIUS サーバはアカウンティングと認証の両方に使用されます。
- RADIUS アカウンティング メッセージの宛先 UDP ポート番号がわかっています。

手順の概要

1. **config t**
2. **radius-server host** {*ipv4-address* | *host-name*} **acct-port** *udp-port*
3. **radius-server host** {*ipv4-address* | *host-name*} **accounting**
4. **exit**

5. **show radius-server**
6. **copy running-config startup-config**

手順の詳細

RADIUS サーバの認証およびアカウンティング属性を設定するには、次の手順を実行します。

	コマンド	目的
ステップ 1	**config t** **Example:** n1000v# config t n1000v(config)#	CLI 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	**radius-server host** {*ipv4-address* | *host-name*} **acct-port** *udp-port* **Example:** n1000v(config)# radius-server host 10.10.1.1 acct-port 2004	（任意）特定のホストに RADIUS アカウンティング メッセージを受信する UDP ポートを関連付けます。デフォルトの UDP ポートは 1812 です。範囲は 0 ～ 65535 です。
ステップ 3	**radius-server host** {*ipv4-address* | *host-name*} **accounting** **Example:** n1000v(config)# radius-server host 10.10.1.1 accounting	（任意）特定の RADIUS ホストをアカウンティング サーバとして指定します。デフォルトでは、アカウンティングと認証の両方に使用されます。
ステップ 4	**exit** **Example:** n1000v(config)# exit n1000v#	CLI EXEC モードに戻ります。
ステップ 5	**show radius-server** **Example:** n1000v(config)# show radius-server	（任意）RADIUS サーバの設定を表示します。
ステップ 6	**copy running-config startup-config** **Example:** n1000v# copy running-config startup-config	（任意）この実行コンフィギュレーションの変更内容を、スタートアップ コンフィギュレーションに保存します。

RADIUS 認証サーバの設定

認証機能を実行するサーバを設定するには、次の手順を実行します。

はじめる前に

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。

- EXEC モードで CLI にログインしていること。
- デフォルトでは、RADIUS サーバはアカウンティングと認証の両方に使用されます。
- RADIUS 認証メッセージの宛先 UDP ポート番号がわかっています。

手順の概要

1. **config t**
2. **radius-server host** {*ipv4-address* | *host-name*} **auth-port** *udp-port*
3. **radius-server host** {*ipv4-address* | *host-name*} **authentication**
4. **exit**
5. **show radius-server**
6. **copy running-config startup-config**

手順の詳細

RADIUS サーバの認証およびアカウンティング属性を設定するには、次の手順を実行します。

	コマンド	目的

ステップ 1	**config t**
	
	Example:
	`n1000v# config t`
	`n1000v(config)#`
		CLI 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	**radius-server host** {*ipv4-address* | *host-name*} **auth-port** *udp-port* **Example:** `n1000v(config)# radius-server host 10.10.2.2 auth-port 2005`	（任意）特定のホストに RADIUS 認証メッセージを受信する UDP ポートを関連付けます。デフォルトの UDP ポートは 1812 です。範囲は 0 ～ 65535 です。
ステップ 3	**radius-server host** {*ipv4-address* | *host-name*} **authentication** **Example:** `n1000v(config)# radius-server host 10.10.2.2 authentication`	（任意）特定の RADIUS ホストを認証サーバとして指定します。デフォルトでは、アカウンティングと認証の両方に使用されます。

ステップ 4	**exit**
	
	Example:
	`n1000v(config)# exit`
	`n1000v#`
		CLI EXEC モードに戻ります。

ステップ 5	**show radius-server** **Example:** `n1000v(config)# show radius-server`	（任意）RADIUS サーバの設定を表示します。
ステップ 6	**copy running-config startup-config** **Example:** `n1000v# copy running-config startup-config`	（任意）この実行コンフィギュレーションの変更内容を、スタートアップ コンフィギュレーションに保存します。

RADIUS サーバの定期モニタリングの設定

RADIUS サーバのモニタリングを設定するには、次の手順を実行します。

はじめる前に

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。

- EXEC モードで CLI にログインしていること。
- テスト アイドル タイマーには、応答しない RADIUS サーバにテスト パケットが送信されるまでの経過時間を指定します。

（注）　セキュリティ上の理由から、RADIUS データベースに存在するユーザ名をテスト ユーザ名として設定しないでください。

（注）　デフォルトのアイドル タイマー値は 0 分です。アイドル時間の間隔が 0 分の場合、NX-OS デバイスは RADIUS サーバの定期モニタリングを実行しません。

手順の概要

1. **config t**
2. **radius-server host** {*ipv4-address* | *host-name*} **test** {**idle-time** *minutes* | **password** *password* [**idle-time** *minutes*] | **username** *name* [**password** *password* [**idle-time** *minutes*]]}
3. **radius-server dead-time** *minutes*
4. **exit**
5. **show radius-server**
6. **copy running-config startup-config**

手順の詳細

	コマンド	目的

ステップ 1	**config t**
	
	Example:
	`n1000v# config t`
	`n1000v(config)#`
		CLI 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	**radius-server host** {*ipv4-address* | *host-name*} **test** {**idle-time** *minutes* | **password** *password* [**idle-time** *minutes*] | **username** *name* [**password** *password* [**idle-time** *minutes*]]} **Example:** `n1000v(config)# radius-server host 10.10.1.1 test username user1 password Ur2Gd2BH idle-time 3`	サーバ モニタリング用のパラメータを指定します。デフォルトのユーザ名は test、デフォルトのパスワードは test です。デフォルトのアイドル タイマー値は 0 分です。指定できる範囲は 0 ～ 1440 分です。 （注）　RADIUS サーバの定期的なモニタリングを行うには、アイドル タイマーに 0 より大きな値を設定する必要があります。

	コマンド	目的
ステップ 3	**radius-server dead-time** *minutes* **Example:** n1000v(config)# radius-server dead-time 5	デッドと宣言された RADIUS サーバにテスト パケットを送信するまで待機する分数を指定します。デフォルト値は 0 分です。指定できる範囲は 1 ～ 1440 分です。
ステップ 4	**exit** **Example:** n1000v(config)# exit n1000v#	CLI EXEC モードに戻ります。
ステップ 5	**show radius-server** **Example:** n1000v# show radius-server	（任意）RADIUS サーバの設定を表示します。
ステップ 6	**copy running-config startup-config** **Example:** n1000v# copy running-config startup-config	（任意）この実行コンフィギュレーションの変更内容を、スタートアップ コンフィギュレーションに保存します。

グローバル デッド タイム間隔の設定

すべての RADIUS サーバのデッド タイム間隔を設定するには、次の手順を実行します。デッド タイム間隔には、RADIUS サーバをデッドであると宣言したあと、そのサーバがアライブになったかどうかを確認するためにテスト パケットを送信するまで待機する時間を指定します。デフォルト値は 0 分です。

（注）　デッド タイム間隔が 0 分の場合、RADIUS サーバは、応答を返さない場合でも、デットとしてマークされません。RADIUS サーバ グループのデッド タイム間隔を設定することもできます（「RADIUS サーバ グループの設定」（P.5-9）を参照）。

はじめる前に

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。

- EXEC モードで CLI にログインしていること。

手順の概要

1. **config t**
2. **radius-server deadtime** *minutes*
3. **exit**
4. **show radius-server**
5. **copy running-config startup-config**

手順の詳細

RADIUS のデッド タイム間隔を設定するには、次の手順を実行します。

	コマンド	目的
ステップ 1	**config t** **Example:** n1000v# config t n1000v(config)#	CLI 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	n1000v(config)# **radius-server deadtime** *minutes* **Example:** n1000v(config)# radius-server deadtime 5	デッド タイム間隔を設定します。デフォルト値は 0 分です。有効な範囲は 1 ～ 1440 分です。
ステップ 3	**exit** **Example:** n1000v(config)# exit n1000v#	CLI EXEC モードに戻ります。
ステップ 4	**show radius-server** **Example:** n1000v# show radius-server	（任意）RADIUS サーバの設定を表示します。
ステップ 5	**copy running-config startup-config** **Example:** n1000v# copy running-config startup-config	（任意）この実行コンフィギュレーションの変更内容を、スタートアップ コンフィギュレーションに保存します。

RADIUS サーバまたはサーバ グループの手動でのモニタリング

RADIUS サーバまたはサーバ グループにテスト メッセージを手動で送信するには、次の手順を実行します。

はじめる前に

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。

- EXEC モードで CLI にログインしていること。

手順の概要

1. **test aaa server radius** {*ipv4-address* | *host-name*} [**vrf** *vrf-name*] *username password*
2. **test aaa group** *group-name username password*

手順の詳細

	コマンド	目的
ステップ 1	**test aaa server radius** {*ipv4-address* | *server-name*} [**vrf** *vrf-name*] *username password* **Example:** `n1000v# test aaa server radius 10.10.1.1 user1 Ur2Gd2BH`	RADIUS サーバにテスト メッセージを送信して可用性を確認します。
ステップ 2	**test aaa group** *group-name username password* **Example:** `n1000v# test aaa group RadGroup user2 As3He3CI`	RADIUS サーバ グループにテスト メッセージを送信して可用性を確認します。

RADIUS 設定の確認

この項のコマンドを使用して、RADIUS 設定を確認します。show コマンド出力の詳細については、『*Cisco Nexus 1000V Command Reference, Release 4.2(1)SV1(4a)*』を参照してください。

コマンド	目的
show running-config radius [**all**]	実行コンフィギュレーションの RADIUS 設定を表示します。
show startup-config radius	スタートアップ コンフィギュレーションの RADIUS 設定を表示します。
show radius-server [*server-name* | *ipv4-address*] [**directed-request** | **groups** | **sorted** | **statistics**]	設定済みのすべての RADIUS サーバのパラメータを表示します。

RADIUS サーバの統計情報の表示

RADIUS サーバのアクティビティに関する統計情報を表示するには、次のコマンドを使用します。

show radius-server statistics {*hostname* | *ipv4-address* }

RADIUS 設定例

次に、RADIUS を設定する例を示します。

```
radius-server key 7 "ToIkLhPpG"
radius-server host 10.10.1.1 key 7 "ShMoMhTl" authentication accounting
aaa group server radius RadServer
    server 10.10.1.1
```

その他の関連資料

RADIUS の実装に関する詳細情報については、次を参照してください。

- 「関連資料」（P.5-23）
- 「標準」（P.5-23）

関連資料

関連項目	参照先
コマンド リファレンス	『*Cisco Nexus 1000V Command Reference, Release 4.2(1)SV1(4a)*』

標準

標準	タイトル
この機能でサポートされる新規の標準または変更された標準はありません。また、既存の標準のサポートは変更されていません。	—

RADIUS 機能の履歴

ここでは、RADIUS のリリース履歴を示します。

機能名	リリース	機能情報
RADIUS	4.0(4)SV1(1)	この機能が導入されました。

CHAPTER 6

TACACS+ の設定

この章では、Terminal Access Controller Access Control System Plus（TACACS+）プロトコルを設定する手順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。

TACACS+ の概要

TACACS+ は、デバイスにアクセスしようとするユーザの検証を集中的に行う場合に使用できます。TACACS+ サービスは、通常 UNIX または Windows NT ワークステーション上で動作する TACACS+ デーモンのデータベースで管理されます。デバイスに設定した TACACS+ 機能を使用可能にするには、TACACS+ サーバにアクセスして TACACS+ サーバを設定しておく必要があります。

TACACS+ は、デバイスにアクセスしようとするユーザの検証を集中的に行うセキュリティ プロトコルです。TACACS+ サービスは、通常 UNIX または Windows NT ワークステーション上で動作する TACACS+ デーモンのデータベースで管理されます。デバイスに設定した TACACS+ 機能を使用可能にするには、TACACS+ サーバにアクセスして TACACS+ サーバを設定しておく必要があります。

TACACS+ は、独立した認証、許可、およびアカウンティング サービスを提供します。TACACS+ デーモンは各サービスを個別に提供します。各サービスを固有のデータベースに結合し、デーモンの機能に応じてそのサーバまたはネットワークで使用できる他のサービスを使用できます。

TACACS+ クライアント/サーバ プロトコルでは、トランスポート要件を満たすため TCP（TCP ポート 49）を使用します。TACACS+ プロトコルを使用して集中型の認証が提供されます。

ここでは、次の内容について説明します。

ユーザ ログインにおける TACACS+ の動作

パスワード認証プロトコル（PAP）を使用して TACACS+ サーバへのログインを試みると、次の一連のイベントが発生します。

1. 接続が確立すると、ユーザ名とパスワードを取得するために TACACS+ デーモンが接続されます。

（注）　TACACS+ では、デーモンがユーザを認証するために十分な情報を得られるまで、デーモンとユーザとの自由な対話を許可します。通常、デーモンはユーザ名とパスワードを入力するよう求めますが、ユーザの母親の旧姓などの追加情報を求めることもできます。

2. TACACS+ デーモンは、次のいずれかの応答を提供します。
   a. ACCEPT：ユーザの認証に成功したので、サービスを開始します。ユーザ許可が必要な場合は、許可が始まります。
   b. REJECT：ユーザの認証に失敗しました。TACACS+ デーモンは、ユーザに対してそれ以上のアクセスを拒否するか、ログイン シーケンスを再試行するよう要求します。
   c. ERROR：デーモンによる認証の途中でエラーが発生したか、またはネットワーク接続でエラーが発生しました。ERROR 応答を受信した場合、デバイスは別の方法でユーザの認証を試行します。

   認証後、さらに許可が必要な場合は、続いてユーザの許可フェーズに入ります。ユーザは TACACS+ 許可に進む前に、まず TACACS+ 認証を正常に完了する必要があります。
3. TACACS+ 許可が必要な場合は、TACACS+ デーモンに接続し、デーモンが ACCEPT または REJECT の許可応答を返します。ACCEPT 応答には、ユーザに対する EXEC または NETWORK セッションの送信に使用される属性が含まれます。また ACCEPT 応答により、ユーザがアクセス可能なサービスが決まります。

   サービスには次が含まれます。
   - Telnet、rlogin、Point-to-Point Protocol（PPP; ポイントツーポイント プロトコル）、Serial Line Internet Protocol（SLIP; シリアル ライン インターネット プロトコル）、EXEC サービス
   - 接続パラメータ（ホストまたはクライアントの IP アドレス、アクセス リスト、およびユーザ タイムアウトを含む）

デフォルトの TACACS+ サーバ暗号化タイプと事前共有キー

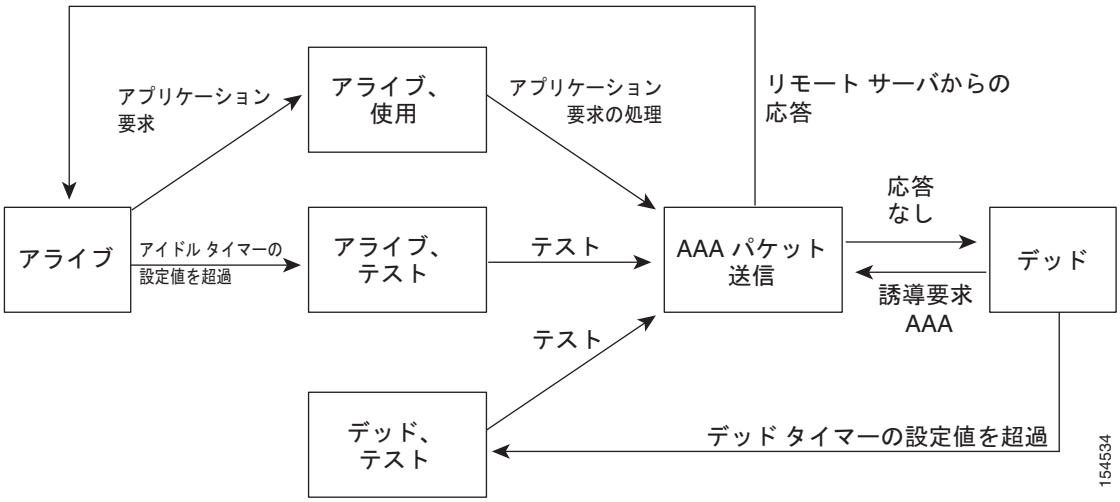
TACACS+ サーバに認証するには、TACACS+ 事前共有キーを設定する必要があります。事前共有キーは、デバイスと TACACS+ サーバ ホストの間で共有される秘密テキスト ストリングです。キーの長さは 63 文字で、出力可能な任意の ASCII 文字を含めることができます（スペースは使用できません）。すべての TACACS+ サーバ設定で使用されるグローバルな事前共有秘密キーを設定できます。

このグローバル事前共有キーの割り当ては、個別の TACACS+ サーバの設定時に明示的に **key** オプションを使用することによって上書きできます。

TACACS+ サーバ モニタリング

応答しない TACACS+ サーバはデッド（dead）としてマークされ、AAA 要求が送信されません。デッド TACACS+ サーバは定期的にモニタされ、応答があればアライブに戻されます。このプロセスにより、TACACS+ サーバが稼動状態であることを確認してから、実際の AAA 要求が送信されます。次の図に、TACACS+ サーバの状態変化によって、どのように Simple Network Management Protocol（SNMP; 簡易ネットワーク管理プロトコル）トラップが生成され、パフォーマンスに影響が出る前に障害を示すエラー メッセージが生成されるかを示します。

図 6-1　TACACS+ サーバの状態



（注）　アライブ サーバとデッド サーバのモニタリング間隔は異なります。これらはユーザが設定できます。TACACS+ サーバ モニタリングを実行するには、テスト認証要求を TACACS+ サーバに送信します。

ベンダー固有属性（VSA）

Internet Engineering Task Force（IETF; インターネット技術特別調査委員会）ドラフト標準には、ネットワーク アクセス サーバと TACACS+ サーバの間で Vendor-Specific Attribute（VSA; ベンダー固有属性）を伝達する方法が規定されています。IETF は、属性 26 を使用します。VSA を使用するとベンダーは、一般的な用途には適合しない独自の拡張属性をサポートできます。

シスコの VSA 形式

シスコの TACACS+ 実装では、IETF 仕様で推奨される形式を使用したベンダー固有オプションを 1 つサポートしています。シスコのベンダー ID は 9、サポートされるオプションのベンダー タイプは 1（名前付き cisco-av-pair）です。値は、次の形式のストリングです。

```
protocol : attribute separator value *
```

protocol は、特定の許可タイプを表すシスコの属性です。separator は、必須属性の場合は =（等号）、任意の属性の場合は *（アスタリスク）です。

認証に TACACS+ サーバを使用した場合、TACACS+ プロトコルでは TACACS+ サーバに対して、認証結果とともに権限付与情報などのユーザ属性を返すように指示します。この許可情報は、VSA で指定されます。

次に、サポートされる VSA プロトコル オプションを示します。

- shell：ユーザ プロファイル情報を提供する access-accept パケットで使用されるプロトコル。
- Accounting：accounting-request パケットで使用されるプロトコル。値にスペースが含まれている場合は、二重引用符で囲む必要があります。

次に、サポートされるその他の属性を示します。

- roles：ユーザが属するすべてのロールの一覧です。値は、ロール名をスペースで区切ったストリングです。このサブ属性は Access-Accept フレームの VSA 部分に格納され、TACACS+ サーバから送信されます。この属性はシェル プロトコル値とだけ併用できます。
- accountinginfo：標準の TACACS+ アカウンティング プロトコルに含まれる属性とともにアカウンティング情報を格納します。この属性は、スイッチ上の TACACS+ クライアントから、Account-Request フレームの VSA 部分にだけ格納されて送信されます。この属性と共に使用できるのは、アカウンティングの Protocol Data Unit（PDU; プロトコル データ ユニット）だけです。

TACACS+ の前提条件

TACACS+ には、次の前提条件があります。

- TACACS+ サーバの IP アドレスまたはホスト名を取得すること。
- TACACS+ サーバから事前共有キーを取得していること。
- Cisco Nexus 1000V が、AAA サーバの TACACS+ クライアントとして設定されていること。
- 次の手順に従って、リモート TACACS+ 認証を含む AAA がすでに設定されていること。
  - 「ログイン認証方式の設定」（P.4-6）
  - 「AAA の設定」（P.4-4）

注意事項および制約事項

TACACS+ に関する注意事項と制約事項は次のとおりです。

- 最大 64 の TACACS+ サーバを設定できます。
- TACACS+ のログレベルは 5 に設定する必要があります。

デフォルト設定

次の表に、TACACS+ のデフォルトを示します。

パラメータ	デフォルト
TACACS+	ディセーブル
デッド タイマー間隔	0 分
タイムアウト間隔	5 秒

パラメータ	デフォルト
アイドル タイマー間隔	0 分
サーバの定期的モニタリングのユーザ名	test
サーバの定期的モニタリングのパスワード	test

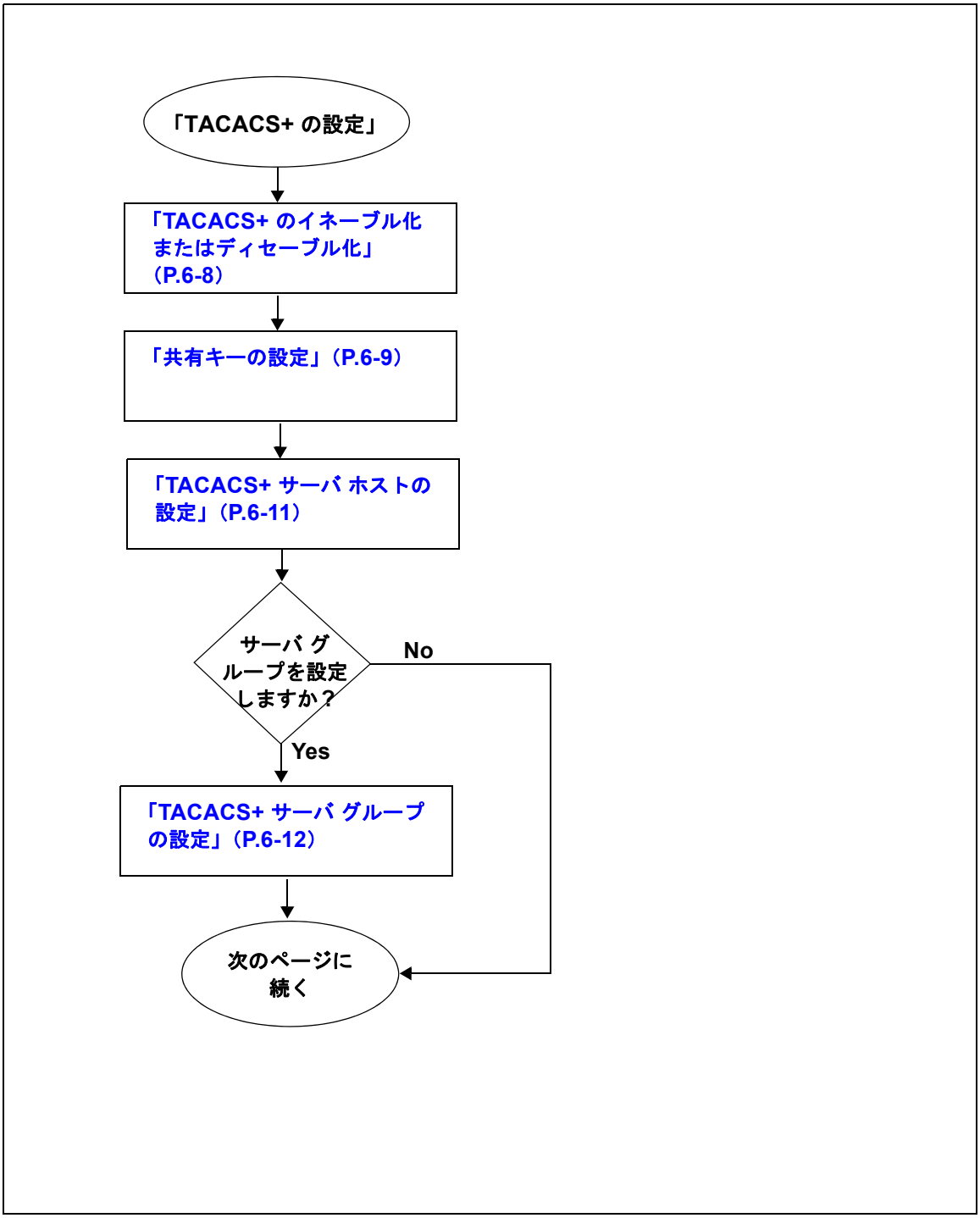
TACACS+ の設定

ここでは、次の内容について説明します。

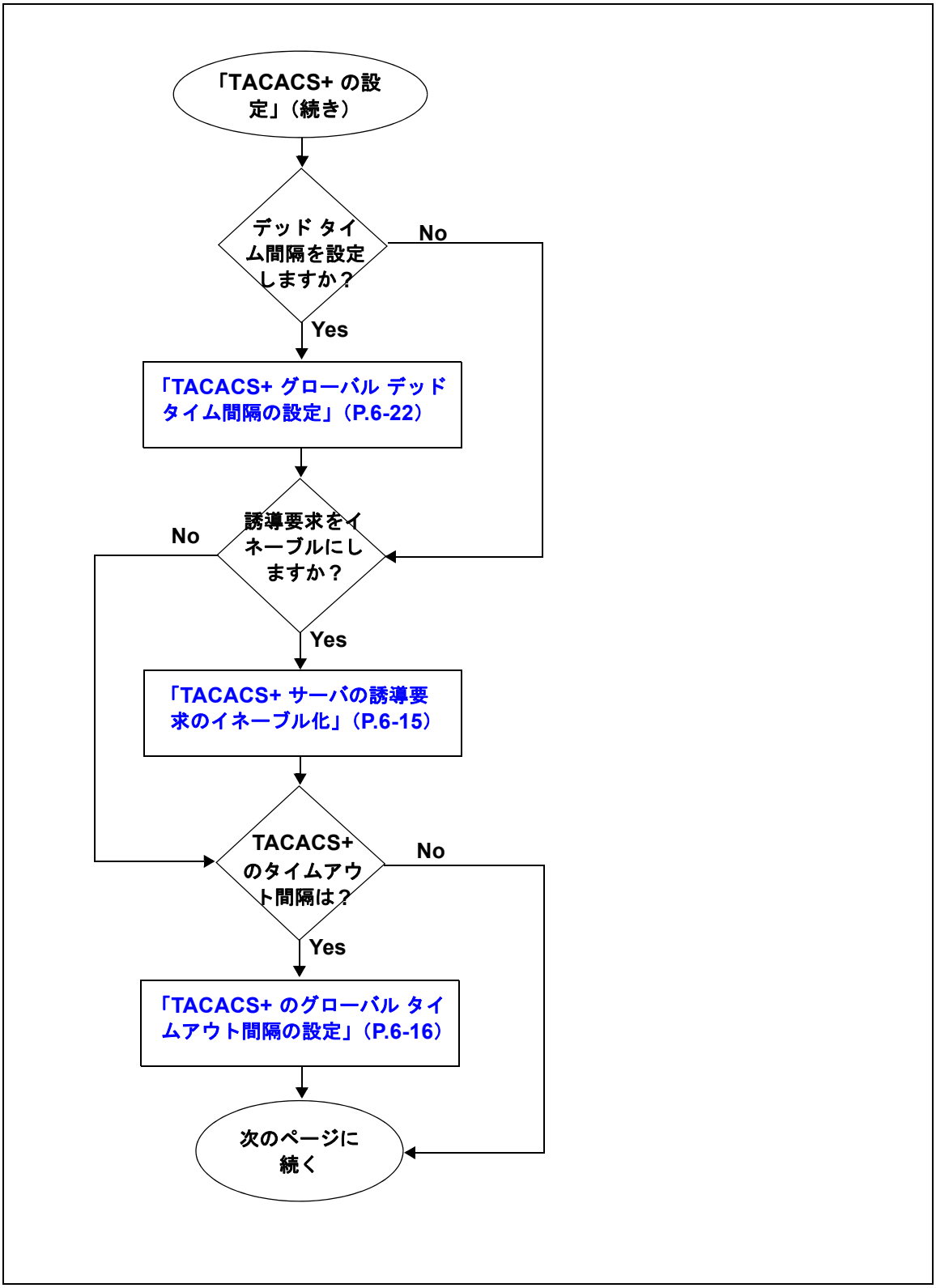
（注）　Cisco Nexus 1000V のコマンドは Cisco IOS のコマンドと異なる場合があることに注意してください。

TACACS+ を設定するには、次のフロー チャートを使用します。

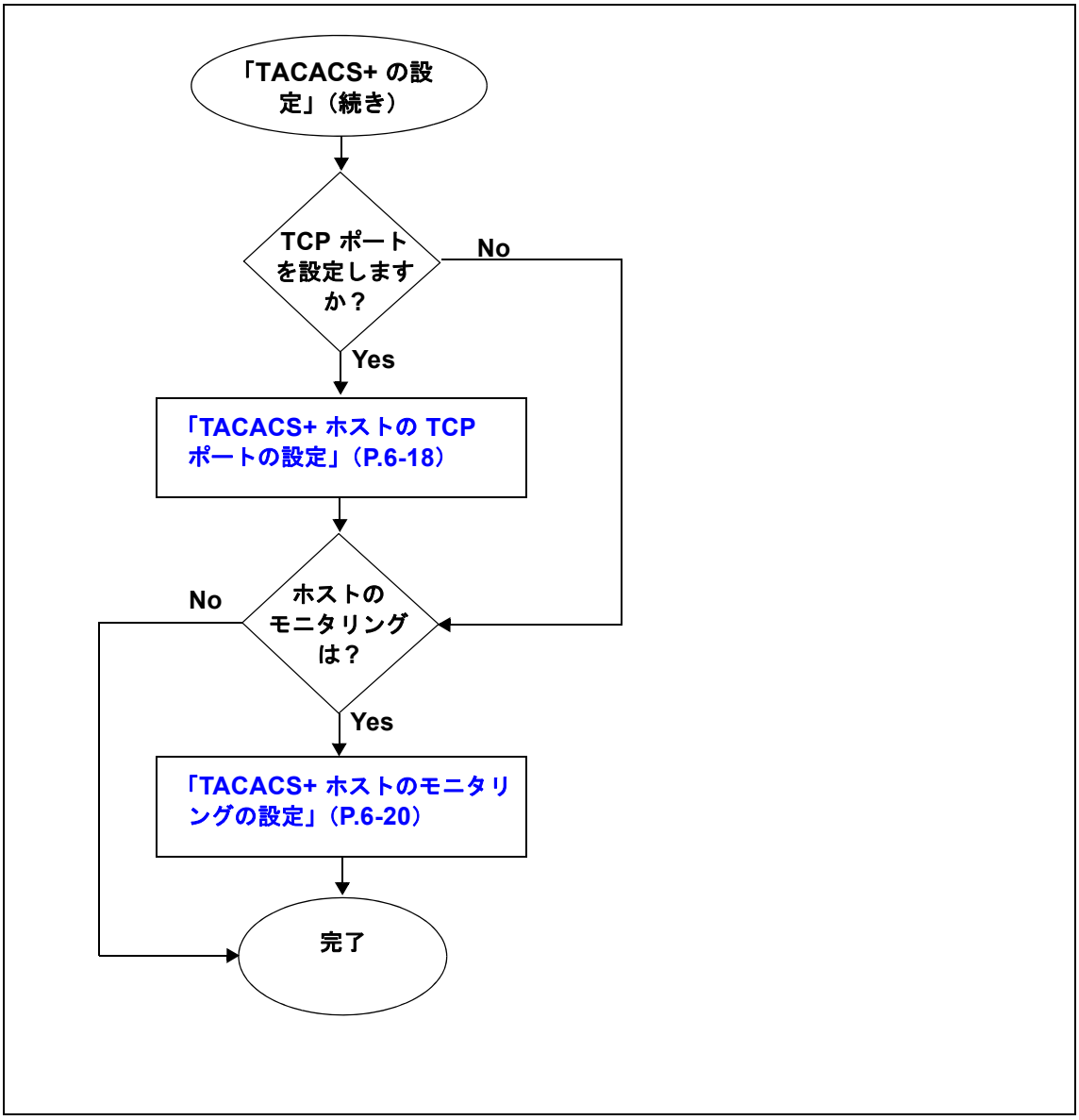
フロー チャート：「TACACS+ の設定」



フロー チャート：「TACACS+ の設定」（続き）



フロー チャート：「TACACS+ の設定」（続き）



TACACS+ のイネーブル化またはディセーブル化

TACACS+ をイネーブルまたはディセーブルにするには、次の手順を実行します。

はじめる前に

この手順を開始する前に、次のことを確認または実行しておく必要があります。

- EXEC モードで CLI にログインしていること。
- デフォルトでは、TACACS+ がディセーブルです。TACACS+ 認証をサポートするコンフィギュレーション コマンドと検証コマンドを使用するには、TACACS+ 機能を明示的にイネーブルにする必要があります。

注意　TACACS+ をディセーブルにすると、関連するすべての設定が自動的に廃棄されます。

手順の概要

1. **config t**
2. **[no] tacacs+ enable**
3. **exit**
4. **copy running-config startup-config**

手順の詳細

	コマンド	目的
ステップ 1	**config t** **Example:** n1000v# config t n1000v(config)#	CLI 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] tacacs+ enable** **Example:** n1000v(config)# tacacs+ enable n1000v(config)# **Example:** n1000v(config)# no tacacs+ enable n1000v(config)#	TACACS+ をイネーブルまたはディセーブルにします。
ステップ 3	**exit** **Example:** n1000v(config)# exit n1000v#	CLI グローバル コンフィギュレーション モードを終了し、EXEC モードに戻ります。
ステップ 4	**copy running-config startup-config** **Example:** n1000v# copy running-config startup-config	（任意）行った変更を、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。

共有キーの設定

次のものを設定するには、次の手順を実行します。

- グローバル キー（Cisco Nexus 1000V とすべての TACACS+ サーバ ホストの間で共有される秘密テキスト ストリング）
- キー（Cisco Nexus 1000V と単一の TACACS+ サーバ ホストの間で共有される秘密テキスト ストリング）

はじめる前に

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。

- EXEC モードで CLI にログインしていること。
- 認証用に TACACS+ がイネーブルになっていること。
「TACACS+ のイネーブル化またはディセーブル化」（P.6-8）の手順を参照してください。
- TACACS+ サーバ ホストのキーがわかっています。
- デフォルトでは、グローバル キーは設定されません。

手順の概要

1. **config t**
2. **tacacs-server key** [**0** | **7**] *global_key*
3. **exit**
4. **show tacacs-server**
5. **copy running-config startup-config**

手順の詳細

	コマンド	目的
ステップ 1	**config t** **Example:** n1000v# config t n1000v(config)#	CLI 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	Do one of the following: • すべての TACACS+ サーバ ホストのグローバル キーを設定する場合は、次のステップに進みます。 • 単一の TACACS+ サーバ ホストのキーを設定する場合は、ステップ 5 に進みます。	
ステップ 3	**tacacs-server key** [**0** | **7**] *global_key* **Example:** n1000v(config)# tacacs-server key 0 QsEFtkI# n1000v(config)#	Cisco Nexus 1000V と TACACS+ サーバ ホストの間で共有されるグローバル キーを指定します。 **0**：使用するクリア テキスト ストリング（キー）を指定します（デフォルト）。 **7**：使用する暗号化ストリング（キー）を指定します。 **global_key**：最大 63 文字のストリングです。 デフォルトでは、グローバル キーは設定されません。
ステップ 4	ステップ 6 に進みます。	
ステップ 5	**tacacs-server host** {*ipv4-address* | *host-name*} **key** [**0** | **7**] *shared_key* **Example:** n1000v(config)# tacacs-server host 10.10.1.1 key 0 PlIjUhYg n1000v(config)#	Cisco Nexus 1000V と指定した TACACS+ サーバ ホストの間で共有されるキーを指定します。 **0**：使用するクリア テキスト ストリング（キー）を指定します（デフォルト）。 **7**：使用する暗号化ストリング（キー）を指定します。 **global_key**：最大 63 文字のストリングです。 グローバル共有キーではなく、この共有キーが使用されます。

	コマンド	目的
ステップ 6	**exit** **Example:** n1000v(config)# exit n1000v#	CLI グローバル コンフィギュレーション モードを終了し、EXEC モードに戻ります。
ステップ 7	**show tacacs-server** **Example:** n1000v# show tacacs-server Global TACACS+ shared secret:******** timeout value:5 deadtime value:0 total number of servers:1 following TACACS+ servers are configured: 10.10.2.2: available on port:49	（任意）TACACS+ サーバの設定を表示します。 **（注）** グローバル共有キーは実行コンフィギュレーションに暗号化形式で保存されます。キーを表示するには、**show running-config** コマンドを使用します。
ステップ 8	**copy running-config startup-config** **Example:** n1000v# copy running-config startup-config	（任意）これらの実行コンフィギュレーションの変更内容を、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。

TACACS+ サーバ ホストの設定

TACACS+ サーバを TACACS+ ホストとして設定するには、次の手順を実行します。

はじめる前に

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。

- EXEC モードで CLI にログインしていること。
- 認証用に TACACS+ がイネーブルになっていること。
  「TACACS+ のイネーブル化またはディセーブル化」（P.6-8）の手順を参照してください。
- 次の手順に従って、共有キーがすでに設定されています。
  「共有キーの設定」（P.6-9）の手順
- リモート TACACS+ サーバ ホストの IP アドレスまたはホスト名がわかっています。
- すべての TACACS+ サーバ ホストはデフォルトの TACACS+ サーバ グループに追加されます。

手順の概要

1. **config t**
2. **tacacs-server host** {*ipv4-address* | *host-name*}
3. **exit**
4. **show tacacs-server**
5. **copy running-config startup-config**

手順の詳細

	コマンド	目的
ステップ 1	**config t** **Example:** n1000v# config t n1000v(config)#	CLI 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	**tacacs-server host** {*ipv4-address* | *host-name*} **Example:** n1000v(config)# tacacs-server host 10.10.2.2	サーバの IP アドレスまたはホスト名を TACACS+ サーバ ホストとして設定します。
ステップ 3	**exit** **Example:** n1000v(config)# exit n1000v#	CLI グローバル コンフィギュレーション モードを終了し、EXEC モードに戻ります。
ステップ 4	**show tacacs-server** **Example:** n1000v# **show tacacs-server** timeout value:5 deadtime value:0 total number of servers:1 following TACACS+ servers are configured: 10.10.2.2: available on port:49 n1000v#	（任意）TACACS+ サーバの設定を表示します。
ステップ 5	**copy running-config startup-config** **Example:** n1000v# copy running-config startup-config	（任意）これらの実行コンフィギュレーションの変更内容を、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。

TACACS+ サーバ グループの設定

メンバー サーバが認証機能を共有する TACACS+ サーバ グループを設定するには、次の手順を実行します。

はじめる前に

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。

- EXEC モードで CLI にログインしていること。
- TACACS+ サーバ グループに追加されたすべてのサーバは、TACACS+ プロトコルを使用する必要があります。
- TACACS+ サーバ グループが設定されると、メンバーのサーバへのアクセスは、サーバを設定した順番で行われます。
- 認証用に TACACS+ がイネーブルになっていること。
「TACACS+ のイネーブル化またはディセーブル化」（P.6-8）の手順を参照してください。

- 次の手順に従って、事前共有キーがすでに設定されています。

  「共有キーの設定」（P.6-9）の手順

- TACACS+ サーバ グループは、1 つのサーバが応答できない場合に備えて、フェールオーバーを提供することができます。グループ内の最初のサーバが応答しない場合は、同じグループ内の次のサーバが試行され、サーバが応答するまでこの処理が行われます。これと同じように、複数のサーバ グループが相互にフェールオーバーを提供できます。

手順の概要

1. **config t**
2. **aaa group server tacacs+** *group-name*
3. **server** {*ipv4-address* | *host-name*}
4. **deadtime** *minutes*
5. **use-vrf** *vrf-name*
6. （任意）**source-interface** {*interface-type*} {*interface-number*}
7. （任意）**show tacacs-server groups**
8. （任意）**copy running-config startup-config**

手順の詳細

	コマンド	目的

ステップ 1	**config t**
	
	Example:
	`n1000v# config t`
	`n1000v(config)#`
		CLI 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	**aaa group server tacacs+** *group-name*
	
	Example:
	`n1000v(config)# aaa group server tacacs+ TacServer`
	`n1000v(config-tacacs+)#`
		指定した名前で TACACS+ サーバ グループを作成し、そのグループの TACACS+ 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	**server** {*ipv4-address* | *host-name*}
	
	Example:
	`n1000v(config-tacacs+)# server 10.10.2.2`
	`n1000v(config-tacacs+)#`
		TACACS+ サーバのホスト名または IP アドレスを TACACS+ サーバ グループのメンバーとして設定します。
		ヒント 指定した TACACS+ サーバが見つからない場合は、**tacacs-server host** コマンドを使用してサーバを設定し、このコマンドをもう一度実行します。

ステップ 4	**deadtime** *minutes*
	
	Example:
	`n1000v(config-tacacs+)# deadtime 30`
	`n1000v(config-tacacs+)#`
		（任意）この TACACS+ グループのモニタリングのデッド タイムを設定します。デフォルト値は 0 分です。指定できる範囲は 0 ～ 1440 です。
		（注） デッド タイム間隔がゼロ（0）より大きい TACACS+ サーバ グループの場合は、その値がグローバル デット タイム値に優先します（「TACACS+ グローバル デッド タイム間隔の設定」（P.6-22）の手順を参照）。

	コマンド	目的
ステップ 5	**use-vrf** *vrf-name* **Example:** n1000v(config-tacacs+)# use-vrf management n1000v(config-tacacs+)#	（任意）このサーバ グループとの接続に使用する Virtual Routing and Forwarding（VRF; 仮想ルーティングおよび転送）インスタンスを指定します。
ステップ 6	**source-interface** {*interface-type*} {*interface-number*} **Example:** n1000v(config-tacacs+)# source-interface mgmt0 n1000v(config-tacacs+)#	（任意）TACACS+ サーバに到達するために使用される送信元インターフェイスを指定します。 • loopback = 0 ～ 1023 の仮想インターフェイス番号 • mgmt = 管理インターフェイス 0 • null = ヌル インターフェイス 0 • port-channel = 1 ～ 4096 のポート チャネル番号
ステップ 7	**show tacacs-server groups**	（任意）TACACS+ サーバ グループの設定を表示します。

Example:

```
n1000v(config-tacacs+)# show tacacs-server groups
total number of groups:1

following TACACS+ server groups are configured:
        group TacServer:
                server 10.10.2.2 on port 49
                deadtime is 30
                vrf is management
n1000v(config-tacacs+)#
```

ステップ 8	**copy running-config startup-config** **Example:** n1000v(config-tacacs+)# copy running-config startup-config	（任意）実行コンフィギュレーションで行ったこれらの変更内容を、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。

Example:

```
n1000v(config)# aaa group server tacacs+ TacServer
n1000v(config-tacacs+)# server 10.10.2.2
n1000v(config-tacacs+)# deadtime 30
n1000v(config-tacacs+)# use-vrf management
n1000v(config-tacacs+)# show tacacs-server groups
total number of groups:1

following TACACS+ server groups are configured:
        group TacServer:
                server 10.10.2.2 on port 49
                deadtime is 30
                vrf is management
n1000v(config-tacacs+)#
```

TACACS+ サーバの誘導要求のイネーブル化

認証要求の送信先の TACACS+ サーバをユーザが指定できるようにするには、次の手順を実行します。これは directed-request（誘導要求）と呼ばれます。

はじめる前に

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。

- EXEC モードで CLI にログインしていること。
- 認証用に TACACS+ がイネーブルになっていること。
「TACACS+ のイネーブル化またはディセーブル化」（P.6-8）の手順を参照してください。

（注）　ユーザ指定のログインは Telnet セッションに限りサポートされます。

- 誘導要求をイネーブルにした場合、ユーザは *username@vrfname:hostname* としてログインできます（*vrfname* は使用する VRF、*hostname* は設定された TACACS+ サーバの名前）。

手順の概要

1. **config t**
2. **tacacs-server directed-request**
3. **exit**
4. **show tacacs-server directed-request**
5. **copy running-config startup-config**

手順の詳細

	コマンド	目的

ステップ 1	**config t**
	
	Example:
	`n1000v# config t`
	`n1000v(config)#`
		CLI 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	**tacacs-server directed-request**
	
	Example:
	`n1000v(config)# tacacs-server directed-request`
	`n1000v(config)#`
		ログイン時に認証要求を送信する TACACS+ サーバを指定するために、誘導要求の使用をイネーブルにします。デフォルトはディセーブルです。

ステップ 3	**exit**
	
	Example:
	`n1000v(config)# exit`
	`n1000v#`
		CLI グローバル コンフィギュレーション モードを終了し、EXEC モードに戻ります。

	コマンド	目的
ステップ 4	**show tacacs-server directed-request** **Example:** n1000v# show tacacs-server directed-request enabled n1000v#	（任意）TACACS+ の directed request の設定を表示します。
ステップ 5	**copy running-config startup-config** **Example:** n1000v# 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。

TACACS+ のグローバル タイムアウト間隔の設定

Cisco Nexus 1000V が任意の TACACS+ サーバからの応答を待つ時間を秒単位で設定するには、次の手順を実行します。これを過ぎるとタイムアウトが宣言されます。

はじめる前に

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。

- EXEC モードで CLI にログインしていること。
- 認証用に TACACS+ がイネーブルになっていること。
「TACACS+ のイネーブル化またはディセーブル化」（P.6-8）の手順を参照してください。
- 個別の TACACS+ サーバに指定したタイムアウトは、グローバル タイムアウト間隔に優先します。個別サーバのタイムアウトの設定については、「個別 TACACS+ ホストのタイムアウト間隔の設定」（P.6-17）の手順を参照してください。

手順の概要

1. **config t**
2. **tacacs-server timeout** *seconds*
3. **exit**
4. **show tacacs-server**
5. **copy running-config startup-config**

手順の詳細

	コマンド	目的
ステップ 1	**config t** **Example:** n1000v# config t n1000v(config)#	CLI 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	**tacacs-server timeout** *seconds* **Example:** n1000v(config)# tacacs-server timeout 10	Cisco Nexus 1000V がサーバからの応答を待つ時間を秒単位で指定します。デフォルトのタイムアウト間隔は 5 秒です。有効な範囲は 1 ～ 60 秒です。

	コマンド	目的
ステップ 3	**exit** **Example:** n1000v(config)# exit n1000v#	CLI グローバル コンフィギュレーション モードを終了し、EXEC モードに戻ります。
ステップ 4	**show tacacs-server** **Example:** n1000v# show tacacs-server Global TACACS+ shared secret:******** timeout value:10 deadtime value:0 total number of servers:1 following TACACS+ servers are configured: 10.10.2.2: available on port:49 n1000v#	（任意）TACACS+ サーバの設定を表示します。
ステップ 5	**copy running-config startup-config** **Example:** n1000v# copy running-config startup-config	（任意）実行コンフィギュレーションで行ったこれらの変更内容を、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。

個別 TACACS+ ホストのタイムアウト間隔の設定

Cisco Nexus 1000V が特定の TACACS+ サーバからの応答を待つ時間を秒単位で設定するには、次の手順を実行します。これを過ぎるとタイムアウトが宣言されます。この設定は TACACS+ ホスト単位で設定します。

はじめる前に

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。

- EXEC モードで CLI にログインしていること。
- 認証用に TACACS+ がイネーブルになっていること。
「TACACS+ のイネーブル化またはディセーブル化」（P.6-8）の手順を参照してください。
- 個別の TACACS+ サーバのタイムアウト設定は、グローバル タイムアウト間隔に優先します。

手順の概要

1. **config t**
2. **tacacs-server host** {*ipv4-address* | *host-name*} **timeout** *seconds*
3. **exit**
4. **show tacacs-server**
5. **copy running-config startup-config**

手順の詳細

	コマンド	目的
ステップ 1	**config t** **Example:** n1000v# config t n1000v(config)#	CLI 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	**tacacs-server host** {*ipv4-address* | *host-name*} **timeout** *seconds* **Example:** n1000v(config)# tacacs-server host 10.10.2.2 timeout 10 n1000v(config)#	特定のサーバのタイムアウト間隔を指定します。デフォルトはグローバル タイムアウト間隔です。 詳細については、「TACACS+ のグローバル タイムアウト間隔の設定」（P.6-16）の手順を参照してください。
ステップ 3	**exit** **Example:** n1000v(config)# exit n1000v#	CLI グローバル コンフィギュレーション モードを終了し、EXEC モードに戻ります。
ステップ 4	**show tacacs-server** **Example:** n1000v# show tacacs-server Global TACACS+ shared secret:******** timeout value:10 deadtime value:0 total number of servers:1 following TACACS+ servers are configured: 10.10.2.2: available on port:49 timeout:10 n1000v#	（任意）TACACS+ サーバの設定を表示します。
ステップ 5	**copy running-config startup-config** **Example:** n1000v# copy running-config startup-config	（任意）実行コンフィギュレーションで行ったこれらの変更内容を、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。

TACACS+ ホストの TCP ポートの設定

ポート 49（TACACS+ 要求のデフォルト）以外の TCP ポートを設定するには、次の手順を実行します。

はじめる前に

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。

- EXEC モードで CLI にログインしていること。
- 認証用に TACACS+ がイネーブルになっていること。
  「TACACS+ のイネーブル化またはディセーブル化」（P.6-8）の手順を参照してください。
- 「TACACS+ サーバ ホストの設定」（P.6-11）の手順に従って TACACS+ サーバが設定されています。

手順の概要

1. **config t**
2. **tacacs-server host** {*ipv4-address* | *host-name*} **port** *tcp-port*
3. **exit**
4. **show tacacs-server**
5. **copy running-config startup-config**

手順の詳細

	コマンド	目的

ステップ 1	**config t**
	
	Example:
	`n1000v# config t`
	`n1000v(config)#`
		CLI 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	**tacacs-server host** {*ipv4-address* | *host-name*} **port** *tcp-port*
	
	Example:
	`n1000v(config)# tacacs-server host 10.10.2.2 port 2`
	`n1000v(config)#`
		使用する TCP ポートを指定します。
		有効な範囲：1 ～ 65535
		デフォルト：49

ステップ 3	**exit**
	
	Example:
	`n1000v(config)# exit`
	`n1000v#`
		CLI グローバル コンフィギュレーション モードを終了し、EXEC モードに戻ります。

ステップ 4	**show tacacs-server**
	
	Example:
	`n1000v# show tacacs-server`
	`Global TACACS+ shared secret:********`
	`timeout value:10`
	`deadtime value:0`
	`total number of servers:1`
	
	`following TACACS+ servers are configured:`
	`10.10.2.2:`
	`available on port:2`
	`timeout:10`
	`n1000v#`
		（任意）TACACS+ サーバの設定を表示します。

ステップ 5	**copy running-config startup-config** **Example:** `n1000v# 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。

TACACS+ ホストのモニタリングの設定

TACACS+ ホストの定期モニタリングを設定するには、次の手順を実行します。

はじめる前に

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。

- EXEC モードで CLI にログインしていること。
- 認証用に TACACS+ がイネーブルになっていること。
「TACACS+ のイネーブル化またはディセーブル化」（P.6-8）の手順を参照してください。
- TACACS+ サーバが設定されていること。
「TACACS+ サーバ ホストの設定」（P.6-11）の手順を参照してください。
- アイドル タイマーには、TACACS+ サーバがアイドル（要求を受信しない）状態を続ける時間を指定します。これを過ぎると TACACS+ サーバにテスト パケットが送信されます。
- デフォルトのアイドル タイマー値は 0 分です。アイドル時間の間隔が 0 分の場合、TACACS+ サーバの定期モニタリングは実行されません。

手順の概要

1. **config t**
2. **tacacs-server host** {*ipv4-address* | *host-name*} **test** {**idle-time** *minutes* | **password** *password* [**idle-time** *minutes*] | **username** *name* [**password** *password* [**idle-time** *minutes*]]}
3. **tacacs-server dead-time** *minutes*
4. **exit**
5. **show tacacs-server**
6. **copy running-config startup-config**

手順の詳細

	コマンド	目的
ステップ 1	**config t** **Example:** n1000v# config t n1000v(config)#	CLI 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	**tacacs-server host** {*ipv4-address* | *host-name*} **test** {**idle-time** *minutes* | **password** *password* [**idle-time** *minutes*] | **username** *name* [**password** *password* [**idle-time** *minutes*]]} **Example:** n1000v(config)# tacacs-server host 10.10.2.2 test username pvk2 password a3z9yjqz7 idle-time 3	サーバ モニタリングを設定します。 **username**：デフォルトは test です。 **（注）** ネットワークのセキュリティを保護するために、TACACS+ データベースに存在しないユーザ名を割り当てることを推奨します。 **password**：デフォルトは test です。 **idle-time**：デフォルトは 0 分です。指定できる範囲は、0 ～ 1440 分です。 **（注）** TACACS+ サーバの定期的なモニタリングを行うには、アイドル タイマーに 0 より大きな値を設定する必要があります。
ステップ 3	**tacacs-server dead-time** *minutes* **Example:** n1000v(config)# tacacs-server dead-time 5	以前に応答しなかった TACACS+ サーバのチェックを始めるまでの時間を分単位で指定します。デフォルト値は 0 分です。有効な範囲は 0 ～ 1440 分です。
ステップ 4	**exit** **Example:** n1000v(config)# exit n1000v#	CLI グローバル コンフィギュレーション モードを終了し、EXEC モードに戻ります。
ステップ 5	**show tacacs-server** **Example:** n1000v# show tacacs-server Global TACACS+ shared secret:******** timeout value:10 deadtime value:0 total number of servers:1 following TACACS+ servers are configured: 10.10.2.2: available on port:2 timeout:10 n1000v#	（任意）TACACS+ サーバの設定を表示します。
ステップ 6	**copy running-config startup-config** **Example:** n1000v# copy running-config startup-config	（任意）これらの実行コンフィギュレーションに行った変更内容を、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。

TACACS+ グローバル デッド タイム間隔の設定

以前に応答しなかったサーバにテスト パケットを送信するまで待機する時間を設定するには、次の手順を実行します。

はじめる前に

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。

- EXEC モードで CLI にログインしていること。
- 認証用に TACACS+ がイネーブルになっていること。
「TACACS+ のイネーブル化またはディセーブル化」（P.6-8）の手順を参照してください。
- TACACS+ サーバが設定されていること。
「TACACS+ サーバ ホストの設定」（P.6-11）の手順を参照してください。
- デッド タイム間隔が 0 分の場合、TACACS+ サーバは、応答を返さない場合でも、デットとしてマークされません。デッド タイマーはグループ単位で設定できます（「TACACS+ サーバ グループの設定」（P.6-12）の手順を参照）。

手順の概要

1. **config t**
2. **tacacs-server deadtime** *minutes*
3. **exit**
4. **show tacacs-server**
5. **copy running-config startup-config**

手順の詳細

	コマンド	目的

ステップ 1	**config t**
	
	Example:
	`n1000v# config t`
	`n1000v(config)#`
		CLI 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	**tacacs-server deadtime** *minutes* **Example:** `n1000v(config)# tacacs-server deadtime 5`	グローバルなデッド タイム間隔を設定します。デフォルト値は 0 分です。有効な範囲は、1 ～ 1440 分です。

ステップ 3	**exit**
	
	Example:
	`n1000v(config)# exit`
	`n1000v#`
		CLI グローバル コンフィギュレーション モードを終了し、EXEC モードに戻ります。

	コマンド	目的
ステップ 4	**show tacacs-server** **Example:** n1000v# show tacacs-server	（任意）TACACS+ サーバの設定を表示します。
ステップ 5	**copy running-config startup-config** **Example:** n1000v# 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。

TACACS+ ホストの統計情報の表示

TACACS+ ホストの統計情報を表示するには、次の手順を実行します。

はじめる前に

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。

- EXEC モードで CLI にログインしていること。
- 認証用に TACACS+ がイネーブルになっていること。
  「TACACS+ のイネーブル化またはディセーブル化」（P.6-8）の手順を参照してください。
- TACACS+ サーバが設定されていること。
  「TACACS+ サーバ ホストの設定」（P.6-11）の手順を参照してください。

手順の概要

1. **show tacacs-server statistics** {*hostname* | *ipv4-address*}

手順の詳細

	コマンド	目的
ステップ 1	**show tacacs-server statistics** {*hostname* | *ipv4-address*}	TACACS+ ホストの統計情報を表示します。

Example:

```
n1000v# show tacacs-server statistics 10.10.1.1
Server is not monitored

Authentication Statistics
        failed transactions: 9
        sucessfull transactions: 2
        requests sent: 2
        requests timed out: 0
        responses with no matching requests: 0
        responses not processed: 0
        responses containing errors: 0

Authorization Statistics
        failed transactions: 1
        sucessfull transactions: 0
        requests sent: 0
```

```
        requests timed out: 0
        responses with no matching requests: 0
        responses not processed: 0
        responses containing errors: 0

Accounting Statistics
        failed transactions: 0
        sucessfull transactions: 0
        requests sent: 0
        requests timed out: 0
        responses with no matching requests: 0
        responses not processed: 0
        responses containing errors: 0
```

TACACS+ の設定例

次に、TACACS+ 設定の例を示します。

```
feature tacacs+
tacacs-server key 7 "ToIkLhPpG"
tacacs-server host 10.10.2.2 key 7 "ShMoMhTl"
aaa group server tacacs+ TacServer
    server 10.10.2.2
```

TACACS+ 機能の履歴

ここでは、TACACS+ のリリース履歴を示します。

機能名	リリース	機能情報
TACACS+	4.0(4)SV1(1)	この機能が導入されました。

その他の関連資料

TACACS+ の実装に関連する詳細情報については、次を参照してください。

- 「関連資料」（P.6-25）
- 「標準」（P.6-25）

関連資料

関連項目	参照先
CLI	*『Cisco Nexus 1000V Command Reference, Release 4.2(1)SV1(4a)』*
システム管理	*『Cisco Nexus 1000V System Management Configuration Guide, Release 4.2(1)SV1(4a)』*

標準

標準	タイトル
この機能でサポートされる新規の標準または変更された標準はありません。また、既存の標準のサポートは変更されていません。	—

CHAPTER 7

SSH の設定

この章では、セキュア シェル（SSH）プロトコルを設定する手順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。

SSH の概要

ここでは、次の内容について説明します。

SSH サーバ

SSH サーバを使用すると、SSH クライアントはセキュアな暗号化された接続を確立できます。SSH は強化暗号化を使用して認証を行います。SSH サーバは、市販の一般的な SSH クライアントとの相互運用が可能です。

SSH では、TACACS+ ユーザ認証およびローカルに保存されたユーザ名とパスワードがサポートされます。

SSH クライアント

SSH クライアントは、SSH プロトコルで稼動しデバイス認証および暗号化を提供するアプリケーションです。SSH クライアントをインストールすると、SSH サーバを実行する任意のデバイスとの間でセキュアな暗号化された接続を確立できるようになります。この接続を通して、暗号化されたアウトバウンド接続が提供されます。SSH クライアントは、認証および暗号化により、非セキュアなネットワーク上でセキュアな通信ができます。

SSH クライアントは、市販の一般的な SSH サーバと連動します。

SSH サーバ キー

SSH では、セキュアな通信を行うためにサーバ キーが必要です。SSH サーバ キーは、次の SSH オプションに使用できます。

- Rivest, Shamir, and Adelman（RSA）公開キー暗号化を使用した SSH バージョン 2
- Digital System Algrorithm（DSA）を使用した SSH バージョン 2

SSH サービスをイネーブルにする前に、正しいバージョンの SSH サーバ キー ペアを取得しておいてください。使用する SSH クライアントのバージョンに応じた SSH サーバ キー ペアを生成します。SSH サービスは、SSH バージョン 2 で使用する次の 2 種類のキー ペアを受け入れます。

- **dsa** オプションを使用すると、SSH バージョン 2 プロトコルに対応する DSA キーペアが生成されます。
- **rsa** オプションを使用すると、SSH バージョン 2 プロトコルに対応する RSA キーペアが生成されます。

デフォルトでは、1024 ビットの RSA キーが生成されます。

SSH は、次の公開キー形式をサポートします。

- OpenSSH
- IETF SSH（SECSH）
- Privacy-Enhanced Mail（PEM）の公開キー証明書

注意　SSH キーをすべて削除すると、SSH サービスを開始できません。

SSH の前提条件

SSH には次の前提条件があります。

- レイヤ 3 インターフェイス上に IP、mgmt 0 インターフェイス上にアウトバンド、またはイーサネット インターフェイス上にインバンドを設定していること
- SSH サーバをイネーブルにする前に、SSH キーを取得すること

注意事項および制約事項

- SSH バージョン 2（SSHv2）のみがサポートされます。
- SSH はデフォルトでイネーブルになります。

- Cisco NX-OS のコマンドは Cisco IOS のコマンドと異なる場合があります。

デフォルト設定

次の表に、SSH のデフォルト設定を示します。

パラメータ	デフォルト
SSH サーバ	イネーブル
SSH サーバ キー	1024 ビットで生成された RSA キー
RSA キー生成ビット数	1024

SSH の設定

ここでは、次の内容について説明します。

SSH サーバ キーの生成

セキュリティ要件に応じた SSH サーバ キーを生成するには、次の手順を実行します。

はじめる前に

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。

- EXEC モードで CLI にログインしていること。
- デフォルトの SSH サーバ キーは、1024 ビットで生成される RSA キーです。

手順の概要

1. **config t**
2. **no feature ssh**
3. **ssh key** {**dsa** [**force**] | **rsa** [*bits* **[force**]]}
4. **feature ssh**
5. **exit**
6. **show ssh key**
7. **copy running-config startup-config**

手順の詳細

	コマンド	目的
ステップ 1	**config t** **Example:** n1000v# config t n1000v(config)#	CLI 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 feature ssh** **Example:** n1000v(config)# no feature ssh	SSH をディセーブルにします。
ステップ 3	**ssh key** {**dsa** [**force**] | **rsa** [*bits* [**force**]]} **Example:** n1000v(config)# ssh key dsa force	SSH サーバ キーを生成します。 *bits* 引数には、キーの生成に使用するビット数を指定します。有効な範囲は 768 ～ 2048 です。デフォルト値は 1024 です。 既存のキーを置き換える場合は、キーワード **force** を使用します。
ステップ 4	**feature ssh** **Example:** n1000v(config)# feature ssh	SSH をイネーブルにします。
ステップ 5	**show ssh key** **Example:** n1000v# show ssh key	（任意）SSH サーバ キーを表示します。
ステップ 6	**copy running-config startup-config** **Example:** n1000v# 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。

```
Example:
n1000v# config t
n1000v(config)# no feature ssh
XML interface to system may become unavailable since ssh is disabled
n1000v(config)# ssh key dsa force
generating dsa key(1024 bits).....
.
generated dsa key
n1000v(config)# feature ssh
n1000v(config)# show ssh key
*************************************
rsa Keys generated:Sun Jul 27 15:18:46 2008

ssh-rsa AAAAB3NzaC1yc2EAAAABIwAAAQEAyKcb7Nv9Ki1OOId9/tdHHa/ngQujlvK5mXyL/n+DeOXK
fVhHbX2a+V0cm7CCLUkBh+BvZRmpmOVTmU/5awfVhVxMKXMiPOPBc+A6/n3FVroyRwupMki6mWoM6Uwa
GID5gsVPqFjFNSgMWtbhjo97XVKhgjFW+wOVt8QoAcrEtnwEfsnQk1EIr/0XIP1mqTsrqTsmjZ2vLk+f
FzTGYAxMvYZI+BrN47aoH2ywS7CpnODjCDXJuDYSPbc3PA8t0ghU/60m9R+s6AZPuljVQbGfxPrahEu4
GVc6sMJNU1JxmqDJkodhMArObB4Umzj7E3Rdby/ZWx/clTYiXQR1X1VfhQ==

bitcount:2048
fingerprint:
fd:ca:48:73:b9:ee:e7:86:9e:1e:40:46:f1:50:1d:44
*************************************
dsa Keys generated:Sun Jul 27 15:20:12 2008
```

```
ssh-dss AAAAB3NzaC1kc3MAAACBALpdxLjXNS/jcCNY+F1QZV9HegxBEb0DMUmq9bSq2N+KAcvHllEh
GnaiHhqarOlcEKqhLbIbuqtKTCvfa+Y1hBIAhWVjg1UR3/M22jqxnfhnxL5YRc1Q7fcesFax0myayAIU
nXrkO5iwv9XHTu+EInRc4kJ0XrG9SxtLmDe/fi2ZAAAAFQDbRabAjZa6GfDpwjXw5smRhrElJwAAAIEA
r50yi3hHawNnb5qgYLXhN+KA8XJF753eCWHtMw7NR8fz6fjQ1R2J97UjjGuQ8DvwpGeNQ5S+AuIo0rGq
svdg7TTecBcbgBOnR7Fs2+W5HiSVEGbvj1xaeK8fkNE6kaJumBB343b8Rgj0G97MP/os1GfkEqmX9glB
0IOM2mgHHyoAAACAfRir27hHy+fw8CxPlsK0R6cFhxYyd/qYYogXFKYIOPxpLoYrjqODeOFThU7TJuBz
aS97eXiruzbffHwzUGfXgmQT5o9IMZRTClWPA/5Ju4O9YABYHccUghf0W+QtgGOT6FOSvBh8uOV0kcHC
GMJAP8omphauZJlc+wgFxhnkyh4=

bitcount:1024
fingerprint:
44:91:32:1f:7a:d1:83:3c:f3:5e:db:53:0a:2d:ce:69
***********************************
```

公開キーを持つユーザ アカウントの設定

SSH 公開キーを設定して、SSH クライアントでパスワードの入力を求められずにログインするには、次の手順を実行します。SSH 公開キーは、次の 3 種類のいずれかの形式で指定できます。

- OpenSSH 形式
- Internet Engineering Task Force（IETF）SECSH 形式
- Privacy Enhanced Mail（PEM）形式の公開キー証明書

OpenSSH キーの設定

ユーザ アカウントに OpenSSH 形式の SSH 公開キーを指定するには、次の手順を実行します。

はじめる前に

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。

- EXEC モードで CLI にログインしていること。
- OpenSSH 形式の SSH 公開キーが生成されています。
- ユーザ アカウントがすでに存在しています。

手順の概要

1. **config t**
2. **username** *username* **sshkey** *ssh-key*
3. **exit**
4. **show user-account**
5. **copy running-config startup-config**

手順の詳細

	コマンド	目的
ステップ 1	**config t** **Example:** n1000v# config t n1000v(config)#	CLI 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	**username** *username* **sshkey** *ssh-key*	既存のユーザ アカウントで OpenSSH 形式の SSH 公開キーを設定します。 ユーザ アカウントを作成するには、次のコマンドを使用します。 **username** *name* **password** *pwd*

Example:

```
n1000v(config)# username user1 sshkey ssh-rsa AAAAB3NzaC1yc2EAAAABIwAAAQEAyK
cb7Nv9Ki1OOId9/tdHHa/ngQujlvK5mXyL/n+DeOXKfVhHbX2a+V0cm7CCLUkBh+BvZRmpmOVTmU/5aw
fVhVxMKXMiPOPBc+A6/n3FVroyRwupMki6mWoM6UwaGID5gsVPqFjFNSgMWtbhjo97XVKhgjFW+wOVt8
QoAcrEtnwEfsnQk1EIr/0XIP1mqTsrqTsmjZ2vLk+fFzTGYAxMvYZI+BrN47aoH2ywS7CpnODjCDXJuD
YSPbc3PA8t0ghU/60m9R+s6AZPuljVQbGfxPrahEu4GVc6sMJNU1JxmqDJkodhMArObB4Umzj7E3Rdby
/ZWx/clTYiXQR1X1VfhQ==
```

ステップ 3	**exit** **Example:** n1000v(config)# exit n1000v#	グローバル コンフィギュレーション モードを終了し、EXEC モードに戻ります。
ステップ 4	**show user-account**	（任意）ユーザ アカウントの設定を表示します。

Example:

```
n1000v# show user-account
user:admin
        this user account has no expiry date
        roles:network-admin
user:user1
        this user account has no expiry date
        roles:network-operator
        ssh public key: ssh-rsa AAAAB3NzaC1yc2EAAAABIwAAAQEAyKcb7Nv9Ki1OOId9/tdH
Ha/ngQujlvK5mXyL/n+DeOXKfVhHbX2a+V0cm7CCLUkBh+BvZRmpmOVTmU/5awfVhVxMKXMiPOPBc+A6
/n3FVroyRwupMki6mWoM6UwaGID5gsVPqFjFNSgMWtbhjo97XVKhgjFW+wOVt8QoAcrEtnwEfsnQk1EI
r/0XIP1mqTsrqTsmjZ2vLk+fFzTGYAxMvYZI+BrN47aoH2ywS7CpnODjCDXJuDYSPbc3PA8t0ghU/60m
9R+s6AZPuljVQbGfxPrahEu4GVc6sMJNU1JxmqDJkodhMArObB4Umzj7E3Rdby/ZWx/clTYiXQR1X1Vf
hQ==
```

ステップ 5	**copy running-config startup-config** **Example:** n1000v# 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。

IETF または PEM キーの設定

ユーザ アカウントに IETF SECSH または PEM 形式の SSH 公開キーを指定するには、次の手順を実行します。

はじめる前に

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。

- EXEC モードで CLI にログインしていること。
- 次のいずれかの形式の SSH 公開キーが生成されています。
  - Internet Engineering Task Force（IETF）SECSH 形式
  - Privacy Enhanced Mail（PEM）形式の公開キー証明書

手順の概要

1. **copy** *server-file* **bootflash:***filename*
2. **config t**
3. **username** *username* **sshkey file bootflash:***filename*
4. **exit**
5. **show user-account**
6. **copy running-config startup-config**

手順の詳細

	コマンド	目的
ステップ 1	**copy** *server-file* **bootflash:***filename*	サーバから SSH キーが入ったファイルをダウンロードします。サーバは FTP、Secure Copy（SCP）、Secure FTP（SFTP）、または TFTP のいずれかを使用できます。

	Example:
	`n1000v# copy tftp://10.78.1.10/secsh_file.pub bootflash:secsh_file.pub vrf management`
	`Trying to connect to tftp server......`
	`Connection to server Established.`
	`|`
	`TFTP get operation was successful`
	`n1000v#`	

ステップ 2	**config t**
	
	Example:
	`n1000v# config t`
	`n1000v(config)#`
		CLI 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	**username** *username* **sshkey file bootflash:***filename* **Example:** `n1000v(config)# username User1 sshkey file bootflash:secsh_file.pub`	SSH 公開キーを設定します。

	コマンド	目的
ステップ 4	**exit** **Example:** n1000v(config)# exit n1000v#	グローバル コンフィギュレーション モードを終了し、EXEC モードに戻ります。
ステップ 5	**show user-account**	（任意）ユーザ アカウントの設定を表示します。

Example:

```
n1000v# show user-account
user:admin
        this user account has no expiry date
        roles:network-admin
user:user2
        this user account has no expiry date
        roles:network-operator
        ssh public key: ssh-rsa
AAAAB3NzaC1yc2EAAAABIwAAAQEAyKcb7Nv9Ki1OOId9/tdHHa/ngQujlvK5mXyL/n+DeOXKfVhHbX2a+V0cm7CC
LUkBh+BvZRmpmOVTmU/5awfVhVxMKXMiPOPBc+A6/n3FVroyRwupMki6
mWoM6UwaGID5gsVPqFjFNSgMWtbhjo97XVKhgjFW+wOVt8QoAcrEtnwEfsnQk1EIr/0XIP1mqTsrqTsmjZ2vLk+f
FzTGYAxMvYZI+BrN47aoH2ywS7CpnODjCDXJuDYSPbc3PA8t0ghU/60m9R+s6AZPuljVQbGfxPrahEu4GVc6sMJN
U1JxmqDJkodhMArObB4Umzj7E3Rdby/ZWx/clTYiXQR1X1VfhQ==
```

ステップ 6	**copy running-config startup-config** **Example:** n1000v# 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。

SSH セッションの開始

IP を使用して SSH セッションを開始し、リモート装置と接続するには、次の手順を実行します。

はじめる前に

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。

- EXEC モードで CLI にログインしていること。
- リモート装置のホスト名と、必要な場合はユーザ名を取得済みです。
- リモート装置で SSH サーバがイネーブルになっています。

手順の概要

1. **ssh** [*username@*]{*hostname* | *username@hostname*} [**vrf** *vrf-name*]
   ssh6 [*username@*]{*hostname* | *username@hostname*} [**vrf** *vrf-name*]

手順の詳細

	コマンド	目的
ステップ 1	**ssh** [root@]{*ip address* | *hostname*} [**vrf** *vrf-name*] **Example:** n1000v(config)# ssh root@172.28.30.77 root@172.28.30.77's password: Last login: Sat Jul 26 11:07:23 2008 from 171.70.209.64	IP を使用してリモート装置との SSH IP セッションを作成します。デフォルトの VRF はデフォルト VRF です。

SSH ホストのクリア

SCP または SFTP を使用してサーバからファイルをダウンロードした際、またはリモート ホストへの SSH セッションを開始した際に追加された信頼できる SSH サーバのリストをアカウントからクリアするには、次の手順を実行します。

手順の概要

1. **clear ssh hosts**

手順の詳細

	コマンド	目的
ステップ 1	**clear ssh hosts** **Example:** n1000v# clear ssh hosts	SSH ホスト セッションをクリアします。

SSH サーバのディセーブル化

SSH サーバをディセーブルにしてスイッチへの SSH アクセスを防止するには、次の手順を実行します。デフォルトでは、SSH サーバはイネーブルになっています。

はじめる前に

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。

- EXEC モードで CLI にログインしていること。
- SSH をディセーブルにした後で再度イネーブルにするには、初めに SSH サーバ キーを生成する必要があります。

  「SSH サーバ キーの生成」（P.7-3）の手順を参照してください。

手順の概要

1. **config t**
2. **no feature ssh**
3. **show ssh server**
4. **copy running-config startup-config**

手順の詳細

	コマンド	目的
ステップ 1	**config t** **Example:** n1000v# config t n1000v(config)#	CLI 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 feature ssh** **Example:** n1000v(config)# no feature ssh XML interface to system may become unavailable since ssh is disabled n1000v(config)#	SSH サーバをディセーブルにします。デフォルトはイネーブルです。
ステップ 3	**show ssh server** **Example:** n1000v(config)# show ssh server ssh is not enabled n1000v(config)#	（任意）SSH サーバの設定を表示します。
ステップ 4	**copy running-config startup-config** **Example:** 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ます。

SSH サーバ キーの削除

SSH サーバをディセーブルにしたあと、SSH サーバ キーを削除するには、次の手順を実行します。

はじめる前に

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。

- EXEC モードで CLI にログインしていること。
- SSH をディセーブルにした後で再度イネーブルにするには、初めに SSH サーバ キーを生成する必要があります。

  「SSH サーバ キーの生成」（P.7-3）の手順を参照してください。

手順の概要

1. **config t**
2. **no feature ssh**

3. **no ssh key [dsa | rsa]**
4. **show ssh key**
5. **copy running-config startup-config**

手順の詳細

	コマンド	目的
ステップ 1	**config t** **Example:** n1000v# config t n1000v(config)#	CLI 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 feature ssh** **Example:** n1000v(config)# no feature ssh	SSH サーバをディセーブルにします。
ステップ 3	**no ssh key** [**dsa** | **rsa**] **Example:** n1000v(config)# no ssh key rsa	SSH サーバ キーを削除します。 デフォルトでは、すべての SSH キーが削除されます。
ステップ 4	**show ssh key** **Example:** n1000v(config)# show ssh key	（任意）SSH サーバ キーの設定を表示します。
ステップ 5	**copy running-config startup-config** **Example:** 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ます。

Example:

```
n1000v# config t
n1000v(config)# no feature ssh
n1000v(config)# no ssh key rsa
n1000v(config)# show ssh key
*************************************
rsa Keys generated:Sun Jul 27 15:18:46 2008

ssh-rsa AAAAB3NzaC1yc2EAAAABIwAAAQEAyKcb7Nv9Ki1OOId9/tdHHa/ngQujlvK5mXyL/n+DeOXK
fVhHbX2a+V0cm7CCLUkBh+BvZRmpmOVTmU/5awfVhVxMKXMiPOPBc+A6/n3FVroyRwupMki6mWoM6Uwa
GID5gsVPqFjFNSgMWtbhjo97XVKhgjFW+wOVt8QoAcrEtnwEfsnQk1EIr/0XIP1mqTsrqTsmjZ2vLk+f
FzTGYAxMvYZI+BrN47aoH2ywS7CpnODjCDXJuDYSPbc3PA8t0ghU/60m9R+s6AZPuljVQbGfxPrahEu4
GVc6sMJNU1JxmqDJkodhMArObB4Umzj7E3Rdby/ZWx/clTYiXQR1X1VfhQ==

bitcount:2048
fingerprint:
fd:ca:48:73:b9:ee:e7:86:9e:1e:40:46:f1:50:1d:44
*************************************
dsa Keys generated:Sun Jul 27 15:20:12 2008

ssh-dss AAAAB3NzaC1kc3MAAACBALpdxLjXNS/jcCNY+F1QZV9HegxBEb0DMUmq9bSq2N+KAcvHllEh
GnaiHhqarOlcEKqhLbIbuqtKTCvfa+Y1hBIAhWVjg1UR3/M22jqxnfhnxL5YRc1Q7fcesFax0myayAIU
nXrkO5iwv9XHTu+EInRc4kJ0XrG9SxtLmDe/fi2ZAAAAFQDbRabAjZa6GfDpwjXw5smRhrElJwAAAIEA
r50yi3hHawNnb5qgYLXhN+KA8XJF753eCWHtMw7NR8fz6fjQ1R2J97UjjGuQ8DvwpGeNQ5S+AuIo0rGq
svdg7TTecBcbgBOnR7Fs2+W5HiSVEGbvj1xaeK8fkNE6kaJumBB343b8Rgj0G97MP/os1GfkEqmX9glB
0IOM2mgHHyoAAACAfRir27hHy+fw8CxPlsK0R6cFhxYyd/qYYogXFKYIOPxpLoYrjqODeOFThU7TJuBz
```

```
aS97eXiruzbffHwzUGfXgmQT5o9IMZRTClWPA/5Ju4O9YABYHccUghf0W+QtgGOT6FOSvBh8uOV0kcHC
GMJAP8omphauZJlc+wgFxhnkyh4=

bitcount:1024
fingerprint:
44:91:32:1f:7a:d1:83:3c:f3:5e:db:53:0a:2d:ce:69
************************************
mcs-srvr43(config)# no ssh key rsa
mcs-srvr43(config)# show ssh key
************************************
could not retrieve rsa key information
************************************
dsa Keys generated:Sun Jul 27 15:20:12 2008

ssh-dss AAAAB3NzaC1kc3MAAACBALpdxLjXNS/jcCNY+F1QZV9HegxBEb0DMUmq9bSq2N+KAcvHllEh
GnaiHhqarOlcEKqhLbIbuqtKTCvfa+Y1hBIAhWVjg1UR3/M22jqxnfhnxL5YRc1Q7fcesFax0myayAIU
nXrkO5iwv9XHTu+EInRc4kJ0XrG9SxtLmDe/fi2ZAAAAFQDbRabAjZa6GfDpwjXw5smRhrElJwAAAIEA
r50yi3hHawNnb5qgYLXhN+KA8XJF753eCWHtMw7NR8fz6fjQ1R2J97UjjGuQ8DvwpGeNQ5S+AuIo0rGq
svdg7TTecBcbgBOnR7Fs2+W5HiSVEGbvj1xaeK8fkNE6kaJumBB343b8Rgj0G97MP/os1GfkEqmX9glB
0IOM2mgHHyoAAACAfRir27hHy+fw8CxPlsK0R6cFhxYyd/qYYogXFKYIOPxpLoYrjqODeOFThU7TJuBz
aS97eXiruzbffHwzUGfXgmQT5o9IMZRTClWPA/5Ju4O9YABYHccUghf0W+QtgGOT6FOSvBh8uOV0kcHC
GMJAP8omphauZJlc+wgFxhnkyh4=

bitcount:1024
fingerprint:
44:91:32:1f:7a:d1:83:3c:f3:5e:db:53:0a:2d:ce:69
************************************
mcs-srvr43(config)# no ssh key dsa
mcs-srvr43(config)# show ssh key
************************************
could not retrieve rsa key information
************************************
could not retrieve dsa key information
************************************
no ssh keys present. you will have to generate them
************************************
n1000v#
```

SSH セッションのクリア

デバイスから SSH セッションをクリアするには、次の手順を実行します。

はじめる前に

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。

- EXEC モードで CLI にログインしていること。

手順の概要

1. **show users**
2. **clear line** *vty-line*
3. **show users**

手順の詳細

	コマンド	目的
ステップ 1	**show users** **Example:** n1000v# show users	ユーザ セッション情報を表示します。
ステップ 2	**clear line** *vty-line* **Example:** n1000v# clear line 0	ユーザ SSH セッションをクリアします。
ステップ 3	**show users** **Example:** n1000v# show users	ユーザ セッション情報を表示します。

```
Example:
n1000v# show users
NAME     LINE         TIME         IDLE          PID COMMENT
admin    tty1         Jul 25 19:13  old         2867
admin    pts/0        Jul 28 09:49 00:02       28556 (10.21.148.122)
admin    pts/1        Jul 28 09:46   .         28437 (::ffff:10.21.148.122)*
n1000v# clear line 0
n1000v# show users
NAME     LINE         TIME         IDLE          PID COMMENT
admin    tty1         Jul 25 19:13  old         2867
admin    pts/1        Jul 28 09:46   .         28437 (::ffff:10.21.148.122)*
mcs-srvr43(config)#
```

SSH の設定の確認

SSH の設定情報を表示するには、次のいずれかのコマンドを使用します。

コマンド	目的
show ssh key [dsa | rsa]	SSH サーバ キー ペアの情報を表示します。
show running-config security [**all**]	実行コンフィギュレーション内の SSH とユーザ アカウントの設定を表示します。キーワード **all** を指定すると、SSH およびユーザ アカウントのデフォルト値が表示されます。
show ssh server	SSH サーバの設定を表示します。

```
Example:
n1000v# show ssh key rsa
**************************************
rsa Keys generated:Mon Jul 28 09:49:18 2008

ssh-rsa
AAAAB3NzaC1yc2EAAAABIwAAAGEAv0a4p6VulQMW4AMgoPfApB2KegF3QTojCzed51iVQnEkNglnM7A/oEIZAtlVLY
k/PEzt+ED7lPal/8pomaqjgRxHSeK2gw1cJKSDbcYH5na8uox1Hr50eK0q2+ZfvMqV

bitcount:768
```

```
fingerprint:
76:6c:a0:5c:79:a6:ae:3d:cb:27:a1:86:62:fa:09:df
**************************************
```

SSH の設定例

OpenSSH キーを使用する SSH を設定するには、次の作業を行います。

ステップ 1　SSH サーバをディセーブルにします。

```
n1000v# config t
n1000v(config)# no feature ssh
```

ステップ 2　SSH サーバ キーを生成します。

```
n1000v(config)# ssh key rsa
generating rsa key(1024 bits).....
.generated rsa key
```

ステップ 3　SSH サーバをイネーブルにします。

```
n1000v(config)# feature ssh
```

ステップ 4　SSH サーバ キーを表示します。

```
n1000v(config)# show ssh key
rsa Keys generated:Sat Sep 29 00:10:39 2007

ssh-rsa AAAAB3NzaC1yc2EAAAABIwAAAIEAvWhEBsF55oaPHNDBnpXOTw6+/OdHoLJZKr+MZm99n2U0
ChzZG4svRWmHuJY4PeDWl0e5yE3g3EO3pjDDmt923siNiv5aSga60K36lr39HmXL6VgpRVn1XQFiBwn4
na+H1d3Q0hDt+uWEA0tka2uOtXlDhliEmn4HVXOjGhFhoNE=

bitcount:1024
fingerprint:
51:6d:de:1c:c3:29:50:88:df:cc:95:f0:15:5d:9a:df
**************************************
could not retrieve dsa key information
**************************************
```

ステップ 5　OpenSSH 形式の SSH 公開キーを指定します。

```
n1000v(config)# username User1 sshkey ssh-rsa
AAAAB3NzaC1yc2EAAAABIwAAAIEAy19oF6QaZl9G+3f1XswK3OiW4H7YyUyuA50rv7gsEPjhOBYmsi6PAVKui1nIf/
DQhum+lJNqJP/eLowb7ubO+lVKRXFY/G+lJNIQW3g9igG30c6k6+XVn+NjnI1B7ihvpVh7dLddMOXwOnXHYshXmSiH
3UD/vKyziEh5S4Tplx8=
```

ステップ 6　設定を保存します。

```
n1000v(config)# copy running-config startup-config
```

Example:

```
n1000v# config t
n1000v(config)# no feature ssh
n1000v(config)# ssh key rsa
generating rsa key(1024 bits).....
n1000v(config)# feature ssh
n1000v(config)# show ssh key
rsa Keys generated:Sat Sep 29 00:10:39 2007
ssh-rsa AAAAB3NzaC1yc2EAAAABIwAAAIEAvWhEBsF55oaPHNDBnpXOTw6+/OdHoLJZKr+MZm99n2U0
```

```
ChzZG4svRWmHuJY4PeDWl0e5yE3g3EO3pjDDmt923siNiv5aSga60K36lr39HmXL6VgpRVn1XQFiBwn4
na+H1d3Q0hDt+uWEA0tka2uOtXlDhliEmn4HVXOjGhFhoNE=
bitcount:1024
fingerprint:
51:6d:de:1c:c3:29:50:88:df:cc:95:f0:15:5d:9a:df
************************************
could not retrieve dsa key information
************************************

n1000v(config)# username User1 sshkey ssh-rsa
AAAAB3NzaC1yc2EAAAABIwAAAIEAy19oF6QaZl9G+3f1XswK3OiW4H7YyUyuA50rv7gsEPjhOBYmsi6PAVKui1nIf/
DQhum+lJNqJP/eLowb7ubO+lVKRXFY/G+lJNIQW3g9igG30c6k6+XVn+NjnI1B7ihvpVh7dLddMOXwOnXHYshXmSiH
3UD/vKyziEh5S4Tplx8=
n1000v(config)# copy running-config startup-config
[########################################] 100%
n1000v(config)#
```

その他の関連資料

RBAC の実装に関連する詳細情報については、次を参照してください。

- 「関連資料」（P.7-15）
- 「標準」（P.7-15）

関連資料

関連項目	参照先
CLI	『*Cisco Nexus 1000V Getting Started Guide, Release 4.2(1)SV1(4a)*』
Telnet	第 8 章「Telnet の設定」

標準

標準	タイトル
この機能でサポートされる新規の標準または変更された標準はありません。また、既存の標準のサポートは変更されていません。	—

SSH 機能の履歴

ここでは、SSH のリリース履歴を示します。

機能名	リリース	機能情報
SSH	4.0(4)SV1(1)	この機能が導入されました。

CHAPTER 8

Telnet の設定

この章では、Telnet を設定する手順を説明します。内容は次のとおりです。

Telnet サーバの概要

Telnet プロトコルは、ホストとの TCP/IP 接続の確立を可能にします。Telnet を使用すると、あるサイトのユーザが別のサイトのログイン サーバと TCP 接続を確立し、デバイス間でキーストロークをやり取りできます。Telnet は、リモート デバイス アドレスとして IP アドレスまたはドメイン名のいずれかを受け入れます。

Telnet の前提条件

Telnet には次の前提条件があります。

- レイヤ 3 インターフェイス上に IP、mgmt 0 インターフェイス上にアウトバンド、またはイーサネット インターフェイス上にインバンドを設定していること

注意事項および制約事項

- Telnet サーバはデフォルトでイネーブルになっています。
- Cisco NX-OS のコマンドは Cisco IOS のコマンドと異なる場合があります。

デフォルト設定

次の表に、Telnet のデフォルト設定を示します。

パラメータ	デフォルト
Telnet サーバ	イネーブル

Telnet の設定

ここでは、次の内容について説明します。

Telnet サーバのイネーブル化

Telnet サーバをイネーブルにするには、次の手順を実行します。Telnet サーバはデフォルトでイネーブルになっていますが、必要な場合は、次の手順を実行して再度イネーブルにすることができます。

はじめる前に

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。

- EXEC モードで CLI にログインしていること。
- デフォルトでは、Telnet サーバはイネーブルに設定されています。

手順の概要

1. **config t**
2. **feature telnet**
3. **exit**
4. **show telnet server**
5. **copy running-config startup-config**

手順の詳細

	コマンド	目的
ステップ 1	**config t** **Example:** n1000v# config t n1000v(config)#	CLI 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	**feature telnet** **Example:** n1000v(config)# feature telnet n1000v(config)#	Telnet サーバをイネーブルにします。
ステップ 3	**show telnet server** **Example:** n1000v(config)# show telnet server telnet service enabled n1000v(config)#	（任意）Telnet サーバの設定を表示します。
ステップ 4	**copy running-config startup-config** **Example:** n1000v(config)# copy running-config startup-config	（任意）実行コンフィギュレーションで行ったこれらの変更内容を、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。

リモート装置との IP Telnet セッションの開始

リモート装置との Telnet セッションを開始するには、次の手順を実行します。

はじめる前に

この手順を開始する前に、次のことを確認または実行しておく必要があります。

- EXEC モードで CLI にログインしていること。
- リモート装置の Telnet サーバがイネーブルであることを確認しています。
- リモート装置のホスト名と、必要な場合はリモート装置のユーザ名が取得済みです。
- Telnet サーバがイネーブルであることが確認済みです。そうでない場合は、「Telnet サーバのイネーブル化」（P.8-2）の手順に従ってイネーブルにしています。デフォルトでは、Telnet サーバはイネーブルに設定されています。

手順の概要

1. **telnet** {*ip address* | *hostname*} [*port-number*] [**vrf** *vrf-name*]

手順の詳細

	コマンド	目的
ステップ 1	**telnet** {*ip address* | *host-name*} [*port-number*] [**vrf** *vrf-name*] **Example:** n1000v# telnet 10.10.1.1	指定した宛先との IP Telnet セッションを作成します。 **port-number**：このセッションで使用するポート番号（1 ～ 65535）です。デフォルトのポート番号は 23 です。 **vrf-name**：デフォルトの VRF はデフォルト VRF です。

Telnet セッションのクリア

Telnet セッションをクリアするには、次の手順を実行します。

はじめる前に

この手順を開始する前に、次のことを確認または実行しておく必要があります。

- EXEC モードで CLI にログインしていること。

手順の概要

1. **show users**
2. **clear line** *vty-line*

手順の詳細

	コマンド	目的
ステップ 1	**show users** **Example:** n1000v# **show users**	ユーザ セッション情報を表示します。
ステップ 2	**clear line** *vty-line* **Example:** n1000v# **clear line 1**	ユーザ Telnet セッションをクリアします。
ステップ 3	**show users** **Example:** n1000v# **show users**	ユーザ セッション情報を表示します。

```
Example:
n1000v# show users
NAME     LINE         TIME         IDLE          PID COMMENT
admin    tty1         Jul 25 19:13  old         2867
admin    pts/1        Jul 28 14:04   .         31453 (::ffff:171.70.209.8)
admin    pts/2        Jul 28 14:04   .         31475 (171.70.209.8)*
n1000v# clear line 1
n1000v# show users
NAME     LINE         TIME         IDLE          PID COMMENT
admin    tty1         Jul 25 19:13  old         2867
admin    pts/2        Jul 28 14:04   .         31475 (171.70.209.8)*
n1000v#
```

Telnet の設定の確認

Telnet の設定情報を表示するには、次のいずれかのコマンドを使用します。

コマンド	目的
show running-config security [**all**]	実行コンフィギュレーションのユーザ アカウント設定を表示します。**all** キーワードを指定すると、ユーザ アカウントのデフォルト値が表示されます。
show telnet server	Telnet サーバの設定を表示します。
show hosts	現在のホストの設定詳細を表示します。
show tcp connection	接続情報を表示します。

```
Example:
n1000v# show running-config security all
version 4.0(1)
username admin password 5 $1$xMw2Q/1S$ZEWRvyAxAJAFV0weuSPvg1  role network-admin
username user2 password 5 $1$byNNnnSP$xfXVKjE5UEScvriwX3Kyj0  role network-operator
username user2 sshkey ssh-rsa
AAAAB3NzaC1yc2EAAAABIwAAAQEAyKcb7Nv9Ki1OOId9/tdHHa/ngQujlvK5mXyL/n+DeOXKfVhHbX2a+V0cm7CCLU
kBh+BvZRmpmOVTmU/5awfVhVxMKXMiPOPBc+A6/n3FVroyRwupMki6mW
oM6UwaGID5gsVPqFjFNSgMWtbhjo97XVKhgjFW+wOVt8QoAcrEtnwEfsnQk1EIr/0XIP1mqTsrqTsmjZ2vLk+fFzTG
YAxMvYZI+BrN47aoH2ywS7CpnODjCDXJuDYSPbc3PA8t0ghU/60m9R+s6AZPuljVQbGfxPrahEu4GVc6sMJNU1
JxmqDJkodhMArObB4Umzj7E3Rdby/ZWx/clTYiXQR1X1VfhQ==
telnet server enable

banner motd # User Access Verification #

ssh key rsa 1024 force
no ssh key dsa force
ssh server enable
```

その他の関連資料

Telnet の実装に関連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.8-5）
- 「標準」（P.8-6）

関連資料

関連項目	参照先
SSH	第 7 章「SSH の設定」
CLI	『*Cisco Nexus 1000V Getting Started Guide, Release 4.2(1)SV1(4a)*』

標準

標準	タイトル
この機能でサポートされる新規の標準または変更された標準はありません。また、既存の標準のサポートは変更されていません。	—

Telnet 機能の履歴

ここでは、Telnet のリリース履歴を示します。

機能名	リリース	機能情報
Telnet	4.0(4)SV1(1)	この機能が導入されました。

CHAPTER 9

IP ACL の設定

この章では、IP アクセス コントロール リスト（ACL）を設定する手順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。

ACL について

ACL は、トラフィックをフィルタリングするための順番に並べられた一連のルールです。デバイスは、パケットを適用する ACL を決定する際に、パケットをルールに対してテストしていきます。最初に一致したルールで、そのパケットが許可されるか拒否されるかが決定されます。一致するルールがない場合は、そのデバイスでのデフォルト ルールが適用されます。デバイスは、許可されたパケットは処理し、拒否されたパケットは廃棄します。詳細については、「暗黙のルール」（P.9-3）を参照してください。

ACL を使用すると、ネットワークおよび特定のホストを、不要なトラフィックや望ましくないトラフィックから保護できます。たとえば、ACL を使用して、厳重にセキュリティ保護されたネットワークからインターネットに HTTP トラフィックが流入するのを禁止できます。また、特定のサイトへの HTTP トラフィックだけを許可することもできます。その場合は、サイトの IP アドレスが、IP ACL に指定されているかどうかによって判定します。

ここでは、次の内容について説明します。

ACL のタイプと適用

ポート ACL をトランク ポートに適用すると、その ACL は、当該トランク ポート上のすべての VLAN 上のトラフィックをフィルタリングします。

レイヤ 2 トラフィックのフィルタリングでは、次のポート ACL のタイプがサポートされます。

- IP ACL：IPv4 ACL は IP トラフィックだけに適用されます。
- MAC ACL：MAC ACL は非 IP トラフィックにだけ適用されます。

ACL の適用順序

ACL は次の順序で適用されます。

1. 着信ポート ACL
2. 発信ポート ACL

ルールについて

ACL によるネットワーク トラフィックのフィルタリング方法を設定する際に、何を作成、変更、削除するかを決めるのがルールです。ルールは実行コンフィギュレーション内に表示されます。ACL をインターフェイスに適用するか、またはインターフェイスにすでに適用されている ACL 内のルールを変更すると、スーパーバイザ モジュールは実行コンフィギュレーション内のルールから ACL のエントリを作成し、それらの ACL エントリを適用可能な I/O モジュールに送信します。

アクセス リスト コンフィギュレーション モードで **permit** または **deny** コマンドを使用すると、ACL にルールを作成できます。これにより、デバイスは許可ルール内の基準と一致するトラフィックを許可し、拒否ルール内の基準と一致するトラフィックをブロックします。ルールに一致するためにトラフィックが満たさなければならない基準を設定するためのオプションが多数用意されています。

ここでは、ルールを設定する際に使用できるオプションをいくつか紹介します。すべてのオプションの説明については、『*Cisco Nexus 1000V Command Reference, Release 4.2(1)SV1(4a)*』の該当する **permit** および **deny** コマンドを参照してください。

ここでは、次の内容について説明します。

送信元と宛先

各ルールには、ルールに一致するトラフィックの送信元と宛先を指定します。指定する送信元および宛先には、特定のホスト、ホストのネットワークまたはグループ、あるいは任意のホストを使用できます。送信元と宛先の指定方法は、IP ACL と MAC ACL のどちらを設定するかによって異なります。送信元と宛先の指定方法については、『*Cisco Nexus 1000V Command Reference, Release 4.2(1)SV1(4a)*』の該当する **permit** および **deny** コマンドを参照してください。

プロトコル

IP ACL および MAC ACL では、トラフィックをプロトコルで識別できます。一部のプロトコルは名前で指定できます。たとえば、IP ACL では、ICMP を名前で指定できます。

プロトコルはすべて番号で指定できます。MAC ACL では、プロトコルをそのプロトコルの Ethertype 番号（16 進数）で指定できます。たとえば、MAC ACL ルールの IP トラフィックの指定に 0x0800 を使用できます。

IP ACL では、インターネット プロトコル番号を表す整数でプロトコルを指定できます。たとえば、Layer 2 Tunneling Protocol（L2TP; レイヤ 2 トンネリング プロトコル）を指定するには、115 を使用します。

各タイプの ACL に名前で指定できるプロトコルのリストは、『*Cisco Nexus 1000V Command Reference, Release 4.2(1)SV1(4a)*』の該当する **permit** および **deny** コマンドを参照してください。

暗黙のルール

IP ACL および MAC ACL には暗黙ルールがあります。暗黙ルールは、実行コンフィギュレーションには設定されていませんが、ACL 内の他のルールと一致しない場合にデバイスがトラフィックに適用するルールです。ACL のルール単位の統計情報を維持するようにデバイスを設定した場合、暗黙ルールの統計情報はデバイスに維持されません。

すべての IP ACL には、不一致の IP トラフィックを拒否する次の暗黙ルールがあります。

```
deny ip any any
```

すべての MAC ACL には、次の暗黙のルールがあります。

```
deny any any
```

この暗黙ルールによって、トラフィックのレイヤ 2 ヘッダーに指定されているプロトコルに関係なく、不一致トラフィックが確実に拒否されます。

その他のフィルタリング オプション

追加のオプションを使用してトラフィックを識別できます。これらのオプションは、ACL のタイプによって異なります。次のリストには、ほとんどの追加フィルタリング オプションが含まれていますが、すべてを網羅しているわけではありません。

- IP ACL は、次の追加フィルタリング オプションをサポートしています。
  - レイヤ 4 プロトコル
  - TCP/UDP ポート
  - ICMP タイプおよびコード
  - IGMP タイプ
  - 優先レベル

  - DiffServ コード ポイント（DSCP）値
  - ACK、FIN、PSH、RST、SYN、または URG ビットがセットされた TCP パケット
- MAC ACL は、次の追加フィルタリング オプションをサポートしています。
  - レイヤ 3 プロトコル
  - VLAN ID
  - サービス クラス（CoS）

ルールに適用できるすべてのフィルタリング オプションについては、『*Cisco Nexus 1000V Command Reference, Release 4.2(1)SV1(4a)*』の該当する **permit** および **deny** コマンドを参照してください。

シーケンス番号

デバイスはルールのシーケンス番号をサポートしています。入力するすべてのルールにシーケンス番号が割り当てられます（ユーザによる割り当てまたはデバイスによる自動割り当て）。シーケンス番号によって、次の ACL 設定作業が容易になります。

- 既存のルールの間に新規のルールを追加する：シーケンス番号を指定することによって、ACL 内での新規ルールの挿入場所を指定します。たとえば、ルール番号 100 と 110 の間に新しいルールを挿入する必要がある場合は、シーケンス番号 105 を新しいルールに割り当てます。
- ルールを削除する：シーケンス番号を使用しない場合は、ルールを削除するのに、次のようにルール全体を入力する必要があります。

  ```
  n1000v(config-acl)# no permit tcp 10.0.0.0/8 any
  ```

  このルールに 101 番のシーケンス番号が付いていれば、次コマンドだけでルールを削除できます。

  ```
  n1000v(config-acl)# no 101
  ```

- ルールを移動する：シーケンス番号を使用すれば、同じ ACL 内の異なる場所にルールを移動する必要がある場合に、そのルールのコピーをシーケンス番号で正しい位置に挿入してから、元のルールを削除できます。この方法により、トラフィックを中断せずにルールを移動できます。

シーケンス番号を使用せずにルールを入力すると、デバイスはそのルールを ACL の最後に追加し、そのルールの直前のルールのシーケンス番号よりも 10 大きい番号を割り当てます。たとえば、ACL 内の最後のルールのシーケンス番号が 225 で、シーケンス番号を指定せずにルールを追加した場合、デバイスはその新しいルールにシーケンス番号 235 を割り当てます。

さらに、ACL 内のルールにシーケンス番号を再割り当てすることも可能です。シーケンス番号の再割り当ては、ACL 内に、100、101 のように連続するシーケンス番号のルールがある場合、それらのルールの間に 1 つ以上のルールを挿入する必要があるときに便利です。

統計

デバイスは IPv4 ACL および MAC ACL に設定する各ルールのグローバル統計を維持できます。1 つの ACL が複数のインターフェイスに適用される場合、ルール統計には、その ACL が適用されるすべてのインターフェイスと一致する（ヒットする）パケットの合計数が維持されます。

（注） インターフェイスレベルの ACL 統計はサポートされていません。

設定する ACL ごとに、その ACL の統計情報をデバイスが維持するかどうかを指定できます。これにより、ACL によるトラフィック フィルタリングが必要かどうかに応じて ACL 統計のオン、オフを指定できます。また、ACL 設定のトラブルシューティングにも役立ちます。

デバイスには ACL の暗黙ルールの統計情報は維持されません。たとえば、すべての IPv4 ACL の末尾にある暗黙の **deny ip any any** ルールと一致するパケットのカウントはデバイスに維持されません。暗黙ルールの統計情報を維持する場合は、暗黙ルールと同じルールを指定した ACL を明示的に設定する必要があります。詳細については、「暗黙のルール」（P.9-3）を参照してください。

IP ACL の前提条件

IP ACL の前提条件は次のとおりです。

- IP ACL を設定するためには、IP アドレッシングおよびプロトコルに関する知識が必要です。
- ACL を設定するインターフェイス タイプについての知識が必要です。

注意事項および制約事項

IP ACL の設定に関する注意事項と制約事項は次のとおりです。

- ほとんどの場合、IP パケットの ACL 処理は、I/O モジュール上で実行されます。管理インターフェイス トラフィックは、常にスーパーバイザ モジュールで処理されます。この場合、速度は遅くなります。
- ACL は、ポート チャネルではサポートされていません。

デフォルト設定

表 9-1 に、IP ACL パラメータのデフォルト設定値を示します。

表 9-1　IP ACL パラメータのデフォルト値

パラメータ	デフォルト
IP ACL	デフォルトでは IP ACL は存在しません。
ACL ルール	すべての ACL に暗黙ルールが適用されます（「暗黙のルール」（P.9-3）を参照）。

IP ACL の設定

ここでは、次の内容について説明します。

IP ACL の作成

デバイスに IPv4 ACL を作成し、これにルールを追加できます。

はじめる前に

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。

- EXEC モードで CLI にログインしていること。

手順の概要

1. **config t**
2. **[no] ip access-list** {*name* | **match-local-traffic**}
3. [*sequence-number*] {**permit | deny**} *protocol source destination*
4. **statistics per-entry**
5. **show ip access-lists** *name*
6. **copy running-config startup-config**

手順の詳細

	コマンド	目的
ステップ 1	**config t** **Example:** n1000v# config t n1000v(config)#	CLI 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 access-list** {*name* | **match-local-traffic**} **Example:** n1000v(config)# ip access-list acl-01 n1000v(config-acl)# **Example:** n1000v(config)# ip access-list match-local-traffic n1000v(config-acl)#	名前付き IP ACL（最大 64 文字）を作成し、IP ACL コンフィギュレーション モードを開始します。 **match-local-traffic** オプションは、ローカルに生成されたトラフィックのマッチングをイネーブルにします。 **no** オプションは指定されたアクセス リストを削除します。

	コマンド	目的
ステップ 3	[*sequence-number*] {**permit** | **deny**} *protocol source destination* **Example:** n1000v(config-acl)# permit ip 192.168.2.0/24 any	IP ACL 内にルールを作成します。多数のルールを作成できます。*sequence-number* 引数には、1 ～ 4294967295 の整数を指定します。 **permit** コマンドと **deny** コマンドには、トラフィックを識別するための多くの方法が用意されています。詳細については、『*Cisco Nexus 1000V Command Reference, Release 4.2(1)SV1(4a)*』を参照してください。
ステップ 4	**statistics per-entry** **Example:** n1000v(config-acl)# statistics per-entry	（任意）その ACL のルールと一致するパケットのグローバル統計をデバイスが維持するように設定します。
ステップ 5	**show ip access-lists** *name* **Example:** n1000v(config-acl)# show ip access-lists acl-01	（任意）IP ACL の設定を表示します。
ステップ 6	**copy running-config startup-config** **Example:** n1000v(config-acl)# 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。

IP ACL の変更

既存の IPv4 ACL に対してルールの追加または削除を行うことができます。既存のルールは変更できません。ルールを変更するには、そのルールを削除してから、変更を加えたルールを再作成します。

既存のルールの間に新しいルールを挿入する必要がある場合で、現在のシーケンス番号の空き状況ではすべてを挿入できないときは、**resequence** コマンドを使用してシーケンス番号を再割り当てします。詳細については、「IP ACL 内のシーケンス番号の変更」（P.9-10）を参照してください。

はじめる前に

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。

- EXEC モードで CLI にログインしていること。

手順の概要

1. **config t**
2. **ip access-list** *name*
3. [*sequence-number*] {**permit | deny**} *protocol source destination*
4. **no** {*sequence-number* | {**permit | deny**} *protocol source destination*}
5. [**no**] **statistics per-entry**
6. **show ip access-list** *name*
7. **copy running-config startup-config**

手順の詳細

	コマンド	目的
ステップ 1	**config t** **Example:** n1000v# config t n1000v(config)#	CLI 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 access-list** *name* **Example:** n1000v(config)# ip access-list acl-01 n1000v(config-acl)#	指定した ACL の IP ACL 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	[*sequence-number*] {**permit** | **deny**} *protocol source destination* **Example:** n1000v(config-acl)# 100 permit ip 192.168.2.0/24 any	（任意）IP ACL 内にルールを作成します。シーケンス番号を指定すると、ACL 内のルール挿入位置を指定できます。シーケンス番号を指定しないと、ルールは ACL の末尾に追加されます。*sequence-number* 引数には、1 ～ 4294967295 の整数を指定します。 **permit** コマンドと **deny** コマンドには、トラフィックを識別するための多くの方法が用意されています。詳細については、『*Cisco Nexus 1000V Command Reference, Release 4.2(1)SV1(4a)*』を参照してください。
ステップ 4	**no** {*sequence-number* | {**permit** | **deny**} *protocol source destination*} **Example:** n1000v(config-acl)# no 80	（任意）指定したルールを IP ACL から削除します。 **permit** コマンドと **deny** コマンドには、トラフィックを識別するための多くの方法が用意されています。詳細については、『*Cisco Nexus 1000V Command Reference, Release 4.2(1)SV1(4a)*』を参照してください。
ステップ 5	[**no**] **statistics per-entry** **Example:** n1000v(config-acl)# statistics per-entry	（任意）その ACL のルールと一致するパケットのグローバル統計をデバイスが維持するように設定します。 **no** オプションを使用すると、デバイスはその ACL のグローバル統計の維持を停止します。
ステップ 6	**show ip access-lists** *name* **Example:** n1000v(config-acl)# show ip access-lists acl-01	（任意）IP ACL の設定を表示します。
ステップ 7	**copy running-config startup-config** **Example:** n1000v(config-acl)# 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。

IP ACL の削除

IP ACL をデバイスから削除できます。

はじめる前に

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。

- EXEC モードで CLI にログインしていること。
- その ACL がインターフェイスに適用されているかどうかを確認します。
- ACL を削除しても、適用されているインターフェイスの設定には影響しません。デバイスは削除された ACL を空であると見なします。

手順の概要

1. **config t**
2. **[no] ip access-list** *name*
3. **show ip access-list** *name* **summary**
4. **copy running-config startup-config**

手順の詳細

	コマンド	目的

ステップ 1	**config t**
	
	Example:
	`n1000v# config t`
	`n1000v(config)#`
		CLI 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 access-list** *name* **Example:** `n1000v(config)# no ip access-list acl-01`	名前で指定した IP ACL を実行コンフィギュレーションから削除します。
ステップ 3	**show ip access-list** *name* **summary** **Example:** `n1000v(config)# show ip access-lists acl-01 summary`	（任意）IP ACL の設定を表示します。ACL がインターフェイスに引き続き適用されている場合は、インターフェイスが表示されます。
ステップ 4	**copy running-config startup-config** **Example:** `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ます。

IP ACL 内のシーケンス番号の変更

IP ACL 内のルールに付けられたすべてのシーケンス番号を変更できます。

はじめる前に

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。

- EXEC モードで CLI にログインしていること。

手順の概要

1. **config t**
2. **resequence ip access-list** *name starting-sequence-number increment*
3. **show ip access-lists** *name*
4. **copy running-config startup-config**

手順の詳細

	コマンド	目的

ステップ 1	**config t**
	
	Example:
	`n1000v# config t`
	`n1000v(config)#`
		CLI 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	**resequence ip access-list** *name starting-sequence-number increment* **Example:** `n1000v(config)# resequence access-list ip acl-01 100 10`	ACL 内に記述されているルールにシーケンス番号を付けます。指定した開始シーケンス番号が最初のルールに付けられます。後続の各ルールには、直前のルールよりも大きい番号が付けられます。番号の間隔は、指定した増分によって決まります。*starting-sequence-number* 引数と *increment* 引数は、1 ～ 4294967295 の整数で指定します。
ステップ 3	**show ip access-lists** *name* **Example:** `n1000v(config)# show ip access-lists acl-01`	（任意）IP ACL の設定を表示します。
ステップ 4	**copy running-config startup-config** **Example:** `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ます。

IP ACL のポート ACL としての適用

IPv4 または ACL をレイヤ 2 インターフェイスの物理ポートに適用してポート ACL を設定するには、次の手順を実行します。

はじめる前に

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。

- EXEC モードで CLI にログインしていること。
- 1 つのインターフェイスに 1 つのポート ACL を適用できます。
- 適用する ACL が存在し、目的に応じたトラフィック フィルタリングが設定されていることを確認します。詳細については、「IP ACL の作成」（P.9-6）または「IP ACL の変更」（P.9-7）を参照してください。
- IP ACL はポート プロファイルに設定することもできます。詳細については、「IP ACL のポート プロファイルへの追加」（P.9-12）の手順を参照してください。

手順の概要

1. **config t**
2. **interface vethernet** *port*
3. **ip port access-group** *access-list* **[in | out]**
4. **show running-config aclmgr**
5. **copy running-config startup-config**

手順の詳細

	コマンド	目的

ステップ 1	**config t**
	
	Example:
	`n1000v# config t`
	`n1000v(config)#`
		CLI 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** *port*
	
	Example:
	`n1000v(config)# interface vethernet 40`
	`n1000v(config-if)#`
		指定した vEthernet 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	**ip port access-group** *access-list* **[in | out]** **Example:** `n1000v(config-if)# ip port access-group acl-l2-marketing-group in`	インバウンドまたはアウトバウンド IPv4 ACL をインターフェイスに適用します。1 つのインターフェイスに 1 つのポート ACL を適用できます。
ステップ 4	**show running-config aclmgr** **Example:** `n1000v(config-if)# show running-config aclmgr`	（任意）ACL の設定を表示します。

	コマンド	目的
ステップ 5	**copy running-config startup-config** **Example:** 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ます。

IP ACL のポート プロファイルへの追加

IP ACL をポート プロファイルに追加するには、次の手順を実行します。

はじめる前に

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。

- EXEC モードで CLI にログインしていること。
- 「IP ACL の作成」（P.9-6）の手順に従ってこのポート プロファイルに追加する IP ACL をすでに作成しており、その IP ACL 名を知っていること。
- 既存のポート プロファイルを使用する場合は、すでにそのポート プロファイルを作成しており、名前を知っていること。
- 新しいポート プロファイルを作成する場合は、インターフェイス タイプ（イーサネットまたは vEthernet）およびそのプロファイルに付与する名前がわかっていること。
- ポート プロファイルの詳細については、『*Cisco Nexus 1000V Port Profile Configuration Guide, Release 4.2(1)SV1(4a)*』を参照してください。
- このポート プロファイルに対して設定する IP アクセス コントロール リストの名前を知っていること。
- アクセス リストのパケット フローの方向を知っています。

手順の概要

1. **config t**
2. **port-profile** [**type** {**ethernet** | **vethernet**}] *profile-name*
3. **ip port access-group** *name* {**in** | **out**}
4. **show port-profile** [**brief** | **expand-interface** | **usage**] [**name** *profile-name*]
5. **copy running-config startup-config**

手順の詳細

	コマンド	説明
ステップ 1	**config t** **Example:** 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	**port-profile** [**type** {**ethernet** | **vethernet**}] *name* **Example:** n1000v(config)# port-profile AccessProf n1000v(config-port-prof)#	名前付きポート 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。
ステップ 3	**ip port access-group** *name* {**in** | **out**} **Example:** n1000v(config-port-prof)# ip port access-group allaccess4 out	着信トラフィックまたは発信トラフィックのポート プロファイルに名前付き ACL を追加します。
ステップ 4	**show port-profile name** *profile-name* **Example:** n1000v(config-port-prof)# show port-profile name AccessProf	（任意）確認のために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** **Example:** n1000v(config-port-prof)# copy running-config startup-config	（任意）リブート後に永続的な実行コンフィギュレーションを保存し、スタートアップ コンフィギュレーションにコピーして再起動します。

管理インターフェイスへの IP ACL の適用

管理インターフェイス mgmt0 に IPv4 または ACL を適用するには、次の手順を実行します。

はじめる前に

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。

- EXEC モードで CLI にログインしていること。
- 適用する ACL が存在し、目的に応じたトラフィック フィルタリングが設定されていることを確認します。詳細については、「IP ACL の作成」（P.9-6）または「IP ACL の変更」（P.9-7）を参照してください。

手順の概要

1. **config t**
2. **interface mgmt0**
3. **[no] ip access-group** *access-list* **[in | out]**
4. **show ip access-lists** *access-list*
5. **copy running-config startup-config**

手順の詳細

	コマンド	目的
ステップ 1	**config t** **Example:** n1000v# config t n1000v(config)#	CLI 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 mgmt0** **Example:** n1000v(config)# interface mgmt0 n1000v(config-if)#	管理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 access-group** *access-list* [**in** | **out**] **Example:** n1000v(config-if)# ip access-group telnet in n1000v(config-if)#	指定したインバウンド IPv4 ACL またはアウトバウンド IPv4 ACL をインターフェイスに適用します。 no オプションは指定された設定を削除します。
ステップ 4	**show ip access-lists** *access-list* **Example:** n1000v(config-if)# show ip access-lists telnet summary IP access list telnet statistics per-entry Total ACEs Configured:2 Configured on interfaces: mgmt0 - ingress (Router ACL) Active on interfaces: mgmt0 - ingress (Router ACL)	（任意）ACL の設定を表示します。
ステップ 5	**copy running-config startup-config** **Example:** 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ます。

IP ACL の設定の確認

IP ACL 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 aclmgr	IP ACL の設定および IP ACL が適用されているインターフェイスを含めて、ACL の設定を表示します。
show ip access-lists [*name*]	すべての IPv4 アクセス コントロール リスト（ACL）または特定の IPv4 ACL を表示します。
show ip access-list [*name*] **summary**	設定済みのすべての IPv4 ACL または名前付き IPv4 ACL の要約を表示します。

コマンド	目的
show running-config interface	ACL が適用されたインターフェイスの設定を表示します。
show running | grep acl-exception	アクセス リスト インストール失敗のエラー検出がイネーブルになっていることを確認します。

IP ACL のモニタリング

IP ACL のモニタリングには、次のコマンドを使用します。

コマンド	目的
show ip access-lists	IPv4 ACL の設定を表示します。IPv4 ACL に **statistics per-entry** コマンドが含まれている場合は、**show ip access-lists** コマンドの出力に、各ルールと一致したパケットの数が含まれます。
clear ip access-list counters	すべての IPv4 ACL または特定の IPv4 ACL の統計情報をクリアします。

IP ACL の設定例

次に、acl-01 という名前の IPv4 ACL を作成し、これをポート ACL として vEthernet インターフェイス 40 に適用する例を示します。

```
ip access-list acl-01
    permit ip 192.168.2.0/24 any
interface vethernet 40
ip port access-group acl-01 in
```

次に、ローカルに生成されたトラフィックのアクセス リスト マッチングをイネーブルにする例を示します。

```
ip access-list match-local-traffic
```

その他の関連資料

IP ACL の実装に関する詳細情報については、次を参照してください。

- 「関連資料」（P.9-16）
- 「標準」（P.9-16）

関連資料

関連項目	参照先
ACL の概念。	*「ACL について」（P.9-1）*
インターフェイスの設定。	『*Cisco Nexus 1000V Interface Configuration Guide, Release 4.2(1)SV1(4a)*』
ポート プロファイルの設定。	『*Cisco Nexus 1000V Port Profile Configuration Guide, Release 4.2(1)SV1(4a)*』
Cisco Nexus 1000V コマンドの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、使用上のガイドライン、および例。	『*Cisco Nexus 1000V Command Reference, Release 4.2(1)SV1(4a)*』

標準

標準	タイトル
この機能でサポートされる新規の標準または変更された標準はありません。また、既存の標準のサポートは変更されていません。	—

IP ACL 機能の履歴

ここでは、IP ACL のリリース履歴を示します。

機能名	リリース	機能情報
mgmt0 インターフェイスの IP ACL	4.2(1) SV1(4)	
IP ACL	4.0(4)SV1(1)	この機能が導入されました。

CHAPTER 10

MAC ACL の設定

この章では、MAC アクセス コントロール リスト（ACL）を設定する手順について次の内容で説明します。

MAC ACL の概要

MAC ACL は、各パケットのレイヤ 2 ヘッダー内の情報を使用してトラフィックをフィルタリングする ACL です。

MAC ACL の前提条件

MAC ACL の前提条件は次のとおりです。

- MAC ACL を設定するために、MAC アドレッシングおよびプロトコルに関する知識があること。
- 「ACL について」（P.9-1）に記載されている内容を理解していること。

注意事項および制約事項

MAC ACL の設定に関する注意事項と制約事項は次のとおりです。

- ほとんどの場合、IP パケットの ACL 処理は、I/O モジュール上で実行されます。管理インターフェイス トラフィックは、常にスーパーバイザ モジュールで処理されます。この場合、速度は遅くなります。
- ACL は、ポート チャネルではサポートされていません。

デフォルト設定

表 10-1 に、MAC ACL のデフォルトを示します。

表 10-1　MAC ACL のデフォルト パラメータ

パラメータ	デフォルト
MAC ACL	デフォルトでは MAC ACL は存在しません。
ACL ルール	すべての ACL に暗黙ルールが適用されます（「暗黙のルール」（P.9-3）を参照）。

MAC ACL の設定

ここでは、次の内容について説明します。

MAC ACL の作成

MAC ACL を作成し、これにルールを追加するには、次の手順を実行します。また、ACL をポート プロファイルに追加する場合にも、次の手順を実行します。

はじめる前に

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。

- EXEC モードで CLI にログインしていること。
- 作成する ACL に割り当てる名前があること。
- また、ポートプロファイルに ACL も追加する場合は、次の事項がわかっていること。

- 既存のポート プロファイルを使用する場合は、『*Cisco Nexus 1000V Port Profile Configuration Guide, Release 4.2(1)SV1(4a)*』に従ってすでにそのポート プロファイルを作成しており、名前を知っていること。
- 新しいポート プロファイルを作成する場合は、インターフェイス タイプ（イーサネットまたは vEthernet）およびそのプロファイルに付与する名前がわかっていること。
- アクセス リストのパケット フローの方向を知っています。

手順の概要

1. **config t**
2. **mac access-list** *name*
3. {**permit | deny**} *source destination protocol*
4. **statistics per-entry**
5. **show mac access-lists** *name*
6. **copy running-config startup-config**

手順の詳細

	コマンド	目的
ステップ 1	**config t** **Example:** n1000v# config t n1000v(config)#	CLI 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	**mac access-list** *name* **Example:** n1000v(config)# mac access-list acl-mac-01 n1000v(config-mac-acl)#	MAC ACL を作成して、ACL 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	{**permit** | **deny**} *source destination protocol* **Example:** n1000v(config-mac-acl)# permit 00c0.4f00.0000 0000.00ff.ffff any	MAC ACL 内にルールを作成します。 **permit** コマンドと **deny** コマンドには、トラフィックを識別するための多くの方法が用意されています。詳細については、『*Cisco Nexus 1000V Command Reference, Release 4.2(1)SV1(4a)*』を参照してください。
ステップ 4	**statistics per-entry** **Example:** n1000v(config-mac-acl)# statistics per-entry	（任意）その ACL のルールと一致するパケットのグローバル統計をデバイスが維持するように設定します。
ステップ 5	**show mac access-lists** *name* **Example:** n1000v(config-mac-acl)# show mac access-lists acl-mac-01	（任意）確認のために MAC ACL 設定を表示します。
ステップ 6	**copy running-config startup-config** **Example:** n1000v(config-mac-acl)# 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。

MAC ACL の変更

既存の MAC ACL を変更して、ルールの追加または削除を行うには、次の手順を実行します。

はじめる前に

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。

- EXEC モードで CLI にログインしていること。
- 既存の MAC ACL では、既存のルールを変更できません。
- 既存の MAC ACL 内で、ルールの追加または削除を実行できます。
- 既存のシーケンス番号の間にルールを追加する場合などに、シーケンス番号を再割り当てするには、**resequence** コマンドを使用します。

手順の概要

1. **config t**
2. **mac access-list** *name*
3. [*sequence-number*] {**permit | deny**} *source destination protocol*
4. **no** {*sequence-number* | {**permit | deny**} *source destination protocol*}
5. [**no**] **statistics per-entry**
6. **show mac access-lists** *name*
7. **copy running-config startup-config**

手順の詳細

	コマンド	目的

ステップ 1	**config t**
	
	Example:
	`n1000v# config t`
	`n1000v(config)#`
		CLI 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	**mac access-list** *name*
	
	Example:
	`n1000v(config)# mac access-list acl-mac-01`
	`n1000v(config-mac-acl)#`
		名前を指定する ACL の ACL 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	[*sequence-number*] {**permit** | **deny**} *source destination protocol* **Example:** `n1000v(config-mac-acl)# 100 permit mac 00c0.4f00.00 0000.00ff.ffff any`	（任意）MAC ACL 内にルールを作成します。シーケンス番号を指定すると、ACL 内のルール挿入位置を指定できます。シーケンス番号を指定しないと、ルールは ACL の末尾に追加されます。 **permit** コマンドと **deny** コマンドには、トラフィックを識別するための多くの方法が用意されています。詳細については、『*Cisco Nexus 1000V Command Reference, Release 4.2(1)SV1(4a)*』を参照してください。

	コマンド	目的
ステップ 4	**no** {*sequence-number* | {**permit** | **deny**} *source destination protocol*} **Example:** n1000v(config-mac-acl)# no 80	（任意）MAC ACL から指定したルールを削除します。 **permit** コマンドと **deny** コマンドには、トラフィックを識別するための多くの方法が用意されています。詳細については、『*Cisco Nexus 1000V Command Reference, Release 4.2(1)SV1(4a)*』を参照してください。
ステップ 5	[**no**] **statistics per-entry** **Example:** n1000v(config-mac-acl)# statistics per-entry	（任意）その ACL のルールと一致するパケットのグローバル統計をデバイスが維持するように設定します。 **no** オプションを使用すると、デバイスはその ACL のグローバル統計の維持を停止します。
ステップ 6	**show mac access-lists** *name* **Example:** n1000v(config-mac-acl)# show mac access-lists acl-mac-01	（任意）MAC ACL の設定を表示します。
ステップ 7	**copy running-config startup-config** **Example:** n1000v(config-mac-acl)# 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。

MAC ACL の削除

MAC ACL を削除するには、次の手順を実行します。

はじめる前に

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。

- EXEC モードで CLI にログインしていること。
- その ACL がインターフェイスに適用されているかどうかを確認します。
- 現在適用されている ACL を削除できます。ACL を削除しても、その ACL が適用されていたインターフェイスの設定は影響を受けません。削除された ACL は空であると見なされます。
- MAC ACL が設定されているインターフェイスを見つけるには、**show mac access-lists** コマンドを **summary** キーワードとともに使用します。

手順の概要

1. **config t**
2. **no mac access-list** *name*
3. **show mac access-lists** *name* **summary**
4. **copy running-config startup-config**

手順の詳細

	コマンド	目的
ステップ 1	**config t** **Example:** n1000v# config t n1000v(config)#	CLI 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 mac access-list** *name* **Example:** n1000v(config)# no mac access-list acl-mac-01 n1000v(config)#	指定した MAC ACL を実行コンフィギュレーションから削除します。
ステップ 3	**show mac access-lists** *name* **summary** **Example:** n1000v(config)# show mac access-lists acl-mac-01 summary	（任意）MAC ACL の設定を表示します。ACL がインターフェイスに引き続き適用されている場合は、インターフェイスが表示されます。
ステップ 4	**copy running-config startup-config** **Example:** 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ます。

MAC ACL 内のシーケンス番号の変更

MAC ACL のルールに割り当てられているシーケンス番号を変更するには、次の手順を実行します。ACL にルールを挿入する必要がある場合で、シーケンス番号が不足しているときは、再割り当てすると便利です。詳細については、「MAC ACL 内のシーケンス番号の変更」（P.10-6）を参照してください。

はじめる前に

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。

- EXEC モードで CLI にログインしていること。

手順の概要

1. **config t**
2. **resequence mac access-list** *name starting-sequence-number increment*
3. **show mac access-lists** *name*
4. **copy running-config startup-config**

手順の詳細

	コマンド	目的
ステップ 1	**config t** **Example:** n1000v# config t n1000v(config)#	CLI 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	**resequence mac access-list** *name starting-sequence-number increment* **Example:** n1000v(config)# resequence mac access-list acl-mac-01 100 10	ACL 内に記述されているルールにシーケンス番号を付けます。starting-sequence number に指定したシーケンス番号が最初のルールに付けられます。後続の各ルールには、直前のルールよりも大きい番号が付けられます。番号の間隔は、指定した増分によって決まります。
ステップ 3	**show mac access-lists** *name* **Example:** n1000v(config)# show mac access-lists acl-mac-01	（任意）MAC ACL の設定を表示します。
ステップ 4	**copy running-config startup-config** **Example:** 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ます。

MAC ACL のポート ACL としての適用

MAC ACL をポート ACL として適用するには、次の手順を実行します。

はじめる前に

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。

- EXEC モードで CLI にログインしていること。
- 適用する ACL が存在し、必要な方法でトラフィックをフィルタリングするように設定されていることを確認します。MAC ACL の設定の詳細については、「MAC ACL の設定」（P.10-2）を参照してください。
- MAC ACL は、ポート プロファイルを使用してポートに適用することもできる。ポート プロファイルについては、『*Cisco Nexus 1000V Port Profile Configuration Guide, Release 4.2(1)SV1(4a)*』を参照してください。

手順の概要

1. **config t**
2. **interface vethernet** *port*
3. **mac port access-group** *access-list* [**in** | **out**]
4. **show running-config aclmgr**
5. **copy running-config startup-config**

手順の詳細

	コマンド	目的
ステップ 1	**config t** **Example:** n1000v# config t n1000v(config)#	CLI 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** *port* **Example:** n1000v(config)# interface vethernet 35 n1000v(config-if)#	指定した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	**mac port access-group** *access-list* [**in** | **out**] **Example:** n1000v(config-if)# mac port access-group acl-01 in	MAC ACL をインターフェイスに適用します。
ステップ 4	**show running-config aclmgr** **Example:** n1000v(config-if)# show running-config aclmgr	（任意）ACL の設定を表示します。
ステップ 5	**copy running-config startup-config** **Example:** 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ます。

MAC ACL のポート プロファイルへの追加

MAC ACL をポート プロファイルに追加するには、次の手順を実行します。

はじめる前に

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。

- EXEC モードで CLI にログインしていること。
- 「MAC ACL の作成」（P.10-2）の手順に従ってこのポート プロファイルに追加する MAC ACL をすでに作成しており、名前を知っていること。
- 既存のポート プロファイルを使用する場合は、すでにそのポート プロファイルを作成しており、名前を知っていること。
- 新しいポート プロファイルを作成する場合は、インターフェイス タイプ（イーサネットまたは vEthernet）およびそのプロファイルに付与する名前がわかっていること。
- ポート プロファイルの詳細については、『*Cisco Nexus 1000V Port Profile Configuration Guide, Release 4.2(1)SV1(4a)*』を参照してください。
- アクセス リストのパケット フローの方向を知っています。

手順の概要

1. **config t**

2. **port-profile** [**type** {**ethernet** | **vethernet**}] *profile-name*
3. **mac port access-group** *name* {**in** | **out**}
4. **show port-profile** [**brief** | **expand-interface** | **usage**] [**name** *profile-name*]
5. **copy running-config startup-config**

手順の詳細

	コマンド	説明
ステップ 1	**config t** **Example:** 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	**port-profile** [**type** {**ethernet** | **vethernet**}] *name* **Example:** n1000v(config)# port-profile AccessProf n1000v(config-port-prof)#	名前付きポート 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。
ステップ 3	**mac port access-group** *name* {**in** | **out**} **Example:** n1000v(config-port-prof)# mac port access-group allaccess4 out	着信トラフィックまたは発信トラフィックのポート プロファイルに名前付き ACL を追加します。
ステップ 4	**show port-profile name** *profile-name* **Example:** n1000v(config-port-prof)# show port-profile name AccessProf	（任意）確認のために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** **Example:** n1000v(config-port-prof)# copy running-config startup-config	（任意）リブート後に永続的な実行コンフィギュレーションを保存し、スタートアップ コンフィギュレーションにコピーして再起動します。

MAC ACL の設定の確認

次のコマンドを使用して、MAC ACL 設定を確認できます。

コマンド	目的
show mac access-lists	MAC ACL の設定を表示します。 例 10-1（P.10-10）を参照してください。
show running-config aclmgr	MAC ACL、MAC ACL が適用されるインターフェイスなど、MAC ACL の設定を表示します。 例 10-2（P.10-10）を参照してください。
show running-config interface	ACL を適用したインターフェイスの設定を表示します。 例 10-3（P.10-10）を参照してください。

例 10-1　show mac access-list

```
n1000v# show mac access-list

MAC access list acl-mac-01
        10 permit 00c0.4f00.0000 0000.00ff.ffff any
n1000v#
```

例 10-2　show running-config aclmgr

```
n1000v# show running-config aclmgr

!Command: show running-config aclmgr
!Time: Mon Jan  3 15:53:50 2011

version 4.2(1)SV1(4)
mac access-list acl-mac-01
  10 permit 00c0.4f00.0000 0000.00ff.ffff any

interface Vethernet35
  mac port access-group acl-mac-01 in

n1000v#
```

例 10-3　show running-config interface

```
n1000v# show running-config interface

!Command: show running-config interface
!Time: Mon Jan  3 15:58:25 2011

version 4.2(1)SV1(4)

interface mgmt0
  ip address 172.23.180.75/24

interface Vethernet35
  mac port access-group acl-mac-01 in

interface Vethernet1998

interface control0
  ip address 10.2.10.10/24

n1000v#
```

MAC ACL のモニタリング

MAC ACL のモニタリングには、次のコマンドを使用します。

コマンド	目的
show mac access-lists	MAC ACL の設定を表示します。MAC ACL に **statistics per-entry** コマンドが含まれている場合は、**show mac access-lists** コマンドの出力に、各ルールと一致したパケットの数が含まれます。
clear mac access-list counters	すべての MAC ACL、または特定の MAC ACL の統計情報を消去します。

MAC ACL の設定例

次に、MAC ACL acl-mac-01 を作成して任意のプロトコルの MAC 00c0.4f00.00.000.00ff.ffff を許可し、ACL を vEthernet インターフェイス 35 の発信トラフィックのポートとして適用する例を示します。

```
config t
mac access-list acl-mac-01
  permit 00c0.4f00.0000 0000.00ff.ffff any
interface vethernet 35
mac port access-group acl-mac-01 out
```

次に、ポート プロファイル *AccessProf* に MAC ACL *allaccess4* を追加する例を示します。

```
config t
port-profile AccessProf
mac port access-group allaccess4 out
show port-profile name AccessProf
port-profile AccessProf
  description: allaccess4
  type: vethernet
  status: disabled
  capability l3control: no
  pinning control-vlan: -
  pinning packet-vlan: -
  system vlans: none
  port-group:
  max ports: 32
  inherit:
  config attributes:
    mac port access-group allaccess4 out
  evaluated config attributes:
    mac port access-group allaccess4 out
  assigned interfaces:
```

その他の関連資料

MAC ACL の実装に関する詳細情報については、次を参照してください。

- 「関連資料」（P.10-12）
- 「標準」（P.10-12）

関連資料

関連項目	参照先
ACL の概念。	*「ACL について」（P.9-1）*
インターフェイスの設定。	『*Cisco Nexus 1000V Interface Configuration Guide, Release 4.2(1)SV1(4a)*』
ポート プロファイルの設定。	『*Cisco Nexus 1000V Port Profile Configuration Guide, Release 4.2(1)SV1(4a)*』
Cisco Nexus 1000V のすべてのコマンドのコマンド構文、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、および例	『*Cisco Nexus 1000V Command Reference, Release 4.2(1)SV1(4a)*』

標準

標準	タイトル
この機能でサポートされる新規の標準または変更された標準はありません。また、既存の標準のサポートは変更されていません。	—

MAC ACL 機能の履歴

ここでは、MAC ACL のリリース履歴を示します。

機能名	リリース	機能情報
MAC ACL	4.0(4)SV1(1)	この機能が導入されました。

CHAPTER 11

ポート セキュリティの設定

この章では、ポート セキュリティを設定する手順について次の内容で説明します。

ポート セキュリティの概要

ポート セキュリティを使用すると、限定的なセキュア MAC アドレスからのインバウンド トラフィックを許可するようにレイヤ 2 インターフェイスを設定することができます。セキュアな MAC アドレスからのトラフィックは、同じ VLAN 内の別のインターフェイス上では許可されません。「セキュア」にできる MAC アドレスの数は、インターフェイス単位で設定します。

ここでは、次の内容について説明します。

セキュア MAC アドレスの学習

MAC アドレスは学習というプロセスによってセキュア アドレスになります。学習できるアドレスの数には制限があります（「セキュア MAC アドレスの最大数」（P.11-3）を参照）。ポート セキュリティがイネーブルになっているインターフェイスでのアドレス学習には、次の方式を使用できます。

- 「ダイナミック方式」（P.11-2）（デフォルトの方式）
- 「スティッキ方式」（P.11-2）

スタティック方式

スタティック学習方式では、ユーザが手動でインターフェイス設定にセキュア MAC アドレスを追加したり、設定から削除したりできます。

スタティック セキュア MAC アドレスのエントリは、明示的に削除するまで、インターフェイスの設定内に維持されます。詳細については、「インターフェイスからのスタティックまたはスティッキ セキュア MAC アドレスの削除」（P.11-11）を参照してください。

スタティック方式では、ダイナミック方式またはスティッキ方式のアドレス学習がイネーブルになっているかどうかに関係なく、セキュア アドレスを追加できます。

ダイナミック方式

デフォルトでは、インターフェイスのポート セキュリティをイネーブルにすると、ダイナミック学習方式がイネーブルになります。この方式では、デバイスは、入力トラフィックがインターフェイスを通過するときに MAC アドレスをセキュア アドレスにします。このようなアドレスがまだセキュア アドレスではなく、デバイスのアドレス数が適用可能な最大数に達していなければ、デバイスはそのアドレスをセキュア アドレスにして、トラフィックを許可します。

ダイナミック アドレスはエージングが行われ、エージングの期限に達すると、ドロップされます（「ダイナミック アドレスのエージング」（P.11-2）を参照）。

ダイナミック アドレスは、再起動後は維持されません。

ダイナミック方式で学習された特定のアドレス、または特定のインターフェイスでダイナミックに学習されたすべてのアドレスを削除する場合は、「ダイナミック セキュア MAC アドレスの削除」（P.11-12）を参照してください。

スティッキ方式

スティッキ方式をイネーブルにすると、デバイスは、ダイナミック アドレス学習と同じ方法で MAC アドレスをセキュア アドレスにします。これらのアドレスは、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（**copy run start**）することにより、再起動後も維持することができます。

ダイナミックとスティッキのアドレス学習は両方同時にイネーブルにできません。あるインターフェイスのスティッキ学習をイネーブルにすると、ダイナミック学習が停止されて、代わりにスティッキ学習が使用されます。スティッキ学習をディセーブルにすると、ダイナミック学習が再開されます。

スティッキ セキュア MAC アドレスはエージングされません。

スティッキ方式で学習された特定のアドレスを削除する場合は、「インターフェイスからのスタティックまたはスティッキ セキュア MAC アドレスの削除」（P.11-11）を参照してください。

ダイナミック アドレスのエージング

ダイナミック方式で学習された MAC アドレスはエージングされ、エージングの期限に達するとドロップされます。エージングの期限は、インターフェイスごとに設定できます。有効な範囲は 0 ～ 1440 分です。0 を設定すると、エージングはディセーブルになります。

アドレス エージングの判断には、2 つの方法があります。

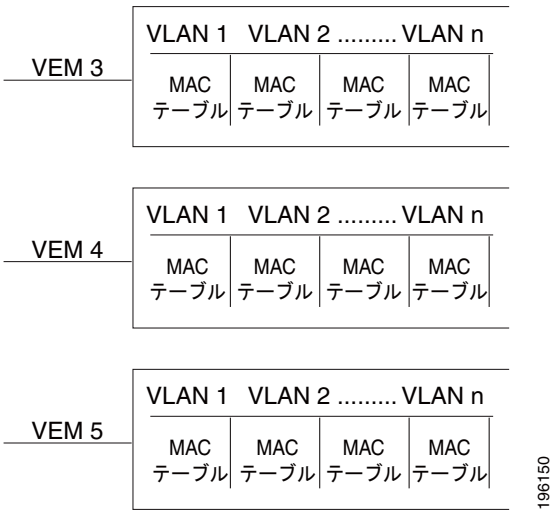
- 非アクティブ：適用可能なインターフェイス上のアドレスからデバイスが最後にパケットを受信して以降の経過時間。
- 絶対時間：デバイスがアドレスを学習して以降の経過時間。これがデフォルトのエージング方法ですが、デフォルトのエージング時間は 0 分（エージングはディセーブル）です。

セキュア MAC アドレスの最大数

セキュア ポート上のセキュア MAC アドレスは、他の標準的な MAC と同じ MAC アドレス テーブルに挿入されます。MAC テーブルの上限に達すると、その VLAN に対する新しいセキュア MAC の学習は行われなくなります。

図 11-1 に示すように、VEM 内の VLAN ごとに 1 つの転送テーブルがあり、各転送テーブルにセキュア MAC アドレスを最大数まで格納できます。現在の MAC アドレスの最大数については、「セキュリティ設定の制限値」（P.17-1）を参照してください。

図 11-1　VEM あたりのセキュア MAC アドレス



インターフェイスのセキュア MAC アドレス

デフォルトでは、各インターフェイスのセキュア MAC アドレスは 1 つだけです。各インターフェイス、またはインターフェイス上の各 VLAN に許容可能な最大 MAC アドレス数を設定できます。最大数は、ダイナミック、スティッキ、スタティックのいずれの方式で学習された MAC アドレスにも適用されます。

ヒント　アドレスの最大数を 1 に設定し、接続された装置の MAC アドレスを設定すると、その装置にはポートの全帯域幅が保証されます。

インターフェイス 1 つあたりの許容されるセキュア MAC アドレスの数は、次の制限値によって決定されます。

- デバイスの最大数：デバイスが許容できるセキュア MAC アドレスの最大数は 8192 です。この値は変更できません。新しいアドレスを学習するとデバイスの最大数を超過してしまう場合、たとえインターフェイスや VLAN の最大数に達していなくても、デバイスは新しいアドレスの学習を許可しません。
- インターフェイスの最大数：ポート セキュリティで保護されるインターフェイスごとに、セキュア MAC アドレスの最大数を設定できます。デフォルトでは、インターフェイスの最大アドレス数は 1 です。インターフェイスの最大数を、デバイスの最大数より大きくすることはできません。
- VLAN の最大数：ポート セキュリティで保護される各インターフェイスについて、VLAN あたりのセキュア MAC アドレスの最大数を設定できます。VLAN の最大数を、インターフェイスの最大数より大きくすることはできません。VLAN 最大数の設定が適しているのは、トランク ポートの場合だけです。VLAN の最大数には、デフォルト値はありません。

  VLAN とインターフェイスの最大数の関係については、「セキュリティ違反と処理」（P.11-4）に例が示されています。

インターフェイスあたりの、VLAN とインターフェイスの最大数は必要に応じて設定できます。ただし、新しい制限値が、適用可能なセキュア アドレス数よりも少ない場合は、まず、セキュア MAC アドレスの数を減らす必要があります。ダイナミックに学習されたアドレスの削除方法については、「ダイナミック セキュア MAC アドレスの削除」（P.11-12）を参照してください。スティッキまたはスタティック方式で学習されたアドレスの削除方法については、「インターフェイスからのスタティックまたはスティッキ セキュア MAC アドレスの削除」（P.11-11）を参照してください。

セキュリティ違反と処理

次のいずれかが発生すると、ポート セキュリティ機能によってセキュリティ違反がトリガーされます。

- あるインターフェイスにセキュア MAC アドレス以外のアドレスから入力トラフィックが着信し、そのアドレスを学習するとセキュア MAC アドレスの適用可能な最大数を超えてしまう場合

  あるインターフェイスに VLAN とインターフェイスの両方の最大数が設定されている場合は、どちらかの最大数を超えると、違反が発生します。たとえば、ポート セキュリティが設定されている単一のインターフェイスについて、次のように想定します。

  - VLAN 1 の最大アドレス数は 5 です。
  - このインターフェイスの最大アドレス数は 10 です。

  次のいずれかが発生すると、違反が検出されます。

  - VLAN 1 のアドレスが 5 つ学習されていて、6 番めのアドレスからのインバウンド トラフィックが VLAN 1 のインターフェイスに着信した場合
  - このインターフェイス上のアドレスが 10 個学習されていて、11 番めのアドレスからのインバウンド トラフィックがこのインターフェイスに着信した場合
- あるインターフェイスのセキュア MAC アドレスになっているアドレスからの入力トラフィックが、そのインターフェイスと同じ VLAN 内の別のインターフェイスに着信した場合

（注） 特定のセキュア ポートでセキュア MAC アドレスが設定または学習された後、同一 VLAN 上の別のポートでポート セキュリティがセキュア MAC アドレスを検出したときに発生する一連のイベントは、MAC 移動の違反と呼ばれます。

インターフェイス上でセキュリティ違反が発生したときは、そのインターフェイスのポート セキュリティ設定で指定されている処理が適用されます。デバイスが実行できる処理は次のとおりです。

- シャットダウン：違反をトリガーしたパケットの受信インターフェイスをシャットダウンします。このインターフェイスはエラー ディセーブル状態になります。これがデフォルトの処理です。インターフェイスの再起動後も、セキュア MAC アドレスを含めて、ポート セキュリティの設定は維持されます。

  シャットダウン後にデバイスが自動的にインターフェイスを再起動するように設定するには、**errdisable** 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。あるいは、**shutdown** および **no shut down** のインターフェイス コンフィギュレーション コマンドを入力することにより、手動でインターフェイスを再起動することもできます。

  Example:
  ```
  n1000v(config)# errdisable recovery cause psecure-violation
  n1000v(config)# copy running-config startup-config (Optional)
  ```

- 保護：違反の発生を防止します。インターフェイスの最大 MAC アドレス数に到達するまでアドレス学習を継続し、到達後はそのインターフェイスでの学習をディセーブルにして、セキュア MAC アドレス以外のアドレスからの入力トラフィックをすべてドロップします。

セキュア MAC アドレスからの入力トラフィックが、そのアドレスをセキュア アドレスにしたインターフェイスとは異なるインターフェイスに着信したことにより違反が発生した場合は、トラフィックを受信したインターフェイスに対して処理が適用されます。MAC の移行違反は、別のインターフェイスですでにセキュアになっている MAC を認識するポートでトリガーされます。

ポート セキュリティとポート タイプ

ポート セキュリティを設定できるのは、レイヤ 2 インターフェイスだけです。各種のインターフェイスまたはポートとポート セキュリティについて次に詳しく説明します。

- アクセス ポート：レイヤ 2 アクセス ポートとして設定したインターフェイスにポート セキュリティを設定できます。アクセス ポートでポート セキュリティが適用されるのは、アクセス VLAN だけです。
- トランク ポート：レイヤ 2 トランク ポートとして設定したインターフェイスにポート セキュリティを設定できます。アクセス ポートには、VLAN 最大数を設定しても効果はありません。デバイスが VLAN 最大数を適用するのは、トランク ポートに関連付けられた VLAN だけです。
- SPAN ポート：SPAN 送信元ポートにはポート セキュリティを設定できますが、SPAN 宛先ポートには設定できません。
- イーサネット ポート：ポート セキュリティはイーサネット ポートではサポートされません。
- イーサネット ポート チャネル：イーサネット ポート チャネルでは、ポート セキュリティはサポートされていません。

アクセス ポートからトランク ポートへの変更による影響

ポート セキュリティが設定されているレイヤ 2 インターフェイスでアクセス ポートをトランク ポートに変更すると、ダイナミック方式で学習されたすべてのセキュア アドレスがドロップされます。ネイティブ トランク VLAN に接続されているデバイスは、スタティック方式またはスティッキ方式で学習したアドレスを移行します。

トランク ポートからアクセス ポートへの変更による影響

ポート セキュリティが設定されているレイヤ 2 インターフェイスでトランク ポートをアクセス ポートに変更すると、ダイナミック方式で学習されたすべてのセキュア アドレスがドロップされます。設定済みの MAC アドレスおよびスティッキ MAC アドレスは、ネイティブ トランク VLAN に存在しない場合、かつ移行先のアクセス ポートに対して設定されたアクセス VLAN とも一致しない場合は、すべてドロップされます。

注意事項および制約事項

ポート セキュリティを設定する場合、次の注意事項に従ってください。

- ポート セキュリティは、次でサポートされていません。
  - イーサネット インターフェイス
  - イーサネット ポートチャネル インターフェイス
  - Switched Port Analyzer（SPAN; スイッチド ポート アナライザ）の宛先ポート
- ポート セキュリティは他の機能に依存しません。
- ポート セキュリティは 802.1X をサポートしていません。
- ポート セキュリティは、スタティック MAC がすでに存在するインターフェイスには設定できません。
- VLAN にスタティック MAC がすでに存在する場合、それが別のインターフェイスでプログラムされている場合でも、その VLAN のインターフェイスでポート セキュリティをイネーブルにすることはできません。

デフォルト設定値

表 11-1 に、ポート セキュリティ パラメータのデフォルトの設定値を示します。

表 11-1　ポート セキュリティ パラメータのデフォルト値

パラメータ	デフォルト
インターフェイス	ディセーブル
MAC アドレス ラーニング方式	ダイナミック
セキュア MAC アドレスのインターフェイス最大数	1
セキュリティ違反時の処理	シャットダウン

ポート セキュリティの設定

ここでは、次の内容について説明します。

- 「レイヤ 2 インターフェイスに対するポート セキュリティのイネーブル化またはディセーブル化」（P.11-7）
- 「スティッキ MAC アドレス ラーニングのイネーブル化またはディセーブル化」（P.11-8）

- 「インターフェイスのスタティック セキュア MAC アドレスの追加」（P.11-9）
- 「インターフェイスからのスタティックまたはスティッキ セキュア MAC アドレスの削除」（P.11-11）
- 「ダイナミック セキュア MAC アドレスの削除」（P.11-12）
- 「MAC アドレスの最大数の設定」（P.11-13）
- 「アドレス エージングのタイプと期間の設定」（P.11-15）
- 「セキュリティ違反時の処理の設定」（P.11-16）
- 「ポート セキュリティ違反がディセーブルなポートの回復」（P.11-17）

レイヤ 2 インターフェイスに対するポート セキュリティ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ポート セキュリティをイネーブルまたはディセーブルにするには、次の手順を実行します。MAC アドレスのダイナミック学習についての詳細は、「セキュア MAC アドレスの学習」（P.11-1）を参照してください。

（注）　ルーテッド インターフェイスでは、ポート セキュリティをイネーブルにできません。

はじめる前に

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。

- EXEC モードで CLI にログインしていること。
- デフォルトでは、ポート セキュリティはすべてのインターフェイスでディセーブルです。
- インターフェイスのポート セキュリティをイネーブルにすると、MAC アドレスのダイナミック学習もイネーブルになります。スティッキ方式の MAC アドレス ラーニングをイネーブルにするには、「スティッキ MAC アドレス ラーニングのイネーブル化またはディセーブル化」（P.11-8）の手順も完了する必要があります。

手順の概要

1. **config t**
2. **interface** *type number*
3. **[no] switchport port-security**
4. **show running-config port-security**
5. **copy running-config startup-config**

手順の詳細

	コマンド	目的
ステップ 1	**config t** **Example:** n1000v# config t n1000v(config)#	CLI 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** *type number* **Example:** n1000v(config)# interface vethernet 36 n1000v(config-if)#	指定した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**] **switchport port-security** **Example:** n1000v(config-if)# switchport port-security	インターフェイス上でポート セキュリティ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ポート セキュリティがディセーブルになります。
ステップ 4	**show running-config port-security** **Example:** n1000v(config-if)# show running-config port-security	ポート セキュリティの設定を表示します。
ステップ 5	**copy running-config startup-config** **Example:** 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ます。

スティッキ MAC アドレス ラーニングのイネーブル化またはディセーブル化

インターフェイスのスティッキ MAC アドレス ラーニングをディセーブルまたはイネーブルにするには、次の手順を実行します。

はじめる前に

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。

- EXEC モードで CLI にログインしていること。
- ダイナミック MAC アドレス ラーニングがインターフェイスのデフォルトです。
- デフォルトでは、スティッキ MAC アドレス ラーニングはディセーブルです。
- ポート セキュリティが目的のインターフェイスでイネーブルになっていることを確認します。
  - 設定を確認する手順については、「ポート セキュリティの設定の確認」（P.11-19）を参照してください。
  - インターフェイスのポート セキュリティをイネーブルにする手順については、「レイヤ 2 インターフェイスに対するポート セキュリティのイネーブル化またはディセーブル化」（P.11-7）を参照してください。

手順の概要

1. **config t**
2. **interface** *type number*
3. [**no**] **switchport port-security mac-address sticky**
4. **show running-config port-security**
5. **copy running-config startup-config**

手順の詳細

	コマンド	目的

ステップ 1	**config t**
	
	Example:
	`n1000v# config t`
	`n1000v(config)#`
		CLI 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** *type number*
	
	Example:
	`n1000v(config)# interface vethernet 36`
	`n1000v(config-if)#`
		指定した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**] **switchport port-security mac-address sticky** **Example:** `n1000v(config-if)# switchport port-security mac-address sticky`	そのインターフェイスのスティッキ MAC アドレス ラーニングをイネーブルにします。 **no** オプションを使用すると、スティッキ MAC アドレス ラーニングがディセーブルになります。
ステップ 4	**show running-config port-security** **Example:** `n1000v(config-if)# show running-config port-security`	ポート セキュリティの設定を表示します。
ステップ 5	**copy running-config startup-config** **Example:** `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ます。

インターフェイスのスタティック セキュア MAC アドレスの追加

レイヤ 2 インターフェイスにスタティック セキュア MAC アドレスを追加するには、次の手順を実行します。

はじめる前に

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。

- EXEC モードで CLI にログインしていること。
- デフォルトでは、インターフェイスにスタティック セキュア MAC アドレスは設定されません。
- インターフェイスのセキュア MAC アドレス最大数に達しているかどうかを判断します（**show port-security** コマンドを使用）。

- 必要な場合は、セキュア MAC アドレスを削除できます。次のいずれかを参照してください。
  - 「インターフェイスからのスタティックまたはスティッキ セキュア MAC アドレスの削除」（P.11-11）
  - 「ダイナミック セキュア MAC アドレスの削除」（P.11-12））
  - 「MAC アドレスの最大数の設定」（P.11-13））。
- ポート セキュリティが目的のインターフェイスでイネーブルになっていることを確認します。
  - 設定を確認する手順については、「ポート セキュリティの設定の確認」（P.11-19）を参照してください。
  - インターフェイスのポート セキュリティをイネーブルにする手順については、「レイヤ 2 インターフェイスに対するポート セキュリティのイネーブル化またはディセーブル化」（P.11-7）を参照してください。

手順の概要

1. **config t**
2. **interface** *type number*
3. [**no**] **switchport port-security mac-address** *address* [**vlan** *vlan-ID*]
4. **show running-config port-security**
5. **copy running-config startup-config**

手順の詳細

	コマンド	目的
ステップ 1	**config t** **Example:** n1000v# config t n1000v(config)#	CLI 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** *type number* **Example:** n1000v(config)# interface vethernet 36 n1000v(config-if)#	指定した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**] **switchport port-security mac-address** *address* [**vlan** *vlan-ID*] **Example:** n1000v(config-if)# switchport port-security mac-address 0019.D2D0.00AE	現在のインターフェイスのポート セキュリティにスタティック MAC アドレスを設定します。そのアドレスからのトラフィックを許可する VLAN を指定する場合は、**vlan** キーワードを使用します。
ステップ 4	**show running-config port-security** **Example:** n1000v(config-if)# show running-config port-security	ポート セキュリティの設定を表示します。
ステップ 5	**copy running-config startup-config** **Example:** 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ます。

インターフェイスからのスタティックまたはスティッキ セキュア MAC アドレスの削除

レイヤ 2 インターフェイスからスタティック方式またはスティッキ方式のセキュア MAC アドレスを削除するには、次の手順を実行します。

はじめる前に

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。

- EXEC モードで CLI にログインしていること。
- ポート セキュリティが目的のインターフェイスでイネーブルになっていることを確認します。
  - 設定を確認する手順については、「ポート セキュリティの設定の確認」（P.11-19）を参照してください。
  - インターフェイスのポート セキュリティをイネーブルにする手順については、「レイヤ 2 インターフェイスに対するポート セキュリティのイネーブル化またはディセーブル化」（P.11-7）を参照してください。

手順の概要

1. **config t**
2. **interface** *type number*
3. **no switchport port-security mac-address** *address* [**vlan** *vlan-ID*]
4. **show running-config port-security**
5. **copy running-config startup-config**

手順の詳細

	コマンド	目的

ステップ 1	**config t**
	
	Example:
	`n1000v# config t`
	`n1000v(config)#`
		CLI 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。

	コマンド	目的
ステップ 2	**interface** *type number* **Example:** n1000v(config)# interface vethernet 36 n1000v(config-if)#	指定した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 switchport port-security mac-address** *address* **Example:** n1000v(config-if)# no switchport port-security mac-address 0019.D2D0.00AE	現在のインターフェイスのポート セキュリティから MAC アドレスを削除します。
ステップ 4	**show running-config port-security** **Example:** n1000v(config-if)# show running-config port-security	ポート セキュリティの設定を表示します。
ステップ 5	**copy running-config startup-config** **Example:** 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ます。

ダイナミック セキュア MAC アドレスの削除

ダイナミックに学習されたセキュア MAC アドレスを削除するには、次の手順を実行します。

はじめる前に

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。

- EXEC モードで CLI にログインしていること。

手順の概要

1. **config t**
2. **clear port-security dynamic** {**interface vethernet** *number* | **address** *address*} [**vlan** *vlan-ID*]
3. **show port-security address**

手順の詳細

	コマンド	目的
ステップ 1	**config t** **Example:** n1000v# config t n1000v(config)#	CLI 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	**clear port-security dynamic** {**interface vethernet** *number* | **address** *address*} [**vlan** *vlan-ID*] **Example:** n1000v(config)# clear port-security dynamic interface vethernet 36	ダイナミックに学習されたセキュア MAC アドレスを削除します。次の方法で指定できます。 **interface** キーワードを使用すると、指定したインターフェイスでダイナミックに学習されたアドレスがすべて削除されます。 **address** キーワードを使用すると、指定した単一のダイナミック学習アドレスが削除されます。 特定の VLAN のアドレスを削除するようにコマンドに制限を加えるには、**vlan** キーワードを使用します。
ステップ 3	**show port-security address** **Example:** n1000v(config)# show port-security address	セキュア MAC アドレスを表示します。

MAC アドレスの最大数の設定

レイヤ 2 インターフェイスで学習可能な MAC アドレスまたはスタティックに設定可能な MAC アドレスの最大数を設定するには、次の手順を実行します。レイヤ 2 インターフェイス上の VLAN 単位でも MAC アドレスの最大数を設定できます。設定できる最大アドレス数は 4096 です。

（注）　インターフェイスですでに学習されているアドレス数またはインターフェイスにスタティックに設定されたアドレス数よりも小さい数を最大数に指定すると、コマンドは拒否されます。

スティッキ方式またはスタティック方式で学習されたアドレスの数を減らす場合は、「インターフェイスからのスタティックまたはスティッキ セキュア MAC アドレスの削除」（P.11-11）を参照してください。

ダイナミック方式で学習されたアドレスをすべて削除するには、**shutdown** および **no shutdown** のコマンドを使用して、インターフェイスを再起動します。

はじめる前に

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。

- EXEC モードで CLI にログインしていること。
- セキュア MAC は L2 Forwarding Table（L2FT; L2 転送テーブル）を共有します。各 VLAN の転送テーブルには最大 1024 エントリを保持できます。
- デフォルトでは、各インターフェイスのセキュア MAC アドレスの最大数は 1 です。
- VLAN には、セキュア MAC アドレス数のデフォルトの最大値はありません。

- ポート セキュリティが目的のインターフェイスでイネーブルになっていることを確認します。
  - 設定を確認する手順については、「ポート セキュリティの設定の確認」（P.11-19）を参照してください。
  - インターフェイスのポート セキュリティをイネーブルにする手順については、「レイヤ 2 インターフェイスに対するポート セキュリティのイネーブル化またはディセーブル化」（P.11-7）を参照してください。

手順の概要

1. **config t**
2. **interface** ***type*** *number*
3. [**no**] **switchport port-security maximum** *number* [**vlan** *vlan-ID*]
4. **show running-config port-security**
5. **copy running-config startup-config**

手順の詳細

	コマンド	目的

ステップ 1	**config t**
	
	Example:
	`n1000v# config t`
	`n1000v(config)#`
		CLI 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** *type number*
	
	Example:
	`n1000v(config)# interface vethernet 36`
	`n1000v(config-if)#`
		指定した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**] **switchport port-security maximum** *number* [**vlan** *vlan-ID*] **Example:** `n1000v(config-if)# switchport port-security maximum 425`	現在のインターフェイスで学習可能な MAC アドレスまたはスタティックに設定可能な MAC アドレスの最大数を設定します。*number* の最大値は 4096 です。**no** オプションを使用すると、MAC アドレスの最大数がデフォルト値（1）にリセットされます。 最大数を適用する VLAN を指定する場合は、**vlan** キーワードを使用します。
ステップ 4	**show running-config port-security** **Example:** `n1000v(config-if)# show running-config port-security`	ポート セキュリティの設定を表示します。
ステップ 5	**copy running-config startup-config** **Example:** `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ます。

アドレス エージングのタイプと期間の設定

ダイナミック方式で学習された MAC アドレスがエージング期限に到達した時期を判断するために使用される MAC アドレス エージングのタイプと期間を設定するには、次の手順を実行します。

はじめる前に

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。

- EXEC モードで CLI にログインしていること。
- デフォルトのエージング タイムは 0 分（エージングはディセーブル）です。
- デフォルトのエージング タイプは絶対エージングです。
- ポート セキュリティが目的のインターフェイスでイネーブルになっていることを確認します。
  - 設定を確認する手順については、「ポート セキュリティの設定の確認」（P.11-19）を参照してください。
  - インターフェイスのポート セキュリティをイネーブルにする手順については、「レイヤ 2 インターフェイスに対するポート セキュリティのイネーブル化またはディセーブル化」（P.11-7）を参照してください。

手順の概要

1. **config t**
2. **interface** ***type*** *number*
3. **[no] switchport port-security aging type {absolute | inactivity}**
4. **[no] switchport port-security aging time** *minutes*
5. **show running-config port-security**
6. **copy running-config startup-config**

手順の詳細

	コマンド	目的
ステップ 1	**config t** **Example:** n1000v# config t n1000v(config)#	CLI 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** *type number* **Example:** n1000v(config)# interface vethernet 36 n1000v(config-if)#	指定した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] switchport port-security aging type {absolute | inactivity}** **Example:** n1000v(config-if)# switchport port-security aging type inactivity	ダイナミックに学習された MAC アドレスにデバイスが適用するエージング タイプを設定します。**no** オプションを使用すると、エージング タイプがデフォルト値（絶対エージング）にリセットされます。

	コマンド	目的
ステップ 4	[no] **switchport port-security aging time** *minutes* **Example:** n1000v(config-if)# switchport port-security aging time 120	ダイナミックに学習された MAC アドレスがドロップされるまでのエージング タイムを分単位で設定します。*minutes* の最大値は 1440 です。**no** オプションを使用すると、エージング タイムがデフォルト値である 0（エージングはディセーブル）にリセットされます。
ステップ 5	**show running-config port-security** **Example:** n1000v(config-if)# show running-config port-security	ポート セキュリティの設定を表示します。
ステップ 6	**copy running-config startup-config** **Example:** 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ます。

セキュリティ違反時の処理の設定

セキュリティ違反に対するインターフェイスの対応方法を設定するには、次の手順を実行します。

はじめる前に

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。

- EXEC モードで CLI にログインしていること。
- デフォルトのセキュリティ処理では、セキュリティ違反が発生したポートがシャットダウンされます。
- セキュリティ違反に対する次のインターフェイスの応答を設定できます。
  - protect：十分な数のセキュア MAC アドレスを削除して MAC アドレス数が最大値を下回るまで、送信元アドレスが不明なパケットをドロップします。
  - restrict：十分な数のセキュア MAC アドレスを削除して MAC アドレス数が最大値を下回るまで、送信元アドレスが不明なパケットをドロップし、SecurityViolation カウンタを増分させます。
  - shutdown：（デフォルト）即時にインターフェイスを errdisable ステートにして、SNMP トラップ通知を送信します。

  詳細については、「セキュリティ違反と処理」（P.11-4）を参照してください。
- ポート セキュリティが目的のインターフェイスでイネーブルになっていることを確認します。
  - 設定を確認する手順については、「ポート セキュリティの設定の確認」（P.11-19）を参照してください。
  - インターフェイスのポート セキュリティをイネーブルにする手順については、「レイヤ 2 インターフェイスに対するポート セキュリティのイネーブル化またはディセーブル化」（P.11-7）を参照してください。

手順の概要

1. **config t**
2. **interface** *type number*

3. [no] **switchport port-security violation** {**protect** | **restrict** | **shutdown**}
4. **show running-config port-security**
5. **copy running-config startup-config**

手順の詳細

	コマンド	目的
ステップ 1	**config t** **Example:** n1000v# config t n1000v(config)#	CLI 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** *type number* **Example:** n1000v(config)# interface vethernet 36 n1000v(config-if)#	指定した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**] **switchport port-security violation** {**protect** | **restrict** | **shutdown**} **Example:** n1000v(config-if)# switchport port-security violation protect	現在のインターフェイスのポート セキュリティにセキュリティ違反時の処理を設定します。**no** オプションを使用すると、違反時の処理がデフォルト値（インターフェイスのシャットダウン）にリセットされます。 • **protect**：十分な数のセキュア MAC アドレスを削除して MAC アドレス数が最大値を下回るまで、送信元アドレスが不明なパケットをドロップします。 • **restrict**：十分な数のセキュア MAC アドレスを削除して MAC アドレス数が最大値を下回るまで、送信元アドレスが不明なパケットをドロップし、SecurityViolation カウンタを増分させます。 • **shutdown**：（デフォルト）即時にインターフェイスを errdisable ステートにして、SNMP トラップ通知を送信します。
ステップ 4	**show running-config port-security** **Example:** n1000v(config-if)# show running-config port-security	ポート セキュリティの設定を表示します。
ステップ 5	**copy running-config startup-config** **Example:** 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ます。

ポート セキュリティ違反がディセーブルなポートの回復

ポート セキュリティ違反がディセーブルなインターフェイスを自動的に回復するには、次の手順を実行します。

はじめる前に

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。

- EXEC モードで CLI にログインしていること。
- インターフェイスを errdisable ステートから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。
- 詳細については、「セキュリティ違反と処理」（P.11-4）を参照してください。

手順の概要

1. **config t**
2. **interface** *type number*
3. **errdisable recovery cause psecure-violation**
4. **errdisable recovery interval** *seconds*
5. **show interface** *type* ***number***

手順の詳細

	コマンド	目的

ステップ 1	**config t**
	
	Example:
	`n1000v# config t`
	`n1000v(config)#`
		CLI 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** *type number*
	
	Example:
	`n1000v(config)# interface vethernet 36`
	`n1000v(config-if)#`
		指定した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	**errdisable recovery cause psecure-violation** **Example:** `n1000v(config-if)# errdisable recovery cause psecure-violation`	セキュリティ違反がディセーブルな特定のポートの期間指定された自動リカバリをイネーブルにします。
ステップ 4	**errdisable recovery interval** *seconds* **Example:** `n1000v(config-if)# errdisable recovery interval 30`	秒単位のタイマー リカバリ間隔を 30 ～ 65535 秒に設定します。
ステップ 5	**show interface** *type number* **Example:** `n1000v(config-if)# show running-config port-security`	確認のために theinterface ステートを表示します。

ポート セキュリティの設定の確認

ポート セキュリティ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 port-security	ポート セキュリティの設定を表示します。
show port-security	ポート セキュリティのステータスを表示します。

このコマンドの出力結果として表示される各フィールドの詳細については、『*Cisco Nexus 1000V Command Reference, Release 4.2(1)SV1(4a)*』を参照してください。

セキュア MAC アドレスの表示

セキュア MAC アドレスを表示するには、**show port-security address** コマンドを使用します。このコマンドの出力結果として表示される各フィールドの詳細については、『*Cisco Nexus 1000V Command Reference, Release 4.2(1)SV1(4a)*』を参照してください。

ポート セキュリティの設定例

次に、VLAN とインターフェイスのセキュア アドレス最大数が指定されている vEthernet 36 インターフェイスのポート セキュリティ設定の例を示します。この例のインターフェイスはトランク ポートです。違反時の処理は Protect（保護）に設定されています。

```
interface vethernet 36
switchport port-security
  switchport port-security maximum 10
  switchport port-security maximum 7 vlan 10
  switchport port-security maximum 3 vlan 20
  switchport port-security violation protect
```

その他の関連資料

ポート セキュリティの実装に関する詳細情報については、次を参照してください。

- 「関連資料」（P.11-20）
- 「標準」（P.11-20）

関連資料

関連項目	参照先
レイヤ 2 スイッチング	*『Cisco Nexus 1000V Layer 2 Switching Configuration Guide, Release 4.2(1)SV1(4)』*
ポート セキュリティ 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 1000V Command Reference, Release 4.2(1)SV1(4a)』*

標準

標準	タイトル
この機能でサポートされる新規の標準または変更された標準はありません。また、既存の標準のサポートは変更されていません。	—

ポート セキュリティの機能の履歴

ここでは、ポート セキュリティ機能のリリース履歴を示します。

機能名	リリース	機能情報
ポート セキュリティ	4.0(4)SV1(1)	この機能が導入されました。

CHAPTER 12

DHCP スヌーピングの設定

この章では、Dynamic Host Configuration Protocol（DHCP）スヌーピングを設定する方法について説明します。次の項で構成されています。

DHCP スヌーピングの概要

ここでは、次の内容について説明します。

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、管理します。このデータベースには、リース IP アドレスがある信頼できないホストに関する情報が保存されています。
- 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。

Dynamic ARP Inspection（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「Dynamic ARP Inspection 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 ごとにグローバルにイネーブルになっています。デフォルトでは、すべての VLAN で DHCP スヌーピングは非アクティブです。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。

信頼できるソースおよび信頼できないソース

DHCP スヌーピングでは、ポートを「信頼できる」または「信頼できない」として識別します。DHCP スヌーピングをイネーブルにすると、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 ウォールを越え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 プロバイダーの環境では、サービス プロバイダー ネットワークにないデバイスは、信頼できない送信元です（カスタマー 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、接続インターフェイスの信頼状態を設定することにより送信元が信頼されることを示します。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。ホスト ポート インターフェイスは、通常、信頼できるインターフェイスとしては設定しません。

（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。DHCP スヌーピングがイネーブルにされた VLAN に、ホストが関連付けられている場合、データベースには、リース IP アドレスがある信頼できない各ホストのエントリが保存されています。データベースには、信頼できるインターフェイスを介して接続するホストに関するエントリは保存されません。

（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 データベースに保存されている各エントリには、ホストの MAC アドレス、リース IP アドレス、リース期間、バインディング タイプ、VLAN 番号、およびホストに関連するインターフェイス情報が保存されます。

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。

リレー エージェント情報オプション

DHCP パケットに VSM MAC アドレスおよび vEthernet ポートを追加するように DHCP を設定できます。これは、DHCP リレー エージェント情報オプションまたはオプション 82 と呼ばれ、DHCP パケットの転送時に DHCP リレー エージェントによって挿入されます。サーバ管理者は、この情報を使用して、IP アドレスの割り当てポリシーを実装できます。

リレー エージェントでは、次が識別されます。

情報オプション	説明
回線 ID	vEthernet ポート名
リモート ID	VSM MAC アドレス

リレー エージェント情報オプションの詳細については、「*RFC-3046, DHCP Relay Agent Information Option*」を参照してください。

リレー エージェントを設定するには、「DHCP のスイッチおよび回線情報のリレー」（P.12-15）の手順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。これらのポートを「信頼できない」と設定しても、そ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。
- Cisco Nexus 1000V からのデバイス アップストリームの接続インターフェイスは、このデバイスで DHCP スヌーピングがイネーブルになっている場合、「信頼できる」として設定する必要があります。
- 128 を超える ACL（MAC と IP ACL の組み合わせ）を設定する場合は、VSM RAM が 3GB（3072 Mb）に設定されていることを確認します。RAM を 3GB に変更する手順は、「Setting the VSM RAM size to 3072 Mb」（ハイパーリンク）で説明されています。

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 パラメータのデフォルト値

パラメータ	デフォルト
DHCP 機能	ディセーブル
DHCP スヌーピング グローバル	ディセーブル
DHCP スヌーピング VLAN	ディセーブル
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 機能をイネーブルにします。詳細については、「DHCP 機能の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　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.12-6）を参照してください。

ステップ 3　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.12-7）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 4　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.12-9）を参照してください。

DHCP 機能のイネーブル化またはディセーブル化

DHCP 機能をグローバルにイネーブルまたはディセーブルにするには、次の手順を実行します。

はじめる前に

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。

- EXEC モードで CLI にログインしていること。
- デフォルトでは、DHCP はディセーブルです。

手順の概要

1. **config t**
2. **feature dhcp**
3. **show feature**
4. **copy running-config startup-config**

手順の詳細

	コマンド	目的
ステップ 1	**config t** **Example:** 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	**feature dhcp** **Example:** n1000v(config)# feature dhcp **Example:** n1000v(config)# no feature dhcp	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 feature** **Example:** n1000v(config)# show feature Feature Name Instance State -------------------- -------- -------- dhcp-snooping 1 enabled http-server 1 enabled lacp 1 enabled netflow 1 disabled port-profile-roles 1 enabled private-vlan 1 disabled sshServer 1 enabled tacacs 1 enabled telnetServer 1 enabled n1000v(config)#	使用可能な各機能の状態（イネーブルまたはディセーブル）を示します。
ステップ 4	**copy running-config startup-config** **Example:** n1000v(config)# copy running-config startup-config	（任意）リブート後に永続的な実行コンフィギュレーションを保存し、スタートアップ コンフィギュレーションにコピーして再起動します。

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。

はじめる前に

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。

- 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** **Example:** 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** **Example:** 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** **Example:** 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** **Example:** n1000v(config)# copy running-config startup-config	（任意）リブート後に永続的な実行コンフィギュレーションを保存し、スタートアップ コンフィギュレーションにコピーして再起動します。

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。

はじめる前に

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。

- EXEC モードで CLI にログインしていること。
- 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** **Example:** 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* **Example:** 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** **Example:** 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** **Example:** n1000v(config)# copy running-config startup-config	（任意）リブート後に永続的な実行コンフィギュレーションを保存し、スタートアップ コンフィギュレーションにコピーして再起動します。

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。

はじめる前に

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。

- EXEC モードで CLI にログインしていること。
- 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** **Example:** 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** **Example:** 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** **Example:** 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** **Example:** n1000v(config)# copy running-config startup-config	（任意）リブート後に永続的な実行コンフィギュレーションを保存し、スタートアップ コンフィギュレーションにコピーして再起動します。

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

はじめる前に

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。

- EXEC モードで CLI にログインしていること。
- 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てください。
- 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。これらのポートを「信頼できない」と設定しても、そ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** **Example:** 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* **Example:** 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* **Example:** 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** **Example:** 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** **Example:** 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** **Example:** n1000v(config-if)# copy running-config startup-config	（任意）リブート後に永続的な実行コンフィギュレーションを保存し、スタートアップ コンフィギュレーションにコピーして再起動します。

DHCP パケットのレート制限の設定

各ポートで受信する DHCP パケット/秒のレートの制限を設定するには、次の手順を実行します。

はじめる前に

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。

- EXEC モードで CLI にログインしていること。
- ポートは、この手順で設定した DHCP パケット/秒のレートの制限を超えると、errdisabled 状態になります。
- インターフェイスまたはポート プロファイルにレート制限を設定できます。

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** **Example:** 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* **Example:** 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 パケット/秒の制限を設定する vEthernet インターフェイスです。
	port-profile *profilename* **Example:** 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* **Example:** n1000v(config-port-prof)# ip dhcp snooping limit rate 30	DHCP パケット/秒（1 ～ 2048）のレートに制限を設定します。**no** オプションはレート制限を削除します。
ステップ 4	**show running-config dhcp** **Example:** 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** **Example:** n1000v(config-if)# copy running-config startup-config	（任意）リブート後に永続的な実行コンフィギュレーションを保存し、スタートアップ コンフィギュレーションにコピーして再起動します。

DHCP レート制限違反がディセーブルなポートの検出

DHCP レート制限の超過がディセーブルになっているポートの検出をグローバルに設定するには、次の手順を実行します。

はじめる前に

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。

- EXEC モードで CLI にログインしていること。
- 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。
- **shutdown** コマンドを入力し、**no shutdown** コマンドを入力して errdisable ステートから手動でインターフェイスを回復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** **Example:** 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** **Example:** n1000v(config)# errdisable detect cause dhcp-rate-limit	DHCP errdisable 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 errdisable 検出がディセーブルになります。
ステップ 3	**show running-config dhcp** **Example:** 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** **Example:** n1000v(config)# copy running-config startup-config	（任意）リブート後に永続的な実行コンフィギュレーションを保存し、スタートアップ コンフィギュレーションにコピーして再起動します。

DHCP レート制限違反がディセーブルなポートの回復

DHCP レート制限の違反がディセーブルになっているポートの自動リカバリをグローバルに設定するには、次の手順を実行します。

はじめる前に

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。

- EXEC モードで CLI にログインしていること。
- レートによって errdisable ステートになるポート。
- **shutdown** コマンドを入力し、**no shutdown** コマンドを入力して errdisable ステートから手動でインターフェイスを回復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**
	
	Example:
	`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** **Example:** `n1000v(config)# errdisable detect cause dhcp-rate-limit`	DHCP errdisable 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 errdisable 回復がディセーブルになります。
ステップ 3	**errdisable recovery interval** *timer-interval* **Example:** `n1000v(config)# errdisable recovery interval 30`	DHCP errdisable 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** **Example:** `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** **Example:** `n1000v(config)# copy running-config startup-config`	（任意）リブート後に永続的な実行コンフィギュレーションを保存し、スタートアップ コンフィギュレーションにコピーして再起動します。

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、次の手順について説明します。

- 「すべてのバインディング エントリの消去」（P.12-13）
- 「インターフェイスのバインディング エントリの消去」（P.12-14）

すべてのバインディング エントリの消去

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。

はじめる前に

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。

- EXEC モードで CLI にログインしていること。

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** **Example:** `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** **Example:** `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。

インターフェイスのバインディング エントリの消去

DHCP スヌーピング データベースからインターフェイスのバインディング エントリを削除するには、次の手順を実行します。

はじめる前に

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。

- EXEC モードで CLI にログインしていること。
- インターフェイスに関する次の情報があること。
  - VLAN ID
  - IP アドレス
  - MAC アドレス

手順の概要

1. **clear ip dhcp snooping binding** [{**vlan** *vlan-id* **mac** *mac-addr* **ip** *ip-addr* **interface** *interface-id*} | **vlan** *vlan-id1* | **interface** *interface-id1*]
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** [{**vlan** *vlan-id* **mac** *mac-addr* **ip** *ip-addr* **interface** *interface-id*} | **vlan** *vlan-id1* | **interface** *interface-id1*] **Example:** n1000v# clear ip dhcp snooping binding vlan 10 mac EEEE.EEEE.EEEE ip 10.10.10.1 interface vethernet 1	DHCP スヌーピング バインディング データベースから、動的に追加されたインターフェイスのエントリを消去します。
ステップ 2	**show ip dhcp snooping binding** **Example:** 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 のスイッチおよび回線情報のリレー

DHCP パケットの VSM MAC アドレスおよび vEthernet ポート情報のリレーをグローバルに設定するには、次の手順を実行します。これは、オプション 82 およびリレー エージェント情報オプションとも呼ばれます。

はじめる前に

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。

- EXEC モードで CLI にログインしていること。
- 詳細については、次の説明を参照してください。
  - 「リレー エージェント情報オプション」（P.12-3）
  - *RFC-3046『DHCP Relay Agent Information Option』*

手順の概要

1. **config t**
2. **[no] ip dhcp snooping information option**
3. **show runing-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** **Example:** 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。

	コマンド	目的

ステップ 2	**[no] ip dhcp snooping information option**
	
	Example:
	`n1000v(config)# ip dhcp snooping information option`
	`n1000v(config)#`
		DHCP パケットの VSM MAC アドレスおよび vEthernet ポート情報をリレーするよう DHCP を設定します。
		この設定を削除するには、**no** オプションを使用します。

ステップ 3	**show running-config dhcp**
	
	Example:
	`n1000v(config)# show running-config dhcp`
	
	`!Command: show running-config dhcp`
	`!Time: Fri Dec 17 11:30:22 2010`
	
	`version 4.2(1)SV1(4)`
	`ip dhcp snooping information option`
	`service dhcp`
	`ip dhcp relay`
	`ip dhcp relay information option`
	
	`n1000v(config)#`
		（任意）確認のために DHCP スヌーピング設定を表示します。

ステップ 4	**copy running-config startup-config** **Example:** `n1000v(config)# copy running-config startup-config`	（任意）リブート後に永続的な実行コンフィギュレーションを保存し、スタートアップ コンフィギュレーションにコピーして再起動します。

DHCP スヌーピング設定の確認

DHCP スヌーピング設定を確認するには、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。
show ip dhcp snooping binding	DHCP スヌーピング バインディング テーブルの内容を表示します。
show feature	DHCP などの使用可能な機能と、それらがイネーブルかどうかを表示します。

これらのコマンドの詳細については、『*Cisco Nexus 1000V Command Reference, Release 4.2(1)SV1(4a)*』を参照してください。

DHCP スヌーピングのモニタリング

DHCP スヌーピングの統計情報をモニタするには、**show ip dhcp snooping statistics** コマンドを使用します。このコマンドの詳細については、『*Cisco Nexus 1000V Command Reference, Release 4.2(1)SV1(4a)*』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。

```
feature dhcp

interface vethernet 5
ip dhcp snooping trust
ip dhcp snooping vlan 1, 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.12-17）
- 「標準」（P.12-17）

関連資料

関連項目	参照先
IPSG	『*Cisco Nexus 1000V Security Configuration Guide, Release 4.2(1)SV1(4a)*』、第 14 章「IP ソース ガードの設定」
Dynamic ARP Inspection（DAI; ダイナミック ARP インスペクション）	『*Cisco Nexus 1000V Security Configuration Guide, Release 4.2(1)SV1(4a)*』、第 13 章「Dynamic ARP Inspection の設定」
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 1000V Command Reference, Release 4.2(1)SV1(4a)*』

標準

標準	タイトル
RFC-2131	『*Dynamic Host Configuration Protocol*』 （http://tools.ietf.org/html/rfc2131）
RFC-3046	『*DHCP Relay Agent Information Option*』 （http://tools.ietf.org/html/rfc3046）

DHCP スヌーピングの機能の履歴

表 12-2 は、この機能のリリースの履歴です。

表 12-2　DHCP スヌーピングの機能の履歴

機能名	リリース	機能情報
リレー エージェント（オプション 82）	4.2(1)SV1(4)	DHCP パケットの VSM MAC およびポート情報のリレーを設定できます。
feature dhcp コマンド	4.2(1)SV1(4)	DHCP 機能をグローバルにイネーブルにするコマンドが追加されました。
DHCP スヌーピング	4.0(4)SV1(2)	この機能が導入されました。

CHAPTER 13

Dynamic ARP Inspection の設定

この章では、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）の設定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。

DAI の概要

ここでは、次の内容について説明します。

ARP について

ARP では、IP アドレスを MAC 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して、ホスト B の ARP キャッシュにホスト A の MAC アドレスがないという場合、ARP の用語では、ホスト B が送信者、ホスト A はターゲットになります。

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について

ARP スプーフィング攻撃とは、要求されていない ARP 応答を送りつけてホストのキャッシュを更新するというものです。それ以降は、攻撃者が検出されて ARP キャッシュ内の情報が修正されない限り、トラフィックは攻撃者を介して転送されます。

ARP スプーフィング攻撃を受けると、レイヤ 2 ネットワークに接続されたホスト、スイッチ、およびルータの ARP キャッシュに偽りの情報が送信されるので、これらの機器に影響が及ぶ可能性があります。図 13-1 に、ARP キャッシュ ポイズニングの例を示します。

図 13-1　ARP キャッシュ ポイズニング

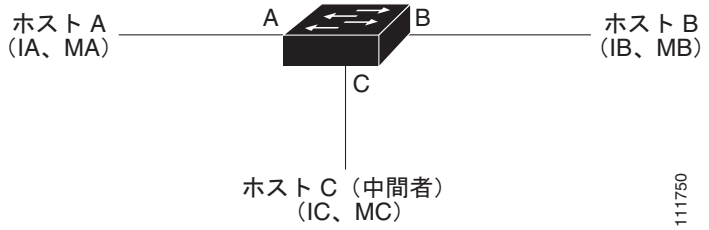


図 13-1 では、ホスト A、B、C はインターフェイス A、B、C を介してデバイスに接続されており、これらのインターフェイスはすべて同じサブネット上にあります。カッコ内は、各ホストの IP アドレスと MAC アドレスを示します。たとえば、ホスト A は IP アドレス IA と MAC アドレス MA を使用します。

ホスト A がホスト B に IP データを送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 アドレスを求める ARP 要求をブロードキャストします。デバイスおよびホスト B がこの ARP 要求を受信すると、IP アドレス IA および MAC アドレス MA を持つホストを表すバインディングが、デバイスおよびホスト B の ARP キャッシュに追加されます。

ホスト B が応答すると、IP アドレス IB および MAC アドレス MB を持つホストを表すバインディングが、デバイスとホスト A の ARP キャッシュに追加されます。

ホスト C は、次の 2 つの ARP 応答を偽造してブロードキャストすれば、ホスト A とホスト B を欺く（スプーフィング）ことができます。

- IP アドレス IA と MAC アドレス MC を持つホストの応答
- IP アドレス IB と MAC アドレス MC を持つホストの応答

このような応答を受け取ると、ホスト B は、IA に送られるはずであったトラフィックの宛先 MAC アドレスとして MC を使用します。つまり、そのトラフィックはホスト C によって代行受信されます。同様に、ホスト A とデバイスは、IB に送られるはずのトラフィックの宛先 MAC アドレスとして MC を使用します。

ホスト C は IA および IB の本当の MAC アドレスを知っているので、代行受信したトラフィックを転送できます。

DAI と ARP スプーフィングについて

DAI は、ARP の要求と応答を検証するための機能です。具体的には、次のような処理を実行します。

- 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。
- ARP キャッシュの更新やパケットの転送を行う前に、そのパケットに対応する有効な IP-to-MAC バインディングが存在することを確認します。
- 無効な ARP パケットはドロップします。

DAI によって ARP パケットの有効性を判断するときの基準となる有効な IP-to-MAC バインディングは、Dynamic Host Configuration Protocol（DHCP）スヌーピング バインディング データベースに保存されています。このデータベースは、VLAN とデバイスに対して DHCP スヌーピングがイネーブルになっている場合に、DHCP スヌーピング機能によって構築されます。このデータベースには、管理者が作成したスタティック エントリが格納されていることもあります。

信頼できるインターフェイス上で受信された ARP パケットは、一切の検査なしで転送されます。信頼できないインターフェイス上では、デバイスは有効性を確認できたパケットだけを転送します。信頼できるインターフェイスの詳細については、「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」（P.13-3）を参照してください。

管理者は、ARP パケットの宛先 MAC アドレス、送信元 MAC アドレス、および IP アドレスの検証をイネーブルまたはディセーブルにすることができます。詳細については、「ARP パケットの検証」（P.13-14）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

DAI によって、インターフェイスは「信頼できる」と「信頼できない」に分類されます。

一般的なネットワークでは、インターフェイスは次のように設定されます。

- 信頼できない（Untrusted）：ホストに接続されているインターフェイス

  パケットは DAI によって検証されます。
- 信頼できる（Trusted）：デバイスに接続されているインターフェイス

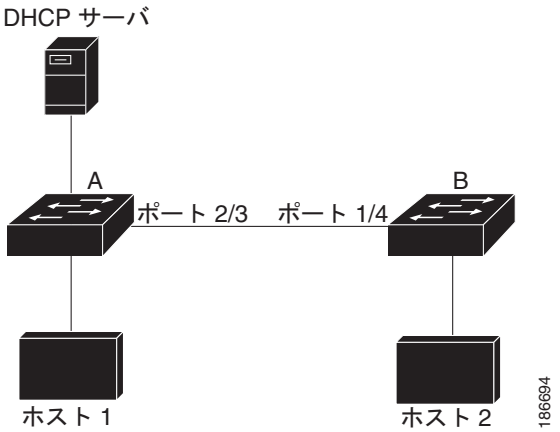
  パケットは、DAI による検証をすべてバイパスします。

この設定では、デバイスからネットワークに送信される ARP パケットはすべて、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。信頼できるインターフェイスの設定方法については、「信頼できる vEthernet インターフェイスの設定」（P.13-7）を参照してください。

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 13-2 では、デバイス A とデバイス B の両方が VLAN に対して DAI を実行しているとします。この VLAN には、ホスト 1 とホスト 2 が含まれています。ホスト 1 およびホスト 2 が、デバイス 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、デバイス A だけがホスト 1 の IP/MAC アドレスをバインドします。デバイス A とデバイス 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 パケットはデバイス B ではドロップされ、ホスト 1 およびホスト 2 の間の接続は切断されます。

図 13-2　DAI をイネーブルにした VLAN での ARP パケット検証



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、ネットワークにセキュリティ ホールが生じる可能性があります。デバイス A が DAI を実行していなければ、ホスト 1 はデバイス B の ARP キャッシュを簡単にポイズニングできます（デバイス間のリンクが信頼できるものとして設定されている場合はホスト 2 も同様）。この状況は、デバイス B が DAI を実行している場合でも起こりえます。

DAI は、DAI が稼動するデバイスに接続されているホスト（信頼できないインターフェイス上）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。ただし、DAI が稼動するデバイスに接続されているホストのキャッシュがネットワークの他の部分のホストによってポイズニングされるのを防ぐことはできません。

（注）　ネットワークの設定によっては、VLAN 内の一部のデバイスで ARP パケットを検証できない場合もあります。

DAI の前提条件

DAI を設定するための前提条件を次に示します。

- 次の機能を理解している。
  - ARP

    詳細については、IETF 標準 RFC-826『*An Ethernet Address Resolution Protocol*』（http://tools.ietf.org/html/rfc826）を参照してください。
  - DHCP スヌーピング

    詳細については、「DHCP スヌーピングの設定」（P.12-1）を参照してください。
- Cisco Nexus 1000V 上で稼動しているソフトウェアが DAI をサポートしている。
- VEM 機能レベルが、DAI をサポートするリリースに更新されている。

  VEM 機能レベルの設定方法については、『*Cisco Nexus 1000V Software Upgrade Guide, Release 4.2(1)SV1(4b)*』を参照してください。

注意事項および制約事項

DAI に関する注意事項と制約事項は次のとおりです。

- 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。
- ホストが接続されているデバイスが DAI をサポートしていない場合や、そのデバイスで DAI がイネーブルになっていない場合は、DAI の効果はありません。1 つのレイヤ 2 ブロードキャスト ドメインだけを標的とする攻撃を防ぐには、DAI が有効なドメインと、そうではないドメインとを分離させてください。これにより、DAI が有効な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 によって、着信 ARP 要求および ARP 応答内の IP-to-MAC アドレス バインディングが検証されます。スタティック エントリが設定されていない場合は、DAI が設定されている VLAN に対して DHCP スヌーピングもイネーブルにする必要があります。詳細については、「DHCP スヌーピングの設定」（P.12-4）を参照してください。
- DAI がサポートされるのは、vEthernet インターフェイスとプライベート VLAN ポートです。
- DAI が ARP パケットの有効性を判断するためにダイナミック IP-MAC アドレス バインディングを使用するように設定する場合は、DHCP スヌーピングが設定されていることを確認します。詳細については、「DHCP スヌーピングの設定」（P.12-4）を参照してください。
- 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 VSD ポートを「信頼できない」と設定しても、DAI では信頼できるポートとして扱われます。

デフォルト設定

表 13-1 に、DAI のデフォルトを示します。

表 13-1　デフォルトの DAI 設定

パラメータ	デフォルト
VLAN	VLAN は DAI の対象としては設定されません。
VSD 内ではない vEthernet インターフェイスの信頼状態	信頼できない
VSD 内の vEthernet インターフェイスの信頼状態	信頼できる
イーサネット ポート チャネルの信頼状態	信頼できる
信頼できないインターフェイスに対する着信 ARP パケット レート制限	15 パケット / 秒（pps）
信頼できるインターフェイスに対する着信 ARP パケット レート制限	無制限
レート制限バースト間隔	1 秒
DAI errdisable ステート インターフェイスの検出と回復	errdisable ステートの検出と回復は設定されません。
有効性検査	検査は実行されません。
VLAN 統計情報	ARP 要求および応答の統計情報

DAI の設定

ここでは、次の内容について説明します。

DAI 対象の VLAN の設定

ここでは、1 つまたは複数の VLAN を DAI 対象として設定する手順を説明します。

はじめる前に

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。

- EXEC モードで CLI にログインしていること。
- デフォルトでは、VLAN は DAI の対象としては設定されません。
- DHCP スヌーピングがイネーブルになっている必要があります。詳細については、「DHCP 機能の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。
- どの VLAN を DAI の対象として設定するかがわかっており、その VLAN が作成済みであることが必要です。

手順の概要

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

手順の詳細

	コマンド	目的

ステップ 1	**config t**
	
	Example:
	`switch# config t`
	`switch(config)#`
		CLI 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 vlan** *list* **Example:** `switch(config)# ip arp inspection vlan 13`	指定した 1 つ以上の VLAN を DAI の対象として設定します。

	コマンド	目的
ステップ 3	**show ip arp inspection vlan** *list* **Example:** `switch(config)# show ip arp inspection vlan 13`	（任意）指定した一連の VLAN の DAI ステータスを表示します。
ステップ 4	**copy running-config startup-config** **Example:** `switch(config-if)# copy running-config startup-config`	（任意）リブート後に永続的な実行コンフィギュレーションを保存し、スタートアップ コンフィギュレーションにコピーして再起動します。

信頼できる vEthernet インターフェイスの設定

ここでは、信頼できる vEthernet インターフェイスを設定する手順を説明します。

はじめる前に

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。

- EXEC モードで CLI にログインしていること。
- デフォルトでは、vEthernet インターフェイスの状態は「信頼できない」です（VSD に属している場合を除く）。
- インターフェイスが信頼できない状態である場合は、すべての ARP 要求および応答の検証が行われ、IP-MAC アドレス バインディングが有効な場合にのみ、ローカル キャッシュが更新されてパケットが転送されます。パケットの IP-MAC アドレス バインディングが無効な場合は、パケットがドロップされます。
- 信頼できるインターフェイスで受信された ARP パケットは、転送されますが、検証は行われません。
- 信頼できるインターフェイスの設定は、次のどちらでも行うことができます。
  - インターフェイス自体
  - インターフェイスが割り当てられている既存のポート プロファイル

    信頼できるインターフェイスの設定をポート プロファイルで行う場合は、ポート プロファイルが作成済みで名前がわかっていることが必要です。

手順の概要

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

   port-profile *profilename*
3. [**no**] **ip arp inspection trust**
4. **show ip arp inspection interface** *type slot*/*number*

   show port-profile *profilename*
5. **copy running-config startup-config**

手順の詳細

	コマンド	目的

ステップ 1	**config t**
	Example:
	`switch# config t`
	`switch(config)#`
		CLI 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*
	Example:
	`switch(config)# interface vethernet 3`
	`switch(config-if)#`
		指定した vEthernet インターフェイスの CLI 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。

	port-profile *profilename*
	Example:
	`switch(config)# port-profile vm-data`
	`switch(config-port-prof)#`
		指定したポート プロファイルの CLI 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。

ステップ 3	**ip arp inspection trust** **Example:** `switch(config-if)# ip arp inspection trust`	インターフェイスを、信頼できる ARP インターフェイスとして設定します。
	ip arp inspection trust **Example:** `switch(config-port-prof)# ip arp inspection trust`	このポート プロファイルに割り当てられるインターフェイスを、信頼できる ARP インターフェイスとして設定します。
ステップ 4	**show ip arp inspection interface vethernet** *interface-number* **Example:** `switch(config-if)# show ip arp inspection interface vethernet 2`	（任意）特定のインターフェイスの信頼状態および ARP パケット レートを表示します。
	show port-profile *profilename* **Example:** `switch(config)# show port-profile vm-data`	（任意）ポート プロファイル設定を表示します。ARP 信頼状態も表示されます。
ステップ 5	**copy running-config startup-config** **Example:** `switch(config-if)# copy running-config startup-config`	（任意）リブート後に永続的な実行コンフィギュレーションを保存し、スタートアップ コンフィギュレーションにコピーして再起動します。

vEthernet インターフェイスの信頼できないインターフェイスへのリセット

vEthernet インターフェイスから信頼できるという指定を削除し、デフォルトの信頼できないという指定に戻すには、次の手順を実行します。

はじめる前に

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。

- EXEC モードで CLI にログインしていること。
- デフォルトでは、vEthernet インターフェイスの状態は「信頼できない」です（VSD に属している場合を除く）。

- インターフェイスが信頼できない状態である場合は、すべての ARP 要求および応答の検証が行われ、IP-MAC アドレス バインディングが有効な場合にのみ、ローカル キャッシュが更新されてパケットが転送されます。パケットの IP-MAC アドレス バインディングが無効な場合は、パケットがドロップされます。

手順の概要

1. **config t**
2. **interface vethernet** *interface-number*
3. **default ip arp inspection trust**
4. **show ip arp inspection interface** *type slot/number*
5. **copy running-config startup-config**

手順の詳細

	コマンド	目的

ステップ 1	**config t**
	Example:
	`switch# config t`
	`switch(config)#`
		CLI 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*
	Example:
	`switch(config)# interface vethernet 3`
	`switch(config-if)#`
		指定した vEthernet インターフェイスの CLI 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	**default ip arp inspection trust** **Example:** `switch(config-if)# default ip arp inspection trust`	インターフェイスから信頼できるという指定を削除し、デフォルトの信頼できない状態に戻します。
ステップ 4	**show ip arp inspection interface vethernet** *interface-number* **Example:** `switch(config-if)# show ip arp inspection interface vethernet 3`	（任意）特定のインターフェイスの信頼状態および ARP パケット レートを表示します。
ステップ 5	**copy running-config startup-config** **Example:** `switch(config-if)# copy running-config startup-config`	（任意）リブート後に永続的な実行コンフィギュレーションを保存し、スタートアップ コンフィギュレーションにコピーして再起動します。

DAI レート制限の設定

ここでは、ARP 要求と応答のレート制限を設定する手順を説明します。

はじめる前に

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。

- EXEC モードで CLI にログインしていること。
- トランク ポートでは集約が行われるので、トランク ポートのレート上限は高く設定してください。

- 着信パケットのレートが設定レートを超えると、インターフェイスは自動的に errdisable 状態になります。
- デフォルトの DAI レート制限は次のとおりです。
  - 信頼できないインターフェイス = 15 パケット / 秒
  - 信頼できるインターフェイス = 無制限
  - バースト間隔 = 1 秒
- インターフェイスのレート制限は、次のどちらでも行うことができます。
  - インターフェイス自体
  - インターフェイスが割り当てられている既存のポート プロファイル

    ポート プロファイルを設定する場合は、ポート プロファイルが作成済みで名前がわかっていることが必要です。

手順の概要

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

   port-profile *profilename*
3. **ip arp inspection limit** {**rate** *pps* [**burst interval** *bint*] | **none**}
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**
	Example:
	`switch# config t`
	`switch(config)#`
		CLI 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*
	Example:
	`switch(config)# interface vethernet 3`
	`switch(config-if)#`
		指定した vEthernet インターフェイスの CLI 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。

	port-profile *profilename*
	Example:
	`switch(config)# port-profile vm-data`
	`switch(config-port-prof)#`
		指定したポート プロファイルの CLI 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。

	コマンド	目的

ステップ 3	**ip arp inspection limit** {**rate** *pps* [**burst interval** *bint*] | **none**}
	Example:
	`switch(config-if)# ip arp inspection limit rate 30`
	Example:
	`switch(config-port-prof)# ip arp inspection limit rate 30`
		インターフェイスまたはポート プロファイルでの ARP インスペクションの制限値を、次のとおりに設定します。
		• **rate**：指定できる値は 1 ～ 2048 パケット / 秒（pps）
		– 信頼できないインターフェイスのデフォルト = 15 パケット / 秒
		– 信頼できるインターフェイスのデフォルト = 無制限
		• **burst interval**：指定できる値は 1 ～ 15 秒（デフォルト = 1 秒）
		• **none**：パケット / 秒の制限なし

ステップ 4	**show running-config dhcp** **Example:** `switch(config)# show running-config dhcp`	（任意）DHCP スヌーピング設定を表示します。DAI の設定も表示されます。
ステップ 5	**copy running-config startup-config** **Example:** `switch(config)# copy running-config startup-config`	（任意）リブート後に永続的な実行コンフィギュレーションを保存し、スタートアップ コンフィギュレーションにコピーして再起動します。

DAI レート制限のデフォルト値へのリセット

ARP 要求および応答のレート制限をデフォルトに設定することで、設定されている値を解除するには、次の手順を実行します。

はじめる前に

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。

- EXEC モードで CLI にログインしていること。
- デフォルトの DAI レート制限は次のとおりです。
  - 信頼できないインターフェイス = 15 パケット / 秒
  - 信頼できるインターフェイス = 無制限
  - バースト間隔 = 1 秒
- インターフェイスのレート制限は、次のどちらでも行うことができます。
  - インターフェイス自体
  - インターフェイスが割り当てられている既存のポート プロファイル

    ポート プロファイルを設定する場合は、ポート プロファイルが作成済みで名前がわかっていることが必要です。

手順の概要

1. **config t**
2. **interface vethernet** *interface-number*
3. **default ip arp inspection limit** {**rate** *pps* [**burst interval** *bint*] | **none**}
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**
	Example:
	`switch# config t`
	`switch(config)#`
		CLI 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*
	Example:
	`switch(config)# interface vethernet 3`
	`switch(config-if)#`
		指定した vEthernet インターフェイスの CLI 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	**default ip arp inspection limit** {**rate** *pps* [**burst interval** *bint*] | **none**} **Example:** `switch(config-if)# default ip arp inspection limit rate`	設定されている DAI レート制限をインターフェイスから削除し、デフォルト値に戻します。 • **rate**： – 信頼できないインターフェイスのデフォルト = 15 パケット / 秒 – 信頼できるインターフェイスのデフォルト = 無制限 • **burst interval :** デフォルト = 1 秒 • **none**：パケット / 秒の制限なし
ステップ 4	**show running-config dhcp** **Example:** `switch(config)# show running-config dhcp`	（任意）DAI レート制限を含む DHCP スヌーピング設定を表示します。
ステップ 5	**copy running-config startup-config** **Example:** `switch(config)# copy running-config startup-config`	（任意）リブート後に永続的な実行コンフィギュレーションを保存し、スタートアップ コンフィギュレーションにコピーして再起動します。

errdisable ステートのインターフェイスの検出と回復

ここでは、errdisable ステートのインターフェイスの検出と回復を設定する手順を説明します。

はじめる前に

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。

- EXEC モードで CLI にログインしていること。
- デフォルトでは、インターフェイスは DAI errdisable 回復を行うようには設定されません。
- インターフェイスを errdisable ステートから手動で回復するには、次の順でコマンドを実行します。

  1. **shutdown**
  2. **no shutdown**

手順の概要

1. **config t**
2. **[no] errdisable detect cause arp-inspection**
3. [**no**] **errdisable recovery cause arp-inspection**
4. **errdisable recovery interval** *timer-interval*
5. **show running-config | include errdisable**
6. **copy running-config startup-config**

手順の詳細

	コマンド	目的

ステップ 1	**config t**
	Example:
	`switch# config t`
	`switch(config)#`
		CLI 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	**errdisable detect cause arp-inspection** **Example:** `switch(config)# errdisable detect cause arp-inspection`	ARP インスペクションの結果 errdisable ステートとなったインターフェイスを検出するように設定します。 **no** オプションを使用すると、検出がディセーブルになります。
ステップ 3	**errdisable recovery cause arp-inspection** **Example:** `switch(config)# errdisable recovery cause arp-inspection`	ARP インスペクションの結果 errdisable ステートとなったインターフェイスを回復するように設定します。
ステップ 4	**errdisable recovery interval** *timer-interval* **Example:** `switch(config)# errdisable recovery interval 30`	ARP インスペクションの結果 errdisable となったインターフェイスの回復間隔を設定します。 **timer-interval**: 指定できる値は 30 ～ 65535 秒です。
ステップ 5	**show running-config | include errdisable** **Example:** `switch(config)# show running-config | include errdisable`	（任意）errdisable の設定を表示します。
ステップ 6	**copy running-config startup-config** **Example:** `switch(config-if)# copy running-config startup-config`	（任意）リブート後に永続的な実行コンフィギュレーションを保存し、スタートアップ コンフィギュレーションにコピーして再起動します。

ARP パケットの検証

ここでは、ARP パケットの検証を設定する手順を説明します。

はじめる前に

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。

- EXEC モードで CLI にログインしていること。
- 検証の対象は次のアドレスです。デフォルトでは、これらの検証はディセーブルになっています。
  - 宛先 MAC アドレス

    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、MAC アドレスが無効であるパケットをドロップします。
  - IP アドレス

    ARP 本体を検査し、無効な、および予期しない IP アドレス（0.0.0.0、255.255.255.255、IP マルチキャスト アドレスなど）を検出します。送信元 IP アドレスの検証は、ARP 要求と応答の両方で行われます。ターゲット IP アドレスは ARP 応答でだけチェックされます。

- 送信元 MAC アドレス

  ARP 要求および応答について、イーサネット ヘッダー内の送信元 MAC アドレスを ARP 本体の送信者 MAC アドレスと比較し、MAC アドレスが無効である場合はパケットをドロップします。

- 管理者が検証の設定を行うと、それまでの検証設定は上書きされます。

手順の概要

1. **config t**
2. **[no] ip arp inspection validate {[src-mac] [dst-mac] [ip]}**
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**
	Example:
	`switch# config t`
	`switch(config)#`
		CLI 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]}** **Example:** `switch(config)# ip arp inspection validate src-mac dst-mac ip`	指定した検証をイネーブルにします。以前保存された既存の検証設定がある場合は上書きします。 • 送信元 MAC • 宛先 MAC • IP この 3 つすべての検証を指定することもできますが、少なくとも 1 つを指定する必要があります。 検証をディセーブルにするには、no オプションを使用します。
ステップ 3	**show running-config dhcp** **Example:** `switch(config)# show running-config dhcp`	（任意）DHCP スヌーピング設定を表示します。DAI の設定も表示されます。
ステップ 4	**copy running-config startup-config** **Example:** `switch(config)# copy running-config startup-config`	（任意）リブート後に永続的な実行コンフィギュレーションを保存し、スタートアップ コンフィギュレーションにコピーして再起動します。

DAI の設定の確認

DAI の設定を表示して確認するには、次のコマンドを使用します。

コマンド	目的
show running-config dhcp	DAI の設定を表示します。
show ip arp inspection	DAI のステータスを表示します。
show ip arp inspection interface vethernet *interface-number*	特定のインターフェイスの信頼状態および ARP パケット レートを表示します。
show ip arp inspection vlan *vlan-ID*	特定の VLAN の DAI 設定を表示します。

コマンド出力の詳しい説明については、『*Cisco Nexus 1000V Command Reference, Release 4.2(1)SV1(4a)*』を参照してください。

DAI のモニタリング

DAI をモニタするには、次のコマンドを使用します。

コマンド	目的
show ip arp inspection statistics	DAI の統計情報を表示します。
show ip arp inspection statistics vlan	指定されている VLAN の DAI 統計情報を表示します。
clear ip arp inspection statistics	DAI 統計情報を消去します。

コマンド出力の詳しい説明については、『*Cisco Nexus 1000V Command Reference, Release 4.2(1)SV1(4a)*』を参照してください。

DAI の設定例

この例では、次の 2 つの VEM が存在するネットワークでの DAI を設定する方法を示します。

- 一方の VEM は、真正な Web サーバと DHCP サーバをホスティングしています。
- 他方の VEM は、クライアント仮想マシン（VM 1）と、不正な Web サーバが存在する仮想マシン（VM 2）をホスティングしています。VM 1 は、vEthernet インターフェイス 3 に接続されています。このインターフェイスはデフォルトで信頼できない状態となっており、VLAN 1 に属しています。VM 2 は、vEthernet 10 と VLAN 1 に接続されています。

DAI がイネーブルでないときは、VM 2 が VM 1 の ARP キャッシュに偽の情報を送る（スプーフィング）こともできてしまいます。その方法は、ARP 要求が生成されていないけれどもパケットを送信するというものです。このパケットを受け取った VM 1 は、自身のトラフィックを、真正な Web サーバではなく VM 2 の Web サーバに送信します。

DAI がイネーブルならば、VM 2 が VM 1 の ARP キャッシュをスプーフィングしようとして、要求されていないにもかかわらず送信した ARP パケットは、ドロップされます。その IP-to-MAC バインディングが不正であることが、DAI によって検出されるからです。ARP キャッシュをスプーフィングする試みは失敗に終わり、VM 1 は真正な Web サーバに接続されます。

（注）　DAI によって着信 ARP 要求および ARP 応答の IP-to-MAC アドレス バインディングを検証するには、DHCP スヌーピング データベースが必要です。IP アドレスを動的に割り当てられた 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。コンフィギュレーションについては、第 12 章「DHCP スヌーピングの設定」を参照してください。

この例の DAI を設定するには、次の手順を使用します。

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

```
n1000v# config t
n1000v(config)# ip arp inspection vlan 1
n1000v(config)# show ip arp inspection vlan 1

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

Vlan : 1
-----------
Configuration   : Enabled
Operation State : Active
n1000v(config)#
```

ステップ 2　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。

```
n1000v# show ip arp inspection statistics vlan 1

Vlan : 1
-----------
ARP Req Forwarded  = 0
ARP Res Forwarded  = 0
ARP Req Dropped    = 0
ARP Res Dropped    = 0
DHCP Drops         = 0
DHCP Permits       = 0
SMAC Fails-ARP Req = 0
SMAC Fails-ARP Res = 0
DMAC Fails-ARP Res = 0
IP Fails-ARP Req   = 0
IP Fails-ARP Res   = 0
n1000v#
```

VM 1 が 2 つの ARP 要求を送信し、この要求で指定された IP アドレスは 10.0.0.1、MAC アドレスは 0002.0002.0002 であるとします。要求が両方とも許可されたことは、次のコマンド出力で確認できます。

```
n1000v# show ip arp inspection statistics vlan 1

Vlan : 1
-----------
ARP Req Forwarded  = 2
ARP Res Forwarded  = 0
ARP Req Dropped    = 0
ARP Res Dropped    = 0
DHCP Drops         = 0
DHCP Permits       = 2
SMAC Fails-ARP Req = 0
SMAC Fails-ARP Res = 0
DMAC Fails-ARP Res = 0
IP Fails-ARP Req   = 0
```

```
IP Fails-ARP Res   = 0
```

VM 2 が IP アドレス 10.0.0.3 を指定して ARP 要求を送信しようとすると、このパケットはドロップされ、エラー メッセージがログに記録されます。

```
00:12:08: %SW_DAI-4-DHCP_SNOOPING_DENY: 2 Invalid ARPs (Req) on vEthernet3, vlan
1.([0002.0002.0002/10.0.0.3/0000.0000.0000/0.0.0.0/02:42:35 UTC Fri Jul 13 2008])
```

この場合に表示される統計情報は次のようになります。

```
n1000v# show ip arp inspection statistics vlan 1
n1000v#

Vlan : 1
-----------
ARP Req Forwarded  = 2
ARP Res Forwarded  = 0
ARP Req Dropped    = 2
ARP Res Dropped    = 0
DHCP Drops         = 2
DHCP Permits       = 2
SMAC Fails-ARP Req = 0
SMAC Fails-ARP Res = 0
DMAC Fails-ARP Res = 0
IP Fails-ARP Req   = 0
IP Fails-ARP Res   = 0
n1000v#
```

その他の関連資料

DAI 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.13-18）
- 「標準」（P.13-18）

関連資料

関連項目	参照先
DHCP スヌーピング	「DHCP スヌーピングの設定」（P.12-1）
DAI および DHCP のコマンド：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 4.2(1)SV1(4a)』*

標準

標準	タイトル
RFC-826	*『An Ethernet Address Resolution Protocol』*（http://tools.ietf.org/html/rfc826）

DAI の機能の履歴

表 13-2 に、DAI 機能のリリース履歴を示します。

表 13-2　DAI の機能の履歴

機能名	リリース	機能情報
DAI	4.0(4)SV1(2)	この機能が導入されました。

CHAPTER 14

IP ソース ガードの設定

この章では、Cisco Nexus 1000V 上で IP ソース ガードを設定する手順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 ガードとは、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、Dynamic Host Configuration Protocol（DHCP）スヌーピング バインディング テーブル内のダイナミックまたはスタティック IP ソース エントリの IP-MAC アドレス バインディングと一致する場合にのみ、IP トラフィックを許可します。

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 Nexus 1000V 内で設定済みのスタティック 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** コマンドによって表示されたバインディング テーブル エントリが次のとおりであるとします。

```
MacAddress          IpAddress     LeaseSec    Type         VLAN       Interface
------------------  ------------  ----------  -----------  ---------  ----------
00:02:B3:3F:3B:99   10.5.5.2        6943      dhcp-snooping  10       vEthernet3
```

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 ガードの前提条件

IP ソース ガードの前提条件は次のとおりです。

- IP ソース ガードを設定するためには、DHCP スヌーピングについての知識が必要です。
- DHCP スヌーピングがイネーブルになっている必要があります（「DHCP スヌーピングの設定」（P.12-4）を参照）。

注意事項および制約事項

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。DHCP スヌーピングの詳細については、第 12 章「DHCP スヌーピングの設定」を参照してください。
- 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。これらのポートを「信頼できない」と設定しても、その設定は無視されます。

デフォルト設定

表 14-1 に、IP ソース ガードのデフォルトを示します。

表 14-1　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

ここでは、次の内容について説明します。

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

ここでは、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する手順を説明します。

はじめる前に

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。

- 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。
- DHCP スヌーピングがイネーブルになっていることを確認してください。詳細については、「DHCP 機能の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。

手順の概要

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

   port-profile *profilename*
3. **[no] ip verify source dhcp-snooping-vlan**
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** **Example:** switch# config t 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 vethernet** *interface-number* **Example:** switch(config)# interface vethernet 3 switch(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* **Example:** switch(config)# port-profile vm-data switch(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。

	コマンド	目的
ステップ 3	[no] **ip verify source dhcp-snooping-vlan** **Example:** `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** **Example:** `switch(config-if)# show running-config dhcp`	（任意）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。IP ソース ガードの設定も表示されます。
ステップ 5	**copy running-config startup-config** **Example:** `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。

スタティック IP ソース エントリの追加または削除

ここでは、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の手順を説明します。

はじめる前に

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。

- 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。

手順の概要

1. **config t**
2. [**no**] **ip source binding** *IP-address MAC-address* **vlan** *vlan-ID* **interface vethernet** *interface-number*
3. **show ip dhcp snooping binding [interface vethernet** *interface-number*]
4. **copy running-config startup-config**

手順の詳細

	コマンド	目的
ステップ 1	**config t** **Example:** switch# config t 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 vethernet** *interface-number* **Example:** switch(config)# ip source binding 10.5.22.17 001f.28bd.0013 vlan 100 interface ethernet 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 vethernet** *interface-number*] **Example:** switch(config)# show ip dhcp snooping binding interface ethernet 3	（任意）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 IP ソース エントリも表示されます。スタティック エントリは、Type カラムに「static」と表示されます。
ステップ 4	**copy running-config startup-config** **Example:** 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。

IP ソース ガードの設定の確認

IP ソース ガードの設定情報を表示するには、次のいずれかのコマンドを使用します。

コマンド	目的
show running-config dhcp	IP ソース ガード設定を含む、DHCP スヌーピング設定を表示します。
show ip verify source	IP-MAC アドレス バインディングを表示します。

コマンド出力の詳しい説明については、『*Cisco Nexus 1000V Command Reference, Release 4.2(1)SV1(4a)*』を参照してください。

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 エントリを作成してから、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 vethernet 3
interface ethernet 2/3
  no shutdown
  ip verify source dhcp-snooping-vlan
```

その他の関連資料

IP ソース ガードの実装に関する詳細情報については、次を参照してください。

- 「関連資料」（P.14-6）
- 「標準」（P.14-6）

関連資料

関連項目	参照先
「DHCP スヌーピングの概要」（P.12-1）	『*Cisco Nexus 1000V Security Configuration Guide, Release 4.2(1)SV1(4a)*』、*第 12 章「DHCP スヌーピングの設定」*
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 1000V Command Reference, Release 4.2(1)SV1(4a)*』
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 1000V Command Reference, Release 4.2(1)SV1(4a)*』

標準

標準	タイトル
この機能でサポートされる新規の標準または変更された標準はありません。また、既存の標準のサポートは変更されていません。	—

IP ソース ガードの機能の履歴

表 14-2 は、この機能のリリースの履歴です。

表 14-2　IP ソース ガードの機能の履歴

機能名	リリース	機能情報
IPSG	4.0(4)SV1(2)	この機能が導入されました。

CHAPTER 15

HTTP サーバのディセーブル化

この章では、HTTP サーバをディセーブルにする方法について説明します。次の項目を取り上げます。

HTTP サーバについて

セキュリティ上の問題に対応するために CLI からオフにすることができる HTTP サーバは、仮想スーパーバイザ モジュール（VSM）に埋め込まれています。

HTTP サーバをオフにする場合は、次の「注意事項および制約事項」を参照してください。

注意事項および制約事項

- HTTP サーバは、デフォルトでイネーブルになっています。
- HTTP サーバがディセーブルの場合、VUM では VEM がインストールされません。VEM のインストール中に、VUM は HTTP サーバに直接通信して、VSM から必要なモジュール情報を取得します。VEM をインストールするには、次のいずれかを実行する必要があります。
  - VEM のインストール中に HTTP サーバをイネーブルにし、VEM のインストール後に HTTP サーバをディセーブルにすることによって、VUM を使用する。
  - VUM を使用せずに手動で VEM をインストールする。
- VSM から Cisco Nexus 1000V XML プラグインを取得するには、HTTP サーバをイネーブルにする必要があります。

デフォルト設定

HTTP サーバは、デフォルトでイネーブルになっています。

HTTP サーバのディセーブル化

HTTP サーバをディセーブルにするには、次の手順を実行します。

はじめる前に

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。

- EXEC モードで CLI にログインしていること。
- デフォルトでは、HTTP サーバはイネーブルになっています。

手順の概要

1. **config t**
2. **no feature http-server**
3. **show http-server**
4. **copy running-config startup-config**

手順の詳細

	コマンド	目的

ステップ 1	**config t**
	
	Example:
	`n1000v# config t`
	`n1000v(config)#`
		CLI 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 feature http-server**
	
	Example:
	`n1000v(config)# no feature http-server`
	`n1000v(config)#`
		HTTP サーバをディセーブルにします。

ステップ 3	**show http-server**
	
	Example:
	`n1000v(config)# show http-server`
	`http-server disabled`
		（任意）HTTP サーバの設定を表示します（イネーブルまたはディセーブル）。

ステップ 4	**copy running-config startup-config**
	
	Example:
	`n1000v(config)# copy running-config startup-config`
	`[########################################]`
	`100%`
	`n1000v(config)#`
		（任意）リブート後に永続的な実行コンフィギュレーションを保存し、スタートアップ コンフィギュレーションにコピーして再起動します。

Example:
```
config t
no feature http-server
```

HTTP 設定の確認

HTTP 設定を表示するには、次のコマンドを使用します。

コマンド	目的
show http-server	HTTP サーバの設定を表示します。 例 15-1 を参照してください。
show feature	LACP などの使用可能な機能と、それらがイネーブルかどうかを表示します。 例 15-2 を参照してください。

例 15-1　show http-server

```
n1000v(config)# show http-server
http-server enabled
n1000v(config)#
```

例 15-2　show feature

```
n1000v(config)# show feature
Feature Name          Instance  State
--------------------  --------  --------
dhcp-snooping         1         disabled
http-server           1         disabled
ippool                1         disabled
lacp                  1         disabled
netflow               1         disabled
private-vlan          1         disabled
sshServer             1         enabled
tacacs                1         disabled
telnetServer          1         disabled
n1000v(config)#
```

その他の関連資料

Telnet の実装に関連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.15-3）
- 「標準」（P.15-4）

関連資料

関連項目	参照先
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、使用上のガイドライン、例	*『Cisco Nexus 1000V Command Reference, Release 4.2(1)SV1(4a)』*

標準

標準	タイトル
この機能でサポートされる新規の標準または変更された標準はありません。また、既存の標準のサポートは変更されていません。	—

HTTP サーバのディセーブル化の機能の履歴

ここでは、HTTP サーバのディセーブル化のリリース履歴を示します。

機能名	リリース	機能情報
HTTP サーバのディセーブル化	4.2(1)SV1(4)	この機能が導入されました。

CHAPTER 16

不明なユニキャスト フラッディングのブロック

この章では、転送パスの不明なユニキャスト パケット フラッディング（UUFB）をブロックする方法について説明します。次の項で構成されています。

UUFB について

UUFB は、転送パスの不明なユニキャスト フラッディングを制限して、VM に到達する望ましくないトラフィックのセキュリティ リスクを防ぎます。UUFB は、vEthernet インターフェイスおよびイーサネット インターフェイスの両方で受信された不明なユニキャスト アドレス宛てのパケットによって、VLAN でフラッディングが発生しないようにします。UUFB が適用されると、VEM はアップリンク ポートに着信した不明なユニキャスト パケットをドロップします。

不明なユニキャスト パケットをグローバルにディセーブルにした後、ポート プロファイルの 1 つのインターフェイスまたはすべてのインターフェイスでのユニキャスト フラッディングを許可できます。

また、インターフェイスまたはポート プロファイルを設定して、不明なユニキャストがブロックされないようにすることもできます。

注意事項および制約事項

UUFB の設定に関する注意事項は次のとおりです。

- UUFB を設定する前に、**show module** コマンドを入力して、VSM の HA ペアとすべての VEM が Release 4.2(1)SV1(4b) にアップグレードされていることを確認します。

- 仮想サービス ドメイン（VSD）ポートに対して UUFB を明示的にディセーブルにする必要があります。これは VSD ポート プロファイルで行うことができます。詳細については、第 16 章「不明なユニキャスト フラッディングを許可するようにポート プロファイルを設定する」を参照してください。
- VMware によって提供される MAC アドレス以外の MAC アドレスを使用して、アプリケーションまたは VM のポートで UUFB を明示的にディセーブルにする必要があります。
- 「不明なユニキャスト フラッディングを許可するようにインターフェイスを設定する」（P.16-3）の手順に従って、不明なユニキャストがブロックされていないようにインターフェイスを設定できます。

デフォルト設定

次の表に、UUFB のデフォルト設定を示します。

パラメータ	デフォルト
uufb enable	ディセーブル
switchport uufb disable	ディセーブル

UUFB の設定

ここでは、次の手順について説明します。

- 「スイッチでの不明なユニキャスト フラッディングのグローバルなブロック」（P.16-2）
- 「不明なユニキャスト フラッディングを許可するようにインターフェイスを設定する」（P.16-3）
- 「不明なユニキャスト フラッディングを許可するようにポート プロファイルを設定する」（P.16-5）

スイッチでの不明なユニキャスト フラッディングのグローバルなブロック

スイッチの転送パスがフラッディングしないように不明なユニキャスト パケットをグローバルにブロックするには、次の手順を使用します。

はじめる前に

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。

- EXEC モードで CLI にログインしていること。

手順の概要

1. **config t**
2. **[no] uufb enable**
3. **show uufb status**
4. **copy running-config startup-config**

手順の詳細

	コマンド	目的
ステップ 1	**config t** **Example:** n1000v# config t n1000v(config)#	CLI 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] uufb enable** **Example:** n1000v(config)# uufb enable n1000v(config)#	VSM の UUFB をグローバルに設定します。
ステップ 3	**show uufb status** **Example:** n1000v(config)# show uufb status UUFB Status: Enabled n1000v(config)#	（任意）VSM の UUFB グローバル設定を表示します。
ステップ 4	**copy running-config startup-config** **Example:** n1000v(config)# copy running-config startup-config [##] 100% n1000v(config)#	（任意）リブート後に永続的な実行コンフィギュレーションを保存し、スタートアップ コンフィギュレーションにコピーして再起動します。

不明なユニキャスト フラッディングを許可するようにインターフェイスを設定する

VSM のフラッディングをグローバルにブロックした場合に、不明なユニキャスト パケットによって vEthernet インターフェイスがフラッディングするのを許可するには、次の手順を実行します。

はじめる前に

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。

- EXEC モードで CLI にログインしていること。
- グローバル設定に関係なく、不明なユニキャストが特定のインターフェイスでブロックされていないことを確認するには、次の手順を実行します。
- すでに不明なユニキャスト パケットをグローバルにディセーブルにしている場合は、ポート プロファイルの 1 つのインターフェイスまたはすべてのインターフェイスでのユニキャスト フラッディングを許可できます。

  ポート プロファイルのすべてのインターフェイスでユニキャスト フラッディングを許可するには、「不明なユニキャスト フラッディングを許可するようにポート プロファイルを設定する」（P.16-5）の手順を参照してください。

手順の概要

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

3. **[no] switchport uufb disable**
4. **show running-config vethernet** *interface-number*
5. **copy running-config startup-config**

手順の詳細

	コマンド	目的
ステップ 1	**config t** **Example:** n1000v# config t n1000v(config)#	CLI 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* **Example:** n1000v(config)# interface vethernet 100 n1000v(config-if)#	指定されたインターフェイスの CLI 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] switchport uufb disable** **Example:** n1000v(config-if)# switchport uufb disable n1000v(config-if)#	指定されたインターフェイスに対するユニキャスト パケット フラッディングのブロックをディセーブルにします。

ステップ 4	**show running-config vethernet** *interface-number*
	
	Example:
	n1000v(config-if)# show running-config interface veth100
	
	!Command: show running-config interface Vethernet100
	!Time: Fri Jun 10 12:43:53 2011
	
	version 4.2(1)SV1(4a)
	
	interface Vethernet100
	  description accessvlan
	  switchport access vlan 30
	  switchport uufb disable
	
	n1000v(config-if)#
		（任意）確認のため、インターフェイス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** **Example:** n1000v(config-if)# copy running-config startup-config [##] 100% n1000v(config-if)#	（任意）リブート後に永続的な実行コンフィギュレーションを保存し、スタートアップ コンフィギュレーションにコピーして再起動します。

不明なユニキャスト フラッディングを許可するようにポート プロファイルを設定する

VSM のフラッディングをグローバルにブロックした場合に、不明なユニキャスト パケットによる既存の vEthernet ポート プロファイルのインターフェイスのフラッディングを許可するには、次の手順を実行します。

はじめる前に

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。

- EXEC モードで CLI にログインしていること。
- グローバル設定に関係なく、不明なユニキャストが特定のポート プロファイルでブロックされていないことを確認するには、次の手順を実行します。
- すでに不明なユニキャスト パケットをグローバルにディセーブルにしている場合は、ポート プロファイルの 1 つのインターフェイスまたはすべてのインターフェイスでのユニキャスト フラッディングを許可できます。

  単一のインターフェイスでユニキャスト フラッディングを許可するには、「不明なユニキャスト フラッディングを許可するようにインターフェイスを設定する」（P.16-3）の手順を参照してください。
- フラッディングを許可する vEthernet ポート プロファイルを事前に設定しておきます。

手順の概要

1. **config t**
2. **port-profile** *profile-name*
3. **[no] switchport uufb disable**
4. **show running-config port-profile** *profile-name*
5. **copy running-config startup-config**

手順の詳細

	コマンド	目的
ステップ 1	**config t** **Example:** n1000v# config t n1000v(config)#	CLI 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	**port-profile** *profile-name* **Example:** n1000v(config)# port-profile accessprof n1000v(config-port-prof)#	指定されたポート プロファイルの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] switchport uufb disable** **Example:** n1000v(config-port-prof)# switchport uufb disable n1000v(config-port-prof)#	指定されたポート プロファイルのすべてのインターフェイスに対するユニキャスト パケット フラッディングのブロックをディセーブルにします。

	コマンド	目的

ステップ 4	**show running-config port-profile** *profile-name*
	
	Example:
	n1000v(config-port-prof)# show running-config port-profile accessprof
	
	!Command: show running-config port-profile accessprof
	!Time: Fri Jun 10 12:06:38 2011
	
	version 4.2(1)SV1(4a)
	port-profile type vethernet accessprof
	  vmware port-group
	  switchport mode access
	  switchport access vlan 300
	  switchport uufb disable
	  no shutdown
	  description all_access
	
	n1000v(config-port-prof)#
		（任意）確認のため、指定されたポート プロファイルの設定を表示します。

ステップ 5	**copy running-config startup-config** **Example:** n1000v(config-port-prof)# copy running-config startup-config [##] 100% n1000v(config-port-prof)#	（任意）リブート後に永続的な実行コンフィギュレーションを保存し、スタートアップ コンフィギュレーションにコピーして再起動します。

UUFB 設定の確認

次のコマンドを使用して、UUFB 設定を確認できます。

コマンド	目的
show uufb status	VSM の UUFB グローバル設定を表示します。
show running-config port-profile *profile-name*	特定のポート プロファイルの実行コンフィギュレーションを表示します。
show running-config interface vethernet *interface-number*	特定のインターフェイスの実行コンフィギュレーションを表示します。
vemcmd show port uufb-override	各ポートの UUFB のディセーブル状態を表示します。

UUFB の設定例

次に、VSM の転送パスがグローバルにフラッディングしないように不明なユニキャスト パケットをブロックする例を示します。

```
Example:
n1000v# config t
n1000v(config)# uufb enable
n1000v(config)# show uufb status
UUFB Status: Enabled
n1000v(config)# copy running-config startup-config
[########################################] 100%
n1000v(config)#
```

次に、VSM の UUFB をグローバルにディセーブルにした場合に、不明なユニキャスト パケットによる vEthernet インターフェイス 100 のフラッディングを許可する例を示します。

```
Example:
n1000v# config t
n1000v(config)# interface vethernet 100
n1000v(config-if)# switchport uufb disable
n1000v(config-if)# show running-config interface veth100

!Command: show running-config interface Vethernet100
!Time: Fri Jun 10 12:43:53 2011

version 4.2(1)SV1(4a)

interface Vethernet100
  description accessvlan
  switchport access vlan 30
  switchport uufb disable

n1000v(config-if)#
```

次に、VSM の UUFB をグローバルにディセーブルにした場合に、不明なユニキャスト パケットによる既存のポート プロファイルのインターフェイスのフラッディングを許可する例を示します。

```
Example:
n1000v# config t
n1000v(config)# port-profile accessprof
n1000v(config-port-prof)# switchport uufb disable
n1000v(config-port-prof)# show running-config port-profile accessprof

!Command: show running-config port-profile accessprof
!Time: Fri Jun 10 12:06:38 2011

version 4.2(1)SV1(4a)
port-profile type vethernet accessprof
  vmware port-group
  switchport mode access
  switchport access vlan 300
  switchport uufb disable
  no shutdown
  description all_access

n1000v(config-port-prof)#
```

その他の関連資料

UUFB の詳細については、次の項を参照してください。

- 「関連資料」（P.16-8）
- 「標準」（P.16-8）

関連資料

関連項目	参照先
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、使用上のガイドライン、例	『*Cisco Nexus 1000V Command Reference, Release 4.2(1)SV1(4a)*』
インターフェイス コンフィギュレーション	『*Cisco Nexus 1000V Interface Configuration Guide, Release 4.2(1)SV1(4a)*』
ポート プロファイル コンフィギュレーション	『*Cisco Nexus 1000V Port Profile Configuration Guide, Release 4.2(1)SV1(4a)*』
レイヤ 2 スイッチングの設定	『*Cisco Nexus 1000V Layer 2 Switching Configuration Guide, Release 4.2(1)SV1(4)*』

標準

標準	タイトル
この機能でサポートされる新規の標準または変更された標準はありません。また、既存の標準のサポートは変更されていません。	—

UUFB の機能の履歴

ここでは、UUFB のリリース履歴を示します。

機能名	リリース	機能情報
UUFB	4.2(1)SV1(4a)	この機能が導入されました。

CHAPTER 17

セキュリティ設定の制限値

表 17-1 に、セキュリティ機能の設定の上限を示します。

表 17-1　セキュリティ設定の上限

セキュリティ機能	最大制限	
アクティブな VLAN の数（すべての VEM の合計）	2048	
VEM 内の VLAN 上の MAC アドレス	32000	
VEM 内の VLAN 1 つあたりの MAC アドレス数	4000	
ACL	128	
ACL あたりの ACE	128	
	DVS あたり	**ホストあたり**
ACL インターフェイス	2048	256
NetFlow ポリシー	32	8
NetFlow インターフェイス	256	32
SPAN/ERSPAN セッション	64	64
ポート セキュリティ	2048	216
マルチキャスト グループ	512	512
Virtual Service Domain（VSD）	64	6
VSD インターフェイス	2048	216

INDEX

A

D

E

F

H

I

M

P

R

S

T

U

V

あ

い

う

お

か

き

く

け

こ

さ

し

せ

た

て

と

に

は

ふ

へ

ほ

ま

ゆ

り

ろ